Efficient and secure cryptographic solutions for medical data

Mohamad Noura

UBFC
UNIVERSITÉ
BOURGOGNE FRANCHE-COMTÉ

UFC
UNIVERSITÉ
DE FRANCHE-COMTÉ

THÈSE DE DOCTORAT DE L'ÉTABLISSEMENT UNIVERSITÉ BOURGOGNE FRANCHE-COMTÉ

PRÉPARÉE À L'UNIVERSITÉ DE FRANCHE-COMTÉ

École doctorale n°37

Sciences Pour l'Ingénieur et Microtechniques

Doctorat d'Informatique

par

MOHAMAD NOURA

Efficient and Secure Cryptographic Solutions for Medical Data

Solutions cryptographiques efficaces et sécurisées pour les données médicales

Thèse présentée et soutenue à Besançon, le 16 Juillet 2019

Composition du Jury :

SPITERI PIERRE	Professeur à l'ENSEEIHT, INP Toulouse	Rapporteur
BONFANTE GUILLAUME	Maîtres de conférence (HDR) à l'Université de Lorraine	Rapporteur
COUTURIER RAPHAËL	Professeur à l'Université Bourgogne Franche-Comté	Directeur de thèse
CHEHAB ALI	Professeur à l'Université Américaine de Beirut (AUB), Liban	Codirecteur de thèse

N° | X | X | X |

école doctorale **sciences pour l'ingénieur et microtechniques**

Titre : Efficient and Secure Cryptographic Solutions for Medical Data

Mots-clés : Soins de santé ; IdOM ; Cybersystème physique médical ; Dispositifs médicaux ; Algorithme de cryptage sélectif ou partiel ; Algorithme de cryptage complet ; Primitives de permutation et de substitution ; Analyse cryptographique ; Algorithmes cryptographiques légers, algorithmes cryptographiques dynamiques à clé dépendante ; Disponibilité, intégrité et confidentialité des données ; Sécurité et analyse des performances.

Résumé :

Dans cette thèse, des schémas cryptographiques efficaces et robustes ont été proposés pour surmonter les problèmes actuels de sécurité et de confidentialité des systèmes et applications médicaux récents. La principale contribution de cette thèse est d'atteindre un haut niveau de sécurité avec un minimum de surcoût de calcul contrairement à de nombreuses autres solutions existantes. Par conséquent, deux schémas de chiffrement et une approche de disponibilité des données ont été proposés pour les données médicales afin de garantir les services de sécurité suivants : confidentialité, intégrité et disponibilité des données ainsi que l'authentification de la source. Les solutions cryptographiques proposées sont basées sur les structures de chiffrement cryptographiques dynamiques pour assurer une meilleure résistance aux attaques existantes et modernes. De plus, ces solutions ont été conçues pour être légères et ne nécessitent qu'un petit nombre d'itérations. La fonction de chiffrement proposée n'est répétée qu'une seule fois et utilise une permutation de bloc dépendante de la clé. Elle satisfait également les propriétés de confusion et de diffusion requises, assurant ainsi les propriétés cryptographiques souhaitables. Les résultats de simulation et d'expérimentation ont démontré l'efficacité et la robustesse des solutions cryptographiques proposées. De plus, l'utilisation des schémas cryptographiques proposés ouvre la porte à des algorithmes cryptographiques dynamiques qui peuvent conduire à un gain de performance et de sécurité significatif par rapport à l'état de l'art.

Title: Efficient and Secure Cryptographic Solutions for Medical Data

Keywords: Healthcare; IoMT; Medical Cyber Physical System; Medical Devices; Selective or partial encryption algorithm; Full encryption algorithm; Permutation and substitution primitives; Cryptographic analysis; Lightweight cryptographic algorithms, Dynamic Key-Dependent cryptographic algorithms; Data availability, integrity and confidentiality; security and performance analysis.

Abstract:

In this thesis, effective and robust cryptographic schemes were proposed to overcome the current security and privacy issues of recent medical systems and applications. The main contribution of this thesis is to reach a high level of security with minimum possible overhead contrary to many other existing solutions. Therefore, two cipher schemes and a data availability approach were proposed for medical data to ensure the following security services: data confidentiality, integrity and availability as well as source authentication. The proposed cryptographic solutions are based on the dynamic cryptographic cipher structures to ensure a better resistance against existing and modern attacks. Moreover, these solutions were designed to be lightweight and they require a small number of iterations. The proposed ciphers round function is iterated only once and uses a key dependent block permutation. It also satisfies the required confusion and diffusion properties, consequently ensuring the desirable cryptographic properties. Simulation and experimental results demonstrated the efficiency and the robustness of the proposed cryptographic solutions. Furthermore, employing the proposed cryptographic schemes open the door to a dynamic cryptographic algorithms that can lead to a significant performance and security gain compared with other recent related state-of-art.

UBFC UNIVERSITÉ BOURGOGNE FRANCHE-COMTÉ

Université Bourgogne Franche-Comté
32, avenue de l'Observatoire
25000 Besanon, France

REMERCIEMENTS

A doctoral thesis is the result of a collective work, for this I would like to send my thanks to the following people : Pierre Spiteri, Professor at the ENSEEIHT and Guillaume Bonfante, Assistant Professor at Lorraine University, who honoured me to review and judge my thesis work.

I would like to express my sincere thanks to my thesis director, Professor Raphaël Couturier, at the UFC in addition to Professor Ali Chehab at American University of Beirut for having introduced me to the field of information security. Also for their competence, patience and for their valuable time throughout the thesis and to the correction of the writing.

My Directors at VAMED for making this thesis possible. I would also like to thank Dr. Hassan Noura for his advices, his support and assistance throughout the thesis. In addition, he supported me over the past few years and given me energy to continue in the most difficult times.

I also would like to thank my family, my friends and my colleagues for supporting me.

SOMMAIRE

I

Context and Problems

1

INTRODUCTION

Currently, traditional healthcare models face a challenge when dealing with the enormous increase in the number of patients as well as the recent technology revolution, thus, mandating a shift in the healthcare sector mindset. As such, it has become essential to benefit from modern technology in order to develop and enhance the services of the healthcare sector (called E-Health services).

E-Health services promise to initiate a revolution in the area of healthcare in general such as the reduction of the congestion in hospital emergency services, remote patient monitoring that can be performed via wearable sensors, hence offering an efficient and low-cost solution. The result is ongoing monitoring and care for patients, resulting in fewer visits to the doctor and helping to reduce the number of medical accidents that can threaten patients' lives. Technically, E-Health services can use a collection of medical devices and applications that connect to healthcare IT systems through secure networks. Medical devices allow machine-to-machine communication by using several wireless connection types such as WI-FI. Moreover, these devices transmit captured data to cloud platforms to be analyzed and stored.

E-Health systems face different security and privacy issues and challenges. In fact, the introduction of new technologies such as Internet of Things (IoT) led to new threats emanating from different sources, starting from attackers with malicious intents and ending with opportunists exploiting vulnerabilities in such systems to cause deliberate or accidental harm. Moreover, the cyber threat landscape has indeed evolved from individual hackers to highly organized criminal groups and advanced cyber-criminal syndicates, having healthcare as a major target. The nature of e-Health devices can be small with limited capabilities. This renders them an easy targets for cyber-attacks that can threaten the highly sensitive nature of the data carried by those simple devices.

Consequently, current research efforts are focused on ensuring a safe and secure deployment of e-Health systems, which will increase the confidence and acceptance of such services such as remote patient monitoring. This can be achieved by implementing the right and appropriate security measures to protect the privacy and security of patients' data.

E-Health applications are tightly linked to sensitive infrastructures. They handle sensitive information about patients, such as their locations and movements, and their general

state of health. The acceptance and wide deployment of E-Health applications will depend on the protection it provides to patients' privacy and the levels of security it guarantees. In addition, E-Health security and privacy requirements are expected to be more essential than those of conventional networked systems. Therefore it is clear that in the absence of robust and efficient security and privacy solutions, attacks may offset E-Health benefits and lead to dangerous consequences and as such, hinder its wide deployment.

Therefore, these healthcare technology advancements came side-by-side with privacy and security issues, due to the fact that these data are vulnerable to interception, and falsification through open networks. In this pursuit, the encryption scheme is mandatory to ensure the confidentiality of medical data for a secure transmission over the public networks. As result, security of medical applications have been increasingly studied in the last decade [Almohri et al., 2017, Kocabas et al., 2016].

To ensure security, two kinds of solutions are available : cryptographic or non-cryptographic algorithms.

Consequently, data protection requires cryptographic algorithms mainly to ensure data confidentiality, data integrity, source authentication and data availability security services in order to achieve secure storage and communication, especially during transmission over public networks.

In addition, confidentiality is generally ensured by the use of encryption algorithms, while a key hash function (or authentication mode) is required to protect against threats to data integrity and source authentication. Encryption can be performed at the block level or in stream mode. In stream cipher, data is mixed with a pseudo-random stream, while in block cipher, data is divided into blocks of fixed size (usually 128 bits). A block cipher employs a round function that is iterated r times on each block and it is a reversible function [Kwon et al., 2005].

Additionally, block cipher can be considered as a stream cipher when the block cipher is used to produce a keystream sequence, which is the case in OFB (Output Feedback) and CTR (CounTeR) operation modes [Dworkin, 2001]. The security in stream cipher is based on different metrics that depend on the quality of the produced keystream sequences, which should ensure high non-linearity, long periodicity and high randomness degree. Furthermore, KDF (Key Derivation Function) and PRNG (Pseudo Random Number Generator) can be based on block cipher, keyed or un-keyed hash functions as described in [Barker et al., 2012].

1.1/ Problem Formulation

Devices with good computational resources and reasonable memory capacity rely on traditional cryptographic algorithms to ensure the required security services such as data confidentiality, data integrity and source authentication. In general, confidentiality is based on Symmetric Key Cryptography (SKC) since it is more efficient than Asymmetric

Key Cryptography (AKC). The SKC Algorithms [Paar et al., 2009a] are based on a secret key shared between two entities and it consists of a cipher algorithm, a keyed hash function, such as HMAC (keyed-Hash Message Authentication Code), and a DPRNG (Deterministic Pseudo Random Number Generator). In addition, a Key Derivation Function (KDF) can be built based on a keyed hash function or a block cipher.

Subsequently, encryption of medical data such as images became mandatory to ensure data confidentiality to prevent eavesdropping attacks, in addition to protecting privacy. This is all the more necessary because medical images contain some patient information (visual and non-visual) in addition to meta-data. However, traditional symmetric-key cryptographic algorithms such as AES [Daemen et al., 2002b] requires multi-rounds and multi-operations (substitution and diffusion) for each round. Therefore, this kind of cipher may be inappropriate for multimedia content (medical images and video), due to the intrinsic features of frames, and the strong correlation among the adjacent pixels [Flayh et al., 2009]. Thus, offering a new kind of cipher structure to secure medical multimedia contents is necessary.

This thesis presents an overview of the existing cryptographic algorithms and explains its limitations. In fact, the static structure of the functions of the rounds used is the main cause of these problems because a large number of rounds and operations are required. This therefore introduces an additional cost in terms of latency and resources.

Alternatively, a new kind of cryptographic algorithm was presented and it is based on chaotic maps, which refer to non-linear dynamic system that can produce pseudo-random sequences or to produce substitution and diffusion primitives. As a result of this propriety, researchers have been investigating Chaotic Cryptography paradigm for the last two decades. Chaos theory proposes good properties for cryptography applications, mainly due to the extreme sensitivity of the initial conditions and parameters owing to the non-linear maps. These initial values could be set as secret keys for the cryptography applications based on chaos, which illustrates the role of chaotic maps with cryptographic applications. Moreover, chaos-cryptography was integrated extensively in order to build symmetric cryptographic algorithms with various applications to secure the digital images such as stream cipher scheme [Lin et al., 2018], block cipher algorithm [Wang et al., 2015b] and hash-encryption system [Li et al., 2016].

However, chaos cryptographic algorithms suffer from different security and implementation issues. Especially with digital images security, where recent algorithms have shown critical issues of resisting differential attacks which led to cryptanalyzed most of them [Li et al., 2011, Rhouma et al., 2010, Li et al., 2002]. Most of these issues are presented since the employed chaotic maps were 1-D and consequently have short periodic [Huang et al., 2009], and they are implemented with a finite computing precision. This makes the system vulnerable to reduce the length of generated sequence periodic which facilitates the tracking of different types of attacks [Arroyo et al., 2009, Alvarez et al., 2009]. In addition, iterating chaotic maps with float precision makes the practical real software or hardware implementation of these solutions very complex in term of efficiency.

1.2/ CONTRIBUTION

To overcome these limitations, this thesis proposes and recommends the deployment of the dynamic cryptographic algorithm structure to reduce the required round number and operations. However, designing dynamic cryptographic primitives with maximum cryptographic performances and efficiency is also reached with the proposed cryptographic variants. Moreover, the proposed dynamic key dependent cryptographic solutions are designed to reach a good balance between the security and performance level.

Firstly, we highlight all the above-mentioned security issues in details with full discussion in their emerging medical health-care such as IoMT. Then, we present the existing security solutions that are required to make these systems secure. However, these security solutions introduce an overhead, which can degrade the system performance. Then, we list the different issues of these security solutions.

The proposed approach ensures several contributions compared to the recent cryptographic schemes to reach a high level of efficiency and security. The main contributions of this thesis in terms of system performance and security level are summarized as follows :

SYSTEM PERFORMANCE

1. The proposed cryptographic algorithms are realized in the block level with a flexible size of blocks that can be adjusted according to the available memory, thus allowing the approach to be realized with tiny limited devices.
2. Efficient key dependent cryptographic primitives are built (with a substitution and permutation tables for cipher scheme, and an invertible diffusion matrix for the data availability scheme) that can ensure good cryptographic performances and can accomplish a good improvement in time and simplicity. This will reduce the time required in order to build these cipher layers and will simplify the hardware implementation. This is essential, since each primitive of these three has its effect and its role in making the proposed cipher scheme secure and efficient.
3. We propose two new cipher schemes that are based on the dynamic key dependent cipher approach. The proposed ciphers require to iterate a round function for only one round iteration with a minimum possible of simple operations compared to the majority of encryption schemes. This reduces the required delay and resources for each block of data.
4. In addition, the proposed algorithm ensures the avalanche effect with only one round since it is based on the dynamic key approach, where a new dynamic key is used for each input image. Moreover, the proposed cipher schemes can ensure a minimum error propagation.

SECURITY PERFORMANCE

1. The proposed cipher scheme presents an efficient collaboration scheme between substitution, byte and block permutation to ensure a high level of security and efficiency.
2. A block permutation operation is introduced to randomize the sequential order of chained blocks. This operation can make the procedure of possible future attacks

complex and consequently ensures a better security level compared to the existing cipher approaches that preserve the encryption sequential order. In addition, this step requires a lower latency overhead and will not degrade the previous performance contributions.

3. The dynamic key approach is used and the key can be changed for each fixed/chosen time (defined by an application or a user) or for each input image which will make the cryptanalysis task unfeasible. The attacker's task becomes more difficult because of the sensitivity of the unpredicted dynamic key especially if this dynamic key is changed for each input image. This will ensure a high level of security against the existing and modern powerful attacks since dynamic cryptographic primitives are unknown.

As a conclusion, the presented results of performance and security tests prove that the proposed approach is efficient and can ensure a high level of security compared to other recent image encryption algorithms that have static or chaotic structures.

Therefore, the proposed cipher can be considered as a good candidate since it ensures a good balance between system performance and security level. **Therefore, we think that the modern cryptographic algorithms should be based on the dynamic approach that can reach a good balance between efficiency and security.**

1.3/ ORGANIZATION

The thesis work is organized as follows :

In Chapter 1, we discuss the different security issues and challenges of E-healthcare systems such as the lack of security and privacy measures, in addition to the necessary training and awareness explained in detail. To enhance the defense level of IoMT against attacks, the right security measures and the required training skills should be applied. Consequently, existing security solutions are presented to make E-healthcare systems more secure and safer to use. In this chapter, the security solutions are divided into two classes : either cryptographic or non-cryptographic. Then, the different solutions are analyzed and compared in terms of computational complexity, required resources, and additional hardware. Unfortunately, ensuring security introduces a trade-off between the security level and system performance. In fact, new lightweight security solutions are required to reduce the delay and resources overhead. On the other hand, non-cryptographic solutions are presented and explained in details. We clearly indicate that there is a need to design an efficient intrusion detection/prevention system that cooperates with dynamic shadow honeypots. Moreover, different forensics issues surrounding the E-healthcare systems are explained. Afterwards, existing digital forensics solutions are also explained to preserve pieces of evidence. Finally, a security solution is proposed, which is divided into five different layers to detect and prevent attacks, in addition to reducing/correcting the damage of these known attacks and preserving the patient's privacy.

The second chapter is devoted to the design of selective medical encryption schemes.

To this end, we study the characteristic of medical images. First of all, we would like to remind you the existing ciphers, and especially the recent lightweight ones. Then, we present the proposed medical image encryption algorithms that require only one round to reduce the required delay and resources. Therefore, a high-security level is ensured, since each medical image is encrypted independently of previous and next images. Then, we quantify the cryptographic performance of cipher primitives, and consequently of the proposed cipher by using different cryptographic metrics such as linear and differential probability approximation, avalanche criteria, and key sensitivity. In addition, a set of performance metrics were used such as the execution time and error propagation. Based on the obtained results, the proposed one round cipher is efficient. Therefore, it can be considered suitable for real-time applications and tiny devices. Moreover, we propose a specific medical image encryption solution that defines three variants of the encryption algorithms(3) : **(a) full, (b) middle-full, and (c) selective**. The full approach encrypts all sub-matrices of a medical image, while the middle-full variant is a middle solution between the selective and full algorithms and its goal is to just hide the type of the medical image(s). Selective encryption identifies a set of sub-matrices of an image according to a statistical average test, known as the region of interest (ROI). The middle-full and selective variant reduces more and more the required latency and resources compared to the traditional full encryption scheme. Consequently, our proposed approach is flexible since it can be applied in either selective, middle-full, or full modes. Also, the size of a sub-matrix is variable and can be changed according to the available memory size.

In the third chapter, we focus on enhancing the first cipher and designing a newly secure and lightweight enhanced one round cipher scheme. In addition, we develop the different cryptographic primitives (layers) based on the key setup algorithm of RC4, which requires less computation complexity compared to the presented ones in the second chapter. Based on these cipher primitives, we then describe the proposed enhanced one round cipher, which uses primitives such as substitution and permutation tables. In fact, based on the obtained results, we can conclude that the second enhanced one round cipher scheme can also resist against data confidentiality attacks as it is more suitable for real-time applications and tiny devices compared to the first one.

The fourth chapter, presents the detailed structure and the study of a new medical data availability and protection scheme. This chapter defines a new data availability solution that is based on the secret sharing algorithm and especially the information dispersal one that can reach better performance compared to Shamir Secret Sharing. This solution will complete the previous cipher solutions to ensure data availability, data integrity source authentication in addition to data confidentiality for medical data. To do this, we first present the existing Information Dispersal Algorithm (IDA) variants and their properties. Then, based on the original IDA, we realize a very efficient AONT-IDA (AONT means All or Nothing Transform), using dynamic key dependent invertible IDA matrices. Let us indicate that a new lightweight information dispersal algorithm variant is presented and it is dependent on the dynamic key, which makes its corresponding structure variable and dynamic. This can consequently help with reaching a higher level of security. Several security and performance tests were realized to prove the effectiveness and the robustness of the proposed information dispersal variant. Finally, we present and analyze the performance of the proposed medical data availability-protection solution, before concluding on

this chapter.

2

Securing Medical Data and Systems : Limitations, Issues and Recommendations

ABSTRACT

Traditional health-care systems suffer from new challenges associated with the constant increase in the number of patients. In order to address this issue, and to increase the accuracy, reliability, efficiency, and effectiveness of the health-care domain, the Internet of Medical Things (IoMT) was proposed. IoMT can be considered as an enhancement and investment to respond more effectively and efficiently to patients' needs. However, IoMT suffers from different issues and challenges such as the lack of security and privacy measures, in addition to the necessary training and awareness. In this chapter, we highlight the importance of implementing the right security measures and the required training skills, in order to enhance the immunity of IoMT against cyber-attacks. Moreover, we review the main IoMT security and privacy issues, and the existing security solutions. These solutions are classified as cryptographic or non-cryptographic. Then, the different solutions are analyzed and compared in terms of computational complexity and required resources. It is important to note that the security measures for IoMT exhibit a trade-off between the security level and the system performance, especially in the rise of digital healthcare v4.0 era. Next, we discuss the appropriate security solutions such as lightweight cryptographic algorithms, and protocols that attempt to reduce the overhead in terms of computations and resources. This leads to the conclusion that there is a need to design an efficient intrusion detection/prevention system that cooperates with dynamic shadow honeypots. Finally, we propose a security solution, which is divided into five different layers to detect and prevent attacks, in addition to reducing/correcting the damage of these known attacks and preserving the patients' privacy. However, it should be noted that zero-day attacks and exploits are still the main challenging issue that surrounds IoMT.

2.1/ Introduction

The integration of medical devices within the Internet of Things (IoT) (see Figure 2.1), led to the emergence of the Internet of Medical Things (IoMT) [Balandina et al., 2015]. With the emergence of the new digitized healthcare era, called Healthcare v4.0

[Thuemmler et al., 2017, Pang et al., 2018], IoT devices were deployed in several medical domains, especially with the excessive use of medical wireless sensors, devices, Unmanned Aeria Vehicles (UAVs), and robots. In fact, medical sensors and actuators are used as wearable devices in the context of body area networks. Instead of keeping patients in hospitals, these devices are capable of constantly monitoring the patient's health in real-time, while offering them better physical flexibility and mobility. On the other hand, medical robots can also serve as surgical robots, as well as hospital robots [Beasley, 2012], which are capable of accurately performing small surgeries. They are also capable of performing several medical tasks such as Cardio-Pulmonary Resuscitation (CPR) [Rosen et al., 2006]. However, the main issue is that many IoMT devices are prone and vulnerable to cyber-attacks simply because medical devices are either poorly secured against potential adversaries, or not secure at all. Therefore, any cyber-attack can have drastic consequences, threatening patients' lives, which would hinder the wider deployment of IoMT.

Furthermore, IoMT applications are closely related to sensitive healthcare services, especially that they handle sensitive information about patients including their names, addresses, and health conditions. The main challenge in the IoMT domain is preserving the patient's privacy without degrading the security level. In addition, appropriate security and privacy solutions should include minimum computations and require minimal resources.

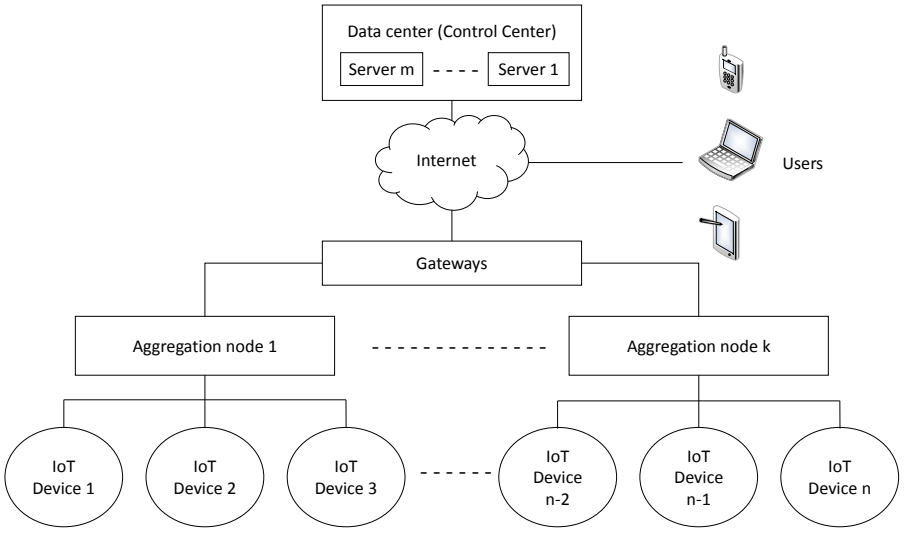


FIGURE 2.1 – An Example of Internet-of-Things System with n IoT Devices, k Aggregation Nodes & m Servers

2.1.1/ MOTIVATIONS & AIMS

Recently, medical IoT systems became among the most important advanced medical technologies. This technology can achieve a significant gain by enhancing the remote monitoring of medical services. Moreover, it can help in detecting any medical issue very early and thus, preserve patients' lives and health.

However, in the IoMT domain, many of the connected medical devices present security vulnerabilities that make them prone to malicious exploitation attempts. Such issues

may lead to drastic consequences, which would affect patients' lives by perturbing (or controlling) medical devices. Therefore, it is mandatory to overcome these issues to preserve the efficiency and accuracy levels of medical IoT systems.

On the other hand, the pervasiveness of medical sensitive data within IoMT systems makes them prone to advanced attacks (e.g. Ransomware) that target their main security aspects including privacy, integrity and confidentiality. This would severely impact the credibility, adoption, and wide deployment of IoMT systems.

Our aim, in this chapter, is to identify the main threats that may compromise the security of IoMT devices and systems, and to identify the necessary and appropriate measures that are essential for their security.

2.1.2/ Related Work

Medical IoT systems became core to the e-Healthcare domain whereby smart medical sensors and devices are installed to improve patients' lifespan and medical conditions. However, this domain came under a variety of attacks such as botnets targeting medical systems [Zhang et al., 2011], as part of targeted cybercrimes [Zhang et al., 2012]. In [Kumar et al., 2014a], IoT security and privacy issues were discussed but were not effectively linked to IoMT. Various intrusion detection [Mitchell et al., 2014, Zarpelão et al., 2017] and authentication/authorisation [Sey, 2018, Trnka et al., 2018] methods were presented to ensure a secure IoT environment with little notice to their application to IoMT. Moreover, only recently more work was directed to the security of healthcare systems. A generic survey on medical big data analysis was conducted in [Kuila et al., 2019] to sort big data issues and challenges of adopting IoMT solutions [Challoner et al., 2019], while an on-demand IoT adoption in hospitals was conducted in [Kang et al., 2019] to enhance nurses' experience based on the pros and cons of the IoT adoption in healthcare technologies [Adhikary et al., 2019]. In this chapter, we present a more detailed, holistic and analytical view point on the IoMT and healthcare domains, as well as the integration of cyber-physical systems within the medical field. All the mentioned cyber-attacks exclusively target healthcare systems, while the presented security measures are discussed in a way to ensure their adoption in such domains.

2.1.3/ Contributions

The novelty of the chapter stems from the fact that it includes a comprehensive overview and analysis of all security and privacy issues related to medical IoT systems. Also, the chapter discusses the recent lightweight security solutions, which consist of cryptographic and non-cryptographic techniques. Moreover, several lessons are learned from the overview and accordingly, several recommendations are proposed towards making medical IoT systems secure and safe to deploy and use.

More specifically, the contributions of this chapter can be summarized in the following points :

- **Perspective & Future Trends** of IoMT systems are presented, including their communication types, device types, and applications.
- **Benefits** of IoMT systems and applications are presented and discussed.

— **Concerns & Risks** are highlighted, especially in terms of public and privacy concerns, while risks are presented and evaluated through a proposed qualitative risk analysis method.
— **Attack Sources & Characteristics** are presented and discussed in details, including their scope and impacts.
— **Cyber-Attacks** are presented per security breach, while exploring malware and code injection attacks. Moreover, real-case cyber-attacks are also presented.
— **Security Measures** including technical and non-technical ones are presented, evaluated and analysed especially in terms of their advantages and limitations.
— **Suggestions & Recommendations** are presented based on the conducted research for a much more efficient and secure IoMT environment.

2.1.4/ ORGANIZATION

This chapter is divided into seven sections, in addition to the introduction, which sheds light on the digitization era of healthcare v4.0. Section 2.2 presents and details the main IoMT communication protocols and application domains. Section 2.3 highlights the main IoMT challenges, constraints, concerns, and risks, while presenting a qualitative risk assessment. Section 2.4 presents and discusses the most recurring cyber-attack types against IoMT main security goals, including real-case cyber-attacks against well-known hospitals in the United Stated (US) and the United Kingdom (UK). Section 2.5 presents various technical and non-technical security measures that are suitable for protecting the IoMT and e-Healthcare systems, communication and devices, along with their advantages and limitations. Section 2.6 presents the most valuable lessons learnt from this survey. Section 2.7 highlights this chapter's main suggestions & recommendations which include the adoption of lightweight cryptogprahic solutions, hybrid and dynamic non-cryptographic solutions, and finally the implementation of artificial intelligence for a higher accuracy and in a real-time. Section 2.8 concludes the presented work with some prospects on future work.

2.2/ IOMT BACKGROUND, PERSPECTIVE & FUTURE

In this section, the main communication types used in IoMT are presented, in addition to the different types of medical devices, as well as the benefits offered by IoMT systems. Moreover, the future prospects of IoMT are also highlighted and presented in FIGURE 2.2.

2.2.1/ IOMT COMMUNICATIONS

Real-time data transmission among medical devices takes place via four main communication networks types. These types include Body Area Networks, Home Area Networks, Neighbourhood Area Networks, and Wide Area Networks.

— **Body Area Network :** A Body Area Network (BAN) is a network medium for the transmission of patients' vital signals, which are measured by either a wearable or a portable sensor. In [Kocabas et al., 2016], Kocabas et al. stated that the communications between medical devices can be secured using biomedical signals. The-

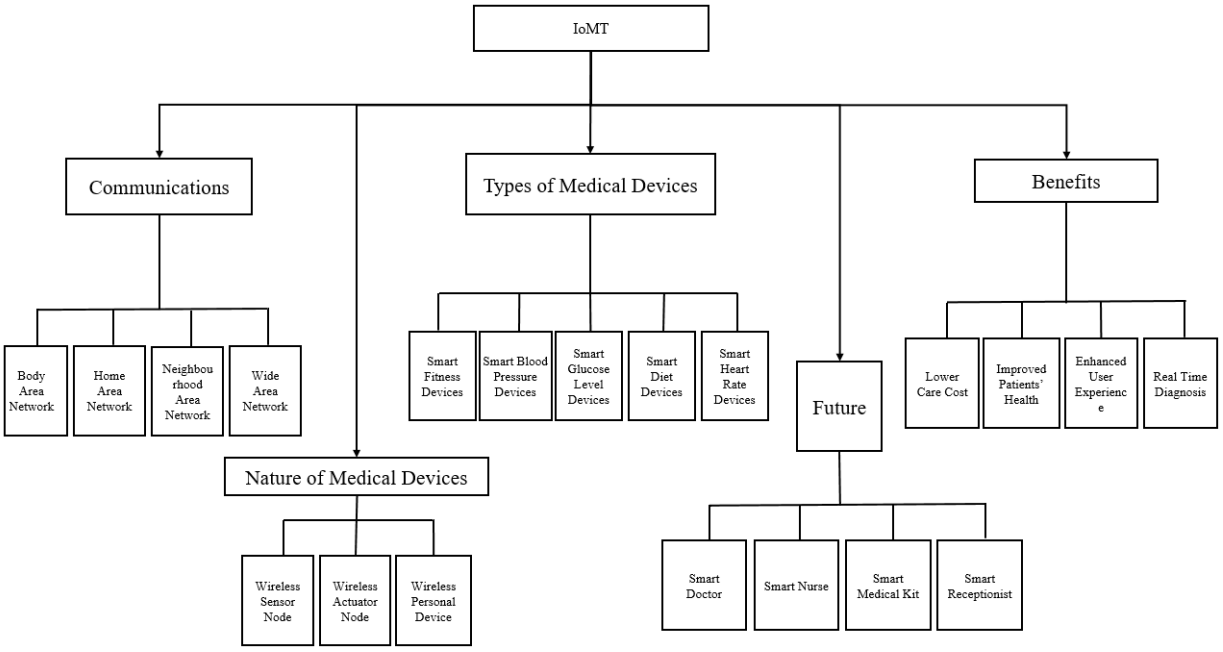


FIGURE 2.2 – IoMT's Communication, Perspective & Future Taxonomy

refore in [Poon et al., 2006], Poon et al. presented a low-power bio-identification mechanism by using an Inter-Pulse Interval (IPI) to secure the communication between Body Area Network sensors. In [Venkatasubramanian et al., 2010], Venkatasubramanian et al. managed to use a physiological signal that agrees over a secret key of the symmetric key cryptosystem for BAN sensor communications. As a result, the collected medical data is sent to the controller in two different ways :

- **Smart-Phone :** transmits the collected data via a mobile network to the base station (BS) that routes it until it reaches the medical data center.
- **Wireless Medical Device :** (see FIGURE 2.3) transmits data using one of several wireless communication protocols such as Zigbee [ZigBee, 2006], Bluetooth [Bhagwat, 2001], or Wi-Fi [Alliance, 2010].

— **Home Area Network :** A Home Area Network (HAN) uses a controller, which handles the communication for sending the gathered data to an available Access Point (AP) located in the patient's home. Transmissions can rely on Wi-Fi, or LTE/LTE-A [Doppler et al., 2009] in case of a Femtocell AP [Chandrasekhar et al., 2008].

— **Neighbourhood Area Network :** A Neighbourhood Area Network (NAN) enables users to quickly connect to the Internet [Ye et al., 2015]. It is used to establish wireless communication between close areas such as homes and their neighbourhoods. It can be based on an omnidirectional antenna that allows a single AP to cover a radius of at least half a mile. Moreover, a NAN can rely on a directional antenna to improve the AP's signal as shown in FIGURE 2.4. As such, the AP forwards the data to a mobile data station, which allows the data sent from the home's AP to be directly received at the mobile Base Station (BS).

— **Wide Area Network :** A Wide Area Network (WAN) represents the communication from a mobile Base Station or from an access point to the mobile/Internet (remote) medical infrastructure. In case of emergencies, a WAN ensures real-time data transmission to emergency response teams. Once the data is received, the

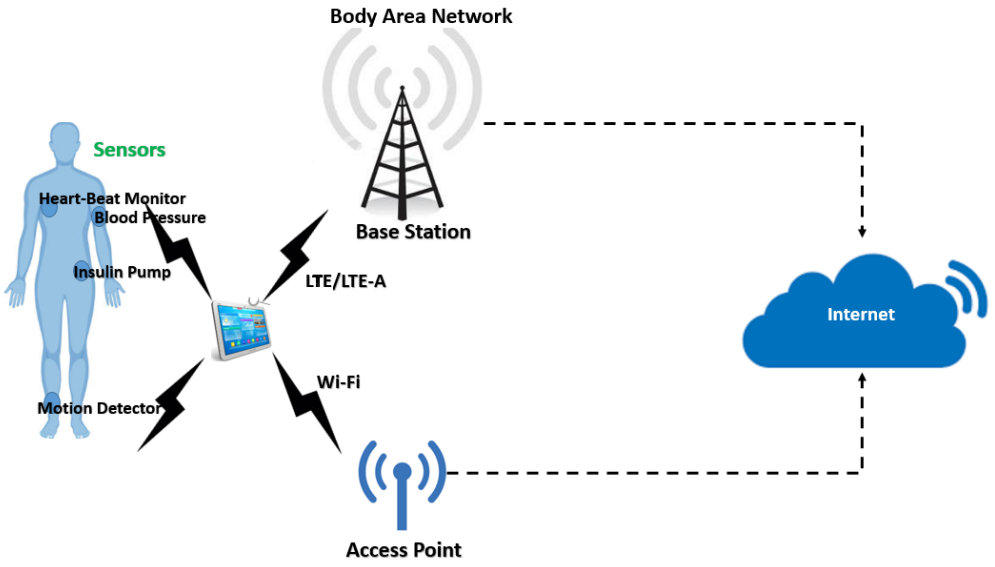


FIGURE 2.3 – Body Area Network

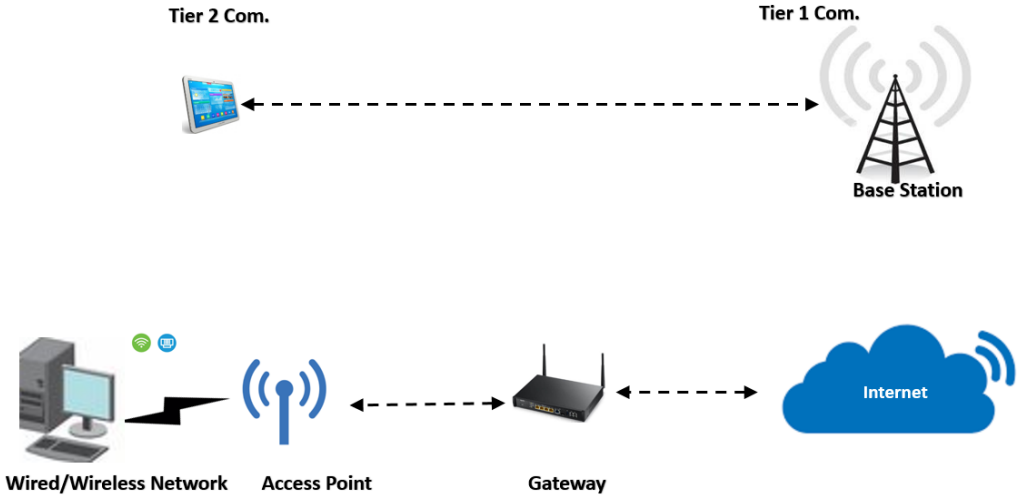


FIGURE 2.4 – Neighbouring Area Network

AP can also send the data to cloud services for storage at the specified server.

2.2.2/ IOMT DEVICES & PROTOCOLS

Medical devices are differentiated according to their needs. In fact, many of them are available as a gadget in the medical market, or are being used by hospitals for real-time smart remote monitoring. These smart medical devices can range from fitness devices, to blood-pressure devices, to sugar-level devices. A set of these medical devices is listed in TABLE 2.2.

Given that the aging population in developed countries is growing, there is a need for a much more sophisticated and suitable health-care system. The recent IoMT technology

is considered as one of the most important solutions, which was introduced to answer the growing needs and demands. IoMT ensures physical mobility for patients, which leads to the reduction of the number of patients in a hospital performing Blood Pressure (BP) tests, or a Cardio-Vascular Disease (CVD) tests, which constitute 30% of global death, as stated by the World Health Organization (WHO). Moreover, diabetic cases can now be remotely monitored from hospitals.

These devices can be either implanted, worn, or held. Moreover, some devices can be used in-home and others are specialized and to be used in hospitals and clinics. In the following, we give examples of such devices. The different protocols supported and employed to (inter-)connect such devices are listed in TABLE 2.1.

TABLE 2.1 – A set of protocols used for IoMT interconnection

Protocol	Classification	Range	Description
4G or LTE	Wireless	Medium Range	Cellular Technologies that Connects Medical Personal and Wearable Devices
Wi-Fi, 802.1x	Wireless	Medium Range	Reliable, Real-Time, High Power and Long Range Medical Connection
Zigbee	Wireless	Medium Range	Used for Low Data Rate Medical Connections with Minimum Latency & Energy Consumption
Z-Wave	Wireless	Medium Range	Used for Low Data Rate Medical Connections, include Sending Alerts & Tele-Home Healthcare (Remote Monitoring)
Bluetooth	Wireless	Short Range	Used for Short Range Connection to a Nearby Medical Device including Smart Medical Sensors
6LoWPan	Wireless	Medium Range	Used for Medical Low Power Wireless Personal Area Networks
Machine-to-Machine (M2M)	Wireless	Long Range	Real-Time Remote Patient Monitoring & Error Detection, Enhanced Patient Care & Attention
Internet Protocol (IP)	Wireless	Long Range	Software Responsible of IoMT and E-Healthcare Communications

— **Wearable and Personal Devices :** these include smart and electronic medical devices that collect, monitor and improve patients' health conditions in a real-time manner, and at a reduced cost [Wang et al., 2015c]. Wearable devices include fitness trackers, smart health watches, wearable Blood Pressure Monitors (BPM), ring-type heart rate monitor and biosensors [Koydemir et al., 2018, Hiremath et al., 2014]. Due to the increase in the number of ageing population and spread of diseases, there is even a higher demand for tele-home healthcare. In the following some of these devices are described in detail.
  — **Smart Fitness Devices** are used to maintain a healthy lifestyle for patients and to improve their health conditions. This is achieved by adopting a daily workout routine, which varies and depends on the patients' ability and physical status, along with their condition, age and gender. Several additional smart fitness devices were mentioned in [Naditz, 2009], including "TomTom Spark 3", which is a fitness tracker and "on-wrist navigator" [Yuen et al., 2017] and "Moov Now", which is also a fitness tracker [Pinto et al., 2017].

- **Smart Blood-Pressure Devices** are deployed in many IoMT fields and domains. They are used to remotely and continuously monitor the blood pressure of patients. These devices check for deviations in blood pressure from the norm towards detecting rapidly any anomaly and transmitting the data in real-time. A set of such devices includes "Omron EVOLV" [Asmar, 2017], "iHealth Feel & View BPM" [Kasl et al., 1966] and "Philips Upper Arm BPM" [Nijboer et al., 1988].
- **Smart Glucose-Level Devices** are used to monitor and to track the real-time sugar levels of patients who suffer from diabetes types I and II. They help in maintaining the right insulin level to protect the patients. This reduces the implications and risks associated with unexpected higher or lower levels of insulin. Examples of such devices include the GlucoWise device [Aggidis et al., 2015], in addition to turning a given IoT device (mainly smartphones) into a blood sugar meter sensor [Swan, 2012], and iBGStar Blood Glucose Meter [Tran et al., 2012]. In case of an insulin drop, signals are sent to the actuators of the insulin pump to inject the appropriate insulin dose. Another actuator example is the spinal cord stimulator, which is implanted in the patient's body to ensure long-term pain relief [Krames, 2002].
- **Smart Heart-Rate Devices** are used in several medical domains and they are capable of saving patients' lives. A set of k devices can monitor patients' heart rates in real-time, while other devices communicate only urgent data, when an anomaly is detected. As such, the main task of these devices is to predict any possible heart-attack before it occurs. These devices may include wearable wireless sensor networks and BANs [Wang et al., 2017], along with different heart-rate monitoring devices [Komulainen, 2001].
- **Smart Diet Devices** are being used to maintain a healthy diet for patients who mainly suffer from eating disorders. They are specifically used by obese people who struggle in following a certain diet or sometimes forget about diet restrictions. In fact, smart diet devices have become a substitute for paper-written diets. Such devices would send users automatic updates about their daily diets, with different nutrition ingredients, via a smart diet software [Marrow et al., 2001].

- **In-home Medical Devices :** these include ventilators, infusion pumps, and dialysis machines that are currently being used outside the hospital or clinic, which are also provided by a health care professional, and rely on simple technologies (e-mail, the Internet, smart medical devices) to communicate with the hospital [Hung et al., 2004]. Among these devices, we mention test kits, first aid equipment, durable medical equipment, feeding equipment, voiding equipment, treatment equipment, respiratory equipment, infant care, and other equipment which are further discussed in [Council et al., 2010].
- **In-Hospitals and Clinics Medical Devices :** hospitals must always be prepared for any emergency or incidence, whether or not these are life threatening. As such, a high level of readiness of both medical equipment and staff is a must to offer the right treatment for patients. In this context, medical donations play a crucial role [Perry et al., 2011]. Among such medical devices we list defibrillators, anesthesia machines, patient monitors, Electrocardiogram (EKG) Machines [Bio, 2019], surgical tables, blanket and fluid warmers, electro-surgical units, surgical tables and lights, which are further discussed in [10P, 2017].

TABLE 2.2 – A set of medical IoT applications [Ullah et al., 2012]

Application	Data rate	Bandwidth (Hz)	Accuracy (bits)
ECG (12 leads)	288 kbps	100–1000	12
ECG (6 leads)	71 kbps	100–500	12
EMG	320 kbps	0– 10,000	16
EEG (12 leads)	43.2 kbps	0–150	12
Blood saturatio n	16 bps	0–1	8
Glucose monitoring	1600 bps	0–50	16
Temperature	120 bps	0–1	8
Motion sensor	35 kbps	0–500	12
Cochlear implant	100 kbps	70-350/3500-8500	16
Artificial retina	50-700 kbps	¡10	12

2.2.3/ IOMT APPLICATION DOMAINS

Despite the challenges that surround the IoMT domain, this technology offers several advantages via health-care applications [Suvarna et al., 2016]. First, and since the vital signs of a patient could be monitored in real-time, this allows patients and the medical staff to communicate instantly. This reduces the cost of medical care by reducing the number of doctor visits. Improving patients health and lifestyle is another benefit of IoMT. The immediate access to a patient vital signs allows the early diagnosis, the prescription of medication and the injection of medication via a wearable device.
The future of IoMT aims at further involving devices and applications in the roles of doctors, nurses, medical kits and receptionists. However, the general public still has concerns about the necessary security, privacy, trust and accuracy of such IoMT systems.

— **Smart-Doctor :** One of the future plans is to introduce the concept of smart-medical robots to perform the role and tasks of a real doctor. Some patients have expressed concerns regarding this matter while others felt more comfortable speaking to a robot doctor about their private medical issues than they would with a real doctor. Despite the opposing views, in the near future, the term smart-doctor will be frequently heard and used.
— **Smart-Nurse :** Smart-medical robots will also be able to perform secondary medical tasks such as taking the role of a nurse. In many cases, they may perform the task of a smart-assistant to a given nurse to facilitate the nurse's tasks. The plan is to rely on robots to perform a secondary or/and supportive medical task, according to the medical conditions and needs.
— **Smart-Medical Technology :** It includes Smart medical equipment and kits that are currently being deployed and used by paramedics to provide immediate help to patients who are in urgent need of medical care and assistance. One example is the use of of medical drones to perform such a task [Haidari et al., 2016]. Medical drones were originally introduced to respond to emergencies related to patients suffering from cardiac arrests [Pulver et al., 2016], since these drones are the fastest to arrive at the emergency scene. The drones would be directed to fly

to specific destinations, which saves time and as such, saves lives since paramedics might end up stuck in traffic, and may not be able to respond as quickly as needed. This encourages the reliance on smart medical robots [Li et al., 2004] to perform surgical operations within a hospital setting. Virtual/Augmented Reality and Artificial-Intelligence (AI)-based medical technologies were also employed for various medical purposes. This includes Virtual-Reality to perform various realistic operations such as simulated training [McCarthy et al., 2019], emergency training [Munzer et al., 2019], and Cardio-Pulmonary Resuscitation (CPR) training [Balian et al., 2019]. AI-based medical technologies are also being used to ensure a higher accuracy rate [Jiang et al., 2017]. This includes exploring bio-chemical interactions [Hunter, 2016], such as IBM Watson and Gene Network Sciences (GNS) Healthcare AI systems [Shah et al., 2019] used to search for the right cancer treatment [Agrawal, 2018].

— **Smart-Receptionist :** A smart-receptionist is yet another trend in the IoMT domain ; a medical robot is capable of operating as a normal receptionist, having the ability to “think” and “understand” a given medical, or urgent case before diverting the patient towards the right medical department. Also, these robots would answer phone calls and book appointments for patients, whilst classifying the urgent and normal appointments. Such a classification could be based on statistical or machine-learning algorithms.

— **Personal Emergency Response Systems (PERS) :** these are seeing increasing use to alert patients and doctors in a real-time manner of any patient’s abnormal medical event (E.g stroke, cardiac arrest, seizure etc.) by remotely sending vital signals to the hospital [Tran, 2013] based on a predictive risk assessment method [Pauws et al., 2017]. PERS are now being modified to become location-based [Peabody, 2012] for a higher accuracy and faster response time. A typical example is the Active-Protective’s smart belt which can be placed on a patient’s waist and uses Bluetooth and AI to transmit real-time data.

— **Ingestible Cameras :** these are cutting-edge and cost-effective capsules that can be swallowed (in-vivo/in-vitro) by a patient to provide internal-organ real-time visual monitoring for early detection of chronic diseases and cancer [Kiourti et al., 2014]. Many ingestible devices were presented including Swallow-able data recorder capsule medical device [Marshall, 2003], ingestible endoscopic optical scanning device [Bandy et al., 2013], and ingestible hydrogel device [Liu et al., 2019]. Ingestible devices rely on an X-ray or camera capsule, a tracking/recording system and the diagnostics toolkit for evaluation.

— **Real-Time Patient Monitoring (RTPM) :** this is a new evolving trend among the new generation, including millennials, due to their heavy reliance on smart devices as a key part of their daily lives [Toohey et al., 2016]. In fact, RTPM is used to ensure a real-time, cost-effective remote consistent monitoring depending on the sensors linked to the patient’s body, either through a homecare telehealth systems [Santoso et al., 2015, McFarland et al., 2019] or telecare monitoring systems [Cullin et al., 2019, Saeed et al., 2019]. This may include monitoring fitness level, glucose level, respiration rate, and heart rate, etc. Many new RTPM trends are now available including, but not limited to, connected inhaler delivery systems, Apple Watch app that monitors depression, Apple’s Research Kit and Parkinson’s Disease and ADAMM intelligence Asthma Monitoring [Anderson et al., 2016, Kang et al., 2018] .

As listed above, IoMT will enable innovative healthcare applications ; however, there are

many challenges that might hinder the evolution of this technology. One of the key challenges is related to the security and privacy issues. In the next section, we discuss the main security concerns, challenges, and risks that might be associated with the deployment of IoMT systems.

2.3/ CONCERNS, CHALLENGES & RISKS

In this section, we highlight the main concerns that are related to IoT systems, in general, with emphasis on medical issues.

2.3.1/ IOMT CONCERNS

IoMT-related concerns can be classified into four key categories, one of them is raised by the general public and is related to the security, privacy, trust and accuracy issues.

— **Security Concerns :** Due to the reliance of IoMT devices on the use of open wireless communications, these devices are prone to various wireless/network attacks. In fact, an attacker can eavesdrop and intercept incoming and outgoing data and information due to the lack of security measures that most IoMT devices either suffer from by design, or due to weak security authentication measures that can be easily bypassed by a skilled attacker. Another security issue is the ability to gain unauthorized access, without being detected, due to the inability to detect and prevent such attacks. This would result into gaining an elevated privilege, injecting malicious codes, or infecting devices with a malware. On the other hand, IoMT devices could be hijacked (as botnets) and used to launch Distributed Denial of Service (DDoS) attacks. In [Clark et al., 2017], Clark et al. showed how medical devices are prone to botnets or “zombies” attacks, which can lead to physical attacks on human patients. An attack, for example, can logically manipulate a drug dose that would kill or have serious health implications on a given patient. Moreover, IoMT devices, when hijacked by terrorists, could be used as a mean for targeted assassination. For this reason, the US Vice President, Dick Cheney, disabled the wireless functionality of his heart implant out of fear of being hacked to eliminate him [Peterson, 2013]. Moreover, as described in [Clark et al., 2017], IoMT devices can have a negative effect on the psychological state of patients, since these can potentially scare patients, causing them to suffer from a heart-attack due to being surrounded by machines instead of humans.

  Manufacturers of medical devices need to focus on security as a primary task to ensure and maintain the security of the Medical-Cyber Physical System (MCPS), along with medical systems and devices alike. In other terms, protection against passive and active attacks is a must to mitigate the main IoMT security concerns. Hence, the need for the right security measures and tools is crucial.

— **Privacy Concerns :** Passive attacks such as traffic analysis leads to privacy issues since it would be possible to gather and disclose information about patients’ identity, in addition to sensitive and confidential information.
  This is a very serious threat for patients since an attacker is capable of identifying his/her medical records and medical conditions, which poses drastic life-

threatening effects on patients.
Another reason for breaching the privacy of patients, through attacking hospitals, is identity theft. Most of these real-case attacks led to a breach of patients' privacy either through the leakage, or through the disclosure of personal/sensitive information.
As a summary, privacy is more than ensuring the secrecy of sensitive and private medical information. It also entails the need for anonymity, non-linkability, and non-observability.

- **Anonymity :** a patient should not be identifiable ; when a patient is in communication, his identity should be kept hidden. In other terms, passive attacks can see what you do, but not who you are.
- **Non-Linkability :** Items of Interest (IoI) such as subjects, messages, events, actions should not be disclosed by passive attacks. This means that the probability of those items not being exposed from the attacker's perspective should stay the same, before and after observation.
- **non-Observability :**
  non-observability is the state of Items Of Interest (IoI) being indistinguishable from any IoI of the same type. This means that messages are not discernible from any random noise(s). In other words, it should not be noticeable whether, a message has been exchanged between a sender/receiver in any relationship.

- **Trust Concerns :** The breach of patients' privacy translates into serious trust issues. Patients are becoming skeptical of the idea of machines taking over the roles of humans (doctors, nurses, and receptionists). As a result, people are more concerned about having a medical robot, or a medical machine, or even a medical device monitoring and controlling their health conditions [Kelly, 2012].
- **Accuracy Concerns :** This type of concern has surfaced after more than 144 patients in the U.S. lost their lives [Birkmeyer et al., 2003] due to accidental mistakes related to medical robots' lack of accuracy and diagnosis. This also resulted into having more than 1,400 patients being partially or permanently injured, where reports of malfunction revealed that more than 8,061 malfunctions have occurred within thirteen years (2000-2013) [Ayala, 2016]. Another example is the false diagnosis of some patients as having dementia or Alzheimer. These incidents indicate the lack of accuracy and precision in the operations being led by medical robots, along with the false diagnosis of patients, and wrong medical prescriptions [Sensmeier, 2017].

2.3.2/ IoMT Challenges

IoMT challenges emerged as soon as the integration of medical devices into IoT systems started. One major challenge is the lack of standardization. In [Hassanalieragh et al., 2015], Hassanalieragh et al. discussed in details the main IoMT challenges. The issue of standardization is essential to having different medical devices operating together, and for vendors to adopt the right security measures to protect them from being hacked. This would lead to higher protection, efficiency, scalability, consistency, and effectiveness. In fact, many of these challenges are mainly related but not limited to various IoMT security constraints (see Figure 2.5).

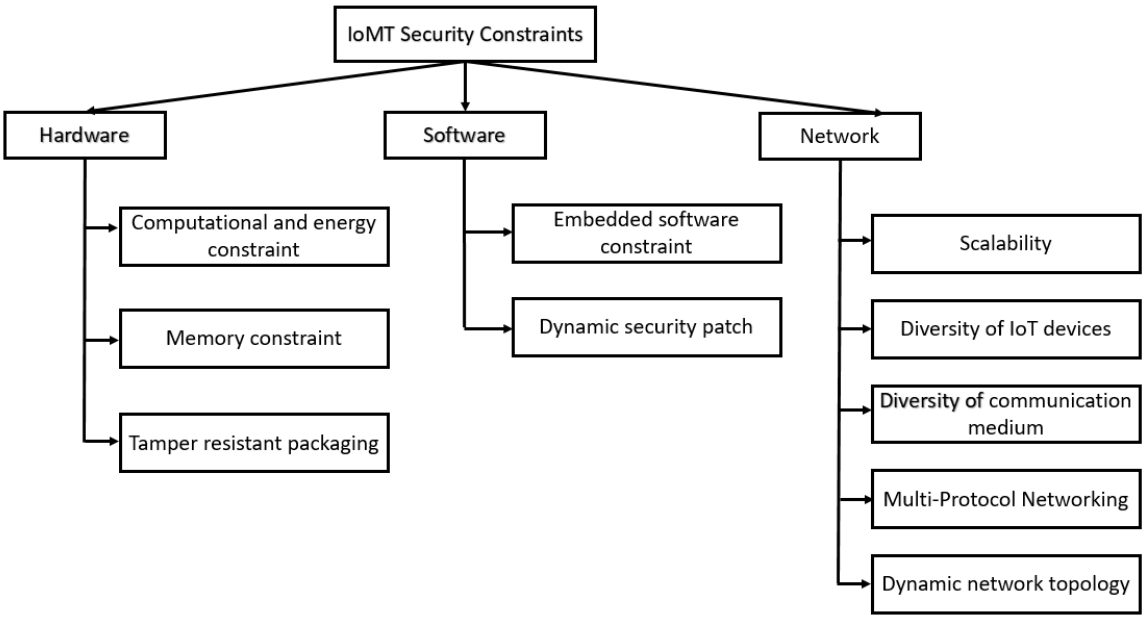


FIGURE 2.5 – IoMT Security Constraints

2.3.3/ IOMT RISKS

The deployment of IoMT systems into the healthcare domain is associated with a number of risks which are listed as follows :

- **Disclosure of Personal Information** can seriously affect patients' medical conditions, as well as hospital's reputation.
- **Data Falsification** can result into having the transmitted data from any medical device altered and modified, which would result into a higher drug dosage or wrong medical description that can lead to further medical complications.
- **Whistle-blowers** are based on unsatisfied or rogue medical employees leaking medical details and information about the hospital or patients by either being bribed, or part of an organised crime activity, risking patients' privacy and lives.
- **Lack of Training** among nurses and doctors can result into risking patients' lives with permanent disabilities or the loss of life.
- **Accuracy** is still a debatable issue and is still responsible for inaccuracies in the medical operations conducted by specialised robots. This can also seriously affect patients' lives and lead to disabilities or fatalities.

Thus, a new risk assessment method is required to quantify the security risks of IoMT attacks, which is a complicated task. Addressing threats in IoMT and analyzing their associated risks is the first step towards identifying the required security solutions to be adopted by IoMT applications and communication protocols. The risk analysis, presented in [Turner et al., 2013], is based on Threat, Risk, and Vulnerability Analysis (TVRA) methodology [Moalla et al., 2012]. This methodology is based on the likelihood of a given attack, and the attack impact on the system including the system assets and its associated threats. In addition, the threat agent which is trying to break the system is also identified by the TVRA method. Therefore, the outputs of TVRA are measures of the risk of the already identified threats and can be determined based on their estimated value of likelihood and impact on the system. The existing threats can be ranked as either critical,

major, or minor, and they are represented in TABLE 2.3, depending on their impact on human emotional conditions, which should also be taken into consideration.

In fact, given the above listed concerns, challenges and risks, it is essential to review the possible security attacks and their causes. Thus, in the next section, we give a detailed description of the attack types, causes and effects.

2.4/ CYBER-ATTACKS AGAINST IOMT

Such attacks can either be targeted, organized or even coordinated, based on the attackers' skills, experience, knowledge, and tools in order to carry out a successful cyber-attack. These attacks target the confidentiality, integrity, availability and/or the authentication of a given system and/or its components. In fact, it depends on the malware type used in order to carry out the attack.

2.4.1/ CHARACTERISTICS OF CYBER-ATTACKS

Before identifying and classifying a given attack, it is important to understand its characteristics. In general, any attack can be classified as one of five main categories (see FIGURE 2.6), based on its nature, target, scope, capacity, and impact, all of which are directly related to the attacker's purpose, aim, objectives and goals. More precisely, it depends on the attacker's skills, knowledge, experience, available tools and resources at his disposal.

- **Attackers' Nature :** There are four categories of attackers, internal, external, passive and active attackers. In some cases, different types of attackers may collude to ensure a more sophisticated cyber-attack.
  - **Internal & External Attackers :** An ***internal attacker*** is mainly a rogue employee who can be a nurse, a doctor or a medical staff who wants to cause damage to a hospital by damaging its reputation via removing or modifying data, or targeting patients' health and privacy. In some cases, it can be a spy masqueraded as a nurse or a doctor who managed to successfully evade all the security measures of a given hospital to eliminate a given patient for either political or other criminal purposes. Internal attackers might pave the way for external attackers to perform their cyber-attacks easily.

    External attackers are mainly classified as malicious hackers who aim at gaining an elevated unauthorized privileged access into the hospital's system. This is mainly achieved through worms, Rootkits, or Remote Access Trojan attacks. In many cases, the attack is based on spear-phishing techniques through sending a malicious Portable Document Format (PDF) file, or any other file as a Curriculum Vitae (CV). Once downloaded, a backdoor or a key-logger will be installed on the given system. The main aim is to breach the privacy of patients and sell them to malicious third parties through the deep dark web for scamming purposes.
  - **Passive & Active Attackers :** A ***passive attacker*** tries to evade detection by remaining ”hidden” in the background, without making any activity. The aim here is to intercept data, transmitted via any wireless communication, between

TABLE 2.3 – **Qualitative Psycho-Emotional Medical Risk Assessment**

Threat	Nature		Motivation		Risk		Emotional/Psychological Impact							
Type	Human	Non-Human	Malicious	Non-Malicious	Likelihood	Impact	Anger	Fear	Mistrust	Sadness	Depression	Anxiety	Guilt	Embarrassment
Medical Information Disclosure	Yes/No	No/Yes	✓	X	High	High	Yes	Yes	Yes	Maybe	Maybe	Yes	Maybe	Yes
Medical Data Manipulation	Yes	No	✓	X	High	High	Yes	Yes	Yes	No	No	No	Yes	No
Medical Data Interception	Yes	No	✓	X	Moderate	High	Yes	Yes	Yes	No	No	Maybe	No	Yes
Medical Data Hijacking	Yes	No	✓	X	High	High	Yes	Yes	Yes	No	No	Yes	No	Yes
Medical Data Exposure	Yes/No	No/Yes	✓/X	X/✓	Low/Moderate	Moderate/High	Yes	Yes	Yes	Maybe	Maybe	Yes	No	Yes
Wrong Dosage	Yes/No	No/Yes	✓/X	X/✓	Low/Moderate	High	Yes	Yes	Yes	Yes	No	Maybe	No	No
Medical Data Delay	Yes/No	No/Yes	✓/X	X/✓	Moderate	Moderate/High	Yes	No	Maybe	No	No	No	No	No
Insiders	Yes	No	✓	X	High	High	Yes	Yes	Yes	No	No	No	No	Yes
Misconfiguration	Yes/No	No/Yes	X	X	Low	Moderate	Maybe	Maybe	Yes	No	No	No	No	Maybe

different medical devices, read them and build up their own information gathering process that can be used for further exploitation, which may lead to a much more sophisticated cyber-attack. Passive attackers can be cooperating with external or even internal attackers as part of the information gathering process.

Unlike a passive attacker, an ***active attacker*** relies on intercepting the communication between a given source and destination. Such interception is done aggressively by altering, modifying and deleting the given information and data being transmitted without the knowledge of the source and destination. Such an attack is very dangerous when used for example to inject a patient with a higher dosage of a drug, or when prescribing the wrong drugs, and thus, seriously risking patients' lives.

- **Malicious & Rational Attackers :** ***Malicious attackers*** do not have a specific goal and do not look for specific results either. They launch their attacks simply because they can do it with the intention to disrupt an IoMT system. This can be done, for example, by transmitting false information to the data center in a specific geographical area. In contrast, ***rational attackers*** have a specific target which can have a very dangerous impact. In other terms, they are unpredictable and generally follow the passive class.
- **Organized & Coordinated Attackers :** Cyber-attacks against IoMT can be organized or coordinated. ***Organized attacks*** are usually based on having prior knowledge of a given medical device or system before launching a cyber-attack against it. In fact, the aim is to either gain an unauthorized access or disclose sensitive information. ***Coordinated attacks*** are based on the cooperation and collaboration between insiders and outsiders. In fact, insiders are rogue/unsatisfied employees (Hospital IT, staff, nurses, receptionists, etc..) having an authorized access to the system and possibly install a malware. Malware types allow outsiders to have an elevated remote access or privilege and carry out a combined attack against a specific medical system. The attack might be carried out in order to hit the system's availability and prevent authorized medical personnel and patients from accessing medical records, book appointments, or disrupt medical operations.

- **Target :** A targeted attack is typically used for assassination or terrorism purposes. Such an attack targets a specific patient or a hospital for various reasons that could be political (assassinating a public figure), ideological, racial or religious reasons. The attackers' goal could be to target a minority group of patients or to target a foreign country with the aim of fueling racism, or spreading terrorism, or part of a cyber-warfare campaign linked to cyber-politics.
- **Scope :** the scope of an attack is related to the targeted area, which may be quantified as small scale or large scale. Typically, attackers try to extend their malicious actions to a large area [Senie et al., 1998, Bagnall et al., 1999] to increase the number of victims, such as patients in hospitals.
- **Impact :** the impact of an attack is quantified by the amount of damage it causes, along with its nature and its scope.
- **Capacity :** this refers to the protection required to prevent, mitigate, or reduce the damage associated with an attack.

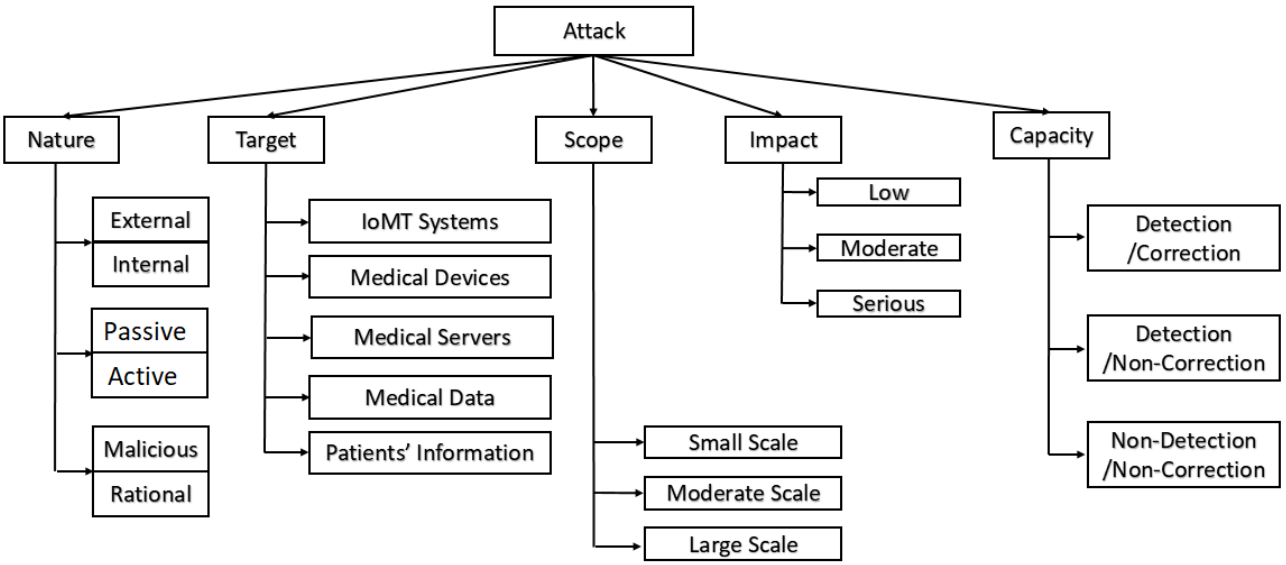


FIGURE 2.6 – Characteristics and profiles of attackers and its corresponding impact

2.4.2/ TARGETED IOMT'S SECURITY ASPECTS

IoMT security seems to be jeopardized by various types of cyber-attacks, which are divided and described depending on the security aspect that they target. As illustrated in FIGURE 2.7, in this section we aim at reviewing the security attacks that target the IoMT data security, including its availability, confidentiality and integrity. On the other hand, we aim to dissect the security attacks that target the system security including user privacy, system availability, confidentiality/trust, authentication and integrity.

2.4.2.1/ DATA CONFIDENTIALITY ATTACKS

In order to hit the confidentiality of IoMT data, gathering information is a must. Due to the open and public nature of IoMT wireless communications, patients are becoming more prone to being intercepted through confidentiality (sniffing) attacks. Therefore, the risk of personal and private information being either leaked, hijacked, modified or even stolen is seriously high. However, in order to achieve it, different passive attacks can be carried out. This includes eavesdropping, traffic analysis, and brute force attacks. TABLE 2.4 presents the main confidentiality attacks.

— **Eavesdropping Attacks** are typically based on gathering information and they are divided into two main types. The first one is **Passive Eavesdropping** [Coleman et al., 2012], where wireless access points are scanned to identify which medical device is connected to them. The second type is the **Active Eavesdropping**, where the adversary can monitor incoming and outgoing data during transmission and Thus, gathering more information in a faster and easier manner.
— **Data Interception Attacks** occur when a man-in-the-middle attack is carried out. This allows the adversary to intercept data and re-transmit it at a later time [He et al., 2017]. This allows the attacker to eavesdrop the Address Resolution Protocol (ARP) request and keeps on repeating it in order to capture a handshake. This handshake is then used to obtain encryption keys and gain unauthori-

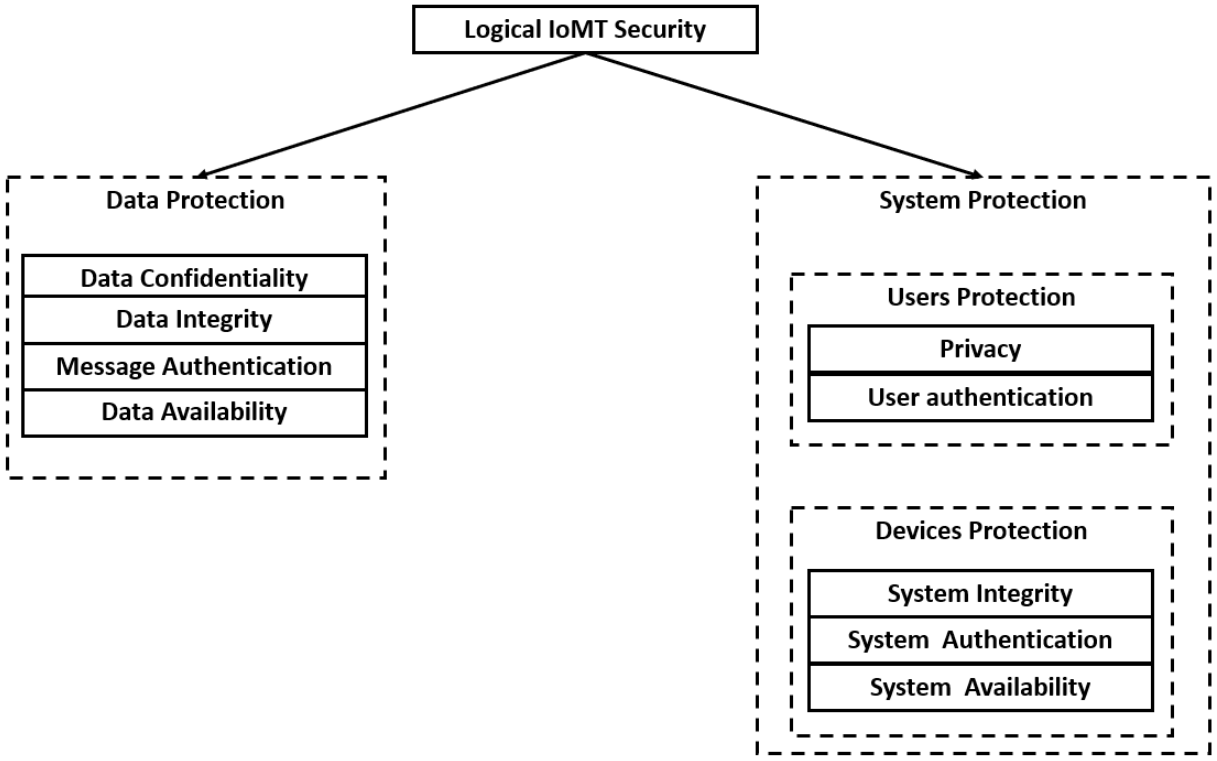


FIGURE 2.7 – IoMT Security Goals

zed access to medical systems and records.

— **Packet Capturing Attacks** or packet sniffing attacks include the capture of the transmitted medical data packets that are unencrypted and revealing their content including patients' medical conditions and passwords. Wireshark is a prime example of a network monitoring software tool.
— **Wiretapping Attacks** include hacking medical telecommunication and telehealthcare devices to intercept real-time incoming/outgoing medical data.
— **Dumpster Diving Attacks** include searching through dumpsters and retrieving any medical information including papers and file thrown in the bin including patients records, medical prescriptions, staff names, etc. This is one of the main reasons why most file and data records are becoming paperless.

2.4.2.2/ SOCIAL ENGINEERING (SE) ATTACKS

Social engineering is a technique used to manipulate people through either baiting or pre-texting in order to lure people to give out information. This includes passwords, names, IDs, private information in order to proceed with a cyber-attack later on. Luring people can be easily achieved by relying on human emotions which seems to be easier than exploiting a system's vulnerability. Therefore, the attacker relies on people's curiosity, or lust, and sends infected adult pictures (phishing), for example, in order to gain access to medical systems or/and records. Different SE attacks are presented in TABLE 2.5.

— **Reverse Engineering Attacks :** A reverse social engineering attack is also known as a person-to-person attack [Irani et al., 2011]. This allows the attacker

TABLE 2.4 – Different types of data confidentiality attacks with their corresponding solutions.

Data Confidentiality Attack	**Solutions**	**Possible Reason(s)**
Eavesdropping	Encryption	• Broadcast nature of messages via wireless channels • Unencrypted communication channel
Data Interception	Encryption	• Non-Secure Channels • Open Wireless Communications
Packet Capturing	Encryption	• Open Wireless Communications • Non-Secure Channels • Lack of Encryption
Wiretapping	• Secure Communications • Closed Communications	• Open Wireless Communication • Non-Secure Channels
Dumpster Diving	• Enhanced Employee Training • Paperless Process	• Lack of Employee Training • Lack of Awareness

to masquerade himself as a technician trying to fix an issue in a hospital's medical system and gaining insight and physical access to the system. It also allows him to possibly upload a malware or detect vulnerabilities that can be exploited. In other cases, an attacker can masquerade himself as a person visiting a patient, asking questions in order to gain a better insight about the used medical systems and devices.

— **Error Debugging Attacks** are usually caused by an improper handling of error, which results into medical systems becoming vulnerable to various security problems [Schaumont, , Yuce, 2018]. Such exploitation can lead to internal error messages that target medical web servers, application servers, and web application environments by displaying database dumps, stack traces and error codes to the attacker. This would mainly result into a system call failure/crash, network timeout or unavailable database. This consumes a high amount of resources and causes a tremendous network overhead, preventing and disrupting the availability of medical services to patients.

— **Phishing Attacks :** Phishing relies on sending fake e-mails, including links to malicious websites, and to direct the victims to these fake and malicious websites [Jagatic et al., 2007, Zhang et al., 2012]. Once a malicious link is clicked on, their sensitive information including user-name and passwords are leaked [Felix et al., 1987]. This allows the attacker to carry out an attack using the obtained credentials.

— **Spear Phishing Attacks :** Such attacks [Parmar, 2012, Smith et al., 2015] usually occur when the attacker creates a fake CV, for example, which is infected with a virus. The attacker intends to send it to the medical staff applying for a medical job. Once the email is received along with the malicious CV, the recruiting staff will open the CV and would not realize that a malicious software

has been installed on their system. This leads to a various range of attacks from elevated privilege, to Root-kit, remote access Trojans, unauthorized access, or even botnets. This also includes whaling (targeting high-profile employees including doctors, specialists and surgeons) [Hong, 2012], and vishing attacks (stealing access/log in credentials) [Griffin et al., 2008] and other aspects of phishing attacks.

TABLE 2.5 – Different types of social engineering attacks with their corresponding solutions.

Social Engineering Attack	**Solutions**	**Possible Reason(s)**	Related Threats
Social Engineering	Training staff against baiting/pretexting	Poor training of employees	May affect the confidentiality and privacy.
Reverse Social Engineering	Training staff against strangers' questions	No identification and verification processes	Depends on the asked questions, primarily targets confidentiality and privacy. In addition, to affecting authentication and availability.
Error Debug	Limit appearing information	Different error questions giving additional information	May affect (data/system's) confidentiality and privacy.
Phishing	Avoid suspicious E-mails and links	Poor training of staff	Depends on the malware task and attacker's goal, may affect (data/system's) confidentiality and privacy.
Spear Phishing	Avoid suspicious folders and file formats	Lack of awareness	May affect (data/system's) confidentiality and privacy.
Whaling	Avoiding Suspicious E-mails	Luring and Lust	Depends on the malware task and attacker's goal

2.4.2.3/ PRIVACY ATTACKS

Ensuring patients' privacy is one of the most important challenges in IoMT. Preserving patients' privacy is mainly related to preventing the disclosure of their real identities, in addition to their location and information. This requires patients to keep their private information protected such as their identity, their behaviour, their past and present location [Ohno-Machado et al., 2004, Terry, 2012, Murer, 2002]. Moreover, in the following, the main privacy attacks are listed and described in TABLE 2.6.

— **Traffic Analysis Attacks :** TAA mainly affects patients' privacy in addition to their data confidentiality. This attack is extremely dangerous and consists of intercepting and analyzing the network traffic pattern(s), trying to infer useful information. This is due to the fact that IoMT devices' activities can potentially reveal enough information, enabling an adversary to cause malicious harm to the medical devices.

More precisely, traffic analysis can target certain information that can be used to establish or facilitate new social engineering attacks.

— **Identity/Location Tracking Attacks :** The attacker spies on an IoMT device during its journey to discover the identity of the patient (relating the patient to a place of work or home). In fact, an attacker may get a trace of the IoMT devices' movements. Studying this trace can reveal the true identity of the patient, in addition to their personal information. Therefore, getting the identity of a given patient can put their privacy and possibly their life at risk.

In order to preserve the privacy of any patient, the MAC and IP addresses must be constantly changed to avoid any possible identity disclosure and denial of service, or spoofing attack [Senie et al., 1998]. Hence the need to design some new algorithms to address the large memory-space dilemma. Therefore, each patient should be allocated a pool of certified pseudonyms obtained from a certificate authority [Wex et al., 2008, Son et al., 2015]. The most popular attack is the Sybil attack. The pool of pseudonyms can be used to pretend they are for different patients whilst sending false messages to a data center. This includes false traffic jams, or false alerts forcing hospitals to react to a false event. The main authorities' goal is to ensure that the identities and their corresponding sensitive data are protected and verified during any communication attempt. In case of any issue, the system operators must interfere, however, it requires knowing the identity of the user (digital forensics). This indicates that a trade-off between privacy and digital forensics, indeed, exists.

TABLE 2.6 – Different types of privacy attacks with their corresponding solutions.

Privacy Attack	**Solutions**	**Possible Reason(s)**
Traffic Analysis	• VPNs & Proxies • Non-Linkability • Pseudonyms	• Source and destination information are not encrypted • Lack of secure channels • Weak encryption algorithm
Identity/Location Tracking	• Anonymity • Non-Linkability • Pseudonyms	• Lack of secure channels • Location and identification parameters are not encrypted

2.4.2.4/ DATA INTEGRITY AND MESSAGE AUTHENTICATION ATTACKS

Integrity attacks are based on the ability to alter the messages that are being transmitted in order to target the integrity of a system or data. Different attacks can be carried out to achieve this goal, such as injection attacks and data interception. Therefore, it is essential to secure and maintain the integrity of data as much as possible [Jones et al., 2013, Shah et al., 2016].

— **Message Tampering-Alteration Attacks :** The attacker here aims to break the data integrity of the exchanged messages. This happens when the attacker manipulates the received messages for his/her own goals [Yang et al., 2013]. This will result into doctors making wrong decisions that might compromise the health of patients.
One of these security methods is using a message authentication algorithm such

as cryptographic keyed hash function as HMAC to ensure data integrity and source authentication.

— **Malicious Data injection :** This kind of attack is generated from an entity that can be legal or can authenticate with the system. Thus, this can cause hazardous effects in the IoMT system and it may lead to fatal accidents [Liu et al., 2011b], by creating a false message and transmitting it to the hospital data center or to doctors. The strategy of this attack is to prevent the real and correct messages from authorised users, and instead inject false messages into the network.
To defend against such an attack, messages should be authenticated.

— **Malicious Script Injection Attacks :** Such attacks introduce false update script system where adversaries can mimic a legitimate server for system backup. This allows a given adversary to gain unauthorized access to any IoMT device and might introduce a backdoor [Rahman et al., 2012].

— **Cloning And Spoofing Attacks** can be combined in order to carry out a more sophisticated attack [Spiekermann, 2015] against a medical system or device. Cloning attacks duplicate the data spoofed, whilst spoofing attacks use the cloned data to gain unauthorised access [Wang et al., 2010].

TABLE 2.7 summarizes the main message integrity and authentication attacks.

TABLE 2.7 – Different types of data integrity and message authentication attacks along their corresponding solutions.

Message Integrity and Authentication Attack	**Solutions**	**Possible Reason(s)**
• Message Tampering-Alteration • Malicious data injection • Malicious Script Injection • Cloning & Spoofing	• Keyed Hash Function (HMAC) ; • Message Authentication Algorithms	No data integrity and source authentication protection scheme

2.4.2.5/ AVAILABILITY ATTACKS

In order to target the availability of medical systems, different attacks are carried out to degrade the performance of medical systems and devices. As a result, the availability attacks can either target data availability or system availability.

— **Data Availability attacks :** The attacker aims to break the data availability of the exchanged messages by dropping these messages. This happens when the attacker manipulates the received messages for his/her own goals, which results into hospital data center or doctors missing important information about the patients' health conditions.

— **System Availability attacks :** The main system availability attacks are listed below and summarized inTABLE 2.8.

  — **Denial of Service Attacks (DoS) :** In order to disrupt the availability of a given medical IoMT system or device, DoS attacks are initiated and launched, preventing legitimate patients from getting proper medications, and preventing

nurses and doctors (GPs) from accessing medical information and records. This prevents real-time data from being sent and received through the disruption and interruption of service.

- **Distributed Denial of Service Attacks (DDoS) :** These attacks can also be simultaneously carried out from different geographical locations and from different countries. This can have a far greater impact on the availability of medical devices and systems resulting into a negative impact on the patients' lives with the inability to respond on time.
- **De-Authentication Attacks :** Such attacks are usually carried out to ensure a single de-authentication attack against a given medical device. It can also be used in order to lead a mass de-authentication process, which prevents all connected devices from being operational either temporarily or permanently. This process also allows the capture of a handshake, which can be used later on to launch a cracking attack, which enables an adversary to gain unauthorized access to a medical system, device or even server.
- **Wireless Jamming** aims to severely interrupt and disrupt any established wireless communication of medical devices between patients and hospitals. More specifically, wireless networks are severely targeted [Vadlamani et al., 2016] by a series of continuous denial of service attacks, which disrupts any communication attempt on secure and non-secure channels, depending on whether the jamming attack is selective or non-selective [Proano et al., 2010]. However, this attack can be mitigated through frequency hopping and frequency shifting, as described in [Grover et al., 2014].
- **Flooding Attacks :** they are based on overwhelming and exhausting the medical system's resources by injecting false information and data to flood the system with false data and information requests [Baig et al., 2013].
  - **ICMP Flooding Attacks** are an Internet Control Message Protocol (ICMP) flood or Ping flood attacks with a Denial-of-Service (DoS) ability that overwhelms a targeted medical device with ICMP echo-requests known as pings [Harshita, 2017]. Attackers rely on exploited IoMT devices (zombies or bots) controlled by a bot master to conduct such type of attacks.
  - **SYN Flooding Attacks** or "half-open" attacks primarily target high-capacity IoMT devices since they rely on Transmission Control Protocol (TCP) services to communicate (i.e email/web servers) [Bogdanoski et al., 2013]. The aim of this attack is to cause a medical server to crash by exhausting the e-Healthcare server's memory reserve to make insecure connections available for further attacks.
  - **Black Nurse Attacks** are highly effective low bandwidth (15-18 Mbit/sec) ICMP attacks that target firewalls with high Central Processing Unit (CPU) load through denial of service attacks [Shan et al., 2017]. This attack results into preventing Local Area Network (LAN) users, including patients and medical staff from transmitting internet network traffic.
- **Delay Attacks :** They introduce high delays for high priority message transmissions. This offers the ability to either re-transmit them or not transmit them at all after the elapsed time.

TABLE 2.8 – Different types of system availability attacks with their corresponding solutions.

Availability Attack	Solutions	Possible Reason(s)
Jamming	Frequency Hooping, direct sequence spread spectrum, beam-forming	Targets Access Points or wireless IoMT devices
Denial Of Service	Backup Devices	Lack of Backup Devices
Distributed Denial of Service (DDOS)	DDOS detection solutions. Increase the security levels of devices to avoid becoming bots.	Exploiting devices turning them into bots
De-authentication	Firewalls, Intrusion Detection Systems, Encryption	Captures a handshake to Launch DoS or Password Cracking Attack
Flood	Timestamps, Certificate Authority, IDS	Overwhelms & Exhausts IoMT's Resources through False Information Injection
Delay	Firewalls, Timestamps, IDS	Overwhelms & Prevent or Severely Delays any Transceiving of Medical Information

2.4.2.6/ DEVICE/USER AUTHENTICATION ATTACKS

Authentication attacks aim to overcome passwords, which are classified as the first and primary line of defence, in order to gain access to a given system [Clark et al., 1996]. Usually, attacks are successful in many cases including when a given password is either too weak or too short, or is static. These attacks can either be encryption cracking (brute force, dictionary, birthday, or rainbow-table attacks), among other attack types mentioned in TABLE 2.9.

— **Man-in-the-Middle Attacks :** This attack is one of the main authentication attacks ; it controls and monitors the communication between two legitimate parties, whilst altering the transmitted data. This attack can either be passive or active. It is considered as a passive attack when the attacker only intercepts and reads the exchanged messages between the two entities. On the other hand, it is considered as an active attack, if the attacker is able to alter, manipulate or/and modify the transmitted data or information without any of the devices' knowledge.
— **Brute Force Attacks** are based on an excessive search for all possible combinations that make up and crack a given password of a medical [Ten et al., 2010]. Such an attack aims to acquire patients' credentials and private medical information for fraud purposes. Most targeted devices include, but are not limited to, remote medical sensors and patient monitors [McMahon et al., 2017].
— **Masquerading Attacks** occur when a wireless network relay node is exploited by a given attacker for malicious purposes. Such attack can constantly send false alarms about an emergency medical condition, and can disrupt the availability of medical services [Kumar et al., 2012]. Moreover, masquerading attacks can modify a patient's medical condition and may result into injecting the wrong drug or an excessive medicine usage, which may result into the loss of human lives.
— **Replay Attacks** modify the control signal being transmitted to another medical de-

vice, especially once an attacker gains a high privilege to the system with the ability to control the system's signals. The adversary may either steal or/and intercept the transmitted information by redirecting it to another location. In some cases, physical damage can be achieved against a given system [Baig et al., 2013], including medical systems. System communications are recorded first before being 'replayed' later to the receiving device [Spiekermann, 2015]. This can lead to either stealing, leaking or disclosing sensitive information to gain an unauthorized access and elevated privilege on a given medical system [Grunwald, 2006].

— **Cracking Attacks** are based on capturing a handshake through a deauthentication attack. Thus, luring the intended AP (Access Point) to respond back with a handshake. Once the handshake is captured, a password cracking attack is conducted against a given medical system or device. This allows the leakage of information and data disclosure.
— **Dictionary Attacks** usually take place when trying to gain access to a given medical system [Nam et al., 2009]. Attacks are usually successful when security measures are less tight than the security measures of a given IoT device. Such attacks occur by relying on a large set of dictionary words in an attempt to guess the password so that the adversary can gain access. In fact, such an attack type is exhaustive in terms of resources and time, and can take time from minutes to hours, and sometimes days. Brute force attacks are usually aimed at targeting a medical device where the security measures are weak [Cho et al., 2011]. In many cases, they still rely on a number combination including the personal identification number (PIN).
— **Rainbow Table Attacks** are usually aimed at targeting the password and its hash value relying on a technique process known as "fault and trial" through the use of reverse engineering. It usually contains a table of passwords along with their hashes, which is executed until a match is found. To overcome this problem, different solutions were presented in [Narayanan et al., 2005, Tahir et al., 2013]. However, salt passwords can be a good solution to mitigate this type of attacks.
— **Session Hijacking Attacks** are also known as TCP Session Hijacking. This attack is achieved by using a Session sniffer that involves a packet sniffer capable of altering, capturing and reading the network traffic (header and data) between two parties. This includes users or/and devices alike. In fact, this attack can capture a valid Session ID (SID).
— **Birthday Attacks** are also due to users relying on weak hashing mechanisms, where two different passwords can have the same hash. Such weakness can easily be exploited to gain an unauthorised access to any medical system. A suggested hash function balance was presented in [Bellare et al., 2004]. However, Secure Hash Algorithm (E.g SHA-3 and SHA-512) mechanisms remain the best solution against such attacks.

2.4.2.7/ MALWARE ATTACKS

Malware can take various forms of harmful software such as Trojans, worms, viruses, spyware, backdoors, botnet, and many others. A malware is based on the exploitation of a software weakness, vulnerability, or/and security gap. This leads to the possibility of having a backdoor to a given medical device or system. Moreover, it is based on gaining unauthorized access, leaking and disclosing sensitive information about a given patient. In fact, the existence of a very advanced malware type such as encrypting services, or po-

TABLE 2.9 – Different types of system authentication attacks with their corresponding solutions.

Authentication Attack	**Solutions**	**Possible Reason(s)**	**Related Threats**
Man-in-the-Middle	Multi-Factor authentication scheme	Poor authentication scheme (one factor)	Depending on attacker goals, it might affect the data's integrity, confidentiality and availability.
Masquerading	Multi-Factor authentication scheme	Poor authentication scheme (one factor)	May affect data's confidentiality.
Cracking	Multi-Factor authentication scheme	Poor authentication scheme (one factor)	may affect the data's confidentiality and integrity.
Replay	• Timestamp or a new random number for each session connection • Multi-Factor authentication scheme	Weakness in the authentication protocol	May affect system's availability.
Dictionary	• Strong password • sufficient size of secret key	Weak password and one authentication factor	May affect the data's confidentiality & integrity
Brute force	• Strong and long password • sufficient size of secret key • Multi-Factor authentication scheme	• Weak password • and one authentication factor	May affect data's confidentiality and integrity
Rainbow Table	Long Salt Passwords	• Weak Usernames/Password • Short Salt Passwords	May affect data's confidentiality and integrity
Birthday	Secure Hash Algorithm	Weak Hashing	May affect data's confidentiality and integrity
Session Hijacking	• Encryption • Sniffing Filters	• Lack of/Poor Encryption • Non-Secure Channels	May affect data's confidentiality, integrity and availability

lymorphic malwares [Nimmo, 2010] imposes a serious threat. Moreover, malware attacks can take many forms and specifications including being based on signature, behavior, or even anomaly. As a result, to prevent the existing kinds of malware, an anti-malware software is required. For this purpose, Section 2.5.2.6 presents the different intrusion detection techniques that can be implemented in order to detect, track down and prevent any possible malware attack.

— **Spyware Attacks :** Spyware's main purpose is to collect and gather data and information about patients and send them to either a third party or sell them through the deep dark web. Thus, keeping users under constantly covert surveillance. In fact, spyware may be used in order to collect enough information about a given patient for a possible assassination. Moreover, spyware is used in order to monitor a patient's health and activity without their knowledge. They can also be called as key-loggers due to their ability to steal patients' credentials [Lee et al., 2005].
— **Ransomware Attack** is a malware that encrypts the data and files stored and hence, denying doctors or patients from accessing patients' medical records. This attack can also be called "cryptoware". Such type of attacks aims at preventing a given doctor from accessing his system and files, whilst urging them to pay a ransom in order to decrypt the files or risk deleting them. The most infamous example is the "WannaCry" [Fruhlinger, 2017].
— **Worm Attacks** Worms are a form of malware that self-replicate vertically over a connected device, after exploiting the device's existing vulnerabilities. Thus, they are capable of self-propagating without any human intervention. In some cases, they can be designed to target a given industrial control system [Falliere et al., 2011]. Worms can be implemented and used against medical systems and devices in order to gather information, damage or even destroy any given device. In some other cases, worms can lead to file deletion or ransoms [Cooke et al., 2005].
— **Remote Access Trojan Attacks :** RAT attacks occur through the exploitation of a medical system's vulnerability, weakness or security gap in a given targeted medical system. Such attacks are based on evading all security procedures and countermeasures by gaining a covert unauthorized access as a backdoor. This leads to overcoming all of the security measures employed. This is mainly achieved by bypassing the authentication process. The most infamous attack was the operation Shady RAT [Alperovitch et al., 2011].
— **Logic Bomb Attacks :** Logic bombs are classified as small programs that logically explode after reaching a certain date or time, damaging the medical systems' components including logs, data, and files. In fact, they are mostly installed by insiders [Northcutt, 2005].
— **Botnet Attacks** are based on exploiting vulnerabilities of embedded physical devices and turning them into bots, awaiting orders from the adversary through command-and-control to send fake or false information to a given patient. They can also be used to bring the whole medical system down through a DoS or DDoS attacks [Stone-Gross et al., 2009, Zhang et al., 2011]. In fact, in many cases, such attacks are aimed at disclosing sensitive information and using them for malicious or personal gains.

All malware attacks and their solutions are summarized in TABLE 2.10.

2.4.2.8/ IMPLEMENTATION ATTACKS

Different implementation attacks on medical systems are presented in this section, including the side channel attacks, fault attacks, and timing attacks.

— **Side Channel Attacks** can possibly occur due to IoMT embedded systems having very limited physical properties. Moreover, they are used to recover the secret key using power consumption, differential power consumption or electromagnetic

TABLE 2.10 – Different types of malware attacks with their corresponding solutions.

Malware Attack	Solutions	Possible Reason(s)	Related Threats
Botnet	Botnet detection solution (anti-malware), pen-testing, intrusion detection	A logical collection of exploited internet-connected devices or IoMT devices	Depends on the attacker's target (confidentiality, integrity, authentication and/or availability)
Worm & Viruses	Anti-virus, anti-malware, pen-testing, intrusion detection	Relies on computer network security failures	Depends on the attacker's (confidentiality, integrity, authentication and/or availability)
Spyware	Use antivirus and anti-spyware solutions, update OS, ensure higher security and privacy levels, intrusion detection	Part of other software or downloads on file-sharing sites	Primarily targets privacy and data confidentiality but it can used for other purposes such as availability, authentication and/or integrity.
Remote Access Trojan	Keep antivirus software up to date, block unused ports, intrusion detection	Downloaded invisibly with a program or update software	Depends on the attacker's (confidentiality, integrity, authentication and/or availability)
Rootkit	Appropriate system configuration, strong authentication, patch and configuration management, intrusion detection	Exploits and targets either the kernel, or the user application space gains root privileges.	Primarily targets sysem's authentication
Ransomware	Up-to-date Anti-Virus/Anti-Malware, Avoid Using Personal Information, Enhanced System's Security, Higher Awareness	Weak Passwords, Weak Multi-Factor, Paying Ransoms	Targets system's Authentication and Availability, in addition to data confidentiality and privacy

analysis. In fact, IoMT devices with Physical non-cloneable Functions (PUF) can guard against different implementation attacks.

— **Fault Attacks** target a physical electronic device by stressing the device by external means. This includes the increase/decrease of voltage to generate errors, which mostly leads to a security failure [Piret et al., 2003].

— **Timing Attacks** are classified as side channel attacks where an attacker attempts to compromise a cryptosystem by analyzing the needed execution time of cryptographic algorithms. In addition, a timing attack is a security exploitation, where an attacker discovers security vulnerabilities surrounding the computer or network system. Moreover, timing attacks are also used to target medical devices that use OpenSSL [Dhem et al., 1998].

This attack can become inefficient when using the ”time stamping mechanism”

for packets of delay-sensitive applications. However, this proposition encountered the problem of time synchronization between entities [Mills et al., 1985, Clark et al., 1992].
All implementation attacks along with their solutions are summarized in TABLE 2.11.

TABLE 2.11 – Different types of implementation attacks with their corresponding solutions.

Implementation Attack	**Solutions**	**Possible Reason(s)**	**Related Threats**
Side Channel Attack	Hardware countermeasure (PUF) and software randomization processes	Limitations of physical properties related to the embedded devices	**It may lead to secret key recovering and consequently affect the data confidentiality.**
Fault Attack	uses protected hardware and Spatial Retreat	Memory & disk manipulation	**May affect the System integrity. This type of attacks modifies the execution code to recover the secret key and consequently affect both data authentication and confidentiality.**
Timing Attack	Constant Cryptographic Computations Execution Time, Independent Cryptographic Algorithm	Possible cryptographic software or algorithm Exploitation	**May cause the secret key recovering and consequently affect data's confidentiality.**

2.4.3/ REAL-CASE CYBER-ATTACKS

Cyber-attacks against healthcare [Decker, 2007, Martin et al., 2017] have recently emerged. Therefore, in this section, the aim is to reveal the most recent cyber-attacks that occurred, in addition to how these attacks were led, their types, and the attackers' motives.

— **NHS :** In May 2017, the National Health Service (NHS) was vulnerable to the WannCry ransomware attack (supposedly led by North Korea-Unit 180 (Lazarus)) [Maron, 2017], where 70,000 infected devices including computers and Magnetic Resonance Imaging (MRI scanners), before establishing a security operations centre. However, the NHS also invested £250,000 in order to raise awareness and train NHS employees.
— **Hancock Regional Hospital :** On January 11th, 2018, Hancock Regional Hospital in Indianapolis was infected by a SamSam Ransomware via an e-mail [Maron, 2017]. Such an attack might have possibly been a phishing attack. Hackers managed to lock the hospital's computer systems and demanded a ransom to be paid through Bitcoin crypto-currency. This forced the hospital to pay

$55,000 as a ransom [Coventry et al., 2018]. However, patient's care was not disclosed nor compromised.

— **UCLA Health :** On September 2014, the University of California, Los Angeles (UCLA) Health fell as a victim to a Medical Device Hijack (MEDJACK), where more than 4.5 million patients had their personal data exposed. This exposure included patients names, birth dates and medicare numbers [Frumento et al., 2016]. Such attack took place because data was being transmitted in the clear (no encryption) from medical devices to electronic health records. As a security measure, cybersecurity firms were hired from outside to guard UCLA's networks.
— **UoWM :** On November 29th, 2013, University of Washington Medicine was subject to an email phishing attack via an e-mail that had a malicious link embedded in it. This led to compromising the personal information of around 90,000 patients [Farringer, 2016]. This included patients' names, addresses, phone numbers and dates of birth [Ahmed et al., 2017]. This resulted into paying a $750,000 settlement and agreeing to a corrective action plan. Between December 4th and 26th, 2019, the University of Washington Medicine was prone to a misconfiguration mistake where the medical data of one million patients was exposed for 3 weeks before being discovered. However, there was no proper estimated cost of the recovery and response to the breach.
— **HPMC :** On February 17th, 2016, Hollywood Presbyterian Medical Center was under a ransomware attack [Winton, 2016]. More precisely, hackers managed to infiltrate the network in order the access the data, before copying it and encrypting it. Once the data was copied and encrypted, the original data was deleted. Moreover, hackers requested 40 Bitcoins worth of $17,000. This led to a delay in patient care. However, control was regained and restored. In fact, the attack was conducted by Turkish hackers as a political statement without stealing any patient's data. On August 5th, 2019, Presbyterian Healthcare Services came once again under a Phishing attack which started between May and June. The data of 116,183,000 patients was potentially breached. Security measures included conducting a thorough review of the impacted emails and alerting federal law enforcement.
— **CHS :** On August 18th, 2014, Community Health Systems was prone to a cyber-attack led by Chinese hackers People Liberation Army's Cyber-Wing [Engstrom, 2018] stealing patient's data of around 4.5 million individuals using a malicious software. The stolen data was sold to third parties in order to commit insurance fraud [Frumento et al., 2016]. Such an attack took place using a malware software over non-secure server, which allowed hackers to locate the Virtual Private Networks (VPNs) before logging into CHS's infrastructure. As a security solution, the focus was on how to enhance the servers' security.
— **IHSL :** On May 19th, 2019, the Imperial Health in Southwest Louisiana came under a ransomware attack [Fournette III, 2018] in the US, with more than 116,262 patients having their data breached. As a protective security measure, a new antivirus was used, and patients were offered precautious measures to follow.
— **KPDvCHC :** On July 25th, 2019 Kentucky's Park DuValle Community Health Center came under a ransomware attack [Fournette III, 2018] in the US, where the data of 20,000 patients was locked for 2 months, before paying hackers $70,000 to decrypt data and end the attack.

To defend the listed attacks, several security measures should be taken, including technical and non-technical ones. In the next section, we review the existing security solutions for IoMT data and systems. In addition, we include the security practices and guidelines

that should be followed to ensure IoMT systems and data confidentiality, integrity, privacy, etc.

2.5/ IoMT Security Measures

Overcoming the rising IoMT security issues and challenges is a challenging task. However, mitigating them can be achieved by implementing multiple security measures, some being technical and others non-technical measures.

2.5.1/ Non-Technical Security Measures

This section is dedicated to highlight the different non-technical security measures that can be applied according to the needs. This includes training the staff and safeguarding the patients' private medical health records.

Training the medical and IT staff could be accomplished in three different ways : raising awareness, conducting technical training, and raising the education level as illustrated in Figure 2.8.

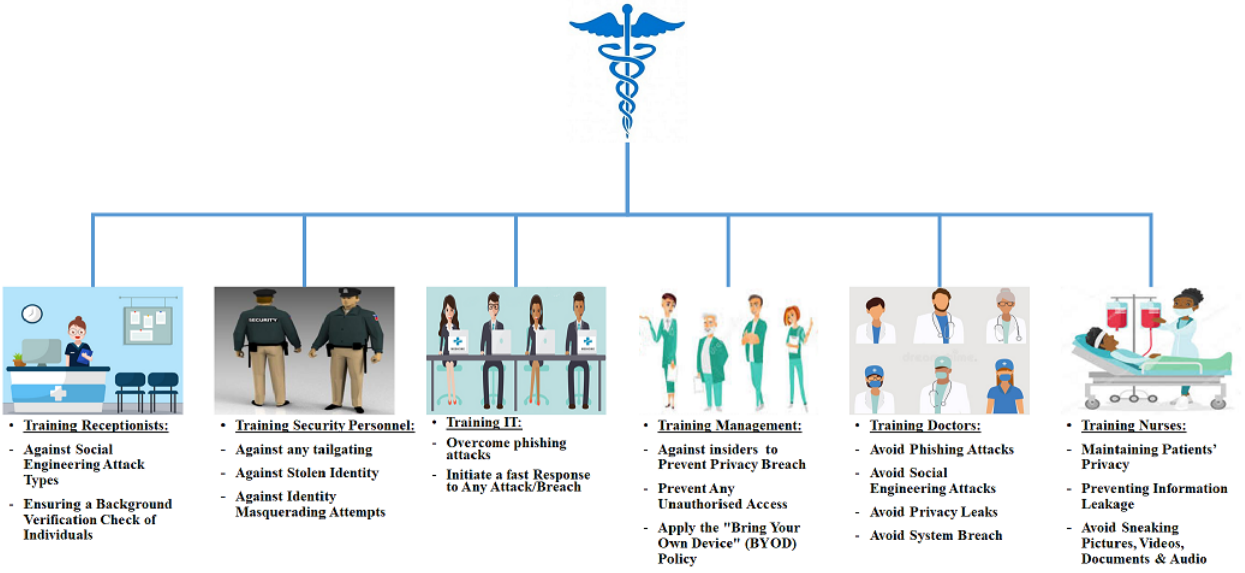


Figure 2.8 – IoMT Staff Training

— **Raising Awareness :** It is highly necessary and recommended to raise awareness among medical employees and staff, mainly the IT department in order to know and identify an occurring attack from normal network behaviour. However, this is not enough, as there is a higher need for defining what is a threat, risk and a vulnerability. This offers them the chance to identify a risk from a threat. It also offers the possibility to assess the likelihood and impact of a risk. Once a risk is assessed, it is also essential to explain how to mitigate it and use the right security measures to deal with any threat and reduce its risk.

— **Technical Training :** Raising awareness is not enough, it is equally important to start training the medical staff and employees of the IT department, right after the

teaching phase. The training must be divided into seven different phases, starting with :

- **Identification Phase** where the IT is capable of identifying a suspicious behaviour from an abnormal behaviour.
- **Confirmation Phase** that is based on the ability to confirm that an attack is occurring.
- **Classification Phase** that is based on the ability to identify the type of the occurring attack.
- **Reaction or Responsive Phase** is based on the ability of the Computer Emergency Response Team (CERT) to quickly react to a given attack using the right security defensive measures and prevent an attack from escalating.
- **Containment Phase** is based on containing the attack incident and overcoming it.
- **Investigation Phase** is the implementation of forensic evidences where an investigation process takes place to identify the cause of the attack, its impact and damage.
- **Enhancement Phase** is based on learning from the lessons of previous attacks.

— **Raising Education Level :** The current focus must be targeted towards raising the level of education, especially for those in the IT domain. This is based on teaching and educating cyber-security and IT staff the necessary techniques to classify each attack and what it targets (confidentiality, integrity, availability, and/or authentication). Attackers are also divided into insiders or outsiders. However, it is important to assess the level of damage of an attack caused by an insider, along with the possibility of a remote or outsider attack. Afterwards, it is also highly recommended to educate them on how to evaluate the possibility of a risk from occurring (likelihood/impact). It is also important to know what encryption or cryptographic technique can or should be used to prevent any alteration or interception. To limit the possibility of insider attacks, the right authorization and authentication techniques should be applied, along with the best Intrusion Detection Systems (IDS) in order to detect any attack based on either signature, anomaly or behaviour.

2.5.2/ Technical Security Measures

In this section, we discuss the technical security measures that should be put in place to ensure an end-to-end secure IoMT system. Thus, the following subsections discuss techniques that aim at ensuring IoMT data and systems security.

2.5.2.1/ Multi-Factor Identification and Verification

In order to prevent any possible unauthorized access to IoMT systems, it is important to ensure a strong identification and verification mechanism. The best solution is to rely on biometric systems. There is also the need for a database to store the biometric templates safely and securely for future use [Douglas et al., 2018]. However, achieving identification and verification requires several biometric techniques, which can be divided into physical and behavioural biometric techniques [Douglas et al., 2018].

— **Physical Biometric Techniques :** Secure physical biometric techniques can be

adopted and used to safeguard and maintain patients' medical privacy without being prone to any insider threat. This includes facial recognition, retina scan, or iris scan.

- **Facial Recognition :** Facial recognition managed to prove a high verification rate [Woodward Jr et al., 2003]. Hence, it was used in order to recognize a person's facial structure, using a specialised digital video camera that identifies and measures the face's structure. This also includes the distance between the triangle of eyes, nose and mouth. Hence, it is able to verify legitimate users from non-legitimate users by comparing a scanned face with the authorized faces registered in the database.
- **Retina Scan :** A retinal recognition scan is based on analyzing the blood vessel region located behind the human eye. It proved to be a very accurate and secure verification method by [Jain et al., 2004].
- **Iris Scan** proved to be essential for both identification and verification purposes, due to its ability to generate accurate and precise measurements [George, 2012]. Iris scan operates by analyzing and scanning the coloured tissue around a specific eye pupil to check if it matches the stored data to either grant access or not.

- **Behavioural Biometric Technique :** A secure behavioural biometric technique that can be used for both identification and verification phases is the hand geometry. Such biometric systems rely on hand measurements, including palm size, hand shape, and finger dimensions [Douglas et al., 2018]. Then, it is compared to the set of stored data in a database to verify users. If there is match, a given staff will be granted access. If not, access will be denied. However, such systems are only limited to one-to-one systems [Al-Ani et al., 2013]. In fact, current systems are capable of differentiating between a living hand and a dead hand. This prevents adversaries from trying to deceive the system and gain any illegal access [Jain et al., 2012].

2.5.2.2/ Multi-Factor Authentication Techniques

Venka & Gupta [Venkatasubramanian et al., 2007] presented a survey that focused on patients' privacy violation, with the reliance on encryption, authentication and access control mechanisms as countermeasures. Authentication is classified as the first line of defence that authenticates the source and destination alike. In fact, authentication can be a single-factor authentication that only relies on a password as the only security measure, which is not preferable. It can also be a two-factor authentication that relies on another security measure aside from the password in order to access a given system. Finally, it can be a multi-factor authentication where a third security mechanism is required in order to access a system. Therefore, authentication plays a key role in providing security for the accessible resources on a given network.
Authentication can be either centralized where two nodes authenticate themselves through a trusted third party, or it can be distributed where two nodes use a pre-defined secret key to authenticate each other, without relying on a trusted third party.

Furthermore, in [Humayed et al., 2017], Halperin et al. presented a cryptography-based key-exchange authentication mechanism that relies on external radio frequency rather than batteries as an energy source. This approach can be used in order to constantly prevent any unauthorized personnel from gaining access [Halperin et al., 2008]. The

out-of-band authentication was also deployed in a number of wearable devices including mainly heart rate and blood pressure monitors [Seepers et al., 2016]. It is based on the use of additional channels including audio and visual channels to generate a key to encrypt and secure the body sensor communications in a given network [Rushanan et al., 2014]. In [Ankaralı et al., 2015], Ankarali et al. presented a physical layer authentication technique which relies on pre-equalization. Furthermore, an enhanced dual-factor user authentication scheme was presented and used by both authors in [He et al., 2010, Yeh et al., 2011] in order to protect WSNs. According to [Wang et al., 2018a], Das et al. presented a smart-card-based password authentication scheme for WSNs [Chen et al., 2010], which mainly lacked user's anonymity [Kim et al., 2014]. In [Li et al., 2013a], Li et al. presented their own advanced temporal credential-based security scheme which included a mutual authentication and key agreement for Wireless Sensor Networks (WSNs). Gope et al. presented another authentication scheme based on a realistic lightweight anonymous authentication protocol used for securing real-time application data access for WSN [Gope et al., 2016]. Kumar et al. [Kumar et al., 2011] attempted to develop a privacy-preserving two-factor authentication framework exclusively for WSNs to overcome various attack types.

2.5.2.3/ AUTHORISATION TECHNIQUES

An assigned authorization must be based on offering the least privilege. Hence, the Role-Based Access Control (RBAC) model is adopted. This model offers the least privilege for a given medical staff or employee to perform a given task with the least (necessary) permissions and functionalities to accomplish a specific task.

— **T-Role-Based Access** (T-RBAC) is mainly designed for cloud computing environments, especially where medical data is stored [Oh et al., 2003]. T-RBAC is a proper access control model for Smart Health-care Systems [Wang et al., 2015a]. In addition, T-RBAC also stands for Temporal Role Based Access Control, and can be spatio-temporal [Ray et al., 2007], intelligent [Muthurajkumar et al., 2014], and generalized [Joshi et al., 2005]. It is also capable of validating any needed access permission for any medical user according to the assigned role and tasks. In fact, T-RBAC can be divided between two task types, the workflow tasks that need to be completed in a particular order (this requires an active access control), and the non-workflow tasks, which can be completed in any order that requires a passive access control.

2.5.2.4/ AVAILABILITY TECHNIQUES

The importance of maintaining availability against any possible disruption or/and interruption of signals is a must. However, maintaining the server's availability requires the implementation of computational devices that act as backup devices, along a verified backup and Emergency Response Plans (ERP) in case of any sudden system failure.

— **Against Jamming :** Jamming can take many forms (see FIGURE 2.9), including DoS, DDoS, or/and de-authentication. In the event of jamming attacks, several medical services would be severely affected, especially with the disruption and interruption of medical services. This can lead to the disruption and prevention of communications between medical devices and the doctor or GP, which leads to missing updates of patients' health records and hence, health complications.

Furthermore, with these medical services being brought down by a jamming attack, first responders will not be able to arrive to the scene on time. This would increase the potential of a given patient being prone to strokes that can possibly lead to their death. For this specific purpose, different security measures must be implemented in order to overcome any attack that would target the availability of any given system. For example, having backup computational medical devices and servers is crucial. In fact, medical devices must be available 24/7 in order to ensure the necessarily medical requirements and needed attention. Furthermore, backup devices must be quick to respond in real-time and activated in case of any emergency that threatens the availability of a given medical system. In fact, additional security measures can be taken into consideration, including Channel surfing, spatial retreat, and priority messages [Xu et al., 2004], which can be very useful against wireless denial of service attacks. This can be a good countermeasure for medical devices, especially in the IoMT domain.

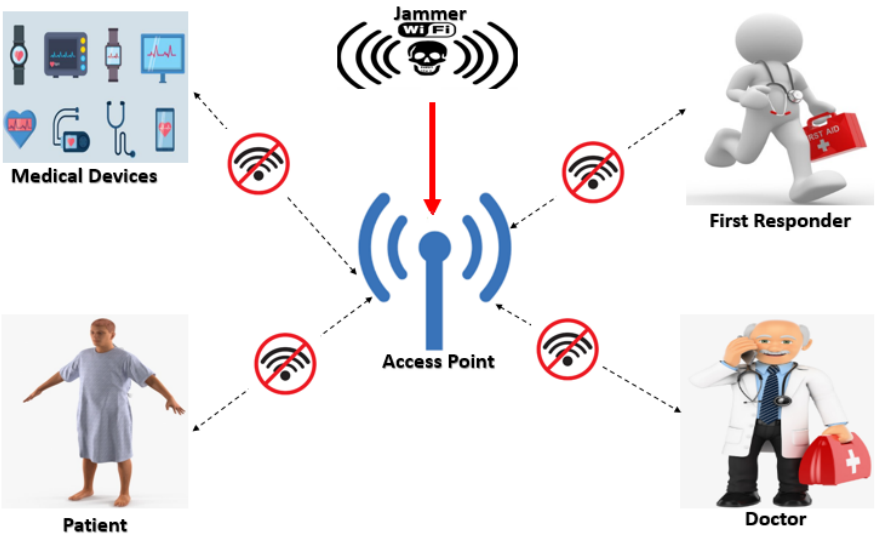


FIGURE 2.9 – An Example Of Possible Jamming Attacks & Their Impact On IoMT Systems Including : Data Center, First responders, Doctors & Patients - Targeting Main IoMT Communication Channels.

2.5.2.5/ HONEYPOTS

Honeypot systems are really useful when it comes to detecting attackers, their targets (see FIGURE 2.10), tools and used methods. However, the reliance on static honeypot systems is challenging. Hence, the need for a dynamic honeypot system configuration. Although there are no specific honeypots for IoMT, some honeypots are being employed in IoT systems and these might also be useful in the IoMT system as well. In [Luo et al., 2017], Luo et al. mentioned that building honeypots for IoT devices is challenging using traditional methods. Therefore, they presented an automatic and intelligent way to collect potential responses using a scanner and a leverage machine technique to learn the correct behaviour during an interaction with an attacker. Their evaluation revealed that their proposed system can improve the session interaction with the attackers to capture further attacks.

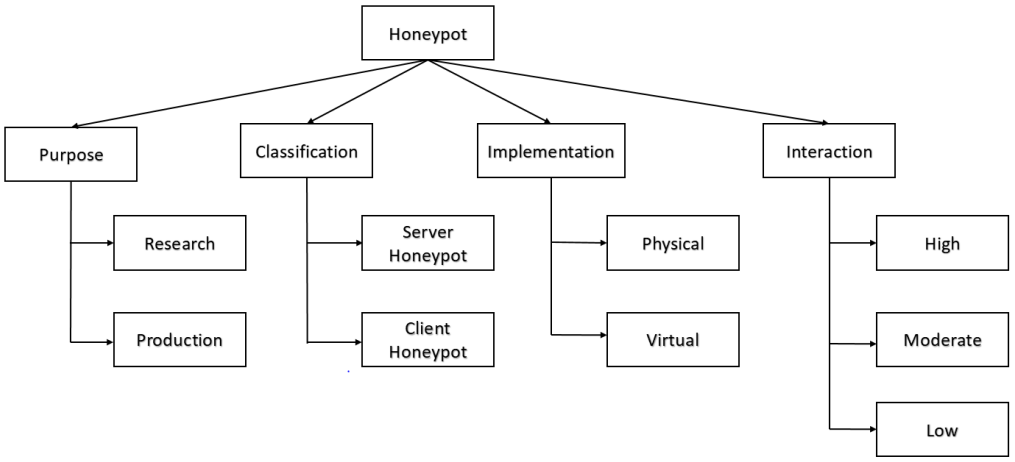


FIGURE 2.10 – Honeypot Taxonomy Based on 4 Metrics : Purpose, Classification, Implementation, & Interaction.

In [La et al., 2016], La et al. developed a game theoretic model to analyze deceptive attacks and defense problems in a honeypot enabled IoT network. In fact, a Bayesian belief update scheme was used in their repeated game. Their presented game model and simulation results showed that whenever facing a high concentration of active attackers, the defender's best interest was to heavily deploy honeypots. This allowed the defenders to use a mixed defensive strategy that keeps the attacker's successful attack rate low. Finally, their game theoretic approach may be suitable for medical health-monitoring systems, and sensor networks.
In [Dowling et al., 2017], Dowling et al. presented an analysis of the results from bespoke ZigBee simulated honeypot deployed on Secure Shell (SSH). This simulated honeypot is used to detect and analyze automated and random attack types before being examined and identified. Brute-force and botnet attacks provided a better material for examination, unlike individual and dictionary attacks. Therefore, these attacks managed to treat the honeypot as an SSH device and concentrated on compromising it. This was done by showing interest in the honey-tokens to manipulate them. Individual attacks have shown an interest in a small number of files that were already downloaded and sandboxed. This also included the scripts that were analyzed, rather than having any specific knowledge towards Zigbee networks. In [Anirudh et al., 2017], Anirudh et al. managed to conduct a detailed study on how a DoS attack is conducted against IoT systems. This included how they can be averted by a honeypot relying on a verification system to maintain the efficiency of transmitted and received data. Their outcome demonstrated the capability of their presented scheme to secure an IoT system through the implementation of honeypots. Their future work includes deploying honeypots to overcome DDoS and botnet attacks.

2.5.2.6/ INTRUSION DETECTION SYSTEMS

Due to cyber-physical systems becoming operational in medical devices, systems and domains, a new term has emerged, which is the Medical Cyber-Physical Systems (MCPS). However, MCPS are prone to various attacks. Hence, in this section, two main IDS types

are presented including anomaly detection and behaviour-rule specification-based detection. Their main purpose is to overcome any possible intrusion such as data injection or code injection attacks (see FIGURE 2.11). Since IoMT devices are resource-constrained, they are prone and vulnerable to different types of threats and challenges. Before proceeding any further, it is recommended to give a clear idea regarding the different IDS types, including Host-based IDS (HIDS), Network-based IDS (NIDS) and Application-based IDS (AIDS). Unlike AIDS, HIDS is attached to a given device to monitor any occurrence of a possible malicious activity. However, NIDS connects to more than one network, if needed, to monitor network traffic and protect it against any malicious activity. In fact, AIDS monitors the applications on a given network or device to monitor and detect malicious activities as early as possible. Moreover, IDS can be specific as signature-based, anomaly-based (machine-learning and programming (rule-based)), or specification-based as discussed in the next subsections. Furthermore, IDS can either be **centralized** by being installed on the router's border, **distributed**, by being installed in each IoMT device, or **hybrid**, which is a combination of both centralized and distributed.

— **Signature Specification-Based Detection :** In their IDS survey in the IoT domain, Zarpelao et al. [Zarpelão et al., 2017] presented different types of IDS that can be applied in IoT in general and in some specific cases, to the IoMT domain. The signature-based IDS is based on detecting any possible intrusion when a network or system behaviour matches a given attack signature stored in the IDS database, which requires a constant update. In case of a match, an alarm is triggered. However, the main drawback is the inability to detect attacks with unknown signatures, or polymorphic malwares [Liao et al., 2013]. Moreover, several interesting approaches were presented by different researchers and authors. In [Liu et al., 2011a], Liu et al. employed Artificial Immune System mechanisms in their signature-based IDS. The attack signatures have been modelled as immune cells that are capable of classifying datagrams as either normal or malicious. These detectors were able to adapt to new conditions and environments. However, no further explanation was presented as to how the solution would be applied in IoT networks and systems. Furthermore, in [Kasinathan et al., 2013b], Kasinathan et al. managed to integrate a signature-based IDS into the network framework that was developed within "ebbits project3". Their aim was to detect DoS attacks in IPv6 over Low-Power Wireless Personal Area Networks-based (6LoWPAN-based) networks. Such signature-based IDS was implemented by adapting the Suricata4 (signature-based IDS employed in 6LoWPAN networks) to send alerts to a DoS protection administrator for further analysis. This made it easier to confirm attacks and to reduce the false alarm rate. Another signature-based approach was presented by [Kasinathan et al., 2013a]. This approach is based on the extended work of the presented approach in [Kasinathan et al., 2013b]. Moreover, in [Oh et al., 2014], Oh et al. focused on reducing computational cost, network overhead and false alarm rate due to the nature of the resource-constrained IoT devices. This was achieved by initiating a comparison between packets payloads and attack signatures.

— **Anomaly-Based Detection** seems to be very fit for overcoming the threat of an undetectable attack. Therefore, [Almohri et al., 2017] surveyed several works that proposed various schemes for the detection of attacks against medical CPS systems and domains [Mitchell et al., 2014]. The survey identified two main models : physical-based and cyber-based. The physical-based model is used to define normal operations within CPS through anomaly detec-

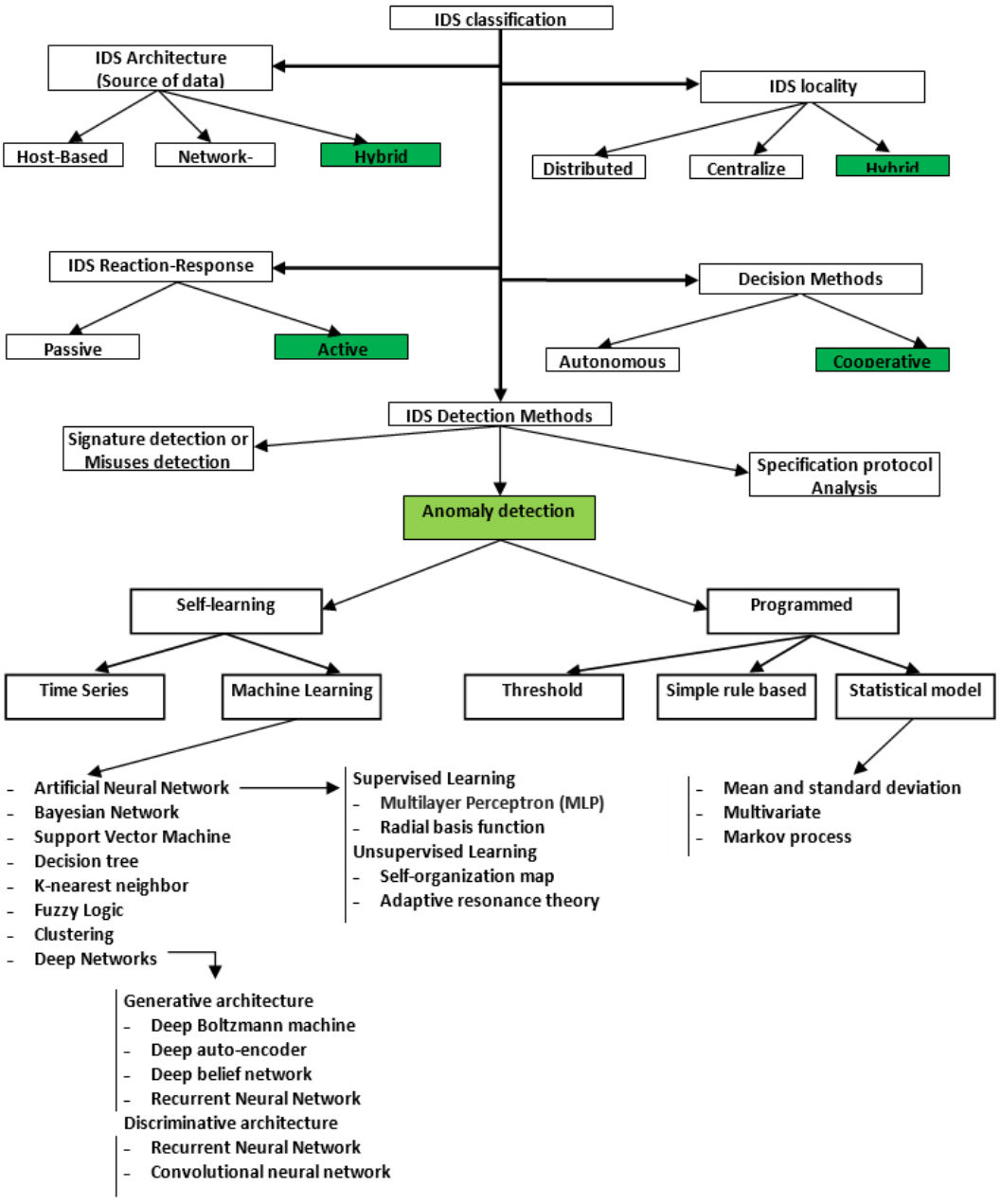


FIGURE 2.11 – Modern IDS Classification Based on 5 Factors : Architecture, Locality, Reaction-Response, Decision Class & Detection Methods.

tion. The cyber-based model is used to recognize potential attacks mentioned in [Xu et al., 2016] and [Shu et al., 2015]. According to [Chen et al., 2016, Abera et al., 2016], their studies revealed how MCPSs were prone to various cyber-attacks. This included code-reuse attacks [Roemer et al., 2012], and malicious code injection attacks [Francillon et al., 2008], along with fake data injection attacks [Alemzadeh et al., 2016], and zero-control data attacks [Hu et al., 2016]. However, in order to be able to detect malicious code injection attacks in MCPS, Zimmer et al. [Zimmer et al., 2010] exploited a worst-case execution time by obtaining information using a static application analysis in CPS. Moreover,

in [Yang et al., 2006], Yang and Hwang investigated an approach capable of fraud detection in healthcare applications. Their approach was anomaly-based, providing measurements capable of validating the effectiveness of data mining implementations.

— **Behaviour-Rule Specification-Based Detection :** As a start, in [Mitchell et al., 2015], Mitchell et al. analyzed a behaviour-rule specification-based technique to employ IDS mainly in MCPS. Moreover, In [Mitchell et al., 2015], Zarpelao et al. presented the transformation of behaviour rules into a state machine. Such approach was capable of detecting any suspicious deviation initiated from any medical device's behaviour specification. In [Mitchell et al., 2014], Asfaw et al. studied a host-based anomaly detection for MCPSs by focusing on attacks against MCPS privacy. In [Porras et al., 1997], Porras and Neumann studied a hierarchical multi-trust behaviour-based IDS that runs with different scopes of multi-trust data (service or domain). Their approach is called "Event Monitoring Enabling Responses to Anomalous Live Disturbances" (EMERALD) [Cheung et al., 2007]. It relies on both signature and anomaly analysis. The anomaly-based analysis is used in order to detect any live intruder, as well as detecting any malicious code. In [Tsang et al., 2005], Tsang and Kwong presented a multi-trust IDS called Multi-agent System (MAS), which includes a function analysis named Ant Colony Clustering Model (ACCM). Such an IDS is capable of collecting audit data, performing analysis, and managing multi-trust communication, among other functionalities. In [Park et al., 2010], Park et al. presented a semi-supervised anomaly-based IDS. Their approach was behaviour-based ; it audits a series of events which include sensor ID, based on time and duration. However, [Mitchell et al., 2015] presented a behaviour rule Specification-based IDS to ensure the safety of MCPS. Such approach relies on attacks that violate MCPS's integrity and it has managed to outperform the existing technique in [Park et al., 2010]. It can detect an attacker without any false negative rate. Moreover, simulation results revealed that their bounding false alarm probability varied between 5% (in some cases below 5%) and 25% for a given attacker. Thus, covering a wider range of noise levels in a given environment.

2.5.2.7/ PRESERVING PRIVACY TECHNIQUES

Various cryptographic solutions were presented in [Pinkas, 2002, Agrawal et al., 2000, Verykios et al., 2004, Kargupta et al., 2003], specifically for the purpose of securing communications between medical devices. This offers the ability to preserve the privacy of patients' data. Moreover, this section will mention specific encryption mechanisms used to secure the communication while maintaining data privacy.

— **Non-Cryptographic Privacy Solutions :** In order to maintain security and privacy, it is important to maintain a high degree of anonymity, which can be done by one of the following techniques :
  — **Pseudonymity** is based on issuing alternative (virtual) identities that can substitute real identities, especially in communication and transaction domains, and they would be known only by trusted entities. The main responsibility is to be able to manage patients' identities, by having them held by the certification Authorities (CA). Each patient is given a well-defined set of pseudonyms to preserve their privacy. However, using the pseudonym more than once will

degrade the patient's privacy. In fact, it is preferable to preserve the location privacy of a patient. This can be achieved by breaking the linkability between two locations, which allows a given patient to update their pseudonym after each transmission. As such, even a powerful adversary would not be able to link the new and old pseudonyms at any time.

- **Aggregation** can be another technique, which allows the combination of data with data of other individuals. Therefore, any disclosure of information of a given patient cannot be retrieved due to the fact that it is mixed with other slices of information. This leads to the inability to retrieve any useful information.
- **Mixing** aims to intertwine transactions, information, or/and communications in a way that they cannot be traced back by a malicious attacker and thus, hindering any attempt to retrieve information.
- **Proxies** are the most popular used technique. They can take a much more advanced form relying on VPNs, or safe browsing such as The Onion Router (TOR). This reduces any attempt to compromise medical information.

— **Cryptographic Privacy Solutions :** Different algorithms can be applied to guard against network eavesdropping and man-in-the-middle attacks.

- **Traditional Cryptographic Algorithms** are based on encryption methodologies [Wunnava et al., 2002], which could be either symmetric [Emanuel et al., 2012] or asymmetric. However, adopting a hybrid methodology [Zhou et al., 1992] is very effective at filling the gaps between the advantages and drawbacks of a given encryption methodology. The hybrid methodology is faster than the asymmetric key approach since the latter is only used for the encryption and decryption of just the symmetric key and not the whole message. On the other hand, the Advanced Encryption Standard (AES) is being rapidly developed and employed for IoT applications. For example, Tohoku University Research Group and Nippon Electric Company (NEC) Corporation created the world's most efficient AES crypto-processing technology for IoT Devices with 50% less energy consumption. Concerning public key encryption, Rivest, Shamir, and Adelman algorithm (RSA) is highly secure, however, it suffers from latency issues. As a result, NTRUEncrypt [Howgrave-Graham et al., 2005] was adopted as a faster approach than RSA, even though it is still being tested and its security has not being confirmed yet.
- **Attribute Based Encryption (ABE) :** In order to secure data storage, preserving privacy is a must. In [Li et al., 2010], authors presented various methods to secure stored data in BANs, while distributing data access controls, mainly the role-based access control [Ferraiolo et al., 2001]. In [Goyal et al., 2006], Goyal et al. used an Attribute-Based Encryption (ABE) scheme to control the access to the patients' data by limiting access to specific authorized personnel only. ABE was applied on a neighbouring local server where the communication between the server and BANs is secured via symmetric key encryption.
- **Homomorphic Encryption :** Relying on conventional encryption schemes means that in order to perform computations on encrypted data, these must be decrypted first, which necessitates trusted storage entities. However, by using homomorphic encryption, it is possible to perform computations on encrypted data [Gentry, 2009, Page et al., 2015], which preserves the patients' privacy.

2.6/ LESSONS LEARNT

From this work, many lessons could be learnt to ensure a safe and secure IoMT environment :

- **Patients' Privacy** needs to be protected at all time against cyber-attacks (remotely) and physical-attacks (insiders).
- **Multi-Factor Authentication** must be adopted to prevent any unauthorised access to medical private information related to patients and medical staff.
- **Medical Training** must start from the top level to the bottom level to ensure that all medical staff, including IT, are trained against various social engineering and phishing attack types.
- **Lightweight Mechanisms** are required for authentication and encryption to ensure a safe transmission of real-time medical data, especially for resource-constrained smart healthcare devices. This require ensuring the right trade-off between IoMT's system performance, and security and privacy mechanisms.
- **Intrusion Detection Systems** must be hybrid, and in some cases lightweight, and linked to machine learning (Artificial Intelligence) for a higher accuracy of detection and protection against a variety of attacks including privacy, confidentiality and integrity.

2.7/ SUGGESTIONS & RECOMMENDATIONS

Failing to implement encryption would lead to intercepting, modifying, and even deleting data beyond recovery. As such, encryption techniques, and more so dynamic encryption, must be implemented to safeguard the data and ensure its privacy and confidentiality (see FIGURE 2.12). Moreover, since most attacks have occurred due to social engineering or phishing attacks, a budget must be allocated to raise the awareness and to conduct training of medical staff, and to raise their technical knowledge to identify any potential phishing or social/reverse engineering attack. Moreover, the IT staff should undergo more specialised training in order to secure, maintain and safeguard the privacy of stored sensitive confidential medical data and information. Additionally, a strong multi-factor authentication must be employed (see FIGURE 2.13).
Note that there is a high level of mistrust among patients who are raising serious concerns about their privacy, especially that the recent attacks disclosed private medical information and data about patients. Therefore, it is crucial to establish trust and it should be given a high priority. Aside from protecting and securing data by ensuring both security and privacy, it is also important to maintain a high level of accuracy of medical robotics operations, to avoid errors that may lead to unnecessary loss of life.

In the following, we list the main recommendations towards securing IoMT systems and data.

2.7.1/ LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS

In general, security is based on cryptographic algorithms (see FIGURE 2.12) to ensure data confidentiality, integrity and availability, with source authentication, and non-repudiation. However, implementing security and privacy countermeasures introduces an

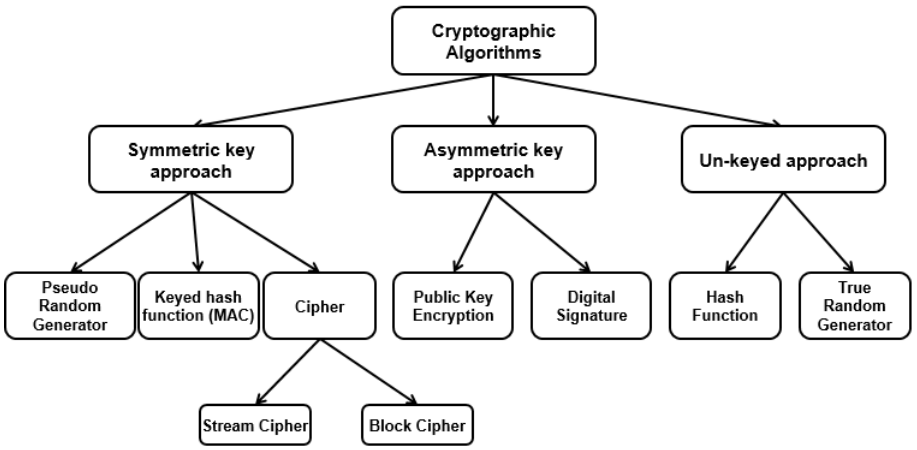


FIGURE 2.12 – Existing Cryptographic Algorithms

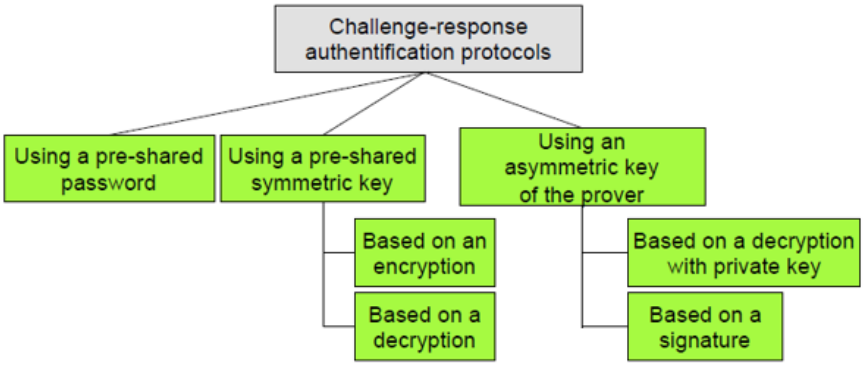


FIGURE 2.13 – Existing Authentication Cryptographic Protocol Techniques

overhead, which is considered high for some type of IoMT devices. Many related works were presented towards reducing the required latency and resources for these countermeasures. In some scenarios, medical data must be exchanged in real-time, without any delay, such is the case of live monitoring and exchanging surveillance data. Moreover, the existing algorithms would quickly drain the battery life of small medical sensors, or small endpoints within IoMT. To address this issue, the cryptographic algorithms proposed in [Melki et al., 2018, Noura et al., 2018b, Noura et al., 2018d] rely on a dynamic structure instead of the typical static structure, whereby the cipher primitives change for each new input message, and thus, they require a small number of rounds to achieve the required security level, which would require multiple rounds in a static structure. In [Noura et al., 2018b], the technique meets the expected requirements and ensures a high level of security that is both essential and mandatory for IoMT.

2.7.2/ LIGHTWEIGHT AUTHENTICATION PROTOCOLS

A survey on the existing authentication protocols for IoMT is presented in [Sey, 2018, Trnka et al., 2018, Ferrag et al., 2017], and typically, such protocols use cryptographic algorithms as a basic element. This includes a hash function (with or without key), as well

as symmetric and asymmetric cryptographic algorithms (see FIGURE 2.13). Designing an efficient cryptographic algorithm for IoMT would lead to reducing the required latency and resources of the corresponding computation. Also, it is important to reduce the required number of exchanged messages, and the size of the messages in the authentication step.

TABLE 2.12 – Recommended Security Layers & Components

Accuracy Layer	
Trust Sub-layer	• Accurate Medical Applications • Least Error Prone • Patients Trust • Trusted Medical Device/Equipment • Certified Authority • Trusted Third Party
Prevention Layer	

Authentication Sub-layer	• User/Device Authentication :
	  • Multi-factor Authentication
	  • Physical Protection
	  • Strong and Variable Password
	• Source Authentication and Message Integrity
	• Access Control

Privacy Sub-layer	• Patients Privacy • Anonymity (Pseudonymity) • Proxies VPN • Preserving Privacy at Cloud (Differential Privacy, Secret Sharing, Homomorphic Encryption)
Data Confidentiality Sub-layer	• Encryption Algorithm
Defensive Layer	
Detection Sub-layer	• Intrusion Detection Systems (Anti-malware) • SIEM • Honeypots • Data System Integrity
Correction Sub-layer	• Intrusion Prevention Systems • Firewalls • Data Backup • Alternative Devices and Configuration

2.7.3/ LAYERED SECURITY ARCHITECTURE

The security layers in IoMT, as shown in TABLE 2.12, should consist of three main layers :

1. **Accuracy Layer :** Accuracy of medical operations and tasks heavily relies on ensuring a three-way mutual trust that is set between medical staff (nurses and doctors) and medical applications and operations, medical staff and patients, patients and applications and operations.
   — **Trust Sub-Layer :** it requires the adoption of the most accurate medical applications, which must be highly accurate in a real-time manner, with zero tolerance

to errors. Moreover, digital medical devices and equipment must also be verified through a certified authority, which may or may not be linked to a trusted third party.

2. **Prevention Layer** is required to prevent any attack from within the organization, and to reduce the likelihood of any remote attack to disclose the patients' medical data. This requires establishing the right authentication, privacy and confidentiality mechanisms.
   - **Authentication Sub-Layer** requires establishing a multi-factor authentication that relies on a strongly dynamic and variable password, and on a biometric technique that is unique for each patient, which makes any attempt to breach into patients' data extremely difficult. This can also be applied to medical staff to establish the right access control mechanism by establishing the least privilege per employee's role. Moreover, user/device authentication must be established to ensure a physical protection when using medical applications to prevent any physical tampering. Finally, source authentication and message integrity must be established by relying on a certified authority between the hospital and the patient.
   - **Privacy Sub-Layer** requires taking into consideration patients' privacy as a high priority. This requires allowing patients to adopt anonymity and pseudonymity, by ensuring that they use a well-established private connection (Proxies and VPN) when being linked to medical websites or applications. Moreover, medical IT staff must rely on privacy preserving data mining techniques based on cloud and fog computing, aside the adoption of traditional privacy preserving data mining techniques such as differential privacy (Signal-to-Noise), secret sharing, and homomorphic encryption.
   - **Data Confidentiality Sub-Layer** must be maintained at all times to guard against passive attacks. This requires the adoption of lightweight cryptographic algorithms, as well as relying on quantum cryptography to protect high-value assets.
3. **Defensive Layer :** to maintain a secure e-health environment, early detection measurements are required before any corrective measures are established.
   - **Detection Sub-Layer** requires establishing and employing the most advanced up-to-date anti-malware and anti-viruses, along AI-based solutions linked to dynamic and hybrid Intrusion Detection Systems Security Information and Event Management (SIEM), and dynamic honeypots. This will ensure an early and highly accurate detection rate.
   - **Correction Sub-Layer** must be maintained as the second line-of-defense to mitigate and overcome security attacks. This includes an enhanced dynamic Intrusion Prevention Systems, dynamic and next generation firewalls, while ensuring a secure and verified data backup, with alternative devices being available for necessary computational requirements.

2.8/ CONCLUSIONS

Despite its advantages, IoMT is prone to a variety of attacks, issues and challenges that mainly target the privacy of patients and the confidentiality, integrity and availability of medical services. In this chapter, we presented and discussed the main problems,

challenges and drawbacks facing IoMT, along with the different security measures that can be implemented to safeguard and secure the IoMT domains and their associated assets, which include medical devices, systems, and medical CPSs. Moreover, different frameworks, taxonomies and approaches were presented to ensure a more enhanced and robust IoMT, and improve the patients' health and experience. Furthermore, it is important to secure the different wireless communication protocols that the IoMT relies on. Finally, it is essential to maintain a high level of security, privacy, trust and accuracy. Hence, it is highly essential and recommended to train medical and IT staff so that they do not fall victims to physical or/and cyber-attacks. As a summary, the aim of is chapter is to tighten the ties between different technical solutions and non-technical solutions to ensure a much more sophisticated, secure and efficient system in all IoMT domains.

II

CONTRIBUTION

3

Lightweight and Secure Cipher Scheme for Medical Images

ABSTRACT

With the exponential growth in Internet-of-Things (IoT) devices, security and privacy issues have emerged as critical challenges that can potentially compromise their successful deployment in many data-sensitive applications such as the medical one. Hence, there is a pressing need to address these challenges, given that medical IoT systems suffer from different limitations, and in general IoT devices are constrained in terms of energy and computational power, which renders them extremely vulnerable to attacks. However, protecting the contents of transmitted or stored medical data is of paramount importance when it comes to preserving patients' privacy. Most existing cryptographic-based solutions rely on traditional encryption algorithms having a multi-round structure, which introduces processing latency and requires increased resources. More specifically, medical images possess special characteristics compared to other types of images. The main goal of this chapter is to leverage these characteristics to design and implement an efficient and secure medical image encryption algorithm. The proposed solution defines three variants of encryption algorithms : **(a) full, (b) middle-full, and (c) selective**. The full approach encrypts all sub-matrices of an medical image, while the middle-full variant is a middle solution between the selective and full algorithms and its goal is to just hide the type of the medical image. Selective encryption identifies a set of sub-matrices of an image according to a statistical average test, known as region of interest (ROI). In the three approaches, a high security level is ensured since each image is encrypted independently of the previous and next images. Also, all primitives of the proposed cipher, such as permutation and substitution, depend on a dynamic key. Furthermore, the encryption scheme is efficient since the proposed round function is lightweight and applied for only one round. This reduces the latency and the required resources as compared to traditional cryptographic schemes. The proposed approach is flexible as it can be applied in either selective, middle-full, or full mode. Also, the size of a sub-matrix is variable and can be changed according to the available memory size. Several security and performance tests are conducted to evaluate the effectiveness of the proposed solution. The results validate the robustness of the proposed scheme against almost all considered types of attacks and show an improvement in terms of latency and resources compared to current image-encryption schemes. Also, the results confirm the robustness of the proposed algorithm in protecting the contents of medical images.

3.1/ INTRODUCTION

Digital medical images are critical diagnostic tools. They are generated using a number of technologies and are mainly used for treating and predicting diseases. These technologies include X-ray radiography, ultrasound, magnetic resonance imaging (MRI), etc. There exists a number of applications which require storing and transmitting medical images across public channels such as the Internet and hence, making them vulnerable to security threats such as privacy, confidentiality, authentication, and integrity. Hospitals are hesitant to allow access to such sensitive data via their networks, and as such, there is a great need to secure such networks and enable them with the various security services, which mainly rely on cryptographic algorithms, to resist the various types of attacks [Paar et al., 2009a, Menezes et al., 1996]. The main security services include Data Confidentiality (DC), privacy, Data integrity (DI) and Source Authentication (SA). Encrypting an image protects its private contents from being accessed by an unauthorized party. This ensures DC and privacy during transmission or storage, which can solve the problems of passive attacks. Moreover, DI service is used to ensure that the received data has not been modified during transmission and SA permits to verify the source of the image [Babel et al., 2012, Kester et al., 2015]. The traditional encryption schemes are based on symmetric key cryptography, which is efficient in terms of computational resources and latency when compared to asymmetric key cryptography (AKC). A symmetric cipher can be block or stream based ; a block cipher divides the data into separate blocks of fixed size such as the Data Encryption Standard (DES) [Smid et al., 1988], the Advanced Encryption Standard (AES) [Daemen et al., 2013] (128-bit length), the International Data Encryption Algorithm (IDEA) [Schneier, 1993], etc.

3.1.1/ PROBLEM DEFINITION

Recently, a set of medical image authentication schemes were presented in [Li et al., 2018a]-[Li et al., 2018b]. While, in this chapter, we focus to design an efficient and secure medical cipher image solution. In fact, The conventional encryption schemes that encrypt the whole plain image and not appropriate when executed on constrained devices and in the case of real-time medical applications over wireless medical networks and in mobile medical services. Recently, a selective image encryption approach was presented to overcome the existing issues of conventional encryption, whereby the insignificant parts are not encrypted, or encrypted using a light encryption method. Selective encryption reduces the computational complexity to the minimum possible level while preserving a sufficient security level. The selective approach is debatable since the most existing schemes are designed based on image compression algorithms, and thus they are codec-specific, while the rest are applied at the pixel level [Puech et al., 2005], [Bruckmann et al., 2000]-[Mostefaoui et al., 2015a]. Recent research works presented a new kind of compression algorithms that are specific for encrypting image and video, and can ensure good performance such as [Schonberg et al., 2008]-[Zhang et al., 2014a]. Therefore, we focus on this class since it provides more flexibility, being codec-independent.

In fact, the selective image encryption approach meets the requirements of real-time applications and tiny devices because a significant reduction of processing time for encryption and decryption is achieved. Different pixel selection techniques have been

suggested in the literature such as edge maps [Zhou et al., 2009], region of interest (ROI) [Ou et al., 2007], entropy-based techniques [Mahmood et al., 2011], and average of sub-matrices [Kanso et al., 2015, Mostefaoui et al., 2015a].

Nonetheless, a number of approaches, based on conventional encryption schemes such as AES, has been proposed to protect medical records in the DICOM system [nat, 2004] and in many other research chapters [Fornazin et al., 2008]-[Lima et al., 2015]. **However, traditional cryptographic algorithms are defined mainly to protect textual data**. Thus, they are not designed for encrypting multimedia contents and do not account for the intrinsic characteristics of multimedia such as (i) large data size, (ii) bulk data capacity, (iii) high redundancy and (iv) strong correlation between adjacent pixels. Therefore, a revision of the current encryption schemes should be done to propose new ones taking into account the application requirements.

Another paradigm that was investigated by researchers in the last decade is the ”Chaos” field, which consists of a non-linear dynamic system that looks like random [Baptista, 1998]. Due to its extreme sensitivity to initial conditions, chaos was integrated extensively into the design of medical image encryption algorithms [Zhou et al., 2009]-[Kanso et al., 2015]. Unfortunately, chaos-based encryption is not always secure ; some of these approaches have security weaknesses and many of them have been cryptanalyzed successfully as in [Ashtiyani et al., 2008]-[Chen et al., 2015] due to the instability arising from the periodicity of mapping [Huang et al., 2009] and the finite computing precision that renders the system vulnerable to different kinds of attacks [Arroyo et al., 2009, Alvarez et al., 2009]. Additionally, the majority of chaotic encryption algorithms is based on non-integer operations, which introduces high resource requirements and computational complexity and consequently overhead in terms of efficiency and latency, especially that a floating-point system is much more expensive than an integer one. Accordingly, we recommend to revise the chaotic cryptographic algorithms and to discretize chaotic maps (integer) to replace the real ones (original form). This is mandatory to reduce the required resources and latency overhead and to simplify the hardware implementation and cost. Recently, an image encryption algorithm for medical images was presented in [Kanso et al., 2015] but unfortunately, it suffers from the limitations of the chaotic paradigm.

It is worth mentioning that focusing on updating chaotic cryptographic algorithms and discretizing chaotic maps is justified since all traditional cryptographic algorithms are based on integer operations such as AES, which can be implemented using bytes or words of size 16 or 32 bits.

3.1.2/ CONTRIBUTION

In this chapter, an efficient encryption scheme suitable for full and selective medical image encryption applications is proposed. It exhibits low processing latency and reduced resource requirements. Depending on the application, the scheme can be used for encrypting (i) the full plain image or (ii) part of the plain image containing sensitive information. We propose to detect the sensitive regions (ROI) and the non-sensitive regions (ROB) in an image using a statistical approach based on the average of each sub-matrix, which should be greater or equal to a threshold that we obtain according to simulation results.

Towards reducing the latency and the required resources, we propose a cipher scheme with a dynamic key that changes for each input image. The proposed scheme presents 4 variants for medical image encryption as shown below :

1. **Selective Encryption-1 (SE1) :** this technique employs only a permutation of the sub-matrices of ROI. This variant requires the minimum computational complexity compared to the other variants. It is the best choice for real-time applications, and systems with constrained devices. However, this variant preserves the type of medical data ;
2. **Selective Encryption-2 (SE2) :** in addition to the permutation technique of SE1, SE2 consists also of a masking operation to the sub-matrices of ROI. As such, it provides a higher security level than SE1 because of the masking process, which is associated with a low overhead in terms of latency and resources ;
3. **Middle-Full (MF) :** this technique consists of masking the sub-matrices of ROI and permuting all the sub-matrices of a plain image (ROI and ROB). This variant is designed to hide the type of a medical image that is preserved using the previous selective variants, SE1 and SE2 ;
4. **Full approach :** this variant consists of masking and permuting all the sub-matrices of a plain image. It requires more overhead compared to the middle and selective variants and it is used to obscure all useful information for the encrypted medical image.

The common property among these variants is that they are all iterated for just one round and have a key-dependent structure. Moreover, the round function is based on a permutation table (P-box) and a substitution table (S-box) that are both dependent on a dynamic key and an initial matrix IM, which is introduced to enhance the statistical randomness of the proposed masking function. The dynamic key generation algorithm produces a key, which depends on a secret key and an Initial Vector (IV) and that should be changed for each input image to guard against cryptanalytic attacks. Additionally, the different steps of the cipher are variable and depend on this dynamic key in contrast to the existing solutions that employ a static cipher structure and require several rounds. The proposed technique reduces the number of rounds to just one since variable cipher primitives are applied to each input image and the desired randomness degree is attained. Consequently, this reduces the execution time while maintaining a high security level. Simulation results verify the high performance and the robustness against existing attacks.
Note that the proposed scheme is easily applicable to other kinds of images that require selective and full encryption. The novelty of the proposed approach is that it is based on a dynamic approach, where the substitution and diffusion operations are variable and can be changed for each new input image. In addition, the proposed cipher only requires one round and its round function is very lightweight compared to the existing solutions such as 3DES and AES.

3.1.3/ ORGANIZATION

The chapter is organized as follows : Section 3.2 describes the statistical approach for the selection of the ROI. Section 3.3 gives a detailed look on the key derivation used in this model. Then, detailed description of the proposed image encryption scheme is presented in Section 3.4. Next, we explain in details the various cipher operations of the proposed

scheme in 3.5. In Sections 3.6 and 3.7, we test a number of parameters to prove that the cipher has the requirements to prevent cryptanalytic attacks. In Section 3.8, we discuss the immunity of the proposed cipher variants against cryptanalysis and we study their corresponding execution times. Finally, the chapter is concluded in Section 3.9.

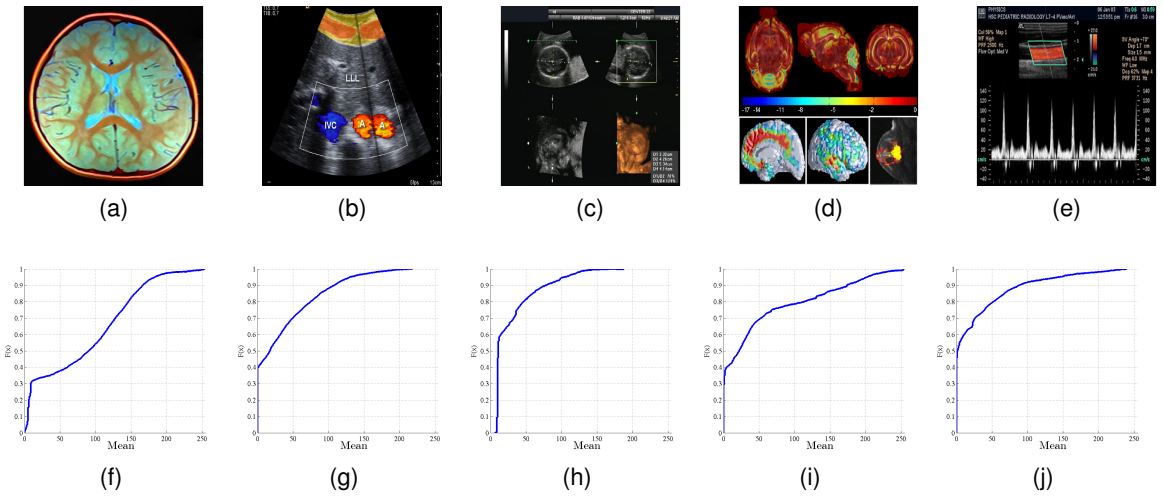


FIGURE 3.1 – Original images studied (a)-(e) and their corresponding ECDF of the sub-matrices average (f)-(j).

3.2/ SELECTIVE ENCRYPTION BASED ON SUB-MATRICES

The proposed image encryption scheme targets digital medical images and can also be applied to other kinds of digital images. Medical images possess special features making them of special interest ; they usually consist of two regions :

— the Region of Interest (ROI), which contains the sensitive information ;
— the Region of Background (ROB), which contains the non-sensitive information.

An input medical image, in matrix form, has a size is $r \times c \times p$, where r is the number of rows, c is the number of columns and p is the number of planes (in gray scale p=1). The number of blocks in the image is padded, if necessary, to obtain a multiple of h^2 complete sub-matrices ; each sub-matrix consists of $(h \times h)$ bytes. In the rest of the chapter, h will be set to 8 and an optimum value may be selected depending on the application and the available memory space. The total number of sub-matrices is α, where $\alpha = \lceil \frac{r \times c \times p}{h^2} \rceil$. In order to locate the Region of Interest, we adopt a threshold segmentation method based on the average and the standard deviation, as explained in [Kanso et al., 2015]. Indeed, in this chapter, for each sub-matrix, the average only is required and it is computed and compared against a threshold to detect its corresponding region.

Different kinds of medical images such as X-ray and Ultra-sound are analyzed in order to quantify the threshold by analyzing the Empirical Cumulative Distribution Function (ECDF) of the average of sub-matrices.

According to experimental (simulation) results, we found that almost all the ROI sub-matrices have an average greater than the threshold $\tau = 10$, as shown in FIGURE 3.1

based on the ECDF of the average of sub-matrices. All sub-matrices of ROI have a mean that falls in the interval [τ, 255].

The average of each sub-matrix is calculated and compared against this threshold to determine whether or not to consider it as significant. If the average of a specific sub-matrix is greater than the threshold, then, it is flagged as part of ROI and it will be encrypted. ROB sub-matrices are not encrypted since they can affect seriously the latency and influence the resources. Note that the encrypted parts from ROI are combined with the unchanged parts from ROB before being stored or sent over the channel.
The decryption scheme applies the same classification in order to locate the encrypted ROI sub-matrices that should have a higher value close to the average (128) since encrypted sub-matrices exhibit the uniformity propriety. On the other hand, TABLE 3.1 presents the notation and symbols used in this chapter.

TABLE 3.1 – Table of Notations

Notation	Definition
L	Number of rows
C	Number of columns
P	Number of planes (in gray scale p=1)
SK	Secret Key
DK	Dynamic Key
IV	Initialization Vector
K_S	Substitution Key
K_P	Permutation Key
IM	Initial Matrix
i	Index of Sub-matrix from [1, l]
IM_i	Dynamic Initial matrix with index i
h	Size of a block (sub-matrix)
ψ	Dynamic Counter
l	Number of sub-matrices (equal to α for the full approach and β for the selective)
α	Number of sub-matrices in one image
β	Number of ROI sub-matrices in one image
rs	Number of rounds to produce a good S-box
rp	Number of rounds to produce a good P-box

3.3/ KEY DERIVATION

In order to achieve low complexity and simple implementation on constrained devices, we consider one Secret Key shared between the transmitter and receiver. To protect the key, it can be renewed by using Elliptic Curve Diffie Hellman (ECDH) and transmitted to the receiver in an encrypted form or via a feedback channel. In order to make the algorithm even more secure, the key is renewed after a periodic interval depending on the application.

3.3.1/ DYNAMIC KEY GENERATION, D_k

The secret key is xor-ed with an initialization vector IV (128 bits), which is then hashed using SHA-512 to form the dynamic key of size 64 bytes. Note that the initial vector is changed for every image hence the dynamic feature of the key is maintained. Next, the dynamic key is divided into 4 sub-keys as such :

- **The Permutation Key**, K_P, is used to generate a dynamic permutation table, P-box, which is used to permute the selected sub-matrices according to the cipher variant. For example, it is used to permute ROI sub-matrices for SE1 or SE2. The 128 bits of K_P are taken from D_k and this sub-key can be used with any stream cipher to produce the required binary key stream to control the proposed Modified Group Operation Permutation algorithm (MGRP). Then, MGRP is iterated for Rp times to obtain the P-box, which has a length of β and its values are within $[1,\ l]$.
- **The Substitution Key**, K_S, is used to generate a dynamic substitution table, S-box. Another set of 128 bits are extracted from D_k and can be used with the same stream cipher to produce the required binary key stream for rs iterations of MGRP. Note that the produced S-box has a length of 256 and its values vary between [0, 255].
- **Initial Matrix**, IM : The third set of 128 bits of D_k will be passed to the same stream cipher to produce a key stream sequence with h^2 byte length. This sequence will be reshaped to form an initial matrix IM with size $h \times h$, which will be used to construct the different IM_i that vary for every sub-matrix, $i = 1, 2, \ldots, \beta$.
- **Counter** ψ : The fourth group of 128 bits is used to obtain another matrix ψ that is also used in the construction of IM.

The above sub-keys are unique for every image and are all derived from one dynamic key that changes for every input image. Below is an explanation of these components. The initial matrix, IM, will be used as a starting point to generate all the required IM_i where i is a variable between [1, l]. As such, we use a different IM for every sub-matrix to add randomness to the system and hence to lower the success probability of cryptanalytic attacks. IM is first xor-ed with the first value of the initial vector ψ. Then, the result will undergo a substitution process using a dynamic key K_S. The result is used as the first IM. The process continues similarly while incrementing the dynamic counter ψ. After each iteration, a right shift operation is applied to the S-box. For example, for the first operation, when $\psi = 1$, no shift operation is done to the S-box, while for $\psi = 2$, one right shift is performed as indicated in Figure 3.3. The importance of this operation is that all the required IM_i can be obtained in parallel for the encryption process. Accordingly, the execution time will be reduced because of the parallelism property inherent in this algorithm. Not only do we achieve a high level of security, but also a lower execution time as compared to existing multi-round cipher algorithms.

3.4/ THE PROPOSED CIPHER ALGORITHM

In this section, the proposed cipher algorithm is described. We start by introducing the selective approach and then, we provide details about the permutation and masking processes. Finally, we describe briefly the decryption process.

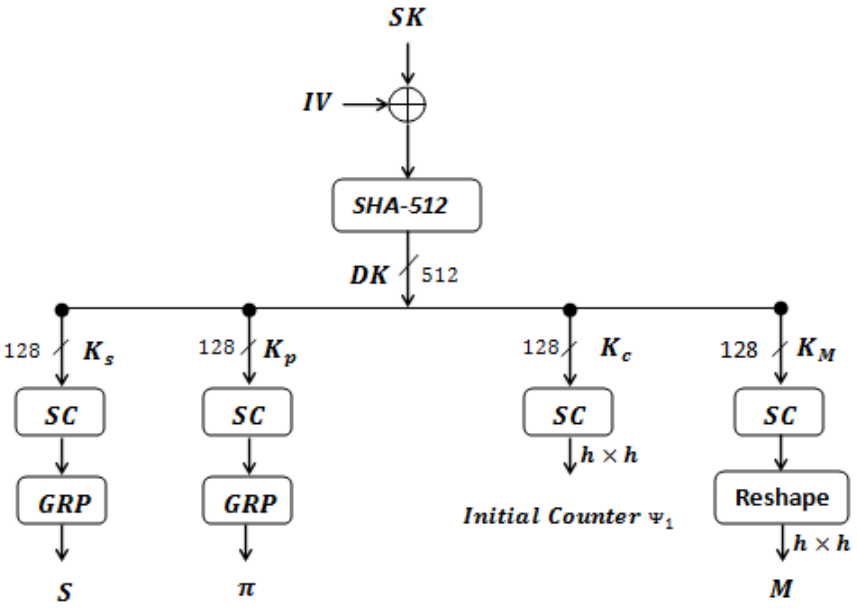


FIGURE 3.2 – Proposed dynamic key generation technique and the corresponding dynamic sub-keys

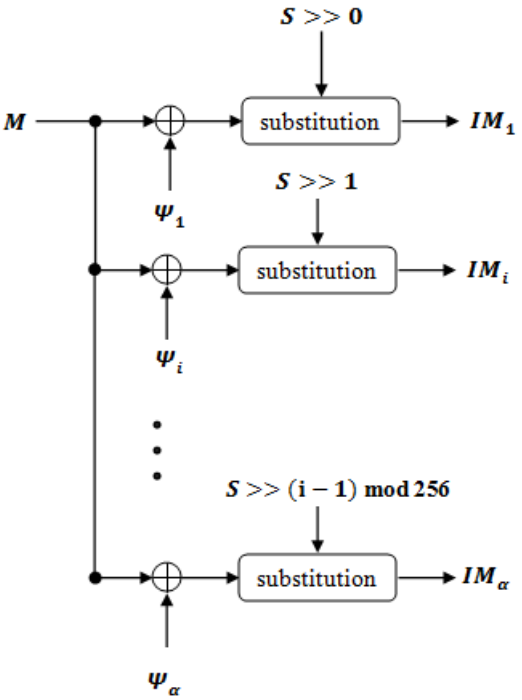


FIGURE 3.3 – The proposed technique to generate the required pseudo-random masking sub-matrices.

3.4.1/ ENCRYPTION PROCESS

In FIGURE 3.4, the encryption scheme is illustrated. First, the input α sub-matrices are subjected to the threshold test. If the average of each sub-matrix exceeds the τ parameter, then this sub-matrix will be considered as a part of ROI, otherwise, it is considered as part

of ROB.

The selective cipher option has two variants, the first one, $SE1$, applies only a permutation among the selected sub-matrices, without the masking operation. While, the second variant, $SE2$, employs additionally the masking operation, which makes the system resilient against cryptanalytic attacks. Accordingly, each selected sub-matrix will be xor-ed with its corresponding IM_i. The result will be also xor-ed with the corresponding dynamic permutation sub-matrix for this selected sub-matrix. Next, another substitution is performed to increase randomness. This whole masking process is done for every sub-matrix. Then, a permutation between the sub-matrices will be performed based on a new P-box that is obtained by flipping the P-box array from right to left. This operation further randomizes the relationship between the selected sub-matrices. Finally, all sub-matrices are concatenated (ROI and ROB) to form the final encrypted image.

The second option, Middle-Full, has the principal objective of hiding any information related to the type of the medical image. A global permutation operation is done on all sub-matrices as compared to the previous operation, $SE2$, which applies it to the β sub-matrices. Global permutation is done on both ROI and ROB regions. Hence, it will be very hard for an attacker to recognize the type of the image. These steps, in the selective or middle approaches, ensure a sufficient level of security for images, and hence provide an efficient approach for medical image encryption.

It is important to note that the execution time of such a scheme is low since only the important regions of the image are encrypted. Also, the use of a dynamic key, a single round, and a low number of operations is sufficient to achieve the required security level. This approach may be extended by additional chaining ; more randomness could be added to the scheme but parallelism will not be feasible. In this work, we achieved satisfactory results without chaining, however, it can be adopted by users who require additional protection for their images. The following equation represents the extended model :

$$C_{ip} = S(X_{ip} \oplus S(X_i \oplus IM_i)), \quad i = \{1, 2, 3, ..., \alpha\} \tag{3.1}$$

where

- S represents a dynamic S-box.
- X_{ip} represents the corresponding permutation of X_i.
- IM_i represents the corresponding initial matrix to be xor-ed with the sub-matrix X_i.

3.4.2/ Decryption Process

Decryption is similar to the encryption process but in a reverse manner. The receiver performs the same encryption steps but in a backward approach, and using the inverses of S-box and P-box. In case of global permutation, we first perform an inverse global permutation. Decryption is complete when all the sub-matrices are decrypted and then grouped to re-construct the original image. Decryption could be represented by :

$$C_{ip} = S^{-1}(Y_{ip} \oplus S^{-1}(Y_i \oplus IM_i)), \quad i = \{1, 2, 3, ..., \alpha\} \tag{3.2}$$

where

- S^{-1} represents the inverse of the dynamic S-box.
- Y_i represents the received encrypted sub-matrix from ROI.

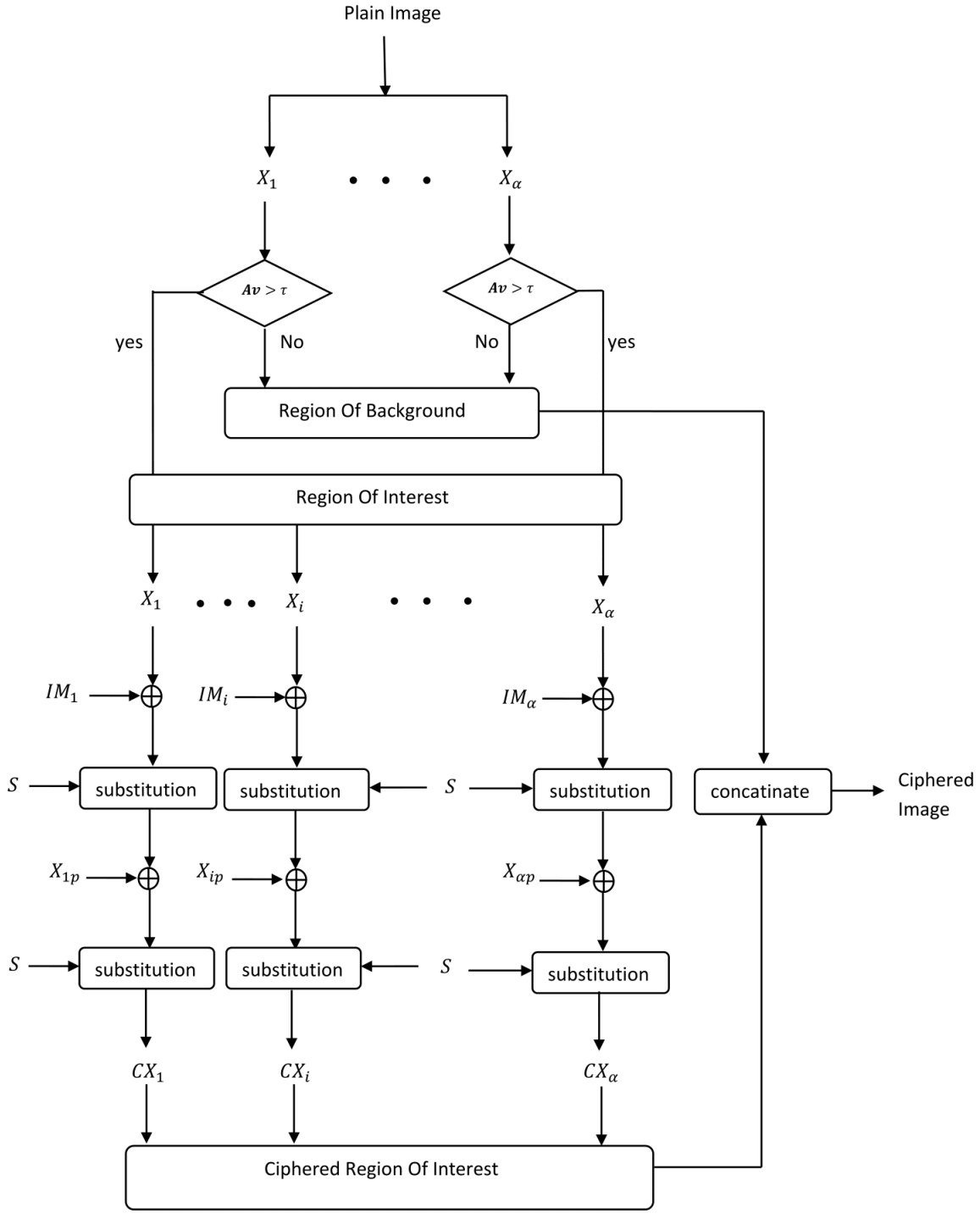


FIGURE 3.4 – Proposed Selective Encryption-2 (SE2) Scheme.

- Y_{ip} represents the corresponding inverse permutation of Y_i at index i.
- IM_i represents the corresponding initial matrix for the sub-matrix Y_i.

In the proposed approach, the channel error will not propagate since every sub-matrix is encrypted independently of the other sub-matrices.

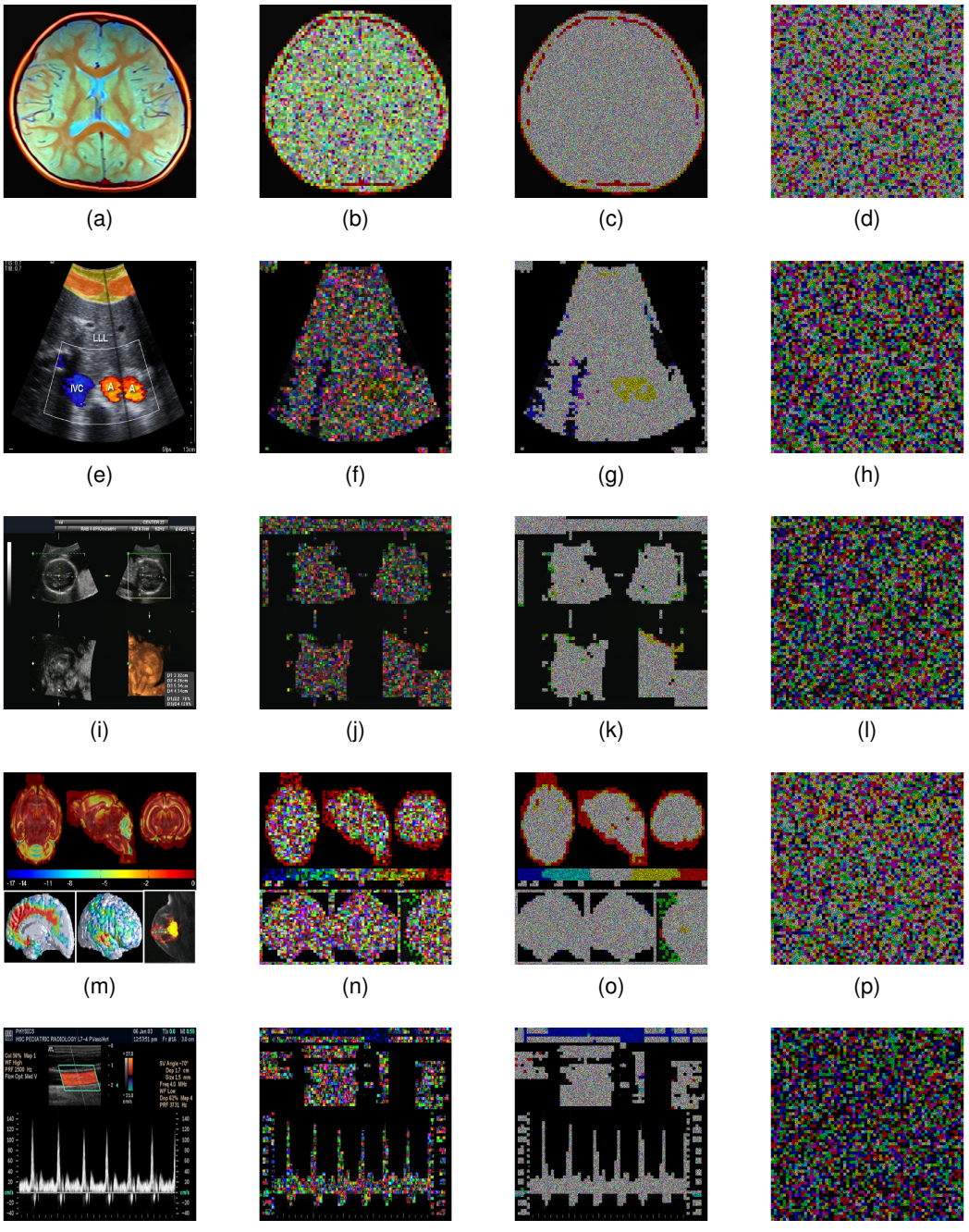


FIGURE 3.5 – (a) Original Brain MRI image, (b) encrypted image after permutation, (c) encrypted image after masking, (d) encrypted image after global permutation.
(e) Original Aorta image, (f) encrypted image after permutation, (g) encrypted image after masking, (h) encrypted image after global permutation.
(i) Original Head-3D , (j) encrypted image after permutation, (k) encrypted image after masking, (l) encrypted image after global permutation.
(m) Original image 06, (n) encrypted image after permutation, (o) encrypted image after masking, (p) encrypted image after global permutation.
(q) Original Spectral Doppler, (r) encrypted image after permutation, (s) encrypted image after masking, (t) encrypted image after global permutation.

Algorithm 1 GRP permutation algorithm

```
1: procedure GRP(R_src, CR, l)
2:     j ← 0
3:                          ▷ If the control register bit is zero, place its corresponding index at left
4:     for i ← 0 to l − 1 do
5:         if CR[i] == 0 then
6:             R_dest[j++] ← R_src[i]
7:      ▷ After that, if the control register bit is one, place its corresponding index at right
8:     for i ← 0 to l − 1 do
9:         if CR[i] == 1 then
10:            R_dest[j++] ← R_src[i]
11:                                  ▷ R_dest is the output substitution vector
12:    Return R_dest
```

3.5/ CONSTRUCTION OF CIPHER PRIMITIVES

The proposed techniques to generate dynamic key-dependent S-boxes and P-boxes are presented next. This is done by using a modified version of the group operation of permutation [Shi, 2004]. key-dependent permutation and substitution tables are generated and used in the encryption process, while their corresponding inverse tables are used in the decryption process.

3.5.1/ CONSTRUCTION OF DYNAMIC PERMUTATION AND SUBSTITUTION TABLES

After the dynamic key generation, permutation and substitution tables are built and the keys are used to produce a corresponding key-stream sequence as described in Section 3.3. The generation of the dynamic permutation and substitution primitives is done using a key-dependent permutation algorithm based on the GRP permutation algorithm [Shi, 2004]. GRP is chosen as a basic element since it is simple, flexible and efficient in terms of software and hardware implementations. The GRP permutation algorithm is described in Algorithm 1. Note that R_src is the input vector, CR is the configuration vector (control register) and R_dest is the output. R_src, CR and R_dest all have the same length, which is equal to l for constructing the permutation table and 256 for the construction of the substitution table.

The basic idea of the GRP is to divide the index into two groups according to the pseudo-random bit sequence (CR). If the bit in CR is 0, this index is moved to the first group, otherwise, the element is moved to the second group as seen in FIGURE 3.6.

However, the original GRP algorithm performs poorly for just one iteration due to the low number of unique output vectors and the high number of fixed points as shown in FIGURE 3.7. As such, and to enhance the GRP algorithm, we iterate for multiple rounds, whereby for each round, a different control CR_i, $i = 1, 2, \ldots, rs$ is used. Also, for each round, CR_i and $\overline{CR_i}$ are used respectively, for the two iterations of the GRP algorithm. The enhanced algorithm is described in TABLE 2.

Algorithm 2 Proposed substitution algorithm

procedure PERM($DK,\ l,\ rt$)
▷ l is the length of input vector
    $R\_src \leftarrow 0$ to $l-1$
    for $w \leftarrow 1$ to rp **do**
        $CR_w \leftarrow CR[(w-1)\times l\ :\ (w)\times l-1]$
        $R\_src = GRP(R\_src,\ CR_w)$
        $CR_w \leftarrow \overline{CR_w}$
        $R\_src = GRP(R\_src,\ CR_w)$
    ▷ Last R_src can be a dynamic $Pbox$ or $S-box$.
    Return R_src

FIGURE 3.6 shows an example of the **proposed** GRP algorithm implementation for 8 elements.

To produce a substitution table (S-box) or permutation table (P−box), an initial vector R_src is used, where $R\_src[j] = j$ and $j = 0, 1, \ldots,\ l$ ($l = 256$ for substitution table and equals to α or β for the permutation table according to the cipher option). Then, the process of permutation is applied for rt times. The output vector R_dest, after each permutation iteration, becomes the input vector R_src for the next one. The cryptographic performance of the output R_dest is quantified for each iteration. This transformation is applied for multiple rounds $irs = 1, 2, \ldots, rs = 10$.

Therefore, dynamic permutation and substitution tables can be produced by applying the proposed permutation algorithm for ≥ 5 rounds (different CR for each iteration). Since the process of the substitution layer generation is based on the use of permutation, the produced S-boxes will feature a high probability of unique dynamic S-boxes (PoU) ($\approx 0.8 \times 2^q!$ as seen in FIGURE 3.7 for $q = 3$) compared to using fixed CR. Even though the dynamically generated P-boxes and S-boxes (output vector R_dest) exhibit good cryptographic characteristics, yet, these are still lower than the maximum achieved by static S-boxes that are used in the modern block cipher (AES).

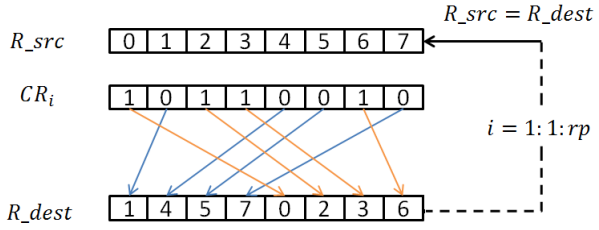


FIGURE 3.6 – Example of constructing a permuted vector ($P-box$) based on the GRP algorithm with $q = 3$ and for a specific CR.

Consequently, a good randomness degree, a large number of different unique S-boxes are generated with a lower probability of fixed points (close to $\frac{1}{2^q}$ on average) and an acceptable CC ($O(2^q)$) can be achieved using the proposed permutation algorithm. An example of producing dynamic S-box for $q = 8$ and its corresponding inverse $(\text{S-box})^{-1}$

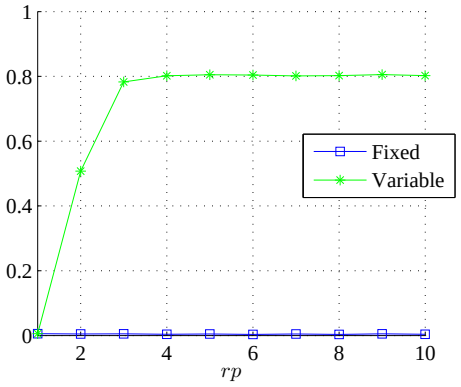
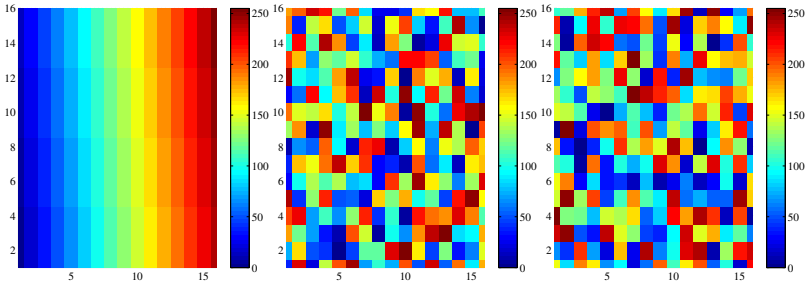


FIGURE 3.7 – Variation of the average of PoU for 2^{15} random CR versus rp (here $rp = rs$) using fixed and variable CR



(a) V in matrix form (b) P-box (c) P-box$^{-}1$

FIGURE 3.8 – Original input matrix of R_src (a), generated P-box by using a random dynamic key (b) and its corresponding inverse one (c) for $l = 256$

are shown in FIGURE 3.8.

3.5.2/ CRYPTOGRAPHIC PERFORMANCE OF DYNAMIC SUBSTITUTION

A robust and efficient key-dependent construction technique of substitution tables (S-boxes) should ensure several cryptographic criteria such as bijectivity, Linear Probability Approximation Function (LPF), Differential Probability Approximation Function (DPF), Strict Avalanche Criterion (SAC), and output Bits Independence Criterion (BIC).

In the following, these criteria are described briefly and the results of the proposed construction technique are presented in order to prove that the proposed technique ensures good cryptographic performance in a dynamic manner.

— **Bijectivity** : This criteria validates that an inverse S-box exist, and hence, the substitution transformation can be reversed in the decryption algorithm. A simple technique to verify the bijectivity is to compute the different number of elements needed for the S-box using the unique function. If the number of unique elements equals to 2^q for Galois field q, then this S-box is bijective, otherwise it is not. In the proposed model, a bijective permutation technique based on GRP algorithm is

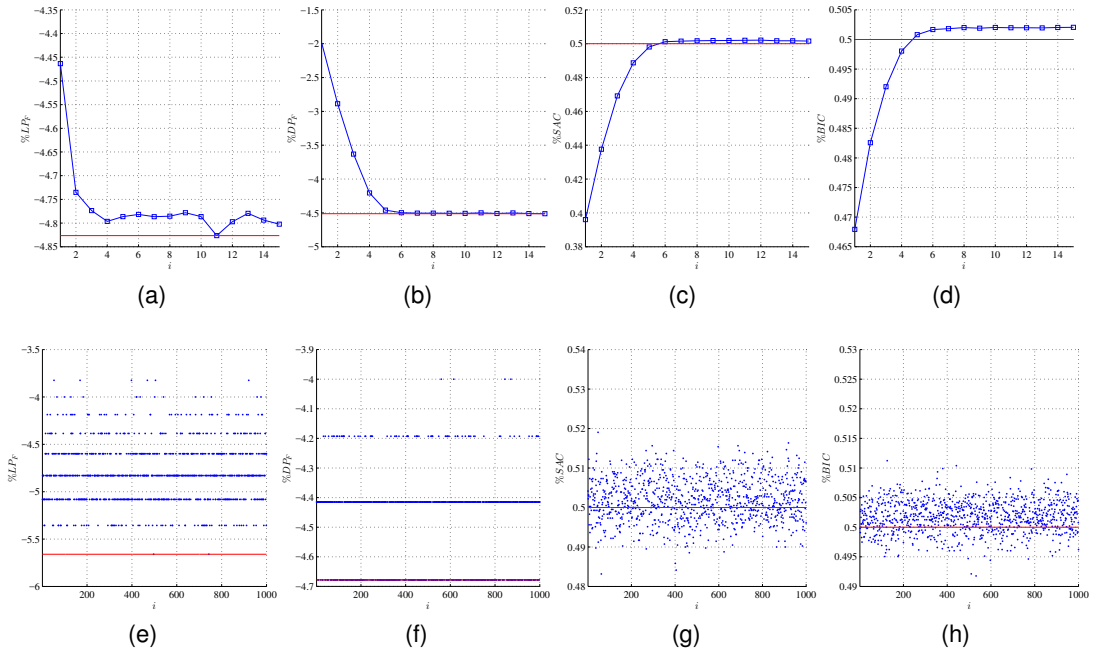


FIGURE 3.9 – Variation of the average LPF (a), DPF (b), SAC (c), and BIC (d) versus rs for the proposed S-box.
Variation of the average LPF (a), DPF (b), SAC (c), and BIC (d) against 1,000 dynamic keys for $rs = 5$.

employed and consequently the proposed S-box is bijective.

— **Linear Probability approximation Function** LPF : A lower LPF value indicates higher immunity against linear attacks since there would be no linear relationship between bits of the plain text and the substituted ones [Heys, 2002]. The average variation of the LPF values *versus* the number of iterations is shown in FIGURE 3.9-(a). The results indicate clearly that the required number of iterations to reach a stable low LPF value, close to $2^{-4.79}$, is 5. Also, in FIGURE 3.9-(e) the variation of LPF for 10,000 random K_S is presented and the maximum, minimum and average values of LPF are $2^{-3.8}$, $2^{-5.7}$ and $2^{-4.8}$, respectively. In fact, the majority of the produced substitution tables have low and acceptable LPF values. This, combined with the dynamic nature of the S-boxes, ensures sufficient resistance against linear attacks.

— **Differential Probability approximation Function** DPF : This criterion shows the effect of a slight change in plain-text pairs on the corresponding substituted pairs. Typically, a low value of DPF indicates high resistance against differential attacks [Biham et al., 2012]. In FIGURE 3.9-(b), the average variation of DPF versus the number of iterations to reach a low stable value of DPF, close to $2^{-4.5}$, is also 5. Additionally, in FIGURE 3.9-(f), the maximum, minimum and average DPF values for 1,000 dynamic keys are shown and they are equal to 2^{-4}, $2^{-4.69}$, and $2^{-4.41}$, respectively.
These results confirm that the generated S-boxes ensure good cryptographic performance against differential attacks.

— **Strict Avalanche Criterion,** SAC : This criterion is to show that a one-bit change in

any element of an S-box produces a different substituted element by at least 50%. The variation of the probability of SAC with regards to different number of iterations is shown in FIGURE 3.9-(c). The results indicate that 5 iterations are necessary to be closer to the SAC ideal value of 0.5. Also, in FIGURE 3.9-(g), the variation of SAC for 1000 produced random S-boxes with the proposed technique are shown and the results indicate that the SAC value is always close to 0.5.
These results validate that the proposed technique is compliant with the SAC criterion.

— **Bit Independence Criterion,** BIC : This states that two output bits j and k must change independently when a single input i is changed for all i, j and k. The probability variation for different number of iterations is illustrated in FIGURE 3.9-(d). It is clear that the probability values of BIC become close to the optimal value 0.5 when $rs = 5$. In FIGURE 3.9-(h) the variation of BIC for all produced S-boxes is close to 0.5. This validates the BIC criterion. Therefore, according to these results, rs and rp are chosen to be equal to 5.

3.6/ ENCRYPTION/DECRYPTION EFFICIENCY ANALYSIS

In this section, we assess the performance of the proposed flexible cipher variants. We consider a number of ordinary and medical images of different structures. Then, selective and full encryption are applied to these images using the proposed variants. In the second selective encryption variant, SE2, ROI is encrypted using the same algorithm as full encryption and we present various tests to prove the robustness of the proposed cipher for selective as well as for full encryption in the next section.

For selective encryption, we consider square blocks of size 8×8 and τ=10. We compute a set of Effective Cumulative Probability Density Functions, to identify a specific threshold. Also, in this section, we present ROI and ROB in the encrypted image. The mean for the ROI encrypted region is close to 128, which is the required criteria for the feasibility of decryption. The recovery of the original plain images was verified since the same regions of the selectively encrypted images are also selected for decryption. In figure 3.10, it is obvious that the five images presented in our tests have a clear average, which makes the decryption possible.

Moreover, the ECDF for the same five images are presented in Figure 3.1 indicating that the ECDF is preserved and the encryption starts from the point that we have no zero-value pixels (black pixels), which are considered as the background. ECDF defines the threshold relative to the average of every sub-matrix in the image. The size of matrix used is 8×8. We select three images from Figure 3.5 for selective and full encryption and the results are presented in Figure 3.11. Comparing the full approach with the selective one, it is clear that the result of global permutation, done after the masking process, is the closest to full encryption, which indicates that the level of security is preserved, yet, with less computational overhead. The recovered images are identical to those presented.

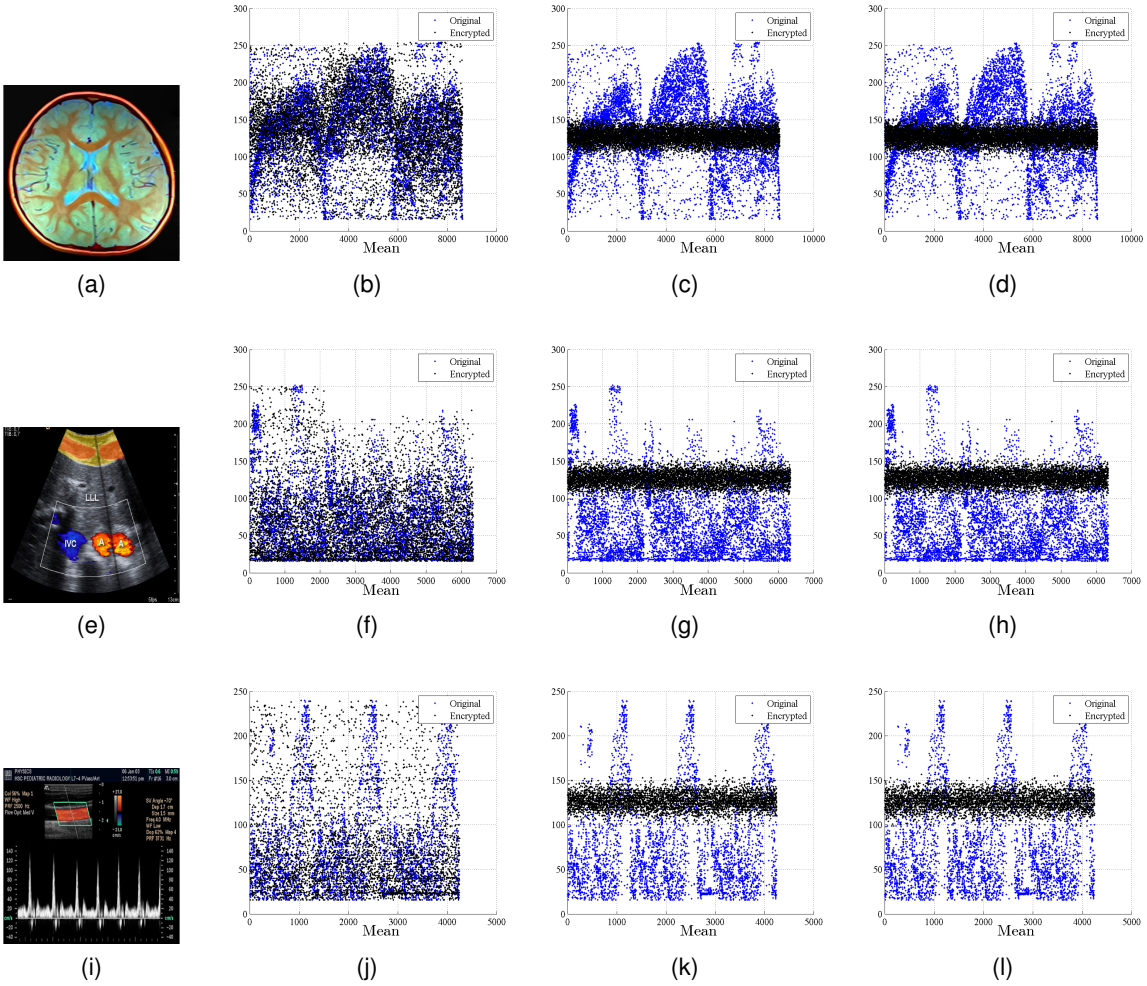
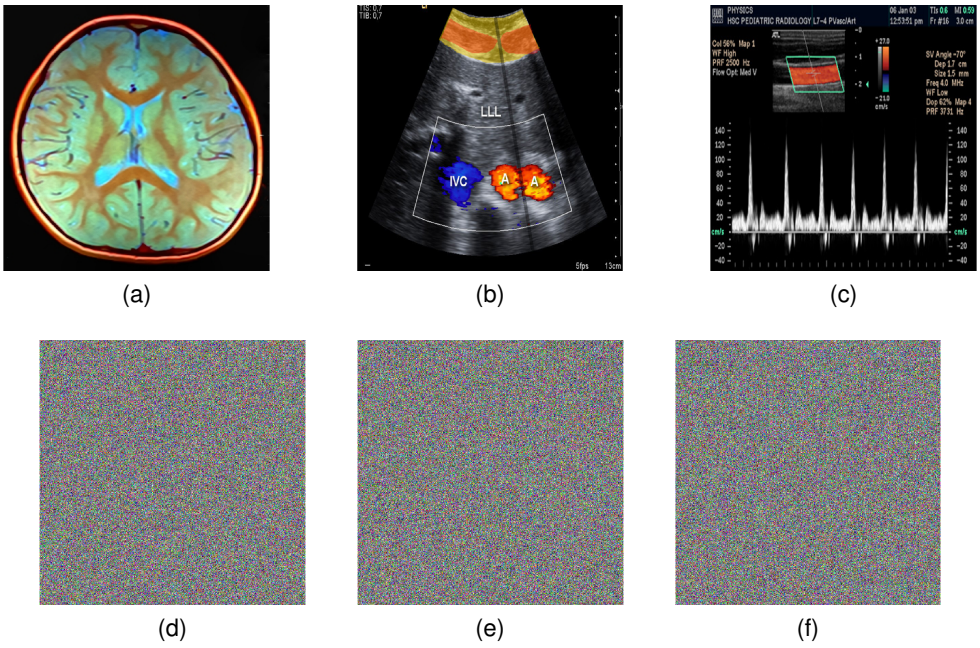


FIGURE 3.10 – Distribution of ROI and ROB ; ROI is represented by the black points and ROB is represented by the blue points. First column represents the original images ; Second column represents the distribution of pixels after permutation ; The third column represents the distribution after masking ; The fourth line represents the distribution after global permutation.

3.7/ STATISTICAL AND SECURITY ANALYSIS

In this section, we assess the cryptographic robustness against different kinds of attacks such as statistical, chosen/known plain text attacks in both approaches, full and selective. Accordingly, several statistical metrics are presented to prove that the cipher images ensure a high randomness degree in addition to key sensitivity, which is an essential criterion since our approach is based on a dynamic key. On the other hand, the required latency is reduced since the core function of the cipher, the round function, is iterated only once. In the following, we prove that one round is sufficient to reach the desired performance. More importantly, the structure of the proposed cipher scheme can be implemented in parallel, which further reduces the associated latency.



(a) (b) (c)

(d) (e) (f)

FIGURE 3.11 – Original images Brain MRI (a), Aorta (b), and Spectral Doppler (d) with their corresponding encrypted results using full encryption approach (d)-(f).

3.7.1/ UNIFORMITY OF PROBABILITY DENSITY FUNCTION

To resist statistical attacks, the encrypted image should have certain random properties. The most important one is the Probability Density Function (PDF) of the encrypted image, which should be uniform ; that is, each symbol has an occurrence probability close to $\frac{1}{n}$, where n is the number of symbols. The PDF of the four original plain-images and their corresponding cipher images are shown in Fig. 3.12. It can be seen that the PDF of the encrypted images using the proposed scheme is close to a uniform distribution with a value close to 0.039 that is $\frac{1}{256}$. Note that, since the permutation doesn't affect the distribution of pixels, we can see that, after masking, the PDF of encrypted ROI tends to be uniform. Additionally, the PDF of encrypted images after full encryption is also similar to the second variant of the selective encryption algorithm. To validate this result at the sub-matrix level, an entropy test is performed and described next.

TABLE 3.2 – Simulation Results with $h = 8$

	min	**mean**	**max**	**std**
Dif	49.8877	49.9997	50.1071	0.0340
Entropy of original sub-matrix	2.1823	4.2014	5.7813	0.7991
Entropy of encrypted sub-matrix	5.4200	5.7666	6.0000	0.0766
KS	49.8828	49.9982	50.1067	0.0349
NPCR	99.5747	99.6097	99.6468	0.0118
UACI	33.2960	33.4646	33.6079	0.0460

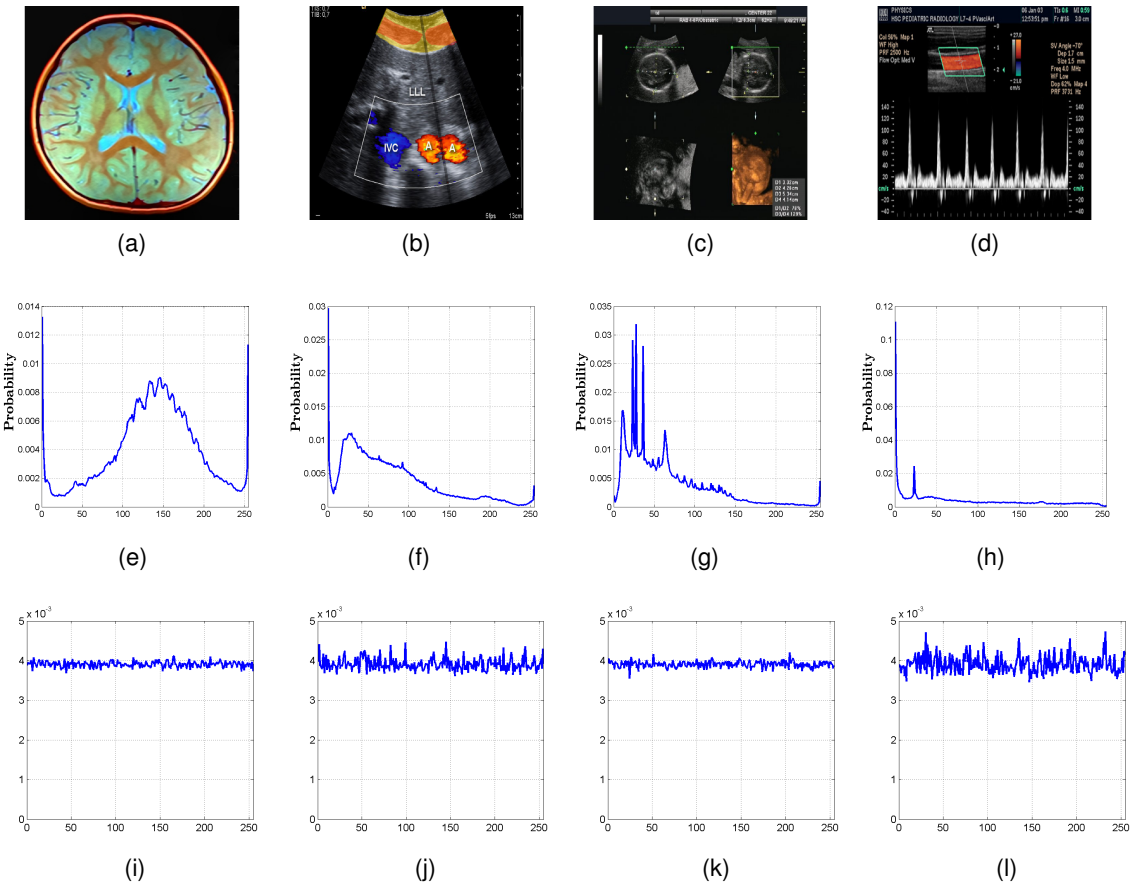


FIGURE 3.12 – Original medical images (a)-(d) and their corresponding PDF (c)-(h). PDF of the corresponding encrypted images after full encryption (i)-(l).

TABLE 3.3 – Simulation Results with $h = 16$

	min	**mean**	**max**	**std**
Dif	49.8955	49.9989	50.1330	0.0343
Entropy (original sub-matrix)	2.7235	4.9910	6.8398	0.9624
Entropy (encrypted sub-matrix)	6.9631	7.1730	7.3445	0.0523
KS	0.0308	0.0359	0.0436	0.0017
NPCR between original and cipher images	49.8581	50.0004	50.1029	0.0342
UACI between original and cipher images	99.5724	99.6093	99.6460	0.0125

3.7.2/ ENTROPY ANALYSIS

The entropy information of an image M is a parameter that measures the level of uncertainty in a random variable, and is defined using the following equation :

$$H(m) = -\sum_{i=1}^{h^2} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{3.3}$$

Where $p(m_i)$ represents the occurrence probability of the symbol m_i, and h^2 is the size of

the square matrix $(h \times h)$; the entropy is expressed in bits. A truly random entropy source is equal to 7 when $h = 16$ for a uniform distribution. We are calculating entropy at the sub-matrix level. A value close to $\log(h^2)$ is the desired value.

$$H(m) = -\sum_{i=1}^{n} \frac{1}{(h \times h)} \log_2 \frac{1}{(h \times h)} = \log_2(h^2)$$

Looking at Figure 3.13, we can clearly see that for $h^2 = 16 \times 16$, H is between 7 and 7.3 for the encrypted image. Also, we can see in the Figure the difference between the entropy of the original plain image and the encrypted one. We can conclude that our system is safe against statistical attacks.

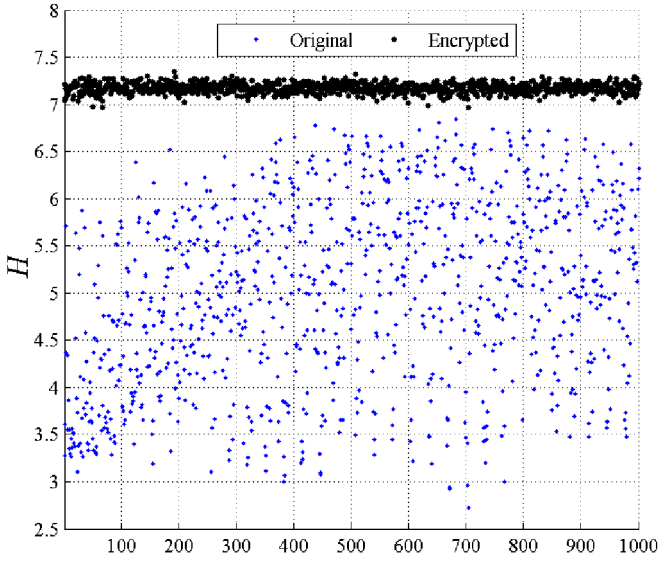


FIGURE 3.13 – Entropy test for the cipher sub-matrices with $h = 16$ for the full approach.

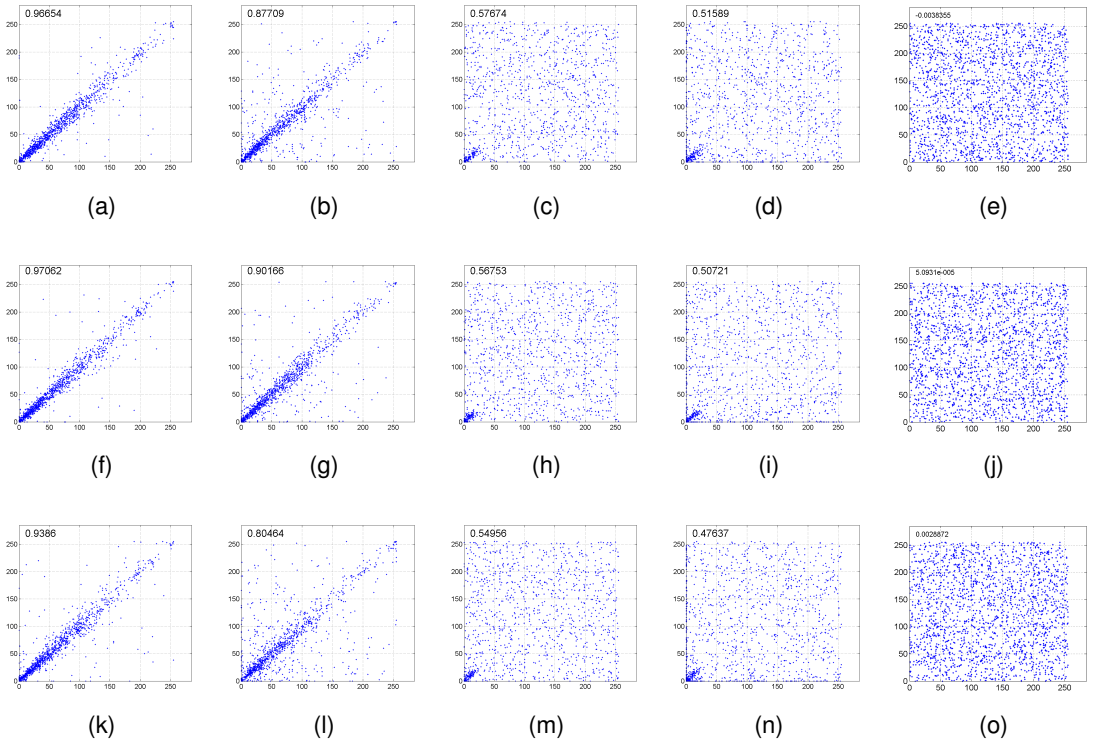


FIGURE 3.14 – For Aorta image , (a), (b), (c), (d), (e) represent the vertical correlation : original, after permutation, after masking, after global encryption and full encryption respectively. (f), (g), (h), (i), (j) represent the horizontal correlation : original, after permutation, after masking, after global encryption and full encryption respectively. (k), (l), (m), (n), (o) represents the diagonal correlation : original, after permutation, after masking, after global encryption and full encryption respectively.

3.7.3/ CORRELATION ANALYSIS

Correlation is an important metric that must be assessed. Removing the correlation among the pixels of an image is a successful indication that the cipher is immune to statistical attacks. Having a correlation coefficient close to zero means that the cipher ensures a high degree of randomness. The correlation test is applied by taking randomly N random pairs of adjacent pixels from the known plain image and their corresponding encrypted ones. The correlation coefficient r_{xy} is calculated using the following equation :

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x) \times D(y)}} \tag{3.4}$$

where

$$E_x = \frac{1}{N} \times \sum_{i=1}^{N} x_i \quad , \quad D_x = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))^2$$

and

$$cov(x,y) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$$

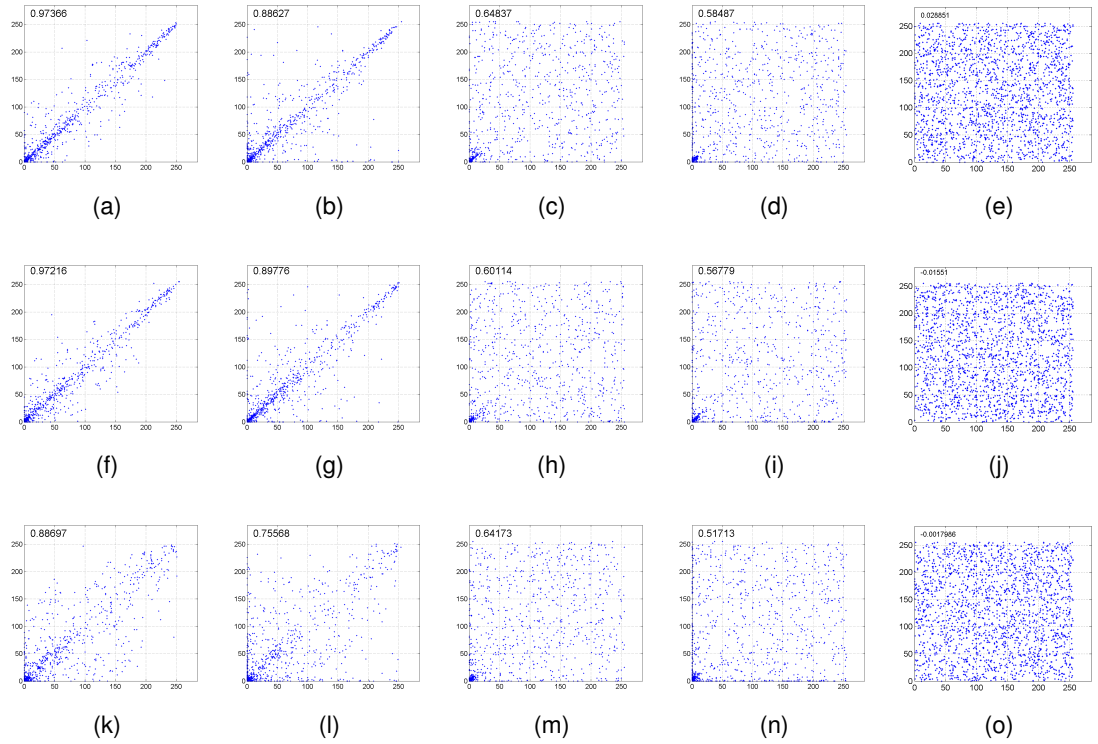


FIGURE 3.15 – For Spectral Doppler image , (a), (b), (c), (d), (e) represent the vertical correlation : original, after permutation, after masking, after global encryption and full encryption, respectively. (f), (g), (h), (i), (j) represent the horizontal correlation : original, after permutation, after masking, after global encryption and full encryption, respectively. (k), (l), (m), (n), (o) represent the diagonal correlation : original, after permutation, after masking, after global encryption and full encryption, respectively.

The correlation is done in the horizontal, vertical and diagonal directions. In FIGURE 3.14, the correlation test for the different plain and encrypted medical images with their corresponding vertical, horizontal, and diagonal correlations are shown for the different proposed approaches. Notice that the first variant of selective encryption, which is based only on permutation of sub matrices doesn't ensure low correlation (still linear as the original image (see FIGURE 3.14-(b, g,l)) since the correlation is quantified at the pixel level and not at the sub-matrix level.

While for the second variant, which entails, in addition to the permutation process, a masking process applied to each sub-matrix of ROI, the correlation is removed between adjacent pixels of ROI sub-matrices (see FIGURE 3.14-(c, h,m)). The middle-full approach gives similar correlation results as the second selective approach (see FIGURE 3.14-(d, i, n)) since the sub-matrices of ROB are not masked. Note that the global permutation of the middle-full approach is very important to ensure a better visual degradation, which permits to hide the structure of the medical image and consequently, its type. See FIGURE 3.14-(e, j, o)).

The lower correlation result is obtained for the encrypted images that use the full encryption approach as shown in FIGURE 3.14-(e, j, o). Correlation in the proposed approach is dependent on the encryption variant, while the best correlation results (close to 0) can be obtained by employing the full approach. In fact, the obtained results for the middle-full

and for the second variant of selective encryption algorithm are also sufficient to provide protection since a masking process is applied for the ROI sub-matrices.

3.7.4/ KEY SENSITIVITY

In this section, we quantify the sensitivity of secret key k and IV and we show the recurrence of the produced dynamic initial matrices and the probability density function for 250 different IM.

The size of the secret and dynamic keys is flexible ; it can be 128, 196, 256 bits for the secret key, and 512 for the dynamic key. It is chosen according to the desired level of security. These sizes are sufficient to make the brute force attacks unfeasible. Concerning IV, in FIGURE 3.16-a, a random bit of a random bye of IV is flipped. The results show that the difference in the produced cipher images is close to 50%. In addition, in FIGURE 3.16-b, a random bit of a random byte of the secret key is flipped and the results show that the difference between the produced cipher images is also close to 50%. This criteria enhances the resistance of the system against brute force attacks and in particular, key-related attacks. On the other hand, the recurrence test is applied to 250 produced IM and the results are shown in FIGURE 3.17-a. The results confirm that the produced IM is highly non-linear. Finally, in FIGURE 3.17-b, we can see that the PDF of these produced IM is very close to being uniform. Therefore, the technique for producing IM strongly enhances the cryptographic performance.

3.7.5/ SENSITIVITY ANALYSIS AND DIFFERENTIAL ATTACKS

Two metrics are commonly used in the sensitivity analysis of any approach : (1) Number of Pixels Change Rate (NPCR) and (2) Unified Average Changing Intensity (UACI). NPCR represents the number of pixels change rate between two images I_1 and I_2, while $UACI$ measures the changing intensity between the two cipher-texts. $NPCR$ and $UACI$ are represented by :

$$D(i,j) = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases}$$

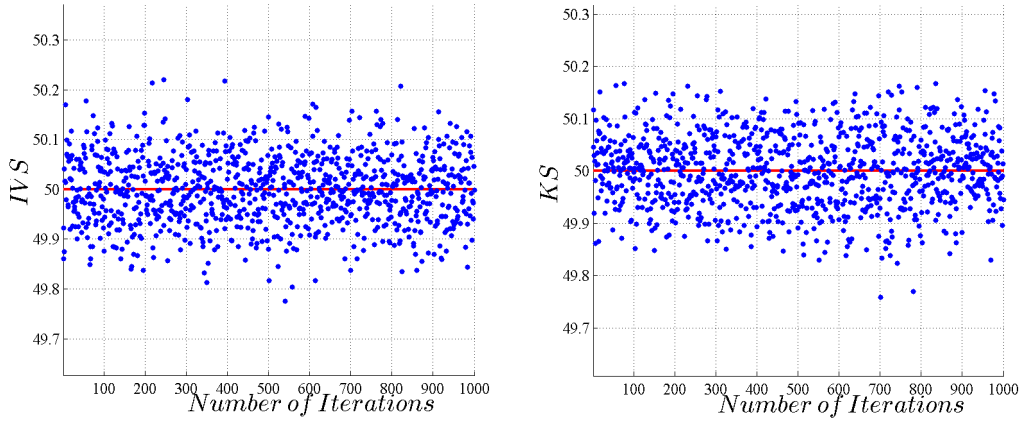
$$NPCR = \frac{\sum_{i,j} D_{i,j}}{M \times N \times P} \times 100\% \tag{3.5}$$

$$UACI = \frac{1}{M \times N \times P} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \tag{3.6}$$

$NPCR$ between original and cipher image is ≥ 99.61, which means that the pixels' positions are highly unrelated to each other. Moreover, an appropriate $UACI$ value is obtained that is close to 33.3, which means that most of the gray level pixels in the encrypted image are changed by the second variant of selective algorithm in addition to full and middle-full.

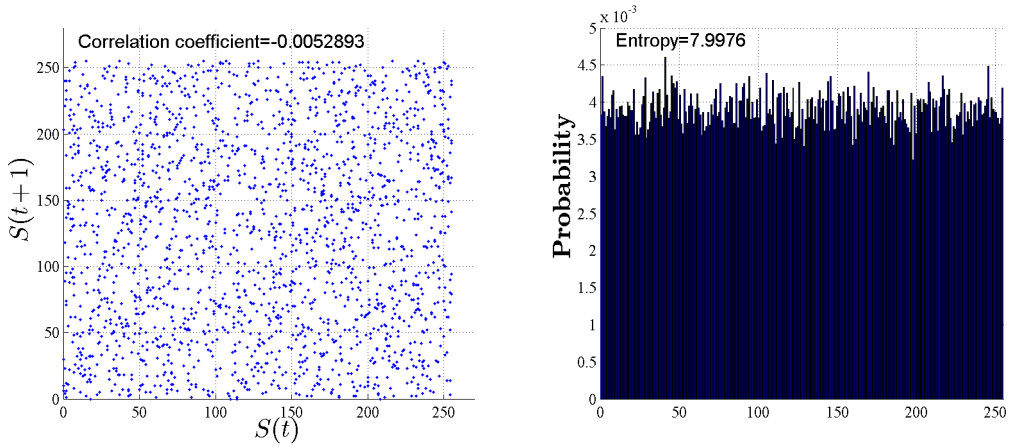
Figure 3.18 illustrates the probability of $NPCR$ and $UACI$ for 1,000 dynamic keys used to encrypt the Lenna plain-image of size 512×512. The theoretical results are $NPCR = 99.61$ and the mean value of $UACI$ is equal to 33.4. The proposed approach shows high values

of $NPCR$ and $UACI$ that are needed for a good cipher scheme. Also, Tables 3.2 and 3.3 summarize the results.



(a) (b)

FIGURE 3.16 – IV (a) and secret key(b) sensitivity for 1000 times.

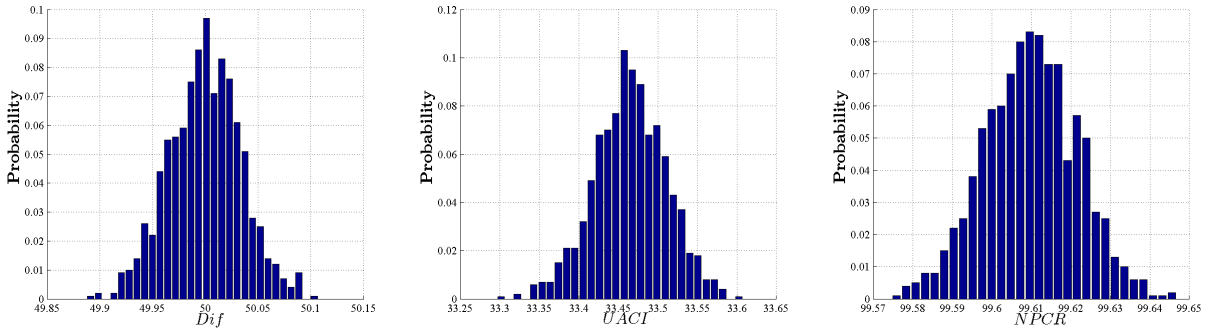


(a) Recurrence (b) PDF

FIGURE 3.17 – The Independance (Recursivity) (a) and the PDF (b) of the produced pseudo-random masking sub-matrices by employing the proposed scheme (see FIGURE 3.3) for a random secret key.

3.7.6/ VISUAL DEGRADATION

An important condition to ensure a robust image encryption algorithm is that the visual content of the original image must not be recognized in the ciphered image. Two well known parameters are considered to measure the encryption visual quality, which are Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity index (SSIM) that are described in [Hore et al., 2010]. A low PSNR value indicates a high difference between the original and the cipher images. Concerning $SSIM$, it is defined after the Human Visual System (HVS) and it has evolved such that we can extract the structural information from



(a) Diff (b) UACI (c) NPCR

FIGURE 3.18 – The PDF of the difference between original and encrypted Lenna in bits (a), UACI (b) and NPCR(c) for h=8

TABLE 3.4 – SSIM and PSNR in selective approaches

Images	Aorta	Head-3D	Brain
PSNR (SE1)	15.019	11.268	9.168
PSNR (SE2)	13.1	10.44	7.91
PSNR (MF)	9.805	9.1841	7.038
PSNR (Full approach)	8.2682	8.2965	8.3262
SSIM (SE1)	0.53097	0.49250	0.0376
SSIM- (SE2)	0.4199	0.391	0.0114
SSIM (MF)	0.211	0.212	0.01291
SSIM (Full approach)	0.0313	0.0360	0.0408

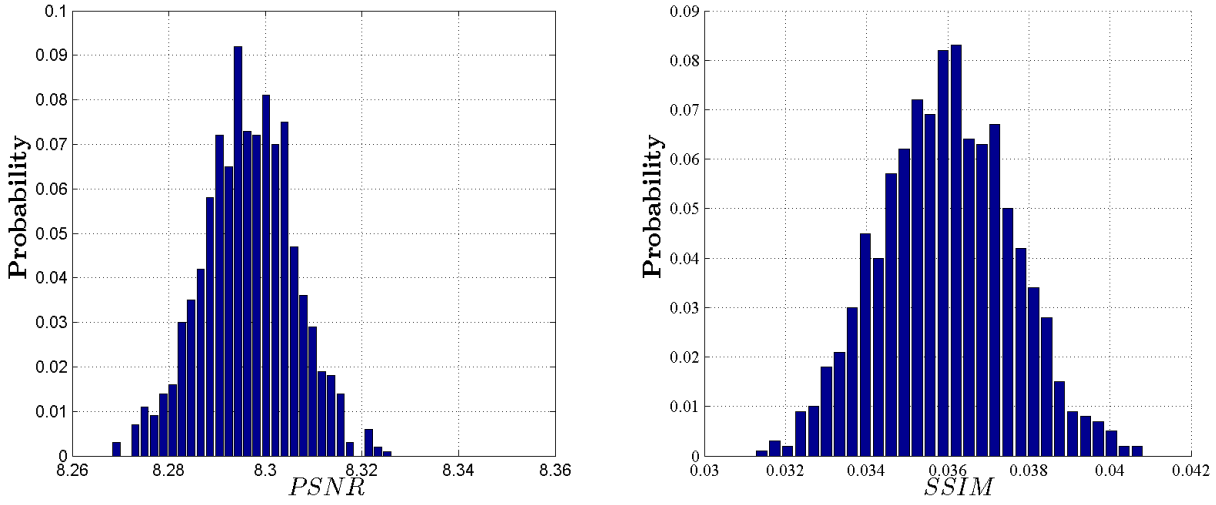
the scene. Thus, the perceived quality of the image by the human eye is highly dependent on the loss of structural information in the image.

$SSIM$ falls within the interval [0,1] ; a value of 0 means that there exists no correlation between the original and the cipher image, while a value close to 1 means that the two images are approximately the same.

According to the obtained results of PSNR and SSIM, all cipher variants introduce visual degradation since low values of PSNR and SSIM are obtained. In fact, the full cipher variant reaches the maximum hard visual degradation, which is normal since all original sub-matrices are encrypted compared to the selective cipher variants. In addition, the visual degradation of the middle cipher approach achieves better visual degradation compared to the selective variants. Note that no useful information can be detected from the encrypted ROI sub-matrices, but only the type of the medical image can be known.

3.7.7/ EXECUTION TIME

Execution time is a crucial metric for any cipher ; a low computational complexity translates into low latency and hence, low resources are needed for the ciphering/deciphering



(a) (b)

FIGURE 3.19 – PDF of PSNR, and SSIM for the full encrption approach for $h = 8$

process. This ensured the cipher applicability to real-time systems and for devices with limited resources. The average calculation time (for $1,000$ iterations) to encrypt the plain Lenna image of size $256 \times 256 \times 1$ is performed using the following software and hardware specifications : **Matlab R2013b simulator, micro-computer Intel Core 2 Duet, 3 GHZ CPU, 2 GB RAM Intel and Microsoft Windows 7**. The execution time of the three approaches were measured ; when only permutation is done on Lenna image (512×512), the average time is 0.0156 sec and designated by $t1$. For SE2, time is $t2 = 3 \times t1$. For the full encryption time is $t3 = 4 \times t1$. In case of full encryption, the execution time is dependent of the size of ROB. For example, if it is 50% of the plain image, the encryption time is $t4 = 2 \times t2 = 6 \times t1$. If the application is time- or resource- sensitive, the user can select the approach that best suits the application requirements.

3.8/ DISCUSSION AND CRYPTANALYSIS

The average of PSNR and SSIM between the original and encrypted images are presented for the different variants in TABLE 3.4 for $1,000$ dynamic keys. The results show that selective encryption has an average visual degradation since it is designed only for ROI zones. Also, the visual degradation of the MF variant is close to the full one. Sure, hard visual degradation can be ensured by using the full scheme. The user can choose any variant to protect the medical image contents. Our goal is to provide a flexible solution according to the limitations and requirements for the medical image.

In addition, the distribution of PSNR and SSIM are shown in Figure 3.19 for the full variant. The obtained results show that a low values of PSNR and SSIM are achieved and this confirms that the proposed encryption technique yields a high difference between the original and encrypted images. Consequently, a high and hard visual distortion is

attained by using the proposed full encryption process. As a conclusion, the proposed scheme gives a sufficient visual degradation for the selective and MF variants and hard degradation for the full one. Indeed, for all these variants, no useful information about the original plain image could be revealed from the cipher image.

By only shuffling the data, the system will not be immune against the different attacks if the secret key is static. However, the proposed approach is based on a dynamic key in order to ensure the forward and backward secrecy. Permutation process is based on changing the pixels positions without affecting their values. hence, this motivates the introduction of the other variants to ensure better resistance against future powerful attacks. Indeed, introducing the masking function ensures the change in the pixels positions as well as values. Moreover, by employing a dynamic non-linear element, the substitution table (S-box), a better randomness degree is achieved and better immunity against powerful attacks is attained. We applied the proposed cipher with the different variants on different images. In selective and middle-full approaches, the PDF of cipher ROI submatrices or the whole cipher image in case of full variant tend to become uniform. This proves that the proposed scheme can resist statistical attacks since the spatial redundancy between adjacent pixels of the image is removed ensuring a good scrambling of the image. Moreover, other tests such as entropy analysis and correlation tests have validated the robustness of proposed variants (except SE1) and their high resistance to statistical attacks. Moreover, key sensitivity is analyzed and the results showed that the proposed cipher can resist chosen/known plain-text attacks.

Additionally, the key space of the secret key is flexible and can be 2^{128}, 2^{196} and 2^{256}, while the size of the dynamic key is 2^{512}. These sizes are sufficiently large to make the brute-force attack unfeasible. Therefore, the system can resist the cipher-text-only attack. Also, an important issue that must be highlighted here is the use of a dynamic key instead of a fixed one. Even if a cryptanalyst has complete knowledge of the used primitives (substitution and permutation techniques) for a plain image, she/he will fail to extract information about the future plain images from the future cipher images, since they lack the dynamic key that is changed for every input image.

TABLE 3.5 – Compare approaches

Approach	**SE-1**	**SE-2**	**MF**	**Full Encryption**
Computation Complexity	+	++	+++	+++
Visual Degradation	+	++	+++	++++
Memory Consumption	+	+	++	++
Error Propagation	+	+	++	++
Level of Security	+	++	+++	++++

3.9/ CONCLUSION

In this chapter, a cipher scheme with three variants (selective, middle-full, and full) is presented to protect medical images. The scheme is based on dynamic diffusion and/or confusion primitives for each input image, which ensures good cryptographic performance. The round number is reduced without degrading the security level, which is a hard challenge that is solved in this chapter. The proposed scheme presents a dynamic key derivation function that generates the dynamic key and consequently the requi-

red sub-keys that are used to construct the basic primitives of the cipher. To perform encryption/decryption, two main primitives are exploited : sub-matrix permutation and a proposed masking function were applied at the sub-matrix level. Then, several security analysis and system performance tests were conducted to prove the credibility of the proposed cipher scheme. As a conclusion, the proposed approaches can be considered as good competitors to the current medical image applications that have to ensure patients privacy and data confidentiality.

4

Enhanced Lightweight and Secure Cipher Scheme for Medical Data

ABSTRACT

In this chapter, we propose a lightweight cipher algorithm based on a dynamic structure with a single round that consists of simple operations compared to the previous image cipher scheme, and that targets all kind of IoT devices (raw data and multimedia). In this solution, the dynamic key is used to build two robust substitution tables, a dynamic permutation table, and two pseudo-random matrices. This dynamic cipher structure minimizes the number of rounds to a single one, while maintaining a high level of randomness and security as the previous cipher. Moreover, the proposed cipher scheme is flexible as the dimensions of the input matrix can be selected to match the devices' memory capacity. Extensive security tests demonstrated the robustness of the cipher against various kinds of attacks. The speed, simplicity and high-security level, in addition to low error propagation, make of this approach a good encryption candidate for IoT devices.

4.1/ Introduction

The increasing number of services provided by the Internet has generated a huge increase in the number of connected devices ; more than 9 billion network devices are connected and used by billions of users. Services offered can be used for communication, entertainment, sharing knowledge and many other purposes. In addition to traditional devices (laptops, smart phones, etc..), devices around us will soon be able to communicate with each other [Atzori et al., 2010, Sundmaeker et al., 2010]. These smart objects, interacting with each other, have transformed the Internet into the "Internet of Things", which is an emerging area in which highly constrained interconnected devices work together to accomplish a specific task and can be used for many purposes such as medical monitoring and collecting data as well as accessing and processing such data. Indeed, IoT is continuously emerging in many fields such as health monitoring, and even in human bodies for patient monitoring in what is being referred to as mHealth [Jara et al., 2013, Chang, 2017], smart houses/buildings/cities, environment monitoring, and traffic monitoring.

However, the major problems that hinder the deployment of IoT systems are the security and privacy issues [Adrianto et al., 2015, Granjal et al., 2015, Amin et al., 2017], since such systems are more susceptible to diverse kinds of attacks (passive and active) than the traditional systems. The passive attacks can seriously impair the confidentiality of the data by trying to extract the contents of transmitted packets, while active attacks can compromise the data integrity and authentication by inserting, deleting or modifying the packets' contents. One solution to guard against such kinds of attacks is to encrypt the packets transmitted by IoT nodes. Hence, it is necessary to ensure that the transmitted data is secured from any unauthorized access and that data is exchanged only between legitimate parties. In this chapter, we address the problem of securing the distributed medical systems in IoT, called Medical Internet of Things (MIoT).

One of the mostly used MIoT devices is surveillance that are essential for monitoring patients to detect suspicious activities. Typically, the transmissions of these sensing data should be secured from eavesdropping and malicious attacks to avoid disclosing any useful information to attackers. MIoT applications have stringent QoS requirements and require security solutions that may entail major resources and latency overhead. This in turn is not practical for MIoT devices that, in some scenarios, might be limited in battery lifetime and computational resources.

As such, medical IoT constrained devices may not be able to support the NIST-approved strong cryptographic algorithms since these have a negative impact on the system performance and may degrade the desirable QoS [McKay et al., 2017], especially since IoT devices exchange massive amounts of data.

4.1.1/ Related Works

For real IoT implementations [Granjal et al., 2015], AES block cipher [Daemen et al., 2002a] in Counter (CTR) mode [Dworkin et al., 2001, Singh et al., 2017] is used, where the ciphering process is independent of plaintext and in this case, block cipher operates as a stream cipher. In general, block cipher such as AES uses a multi-round structure whereby a round function undergoes several iterations r. Round functions can be based on either Feistel Networks (FN) or Substitution-Permutation Networks (SPN). Typically, in each round, the round function applies several operations to ensure the confusion and diffusion properties.

For more than a decade, many efforts have been spent to make AES act as a lightweight block cipher and thus, to make it practical for tiny-limited devices. Indeed, several improvements have been realized to reach this goal in both hardware and software implementations. Examples of these variations include AES-128 hardware ASCI implementation with 2400 Gate Equivalents (GE) is presented in [Moradi et al., 2011], while efficient software AES implementations for 8-bit in [Osvik et al., 2010], 16-bit in [Buhrow et al., 2014] and 32-bit in [Tillich et al., 2006]. Moreover, AES optimized instructions were added to the instruction set of Intel's [Gueron, 2009, O'Melia et al., 2010]. At the time of this writing, there are no further optimization techniques to AES, and there might be no more possible optimization [Beaulieu et al., 2015].

However, even with the current optimization to AES and the attempts to make it applicable to constrained devices and adaptive to the increasing data rates, the enhancements still suffer from several limitations that cannot be easily overcome. According to NIST [McKay et al., 2017], AES might not meet the future requirements and consequently, a new project has been launched to design new lightweight cryptographic algorithms with lower number of GE (preferably, less than 2,000 [Khattab et al., 2016]).

Even though the AES hardware implementation is fast, however, the implementation itself is complex and is not suitable for constrained devices [Beaulieu et al., 2015]. On the other hand, a simple AES hardware implementation decreases its efficiency. Consequently, AES hardware implementation suffers from a trade-off between efficiency and implementation complexity [Beaulieu et al., 2015]. Moreover, the presented implementation in [Lee et al., 2009] shows that AES rapidly decreases the lifetime of battery nodes and networks such as in ZigBee [Evans-Pughe, 2003], and WirlessHART [Raza et al., 2009]. As such, it is safe to conclude that AES is not really suitable for constrained devices, such as IoT ones, as stated in [McKay et al., 2017, Beaulieu et al., 2015, Nithya et al., 2016].

Consequently, a different cipher methodology has been presented recently [Beaulieu et al., 2015] to solve this issue by reducing the size of the secret key and/or the block size to meet the constrained requirements of tiny devices. Examples of such techniques include LEA [Hong et al., 2014], FeW[Kumar et al., 2014b], Prince [Borghoff et al., 2012], TWINE [Suzaki et al., 2013], Lblock [Wu et al., 2011], Piccolo [Shibutani et al., 2011], LED [Guo et al., 2011] and other ciphers, a list of which is shown in TABLE 4.1.

However, all of these ciphers are based on static substitution and diffusion primitives, which require iterating the round function for a large number of r (see TABLE 4.1) to ensure the required security level. Unfortunately, the multi-round structure that is used in the these ciphers provides a high level of security but at the expense of high computational complexity. Therefore, to use these cipher algorithms in MIoT devices, there is a trade-off between security and performance : the required execution time of these ciphers is r times the round function's execution time, and the required resources are also multiplied by r.

The incorporation of encryption into MIoT devices introduces an overhead that might prevent such devices from ensuring their main functionality and consequently impacting the overall system performance [McKay et al., 2017]. Accordingly, the limitations of IoT devices mandate the design of a new cipher methodology that can ensure secure data transmission among IoT nodes with low computational complexity and resources. This chapter presents a new methodology to reduce r to 1 and to form a dynamic key-dependent lightweight round function to fulfill the security aspects efficiently. Consequently, this chapter proposes a new cipher design methodology that may help in the design of future lightweight cryptographic algorithms.

TABLE 4.1 – List of recent lightweight cryptographic algorithms

Algorithm	No. of rounds	Key size	Block size	Structure
TEA	64	128	64	FN
XTEA	64	128	64	FN
LEA [Hong et al., 2014]		128	64	FN
HEIGHT	32	128	64	GFS
FeW[Kumar et al., 2014b]	32	80/128	64	FN-M
SIMON	32/36/42/44/52/54/68/69/72	64/72/96/128/144/192/256	32/48/64/92/128	FNl
PRESENT	31	80/128	64	SPN
RECTANGLE	25	80/120	64	SPN
LEA	24/28/32	128/192/256	128	FN
SPECK	22/23/26/27/28/29/32/33/34	64/72/96/128/144/192/256	32/48/64/92/128	FN
Prince [Borghoff et al., 2012]	11	128	64	SPN
AES	10/12/14	128/192/256	128	SPN
RC5	12	128	32/64/128	FN
Hummingbird2	4	256	16	SPN

4.1.2/ MOTIVATION & CONTRIBUTION

In this chapter, we present a new efficient, lightweight cipher algorithm for MIoT applications. Contrary to other cryptography algorithms (multiple rounds), the proposed cipher only employs a single dynamic key-dependent round function. The proposed round function is based on simple operations and achieves the required cryptographic performance. To accomplish this objective, we relied on the dynamic key approach whereby a dynamic key is generated for each input audio, image or video. This dynamic key depends on a secret key and a Nonce similar to [Noura et al., 2017b]. Then, this dynamic key is used to build several efficient key-dependent diffusion and confusion primitives, which ensure a good cryptographic performance [Adams et al., 1989, Keliher et al.,].

The proposed cipher scheme includes several contributions that led to a high level of efficiency and security for IoT devices compared to the recent lightweight block ciphers, recent chaotic ciphers and our previous dynamic key-dependent dynamic cipher schemes.

SYSTEM PERFORMANCE

— **Lightweight** :The minimum required number of iterations, for recent lightweight cryptographic algorithms, is 4 such as the Hummingbird2 cipher. Furthermore, the recent lightweight chaotic image encryption algorithms such as [Boriga et al., 2014, Laiphrakpam et al., 2017, Ghebleh et al., 2014, Janakiraman et al., 2018, Mondal et al., 2017] use also the multi-round structure in addition to floating-point calculations and conversion operations, which introduces an important overhead in terms of latency and required resources. In addition, [Laiphrakpam et al., 2017] requires asymmetric encryption, which requires more resources and introduces a higher latency [Granjal et al., 2015] when compared to the symmetric one.

There is only one chaotic cipher that was presented with a single round [El Assad et al., 2016], but it requires a huge memory capacity. Also, according to [Noura et al., 2017a], the results are not accurate and the approach actually requires at least 6 iterations to reach the desired cryptogra-

phic performance. Moreover, the approach suffers from maximum error propagation, since the avalanche effect propagates to the whole image instead of being restricted to the block level. Our previous dynamic key-dependent cipher schemes [Fawaz et al., 2016, Noura et al., 2017b] require at least two rounds of substitution and diffusion. The scheme we propose in this chapter avoids the use of a static diffusion operation such as the MixColumn transformation of AES [Daemen et al., 2002a] or the key-dependent integer/binary diffusion operations of [Fawaz et al., 2016, Noura et al., 2017b], since such operations consume a high percentage of the execution time [Noura et al., 2017b, Wadi et al., 2014]. Hence, the proposed scheme requires only one round iteration of a lightweight simple and flexible round function without using any diffusion operation. As such, this minimizes the computational complexity of the proposed cipher and consequently the required latency and resources. Moreover, the proposed encryption scheme can be realized in parallel, while the decryption algorithm can be partially parallelized.

— **Flexibility :** The proposed cipher operates on data at the sub-matrix level, which can have a flexible size of ($h \times h$ bytes), to be set according to the devices' limitations. In other words, the proposed approach is configured according to the devices' characteristics.
— **Simple hardware and software implementations :** The proposed cipher is based on logical operations (exclusive or), load and store operations (substitution and permutation), which renders the corresponding hardware and software implementations to be simple and efficient.
— **Low error propagation** : Since the encryption is done at the sub-matrix level, an error that occurs in a byte of an encrypted sub-matrix will affect only two bytes and it will not affect the whole corresponding sub-matrix. In addition, the proposed cipher scheme is designed to avoid the chaining operations to limit the effect of the corrupted bytes only to both sub-matrices. This will not affect all of the two sub-matrices as in [Fawaz et al., 2016, Noura et al., 2017b] or the whole image as in [El Assad et al., 2016]. Thus, low error propagation is guaranteed and an error correction scheme is presented, which is a great advantage for the proposed cipher scheme.

These enhancements reduce the delay of the encryption and decryption processes and simplify their corresponding hardware implementations. This is essential since each primitive has its own impact on the security and efficiency of the proposed cipher scheme.

SECURITY PERFORMANCE

— **Key Dependence Approach :** The proposed cipher is based on key-dependent substitution and permutation primitives that ensure simplicity in addition to the required cryptographic properties.
— **Dynamic Key Approach :** In contrast to the existing cipher solutions, the proposed approach is based on a dynamic key, which is variable and changes in a pseudo-random manner for each new session. The periodic interval of a session depends on the application or user requirements. For example, a new session can be established for each new input image. Therefore, the cryptanalysis process against the proposed cipher algorithm is very challenging because of the unpredictability of the cipher primitives as they change according to the dyna-

mic key. In addition, changing the dynamic key produces different cipher primitives and consequently different encrypted/decrypted images (sensitivity is verified in Section 4.4). The dynamic nature of the proposed cipher provides high robustness against any kind of attacks. [Noura et al., 2017b, Fawaz et al., 2016, Zhang et al., 2010, Pradeep et al., 2013].

— **Dynamic Sub-matrices Selection** : A dynamic pseudo-random selection operation is introduced to control and randomize the sequential order of the encryption and decryption sub-matrices. This complicates the procedure for the possible attacks. This makes the proposed cipher approach more robust compared to existing ones since the sequential order of encryption/decryption is variable and depends on the dynamic key. This step is designed and realized to achieve low latency and resources overhead towards preserving the previous advantages.

Therefore, an efficient collaboration scheme is proposed and relates substitution, pseudo-random matrices and block selection (based on a generated permutation table) to reach a better level of robustness and efficiency. This is proved according to the results of a set of performance and security tests.

Accordingly, a good lightweight, flexible, cipher candidate for MIoT is proposed. This is justified since the trade-off between system performance and the security level is reduced in addition to its simple hardware and software implementations.

4.1.3/ ORGANIZATION

The rest of the chapter is organized as follows. Section 4.2 presents the proposed key derivation algorithm along with the proposed cipher construction primitives. In Section 4.3, we describe all the steps necessary to undergo the encryption and decryption processes. Then, an extensive security analysis and a performance evaluation are conducted in Section 4.4 to prove the robustness and effectiveness of the proposed scheme. Then, in Section 4.5, we prove the immunity of the proposed algorithm against different kinds of existing attacks. Finally, in Section 4.6, the conclusions are drawn along with directions for future work.

4.2/ INITIALIZATION

In this section, the generation process of the dynamic key and the associated sub-keys that are used in the cipher are explained. FIGURE 4.1 illustrates the key derivation function, which takes as input a secret key SK and a nonce N_o that are unique for every session or input image. These inputs are described in the following :

— **Secret key** SK **:** This secret key is only shared between the communicating entities after the mutual authentication step (handshake). For better protection, the secret key is changed after a specific period of time to be specified by the underlying application. It can be renewed in different ways such as using Binary Elliptic Curve Diffie Hellman protocol (ECDH) [Miller, 1985].

— **Nonce** N_o **:** A pseudo-random generator is used to generate this $Nonce$. It is important to generate a new $Nonce$ for each input image. N_o can be sent to the receiver encrypted using the shared public key of the other entity if the asymmetric

TABLE 4.2 – Summary of notations used.

Notation	Definition
SK	Secret Key
N_o	Nonce
DK	Dynamic Key
K_{S1}	First dynamic substitution sub-key used to construct $S-box_1$
K_{S2}	Second dynamic substitution sub-key used to construct $S-box_2$
K_{RM}	Matrix dynamic sub-key used to create RM_1 and RM_2
K_P	Permutation sub-Key used to create π
S_1	The first produced dynamic S-box
S_1^{-1}	The inverse corresponding of the first S-box
S_2	The second produced dynamic S-box
S_2^{-1}	The inverse corresponding of the second S-box
RM_1	First initial dynamic pseudo-random matrix
RM_2	Second initial dynamic pseudo-random matrix
π	A Dynamic produced permutation table (P-box)
π^{-1}	The inverse corresponding the permutation table (P-box)
L	Rows Number
C	Columns Number
P	Plane Number (for gray-scale is equal to 1)
$h \times h$	The size of each sub-matrix
α	The number of $h \times h$ sub-matrices
x_i	Original plain sub-matrix at the i^{th} index
y_i	The corresponding permuted sub-matrix of x_i
cx_i	The corresponding encrypted sub-matrix of x_i
cy_i	The corresponding encrypted sub-matrix of y_i

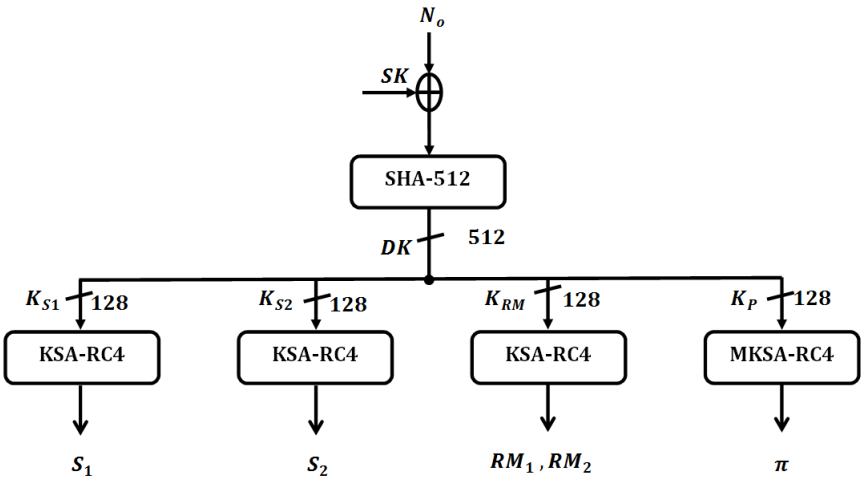


FIGURE 4.1 – The Proposed Dynamic Sub-Keys Generation Scheme.

approach is used. Another way for sharing N_o is to have a good synchronization between the sender and the receiver where each entity derives it separately with no need for transmission and starting from the same seed.

Then, the secret key SK and N_o are Xored and its corresponding output is hashed to produce the dynamic key DK. Next, DK is divided into four different sub-keys that form the seeds for the different cipher primitives and these are described in the following subsections. Let us indicate that the secure hash function $(SHA-512)$ is selected for this step since it posses the best desirable cryptographic hash properties such as the high resistance against collision. This can assure that the produced DK is renewed for every session or input image and consequently provides different cipher primitives ; which introduces randomness into the scheme. Employing dynamic key will provide high immunity against existing and modern attacks.

4.2.1/ Dynamic Key & Sub-keys Derivation

Indeed, DK can be changed frequently as needed by the user or by the application. Furthermore, as $SHA-512$ is used, DK has 512 bits length (64 bytes) and it will be split into four sub-keys, where each one has a size 128 bits (16 bytes). These sub-keys are $\{K_{S1},\ K_{S2},\ K_{RM},\ K_p\}$ and are described in the following knowing that each of the sub-keys will be used for a different purpose.

- **First substitution sub-key** K_{S1} : It consists of the most significant 16 bytes of DK.
- **Second substitution sub-key** K_{S2} : It consists of the next most significant 16 bytes of DK.
- **Dynamic matrices sub-key** K_{RM} : K_{RM} consists of the third most significant 16 bytes.
- **Permutation sub-key** K_P : Finally, the least significant 16 bytes of DK.

Table 4.2 shows all the notations used in this chapter. The derived dynamic key is renewed for each input image and any bit changed in it will lead to a completely different set of sub-keys and consequently different cipher primitives will be produced. Next, the construction of the proposed cipher primitives that are based on these four sub-keys is described.

4.2.2/ Construction of Cipher Primitives

We aim to design a simple, yet very effective lightweight cipher algorithm with only one round, which can be used with constrained IoT devices. According to Shannon, round function should mandatory ensure the confusion and diffusion properties. While this round function should be iterated for multi-iterations to consider it as a successful cipher scheme. This is the logic of the existing symmetric block cipher algorithms since static substitution and diffusion primitives are mainly used. Moreover, as mentioned previously, static keys would render the system vulnerable to many future threats [Zhang et al., 2010, Pradeep et al., 2013, Paar et al., 2009a]. Fortunately, a dynamic key approach can provide a better-desired security level against existing and future powerful attacks [Noura et al., 2017b]. This is ensured since all the used sub-keys depend on the produced dynamic key and consequently, cipher primitives become variable, which prevents attackers to recover any information from the collected set of original encrypted images. More important, this helps cryptographic engineering reduce the required round number of iterations and consequently, this will reduce the required resources and latency that are both necessary to preserve the main functionality of MIoT devices. Therefore, defining key dependent cipher primitives with a high level of efficiency and security is necessary for the proposed dynamic approach. In the following, the proposed techniques to construct the key dependent cipher primitives are explained.

4.2.2.1/ DYNAMIC SUBSTITUTION PRIMITIVE

The proposed cipher scheme requires two substitutions table (S_1 and S_2). In this chapter, we propose to use the KSA of the $RC4$ stream cipher algorithm [Rivest, 1992] to produce the required two substitution boxes (S-boxes) instead of GRP algorithm, which was presented in the second chapter. KSA algorithm is described in Algorithm 3, where an input key with LK bytes is introduced to produce a dynamic substitution table S as an output. The size of the sub-substitution dynamic keys (K_{S1} and K_{S2}) is set to $L = 16$ bytes.

Algorithm 3 KSA for RC4

```
1: procedure RC4_KSA(K = {k_1, k_2, ..., k_Lk}, L)
2:     for i ← 0 to 255 do
3:         S [i] ← i
4:     j ← 0
5:     for i ← 0 to 255 do
6:         j ← (j + S[i] + k[j mod L]) mod 256
7:         swap(S[i], S[j])
8:     return S
```

Therefore, K_{S1} is used as a key for the KSA algorithm to produce the first substitution table S_1. Similarly, S_{k2} is used to produce the second dynamic substitution $S - box$, S_2. Moreover, the proposed technique to build key-dependent substitution tables S showed good robustness and cryptographic strength according to several criteria that are summarized as follows :

- **Linear Probability Approximation Function (LPF)** : For $LK \geq 4$, the average LPF value stabilizes and becomes close to $2^{-4.8}$.
- **Differential Probability Approximation Function (DPF)** : For $LK \geq 4$, the average of DPF converges to the minimum possible value, which is $2^{-4.5}$.
- **Strict Avalanche Criterion (SAC)** : For $LK \geq 4$, the produced $S - boxes$ become more close to the ideal value. This criterion is important, since it quantifies the sensitivity probability against any modification on any bit and it helps to ensure the avalanche effect if a good diffusion primitive is used.
- **Output Bit Independence Criterion (BIC)** : In fact, the BIC value become very close to the desired value (0.5) for $LK \geq 4$.

TABLE 4.3 – The values of LPF, DPF, SAC, and BIC for $LK = 4$ iterations.

LPF	DPF	SAC	BIC
$2^{-4.8}$	$2^{-4.5}$	0.5	0.51

The average values of these criteria are shown in TABLE 4.3 for $L = 4$. The obtained results were sufficient to indicate that the proposed construction technique of key-dependent substitution produces a robust and efficient substitution table (S-box). Furthermore, S_1 and S_2 make the proposed cipher algorithm with one round immune against differential and linear attacks since they are changed in a pseudo-random manner.

On the other hand, the inverse substitution table is necessary for the decryption process.

Indeed, as the produced S is bijective, the inverse of S, S^{-1}, can be obtained easily by the following operation $S^{-1}[S(i)]=i$.

4.2.2.2/ DYNAMIC SELECTION SUB-MATRICES

The proposed cipher algorithm requires producing a dynamic key dependent flexible permutation table π. Indeed, π is not only used to permute the sub-matrices of the input image (α sub-matrices), but also to control the encryption/decryption processes. Let us indicate that the proposed cipher scheme requires two sub-matrices as input, one at a time. In fact, the second sub-matrix is chosen according to the permutation table π. The proposed technique to build the dynamic flexible permutation table π is similar to that of the substitution tables. It is based on a minor modification of the KSA of RC4 (see Algorithm 3), which requires to replace α instead of 255 in lines 2 and 6. The modification is presented in KSA-RC4 (simple and efficient) to be sure that the same hardware implementation of KSA can be used to construct the substitution and permutation primitives in a real implementation and to reach a lower number of GE.

Therefore, K_p is used as a seed for the proposed modified KSA algorithm to build the flexible key dependent permutation table π with length α elements. Moreover, The i^{th} original/encrypted sub-matrix (x_i) requires the $\pi(i)^{th}$ original/encrypted ($X_{\pi(i)}$) to be encrypted or decrypted, respectively. Where $\pi(i)$ represents the value of the π at the i^{th} index and $1 \leq \pi(i) \leq \alpha$. The process of permutation is realized by employing a swap function, where (i) and $(\pi(i))$ are the original and permuted sub-matrix positions of the image, respectively.

4.2.2.3/ DYNAMIC PSEUDO RANDOM MATRICES

The proposed cipher requires two sub-matrices RM_1 and RM_2 in the encryption/decryption process to ensure better randomness properties and to remove any existing patterns from the encrypted sub-matrices. $RC4$ algorithm with K_{RM} is used to produce $2 \times h^2$ bytes, where the first h^2 bytes are used to form RM_1 and the last h^2 bytes ares used to form RM_2. Let us indicate that the PRGA algorithm of $RC4$ should be used in addition to KSA in this step.

Note that the choice of RC4 is due to its simple software and hardware implementations and its ability to generate substitution and permutation primitives with good cryptographic performance. In this chapter, RC4 is used only to produce the cipher primitives and not for the encryption/decryption process. However, any other key-dependent substitution/permutation generation algorithm can be used as well.

4.3/ ENCRYPTION AND DECRYPTION ALGORITHMS

In this section, the different steps of the encryption and decryption algorithms are shown and they are described in Figures 4.2 and 4.3, respectively.
The proposed algorithm is symmetric and is based on a secret key SK shared between

the sender and the receiver. As stated earlier, this key is employed with a $Nonce$ to produce a dynamic key, which is split to obtain four sub-keys that will be used to construct the primitives of the encryption/decryption processes. This cipher is based on only **one round** since a dynamic key with a large size is used. In the encryption process, an input image of size $L \times C \times P$ is divided into α sub-matrices $\{x_1,\ x_2,\ \ldots,\ x_\alpha\}$. Each sub-matrix has a square size equal to $h \times h$ bytes. If the number of bytes of an image is not a multiple of h^2, a padding operation is performed to adjust the size of the last sub-matrix (x_α). In addition, h can be equal to 4, 8, 16 or 32. On the other hand, the sub-matrices number α is obtained as follows :

$$\alpha = \frac{R \times C \times P}{h^2} \tag{4.1}$$

In the rest of the chapter, we fix h to 8. Note that h can be changed according to the device limitations.

4.3.1/ Encryption Algorithm

Algorithm 4 summarizes the proposed encryption algorithm that can be divided into four sub-functions, which are Sub – MatrixSelection, Function – f, Function – g, SwitchOperation and they are described in the following :

4.3.1.1/ Sub-Matrix Selection

In general, the first step in the encryption/decryption processes is to control the selection of the second sub-matrix of the input image. Usually, this step is introduced to add more randomness and to eliminate the sequential relation between the neighboring sub-matrices elements in an image to introduce more difficulty to attackers. As indicated previously, a dynamic permutation table π is used to control the selection of the two input sub-matrices in the encryption/decryption process. A pair of sub-matrices ($x_i = X_{\pi(i)}$ and $y_i = X_{\pi(i+\frac{\alpha}{2})}$) is selected to be encrypted/decrypted at one time. $X_{\pi(i)}$ represents the $\pi(i)^{th}$ sub-matrix of X that can be accessed via $X[i]$ and $i = \{1,\ 2, \ldots, \alpha\}$. While $y_i = x_{\pi(i)}$ represents the $pi(i + \frac{\alpha}{2})^{th}$ sub-matrix and can be accessed via $X[\pi[i + \frac{\alpha}{2}]]$. Next, each couple of sub-matrices x_i and y_i will undergo different operations. Each sub-matrix will be subjected to a different nonlinear function. The sub-matrix x_i will go through a function f, while the sub-matrix y_i will undergo another function g. Both functions are explained below.

4.3.1.2/ Function f

In this step, both dynamic S-boxes, S_1 and S_2, are being used. First, x_i is substituted by employing S_1, and then, the output is Xored with the first dynamic matrix RM_1 and the sub-matrix y_i. This is represented by the following equation.

$$O_i = RM_1 \oplus S_1(x_i) \oplus y_i \tag{4.2}$$

Next, the output O_i will be subjected to another substitution operation, which employs S_2

as expressed by the following equation :

$$cx_i = S_2(O_i) \tag{4.3}$$

Function f can be summarized as follows :

$$f = S_2(S_1(x_i) \oplus RM_1 \oplus y_i) \tag{4.4}$$

4.3.1.3/ FUNCTION g

The second round function g is applied in parallel to function f. Sub-matrix y_i will be subjected to this function. First, y_i will undergo a substitution operation by using S_2. Then, the output is Xored with the two dynamic matrices RM_1 and RM_2. This is illustrated by the following equation :

$$O'_i = RM_1 \oplus S_2(y_i) \oplus RM_2 \tag{4.5}$$

Then, the output O'_i goes through another substitution operation using S_1, and the output will be denoted as cy_i.

$$cy_i = S_1(O'_i) \tag{4.6}$$

Function g can be summarized as follows :

$$g = S_1(S_2(y_i) \oplus RM_1 \oplus RM_2) \tag{4.7}$$

4.3.1.4/ SWITCH OPERATION

After computing cx_i and cy_i, these two results are switched and hence, cx_i will take the position of cy_i and vice versa. This will add more randomness and will remove any sequential relation between the permuted-substituted sub-matrices.

Finally, all the sub-matrices will be reshaped to form the encrypted image I', which will be sent securely to the desired receiver or will be safely stored. In the next subsection, the decryption algorithm at the receiver side is explained.

Algorithm 4 The proposed One Round Encryption Algorithm.

procedure ONE_ROUND_ENCRYPTION(X, S_1, S_2, RM_1, RM_2, π)
  for $i = 1$ to $\frac{\alpha}{2}$ **do**
    $CX[\pi[i + \frac{\alpha}{2}]] = S_2(S_1(X[\pi[i]]) \oplus RM_1 \oplus X[\pi[i] + \frac{\alpha}{2}])$
    $CX[\pi[i]] = S_1(S_2(X[\pi[i + \frac{\alpha}{2}]]) \oplus RM_1 \oplus RM_2)$
    return CX

4.3.2/ DECRYPTION ALGORITHM

The decryption scheme is presented in FIGURE 4.3. After receiving the encrypted image, the receiver will use the decryption algorithm to recover the original image. The decryption algorithm has minor modifications compared to the encryption algorithm,

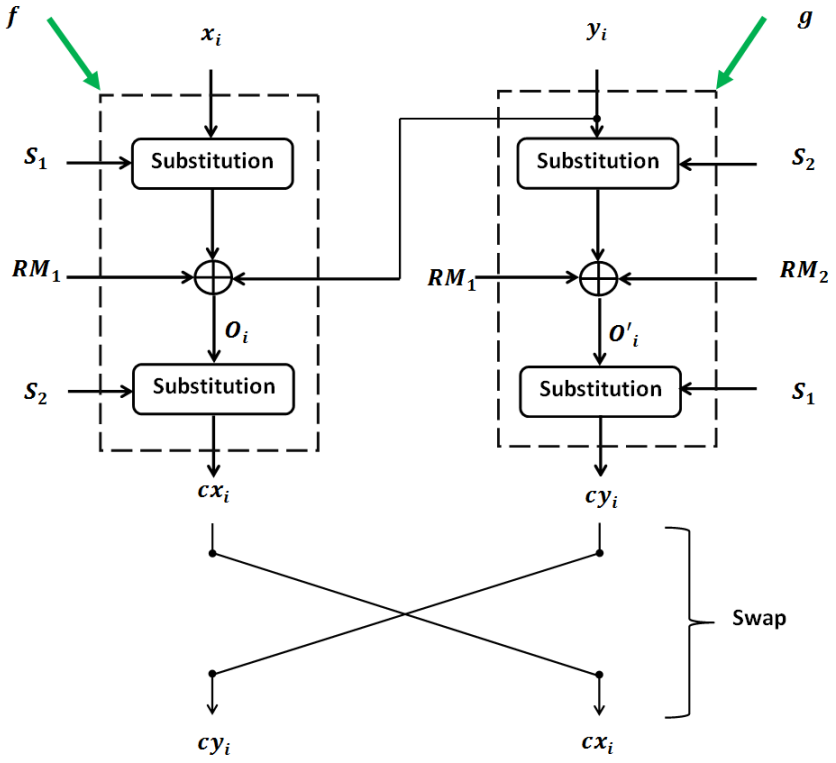


FIGURE 4.2 – The Proposed Encryption Scheme.

which are using the inverse function of f (f^{-1}) and of g (g^{-1}). In addition, these inverse functions require also the inverse substitution tables S_1^{-1} and S_2^{-1}.

The other primitive such as π is preserved and there is no need for the inverse permutation box π^{-1}, since the swap function is repeated at the legal destination side. First, the received encrypted image will be reshaped to α sub-matrices to start the decryption process.

Then, the decryption process as indicated in Algorithm 5 will be realized. In the following, we describe only the inverse functions f^{-1} and g^{-1} that are the only difference between the encryption and decryption algorithms.

4.3.2.1/ INVERSE OF FUNCTION f (f^{-1})

Each sub-matrix (cx_i) with its corresponding selected sub-matrix cy_i will be processed together. Next, the inverse substitution operation is realized by using S_2^{-1} and is applied on cx_i. Then, this result, O_i^{-1}, will be Xored with RM_1 and y_i, and then subjected to another inverse substitution operation by using S_1^{-1}. This is shown in the following equations :

$$O_i^{-1} = S_2^{-1}(cx_i) \tag{4.8}$$

After that, the resultant will be the following :

$$x_i = S_1^{-1}(O_i^{-1} \oplus RM_1 \oplus y_i) \tag{4.9}$$

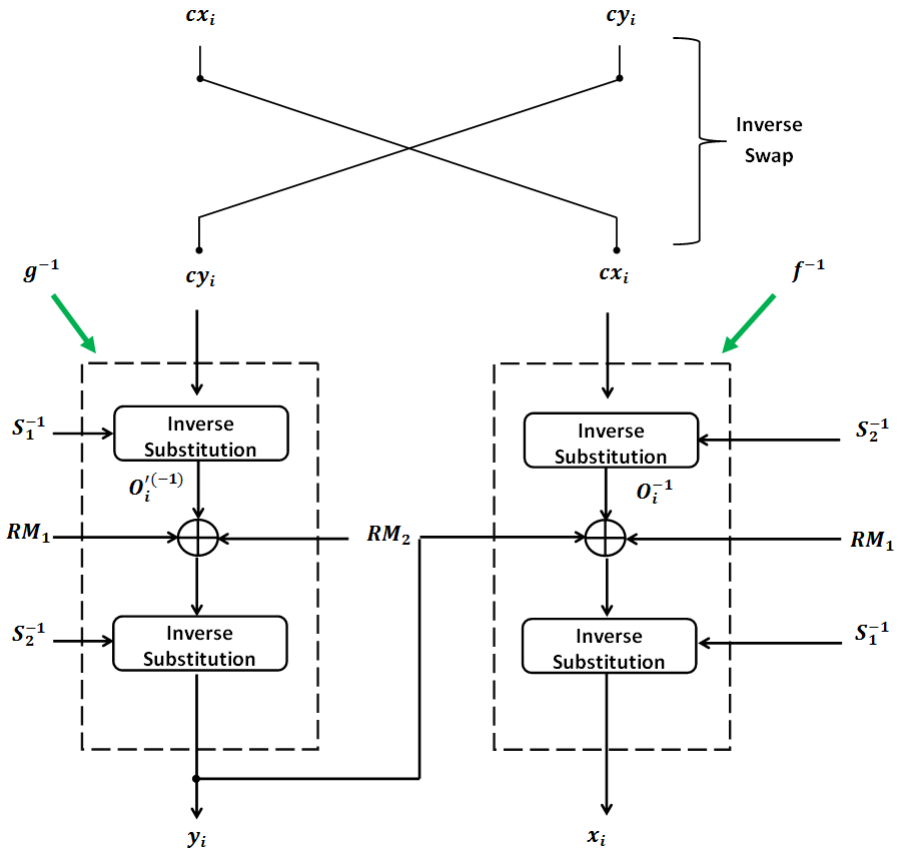


FIGURE 4.3 – The Proposed Decryption Scheme.

As it is shown clearly, we need to know y_i and consequently x_i will be deduced. This is where the inverse function g^{-1} is used.

4.3.2.2/ INVERSE OF FUNCTION g (g^{-1})

First, S_1^{-1} will be applied on the resultant cy_i. Then, this result will be Xored with RM_1 and RM_2 and will be subjected to another inverse substitution operation S_2^{-1}, respectively as seen in the following equations.

$$O_i'^{(-1)} = S_1^{-1}(cy_i) \tag{4.10}$$

$$y_i = S_2^{-1}(O_i'^{(-1)} \oplus RM_1 \oplus RM_2) \tag{4.11}$$

Finally, after obtaining y_i, x_i can be calculated using Equation 4.7 :

$$x_i = S_1^{-1}(O_i^{-1} \oplus RM_1 \oplus y_i) \tag{4.12}$$

In conclusion, this is a simple cipher that reaches the confusion and diffusion properties with just a single round via a dynamic key dependent manner. The efficiency and robustness are demonstrated in the following sections. Let us indicate that the proposed cipher

Algorithm 5 One round decryption

procedure ONE_ROUND_DECRYPTION(CX, S_1^{-1}, S_2^{-1}, RM_1, RM_2, π)
  for $i = 1$ to $\frac{\alpha}{2}$ **do**
    $X[\pi[i + \frac{\alpha}{2}]] = S_2^{-1}(S_1^{-1}(CX[\pi[i]]) \oplus RM_1 \oplus RM_2)$
    $X[\pi[i]] = S_1^{-1}(S_2^{-1}(CX[\pi[i + \frac{\alpha}{2}]]) \oplus RM_1 \oplus X[\pi[i + \frac{\alpha}{2}]])$
  return X

in this chapter is more simple and require less computation compared to the proposed one in the second chapter.

4.4/ SECURITY ANALYSIS

In this section, a security analysis for the proposed scheme is performed to demonstrate its robustness against all known confidentiality attacks such as statistical, differential, chosen/known plain-text, and brute-force attacks [Cho et al., 2011, ElGamal, 1985, Nyberg et al., 1995]. Several security experiments were conducted using the standard image Lenna. These experiments are based on different security measures like : statistical analysis, visual degradation, sensitivity. Statistical results of all security tests are shown in TABLE 4.4. Accordingly, The obtained results validate the robustness of the proposed approach.

4.4.1/ STATISTICAL ANALYSIS

A cipher scheme requires specific random properties in order to resist efficiently statistical attacks [Xu et al., 2008]. To prove the effectiveness of the proposed model, several statistical security tests were carried out to validate the uniformity and the independence properties.

4.4.1.1/ UNIFORMITY ANALYSIS

The PDF of the original plain-image and its corresponding cipher-image are both shown in Figure 4.4. It can be seen that the PDF of the encrypted image using the proposed scheme is similar to a uniform distribution with a value close to 0.039 ($\frac{1}{256}$). To validate this result at the sub-matrix level, an entropy test is performed and this is described next.

4.4.1.2/ ENTROPY TEST

The entropy test for the original and encrypted Lena images at the sub-matrix level and with a random dynamic key for $h = 8$ is shown in FIGURE 4.5. According to the results, the entropy of the encrypted sub-matrices has a value close to the desired value of 6, in case of $h = 8$, and close to 7.17 for $h = 16$, which indicates that the uniform distribution is ensured. Hence, the redundancy at the sub-matrix level is eliminated.

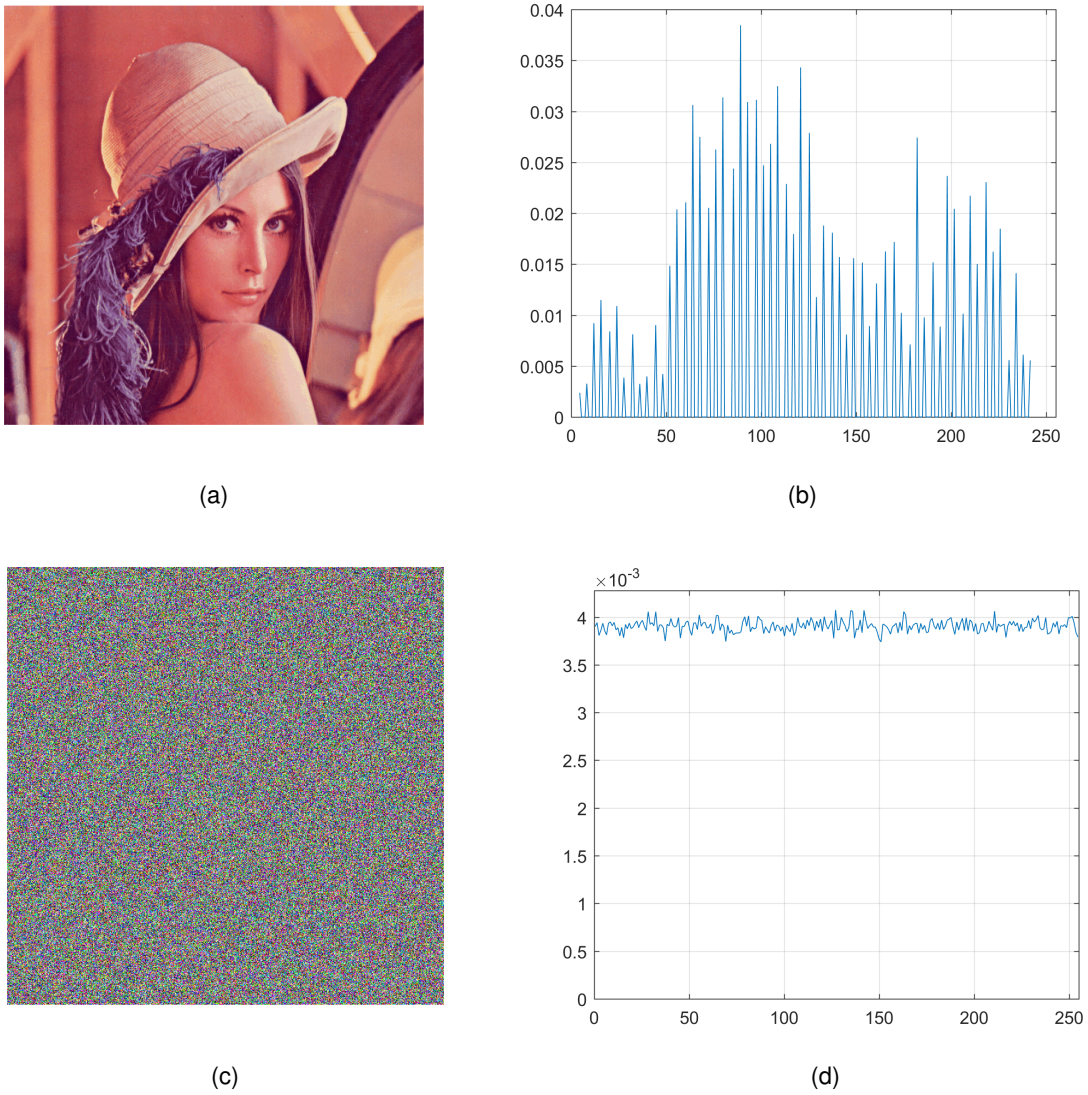
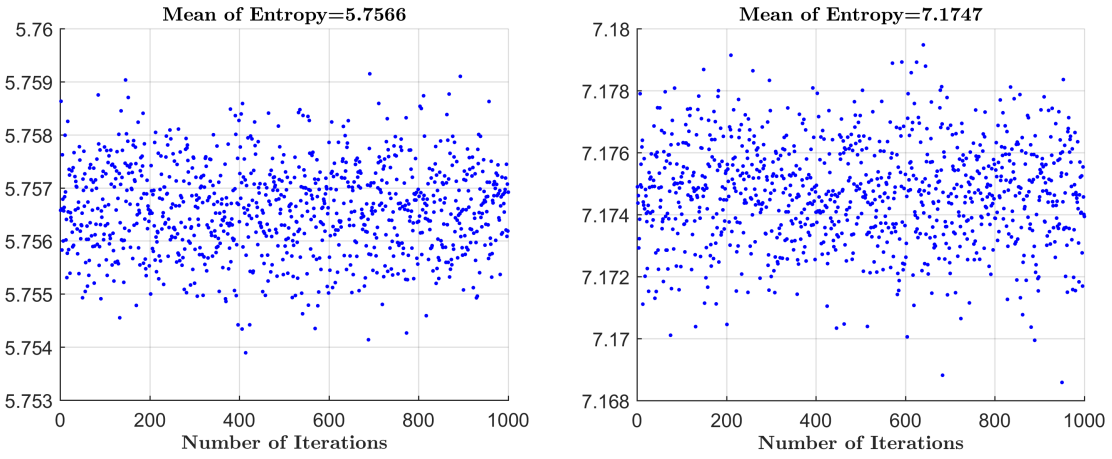


FIGURE 4.4 – (a) Original Lena, (b) PDF of original Lena with size $512 \times 512 \times 3$, (c) Encrypted Lena, (d) PDF of encrypted Lena

4.4.1.3/ TEST CORRELATION BETWEEN ORIGINAL AND CIPHER IMAGES

The correlation test is performed by taking randomly $N = 4,066$ pairs of adjacent pixels from the original and encrypted Lenna images. The correlation is quantified in horizontal, vertical and diagonal directions.

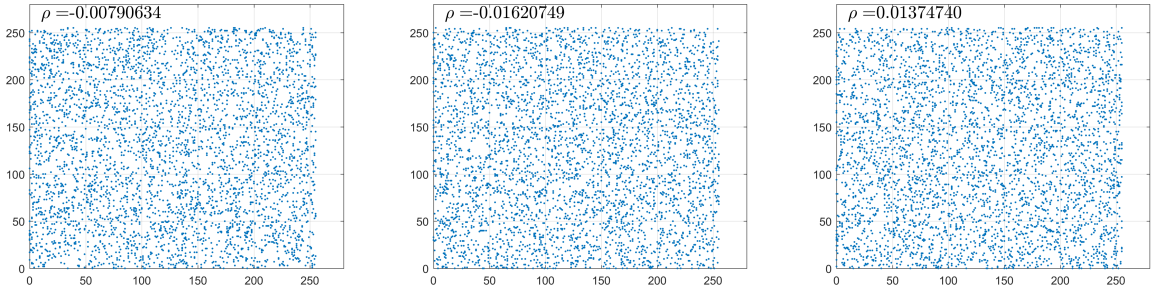
Obviously, the correlation between adjacent pixels in the plain image is high and its corresponding correlation coefficient is close to 1 [Fawaz et al., 2016, Noura et al., 2017b]. FIGURE 4.6 shows the correlation between adjacent pixels in the different directions for a random secret key. While, FIGURE 4.7 shows the variation of the coefficient correlation in the different directions for 1000 encrypted images, where each encrypted image uses a different secret key. According to these results, the ciphered images have a very low correlation coefficient (close to 0), which clearly shows that the proposed scheme drastically



(a) $h = 8$ (b) $h = 16$

FIGURE 4.5 – The entropy test of the sub-matrices of the encrypted Lena image with a random dynamic key for $h = 8$ (a) and $h = 16$ (b).

reduces the spatial redundancy.



(a) (b) (c)

FIGURE 4.6 – Adjacent pixels correlation for the ciphered Lena image with one random secret key : (a) horizontally, (b) vertically and (c) diagonally.

4.4.2/ VISUAL DEGRADATION

We calculated the PSNR and SSIM values between the original and the encrypted Lena image for $1,000$ dynamic keys. The results are shown in FIGURE 4.8. As shown, the average PSNR value is 8.5894 dB, which is a low value. This confirms that the proposed cipher produces a large difference between the original and the encrypted images. Similarly, the maximum SSIM value for $1,000$ dynamic keys did not exceed 0.04, which confirms a high and adequate visual distortion. As such, sufficient visual degradation is achieved since no useful information or any pattern could be revealed from the encrypted image.

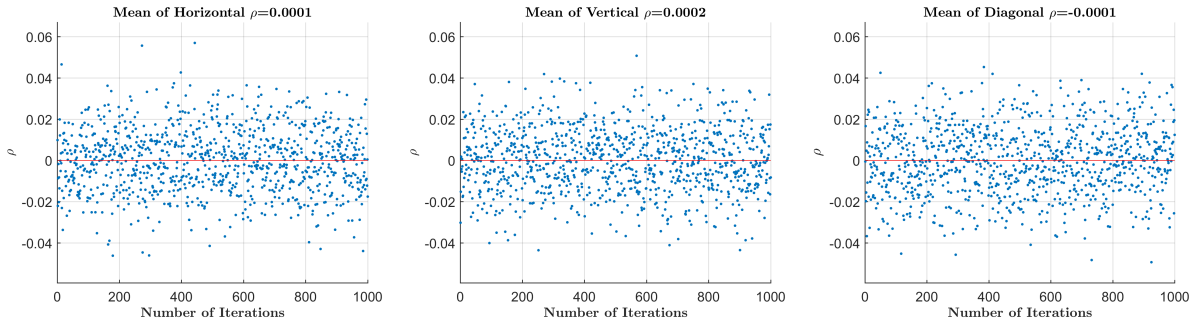


FIGURE 4.7 – Coefficient Correlation of adjacent pixels in encrypted Lenna : (a) horizontally, (b) vertically and (c) diagonally versus 1000 random secret keys.

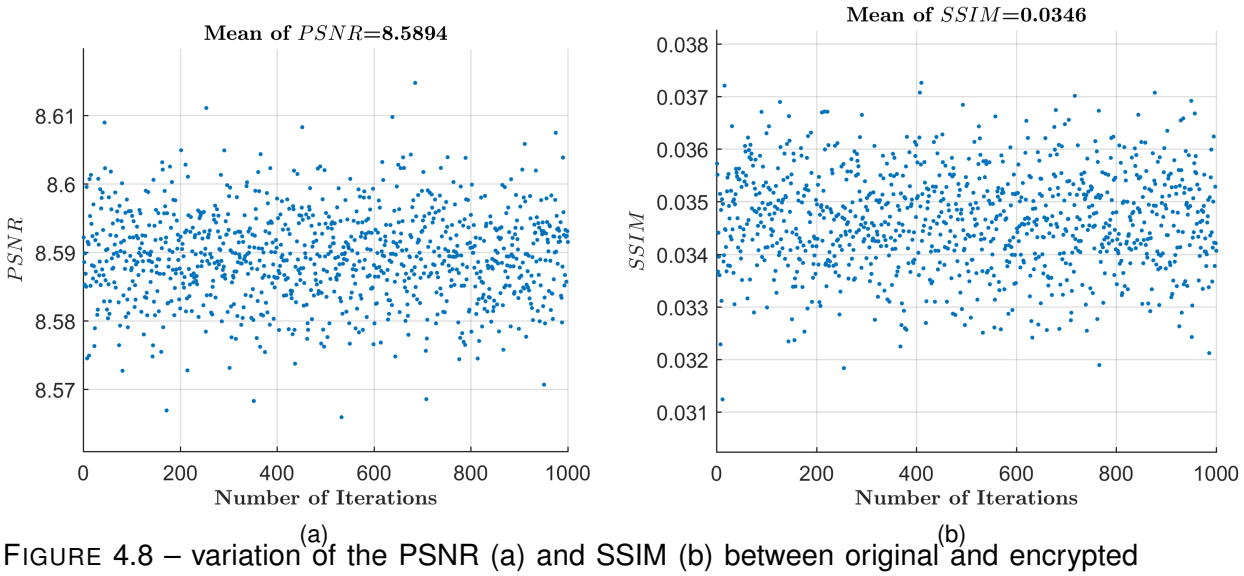


FIGURE 4.8 – variation of the PSNR (a) and SSIM (b) between original and encrypted Lena images versus $1,000$ dynamic keys.

4.4.3/ DIFFERENCE BETWEEN PLAIN AND CIPHER IMAGES

The difference between original and encrypted images at the bit level must reach a value very close to the ideal one (50%). We show the percent variation of the bit difference between the original and cipher Lena images for $1,000$ random dynamic keys in FIGURE 4.9. The results show that the percentage difference is always close to 50%. Hence, the proposed cipher satisfies the independence criteria.

4.4.4/ SENSITIVITY TEST

To avoid differential attacks, the relation between two encrypted images must be studied. Any slight difference in the plain image or in the key (usually one bit difference) must drastically affect the resultant encrypted image. As the percentage of change increases, the scheme will have better sensitivity. Two types of sensitivity require to be tested are :

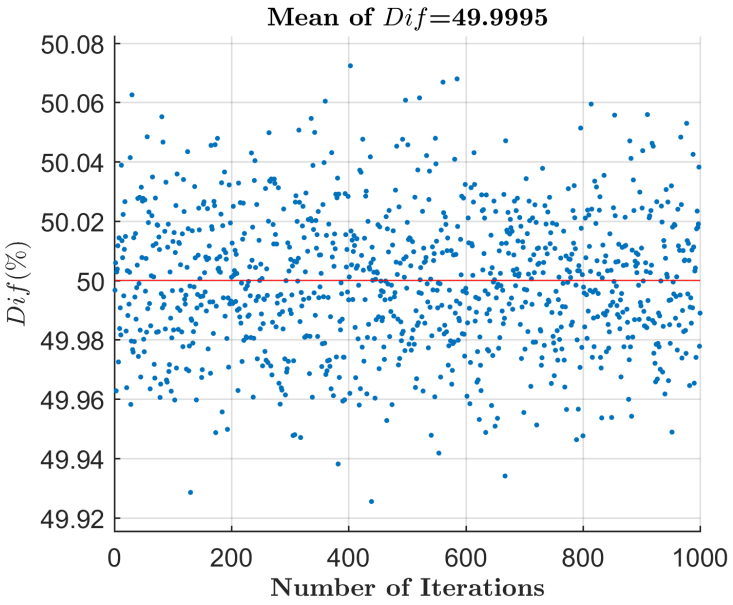


FIGURE 4.9 – Percentage Difference between plain and ciphered Lena for 1,000 random dynamic keys.

Plain Sensitivity (PS) and **Key Sensitivity (KS)**.

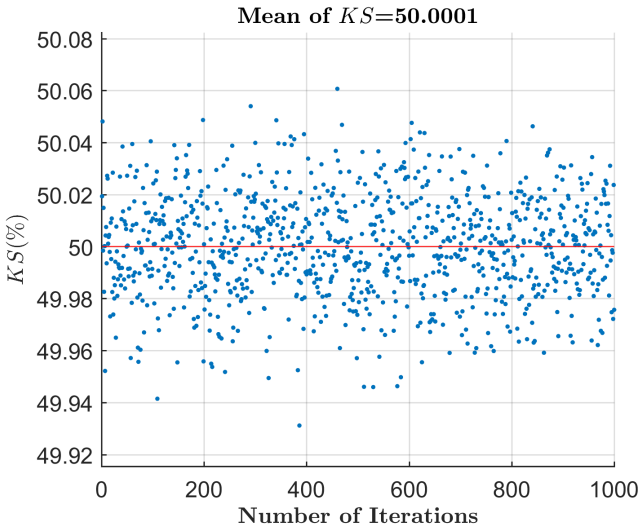


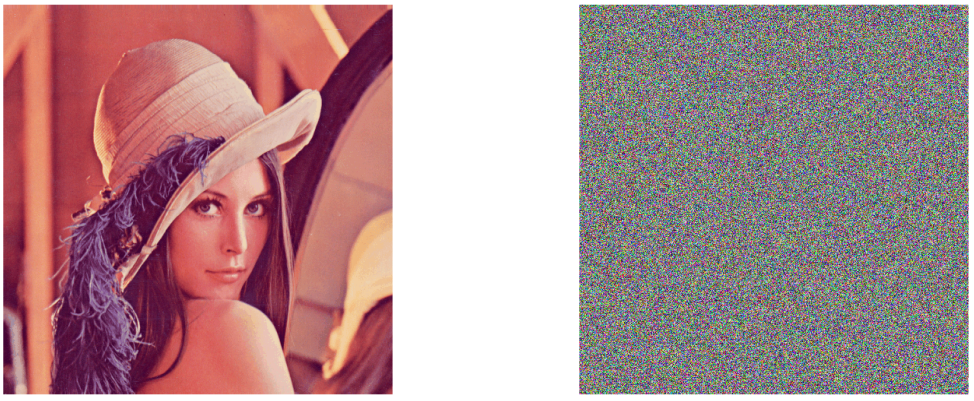
FIGURE 4.10 – Key sensitivity against 1,000 random dynamic keys.

Plain-text Sensitivity : This type of sensitivity is not relevant to the proposed algorithm since different dynamic keys can be used for each input image. Accordingly, the scheme produces totally different cipher images. Hence, the cipher successfully meets the avalanche effect due to the dynamic key approach and this will not provide any information about the secret key.

Concerning the **Key Sensitivity** test, it is one of the most important tests and permits to quantify the sensitivity against a slight change in the secret key. In fact, the proposed

key derivation function is based on a secret key and an initial vector. To study the key sensitivity, two dynamic keys are used : DK_1 and DK_2 that only differ by one random bit. The two plain-images are encrypted separately and the Hamming distance of the corresponding cipher-images C_1 and C_2 is computed and illustrated in FIGURE 5.18 against $1,000$ random dynamic keys. The majority of values can be seen to be close to the optimal value of $(50\ \%)$, indicating that the proposed encryption model is robust and has enough strength against any minor change in the dynamic key.

A decrypted Lena image is shown in Figure 4.11, which was decrypted using a dynamic key with a one-bit error. It is clear that this algorithm is highly sensitive to the dynamic key and any change in the latter will lead to a different decrypted image with no useful information. This test, in addition to the tests done previously, guarantees that a high sensitivity level and a high randomness degree are achieved with the proposed cipher scheme.



(a) (b)

FIGURE 4.11 – Decrypted Lena image with its corresponding correct dynamic (a) and with one bit error in the dynamic key used (b).

TABLE 4.4 – Statistical results of the listed tests by using original Lena image with the proposed cipher scheme and for 1,000 random keys.

Proposed Scheme				
	Min	Mean	Max	Std
Dif	49.9254	49.9995	50.0724	0.0229
KS	49.9311	50.0001	50.0607	0.0196
$H-E$ (h=8)	5.7539	5.7566	5.7591	0.0008
$\rho-h$	-0.0462	0.0001	0.0569	0.0154
$\rho-v$	-0.0617	-0.0005	0.0529	0.0157
$\rho-d$	-0.0503	-0.0001	0.0455	0.0158
PSNR	8.5659	8.5894	8.6147	0.0065
SSIM	0.0312	0.0346	0.0373	0.0009

4.4.5/ CRYPTANALYSIS : RESISTANCE AGAINST WELL-KNOWN TYPES OF ATTACKS

The proposed scheme was tested using a set of security tests repeated 1,000 times to prove its immunity against attacks. Next, we present a brief cryptanalysis discussion to demonstrate the security of the cipher and its ability to resist the existing and modern confidentiality attacks. Different statistical tests were performed and they proved that the proposed cipher satisfies the uniformity and independence properties. Hence, a high randomness level is achieved in a dynamic manner, which makes the proposed cipher immune against statistical attacks.

Moreover, we performed sensitivity tests on the proposed cipher scheme. The results proved that the cipher exhibits a high level of sensitivity, which makes it immune against key-related attacks.

On the other hand, the proposed cipher can resist brute force attacks since the secret key has a flexible size of either 128, 196, 256 or 512 bits, and the Nonce has a size of 512 bits. Moreover, the size of the dynamic key is also 512 bits. Therefore, the size of the static secret key, dynamic key and Nonce are sufficient to make the brute force attack unfeasible.

More importantly, the dynamic key-dependent structure plays a significant role in making the proposed cipher scheme immune against the current and future powerful attacks such as chosen/known plain/cipher text attacks.

In conclusion, the security level of the proposed cipher scheme is confirmed. In the following section, we verify the efficiency of the proposed cipher as a good cipher candidate.

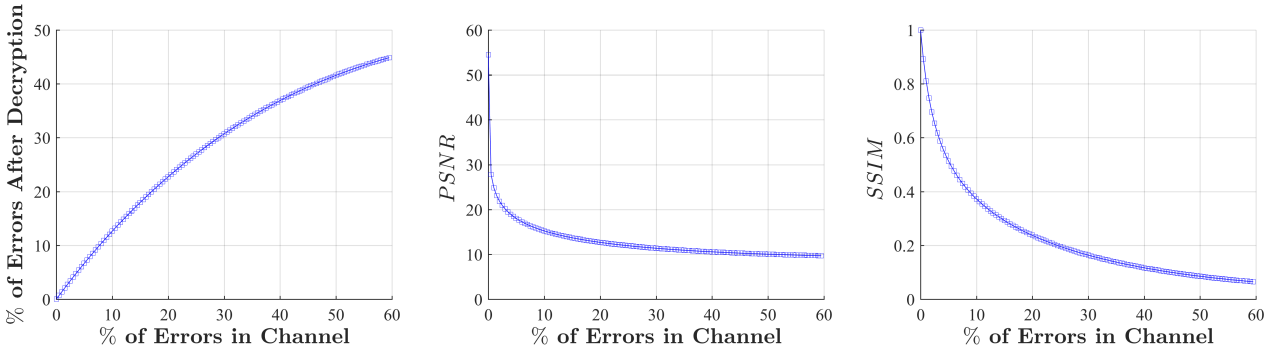
4.5/ PERFORMANCE ANALYSIS

In this section, the performance of the proposed cipher scheme is analyzed to validate its effectiveness. Several performance experiments were done such as studying the effect of the error propagation and measuring the execution time. The results indicate clearly the efficiency of the proposed cipher.

4.5.1/ ERROR PROPAGATION

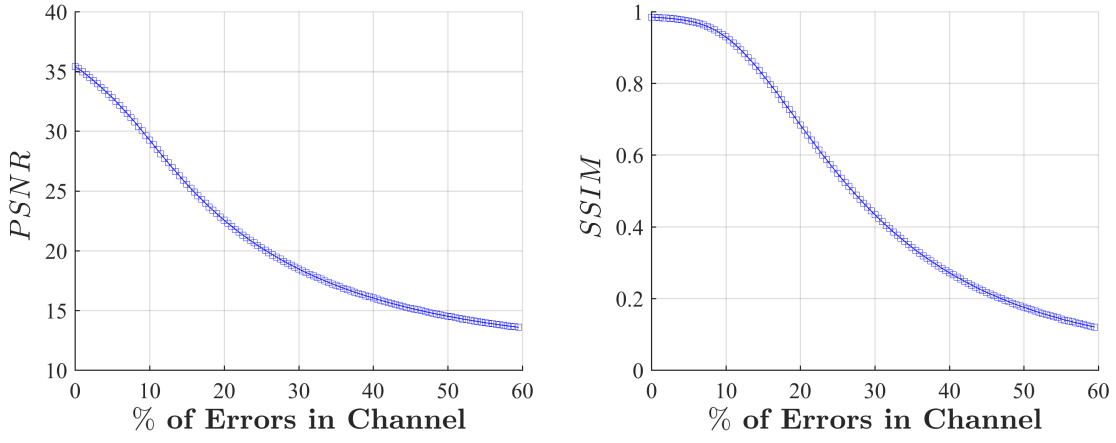
In fact, the lower the error propagation, the more effective and practical the cipher scheme will be. In the proposed cipher, the error will **only** affect the corresponding sub-matrices (x_i, y_i). More precisely, the effect of a bit error introduces only a specific sub-matrix error at the same byte position of the error in the decrypted image. Hence, the error in the proposed scheme is not propagated randomly to both sub-matrices as in [Fawaz et al., 2016, Noura et al., 2017b]. In order to quantify the visual degradation, we use again the two well-known parameters, PSNR and SSIM. The variation of SSIM and PSNR versus the percentage of errors are shown in FIGURE 4.12. The proposed solution shows a linear difference, and the variations of SSIM and PSNR show that the scheme is immune to a highly erroneous channel. This conclusion is confirmed by showing the

decrypted image corresponding to a large number of errors (FIGURE 4.14). In addition, when an image is decrypted with errors, the tests showed that applying a filter to clean the image can solve the noise problem. In our simulations, a random noise was added (up to 20%) and a median filter was capable of removing the added noise. Note that the size of the median filter should not exceed the size of the sub-matrix, which is $h \times h$. This is shown in FIGURE 4.13 and 4.15 and it is clear that the filtered images are flawless with no errors appearing visually.



(a) (b) (c)

FIGURE 4.12 – Variation of the impact of the error propagation (% of bits difference between decrypted images) (a) and the variation of SSIM (b) and PSNR (c) versus the percentage of errors in channel for the proposed approach.



(a) (b)

FIGURE 4.13 – Variation of PSNR and (b) SSIM versus the percentage of errors in channel for the proposed approach after applying a median filter.

4.5.2/ EXECUTION TIME

An efficient cipher scheme must reach low computational complexity to ensure low latency and consequently low resources and energy consumption.

In order to show the efficiency of the proposed cipher scheme for IoT devices, a compa-

(a) 1% (b) 5% (c) 9% (d) 15% (e) 20%

FIGURE 4.14 – Decrypted images in function of the percentage of errors in channel for the proposed approach.

(a) 1% (b) 5% (c) 9% (d) 15% (e) 20%

FIGURE 4.15 – The result of applying a median filter to Lena decrypted images with different percentages of errors.

rison with AES OpenSSL was performed. OpenSSL is commonly used and considered as one of the most important and efficient cryptographic libraries that can provide a robust, commercial-grade, and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. On the other hand, the proposed approach has been implemented in Matlab, C and Java. Therefore, to show a better system performance, the ”C” implementation is selected to be compared with the AES OpenSSL implementation on two very common IoT hardware **Raspberry Pi Zero W (wireless) and Raspberry Pi 2**. The ”Raspberry Pi Zero” has a Broadcom BCM2836 SoC with a 1 GHz single-core ARM1176JZF-S. The ”Raspberry Pi 2” has a Broadcom BCM2836 SoC with a 900 MHz 32-bit quad-core ARM Cortex-A7 processor.

We record the average time (for $1,000$ iterations) to encrypt the plain Lena image of size $512 \times 512 \times 3$. For the Raspberry Pi Zero W (called RPi Zero later) and for the Rasberry Pi 2 (called RPi 2 later) the optimal size of blocks is 32.

The encryption and decryption times of our one round approach and of AES (128 bits) are presented in Table 4.5. The time ratio shows that the proposed approach is 7% faster on the RPi Zero for the encryption process and 21% faster in the case of decryption. On the RPi 2, the gain in encryption is 29% and 33% in decryption. It should be noted that the proposed algorithm is completely written in C while OpenSSL uses assembly optimization [Bernstein et al., 2014]. Despite this optimization, an important reduction in encryption and decryption times is achieved. This primary result indicates clearly that, by optimizing the proposed approach and by employing assembly optimization, a better reduction in latency and energy consumption can be achieved. In fact, this is our future perspective. Moreover, in FIGURE 4.16, we show the variation of the execution time for the encryption and decryption algorithms versus h is presented. The experiments were performed on two different hardware devices, RPi W and RPi 2. The results indicate clearly

that increasing h reduces the required latency at the expense of additional memory overhead. Therefore, the choice of h depends on the latency and hardware requirements ; the proposed approach provides the user with the opportunity to choose the value of h depending on the application requirements. In fact, when devices have high memory capacity, a high value of h can be chosen (16 or 32). While, for low-cost devices that have limited memory capacity, a low value of h must be chosen (4 or 8). In this chapter, extensive security tests are performed with h equals to 8, which represents a good balance between computational complexity and memory consumption.

TABLE 4.5 – The mean encryption time (in seconds) of AES and the proposed cipher approach for $512 \times 512 \times 3$ Lena image and for $1,000$ iterations.

Hardware	Algorithm	Encryption Time (s)	Decryption Time (s)
RPi Zero W	One round	0.0388	0.0340
	AES	0.0418	0.0432
RPi 2	One round	0.0260	0.0251
	AES	0.0367	0.0374

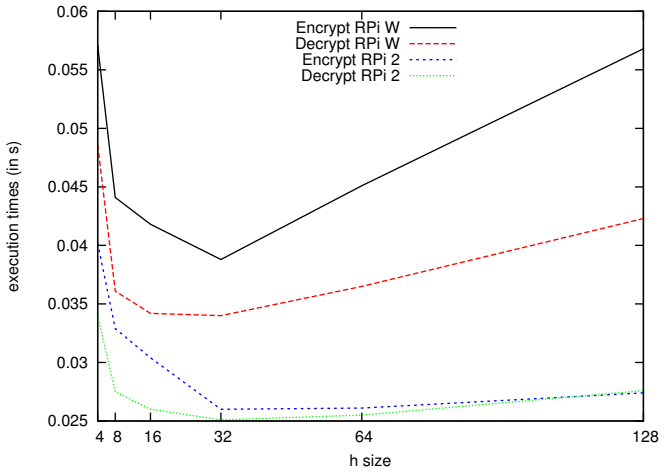


FIGURE 4.16 – Execution times on RPi W and RPi 2 versus h.

4.6/ CONCLUSIONS AND FUTURE WORK

A single-round, flexible, dynamic, key-dependent lightweight cipher scheme targeted for IoT devices(medical) has been presented. The scheme has been shown to be efficient and secure, with fast execution time. The scheme is based on a dynamic structure in contrast to standard techniques. This will provide better robustness against different powerful attacks because of the different substitution and permutation primitives in addition to the two dynamic pseudo-random matrices that are generated in a dynamic manner. Moreover, the proposed substitution and diffusion primitives ensure the desirable cryptographic performance in an efficient manner and simple hardware implementation. The proposed cipher scheme requires only one iteration and its corresponding round function consists of simple operations, which addresses the limitations of IoT devices. An extensive security analysis revealed that the proposed approach is strong enough against different kinds of attacks. Finally, the results clearly showed that the scheme outperforms the optimized AES implementation of OpenSSL, which indicates that the

approach is more suitable for delay-sensitive medical applications.

5

Efficient & Secure Medical Data Availability and Protection Scheme

ABSTRACT

Recently, several cipher algorithms have been proposed to deal with the specific characteristics of medical contents such as size, redundancy, etc. The majority of the existing solutions consider one security service, data confidentiality. In this chapter, we present a comprehensive solution for securing images, providing confidentiality, integrity, availability, and source authentication based on a dynamic key-dependent approach. A dynamic key is generated for every input image towards ensuring a high level of resistance against powerful attacks targeting data confidentiality and availability. Each dynamic key is divided into five sub-keys, and each sub-key is used to generate or update a cryptographic primitive by using a specific permutation table. The image confidentiality is guaranteed by using a single round cipher scheme based on a dynamic byte (or block) permutation operation. Moreover, the image availability is ensured via a modified information dispersal algorithm (IDA). The proposed modifications to the original IDA include : i) using a set of fragmentation matrices instead of one ; ii) relating the fragmentation matrices to a dynamic sub-key ; iii) applying the fragmentation algorithm at the block (h bytes) level instead of the whole message whereby the input image is divided into a set of blocks, and each block has k bytes elements, and it can also be applied at the sub-matrix ($h \times h$) level ; iv) selecting the fragmentation matrices for each block based on a dynamic key-dependent table. This selection table is produced based on a dynamic sub-key and it is updated for each new input image through a permutation operation. The image integrity and source authentication are achieved by using a keyed hash function that employs a dynamic integrity-authentication sub-key. The aim of the proposed solution is to strike a good balance between the required security level and the system performance. The security analysis confirms the robustness of the proposed scheme, which exhibits a high degree of randomness and uniformity, hard visual degradation, and a high key sensitivity. Moreover, a performance analysis was performed to verify that the proposed solution ensures a high level of efficiency and a low error propagation rate. Finally, the proposed solution can be applied to protect different types of data and is not limited to image contents.

5.1/ INTRODUCTION

Data security is a major concern in the networking domain. With the emergence of new types of applications in future networks, tremendous amounts of critical data will be stored/shared in a digital form (e.g. images). Accordingly, security concerns such as confidentiality, integrity, and availability become even more crucial than before. Several solutions have been proposed to ensure the security and privacy of this type of critical data and to protect it from any unauthorized access.

In general, data confidentiality can be ensured by using symmetric key encryption, which can be applied at the either the block or the stream level. However, the encryption of an image is different than that of plain text due to the specific data characteristics within an image [Mostefaoui et al., 2015b, Noura et al., 2017c, Noura et al., 2018b]. As such, traditional block cipher schemes such as AES [Daemen et al., 2013] (Advanced Encryption Standard) have been optimized towards being suitable for securing images, but these solutions are based on applying a round function over multiple round ; In every round, several substitution and diffusion operations are performed, which is computationally expensive. However, recent image cipher schemes [Noura et al., 2017c, Noura et al., 2018b, Noura et al., 2018e, Noura et al., 2018c, Noura et al., 2018a] with a low number of rounds (1 or 2) have been proposed to overcome the multi-round computational complexity. These schemes are based on the dynamic key approach where the structure of all the cipher primitives changes depending on the dynamic key. These primitives are updated for each new input image, and this takes place at a low computational cost. However, these cipher schemes require hardware optimization similar to that of AES to achieve a better cost reduction when compared to optimized AES.

On the other hand, data availability is key to prevent system failure since new attacks suck as ransomwares (e.g. WannaCry) have shown their potential to compromise data communication systems. Typically, distributed storage systems can provide a reliable access to data through redundancy where data is distributed among a group of nodes, and each node holds the whole data in encrypted or plaintext form. However, a better solution is to disperse the data into fragments and spread them among a set of nodes, where an individual node holds only an encrypted part of the original data.

Thus, dispersing data fragments over multiple locations limits the risk of an attacker to gain access to the whole data in contrast to the traditional approach. The data fragments are normally generated using secret sharing such as Shamir secret sharing, information dispersal algorithms, or data shredding [Kapusta et al., 2017, Kapusta et al., 2016].

In this chapter, a set of existing secret sharing schemes are presented, and they are described briefly in Section 5.2. These techniques ensure secure data redundancy whereby each entity holds only a portion of the secret.

5.1.1/ RELATED WORKS

Data can be fragmented in various ways such as the case in perfect secret sharing [Shamir, 1979], computational secret sharing [Resch et al., 2011, Krawczyk, 1994], information dispersal [Rabin, 1989], and data shredding [Cincilla et al., 2015,

Fabre et al., 1994].

Since Shamir [Shamir, 1979] and Blakley [Blakley, 1899] proposed their secret sharing schemes in 1979, the issues of secret sharing have been investigated widely in the last decades. Also, the concept of (k, n)-threshold Secret Image Sharing (SIS) has been further extended [Thien et al., 2002, Cimato et al., 2017, Lee et al., 2014, Wei et al., 2015]. SIS schemes can be divided into two sub-classes including polynomial-based, and boolean-operation based schemes.

In general, a secret image is encoded into several shadow images (so-called shares or sub-images) using a Visual Secret Sharing (VSS) scheme [Naor et al., 2017, Cimato et al., 2017]. This turns an image into n different noise-like shares. The reconstructed secret image can be recognized by the human visual system by superimposing any k shares, where $n \geq k$. No information about the secret image could be revealed by collecting less than k shares. This is a so-called k-out-of-n scenario.

In [Thien et al., 2002], the authors presented a k-out-of-n polynomial-based secret image sharing (PSIS) scheme to reconstruct loss-less secret images by applying the Lagrange interpolation technique. Later on, many extensions to PSIS have been presented to meet different goals such as authentication [Ulutas et al., 2013], progressive secret image recovery [Guo et al., 2012], and essential shadows [Li et al., 2013b].

On the other hand, IDA was presented and described [Rabin, 1989] ; the input file of size $|M|$ is divided into k pieces with each piece having a size of $\frac{|M|}{k}$. Then, these k pieces are encoded by multiplying them by a static integer matrix to produce n data chunks (coded pieces), and stored at n different storage devices. The main property of the selected matrix is that any k rows of this matrix should form a square invertible matrix. In addition, each data share is a linear combination (according to the employed specific column matrix) of all data chunks and matrix elements. The recovery is only possible when k fragments are gathered.

5.1.2/ Problem Formulation

A new scheme, intermediary between secret sharing and information dispersal algorithms, was recently sketched out in [Anonymized, 2016]. However, this approach suffers from high error propagation, and the computational operations cannot be performed in parallel.

The choice of the most appropriate method depends on the particularity of the use-case : perfect secret sharing may be highly secure but it is slow and very costly in terms of memory and storage. While the original IDA (threshold secret sharing scheme) can be resilient and relatively fast, but it is not highly secure. In fact, Rabin's IDA has several advantages : it adds resiliency to data, produces almost ($n-k$ fragments) storage overhead, and uses simple arithmetic operations. However, this scheme only guarantees an incremental confidentiality level. An eavesdropper who knows the dispersal matrix can verify whether a fragment has a predetermined value or not. Moreover, an attacker can guess the content of missing fragments when the data has recognizable patterns. Despite such problems, IDAs are still being used in the context of data protection.

Towards overcoming the security issue of IDA, a new variant, "AONT-RS", is presented ;

it combines symmetric encryption (AES) with the original IDA. This solution is more secure than the original IDA and it is scalable, but in some circumstances, it might be less efficient than the information dispersal.

Typically, any data protection solution needs to consider the complex trade-off between cost effectiveness (including memory usage, processing, and computational complexity), and the required security level. Thus, there is a need for an efficient lightweight cryptographic scheme that can achieve strong data protection (data confidentiality, data integrity, and data availability) with the minimal processing overhead when applied to large size contents such as images.

However, the existing secure variant of IDA (i.e. AONT) introduces processing and memory overhead, which hinders its adoption. Our main goal is to show how we can ensure a high security level without a negative impact on the system performance.

Note that, designing an efficient AONT-RS variant that avoids complex operations is not a straightforward task since the algorithm should guarantee a high security level while not impacting the system performance.

5.1.3/ MOTIVATIONS AND CONTRIBUTIONS

In this chapter, we modify the original IDA scheme and we propose an algorithm that exhibits high efficiency in terms of storage and communication, low computational complexity, and a high security level when compared to AONT.

The proposed solution is suitable for the scenarios of limited processing and memory resources. It is based on a dynamic key-dependent IDA and dynamic cipher operations. The security performance results show that the proposed approach can prevent severe attacks without degrading the system performance in terms of latency and energy consumption.

As shown in Figure 5.1, our model consists of a source node that aims at securely storing an image by distributing it over n storage nodes.

Overall, the proposed scheme has been designed to achieve the following goals :

1. **Robustness against attacks** : The proposed cryptographic solution is robust since it is based on the dynamic key approach. Different dynamic cryptographic primitives are actually used for each new input image : a set of IDA matrices instead of a static one, a permutation cipher table, and two pseudo-random selection tables. Moreover, a high level of randomness, uniformity, and key sensitivity are also achieved. According to the sensitivity tests, any slight modification in the Nonce or in the secret keys leads to different shares with a probability of difference close to $\frac{1}{2}$. Also, the secret key size is flexible and can be set to either 128, 196 or 256 as AES, and the size of the dynamic key is 512 bits. This makes the proposed solution challenging to break by brute force attacks. [Paar et al., 2009b].
2. **Fast response time** : The employment of a one-round cipher with a single operation (permutation) results in low computational complexity and a faster encryption algorithm when compared to the existing cipher algorithms. In addition, the

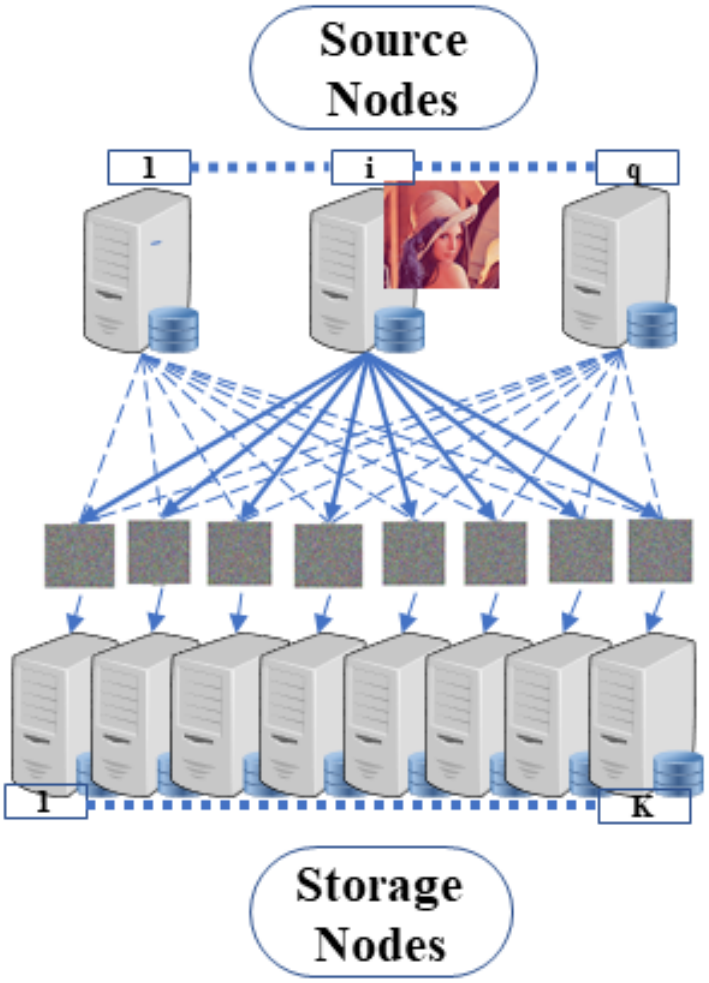


FIGURE 5.1 – Distributed Storage Model

fragmentation/de-fragmentation algorithm can be implemented in parallel for different blocks, which reduces the computation overhead by a factor of q, where q represents the number of threads.

3. **Adaptable to constrained devices :** The low execution time, simple implementation, and low memory requirements are all mandatory conditions to have an efficient model that accounts for the short battery life and low memory and processing resources, especially in the case when there is a need to store private images on personal devices.
4. **Low propagation error** : Since the key is dynamic and not fixed, it is possible to safely apply the proposed algorithm in ECB mode since the same image, if repeated, will be encrypted with a different key and this will result in a different cipher image ; such a scheme is no longer a code-book scheme and exhibits a low error propagation rate.
5. **Simple implementation** : The proposed algorithm is based on simple operations

such as look-up tables for the permutation, and selection and update primitives. Moreover, it uses arithmetic operations that also can be optimized by using look-up tables for matrix multiplications.

5.1.4/ ORGANIZATION

The rest of this chapter is organized as follows : Section 5.2 presents existing secret sharing schemes. Then, Section 5.3 presents the proposed algorithm including the generation of the dynamic keys and the required cryptographic primitives such as the two pseudo-random selection tables, the permutation table, and the set of IDA matrices. Next, Section 5.4 presents the details of the proposed key-dependent fragmentation and encryption/decryption schemes. In Section 5.6, we describe the performance evaluation of the proposed solution, and we conduct a security analysis to assess its robustness. Section 5.8 illustrates the results of the performed tests. Finally, we conclude and present the future work in Section 5.9.

5.2/ SECRET SHARING SCHEMES

This section presents the most relevant schemes related to secret sharing, information dispersal, data shredding, and all-or-nothing transform. Later in this chapter, we show a comparison in terms of security and performance of these algorithms along with those of our own proposed solution.

5.2.1/ INFORMATION DISPERSAL ALGORITHMS

An Information Dispersal Algorithm (IDA) [Rabin, 1989] divides data d into n fragments, each of size $\frac{d_{size}}{k}$, such that any k fragments could be used together for the reconstruction of the original data. More precisely, n data fragments (data shares) are obtained by multiplying the initial data by a $k \times n$ non-singular generator matrix. Data recovery consists of multiplying any k fragments by the inverse of a $k \times k$ matrix built from k rows of the generator matrix. Information dispersal adds redundancy to data without any storage overhead. In [Li, 2012], Li analyzed the confidentiality of IDAs. For instance, Rabin's IDA proposal was found to have high data confidentiality since the original data cannot be explicitly reconstructed from a number of fragments less than k. However, even though it is not possible to recover the initial data, yet some information about its content could be leaked since the data patterns are preserved inside the fragments when the same matrix is reused to encode different data chunks. A similar problem occurs when using symmetric encryption with the Electronic Code Book (ECB) mode of operation [Barker et al., 2011].

The proposed IDA encoding step is defined by the following matrix equation :

$$F = E(m, k) = G \odot M \tag{5.1}$$

where M is the plaintext (reshaped to k rows), G is an integer $n \times k$ matrix. The inverse IDA process is simply applied to the matrix multiplication by using the inverse corresponding matrix G_k of the specific k received data shares. The inverse IDA process to recover the

original file is obtained according to the following equation :

$$M = D(m,k) = K^{-1} \odot E(m,k) = G_k^{-1} \odot F_k \tag{5.2}$$

Where G_k consists of k rows of the IDA matrix G and G_k^{-1} is its corresponding inverse. In addition, F_k represents k data shares that are obtained by multiplying G_k with M.

5.2.2/ SHAMIR'S SECRET SHARING

Shamir's perfect secret sharing scheme (SSS) [Shamir, 1979] takes as input the message data d and divides it into n fragments $F_1, \ldots, F_n$, of which at least k are needed for initial data recovery. This algorithm is based on the fact that given k unequal points $x_1, \ldots, x_k$ and arbitrary values $F_1, ..., F_k$, there is at most one polynomial $y(x)$, of degree less or equal to $k-1$, such that $y(x_i) = F_i, i = 1, ..., k$. The algorithm provides high level of confidentiality, but has quadratic complexity in function of k and exhibits a high memory overhead since the size of each fragment is as large as the size of the initial data. Therefore, SSS is usually applied to ensure the protection of small or critical data like encryption keys. In such a case, drawbacks of the SSS scheme are acceptable and negligible, but for a larger data, they present a major issue.

Shamir proposed (k, t) threshold mechanism that is also called a secret sharing scheme based on polynomial interpolation in 1979 (Shamir,1979). The basic idea of Shamir's scheme is based on the fact that two points are needed to determine a line, three points are needed to determine a quadratic, and so on. Suppose we have a prime p, which is larger than all the possible messages and also larger than the number of participants, n. All the calculations are carried out by mod p. Here, we can also use a composite number n, however, it will not guarantee that the obtained matrices have inverses.

5.2.3/ SECRET SHARING MADE SHORT

Krawczyk's Secret Sharing Made Short (SSMS) [Krawczyk, 1994] combines symmetric encryption with a perfect secret sharing for the protection of larger data. Data d is encrypted using a symmetric encryption algorithm, then fragmented using an IDA (Krawczyk introduces his own IDA). The encryption key is fragmented using a perfect secret sharing scheme and is dispersed within data fragments. Accordingly, the solution does not require an explicit key management, and the storage overhead does not depend on the data size, but is equal to the size of the key per data fragment. The performance of the SSMS technique depends on the details of the chosen encryption and IDA techniques.

5.2.4/ AONT-RS

The AONT-RS technique [Resch et al., 2011] is similar to SSMS as it combines symmetric encryption with data dispersal. It applies an all-or-nothing transform (AONT) [Rivest, 1997] to create k fragments : encrypted data is divided into $k-1$ fragments and an additional fragment is generated by *xor*-ing hashes of these data fragments with the encryption key. Additional $n-k$ fragments are produced using a systematic Reed-Solomon error correction code. Data integrity is ensured by the use of a canary that is dispersed within the fragments.

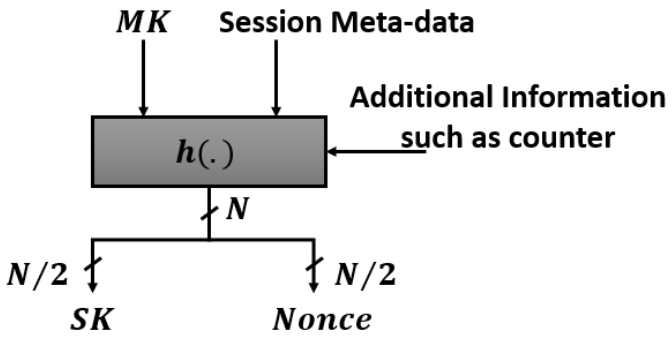


FIGURE 5.2 – Proposed Session Key and Nonce Generation process

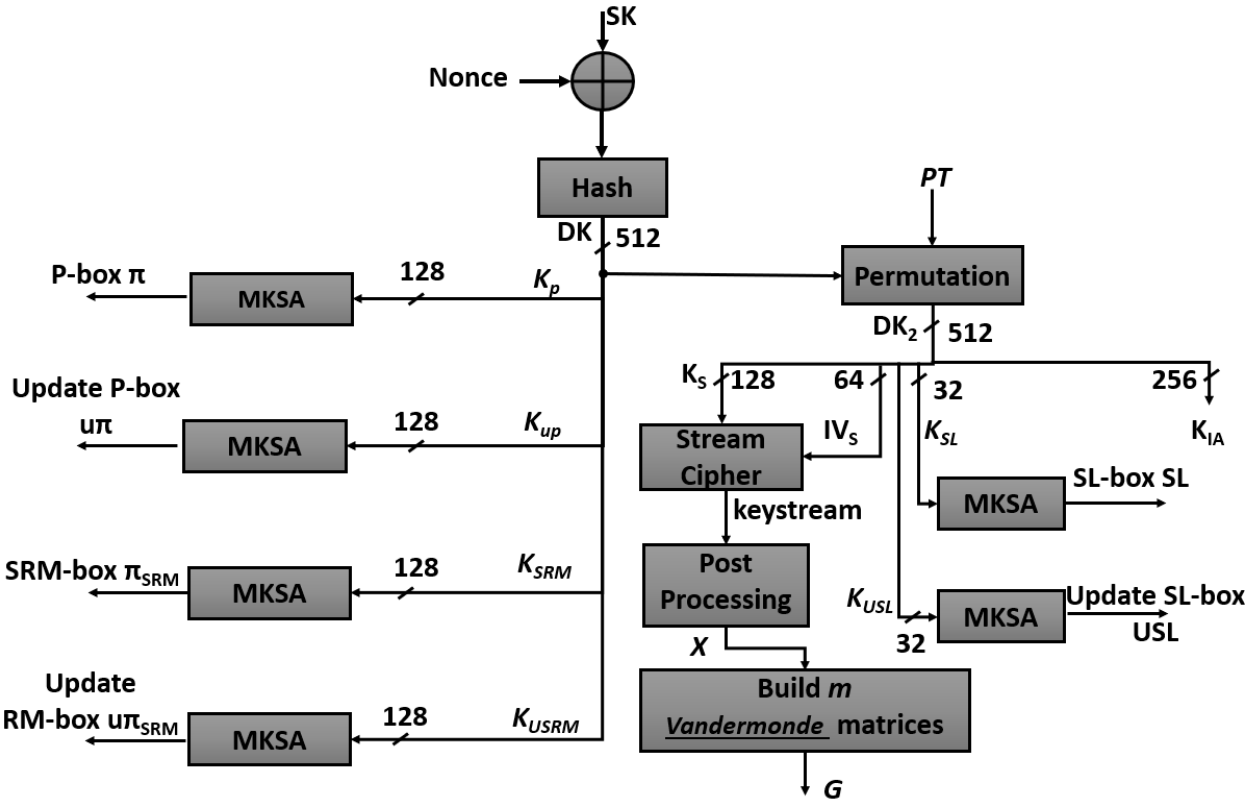


FIGURE 5.3 – Proposed key derivation function and its corresponding cipher and update primitives generation process

5.3/ PROPOSED KEY DERIVATION SCHEME

In this section, we explain the generation process of the dynamic key(s) and the associated sub-keys that are used in the different cryptographic primitives.

FIGURE 5.3 illustrates the key derivation function, which takes as input a secret session key SK and a nonce N_o that are unique for every session :

— **Secret Session key** SK **:** This secret session key is produced for every new session (specified by the underlying application) to increase the security level. An effi-

cient technique to produce the session keys is through any Deterministic Pseudo-Random Number Generator (DRBG) [Barker et al., 2011] and by using a master key as a seed.

— **Nonce N_o :** A a new $Nonce$ is generated at each new application session. N_o can be also generated using a DBRG, a master key, and some meta-data. Moreover, $Nonce$ has the same length of the session key.

The proposed solution to produce a new session key and Nonce is illustrated in FIGURE 5.2.

The secret session key SK and N_o are Xored and the corresponding output is hashed to produce the dynamic key $DK = h(SK \oplus N_o)$, where h is a secure hash function such as SHA-512. This operation ensures simultaneously the sensitivity of the cipher key and the nonce. Note that, the secure hash function ($SHA-512$) is selected because it offers the desirable cryptographic hash properties such as the high resistance against collision attacks. This ensures that the produced DK is renewed for every session and consequently, different cryptographic updates and primitives will be produced, which guarantees the randomness of the scheme. Employing a dynamic key will provide high immunity against existing and modern attacks.

Next, DK is divided into four different sub-keys that form the seeds for the different cipher primitives as described next.

5.3.1/ DYNAMIC KEY & SUB-KEYS DERIVATION

DK can be changed as frequently as needed by the user or by the application by modifying the session time. Furthermore, as $SHA-512$ is used, DK has a size of 512 bits (64 bytes) and it will be split into four sub-keys, where each one has a size of 128 bits (16 bytes). These sub-keys are $\{K_p,\ K_{up},\ K_{SRM},\ K_{USRM}\}$ and each will be used for a different purpose within the algorithm (see FIGURE 5.3).

— **Permutation sub-key K_p** : it consists of the most significant 16 bytes of DK.
— **Update permutation sub-key K_{up}** : it consists of the next most significant 16 bytes of DK.
— **Selection matrices sub-key K_{SRM}** : this consists of the third most significant 16 bytes.
— **Update selection matrices sub-key K_{USRMP}** : the least significant 16 bytes of DK.

In parallel, another dynamic key DK_2 is obtained by permuting DK using the initial permutation table of DES PT [Stallings, 2017, Paar et al., 2009b].

Furthermore, as DK is only permuted, then $DK2$ has a 512-bit length (64 bytes) and it will be split into five sub-keys where two (K_SL and K_USL) of them have a size of 32 bits, the third one IV_S has a size of 64 bits, the fourth one K_S has a size of 128 bits (16 bytes) and the last one has a size of 256 bits. Each of these sub-keys will be used for a different purpose within the algorithm (see FIGURE 5.3).

— **Seed sub-key K_S** : it consists of the most significant 16 bytes of DK_2.
— **Initial Vector sub-key IV_S** : it consists of the next most significant 8 bytes of DK_2.
— **Update Selection sub-key K_{USL}** : it consists of the next most significant 4 bytes of DK_2.
— **Selection sub-key K_{SL}** : it consists of the next most significant 4 bytes of DK_2.

— **Message Integrity-Authentication sub-key** K_{IA} : the least significant 32 bytes of DK_2.

In summary, the size of the dynamic sub-keys (K_p, K_{up}, K_{SRM}, and K_{USRM}) is set to $L = 16$ bytes, while K_{SL} and K_{USL} are set to 4 bytes.

Table 5.1 shows all the notations used in this chapter. The derived dynamic key is renewed for each input image and any bit change will lead to a completely different set of sub-keys and consequently different cipher primitives will be generated. In the next section, we describe the construction of the proposed cipher primitives that are based on these four sub-keys.

5.3.2/ Construction of Cryptographic Primitives

We aim to design a simple, yet very effective and efficient lightweight AONT-RS variant, which uses a cipher algorithm with only one round and one flexible permutation operation that can preserve the homomorphic properties. The objective is for the proposed solution to be employed with constrained user devices.

Fortunately, the dynamic key approach can provide a high security level against existing and future powerful attacks [Noura et al., 2017c, Noura et al., 2018a, Noura et al., 2018e]. This is ensured since all the used sub-keys depend on the produced dynamic key and consequently, the cryptographic primitives become variable, which prevents attackers from recovering any information from the collected/chosen/known set of original encrypted images. More importantly, the dynamic key approach helps in reducing the required number of iterations [Noura et al., 2018a]. Additionally, it reduces the required processing and memory resources and latency, which are key for preserving the main functionality of real-time applications.In fact, K_p, K_{up}, K_{SRM}, K_{USRM}, K_{SL} and K_{USL} are used in the proposed modified KSA algorithm to produce the permutation tables π, $u\pi$, π_{SRM}, $u\pi_{SRM}$, SL, and USL, respectively. In the following, we describe the techniques for the construction of the key dependent cipher primitives.

5.3.2.1/ Dynamic Permutation Primitives

In general, a permutation operation is used to ensure the diffusion property. In this chapter, we propose a one-round key-dependent encryption scheme based on the permutation operation either at the byte or at the block level. The scheme is based on the dynamic key-dependent cipher structure for the generation of a dynamic permutation table, and it can achieve high performance according to [Noura et al., 2015a] since it requires only one operation, which presents a linear computational complexity. The permutation table π with (α bytes or blocks) is updated for each new input image by using the update permutation table ($u\pi$).

In this chapter, the modified KSA of $RC4$ presented previously is used to produce the required permutation tables.

Moreover, the proposed technique to build dynamic key-dependent flexible permutation tables P showed high robustness and cryptographic strength for $L \geq 4$.

On the other hand, the inverse permutation table is necessary for the decryption process. Since the produced P is bijective, the inverse of P, P^{-1}, can be obtained easily by the

TABLE 5.1 – Summary of notations used.

Notation	Definition
SK	Secret Key
N_o	Nonce
DK	Dynamic Key
DK_2	Second Dynamic Key and it is obtained by permuting DK using the initial permutation table of DES.
K_p	Permutation sub-key used to construct the permutation table π
K_{up}	Update permutation sub-key used to construct the update permutation table $u\pi$, which is used to update the permutation table for each new input image file
K_{SRM}	Selection matrices sub-key used to construct the selection matrix table π_{SRM} that is used to select which one of the IDA matrices will be used during each input block
K_{USRMP}	Update selection matrices sub-key used to construct the update permutation table $u\pi_{SRM}$, which is used to update the selection table π_{SRM} for each new input image file
K_S	Seed sub-key used as seed of any stream cipher that produces a keystream, which is post-processing to form m IDA matrices
IV_S	Initial Vector sub-key
K_{USL}	Update selection sub-key used to construct the update selection table π_{USL}
K_{SL}	Selection sub-key used to construct the update selection table π_{SL}
K_{IA}	Message Integrity-Authentication sub-key
π	A Dynamic produced permutation table (P-box)
π^{-1}	The inverse corresponding to the permutation table (P-box)
$\pi(i)$	The corresponding permuted value at the i index of π
X	the produced filtered keystream
x_i	the i^{th} block of X and it is used to construct the G_i IDA vandermode matrix
G	A set of m dynamic IDA matrices
$G(i)$	The i^{th} dynamic IDA matrix
$G_k(i)$ and $G_k^{-1}(i)$	a $k \times k$ of the i^{th} dynamic IDA matrix ($G(i)$) and its corresponding inverse matrix.
M	Original image file
$\|M\|$	size of the original image I
data chunk	k consecutive bytes of permuted image file
data share	an encoded data chunk with length n bytes
fragment	a final data fragment, which represents the same column of all the data shares and is stored in one location storage entity
k	number of fragments required for data recovery
nr	number of data chunks inside initial data
$n, n \geq k$	total number of fragments
DC_i	i^{th} data chunk set, a set of k bytes of data chunks
DS_i	i^{th} data share set, a set of n bytes of data shares
C hline R	Columns Number Rows Number
P	Plane Number (for gray-scale is equal to 1
α	The number of bytes in an input image file after reshaped it to a vector
x_i	the i^{th} block of the produced filtered keystream X and it is used to construct the G_i IDA vandermode matrix

following operation $P^{-1}[P(i)]=i$.

Where $\pi(i)$ represents the value of the π at the i^{th} index and $1 \leq \pi(i) \leq \alpha$. The process of permutation is realized by employing a swap function, where (i) and $(\pi(i))$ are the original and permuted byte/block positions of the image.

5.3.2.2/ Dynamic Selection Sub-matrices Table

K_{SRM} is used as a seed for the proposed modified KSA algorithm to build the flexible key-dependent selection IDA matrix table SRM with nr elements. Moreover, the i^{th} IDA matrix used for the i^{th} permuted block (k bytes) is selected according to $\pi_{SRM}(i)^{th}$. In addition, $\pi_{SRM}(i)$ represents the value of the π_{SRM} at the i^{th} index and $1 \leq \pi_{SRM}(i) \leq m$, where m represents the produced IDA matrices and $m \leq nr$.

Similarly, for the decryption process, the same operations are performed, but with the inverse IDA matrix $G_k{-}1(\pi_{SRM}(i))$. This means that π_{SRM} is used to control the modified IDA and inverse IDA processes.

Another permutation table is required to control the IDA matrices during the fragmentation process (π_{SRM}), which is updated for each new input image via the update permutation table $u\pi_{SRM}$.

5.3.2.3/ Dynamic Fragments Distribution Table based on π_{SL}

We use another permutation table, SL, Where $SL(i)$ represents the value of the SL at the i^{th} index and $1 \leq SL(i) \leq n$.

SL can be considered as a permutation table with n elements, and it is used to control the distribution of the fragments to n different storage entities. SL is updated after each new input file by using the update permutation table USL. As such, the fragments of each image are distributed differently compared to the previous or next images. This increases the security level since if a storage entity is compromised, it would contain different fragments for different images, which is better than having a specific index fragment of all images at one entity.

5.3.2.4/ Dynamic Key-Dependent Pseudo Random IDA Matrices

The IDA key is divided into two parts ($\{K_S;\ IV_S\}$). The proposed modified IDA scheme requires m IDA matrices that are chosen in a dynamic manner to ensure high randomness properties and to remove any existing patterns from the permuted message blocks. Each IDA matrix requires only a row of n unique and non zero bytes. In fact, in this step, the $RC4$ stream cipher algorithm is used and it is iterated with a dynamic seed K_S and a dynamic initial vector IV_S towards producing the required key-stream of length $m \times n$ bytes. The produced key-stream is used to form a bank of m invertible matrices.

The key-stream is post-processed and reshaped into m rows, each with n bytes such that each row does not contain any repeated or zero values. If these n bytes have zero bytes or repeated value(s), the stream cipher is re-iterated to replace them until no repeated or zero values are found in this block. These conditions are necessary to preserve the

invertibility property of the obtained matrices (to recover the initial data). Each filtered row is used to construct an $n \times k$ IDA Vandermonde matrix (using Vandermonde matrix form). The obtained IDA Vandermonde matrices are used during the fragmentation process. Any k rows of any of these IDA matrices form an invertible $k \times k$ matrix. In fact, the Vandermode matrix form can help to produce invertible matrices, but only if the input block used to construct this matrix does not contain repeated or zero values. On the other hand, the dynamicity of the stream cipher avoids any possible security weakness and consequently, it ensures a high level of randomness, uniformity, and periodicity. Note that any efficient secure stream cipher can be used, and the choice of RC4 is due to its simple software and hardware implementations and its ability to generate permutation primitives with good cryptographic performance. In this chapter, the RC4 stream cipher [Paul et al., 2011] is used only to produce the IDA matrices (cryptographic primitives) and not for the encryption/decryption process.

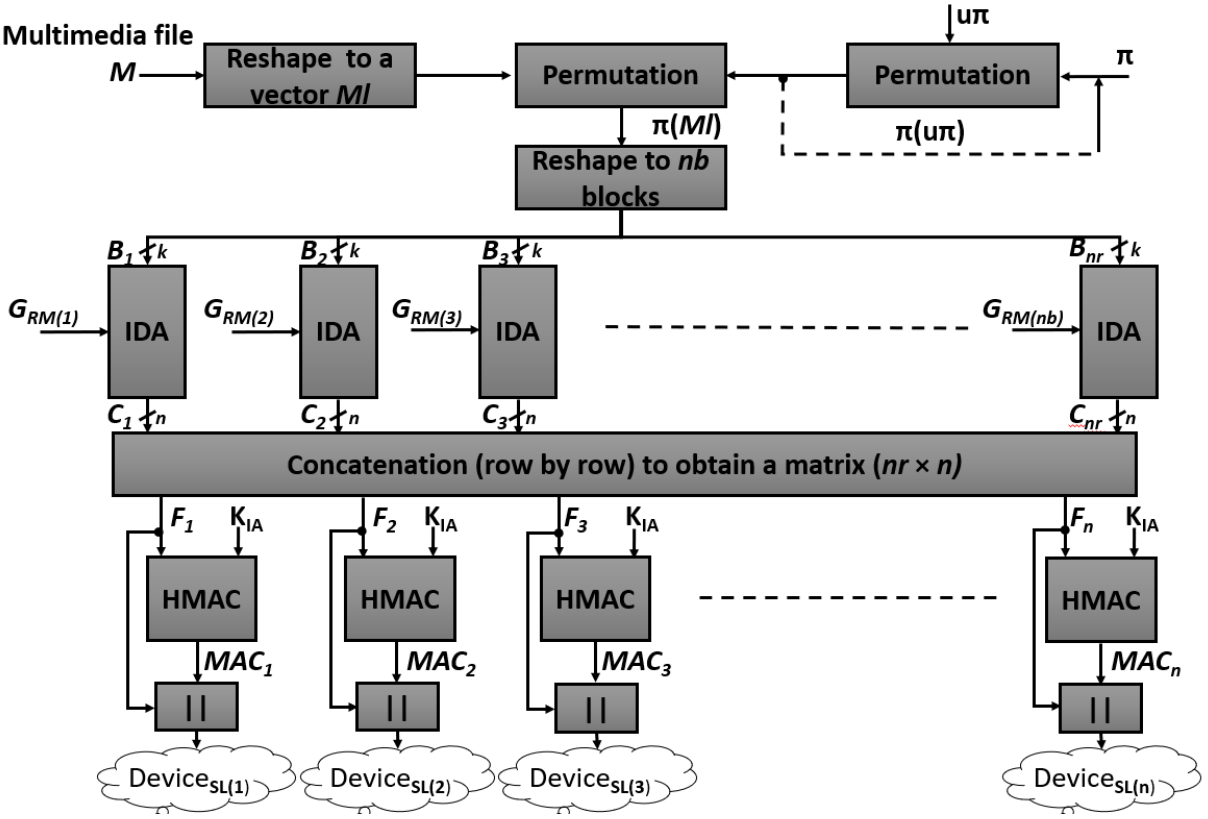


FIGURE 5.4 – Proposed Cryptographic Solution

5.4/ PROPOSED CRYPTOGRAPHIC SOLUTION

This section describes in details the proposed cryptographic scheme. Figures 5.4 and 5.5 present an outline of the proposed data confidentiality-Availability-Integrity solution. The inverse cryptographic solution is not presented in details simply because it consists of the same operations (with slight changes such as the use of the inverse matrices in the multiplication) in reverse order.
The proposed algorithm is symmetric and is based on a secret key SK shared between

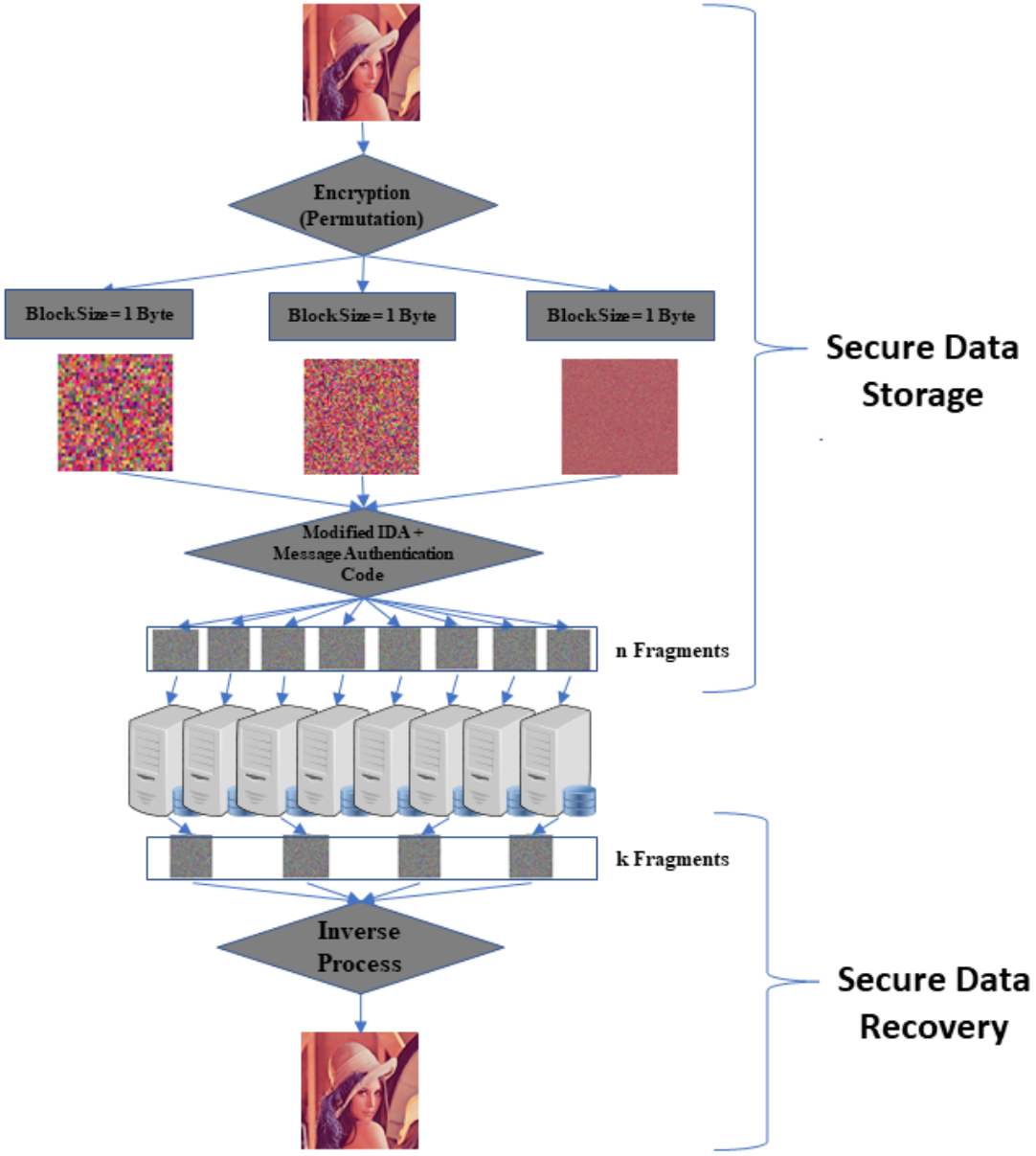


FIGURE 5.5 – An example of the proposed Cryptographic Solution

the sender and the receiver. As stated earlier, this key is combined with a $Nonce$ to produce a dynamic key, which is split into sub-keys that are used to construct the cryptographic primitives.

The first step is the encryption process, then the modified IDA process, which produces n fragments. Next, for each fragment, we apply a data integrity and source authentication process.

5.4.1/ ENCRYPTION PERMUTATION PROCESS

The encryption process is based only on **one round and one permutation operation**. First, an input image file M of size $C \times R \times P$ is reshaped into a vector Ml of α bytes, where $\alpha = \frac{C \times R \times P}{TB}$, TB represents the block length, and $Ml = \{m_1, m_2, \ldots, m_\alpha\}$. Then, The permutation is applied on Ml by using a dynamic permutation table π. Such a scheme exhibits very low computational complexity and resources [Noura et al., 2015a],[Zhang et al., 2010].

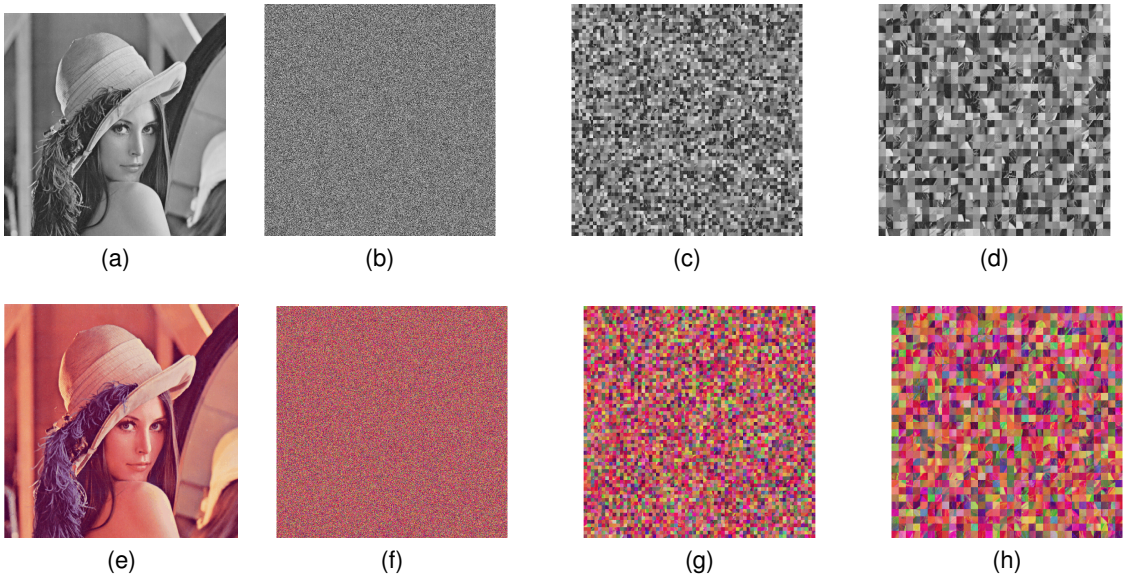
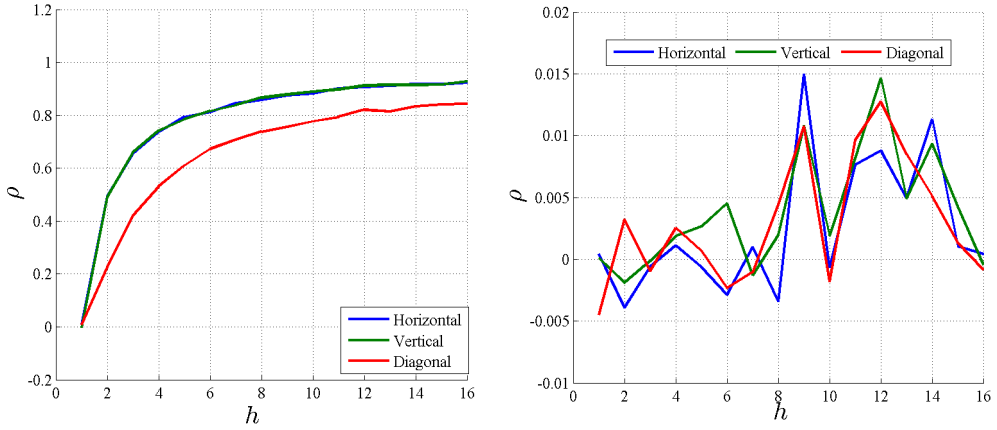


FIGURE 5.6 – (a) Original Gray Lenna image, (b)-(d) the corresponding permutations, (e) colored Lenna image, and (f)-(h) the corresponding permutations ; for block size $TB = 1$, 8×8 and 16×16, respectively.

Let the employed permutation table π of dimension α be defined by : $\pi=[p_i]_{1\leq i\leq \alpha}$.
A plain-text Ml of length α is given by : $Ml = [Ml_i]_{1\leq i\leq \alpha}$.
After permutation $\pi(Ml) = [Ml_{p_i}]_{1\leq i\leq \alpha}$.

For each input image, the permutation table is updated using the update permutation table and thus, each image is permuted differently compared to the previous or next images. An example of the proposed key-dependent permutation image encryption scheme is presented in FIGURE 5.6 for the original gray and color Lenna images for different permutation block size $TB = 1 \times 1$, 8×8 and 16×16, respectively.

A trade-off between the size of the permutation block size TB and the randomness degree is visually clear as shown in figure 5.6, where permuted gray and Lenna images are presented for different values of TB. In figure 5.7-a the results indicate that increasing the value of TB leads to an increase in the correlation between the adjacent pixels. From FIGURE5.7-b, showing the results for the fragmented encrypted images (permutation and IDA steps), we can see that for any value of TB, a low correlation between the adjacent pixels is obtained. Consequently, the proposed IDA algorithm decreases noticeably the correlation between adjacent pixels and removes the spacial redundancy.



(a) (b)

FIGURE 5.7 – (a) Correlation between adjacent pixels of encrypted image (permutation only) and (b), applying permutation with the proposed modified IDA algorithm on Lenna image versus h.

5.4.2/ MODIFIED IDA ALGORITHM

The modified IDA algorithm is presented in Algorithm 6. The IDA algorithm can be considered as a data encoding step and it is based on matrix multiplication. The input is a permuted image vector Ml that is padded (if the number of bytes of the permuted message is not a multiple of k) and reshaped to form nr data chunks $DC_1, \ldots, DC_{nr}$, where $nr = \lceil \frac{|Ml|}{k} \rceil$ and the length of each data chunk is k bytes. These data chunks are encoded one by one into nr data shares $DS_1, \ldots, DS_{nr}$ and the length of each data share is n bytes. Each data share contains only n bytes. For convenient processing, the data chunks are regrouped into nr data chunk sets (blocks) of k elements, where $DC_i(j)$ is the jth byte in the ith data chunk block. The i^{th} data chunk DC_i is encoded using one of the set of m IDA matrices. The selection of the dynamic encoding IDA matrix depends on the use of the selection permutation table, $\pi_{SRM} = [\pi_{SRM}(i)]_{1 \leq i \leq nr}$ and it has the same length of data chunks/data shares, nr. Moreover, $\pi_{SRM}(i)$ is an integer value between 1 and m. The selection of the corresponding encoding matrix is controlled by using the permutation table π_{SRM} that has a length equals to nr and this table contains elements that vary from 1 to m, where m is the number of possible IDA matrices. $G = GS(\pi_{SRM}(i)$ indicates that $\pi_{SRM}(i)$ IDA matrix is used. Additionally, data shares are regrouped into nr data shares of n elements each. Finally, data shares are distributed into n final fragments, where each column of DS represents a fragment. This means that the column i of data shares represents the i^{th} fragment.

In addition, k is flexible, however, increasing it leads to an increase of the security level and a decrease of the resiliency degree. In the rest of this chapter, we fix k to 8. Note that k and n can be changed according to the possible number of storage devices. Any k fragments are needed for data recovery.

Note that the enhanced IDA is built without altering some homomorphic properties (addition and multiplication by scalar) in contrast to AONT-RS where the homomorphic properties are lost (uses AES that relies on a substitution operation).

Algorithm 6 Fragmentation algorithm outline.

1: $DC = DC_1, DC_2, , \ldots, C_{nr}$
2: $DS = DS_1, DS_2, \ldots, DS_{nr}$
3: **for** $i = 1 \rightarrow nr$ **do**
4: $\quad G_i \leftarrow G(\pi_{SRM}[i])$
5: $\quad DS(j) \leftarrow (G \odot DC_j)$
6: $F \leftarrow reshape((DS_1 || DS_2 || \ldots || DS_{nr}), n, nr)$
7: **for** $i = 1 \rightarrow n$ **do**
8: $\quad F_i \leftarrow Fi, 1 \rightarrow end$

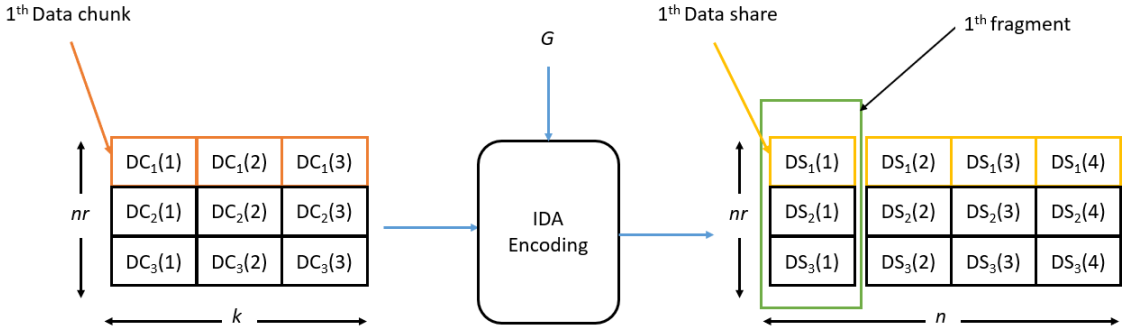


FIGURE 5.8 – Example for $k = 3$: Encoding of the i^{th} data chunk DC_i (left) is transformed into i^{th} data share DS_i (right) and $i = 1, 2, \ldots, nr$.

5.4.3/ DATA ORIGIN AUTHENTICATION SCHEME

The output of the enhanced IDA process is n fragments $F = \{F_1, F_2, \ldots, F_n\}$. Each fragment F_i is hashed using a keyed cryptographic hash function such as the lightweight HMAC presented in [Noura et al., 2015b] wit K_{IA} as a secret key. The authentication key is K_{IA} and it is used to authenticate each fragment F_i. MAC_i is the i^{th} Message Authentication Code (MAC_i), which is concatenated at the end of its corresponding fragment ($F_i || MAC_i$) and sent to one of the n storage devices.

5.5/ INVERSE CRYPTOGRAPHIC SOLUTION

The inverse process of the proposed cryptographic solution uses the same operations in reverse order. Having DK, all the secret cryptographic primitives can be generated and consequently, their corresponding inverse ones.

The decryption process is based on the following steps :

1. First, the dynamic key generation and cipher primitives construction are performed.
2. **Collection of k fragments received from k different location storage devices**.
3. **Verification of the received fragments** : The data integrity and source authentication of each received fragment are verified by applying the same keyed hash function with the specific origin authentication key K_IA. Each fragment is validated if the received MAC is equal to the computed one.

4. **Inverse IDA Decoding (De-fragmentation)** : The verified k fragments are grouped into a matrix, where each row represents k bytes of the data share. Then, the inverse modified IDA process is performed by using the inverse IDA matrices of the received k fragments. The receiving end host can generate the same secret IDA matrices and the same dynamic matrix selection permutation algorithm by using the corresponding dynamic key. The inverse modified IDA decoding algorithm is done per block and by multiplying with the inverse matrices G_k^{-1} (according to the selected k fragments).

   Accordingly, the matrix multiplication of each encoded block and its corresponding inverse matrix is performed to recover the permuted block. Next, all encoded blocks are stored row by row to form a matrix of $nr \times K$, that will be reshaped to form the permuted image vector.

5. **Decryption (Inverse Permutation using the inverse permutation table π^{-1})** : At this stage, the inverse corresponding dynamic key-dependent permutation table π^{-1} is applied on the permuted image vector to recover the original image. In fact, the inverse permutation table can be obtained from the original permutation table by : $\pi^{-1}[\pi[i]] = i$. Finally, the image is reshaped to the original size $L \times C \times P$.

5.6/ SECURITY ANALYSIS

The security analysis of the proposed scheme is based on the methodology presented in [Noura et al., 2018a, Noura et al., 2014]. In fact, an efficient cryptographic solution should protect data against the most known types of confidentiality, integrity and availability attacks such as statistical, differential, chosen/known plain-text, and brute-force attacks [Noura et al., 2018b]. Extensive experiments are performed in this section to demonstrate the robustness of the proposed scheme against these attacks. In the following, the uniformity and independence properties are analyzed in details, in addition to the sensitivity of the dynamic keys and the difference between the original and the fragmented encrypted data.

Statistical Tests (randomness tests such as Correlation between plain and fragmented images and uniformity tests such as entropy and Probability Density Function (PDF) tests) were adapted to the fragment level instead of the message level. For instance, tests were realized in function of the number of fragments k.

The security analysis results show that the proposed solution ensures a high level of randomness as presented in Section 5.6.1. The uniformity and independence of the fragmented data are shown in Section 5.6.2 and 5.6.3, respectively. Moreover, in Section 5.6.4, the sensitivity test of the proposed scheme is performed and the results indicate that the proposed solution exhibits a high sensitivity level.

All tests were performed using Matlab. The standard original images such as Lenna and peppers (512 pixel width, 512 pixel height and 8-bits gray image) are used. Figures 5.12 and 5.13 show these images with some of the corresponding fragment images (shadow). In this test, $k =$ is equal to 4 and $n =$ to 8. This means 8 shadow images are produced for each new input image. In addition, the size of each shadow image is 128×128 since the size of the original image is 512×512, and $k = 4$. To recover the original image, any k shadow images can be used.

In contrary to Rabin's IDA scheme that struggles with the problem of data patterns appearing in the fragmented data, the proposed scheme does not preserve distances between encoded data parts (see FIGURE 5.9 and 5.10), since the dynamic key-dependent approach is used in the different cryptographic processes such as encryption, modified IDA (a set of m IDA matrices instead of static ones), and data origin authentication.

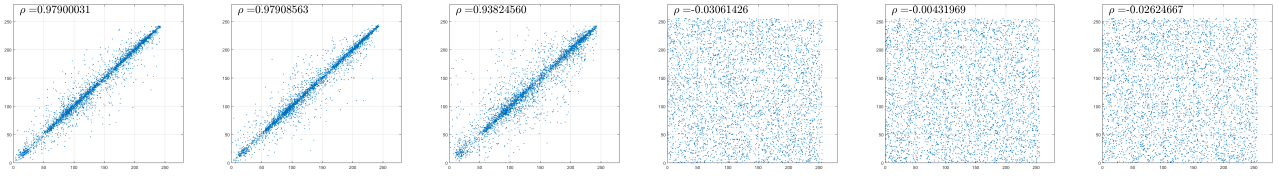
The permutation cipher algorithm is introduced before the fragmentation process to increase the randomness of the fragmentation input. Moreover, the modified IDA applies the IDA encoding at the row level and not on the whole matrix, which makes the parallel processing possible and efficient. Also, the modified IDA scheme uses a set of dynamic matrices (instead of one), and for each block (row), an IDA matrix is selected according to a dynamic selection table.

5.6.1/ RANDOMNESS TESTS

The original images have a high spacial redundancy, which should be removed after the encryption step, if an efficient cipher scheme [Noura et al., 2018e, Noura et al., 2018a] is used. Two original plain-images and their corresponding fragmented images (Lenna and Pepper) are shown in figures 5.12, 5.13, respectively.

To measure the randomness introduced by the proposed solution, we used the correlation test. This test randomly takes $N = 4,000$ pairs of adjacent pixels from the two plain images and their corresponding fragmented images.

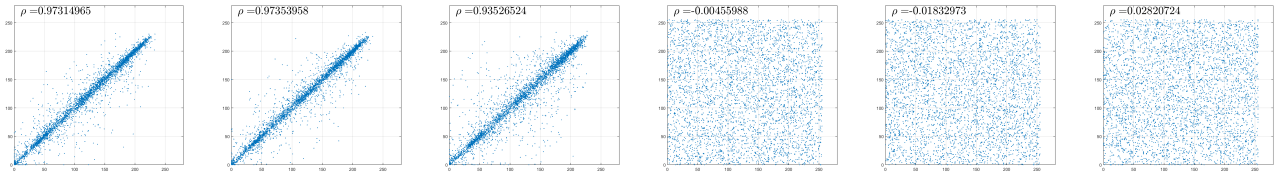
The obtained results for two standard images (Lenna and peppers) at their first shadow images level are presented in FIGURE 5.9, 5.10 and 5.11 for 100 random secret session keys. The results clearly indicate the high correlation between adjacent pixels in the original images (correlation coefficient close to 1). As for the fragmented shadow images, the correlation coefficient becomes very low (close to 0), which clearly indicates that the proposed fragmentation-encryption scheme reduces noticeably the spatial redundancy. Moreover, the statistical results are presented in Table 5.2.



(a) (b) (c) (d) (e) (f)

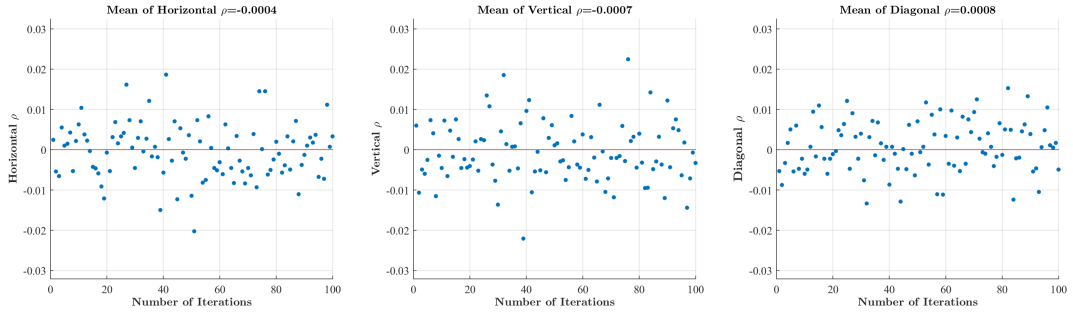
FIGURE 5.9 – Correlation in adjacent pixels in original Lenna : (a) horizontally, (b) vertically and (c) diagonally.
Correlation in adjacent pixels in fragmented Lenna :(d) horizontally, (e) vertically and (f) diagonally.

According to the obtained results, the proposed encryption-fragmentation algorithm ensures a low correlation since the obtained coefficient correlation of adjacent pixels is always close to zero for the different directions. This confirms that no detectable correlation exists in the adjacent pixels of the fragments parts. Therefore, the proposed scheme results in encrypted-fragmented images with a high level of randomness.



(a) (b) (c) (d) (e) (f)

FIGURE 5.10 – Correlation in adjacent pixels in original Pepper :(a) horizontally, (b) vertically and (c) diagonally.
Correlation in adjacent pixels in one fragmented Pepper image : (d) horizontally, (e) vertically and (f) diagonally.



(a) (b) (c)

FIGURE 5.11 – Variation of the correlation coefficient in adjacent pixels in one fragmented Pepper image : (a) horizontally, (b) vertically and (c) diagonally.

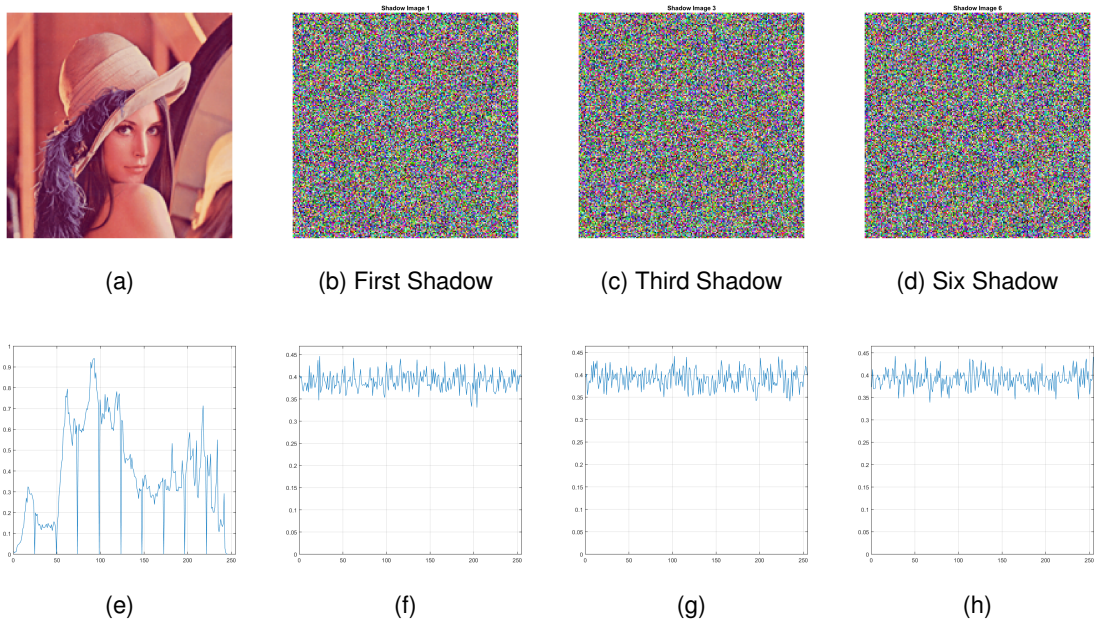
TABLE 5.2 – The average Correlation coefficient r_{xy} of the encrypted fragmented image under the proposed approach

Encrypted Images	Statistical tests		
	Horizontal	Vertical	Diagonal
Lena	0.0029	0.0014	-0.0017
Pepper	-0.0290	-0.0254	-0.0094
Baboon	-0.0134	0.0348	-0.0091
Boat	0.0280	0.0083	-0.0001
Cameraman	-0.0205	-0.0232	0.0030
Fruits	-0.0209	0.0042	-0.0008
Goldhill	-0.0111	0.0147	-0.0122

5.6.2/ UNIFORMITY ANALYSIS

To measure the uniformity of encrypted-fragmented data, both the probability density function (PDF) and entropy tests are applied. To resist the common statistical attacks, the fragmented image should have a uniform PDF in addition to a high level of randomness. The PDF of two original plain-images and their corresponding encrypted-fragmented images are shown in figures 5.12, 5.13. It can be observed that the PDF of the pro-

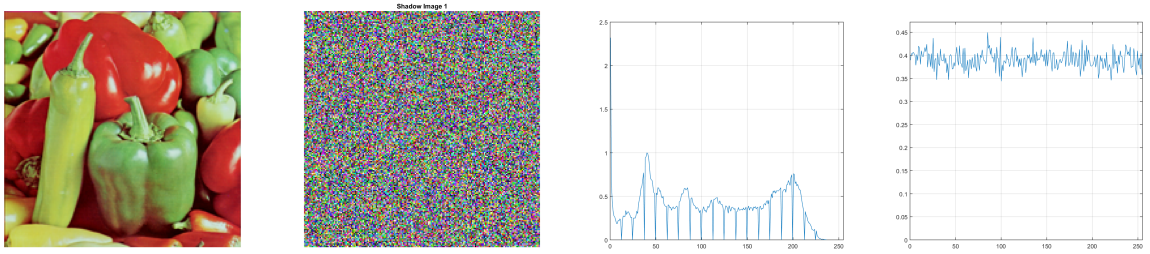
duced encrypted sub-images is close to a uniform distribution, which is $\frac{1}{256}$.



(a) (b) First Shadow (c) Third Shadow (d) Six Shadow

(e) (f) (g) (h)

FIGURE 5.12 – (a) Original Lenna, (b) First Shadow of Lenna image,(c) third Shadow of Lenna image,(d) six Shadow of Lenna image, and (e)-(h) its corresponding (e)-(h) PDF, respectively.



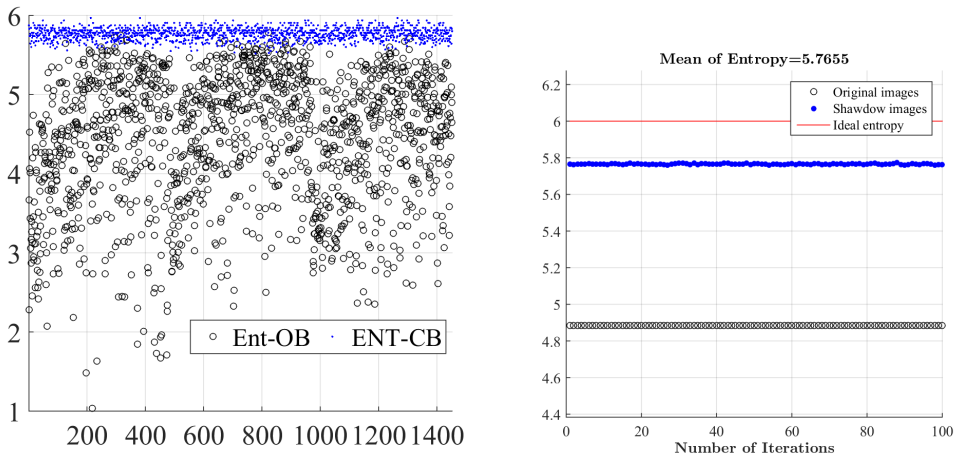
(a) (b) (c) (d)

FIGURE 5.13 – (a) Original Pepper, (b) First shadow of pepper image, and its corresponding (c)-(d) PDF, respectively.

To validate this result at the sub-matrix level, an entropy test is performed.

The entropy analysis for the sub-matrices of the original and encrypted-fragmented Lenna images for $h = 4, 8$ are shown in FIGURE 5.14.

The results indicate that the encrypted fragmented sub-matrices have an entropy always close to the desired value, which is 4, 6 and 8 in case of $h = 4$, $h = 8$ and $h = 16$, respectively. TABLE 5.3 shows the values obtained from the entropy analysis. Therefore, the proposed encryption-fragmentation algorithm is sufficiently secure against statistical attacks.



(a) (b)

FIGURE 5.14 – The Entropy analysis for the sub-matrices of original and first shadow Lena image a) under the use of a random dynamic key for $h = 8$ and b) the average of entropy versus 100 random keys.

TABLE 5.3 – Entropy Statistical Tests

Statistical Tests					
		Min	Mean	Max	Std
h=4	$H(m)$	0	3.1625	4.0000	0.5014
	$H(C)$	3.3750	3.9421	4	0.0828
h=8	$H(m)$	2.1823	4.2014	5.7813	0.7991
	$H(C)$	5.4452	5.7653	5.9688	0.0754
h=16	$H(m)$	2.7235	4.9910	6.8398	0.9624
	$H(C)$	7.0386	7.1754	7.3299	0.0514

According to the obtained results, the proposed encryption-fragmentation algorithm ensures a low correlation since the obtained correlation coefficient is always close to zero for the different shadow images as shown in FIGURE 5.15. This demonstrates that no detectable correlation exists between the original and the fragment parts and consequently ensures the independence at the level of fragments. Note that the original image is resized to the size of the shadow image in this test.

5.6.3/ INDEPENDENCE

Fragmented-encrypted images should be very different from the original ones, and their inter-correlation should be very low.

5.6.3.1/ INDEPENDENCE AMONG SHADOW IMAGES

In FIGURE 5.16-a), the correlation coefficient among 8 different fragments is presented in table-view. The results demonstrate a low correlation between the different fragments,

which reveals the dissimilarity between the fragments shadow images.

5.6.3.2/ DIFFERENCE TEST

This test is performed to calculate the percentage of difference at the bit level between the original and the fragmented data. More importantly, the difference test should be applied also among the fragmented parts. A secure fragmentation algorithm should ensure a difference percentage at the bit level close to 50% between the fragmented and the original parts. We can see in Figure 5.17-a) that the proposed method achieves 49.936% as difference between the original and the fragmented data. Similarly, it is also required to have up to 50% difference in bits among the fragmented parts. In addition, the average difference (without the diagonal part) at the bit level between each couple of the fragmented and the original data is calculated for 10,000 times and shown in Figure 5.17-b). A careful examination of the results indicates that the obtained value is close to the ideal one, and the mean value is close to 50% with a low standard deviation equal to 0.3095. Consequently, the proposed fragmentation algorithm ensures the required level of difference between the original and the fragmented data. In addition, FIGURE 5.16-b) shows the difference percentage for the different couples of the fragmented images and the obtained values are very close to 50%.

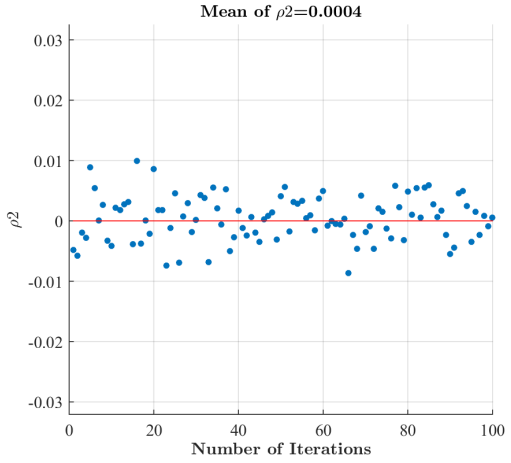


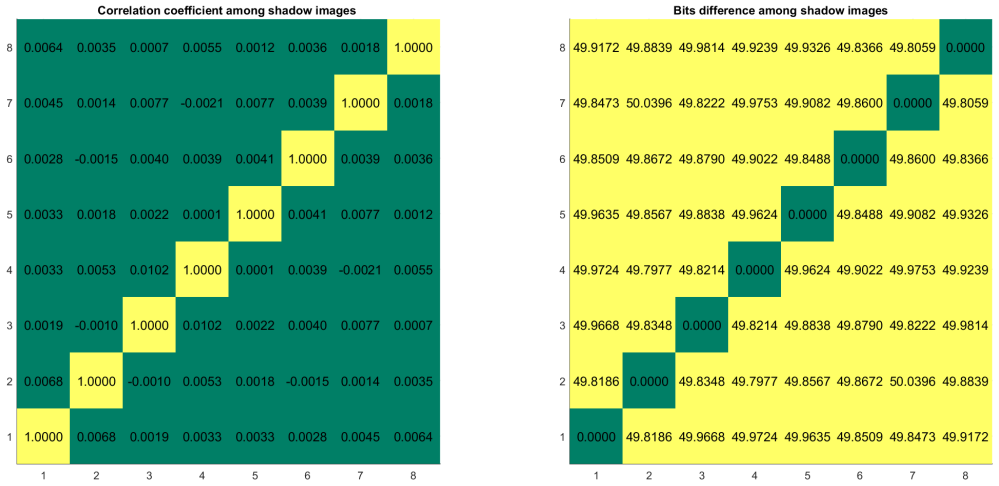
FIGURE 5.15 – Variation of the correlation coefficient between original and encrypted-fragments (shadow) imges.

5.6.4/ SENSITIVITY TEST

TABLE 5.4 – Statistical Results of sensitivity

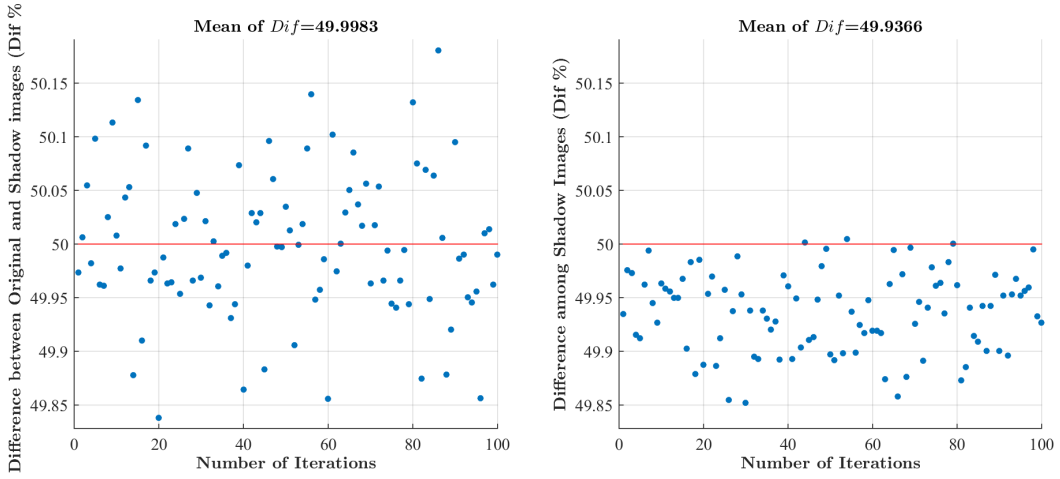
Statistical results				
	Min	Mean	Max	Std
Dif	49.8676	49.9791	50.1109	0.0360
KS	49.8706	49.9770	50.1031	0.0338

Differential attacks are based on studying the relation between fragmented images obtained with a slight change in the encryption key. Usually, a change of one bit in the



(a)

FIGURE 5.16 – Variation of the coefficient correlation among 8 different fragments (a) and its corresponding bit difference (b) for a Lenna standard image with a random dynamic key.

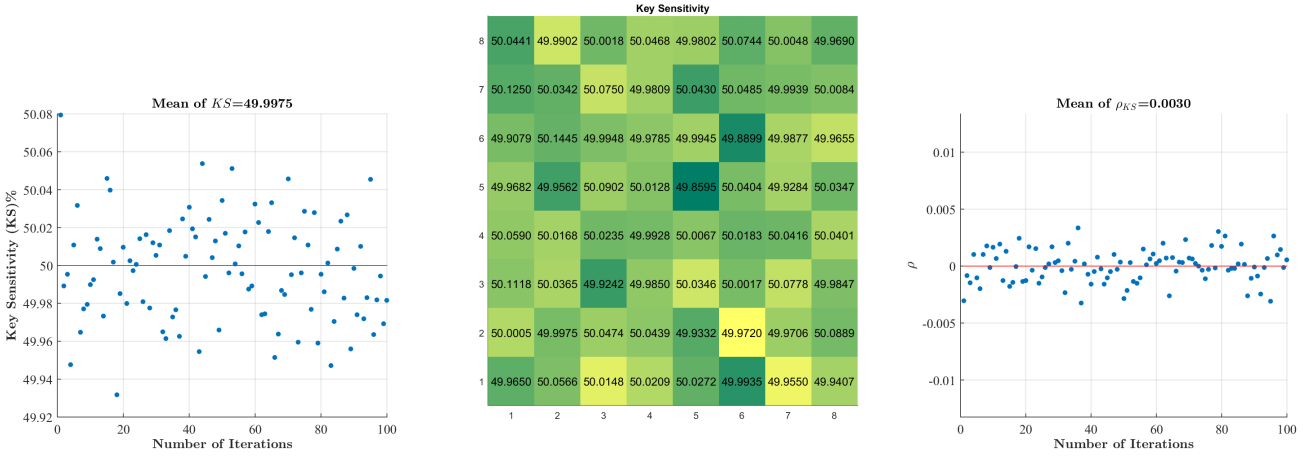


(a) Difference between original and fragment parts (b) Difference between Shadow fragments

FIGURE 5.17 – Difference between plain Lenna and shadow Lena (a) for 100 random keys and difference

original dynamic key should produce different encrypted fragmented sub-images since different cryptographic primitives are being produced. A sensitivity test shows how much a slight change in the key will affect the resulted fragmented encrypted images. In other words, the higher the data fragments change with a slight change of the dynamic key, the better the sensitivity of the fragmentation algorithm is. Below we analyze different types of sensitivity.

The **Plain-text Sensitivity** is not considered since the cryptographic primitives are



(a) (b) (c)

FIGURE 5.18 – key sensitivity against 1000 random dynamic keys (a) and among shadow images for a random key (b).

re-generated for each new session and they are updated for each new input image. Consequently, this results in totally different fragment (shadow) images for the same original image. Therefore, the proposed solution successfully satisfies the avalanche effect, but in a different manner based on the use of the dynamic key-dependent fragmentation-encryption approach.

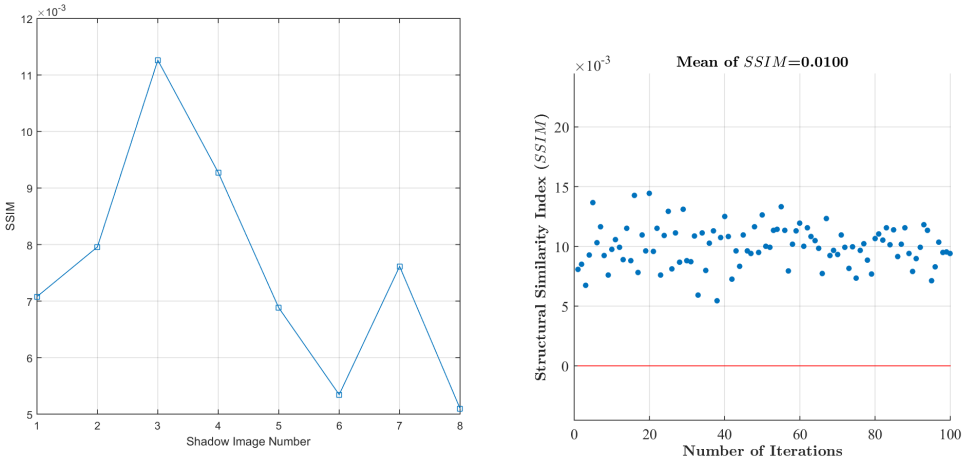
Concerning the **key Sensitivity** test, it is one of the most important tests and it quantifies the sensitivity against any slight change(s) introduced to the key. This test is realized to compute the percentage of change in the fragmented images due to a slight change in the secret key or nonce. The fragmentation algorithm should ensure a percentage of sensitivity close to 50% to be considered secure.

In FIGURE 5.18-a), the KS test is done for 100 iterations ; the mean value is close to 50% with a low standard deviation equals to 0.3128, which means that the proposed fragmentation algorithm achieves the required key sensitivity level, which can consequently ensure a high resistance degree against different attack types.

5.6.5/ VISUAL DEGRADATION

In this context, $SSIM$ was computed considering the original and the fragmented Lena image for $1,000$ pseudo-random seeds and the results are presented in FIGURE 5.19 and TABLE 5.5. As shown, the $SSIM$ value has a maximum value of 0.0414, which means that a high and hard visual distortion is achieved using the proposed fragmentation-encryption scheme. This validates that the proposed encryption technique provides a high difference between the original and the shadow images. As a conclusion, the proposed fragmented-encryption scheme gives a sufficient visual degradation such that no useful information could be revealed about the original image from the fragmented ones.

In addition, let us indicate that the original image is re-sized also in this test to the size of the shadow image.



(a) (b)

FIGURE 5.19 – $SSIM$ variation between the original and the fragmented Lenna image for one key (a). In addition, the average of $SSIM$ (b) versus 100 random key with $k = 8$.

TABLE 5.5 – Statistical Results of visual degradation

Statistical results				
	Min	Mean	Max	Std
SSIM(K=4)	7.8744	8.315	8.4241	0.0421
SSIM (k=8)	0.0297	0.0359	0.0414	0.0019

5.7/ CRYPTANALYSIS DISCUSSION

The cryptographic strength of the proposed solution relies on the use of the dynamic key approach, and on the use of different cryptographic primitives in a pseudo-random manner. A complete knowledge of the fragments of a certain image does not permit the recovery of previous nor future data since for each input image, new cryptographic primitives are generated. In addition, the dynamic key is produced using a one-way cryptographic hash function. Therefore, the backward secrecy and forward security are ensured since each session key requires a new nonce.

Additionally, in the considered scenario, n fragments are dispersed over n different entities. Thus, the original data protection relies on the difficulty of collecting k fragments of the n dispersed ones. Indeed, an attacker needs to know the location of the fragments before accessing them. Moreover, the attacker must first guess or obtain the right order of fragments, the bank of matrices along with their corresponding order, and the encryption permutation table in order to recover the original image. In this case, the knowledge of k fragments only does not reveal any useful information to the attacker.

In the following, some of the most known attacks (statistical, differential, chosen/known plain-test, and brute-force) are discussed in a situation where k fragments have been revealed to an attacker. Additionally, the proposed fragmentation scheme is considered to be known to the attacker.

5.7.1/ STATISTICAL ATTACKS

This category of attacks exploits the fact that the encoded data may reveal some statistical properties. Therefore, in an ideal situation, the frequency analysis of data within a fragment should be indistinguishable from the output of a random generator. Previous statistical tests (entropy analysis, probability density function, correlation tests) have confirmed the robustness of the proposed against statistical attacks.

5.7.2/ BRUTE-FORCE ATTACK

The size of the secret key can be 128, 196 and 256 bits, while the size of the dynamic key is 512 bits. Therefore, the size of the secret and dynamic keys are sufficient enough to make brute force attacks unfeasible.

5.7.3/ KNOWN AND CHOSEN PLAIN/CIPHER TEXT ATTACKS

A different set of cryptographic primitives are generated and used for each input image in order to protect the data against the known or chosen plain text attack types.

5.7.4/ LINEAR AND DIFFERENTIAL ATTACKS

The dynamic cryptographic primitives are updated for each new input image, which eliminates any similarity among the resulted shadow images for the same original one. Section 5.6.4 indicates clearly that high key sensitivity is reached with the proposed solution, so even a single bit change in the secret key or Nonce is sufficient to obtain different cryptographic primitives and consequently different shadows images.

Moreover, sensitivity analysis demonstrates the efficiency of the proposed cryptographic algorithm against key related attacks [Dwivedi et al., 2018] since a key derivation function is used to produce dynamic cryptographic primitives and update mechanism. These results indicate that no useful information could be detected from the fragmented shadow images where all pixels of the fragmented image are changed.

The known cryptanalytic tests, considered in the literature, have been performed, and a brief analysis of the proposed solution against several cryptanalytic attacks is provided. The proposed fragmentation-encryption algorithm is considered to be public, and the cryptanalyst has a complete knowledge of all operations, but has no knowledge about the secret key and the nonce. However, the proposed scheme is based on variable dynamic key and update mechanism for the cryptographic primitives, for every input image. Accordingly, the problem of single image failure and accidental seed disclosure is avoided by this scheme.

5.8/ PERFORMANCE ANALYSIS

The proposed approach is based on dividing the encrypted image into k fragments where the size of k has to meet the trade-off between performance and randomness levels. On

the other hand, the principal advantage of the proposed approach is that the modified IDA scheme can be performed in parallel, which leads to reduction of the execution time.

Note that, for lower value of k, less execution time is required, but less randomness is achieved, while with higher value of $k \geq 2$, the execution time increases and the degree of robustness increases. Hence, we have to select k according to the application needs. In figure 5.20, different values of n and k were used times for a file of size 256 MBytes.

The variation of execution time versus different values of n is represented as a linear function. In addition, increasing k leads to introduce more execution overhead.

5.8.1/ THEORETICAL PERFORMANCE

The required computation complexity and storage overhead of the proposed scheme with other relevant state-of-the-art works such as Shamir's secret sharing, IDAs, and AONT-RS are presented in TABLE 5.6. A precise evaluation is hard due to the variety of implementations. The cost of an IDA is the cost of multiplying data by a $n \times k$ matrix ($Matrix$). The performance of AONT depends on the chosen encryption and hash algorithms, as well as the data size. For redundant fragments, AONT uses the same technique as the proposed scheme.

Moreover, the proposed encryption scheme is based on the dynamic key-dependent approach and it requires a single round and a single operation instead of multiple rounds and operations in the case of standard ciphers such as AES. Similarly, the selected keyed hash function is also based on one round. Consequently, the required computation complexity for the data confidentiality and integrity in addition to source authentication requires less computation compared to AONT with the employed standard cryptographic algorithms.

The data is fragmented into n fragments and to $\frac{M}{k \times TB}$ blocks. In addition, a matrix multiplication operation is required for each data chunk (block). Therefore, the proposed modified IDA can strongly benefit from this parallelization since each data chunk is coded or recovered independently from the others. The fragmentation (de-fragmentation) process ensures better parallelization using a different thread for each computation compared to the original IDA.

TABLE 5.6 – *Running time and storage requirements. (w - key size, c - chunk size)*

Scheme	Running time	Storage
SSS	Poly(n,k,—M—)	$n\|M\|$
IDA	Matrix(n,k)	$\frac{n\times\|M\|}{k}$
AONT-RS	AONT(—d—) + RS(n-k,k,d)	$\frac{n\times(\|M\|+w)}{k}$
Our proposal	Matrix(n,k)/nt	$\frac{n\times\|M\|}{k}$

5.8.2/ STORAGE/COMMUNICATION OVERHEAD

The size of the produced fragments is close to the optimal value $|M|/k$. Therefore, the fragmentation procedure presented in FIGURE 5.4 does not incur any data overhead and

preserves the benefits of the original IDA. The storage overhead ($\frac{(n-k)\times|M|}{k}$) is caused only by having redundant fragments, which is inevitable for preventing data loss in case of damage or alteration, which is the case for the original IDA.

5.8.3/ PROPAGATION OF ERRORS

An important criteria for any cryptographic solution is the low error propagation property. The interference and noise in the transmission channel (or in the storage system) are the main cause of errors. A bit error refers to the substitution of '0' bit by '1' bit or vice versa. This error may propagate resulting in the destruction of data, which is a big challenge since there is a trade-off between the avalanche effect and error propagation [Massoudi et al., 2008]. In this proposal, if a bit error takes place in any of the fragmented shadow images, it will affect only its corresponding de-fragmented data block (n bytes). Therefore, error propagation is limited to the block level.

5.8.4/ EXECUTION TIMES

In the following, experiments have been performed with a C code on an Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz machine with 64GB of RAM.

In Table 5.7, the execution times of our approach are reported in two different situations. In the first columns, the size of the file is given. In columns 2 to 4, parameters k, n and the execution times are given. In fact, the number of fragments (n) is fixed and k varies from 4, 8 and 12. It can be observed that when n is fixed, the execution time does not vary significantly when k varies. In columns 5 to 7, another scenario is considered : n varies from 8, 16 and 24 and the number of fragments for the recovery (k) is equals to $1/4\times n+1$. In this case, it can be seen that when k increases the execution time also increases.

In Figure 5.20, the execution times of our algorithm are reported for a file of size 256MB. It can also be seen that when n increases, the execution time also increases. Moreover, k is not so significant since when this number is doubled, the execution time slightly increases.

It can be seen with both these experiments that this algorithm is very efficient. It allows to split files into fragments very quickly. Consequently, our solution is ready to be used with real implementations.

5.9/ CONCLUSION

In this chapter, a dynamic key-dependent cryptographic solution is presented to provide data confidentiality, integrity, availability, and message authentication for medical data. The robustness of the proposed solution is based on the dynamic key-dependent approach such that different cryptographic primitives are produced for each new input message (image in this chapter) and not only for each new session. In addition, efficiency is ensured since simple operations with a low number of rounds are required, leading to a fast execution time. Further optimization of the data availability scheme can be achieved using look-up tables instead of applying the matrix multiplication operation. In addition, the authentication-encryption scheme can be realized in parallel. Several security analysis tests were performed in order to prove the high level of security of the proposed

TABLE 5.7 – Execution times of our approach with different sizes of messages and different values of fragments for recovery and fragments.

Size	k	n	Exec. time (s)	k	n	Exec. time (s)
16KB	4	16	0.00086	3	8	0.00068
16KB	8	16	0.00096	5	16	0.00086
16KB	12	16	0.0011	7	24	0.0011
64KB	4	16	0.003	3	8	0.0019
64KB	8	16	0.003	5	16	0.003
64KB	12	16	0.0036	7	24	0.0038
256KB	4	16	0.0093	3	8	0.0047
256KB	8	16	0.011	5	16	0.0098
256KB	12	16	0.012	7	24	0.012
1MB	4	16	0.019	3	8	0.01
1MB	8	16	0.023	5	16	0.022
1MB	12	16	0.027	7	24	0.028
4MB	4	16	0.061	3	8	0.038
4MB	8	16	0.066	5	16	0.062
4MB	12	16	0.073	7	24	0.086
16MB	4	16	0.23	3	8	0.13
16MB	8	16	0.24	5	16	0.22
16MB	12	16	0.27	7	24	0.31
64MB	4	16	0.87	3	8	0.51
64MB	8	16	0.98	5	16	0.9
64MB	12	16	1.07	7	24	1.21
256GB	4	16	3.48	3	8	2.02
256GB	8	16	4.01	5	16	3.5
256GB	12	16	4.3	7	24	4.85

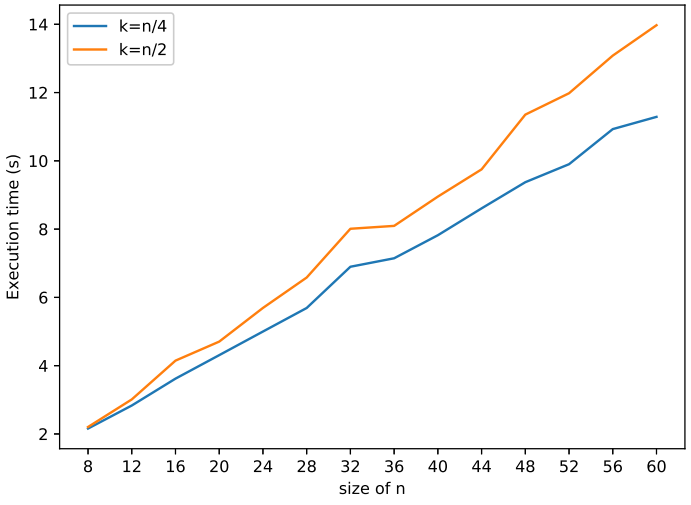


FIGURE 5.20 – Executions times for different number of fragments n for a file of size 256MB

solution. As a conclusion, due to its flexibility, high security, low computational complexity, the proposed solution can be considered as a competitive cryptographic solution for securing medical contents.

III

General Conclusion

6

CONCLUSION & PERSPECTIVES

In this thesis work, we have studied and designed efficient lightweight dynamic key dependent cryptographic primitives which are consequently used to design efficient cryptographic algorithms. Moreover, we have studied and analyzed the performance and security level of each proposed cryptographic algorithm.

In Chapter 1, we list and describe the different security issues and challenges of E-health systems and especially for the emerging medical IoT systems. In addition to the employment of different security measures in use to protect and secure the E-health system (and especially medical IoT domains) and its associated assets. Then, we have identified the main assumptions and characteristics of security and its services, and have shown the interest of lightweight security solutions towards reducing the trade-off between system performance and security level.

In Chapter 2, we analyze the characteristic of medical images. In addition, we list the different classes of encryption algorithm used to encrypt a medical image. Then, we propose a medical image cipher scheme with three variants (selective, middle-full, and full). The scheme is based on dynamic cryptographic primitives for each input image in contrast to standard cipher techniques. The round number is reduced to one without degrading the security level, which was a hard challenge before being solved in this chapter. Furthermore, in this chapter, we define a dynamic key derivation function that generates the dynamic key and consequently the required sub-keys that are used to construct the basic cipher primitives. To perform encryption/decryption, two main operations were applied at the sub-matrix level, which are sub-matrix permutation and a masking function. Then, several security analysis and system performance tests were realized to validate the credibility of the proposed medical image cipher scheme. This cipher solution can be considered as a good cipher candidate to protect medical contents.

In Chapter 3, an enhanced one-round, flexible, dynamic, key-dependent lightweight cipher scheme targeted for medical data has been presented. The proposed cipher scheme has been shown to be efficient and secure, with fast execution time compared to the first cipher scheme of chapter 2. In addition, this cipher also provides better robustness against different powerful attacks due to its different substitution and permutation primitives in addition to the two dynamic pseudo-random matrices that are generated in a dynamic manner for each new input message. Moreover, the proposed substitution and permutation primitives ensure the desirable cryptographic performance in an efficient

manner and simple hardware implementation compared to the presented ones in chapter 2. The proposed cipher scheme requires only one iteration and its corresponding round function consists of simple operations, which addresses the limitations of medical IoT multimedia devices. An extensive security analysis revealed that the proposed approach is strong enough against different kinds of attacks. Finally, the results clearly showed that the scheme outperforms the optimized AES implementation of OpenSSL, which indicates that the approach is more suitable for delay-sensitive multimedia applications.

In Chapter 4, a dynamic key dependent cryptographic solution is presented to provide data confidentiality, integrity, availability, and message authentication. In this chapter, we use dynamic key dependent byte permutation cipher scheme, which means only one round and only one operation is used instead of several operations. In addition, several optimizations of the data availability scheme are introduced such as using lookup tables instead of applying the multiplication operation. In addition, authentication-encryption and data availability schemes can be applied in parallel. Several security and performance analysis tests were performed in order to prove the high levels of security and efficiency of the proposed cryptographic solution, respectively. As a conclusion, due to its flexibility, high security,low computation complexity, this proposed solution can be considered as a competitive cryptographic solution for securing image contents.

6.1/ PERSPECTIVES

As future work, the proposed cipher can be further optimized via an assembly optimization to achieve a better reduction in delay and required resources. Additionally, the proposed cipher scheme should be adapted to be a post-crypto-compression scheme to ensure format compliance.

This means that we will adapt the previous one round cipher solution to be applied to the compressed medical images. It is interesting to encrypt a compressed image because in that case, the size of data to encrypt is reduced. In addition, this cipher should ensure the format compliant property to preserve that the encrypted image can be decoded. Let us also indicate that this variant can also be selective and 5% of compressed medical data are required to reach a hard visual degradation.

In addition, we like to define a new lightweight one round message authentication algorithm for medical images (selective or full) to ensure data integrity and source authentication security services. The proposed solution should be based on a keyed hash function that can reach the required desirable cryptographic performance (such as plaintext and key sensitivity and strong collision resistance) with only one round to reduce the required overhead in terms of latency and resources.

Although, we plan to define a new watermarking algorithm for medical contents that can help to ensure source authentication and data integrity in an efficient manner. Additionally, the design of a multi-factor device/user authentication scheme is mandatory to reinforce the control access and it can be one of the main perspective points.

Finally, we like to add all the proposed solutions in telemedicine applications.

BIBLIOGRAPHIE

[nat, 2004] (2004). **Digital imaging and communications in medicine (DICOM) Part 15 : Security and System Management Profiles.** National Electrical Manufacturers Association and American College of Radiology.

[10P, 2017] (2017). **10 pieces of medical equipment all hospitals need**. https://www.futurehealthconcepts.com/blog/posts/10-pieces-of-medical-equipment-all-hospitals-need.html.

[Bio, 2019] (2019). **Biomedical equipment list - medshare**. https://www.medshare.org/biomedical-equipment/.

[Abdmouleh et al., 2013] Abdmouleh, M. K., Khalfallah, A., et Bouhlel, M. S. (2013). **Dynamic chaotic look-up table for mri medical image encryption**. Dans *the International Conference On Systems, Control, Signal Processing And Informatics (SCSI 2013)*, pages 16–19.

[Abera et al., 2016] Abera, T., Asokan, N., Davi, L., Ekberg, J.-E., Nyman, T., Paverd, A., Sadeghi, A.-R., et Tsudik, G. (2016). **C-flat : control-flow attestation for embedded systems software**. Dans *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 743–754. ACM.

[Adams et al., 1989] Adams, C., et Tavares, S. (1989). **Good s-boxes are easy to find**. Dans *Conference on the Theory and Application of Cryptology*, pages 612–615. Springer.

[Adhikary et al., 2019] Adhikary, T., Jana, A. D., Chakrabarty, A., et Jana, S. K. (2019). **The internet of things (iot) augmentation in healthcare : An application analytics**. Dans *International Conference on Intelligent Computing and Communication Technologies*, pages 576–583. Springer.

[Adrianto et al., 2015] Adrianto, D., et Lin, F. J. (2015). **Analysis of security protocols and corresponding cipher suites in etsi m2m standards**. Dans *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*, pages 777–782. IEEE.

[Aggidis et al., 2015] Aggidis, A. G., Newman, J. D., et Aggidis, G. A. (2015). **Investigating pipeline and state of the art blood glucose biosensors to formulate next steps**. *Biosensors and Bioelectronics*, 74 :243–262.

[Agrawal, 2018] Agrawal, P. (2018). **Artificial intelligence in drug discovery and development**. *Journal of Pharmacovigilance*, 6 :1–2.

[Agrawal et al., 2000] Agrawal, R., et Srikant, R. (2000). **Privacy-preserving data mining**, volume 29. ACM.

[Ahmed et al., 2017] Ahmed, M., et Ullah, A. S. B. (2017). **False data injection attacks in healthcare**. Dans *Australasian Conference on Data Mining*, pages 192–202. Springer.

[Al-Ani et al., 2013] Al-Ani, M. S., et Rajab, M. A. (2013). **Biometrics hand geometry using discrete cosine transform (dct)**. *Science and Technology*, 3(4) :112–117.

[Alemzadeh et al., 2016] Alemzadeh, H., Chen, D., Li, X., Kesavadas, T., Kalbarczyk, Z. T., et Iyer, R. K. (2016). **Targeted attacks on teleoperated surgical robots : Dynamic model-based detection and mitigation**. Dans *Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on*, pages 395–406. IEEE.

[Ali et al., 2015] Ali, S., et Cherif, A. (2015). **Performances analysis of image encryption for medical applications**. *Journal of Information Sciences and Computing Technologies*, 1(1) :78–87.

[Alliance, 2010] Alliance, W.-F. (2010). **Wi-fi certified wi-fi direct**. *White paper*.

[Almohri et al., 2017] Almohri, H., Cheng, L., Yao, D., et Alemzadeh, H. (2017). **On threat modeling and mitigation of medical cyber-physical systems**. Dans *Connected Health : Applications, Systems and Engineering Technologies (CHASE), 2017 IEEE/ACM International Conference on*, pages 114–119. IEEE.

[Alperovitch et al., 2011] Alperovitch, D., et others (2011). **Revealed : operation shady RAT**, volume 3. McAfee.

[Alvarez et al., 2009] Alvarez, G., et Li, S. (2009). **Cryptanalyzing a nonlinear chaotic algorithm (nca) for image encryption**. *Communications in Nonlinear Science and Numerical Simulation*, 14(11) :3743–3749.

[Amin et al., 2017] Amin, R., Islam, S. H., Vijayakumar, P., Khan, M. K., et Chang, V. (2017). **A robust and efficient bilinear pairing based mutual authentication and session key verification over insecure communication**. *Multimedia Tools and Applications*, pages 1–26.

[Anderson et al., 2016] Anderson, K., Burford, O., et Emmerton, L. (2016). **Mobile health apps to facilitate self-care : a qualitative study of user experiences**. *PLoS One*, 11(5) :e0156164.

[Anirudh et al., 2017] Anirudh, M., Thileeban, S. A., et Nallathambi, D. J. (2017). **Use of honeypots for mitigating dos attacks targeted on iot networks**. Dans *Computer, Communication and Signal Processing (ICCCSP), 2017 International Conference on*, pages 1–4. IEEE.

[Ankaralı et al., 2015] Ankaralı, Z. E., Demir, A. F., Qaraqe, M., Abbasi, Q. H., Serpedin, E., Arslan, H., et Gitlin, R. D. (2015). **Physical layer security for wireless implantable medical devices**. Dans *Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2015 IEEE 20th International Workshop on*, pages 144–147. IEEE.

[Anonymized, 2016] Anonymized (2016). **Poster : A keyless efficient algorithm for data protection by means of fragmentation**. Dans *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 1745–1747, New York, NY, USA. ACM.

[Arroyo et al., 2009] Arroyo, D., Li, C., Li, S., Alvarez, G., et Halang, W. A. (2009). **Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm**. *Chaos, Solitons & Fractals*, 41(5) :2613–2616.

[Ashtiyani et al., 2008] Ashtiyani, M., Birgani, P. M., et Hosseini, H. M. (2008). **Chaos-based medical image encryption using symmetric cryptography**. Dans *Information and Communication Technologies : From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, pages 1–5. IEEE.

[Asmar, 2017] Asmar, R. (2017). **Validation of the automatic blood pressure measurements device, the omron evolv (hem-7600 te)® in pregnancy according to the modified european society of hypertension international protocol (esh-ip).**

[Atzori et al., 2010] Atzori, L., Iera, A., et Morabito, G. (2010). **The Internet of Things : A survey**. *Computer networks*, 54(15) :2787–2805.

[Ayala, 2016] Ayala, L. (2016). **Active medical device cyber-attacks**. Dans *Cybersecurity for Hospitals and Healthcare Facilities*, pages 19–37. Springer.

[Babel et al., 2012] Babel, M., Pasteau, F., Strauss, C., Pelcat, M., Bédat, L., Blestel, M., et Déforges, O. (2012). **Preserving data integrity of encoded medical images : the lar compression framework**. Dans *Advances in Reasoning-Based Image Processing Intelligent Systems*, pages 91–125. Springer.

[Bagnall et al., 1999] Bagnall, P., Briscoe, R., et Poppitt, A. (1999). **Taxonomy of communication requirements for large-scale multicast applications**. Rapport technique.

[Baig et al., 2013] Baig, Z. A., et Amoudi, A.-R. (2013). **An analysis of smart grid attacks and countermeasures**. *Journal of Communications*, 8(8) :473–479.

[Balandina et al., 2015] Balandina, E., Balandin, S., Koucheryavy, Y., et Mouromtsev, D. (2015). **Iot use cases in healthcare and tourism**. Dans *Business Informatics (CBI), 2015 IEEE 17th Conference on*, volume 2, pages 37–44. IEEE.

[Balian et al., 2019] Balian, S., McGovern, S. K., Abella, B. S., Blewer, A. L., et Leary, M. (2019). **Feasibility of an augmented reality cardiopulmonary resuscitation training system for health care providers**. *Heliyon*, 5(8) :e02205.

[Bandy et al., 2013] Bandy, W. R., Jamieson, B. G., Powell, K. J., Salsman, K. E., Schober, R. C., Weitzner, J., et Arneson, M. R. (2013). **Ingestible endoscopic optical scanning device**. US Patent 8,529,441.

[Baptista, 1998] Baptista, M. (1998). **Cryptography with chaos**. *Physics Letters A*, 240(1) :50–54.

[Barker et al., 2012] Barker, E., et Kelsey, J. (2012). **Recommendation for Random Number Generation Using Deterministic Random Bit Generators**. *NIST Special Publication*, 800 :90A.

[Barker et al., 2011] Barker, E. B., et Kelsey, J. M. (2011). **Recommendation for random number generation using deterministic random bit generators (revised)**. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory.

[Beasley, 2012] Beasley, R. A. (2012). **Medical robots : current systems and research directions**. *Journal of Robotics*, 2012.

[Beaulieu et al., 2015] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., et Wingers, L. (2015). **Simon and speck : Block ciphers for the internet of things.** *IACR Cryptology ePrint Archive*, 2015 :585.

[Bellare et al., 2004] Bellare, M., et Kohno, T. (2004). **Hash function balance and its impact on birthday attacks**. Dans *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 401–418. Springer.

[Bernstein et al., 2014] Bernstein, D. J., Van Gastel, B., Janssen, W., Lange, T., Schwabe, P., et Smetsers, S. (2014). **Tweetnacl : A crypto library in 100 tweets**. Dans *International Conference on Cryptology and Information Security in Latin America*, pages 64–83. Springer.

[Bhagwat, 2001] Bhagwat, P. (2001). **Bluetooth : technology for short-range wireless apps**. *IEEE Internet Computing*, 5(3) :96–103.

[Biham et al., 2012] Biham, E., et Shamir, A. (2012). **Differential cryptanalysis of the data encryption standard**. Springer Science & Business Media.

[Birkmeyer et al., 2003] Birkmeyer, J. D., Stukel, T. A., Siewers, A. E., Goodney, P. P., Wennberg, D. E., et Lucas, F. L. (2003). **Surgeon volume and operative mortality in the united states**. *New England Journal of Medicine*, 349(22) :2117–2127.

[Blakley, 1899] Blakley, G. (1899). **Safeguarding cryptographic keys**. Dans *afips*, page 313. IEEE.

[Bogdanoski et al., 2013] Bogdanoski, M., Suminoski, T., et Risteski, A. (2013). **Analysis of the syn flood dos attack**. *International Journal of Computer Network and Information Security (IJCNIS)*, 5(8) :1–11.

[Borghoff et al., 2012] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., Leander, G., Nikov, V., Paar, C., Rechberger, C., et others (2012). **Prince–a low-latency block cipher for pervasive computing applications**. Dans *Advances in Cryptology–ASIACRYPT 2012*, pages 208–225. Springer.

[Boriga et al., 2014] Boriga, R., Dăscălescu, A. C., et Priescu, I. (2014). **A new hyperchaotic map and its application in an image encryption scheme**. *Signal Processing : Image Communication*, 29(8) :887 – 901.

[Brahimi et al., 2008] Brahimi, Z., Bessalah, H., Tarabet, A., Kholladi, M., et others (2008). **Selective encryption techniques of jpeg2000 codestream for medical images transmission**. *WSEAS Transactions on Circuits and Systems*, 7(7) :718–727.

[Bruckmann et al., 2000] Bruckmann, A., et Uhl, A. (2000). **Selective medical image compression techniques for telemedical and archiving applications**. *Computers in Biology and Medicine*, 30(3) :153–169.

[Buhrow et al., 2014] Buhrow, B., Riemer, P., Shea, M., Gilbert, B., et Daniel, E. (2014). **Block cipher speed and energy efficiency records on the msp430 : System design trade-offs for 16-bit embedded applications**. Dans *International Conference on Cryptology and Information Security in Latin America*, pages 104–123. Springer.

[Challoner et al., 2019] Challoner, A., et Popescu, G. H. (2019). **Intelligent sensing technology, smart healthcare services, and internet of medical things-based diagnosis**. *American Journal of Medical Research*, 6(1) :13–18.

[Chandrasekhar et al., 2008] Chandrasekhar, V., Andrews, J. G., et Gatherer, A. (2008). **Femtocell networks : a survey**. *IEEE Communications magazine*, 46(9).

[Chang, 2017] Chang, V. (2017). **Data analytics and visualization for inspecting cancers and genes**. *Multimedia Tools and Applications*, pages 1–15.

[Chen et al., 2016] Chen, D. D., Woo, M., Brumley, D., et Egele, M. (2016). **Towards automated dynamic analysis for linux-based embedded firmware.** Dans *NDSS*.

[Chen et al., 2015] Chen, L., et Wang, S. (2015). **Differential cryptanalysis of a medical image cryptosystem with multiple rounds**. *Computers in biology and medicine*, 65 :69–75.

[Chen et al., 2010] Chen, T.-H., et Shih, W.-K. (2010). **A robust mutual authentication protocol for wireless sensor networks**. *ETRI journal*, 32(5) :704–712.

[Cheung et al., 2007] Cheung, S., Dutertre, B., Fong, M., Lindqvist, U., Skinner, K., et Valdes, A. (2007). **Using model-based intrusion detection for scada networks**. Dans *Proceedings of the SCADA security scientific symposium*, volume 46, pages 1–12. Citeseer.

[Cho et al., 2011] Cho, J.-S., Yeo, S.-S., et Kim, S. K. (2011). **Securing against brute-force attack : A hash-based rfid mutual authentication protocol using a secret value**. *Computer Communications*, 34(3) :391–397.

[Cimato et al., 2017] Cimato, S., et Yang, C.-N. (2017). **Visual cryptography and secret image sharing**. CRC press.

[Cincilla et al., 2015] Cincilla, P., Boudguiga, A., Hadji, M., et Kaiser, A. (2015). **Light blind : Why encrypt if you can share ?** Dans *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*, volume 04, pages 361–368.

[Clark et al., 1992] Clark, D. D., Shenker, S., et Zhang, L. (1992). **Supporting real-time applications in an integrated services packet network : Architecture and mechanism**. Dans *ACM SIGCOMM Computer Communication Review*, volume 22, pages 14–26. ACM.

[Clark et al., 2017] Clark, G. W., Doran, M. V., et Andel, T. R. (2017). **Cybersecurity issues in robotics**. Dans *Cognitive and Computational Aspects of Situation Management (CogSIMA), 2017 IEEE Conference on*, pages 1–5. IEEE.

[Clark et al., 1996] Clark, J., et Jacob, J. (1996). **Attacking authentication protocols**. *High Integrity Systems*, 1 :465–474.

[Coleman et al., 2012] Coleman, D. D., et Westcott, D. A. (2012). **Cwna : certified wireless network administrator official study guide : exam Pw0-105**. John Wiley & Sons.

[Cooke et al., 2005] Cooke, E., Jahanian, F., et McPherson, D. (2005). **The zombie roundup : Understanding, detecting, and disrupting botnets.** *SRUTI*, 5 :6–6.

[Council et al., 2010] Council, N. R., et others (2010). **The role of human factors in home health care : Workshop summary**. National Academies Press.

[Coventry et al., 2018] Coventry, L., et Branley, D. (2018). **Cybersecurity in healthcare : A narrative review of trends, threats and ways forward**. *Maturitas*, 113 :48–52.

[Cullin et al., 2019] Cullin, P., et Bergdahl, T. (2019). **A telecare system**. US Patent App. 16/310,127.

[Daemen et al., 2002a] Daemen, J., et Rijmen, V. (2002a). **The Design of Rijndael : AES - The Advanced Encryption Standard**. Springer Verlag, Berlin, Heidelberg, New York.

[Daemen et al., 2002b] Daemen, J., et Rijmen, V. (2002b). **The design of Rijndael : AES-the advanced encryption standard**. Springer Science & Business Media.

[Daemen et al., 2013] Daemen, J., et Rijmen, V. (2013). **The design of Rijndael : AES-the advanced encryption standard**. Springer Science & Business Media.

[Dai et al., 2012] Dai, Y., et Wang, X. (2012). **Medical image encryption based on a composition of logistic maps and chebyshev maps**. Dans *Information and Automation (ICIA), 2012 International Conference on*, pages 210–214. IEEE.

[Decker, 2007] Decker, C. (2007). **Cyber crime 2.0 : An argument to update the united states criminal code to reflect the changing nature of cyber crime**. *S. Cal. L. Rev.*, 81 :959.

[Dhem et al., 1998] Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestré, P., Quisquater, J.-J., et Willems, J.-L. (1998). **A practical implementation of the timing attack**. Dans *International Conference on Smart Card Research and Advanced Applications*, pages 167–182. Springer.

[Doppler et al., 2009] Doppler, K., Rinne, M., Wijting, C., Ribeiro, C. B., et Hugl, K. (2009). **Device-to-device communication as an underlay to lte-advanced networks**. *IEEE Communications Magazine*, 47(12).

[Douglas et al., 2018] Douglas, M., Bailey, K., Leeney, M., et Curran, K. (2018). **An overview of steganography techniques applied to the protection of biometric data**. *Multimedia Tools and Applications*, 77(13) :17333–17373.

[Dowling et al., 2017] Dowling, S., Schukat, M., et Melvin, H. (2017). **A zigbee honeypot to assess iot cyberattack behaviour**. Dans *Signals and Systems Conference (ISSC), 2017 28th Irish*, pages 1–6. IEEE.

[Dwivedi et al., 2018] Dwivedi, A. D., Morawiecki, P., Singh, R., et Dhar, S. (2018). **Differential-linear and related key cryptanalysis of round-reduced scream**. *Information Processing Letters*, 136 :5–8.

[Dworkin, 2001] Dworkin, M. (2001). **Recommendation for block cipher modes of operation. methods and techniques**. Rapport technique, DTIC Document.

[Dworkin et al., 2001] Dworkin, M., Dworkin, M., Gallagher, P. D., et f, D. N. S. P. (2001). **Recommendation for block cipher modes of operation : Methods and techniques**.

[El Assad et al., 2016] El Assad, S., et Farajallah, M. (2016). **A new chaos-based image encryption system**. *Signal Processing : Image Communication*, 41 :144–157.

[ElGamal, 1985] ElGamal, T. (1985). **A public key cryptosystem and a signature scheme based on discrete logarithms**. Dans *Advances in Cryptology*, pages 10–18. Springer.

[Emanuel et al., 2012] Emanuel, E., Tanden, N., Altman, S., Armstrong, S., Berwick, D., de Brantes, F., Calsyn, M., Chernew, M., Colmers, J., Cutler, D., et others (2012). **A systemic approach to containing health care spending**.

[Engstrom, 2018] Engstrom, J. (2018). **Systems confrontation and system destruction warfare**. *RR1708, Rand Corporation*.

[Evans-Pughe, 2003] Evans-Pughe, C. (2003). **Bzzzz zzz [ZigBee wireless standard]**. *IEE Review*, 49(3) :28–31.

[Fabre et al., 1994] Fabre, J.-C., Deswarte, Y., et Randell, B. (1994). **Designing secure and reliable applications using fragmentation-redundancy-scattering : an object-oriented approach**, pages 21–38. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Falliere et al., 2011] Falliere, N., Murchu, L. O., et Chien, E. (2011). **W32. stuxnet dossier**. *White paper, Symantec Corp., Security Response*, 5(6) :29.

[Farringer, 2016] Farringer, D. R. (2016). **Send us the bitcoin or patients will die : addressing the risks of ransomware attacks on hospitals**. *Seattle UL Rev.*, 40 :937.

[Fawaz et al., 2016] Fawaz, Z., Noura, H., et Mostefaoui, A. (2016). **An efficient and secure cipher scheme for images confidentiality preservation**. *Signal Processing : Image Communication*, 42 :90–108.

[Felix et al., 1987] Felix, J., et Hauck, C. (1987). **System security : a hacker's perspective**. *Interex Proceedings*, 1 :6–6.

[Ferrag et al., 2017] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., et Shu, L. (2017). **Authentication protocols for internet of things : a comprehensive survey**. *Security and Communication Networks*, 2017.

[Ferraiolo et al., 2001] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., et Chandramouli, R. (2001). **Proposed nist standard for role-based access control**. *ACM Transactions on Information and System Security (TISSEC)*, 4(3) :224–274.

[Flayh et al., 2009] Flayh, N. A., Parveen, R., et Ahson, S. I. (2009). **Wavelet based partial image encryption**. Dans *Multimedia, Signal Processing and Communication Technologies, 2009. IMPACT'09. International*, pages 32–35. IEEE.

[Fornazin et al., 2008] Fornazin, M., Netto Jr, D. B., Cavenaghi, M. A., et Marana, A. N. (2008). **Protecting medical images with biometric information**. Dans *Advances in Computer and Information Sciences and Engineering*, pages 284–289. Springer.

[Fournette III, 2018] Fournette III, A. (2018). **A Guide to Inform of the Best Practices for Protection against Ransomware**. PhD thesis, Utica College.

[Francillon et al., 2008] Francillon, A., et Castelluccia, C. (2008). **Code injection attacks on harvard-architecture devices**. Dans *Proceedings of the 15th ACM conference on Computer and communications security*, pages 15–26. ACM.

[Fruhlinger, 2017] Fruhlinger, J. (2017). **What is wannacry ransomware, how does it infect, and who was responsible**.

[Frumento et al., 2016] Frumento, E., et Freschi, F. (2016). **How the evolution of workforces influences cybercrime strategies : The example of healthcare**. Dans *Combatting Cybercrime and Cyberterrorism*, pages 237–258. Springer.

[Fu et al., 2015] Fu, C., Lin, Y., Jiang, H.-y., et Ma, H.-f. (2015). **Medical image protection using hyperchaos-based encryption**. Dans *Medical Information and Communication Technology (ISMICT), 2015 9th International Symposium on*, pages 103–107. IEEE.

[Gentry, 2009] Gentry, C. (2009). **Fully homomorphic encryption using ideal lattices. proceedings of the 41st annual acm symposium on symposium on theory of computing-stoc'09. vol. 9**.

[George, 2012] George, J. P. (2012). **Development of efficient biometric recognition algorithms based on fingerprint and face**. PhD thesis, Christ University.

[Ghebleh et al., 2014] Ghebleh, M., Kanso, A., et Noura, H. (2014). **An image encryption scheme based on irregularly decimated chaotic maps**. *Signal Processing : Image Communication*, 29(5) :618–627.

[Gope et al., 2016] Gope, P., Hwang, T., et others (2016). **A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks.** *IEEE Trans. Industrial Electronics*, 63(11) :7124–7132.

[Goyal et al., 2006] Goyal, V., Pandey, O., Sahai, A., et Waters, B. (2006). **Attribute-based encryption for fine-grained access control of encrypted data**. Dans *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98. Acm.

[Granjal et al., 2015] Granjal, J., Monteiro, E., et Silva, J. S. (2015). **Security for the internet of things : a survey of existing protocols and open research issues**. *IEEE Communications Surveys & Tutorials*, 17(3) :1294–1312.

[Griffin et al., 2008] Griffin, S. E., et Rackley, C. C. (2008). **Vishing**. Dans *Proceedings of the 5th annual conference on Information security curriculum development*, pages 33–35. ACM.

[Grover et al., 2014] Grover, K., Lim, A., et Yang, Q. (2014). **Jamming and anti-jamming techniques in wireless networks : a survey**. *International Journal of Ad Hoc and Ubiquitous Computing*, 17(4) :197–215.

[Grunwald, 2006] Grunwald, L. (2006). **New attacks against rfid-systems**. *GmbH Germany*.

[Gueron, 2009] Gueron, S. (2009). **Intel's new aes instructions for enhanced performance and security.** Dans *FSE*, volume 5665, pages 51–66. Springer.

[Guo et al., 2012] Guo, C., Chang, C.-C., et Qin, C. (2012). **A hierarchical threshold secret image sharing**. *Pattern Recognition Letters*, 33(1) :83–91.

[Guo et al., 2011] Guo, J., Peyrin, T., Poschmann, A., et Robshaw, M. (2011). **The LED block cipher**. Dans *Cryptographic Hardware and Embedded Systems–CHES 2011*, pages 326–341. Springer.

[Haidari et al., 2016] Haidari, L. A., Brown, S. T., Ferguson, M., Bancroft, E., Spiker, M., Wilcox, A., Ambikapathi, R., Sampath, V., Connor, D. L., et Lee, B. Y. (2016). **The economic and operational value of using drones to transport vaccines**. *Vaccine*, 34(34) :4062–4067.

[Halperin et al., 2008] Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., Fu, K., Kohno, T., et Maisel, W. H. (2008). **Pacemakers and implantable cardiac defibrillators : Software radio attacks and zero-power defenses**. Dans *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 129–142. IEEE.

[Harshita, 2017] Harshita, H. (2017). **Detection and prevention of icmp flood ddos attack**. *International Journal of New Technology and Research*, 3(3).

[Hassanalieragh et al., 2015] Hassanalieragh, M., Page, A., Soyata, T., Sharma, G., Aktas, M., Mateos, G., Kantarci, B., et Andreescu, S. (2015). **Health monitoring and management using internet-of-things (iot) sensing with cloud-based processing : Opportunities and challenges**. Dans *2015 IEEE international conference on services computing (SCC)*, pages 285–292. IEEE.

[He et al., 2017] He, D., Chan, S., et Guizani, M. (2017). **Drone-assisted public safety networks : The security aspect**. *IEEE Communications Magazine*, 55(8) :218–223.

[He et al., 2010] He, D., Gao, Y., Chan, S., Chen, C., et Bu, J. (2010). **An enhanced two-factor user authentication scheme in wireless sensor networks.** *Ad hoc & sensor wireless networks*, 10(4) :361–371.

[Heys, 2002] Heys, H. M. (2002). **A tutorial on linear and differential cryptanalysis**. *Cryptologia*, 26(3) :189–221.

[Hiremath et al., 2014] Hiremath, S., Yang, G., et Mankodiya, K. (2014). **Wearable internet of things : Concept, architectural components and promises for person-centered healthcare**. Dans *2014 4th International Conference on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, pages 304–307. IEEE.

[Hong et al., 2014] Hong, D., Lee, J.-K., Kim, D.-C., Kwon, D., Ryu, K. H., et Lee, D.-G. (2014). **LEA : A 128-Bit Block Cipher for Fast Encryption on Common Processors**. Dans *Information Security Applications*, pages 3–27. Springer.

[Hong, 2012] Hong, J. (2012). **The state of phishing attacks**. *Communications of the ACM*, 55(1) :74–81.

[Hore et al., 2010] Hore, A., et Ziou, D. (2010). **Image quality metrics : PSNR vs. SSIM**. Dans *Pattern Recognition (ICPR), 2010 20th International Conference on*, pages 2366–2369. IEEE.

[Howgrave-Graham et al., 2005] Howgrave-Graham, N., Silverman, J. H., et Whyte, W. (2005). **Choosing parameter sets for ntruencrypt with naep and sves-3**. Dans *Cryptographers' Track at the RSA Conference*, pages 118–135. Springer.

[Hu et al., 2016] Hu, H., Shinde, S., Adrian, S., Chua, Z. L., Saxena, P., et Liang, Z. (2016). **Data-oriented programming : On the expressiveness of non-control data attacks**. Dans *Security and Privacy (SP), 2016 IEEE Symposium on*, pages 969–986. IEEE.

[Huang et al., 2009] Huang, F., et Feng, Y. (2009). **Security analysis of image encryption based on twodimensional chaotic maps and improved algorithm**. *Frontiers of Electrical and Electronic Engineering in China*, 4(1) :5–9.

[Humayed et al., 2017] Humayed, A., Lin, J., Li, F., et Luo, B. (2017). **Cyber-physical systems security—a survey**. *IEEE Internet of Things Journal*, 4(6) :1802–1831.

[Hung et al., 2004] Hung, K., Zhang, Y.-T., et Tai, B. (2004). **Wearable medical devices for tele-home healthcare**. Dans *The 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, volume 2, pages 5384–5387. IEEE.

[Hunter, 2016] Hunter, J. (2016). **Adopting ai is essential for a sustainable pharma industry**. *Drug Discov. World*, pages 69–71.

[Irani et al., 2011] Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., et Pu, C. (2011). **Reverse social engineering attacks in online social networks**. Dans *International conference on detection of intrusions and malware, and vulnerability assessment*, pages 55–74. Springer.

[Jagatic et al., 2007] Jagatic, T. N., Johnson, N. A., Jakobsson, M., et Menczer, F. (2007). **Social phishing**. *Communications of the ACM*, 50(10) :94–100.

[Jain et al., 2012] Jain, A. K., et Kumar, A. (2012). **Biometric recognition : an overview**. Dans *Second generation biometrics : The ethical, legal and social context*, pages 49–79. Springer.

[Jain et al., 2004] Jain, A. K., Ross, A., et Prabhakar, S. (2004). **An introduction to biometric recognition**. *IEEE Transactions on circuits and systems for video technology*, 14(1) :4–20.

[Janakiraman et al., 2018] Janakiraman, S., Thenmozhi, K., Rayappan, J. B. B., et Amirtharajan, R. (2018). **Lightweight chaotic image encryption algorithm for real-time embedded system : Implementation and analysis on 32-bit microcontroller**. *Microprocessors and Microsystems*, 56(Supplement C) :1 – 12.

[Jara et al., 2013] Jara, A. J., Zamora-Izquierdo, M. A., et Skarmeta, A. F. (2013). **Interconnection framework for mHealth and remote monitoring based on the Internet of Things**. *IEEE Journal on Selected Areas in Communications*, 31(9) :47–65.

[Jiang et al., 2017] Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., et Wang, Y. (2017). **Artificial intelligence in healthcare : past, present and future**. *Stroke and vascular neurology*, 2(4) :230–243.

[Jones et al., 2013] Jones, N., et Sherry, J. (2013). **System and method for authenticating a user using a graphical password**. US Patent 8,347,103.

[Joshi et al., 2005] Joshi, J. B., Bertino, E., Latif, U., et Ghafoor, A. (2005). **A generalized temporal role-based access control model**. *IEEE Transactions on Knowledge and Data Engineering*, 17(1) :4–23.

[Kang et al., 2018] Kang, M., Park, E., Cho, B. H., et Lee, K.-S. (2018). **Recent patient health monitoring platforms incorporating internet of things-enabled smart devices**. *International neurourology journal*, 22(Suppl 2) :S76.

[Kang et al., 2019] Kang, S., Baek, H., Jung, E., Hwang, H., et Yoo, S. (2019). **Survey on the demand for adoption of internet of things (iot)-based services in hospitals : Investigation of nurses' perception in a tertiary university hospital**. *Applied Nursing Research*, 47 :18–23.

[Kanso et al., 2015] Kanso, A., et Ghebleh, M. (2015). **An efficient and robust image encryption scheme for medical applications**. *Communications in Nonlinear Science and Numerical Simulation*, 24(1) :98–116.

[Kapusta et al., 2016] Kapusta, K., Memmi, G., et Noura, H. (2016). **Poster : A keyless efficient algorithm for data protection by means of fragmentation**. Dans *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 1745–1747. ACM.

[Kapusta et al., 2017] Kapusta, K., Memmi, G., et Noura, H. (2017). **Secure and resilient scheme for data protection in unattended wireless sensor networks**. Dans *Cyber Security in Networking Conference (CSNet), 2017 1st*, pages 1–8. IEEE.

[Kargupta et al., 2003] Kargupta, H., Datta, S., Wang, Q., et Sivakumar, K. (2003). **On the privacy preserving properties of random data perturbation techniques**. Dans *Data Mining, 2003. ICDM 2003. Third IEEE International Conference on*, pages 99–106. IEEE.

[Kasinathan et al., 2013a] Kasinathan, P., Costamagna, G., Khaleel, H., Pastrone, C., et Spirito, M. A. (2013a). **An ids framework for internet of things empowered by 6lowpan**. Dans *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 1337–1340. ACM.

[Kasinathan et al., 2013b] Kasinathan, P., Pastrone, C., Spirito, M. A., et Vinkovits, M. (2013b). **Denial-of-service detection in 6lowpan based internet of things**. Dans *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)*, pages 600–607. IEEE.

[Kasl et al., 1966] Kasl, S. V., et Cobb, S. (1966). **Health behavior, illness behavior and sick role behavior : I. health and illness behavior**. *Archives of Environmental Health : An International Journal*, 12(2) :246–266.

[Keliher et al.,] Keliher, L., et Meijery, H. **A new substitution-permutation network cipher using key-dependent s-boxes**.

[Kelly, 2012] Kelly, K. (2012). **Better than human : Why robots will—and must—take our jobs**. *Wired. http ://www. wired. com/2012/12/ff-robots-will-take-our-jobs/(Accessed 4 August 2014.)*.

[Kester et al., 2015] Kester, Q.-A., Nana, L., Pascu, A. C., Gire, S., Eghan, J. M., et Quaynor, N. N. (2015). **A security technique for authentication and security of medical images in health information systems**. Dans *Computational Science and Its Applications (ICCSA), 2015 15th International Conference on*, pages 8–13. IEEE.

[Khattab et al., 2016] Khattab, A., Jeddi, Z., Amini, E., et Bayoumi, M. (2016). **RFID Security : A Lightweight Paradigm**. Springer.

[Kim et al., 2014] Kim, J., Lee, D., Jeon, W., Lee, Y., et Won, D. (2014). **Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks**. *Sensors*, 14(4) :6443–6462.

[Kiourti et al., 2014] Kiourti, A., Psathas, K. A., et Nikita, K. S. (2014). **Implantable and ingestible medical devices with wireless telemetry functionalities : A review of current status and challenges**. *Bioelectromagnetics*, 35(1) :1–15.

[Kocabas et al., 2016] Kocabas, O., Soyata, T., et Aktas, M. K. (2016). **Emerging security mechanisms for medical cyber physical systems**. *IEEE/ACM transactions on computational biology and bioinformatics*, 13(3) :401–416.

[Komulainen, 2001] Komulainen, O. (2001). **Heart rate monitor**. US Patent App. 29/131,645.

[Koydemir et al., 2018] Koydemir, H. C., et Ozcan, A. (2018). **Wearable and implantable sensors for biomedical applications**. *Annual Review of Analytical Chemistry*, 11 :127–146.

[Krames, 2002] Krames, E. (2002). **Implantable devices for pain control : spinal cord stimulation and intrathecal therapies**. *Best Practice & Research Clinical Anaesthesiology*, 16(4) :619–649.

[Krawczyk, 1994] Krawczyk, H. (1994). **Secret sharing made short**. Dans *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '93, pages 136–146, London, UK. Springer-Verlag.

[Kuila et al., 2019] Kuila, S., Dhanda, N., Joardar, S., Neogy, S., et Kuila, J. (2019). **A generic survey on medical big data analysis using internet of things**. Dans *First International Conference on Artificial Intelligence and Cognitive Computing*, pages 265–276. Springer.

[Kumar et al., 2014a] Kumar, J. S., et Patel, D. R. (2014a). **A survey on internet of things : Security and privacy issues**. *International Journal of Computer Applications*, 90(11).

[Kumar et al., 2014b] Kumar, M., Pal, S. K., et Panigrahi, A. (2014b). **FeW : A Lightweight Block Cipher.** *IACR Cryptology ePrint Archive*, 2014 :326.

[Kumar et al., 2011] Kumar, P., Choudhury, A. J., Sain, M., Lee, S.-G., et Lee, H.-J. (2011). **Ruasn : a robust user authentication framework for wireless sensor networks**. *Sensors*, 11(5) :5020–5046.

[Kumar et al., 2012] Kumar, P., et Lee, H.-J. (2012). **Security issues in healthcare applications using wireless medical sensor networks : A survey**. *sensors*, 12(1) :55–91.

[Kwon et al., 2005] Kwon, T., Lee, H., Choi, S., Kim, J., Cho, D.-H., Cho, S., Yun, S., Park, W.-H., et Kim, K. (2005). **Design and implementation of a simulator based on a cross-layer protocol between mac and phy layers in a wibro compatible. ieee 802.16 e ofdma system**. *Communications Magazine, IEEE*, 43(12) :136–146.

[La et al., 2016] La, Q. D., Quek, T. Q., et Lee, J. (2016). **A game theoretic model for enabling honeypots in iot networks**. Dans *Communications (ICC), 2016 IEEE International Conference on*, pages 1–6. IEEE.

[Laiphrakpam et al., 2017] Laiphrakpam, D. S., et Khumanthem, M. S. (2017). **A robust image encryption scheme based on chaotic system and elliptic curve over finite field**. *Multimedia Tools and Applications*, pages 1–24.

[Lee et al., 2009] Lee, H., Lee, K., et Shin, Y. (2009). **Aes implementation and performance evaluation on 8-bit microcontrollers**. *CoRR*, abs/0911.0482.

[Lee et al., 2014] Lee, K.-H., et Chiu, P.-L. (2014). **Digital image sharing by diverse image media**. *IEEE transactions on information forensics and security*, 9(1) :88–98.

[Lee et al., 2005] Lee, Y., et Kozar, K. A. (2005). **Investigating factors affecting the adoption of anti-spyware systems**. *Communications of the ACM*, 48(8) :72–77.

[Li et al., 2011] Li, C., Chen, M. Z., et Lo, K.-T. (2011). **Breaking an image encryption algorithm based on chaos**. *International Journal of Bifurcation and Chaos*, 21(07) :2067–2076.

[Li et al., 2013a] Li, C.-T., Weng, C.-Y., et Lee, C.-C. (2013a). **An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks**. *Sensors*, 13(8) :9589–9603.

[Li et al., 2018a] Li, J., Lin, Q., Yu, C., Ren, X., et Li, P. (2018a). **A qdct-and svd-based color image watermarking scheme using an optimized encrypted binary computer-generated hologram**. *Soft Computing*, 22(1) :47–65.

[Li, 2012] Li, M. (2012). **On the confidentiality of information dispersal algorithms and their erasure codes**. *CoRR*, abs/1206.4123.

[Li et al., 2010] Li, M., Lou, W., et Ren, K. (2010). **Data security and privacy in wireless body area networks**. *IEEE Wireless communications*, 17(1).

[Li et al., 2004] Li, M., et Taylor, R. H. (2004). **Spatial motion constraints in medical robot using virtual fixtures generated by anatomy**. Dans *Robotics and Automation, 2004. Proceedings. ICRA'04. 2004 IEEE International Conference on*, volume 2, pages 1270–1275. IEEE.

[Li et al., 2017] Li, P., Li, T., Yao, Z.-A., Tang, C.-M., et Li, J. (2017). **Privacy-preserving outsourcing of image feature extraction in cloud computing**. *Soft Computing*, 21(15) :4349–4359.

[Li et al., 2013b] Li, P., Yang, C.-N., Wu, C.-C., Kong, Q., et Ma, Y. (2013b). **Essential secret image sharing scheme with different importance of shadows**. *Journal of Visual Communication and Image Representation*, 24(7) :1106–1114.

[Li et al., 2002] Li, S., et Zheng, X. (2002). **Cryptanalysis of a chaotic image encryption method**. Dans *Circuits and Systems, 2002. ISCAS 2002. IEEE International Symposium on*, volume 2, pages II–708. IEEE.

[Li et al., 2016] Li, Y., Ge, G., et Xia, D. (2016). **Chaotic hash function based on the dynamic s-box with variable parameters**. *Nonlinear Dynamics*, 84(4) :2387–2402.

[Li et al., 2018b] Li, Y., Wang, G., Nie, L., Wang, Q., et Tan, W. (2018b). **Distance metric optimization driven convolutional neural network for age invariant face recognition**. *Pattern Recognition*, 75 :51–62.

[Liao et al., 2013] Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., et Tung, K.-Y. (2013). **Intrusion detection system : A comprehensive review**. *Journal of Network and Computer Applications*, 36(1) :16–24.

[Lima et al., 2015] Lima, J., Madeiro, F., et Sales, F. (2015). **Encryption of medical images based on the cosine number transform**. *Signal Processing : Image Communication*, 35 :1–8.

[Lin et al., 2018] Lin, Z., Wang, G., Wang, X., Yu, S., et Lü, J. (2018). **Security performance analysis of a chaotic stream cipher**. *Nonlinear Dynamics*, 94(2) :1003–1017.

[Liu et al., 2011a] Liu, C., Yang, J., Chen, R., Zhang, Y., et Zeng, J. (2011a). **Research on immunity-based intrusion detection technology for the internet of things**. Dans *2011 Seventh International Conference on Natural Computation*, volume 1, pages 212–216. IEEE.

[Liu et al., 2019] Liu, X., Steiger, C., Lin, S., Parada, G. A., Liu, J., Chan, H. F., Yuk, H., Phan, N. V., Collins, J., Tamang, S., et others (2019). **Ingestible hydrogel device**. *Nature communications*, 10.

[Liu et al., 2011b] Liu, Y., Ning, P., et Reiter, M. K. (2011b). **False data injection attacks against state estimation in electric power grids**. *ACM Transactions on Information and System Security (TISSEC)*, 14(1) :13.

[Liu et al., 2014] Liu, Y., Tang, J., et Xie, T. (2014). **Cryptanalyzing a rgb image encryption algorithm based on dna encoding and chaos map**. *Optics & Laser Technology*, 60 :111–115.

[Luo et al., 2017] Luo, T., Xu, Z., Jin, X., Jia, Y., et Ouyang, X. (2017). **Iotcandyjar : Towards an intelligent-interaction honeypot for iot devices**. *Black Hat*.

[Mahmood et al., 2011] Mahmood, A. B., et Dony, R. D. (2011). **Segmentation based encryption method for medical images**. Dans *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, pages 596–601. IEEE.

[Maron, 2017] Maron, D. (2017). **Us hospitals not immune to crippling cyber-attacks : Outdated systems and earlier breaches underscore america's healthcare data security risks**. *Scientific American. Last modified May*, 15.

[Marrow et al., 2001] Marrow, P., Koubarakis, M., van Lengen, R.-H., Valverde-Albacete, F., Bonsma, E., Cid-Suerio, J., Figueiras-Vidal, A. R., Gallardo-Antolín, A., Hoile, C., Koutris, T., et others (2001). **Agents in decentralised information ecosystems : the diet approach**.

[Marshall, 2003] Marshall, D. R. (2003). **Swallowable data recorder capsule medical device**. US Patent 6,632,175.

[Martin et al., 2017] Martin, G., Kinross, J., et Hankin, C. (2017). **Effective cybersecurity is fundamental to patient safety**.

[Massoudi et al., 2008] Massoudi, A., Lefebvre, F., De Vleeschouwer, C., Macq, B., et Quisquater, J.-J. (2008). **Overview on selective encryption of image and video : challenges and perspectives**. *EURASIP Journal on Information Security*, 2008 :5.

[McCarthy et al., 2019] McCarthy, C. J., et Uppot, R. N. (2019). **Advances in virtual and augmented reality—exploring the role in health-care education**. *Journal of Radiology Nursing*.

[McFarland et al., 2019] McFarland, S., Coufopolous, A., et Lycett, D. (2019). **The effect of telehealth versus usual care for home-care patients with long-term conditions : A systematic review, meta-analysis and qualitative synthesis**. *Journal of Telemedicine and Telecare*, page 1357633X19862956.

[McKay et al., 2017] McKay, K. A., Bassham, L. E., Turan, M. S., et Mouha, N. W. (2017). **Report on lightweight cryptography**. *NIST Interagency/Internal Report (NISTIR)-8114*.

[McMahon et al., 2017] McMahon, E., Williams, R., El, M., Samtani, S., Patton, M., et Chen, H. (2017). **Assessing medical device vulnerabilities on the internet of things**. Dans *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 176–178. IEEE.

[Melki et al., 2018] Melki, R., Noura, H. N., Mansour, M. M., et Chehab, A. (2018). **An efficient ofdm-based encryption scheme using a dynamic key approach**. *IEEE Internet of Things Journal*, pages 1–1.

[Menezes et al., 1996] Menezes, A. J., Van Oorschot, P. C., et Vanstone, S. A. (1996). **Handbook of applied cryptography**. CRC press.

[Miller, 1985] Miller, V. S. (1985). **Use of elliptic curves in cryptography**. Dans *Conference on the Theory and Application of Cryptographic Techniques*, pages 417–426. Springer.

[Mills et al., 1985] Mills, D., et others (1985). **Network time protocol**. Rapport technique, RFC 958, M/A-COM Linkabit.

[Mitchell et al., 2014] Mitchell, R., et Chen, I.-R. (2014). **A survey of intrusion detection techniques for cyber-physical systems**. *ACM Computing Surveys (CSUR)*, 46(4) :55.

[Mitchell et al., 2015] Mitchell, R., et Chen, R. (2015). **Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems**. *IEEE Transactions on Dependable and Secure Computing*, 12(1) :16–30.

[Moalla et al., 2012] Moalla, R., Labiod, H., Lonc, B., et Simoni, N. (2012). **Risk analysis study of its communication architecture**. Dans *Network of the Future (NOF), 2012 Third International Conference on the*, pages 1–5. IEEE.

[Mondal et al., 2017] Mondal, B., et Mandal, T. (2017). **A light weight secure image encryption scheme based on chaos & dna computing**. *Journal of King Saud University - Computer and Information Sciences*, 29(4) :499 – 504.

[Moradi et al., 2011] Moradi, A., et Poschmann, A. (2011). **Pushing the limits : a very compact and a threshold implementation of aes.** Dans *Eurocrypt*, volume 6632, pages 69–88. Springer.

[Mostefaoui et al., 2015a] Mostefaoui, A., Noura, H., et Fawaz, Z. (2015a). **An integrated multimedia data reduction and content confidentiality approach for limited networked devices**. *Ad Hoc Networks*, 32 :149–156.

[Mostefaoui et al., 2015b] Mostefaoui, A., Noura, H., et Fawaz, Z. (2015b). **An integrated multimedia data reduction and content confidentiality approach for limited networked devices**. *Ad Hoc Networks*, 32 :81–97.

[Munzer et al., 2019] Munzer, B. W., Khan, M. M., Shipman, B., et Mahajan, P. (2019). **Augmented reality in emergency medicine : A scoping review**. *Journal of medical Internet research*, 21(4) :e12368.

[Murer, 2002] Murer, C. G. (2002). **Protecting patient privacy**. *Public Law*, 104 :191.

[Muthurajkumar et al., 2014] Muthurajkumar, S., Vijayalakshmi, M., et Kannan, A. (2014). **Intelligent temporal role based access control for data storage in cloud database**. Dans *Advanced Computing (ICoAC), 2014 Sixth International Conference on*, pages 184–188. IEEE.

[Naditz, 2009] Naditz, A. (2009). **Telemedicine named one of space race's top tech breakthroughs**. *Telemedicine and e-Health*, 15(8) :735–736.

[Nam et al., 2009] Nam, J., Paik, J., Kang, H.-K., Kim, U. M., et Won, D. (2009). **An off-line dictionary attack on a simple three-party key exchange protocol**. *IEEE Communications Letters*, 13(3) :205–207.

[Naor et al., 2017] Naor, M., et Shamir, A. (2017). **Visual cryptography [j/ol]**. *Lecture Notes in Computer Science*, 950(1) :1–12.

[Narayanan et al., 2005] Narayanan, A., et Shmatikov, V. (2005). **Fast dictionary attacks on passwords using time-space tradeoff**. Dans *Proceedings of the 12th ACM conference on Computer and communications security*, pages 364–372. ACM.

[Nijboer et al., 1988] Nijboer, J., Dorlas, J., et Lubbers, J. (1988). **The difference in blood pressure between upper arm and finger during physical exercise**. *Clinical Physiology*, 8(5) :501–510.

[Nimmo, 2010] Nimmo, K. (2010). **Will stuxnet malware be used in false flag attack**. *Infowars.com*.

[Nithya et al., 2016] Nithya, R., et Kumar, D. S. (2016). **Where aes is for internet, simon could be for iot**. *Procedia Technology*, 25 :302–309.

[Northcutt, 2005] Northcutt, S. (2005). **Logic bombs, trojan horses, and trap doors**. Dans *SANS*, pages 2005–2016.

[Noura et al., 2018a] Noura, H., Chehab, A., Noura, M., Couturier, R., et Mansour, M. M. (2018a). **Lightweight, dynamic and efficient image encryption scheme**. *Multimedia Tools and Applications*, pages 1–35.

[Noura et al., 2018b] Noura, H., Chehab, A., Sleem, L., Noura, M., Couturier, R., et Mansour, M. M. (2018b). **One round cipher algorithm for multimedia iot devices**. *Multimedia Tools and Applications*, pages 1–31.

[Noura et al., 2015a] Noura, H., et Couroussé, D. (2015a). **Lightweight, dynamic, and flexible cipher scheme for wireless and mobile networks**. Dans *International Conference on Ad Hoc Networks*, pages 225–236. Springer.

[Noura et al., 2015b] Noura, H., Hussein, S., Martin, S., Boukhatem, L., et Agha, K. A. (2015b). **Erdia : An efficient and robust data integrity algorithm for mobile and wireless networks**. Dans *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2103–2108.

[Noura et al., 2014] Noura, H., Martin, S., Agha, K. A., et Chahine, K. (2014). **Erss-rlnc : Efficient and robust secure scheme for random linear network coding**. *Computer Networks*, 75, Part A :99 – 112.

[Noura et al., 2018c] Noura, H., Melki, R., Chehab, A., Mansour, M. M., et Martin, S. (2018c). **Efficient and secure physical encryption scheme for low-power wireless m2m devices**. Dans *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 1267–1272. IEEE.

[Noura et al., 2017a] Noura, H., Sleem, L., et Couturier, R. (2017a). **A revision of a new chaos-based image encryption system : Weaknesses and limitations**. *CoRR*, abs/1701.08371.

[Noura et al., 2017b] Noura, H., Sleem, L., Noura, M., Mansour, M. M., Chehab, A., et Couturier, R. (2017b). **A new efficient lightweight and secure image cipher scheme**. *Multimedia Tools and Applications*.

[Noura et al., 2017c] Noura, H., Sleem, L., Noura, M., Mansour, M. M., Chehab, A., et Couturier, R. (2017c). **A new efficient lightweight and secure image cipher scheme**. *Multimedia Tools and Applications*, pages 1–28.

[Noura et al., 2018d] Noura, H., Sleem, L., Noura, M., Mansour, M. M., Chehab, A., et Couturier, R. (2018d). **A new efficient lightweight and secure image cipher scheme**. *Multimedia Tools and Applications*, 77(12) :15457–15484.

[Noura et al., 2018e] Noura, H. N., Noura, M., Chehab, A., Mansour, M. M., et Couturier, R. (2018e). **Efficient and secure cipher scheme for multimedia contents**. *Multimedia Tools and Applications*, pages 1–30.

[Nyberg et al., 1995] Nyberg, K., et Knudsen, L. R. (1995). **Provable security against a differential attack**. *Journal of Cryptology*, 8(1) :27–37.

[Oh et al., 2014] Oh, D., Kim, D., et Ro, W. W. (2014). **A malicious pattern detection engine for embedded security systems in the internet of things**. *Sensors*, 14(12) :24188–24211.

[Oh et al., 2003] Oh, S., et Park, S. (2003). **Task–role-based access control model**. *Information systems*, 28(6) :533–562.

[Ohno-Machado et al., 2004] Ohno-Machado, L., Silveira, P. S. P., et Vinterbo, S. (2004). **Protecting patient privacy by quantifiable control of disclosures in disseminated databases**. *International Journal of Medical Informatics*, 73(7-8) :599–606.

[O'Melia et al., 2010] O'Melia, S., et Elbirt, A. J. (2010). **Enhancing the performance of symmetric-key cryptography via instruction set extensions**. *IEEE transactions on very large scale integration (VLSI) systems*, 18(11) :1505–1518.

[Osvik et al., 2010] Osvik, D. A., Bos, J. W., Stefan, D., et Canright, D. (2010). **Fast software aes encryption**. Dans *Fast Software Encryption : 17th International Workshop, FSE 2010, Seoul, Korea, Februara 7-10, 2010 Revised Selected Papers*, volume 6147, page 75. Springer Science & Business Media.

[Ou et al., 2007] Ou, Y., Sur, C., et Rhee, K. H. (2007). **Region-based selective encryption for medical imaging**. Dans *Frontiers in Algorithmics*, pages 62–73. Springer.

[Paar et al., 2009a] Paar, C., et Pelzl, J. (2009a). **Understanding cryptography : a textbook for students and practitioners**. Springer Science & Business Media.

[Paar et al., 2009b] Paar, C., et Pelzl, J. (2009b). **Understanding Cryptography : A Textbook for Students and Practitioners**. Springer Publishing Company, Incorporated, 1st édition.

[Page et al., 2015] Page, A., Soyata, T., Couderc, J.-P., Aktas, M., Kantarci, B., et Andreescu, S. (2015). **Visualization of health monitoring data acquired from distributed sensors for multiple patients**. Dans *Global Communications Conference (GLOBECOM), 2015 IEEE*, pages 1–7. IEEE.

[Panduranga et al., 2013] Panduranga, H., et Naveenkumar, S. (2013). **Selective image encryption for medical and satellite images**. *International Journal of Engineering and Technology (IJET)*, 5(1) :115–121.

[Pang et al., 2018] Pang, Z., Yang, G., Khedri, R., et Zhang, Y.-T. (2018). **Introduction to the special section : convergence of automation technology, biomedical engineering, and health informatics toward the healthcare 4.0**. *IEEE Reviews in Biomedical Engineering*, 11 :249–259.

[Park et al., 2010] Park, K., Lin, Y., Metsis, V., Le, Z., et Makedon, F. (2010). **Abnormal human behavioral pattern detection in assisted living environments**. Dans *Proceedings of the 3rd International Conference on PErvasive Technologies Related to Assistive Environments*, page 9. ACM.

[Parmar, 2012] Parmar, B. (2012). **Protecting against spear-phishing**. *Computer Fraud & Security*, 2012(1) :8–11.

[Paul et al., 2011] Paul, G., et Maitra, S. (2011). **RC4 stream cipher and its variants**. CRC press.

[Pauws et al., 2017] Pauws, S. C., Nassabi, M. H., Schertzer, L., Smits, T., DEN BUIJS, J. O., et Van Deursen, P. W. (2017). **Personal emergency response system with predictive emergency dispatch risk assessment**. US Patent App. 15/317,440.

[Peabody, 2012] Peabody, S. R. (2012). **System containing location-based personal emergency response device**. US Patent 8,116,724.

[Perry et al., 2011] Perry, L., et Malkin, R. (2011). **Effectiveness of medical equipment donations to improve health systems : how much medical equipment is broken in the developing world ?**

[Peterson, 2013] Peterson, A. (2013). **Yes, terrorists could have hacked dick cheney's heart**. *Washington Post*.

[Pinkas, 2002] Pinkas, B. (2002). **Cryptographic techniques for privacy-preserving data mining**. *ACM Sigkdd Explorations Newsletter*, 4(2) :12–19.

[Pinto et al., 2017] Pinto, M. B., et Yagnik, A. (2017). **Fit for life : A content analysis of fitness tracker brands use of facebook in social media marketing**. *Journal of Brand Management*, 24(1) :49–67.

[Piret et al., 2003] Piret, G., et Quisquater, J.-J. (2003). **A differential fault attack technique against spn structures, with application to the aes and khazad**. Dans *International workshop on cryptographic hardware and embedded systems*, pages 77–88. Springer.

[Poon et al., 2006] Poon, C. C., Zhang, Y.-T., et Bao, S.-D. (2006). **A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health**. *IEEE Communications Magazine*, 44(4) :73–81.

[Porras et al., 1997] Porras, P. A., et Neumann, P. G. (1997). **Emerald : Event monitoring enabling response to anomalous live disturbances**. Dans *Proceedings of the 20th national information systems security conference*, pages 353–365.

[Pradeep et al., 2013] Pradeep, L., et Bhattacharjya, A. (2013). **Random key and key dependent s-box generation for aes cipher to overcome known attacks**. Dans *International Symposium on Security in Computing and Communication*, pages 63–69. Springer.

[Proano et al., 2010] Proano, A., et Lazos, L. (2010). **Selective jamming attacks in wireless networks**. Dans *2010 IEEE International Conference on Communications*, pages 1–6. IEEE.

[Puech et al., 2005] Puech, W., et Rodrigues, J. M. (2005). **Crypto-compression of medical images by selective encryption of dct**. Dans *Signal Processing Conference, 2005 13th European*, pages 1–4. IEEE.

[Pulver et al., 2016] Pulver, A., Wei, R., et Mann, C. (2016). **Locating aed enabled medical drones to enhance cardiac arrest response times**. *Prehospital Emergency Care*, 20(3) :378–389.

[Qin et al., 2018] Qin, C., Chen, X., Luo, X., Zhang, X., et Sun, X. (2018). **Perceptual image hashing via dual-cross pattern encoding and salient structure detection**. *Information Sciences*, 423 :284–302.

[Qin et al., 2015] Qin, C., et Zhang, X. (2015). **Effective reversible data hiding in encrypted image with privacy protection for image content**. *Journal of Visual Communication and Image Representation*, 31 :154–164.

[Rabin, 1989] Rabin, M. O. (1989). **Efficient dispersal of information for security, load balancing, and fault tolerance**. *J. ACM*, 36(2) :335–348.

[Rahman et al., 2012] Rahman, M. A., et Mohsenian-Rad, H. (2012). **False data injection attacks with incomplete information against smart power grids**. Dans *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 3153–3158. Citeseer.

[Ray et al., 2007] Ray, I., et Toahchoodee, M. (2007). **A spatio-temporal role-based access control model**. Dans *IFIP Annual Conference on Data and Applications Security and Privacy*, pages 211–226. Springer.

[Raza et al., 2009] Raza, S., Slabbert, A., Voigt, T., et Landernäs, K. (2009). **Security considerations for the wireless hart protocol**. Dans *Proceedings of the 14th IEEE international conference on Emerging technologies & factory automation*, ETFA'09, pages 242–249, Piscataway, NJ, USA. IEEE Press.

[Resch et al., 2011] Resch, J. K., et Plank, J. S. (2011). **Aont-rs : Blending security and performance in dispersed storage systems**. Dans *Proceedings of the 9th USENIX Conference on File and Stroage Technologies*, FAST'11, pages 14–14, Berkeley, CA, USA. USENIX Association.

[Rhouma et al., 2010] Rhouma, R., Solak, E., et Belghith, S. (2010). **Cryptanalysis of a new substitution–diffusion based image cipher**. *Communications in Nonlinear Science and Numerical Simulation*, 15(7) :1887–1892.

[Rivest, 1992] Rivest, R. (1992). **The rc4 encryption algorithm. rsa data sec**. *Inc.(March 1998)*.

[Rivest, 1997] Rivest, R. L. (1997). **All-or-nothing encryption and the package transform**. Dans *In Fast Software Encryption, LNCS*, pages 210–218. Springer-Verlag.

[Roemer et al., 2012] Roemer, R., Buchanan, E., Shacham, H., et Savage, S. (2012). **Return-oriented programming : Systems, languages, and applications**. *ACM Transactions on Information and System Security (TISSEC)*, 15(1) :2.

[Rosen et al., 2006] Rosen, J., et Hannaford, B. (2006). **Doc at a distance**. *IEEE spectrum*, 43(10) :34–39.

[Rushanan et al., 2014] Rushanan, M., Rubin, A. D., Kune, D. F., et Swanson, C. M. (2014). **Sok : Security and privacy in implantable medical devices and body area networks**. Dans *2014 IEEE Symposium on Security and Privacy (SP)*, pages 524–539. IEEE.

[Saeed et al., 2019] Saeed, N., Manzoor, M., et Khosravi, P. (2019). **An exploration of usability issues in telecare monitoring systems and possible solutions : a systematic literature review**. *Disability and Rehabilitation : Assistive Technology*, pages 1–11.

[Santoso et al., 2015] Santoso, F., et Redmond, S. J. (2015). **Indoor location-aware medical systems for smart homecare and telehealth monitoring : state-of-the-art**. *Physiological measurement*, 36(10) :R53.

[Schaumont,] Schaumont, P. **Fault attacks on embedded software : Threats, design, and mitigation**.

[Schneier, 1993] Schneier, B. (1993). **The idea encryption algorithm-the international data encryption algorithm (idea) may be one of the most secure block algorithms available to the public today. bruce examines its 128-bit-long key**. *Dr Dobb's Journal-Software Tools for the Professional Programmer*, 18(13) :50–57.

[Schonberg et al., 2008] Schonberg, D., Draper, S. C., Yeo, C., et Ramchandran, K. (2008). **Toward compression of encrypted images and video sequences**. *IEEE Transactions on Information Forensics and Security*, 3(4) :749–762.

[Seepers et al., 2016] Seepers, R. M., Weber, J. H., Erkin, Z., Sourdis, I., et Strydis, C. (2016). **Secure key-exchange protocol for implants using heartbeats**. Dans *Proceedings of the ACM International Conference on Computing Frontiers*, pages 119–126. ACM.

[Senie et al., 1998] Senie, D., et Ferguson, P. (1998). **Network ingress filtering : Defeating denial of service attacks which employ ip source address spoofing**. *Network*.

[Sensmeier, 2017] Sensmeier, J. (2017). **Harnessing the power of artificial intelligence**. *Nursing management*, 48(11) :14–19.

[Sey, 2018] Sey, D. (2018). **A survey on authentication methods for the internet of things**. *PeerJ Preprints*, 6 :e26474v1.

[Shah et al., 2019] Shah, P., Kendall, F., Khozin, S., Goosen, R., Hu, J., Laramie, J., Ringel, M., et Schork, N. (2019). **Artificial intelligence and machine learning in clinical development : a translational perspective**. *NPJ digital medicine*, 2(1) :69.

[Shah et al., 2016] Shah, Y. C., Schmidt, A., Choyi, V. K., Subramanian, L., et Leicher, A. (2016). **Multi-factor authentication to achieve required authentication assurance level**. US Patent App. 14/786,688.

[Shamir, 1979] Shamir, A. (1979). **How to share a secret**. *Communications of the ACM*, 22(11) :612–613.

[Shan et al., 2017] Shan, Y., Kesidis, G., Fleck, D., et Stavrou, A. (2017). **Preliminary study of fission defenses against low-volume dos attacks on proxied multiserver systems**. Dans *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*, pages 67–74. IEEE.

[Shi, 2004] Shi, Z. J. (2004). **Bit permutation instructions : Architecture, implementation and cryptographic properties**. *Princeton University, Princeton, NJ*.

[Shibutani et al., 2011] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., et Shirai, T. (2011). **Piccolo : an ultra-lightweight blockcipher**. Dans *Cryptographic Hardware and Embedded Systems–CHES 2011*, pages 342–357. Springer.

[Shu et al., 2015] Shu, X., Yao, D., et Ramakrishnan, N. (2015). **Unearthing stealthy program attacks buried in extremely long execution paths**. Dans *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 401–413. ACM.

[Singh et al., 2017] Singh, S., Sharma, P. K., Moon, S. Y., et Park, J. H. (2017). **Advanced lightweight encryption algorithms for iot devices : survey, challenges and solutions**. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–18.

[Smid et al., 1988] Smid, M. E., et Branstad, D. K. (1988). **Data encryption standard : past and future**. *Proceedings of the IEEE*, 76(5) :550–559.

[Smith et al., 2015] Smith, C. H., Maclean, K., Liu, J. J., Mann, S., Wendy, M., et Chapin, R. (2015). **System and method for advanced malware analysis**. US Patent 9,106,692.

[Som et al., 2013] Som, S., et Sen, S. (2013). **A non-adaptive partial encryption of grayscale images based on chaos**. *Procedia Technology*, 10 :663–671.

[Son et al., 2015] Son, J., Kim, D., Hussain, R., Tokuta, A., Kwon, S.-S., et Seo, J.-T. (2015). **Privacy aware incentive mechanism to collect mobile data while preventing duplication**. Dans *Military Communications Conference, MILCOM 2015-2015 IEEE*, pages 1242–1247. IEEE.

[Spiekermann, 2015] Spiekermann, S. (2015). **Ethical IT innovation : A value-based system design approach**. Auerbach Publications.

[Stallings, 2017] Stallings, W. (2017). **Cryptography and network security : principles and practice**. Pearson Upper Saddle River, NJ.

[Stone-Gross et al., 2009] Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C., et Vigna, G. (2009). **Your botnet is my botnet : analysis of a botnet takeover**. Dans *Proceedings of the 16th ACM conference on Computer and communications security*, pages 635–647. ACM.

[Sundmaeker et al., 2010] Sundmaeker, H., Guillemin, P., Friess, P., et Woelfflé, S. (2010). **Vision and Challenges for Realising the Internet of Things**. *Cluster of European Research Projects on the Internet of Things, European Commision*, 3(3) :34–36.

[Suvarna et al., 2016] Suvarna, R., Kawatkar, S., et Jagli, D. (2016). **Internet of medical things [iomt]**. *International Journal*, 4(6).

[Suzaki et al., 2013] Suzaki, T., Minematsu, K., Morioka, S., et Kobayashi, E. (2013). TWINE **: A Lightweight Block Cipher for Multiple Platforms**. Dans Knudsen, L., et Wu, H., éditeurs, *Selected Areas in Cryptography*, volume 7707 de *Lecture Notes in Computer Science*, pages 339–354. Springer Berlin Heidelberg.

[Swan, 2012] Swan, M. (2012). **Sensor mania ! the internet of things, wearable computing, objective metrics, and the quantified self 2.0**. *Journal of Sensor and Actuator Networks*, 1(3) :217–253.

[Tahir et al., 2013] Tahir, R., Hu, H., Gu, D., McDonald-Maier, K., et Howells, G. (2013). **Resilience against brute force and rainbow table attacks using strong icmetrics session key pairs**. Dans *Communications, Signal Processing, and their Applications (ICCSPA), 2013 1st International Conference on*, pages 1–6. IEEE.

[Ten et al., 2010] Ten, C.-W., Manimaran, G., et Liu, C.-C. (2010). **Cybersecurity for critical infrastructures : Attack and defense modeling**. *IEEE Transactions on Systems, Man, and Cybernetics-Part A : Systems and Humans*, 40(4) :853–865.

[Terry, 2012] Terry, N. P. (2012). **Protecting patient privacy in the age of big data**. *UMKC L. Rev.*, 81 :385.

[Thien et al., 2002] Thien, C.-C., et Lin, J.-C. (2002). **Secret image sharing**. *Computers & Graphics*, 26(5) :765–770.

[Thuemmler et al., 2017] Thuemmler, C., et Bai, C. (2017). **Health 4.0 : How virtualization and big data are revolutionizing healthcare**. Springer.

[Tillich et al., 2006] Tillich, S., et Großschädl, J. (2006). **Instruction set extensions for efficient aes implementation on 32-bit processors**. Dans *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 270–284. Springer.

[Toohey et al., 2016] Toohey, S. L., Wray, A., Wiechmann, W., Lin, M., et Boysen-Osborn, M. (2016). **Ten tips for engaging the millennial learner and moving an emergency medicine residency curriculum into the 21st century**. *Western Journal of Emergency Medicine*, 17(3) :337.

[Tran, 2013] Tran, B. (2013). **Personal emergency response (per) system**. US Patent 8,531,291.

[Tran et al., 2012] Tran, J., Tran, R., et White, J. R. (2012). **Smartphone-based glucose monitors and applications in the management of diabetes : an overview of 10 salient "apps" and a novel smartphone-connected blood glucose monitor**. *Clinical Diabetes*, 30(4) :173–178.

[Trnka et al., 2018] Trnka, M., Cerny, T., et Stickney, N. (2018). **Survey of authentication and authorization for the internet of things**. *Security and Communication Networks*, 2018.

[Tsang et al., 2005] Tsang, C.-H., et Kwong, S. (2005). **Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction**. Dans *Industrial Technology, 2005. ICIT 2005. IEEE International Conference on*, pages 51–56. IEEE.

[Turner et al., 2013] Turner, A., Glantz, K., et Gall, J. (2013). **A practitioner-researcher partnership to develop and deliver operational value of threat, risk and vulnerability assessment training to meet the requirements of emergency responders**. *Journal of Homeland Security and Emergency Management*, 10(1) :319–332.

[Ullah et al., 2012] Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., et Kwak, K. S. (2012). **A comprehensive survey of wireless body area networks**. *Journal of medical systems*, 36(3) :1065–1094.

[Ulutas et al., 2013] Ulutas, G., Ulutas, M., et Nabiyev, V. V. (2013). **Secret image sharing scheme with adaptive authentication strength**. *Pattern Recognition Letters*, 34(3) :283–291.

[Usman et al., 2007] Usman, K., Juzoji, H., Nakajima, I., Soegidjoko, S., Ramdhani, M., Hori, T., et Igi, S. (2007). **Medical image encryption based on pixel arrangement and random permutation for transmission security**. Dans *e-Health Networking, Application and Services, 2007 9th International Conference on*, pages 244–247. IEEE.

[Vadlamani et al., 2016] Vadlamani, S., Eksioglu, B., Medal, H., et Nandi, A. (2016). **Jamming attacks on wireless networks : A taxonomic survey**. *International Journal of Production Economics*, 172 :76–94.

[Venkatasubramanian et al., 2007] Venkatasubramanian, K., et Gupta, S. (2007). **Security in distributed, grid, mobile, and pervasive computing, chapter security solutions for pervasive healthcare**.

[Venkatasubramanian et al., 2010] Venkatasubramanian, K. K., Banerjee, A., et Gupta, S. K. S. (2010). **Pska : Usable and secure key agreement scheme for body area networks**. *IEEE Transactions on Information Technology in Biomedicine*, 14(1) :60–68.

[Verykios et al., 2004] Verykios, V. S., Bertino, E., Fovino, I. N., Provenza, L. P., Saygin, Y., et Theodoridis, Y. (2004). **State-of-the-art in privacy preserving data mining**. *ACM Sigmod Record*, 33(1) :50–57.

[Wadi et al., 2014] Wadi, S. M., et Zainal, N. (2014). **High definition image encryption algorithm based on aes modification**. *Wireless personal communications*, 79(2) :811–829.

[Wang et al., 2018a] Wang, D., Li, W., et Wang, P. (2018a). **Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks**. *IEEE Transactions on Industrial Informatics*.

[Wang et al., 2010] Wang, H., Zhang, M., et Wang, J. (2010). **Design and implementation of an emergency search and rescue system based on mobile robot and wsn**. Dans *Informatics in Control, Automation and Robotics (CAR), 2010 2nd International Asia Conference on*, volume 1, pages 206–209. IEEE.

[Wang et al., 2015a] Wang, P., et Jiang, L. (2015a). **Task-role-based access control model in smart health-care system**. Dans *MATEC Web of Conferences*, volume 22, page 01011. EDP Sciences.

[Wang et al., 2017] Wang, R., Blackburn, G., Desai, M., Phelan, D., Gillinov, L., Houghtaling, P., et Gillinov, M. (2017). **Accuracy of wrist-worn heart rate monitors**. *Jama cardiology*, 2(1) :104–106.

[Wang et al., 2013] Wang, X., et Liu, L. (2013). **Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos**. *Nonlinear Dynamics*, 73(1-2) :795–800.

[Wang et al., 2015b] Wang, X., Liu, L., et Zhang, Y. (2015b). **A novel chaotic block image encryption algorithm based on dynamic random growth technique**. *Optics and Lasers in Engineering*, 66 :10–18.

[Wang et al., 2015c] Wang, X., White, L., Chen, X., Gao, Y., Li, H., et Luo, Y. (2015c). **An empirical study of wearable technology acceptance in healthcare**. *Industrial Management & Data Systems*.

[Wang et al., 2018b] Wang, Y.-G., Zhu, G., et Shi, Y.-Q. (2018b). **Transportation spherical watermarking**. *IEEE Transactions on Image Processing*.

[Wei et al., 2015] Wei, S.-C., Hou, Y.-C., et Lu, Y.-C. (2015). **A technique for sharing a digital image**. *Computer Standards & Interfaces*, 40 :53–61.

[Wex et al., 2008] Wex, P., Breuer, J., Held, A., Leinmuller, T., et Delgrossi, L. (2008). **Trust issues for vehicular ad hoc networks**. Dans *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2800–2804. IEEE.

[Winton, 2016] Winton, R. (2016). **Hollywood hospital pays 17,000$ in bitcoin to hackers ; fbi investigating**. *Los Angeles Times*, 18.

[Woodward Jr et al., 2003] Woodward Jr, J. D., Horn, C., Gatune, J., et Thomas, A. (2003). **Biometrics : A look at facial recognition**. Rapport technique, RAND CORP SANTA MONICA CA.

[Wu et al., 2011] Wu, W., et Zhang, L. (2011). **LBlock : a lightweight block cipher**. Dans *Applied Cryptography and Network Security*, pages 327–344. Springer.

[Wunnava et al., 2002] Wunnava, S. V., et Rassi, E. (2002). **Data encryption performance and evaluation schemes**. Dans *SoutheastCon, 2002. Proceedings IEEE*, pages 234–238. IEEE.

[Xiang et al., 2007] Xiang, T., Wong, K.-w., et Liao, X. (2007). **Selective image encryption using a spatiotemporal chaotic system**. *Chaos : An Interdisciplinary Journal of Nonlinear Science*, 17(2) :023115.

[Xu et al., 2018] Xu, J., Wei, L., Zhang, Y., Wang, A., Zhou, F., et Gao, C.-z. (2018). **Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures**. *Journal of Network and Computer Applications*.

[Xu et al., 2016] Xu, K., Tian, K., Yao, D., et Ryder, B. G. (2016). **A sharper sense of self : Probabilistic reasoning of program behaviors for anomaly detection with context sensitivity**. Dans *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 467–478. IEEE.

[Xu et al., 2008] Xu, S., Wang, Y., Wang, J., et Tian, M. (2008). **Cryptanalysis of two chaotic image encryption schemes based on permutation and xor operations**. Dans *Computational Intelligence and Security, 2008. CIS'08. International Conference on*, volume 2, pages 433–437. IEEE.

[Xu et al., 2004] Xu, W., Wood, T., Trappe, W., et Zhang, Y. (2004). **Channel surfing and spatial retreats : defenses against wireless denial of service**. Dans *Proceedings of the 3rd ACM workshop on Wireless security*, pages 80–89. ACM.

[Yang et al., 2013] Yang, C.-W., Hwang, T., et Lin, T.-H. (2013). **Modification attack on qsdc with authentication and the improvement**. *International Journal of Theoretical Physics*, 52(7) :2230–2234.

[Yang et al., 2006] Yang, W.-S., et Hwang, S.-Y. (2006). **A process-mining framework for the detection of healthcare fraud and abuse**. *Expert Systems with Applications*, 31(1) :56–68.

[Ye et al., 2015] Ye, F., Qian, Y., et Hu, R. Q. (2015). **Energy efficient self-sustaining wireless neighborhood area network design for smart grid**. *IEEE Transactions on Smart Grid*, 6(1) :220–229.

[Yeh et al., 2011] Yeh, H.-L., Chen, T.-H., Liu, P.-C., Kim, T.-H., et Wei, H.-W. (2011). **A secured authentication protocol for wireless sensor networks using elliptic curves cryptography**. *Sensors*, 11(5) :4767–4779.

[Yuce, 2018] Yuce, B. (2018). **Fault attacks on embedded software : New directions in modeling, design, and mitigation**. PhD thesis, Virginia Tech.

[Yuen et al., 2017] Yuen, S. G. J., Park, J., Ghoreyshi, A., et Wu, A. (2017). **User identification via motion and heartbeat waveform data**. US Patent 9,851,808.

[Zarpelão et al., 2017] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., et de Alvarenga, S. C. (2017). **A survey of intrusion detection in internet of things**. *Journal of Network and Computer Applications*, 84 :25–37.

[Zeng et al., 2015] Zeng, L., et Liu, R. (2015). **Cryptanalyzing a novel couple images encryption algorithm based on dna subsequence operation and chaotic system**. *Optik-International Journal for Light and Electron Optics*, 126(24) :5022–5025.

[Zhang et al., 2011] Zhang, L., Yu, S., Wu, D., et Watters, P. (2011). **A survey on latest botnet attack and defense**. Dans *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on*, pages 53–60. IEEE.

[Zhang et al., 2015a] Zhang, L., Zhu, Z., Yang, B.-Q., Liu, W.-Y., Zhu, H.-F., et Zou, M.-Y. (2015a). **Cryptanalysis and improvement of an efficient and secure medical image protection scheme**. *Mathematical Problems in Engineering*, 2015.

[Zhang et al., 2015b] Zhang, L.-b., et Yang, B.-q. (2015b). **An efficient cryptosystem for medical image encryption**. *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 8(7) :327–340.

[Zhang et al., 2010] Zhang, P., Jiang, Y., Lin, C., Fan, Y., et Shen, X. (2010). **P-coding : secure network coding against eavesdropping attacks**. Dans *INFOCOM, 2010 Proceedings IEEE*, pages 1–9. IEEE.

[Zhang et al., 2014a] Zhang, X., Ren, Y., Shen, L., Qian, Z., et Feng, G. (2014a). **Compressing encrypted images with auxiliary information**. *IEEE Transactions on Multimedia*, 16(5) :1327–1336.

[Zhang et al., 2014b] Zhang, X., Sun, G., Shen, L., et Qin, C. (2014b). **Compression of encrypted images with multi-layer decomposition**. *Multimedia tools and applications*, 72(1) :489–502.

[Zhang et al., 2013] Zhang, Y., et Xiao, D. (2013). **Cryptanalysis of s-box-only chaotic image ciphers against chosen plaintext attack**. *Nonlinear Dynamics*, 72(4) :751–756.

[Zhang et al., 2012] Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., et Deng, H. (2012). **A survey of cyber crimes**. *Security and Communication Networks*, 5(4) :422–437.

[Zhou et al., 2013] Zhou, J., Liu, X., et Au, O. C. (2013). **On the design of an efficient encryption-then-compression system**. Dans *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 2872–2876. IEEE.

[Zhou et al., 1992] Zhou, M., DiCesare, F., et Desrochers, A. A. (1992). **A hybrid methodology for synthesis of petri net models for manufacturing systems**. *IEEE transactions on robotics and automation*, 8(3) :350–361.

[Zhou et al., 2009] Zhou, Y., Panetta, K., et Agaian, S. (2009). **A lossless encryption method for medical images using edge maps**. Dans *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE*, pages 3707–3710. IEEE.

[ZigBee, 2006] ZigBee, A. (2006). **Zigbee-2006 specification**. *http ://www. zigbee. org/*.

[Zimmer et al., 2010] Zimmer, C., Bhat, B., Mueller, F., et Mohan, S. (2010). **Time-based intrusion detection in cyber-physical systems**. Dans *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*, pages 109–118. ACM.

TABLE DES FIGURES

LISTE DES TABLES

Document réalisé avec LaTeX et :
le style LaTeX pour Thèse de Doctorat créé par S. Galland — http://www.multiagent.fr/ThesisStyle
la collection de paquets `tex-upmethodology` — http://www.arakhne.org/tex-upmethodology/