Optical Image encryption based on apertured FrMT in the Diffraction domain

Mengmeng Wang

THESIS

Pour l'obtention du Grade de
DOCTEUR DE L'UNIVERSITE DE POITIERS

(Faculté des Sciences Fondamentales et Appliquées)
(Diplôme National - Arrêté du 25 mai 2016)

Ecole Doctorale: SISMI

Secteur de Recherche: Traitement du Signal et des images

Présentée par: Mengmeng WANG

……

****

Optical image encryption based on apertured fractional Mellin transform in the diffraction domain

****

Directeur de thèse Yannis POUSSET, Clency PERRINE
Co-Directeur de thèse Jianhua WU, Nanrun ZHOU

****

Soutenue le 18 décembre 2019

devant la Commission d'Examen

****

JURY

LIU Zhengjun Rapporteur, Harbin institute of Technology (China)
CHARRIER Christophe Rapporteur, GREYC lab. Université de Normandie
COUDOUX François Xavier, IEMN-Université Polytechnique de Haut de France
Yannis POUSSET Directeur de thèse, Université de Poitiers
Nanrun ZHOU Co-Directeur de thèse, Nanchang University (China)
Clency PERRINE Co-encadrant de thèse, Université de Poitiers
Philippe CARRE Examinateur, Université de Poitiers

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 65,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 150 figures.

Mengmeng WANG

December 2019

Acknowledgements

Firstly, I would like to express my sincere gratitude to all my supervisors, professor Yannis POUSSET, professor Philippe CARRE, and accociate professor Clency PERRINE as well as professor Jianhua WU and professor Nanrun ZHOU. They always gave me great help by providing consistent and illuminating guidances during my PhD's studies. Without their encouragement and help, this thesis could not have reached its present form. Secondly, I would like to thank University of Poitiers and Nanchang University for giving me the opportunity and financial support of taking part in joint training of PhD thesis. Thirdly, I also show my appreciation to all the colleagues in Xlim institute of University of Poitiers and colleagues in department of information electronic engineering of Nanchang University.

I would like to express my special gratitude to my beloved family. My parents, Wang Henglu and Wang Chunju, always give me ceaseless care and support. I also feel grateful to my grandmother and little sister for their encouragement. I always obtain comfort from their unconditional love when I'm stuck in the place of feeling down.

Last but not least, I would like to thank my friends and classmates for their help in my study and life. Special thanks to Yu Fan, Xinwen Xie, Hai Liu, Sihang Liu, Weiping Zhou and Jiahan Liu for their help in my study and life.

This work was partially financed by the National Natural Science Foundation of China (grant numbers 61662047, 61861029).

Abstract

Apertures are not considered in most existing optical image encryption systems. However, apertures always exist in most practical optical systems. Hence, this thesis focuses on the study of introducing the aperture into optical fractional Mellin transform (FrMT) and its application in optical image encryption system. The feasibility of the proposed encryption schemes is verified by a series of numerical simulations. The main work is as follows:

Firstly, an optical image encryption scheme based on the fractional Mellin transform with a hard aperture has been proposed. The apertured fractional Mellin transform (apertured FrMT) can be performed through the log-polar transform and the optical apertured fractional Fourier transform. The side-lengths of the hard aperture serve as a key to improve the security and further increase the key space of the encryption system. This hard aperture is not only used to control the amount of light passing the lens by adjusting its size, but also reduces the leakage of light, which will, to some extent, enhance the robustness against direct attacks.

Secondly, the Gaussian aperture, as a soft aperture for balancing between hard aperture and no aperture, is introduced into the apertured FrMT. With the Gaussian apertured FrMT in diffraction domain, a reality-preserving transform is proposed and used for image encryption. In this encryption scheme, for gray image, the Arnold transform and the bitwise XOR operation are also adopted to encrypt the image in order to enhance the security.

Finally, the encryption algorithm based on Gaussian apertured reality-preserving FrMT (GARPFrMT) used for color image is proposed. Besides, nonlinear GARPFrMT, color space rotation, together with 3D scrambling and bitwise XOR operation make the proposed color image encryption algorithm have good performance.

The simulation results have shown that the proposed encryption schemes are capable of resisting different common attacks and robust against noise and occlusion attacks.

Keywords: Optical image encryption, hard aperture, Gaussian aperture, Collins

diffraction, nonlinear apertured FrMT, fractional Fourier transform, phase coding, real cipher-text, nonlinear Gaussian apertured reality-preserving FrMT, Arnold transform; bitwise XOR.

Résumé

Les apertures ne sont pas considérées dans la plupart des systèmes d'encryption des images opticaux. Mais en fait, des apertures toujours existent dans la plupart des systèmes opticaux. Cette thèse se concentre sur l'étude de l'introduction de l'ouverture dans la transformation frationnelle de Mellin (TFrM) dans le domaine de diffraction et son application dans le système de cryptage d'images optiques. La faisabilité des schémas de cryptage proposés est vérifiée par une série de simulations numériques. Les travaux principaux sont les suivants:

Tout d'abord, un système de cryptage d'images optiques basé sur la transformation fractionnelle de Mellin avec une ouverture dure (TFrM à ouverture dure) a été proposé. La TFrM à ouverture dure peut être effectuée par la transformation log-polar et la transformation fractionnelle de Fourier à ouverture dans le domaine de diffraction. Les longueurs latérales de l'ouverture dure servent de clé pour améliorer la sécurité et augmenter encore l'espace clé du système de cryptage. Cette ouverture dure n'est pas seulement utilisée pour contrôler la quantité de lumière passant la lentille en ajustant sa taille, mais réduit également la fuite de lumière, ce qui, dans une certaine mesure, améliorera la robustesse contre les attaques directes.

Deuxièmement, l'ouverture gaussienne, comme une ouverture douce pour équilibrer entre l'ouverture dure et aucune ouverture, est introduite dans la TFrM à ouverture. Avec la TFrM à ouverture gaussienne dans le domaine de diffraction, une transformation de préservation de la réalité est proposée et utilisée pour cryptage d'images. Dans ce schéma de cryptage pour l'image en niveaux de gris, la transformation d'Arnold et l'opération d'XOR bitwise sont également adoptées pour cypter l'image afin d'améliorer la sécurité.

Enfin, l'algorithme de cryptage basé sur la TFrM à ouverture gaussian et de préservation de la réalité (TFrMOGPR) utilisé pour l'image couleur est proposé. Outre TFrMOGPR non linéaire, rotation de l'espace couleur, avec brouillage 3D et XOR

opération bitwise rend l'algorithme de cryptage d'image de couleur proposé bien performer.

Les résultats de la simulation ont montré que les systèmes de cryptage proposés sont capables de résister à différentes attaques communes et robustes contre les attaques de bruit et d'occlusion.

Mots-clés: Cyptage d'image optique, ouverture dure, ouverture gaussianne, diffraction de Collins, TFrM à ouverture non linéaire, transformation fractionnelle de Fourier, codage de phase, ciphertext réel, TFrM non linéaire à ouverture gaussian et de préservation de la réalité, transformation d’Arnold, XOR bitwise.

Table of contents

List of figures

List of tables

Chapter 1 Introduction

1.1 Context and motivation

Multimedia and network technique have been extensively involved in all aspects of life, and modern life has already entered an information age. It is inevitable for business, accounting, finance, education, health care and more areas to use the internet to transfer information in extremely productive ways. With the rapid development of computer and information technology in recent years, the forms of information expression turn out to be various and complex, among which, the expression of image information is widely used due to its strong intuitiveness and comprehensiveness. Hence, most information that we can access to each day is presented in the form of images [1]. Images as one of the most important carriers of information may involve personal privacy, business secrets, medical history, e-banking transactions, records etc. However, image information including personal and business privacy may be stolen by illegal users during transmission process in network, which causes information to be tampered, distributed illegally and revealed. Consequently, how to solve the security issues transmission or storage has become a great concern. Information security techniques have become a key technology for protecting digital information from harming and discriminating users' legal identity in the huge internet digital information society today. In fact, the network interaction between the sender and receiver must be confidential communication [2]. Image encryption technology is used to change the image from regular data state to unrecognizable one. Unlike text information, digital image has high redundancy and human eye recognition for gray scale is limited, hence, it is allowed that the digital image is distorted to some extent. Therefore, in view of some characteristics of digital image, the research on image encryption system can make the transmission technology of data encryption meet people’s expectations and demands for communication security, which has a very important social and economic significance.

The image encryption technology based on optical theory and method is an

interdisciplinary subject that rises in recent years due to its inherent distinctive characteristics, such as ability to process data in parallel and multi-dimensions [3-7]. In an optical system, all pixels in a two-dimensional image can be propagated and processed synchronously. The optical encryption device has more freedom than electronic encryption, and the information may be hidden in multiple freedoms. By calculation of the light interference, diffraction, filtering, imaging, holography and other processes, the involved wavelength, focal distance, amplitude, light intensity, phase, polarization, spatial frequency and optical element parameters are encoded to realize multi-encryption [3-8]. Hence, compared with traditional information security techniques based on computer cryptology, optical image encryption has significant advantages. What's more, the optical encryption systems can be implemented not only by optical methods but also by digital cryptographic algorithms and systems based on the optical theory.

The optical image encryption system has been widely used and analyzed since double random phase encoding (DRPE) was first introduced into encryption system in 1995 [9], which greatly promotes the development of image encryption in optics field [3-12]. Some typically optical encryption systems in different domains have been proposed over the years, such as the Fourier transform (FT) [13-15], factional Fourier transform (FrFT) [16-22], Fresnel transform (FsT) [23-24], fractional Mellin transform (FrMT) [26-28], fractional random transform (FrRT) [29], canonical transform (LCT) [30], fractional cosine transform (FrCT) [31-35], fractional wavelet transform [36] and gyrator transform (GT) domains [37-39, 77].

The encryption algorithms based on FrFT have been a research hotspot, in which there have already many fruitful research results. There is a close relationship between the FrFT and Fresnel diffraction because the FrFT can be performed by Fresnel transform, which makes the FrFT be realized by optical methods. For the optical systems with lens, the FrFT can be achieved with the propagation of light wave and the Fourier lens. The lens is basic component in optical imaging and information processing systems, and the Fourier transform characteristics of lens is the basics of optical information processing, which makes the Fourier analysis effectively be applied in information optics. Hence, various encryption algorithms based on the optical FrFT have been proposed due to its representation property both in space and frequency domains with different orders. Generally, there are no apertures in optical image encryption systems. However, in practice, apertures always exist in most optical

systems, such as the finite size of lens [40]. The implementation of the aperture can facilitate the reduction and control of light leakage in optical systems. Therefore, it is necessary and practical to analyze the performance of optical encryption systems with aperture. At the same time, to some extent, the linear FrFT-based encryption system has some potential security risks [41-42]. To avoid the disadvantages stemming from the linearity of classical optical system, it is also necessary to choose a nonlinear transform suitable for optical image encryption. The image encryption schemes proposed by Zhou are implemented by digital encryption algorithms, such as discrete fractional Fourier transform (DFrFT), reality-preserving transform in DFrFT domain [25-28], which does not fully demonstrate the characteristics of optical encryption. FrMT can be realized by log-polar transform and the fractional Fourier transform as shown in Fig. 1.1. Due to the nonlinearity of log-polar transform, FrMT also owns the nonlinear property, which reduces the potential insecurity caused by linear optical system. Thus, in this thesis, we focus on the apertured FrMT in diffraction domain and try to design new optical encryption algorithms in FrMT domain to encrypt the image.

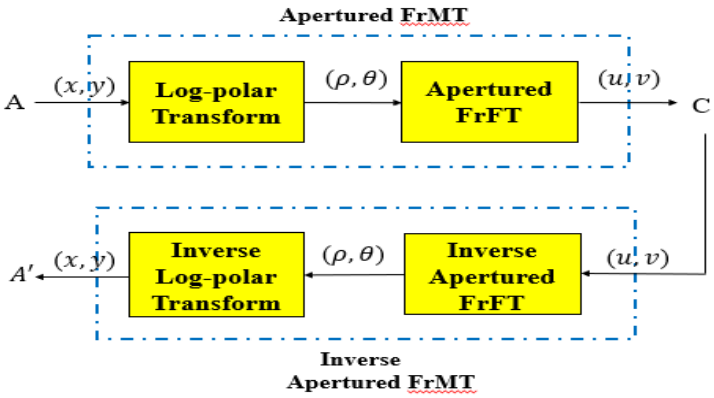


Fig. 1.1 Chart for performing apertured FrMT and its inverse.

1.2 Purpose of the thesis

Based on the theories of image encryption, FrFT, Collins diffraction, apertured FrFT, reality-preserving transform, chaotic map and evaluation criterion of image encryption, the thesis studies the apertured FrMT, the reality-preserving apertured FrMT and its application in optical image encryption. The main purposes of the thesis are as follows:

1. Design of an apertured nonlinear fractional Mellin transform. The log-polar transform and Collins diffraction equations with rectangle or circular hard aperture is utilized to perform apertured FrMT.

2. A new optical image encryption scheme based on apertured FrMT. An optical encryption algorithm based on apertured FrMT is designed. The influence of the size of the hard aperture on the key space will be analyzed. At the same time, the size of the hard aperture and the wavelength are designed as keys to increase the security of the encryption algorithm. The performance of the encryption algorithm will be analyzed.

3. An image encryption scheme based on Gaussian apertured reality-preserving FrMT (GARPFrMT). A Gaussian aperture, like a soft aperture, is designed to perform Gaussian apertured FrMT to improve the amount of light that passes through the lens. What's more, the reality-preserving transform in the diffraction domain will be constructed to ensure that the cipher-text is real, which is of convenience in display, transmission and storage.

4. A color image encryption scheme based on GARPFrMT. The proposed GARPFrMT will be used in color image encryption algorithm to test its implementation in a three-channel optical system. The 3D logistic map serves to scramble the three channels. The simulation results of the proposed algorithm will be analyzed and discussed.

1.3 Thesis organization

This thesis is organized as follows: Chapter 2 provides fundamentals and the evaluation criterion of image encryption algorithm, the principles of the FrFT, chaotic system, fractional Fourier transform, Fresnel diffraction integral, apertured FrFT, Mellin and fractional Mellin transforms.

Chapter 3 proposes a new optical image encryption scheme based on apertured fractional Mellin transform. The apertured FrMT is performed by the log-polar transform and Collins diffraction equations with rectangle or circular hard aperture. The side-length of hard aperture is designed as the cipher key, and the influence of the side-length on the key space will be analyzed. The experimental results are analyzed and discussed, and the summary is presented at the end of the chapter.

Chapter 4 constructs the Gaussian apertured reality-preserving FrMT in the diffraction domain. An optical image encryption scheme based on GARPFrMT is proposed to improve the amount of light that passes through the lens and ensures that the cipher-text is real. And the GARPFrMT is extended to color image encryption

scheme. The simulation results verify the performance of the encryption algorithms.

Finally, the conclusion and perspective are drawn in Chapter 5.

Chapter 2 Fundamentals

Optical image encryption technology has attracted more and more attention of research due to its inherent distinctive characteristics, such as the ability of high speed for processing data in parallel. Compared with mathematical traditional information security and the computer cryptology, optical image encryption has many advantages, such as multi-dimensions, high-capacity, high design freedom, high robustness, parallelism and difficult to break [3]. This chapter introduces the image encryption theory, the research status of image encryption technology and the basic knowledge of image encryption. Due to the lack of space of thesis, the knowledge closely related to subsequent chapters is introduced briefly.

This chapter is arranged as follows: Section 2.1 introduces the image encryption theory and research status of image encryption. Section 2.2 gives the evaluation criterions of image encryption algorithm. Section 2.3 describes the chaotic logistic maps briefly. The fractional Fourier transform is described in Section 2.4. The fractional Mellin transform is reviewed in Section 2.5. Section 2.6 summarizes the chapter.

2.1 Image encryption theory and research status

2.1.1 Image encryption theory

Image encryption technology is used to convert the original (plaintext) image to unrecognized quasi-random noise information, which protects effectively the image information. Researchers have proposed various image encryption methods with different safety performance. However, no matter which encryption method is utilized, the encryption results will fall into the following three categories: (1) Scrambling encryption. Scrambling encryption is the rearrangement of image pixels in space to convert the original image to be meaninglessly confused image. (2) Gray encryption. The encryption with only gray value change is called gray encryption. (3) Hybrid encryption. Hybrid encryption is the change of both the pixel position and the gray value.

2.1.2 Research status of optical image encryption

In optical encryption and decryption security field, in 1995, Refregier and Javidi [9] from University of Connecticut, United States, first proposed an optical image encryption method based on input plane and Fourier plane random encoding (double random plane encryption, DRPE), as shown in Fig. 2.1. In DRPE optical security system, the encrypted image can be obtained by using double random phase masks placed standard $4f$ optical signal processor. Let 2D random phases $\exp[\mathrm{i}\alpha(x,y)]$ and $\exp[\mathrm{i}\beta(x,y)]$ denote masks 1 and 2, where $\mathrm{i}=\sqrt{-1}$, the two random phases are in the range of $[0,2\pi]$. First, the image $f(x,y)$ is multiplied by mask 1 placed in the input plane

$$P(x,y)=f(x,y)\exp[\mathrm{i}\alpha(x,y)] \tag{2.1}$$

Then $P(x,y)$ is modulated by mask 2 located in the Fourier domain

$$H(u,v)=\mathrm{FT}\{P(x,y)\}\exp[\mathrm{i}\beta(u,v)] \tag{2.2}$$

Finally, the inverse Fourier transform (IFT) is performed, and the encoded image is captured by a CCD photo detector.

$$O(\xi,\eta)=\mathrm{IFT}\{H(u,v)\} \tag{2.3}$$

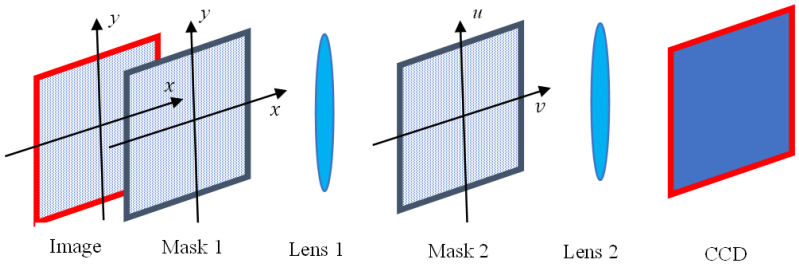


Fig. 2.1 DRPE optical security system [4]

Since DRPE was proposed by Refregier and Javidi, the optical security technology has become a very active area of image encryption [43-45]. Javidi and Nomura [46], in 2000, proposed an information encryption way based on the digital holographic and DRPE techniques. This security system allows the encrypted information to be stored, transmitted and decrypted digitally. Tajahuerce et al. [47] proposed an optoelectronic encryption method by combining the DRPE and digital phase-shifting interferometry, which makes the use of CCD capabilities more effectively and the complex information recorded fully. This technology also described the encryption process in the Fraunhofer or Fresnel diffraction domain.

In reality, the DRPE system are also used in different transform domains [11, 17-18, 24, 39, 47-49], such as the Fresnel, gyrator and fractional Fourier transform domains.

Situ and Zhang, in 2004, proposed an optical encryption system using DRPE in Fresnel domain. In this security system, except the phase codes, the positions of the planes and the wavelength served as keys as well to achieve a higher security. In 2006, Chen and Zhao [49] proposed an encryption method for color images based on DRPE algorithm in Fresnel domain using wavelength multiplexing. Unnikrishnan [17], in 2000, proposed an optical architecture in fractional Fourier domain based on DRPE to convert the image into stationary white noise. Since this architecture was performed in fractional domain instead of Fourier domain, the orders of FrFT serve as keys, which further improves the security of the optical encryption system. Chen and Chang et al., in 2017, proposed an optical image conversion and encryption method by diffraction, phase retrieval and incoherent superposition in Fresnel domain. This method used phase iterative algorithms, which can greatly increase the system security.

However, it is proved that DRPE could be attacked under some conditions [51-53]. Therefore, many researchers have proposed various image encryption methods by combining DRPE and other algorithms to enhance the security of schemes. Singh and Sinha [30] proposed a multiple image encryption algorithm based on random phase masks generated by chaotic maps in canonical domain. This encryption algorithm combined the Kaplan-Yorke map and random phase masks to effectively enhance the key space. A double image encryption algorithm by utilizing an iterative random binary encoding in gyrator domain was proposed by Liu [48]. An information hiding method using DRPE and public-key cryptography was proposed by Sheng [54], which combines the complementary advantages of DPRE and Rivest-SHAMIR-Adleman encryption algorithms to improve the performance of security. Liu and Yu et al. [56] proposed encryption algorithm using cascaded FrFT and random phase filtering. Han [57] proposed an optical encryption method based on the exclusive-OR (XOR) operation and constructed an optical security system to perform the XOR operation.

By referring to the encryption methods using fractional Fourier transform, the concept of fractional order transform was generalized to design new image encryption technologies. Zhao and Li et al. [58], in 2009, proposed an optical encryption algorithm based on 2D generalization of the redefined fractional Hartley transform (FrHT) [22, 59-60, 81]. This encryption algorithm encrypted image using two fractional orders of FrHT and random phase codes (RPC). In addition, the fractional orders served as additional keys, which strengthened image security, and the feasibility of the proposed method was confirmed by computer simulations. Singh [79], in 2017, proposed an

optical encryption scheme in FrHT domain using Arnold transform and singular value decomposition. An optical image encryption method by combining Hartley transform (HT) and logistic map was proposed by Singh in 2009 [60]. This proposed technique using HT with jigsaw transform to solve the problem of bare decryption with HT, and the optical implementation of HT was given. The logistic map was used to generate chaotic random intensity mask. Ozaktas and Mendlovic et al. gave the relationship between the FrFT and wavelet transform (WT) in 1994 [61]. Mendlovic [62], in 1997, proposed the concept of fractional wavelet transform (FrWT) using association with both the wavelet transform and the fractional Fourier transform. And the optical implementation of the FrWT was given as well. A novel optical image encryption scheme using FrWT was proposed by Chen and Zhao in 2005 [36]. This novel method based on FrWT used the fractional orders and a range of scaling factors as keys. The image could be recovered only with all of these correct keys. At the same time, this method can also achieve the partial image encryption. Liu [78], in 2018, proposed an optical encryption based on compressed sensing in FrWT domain. Wu et al. [33-34, 63-64], proposed the encryption methods based on fractional cosine transforms (FrCT). Due to the relationship between the cosine transform and Fourier transform, the FrCT can be realized by optical implementation. In Wu's methods, the FrCT was often combined with logistic maps to enhance the security.

Many image coding algorithms using optical interference technique were also proposed recently [65-70]. Niu [65], in 2010, proposed an encryption and verification algorithm using interference principle. This encryption process encodes two different images into three diffractive phase elements, and the wavelengths and distance parameters serve as keys. Cai [66], in 2015, proposed an asymmetric optical encryption method using coherent superposition. The equal modulus decomposition was used to construct a sufficient trapdoor one-way function to achieve a high robustness. An optical color image encryption based on phase-only encoding was proposed by Liu [67] in 2015. The components of color image were encoded into three phase masks using phase retrieval algorithm, and then the masks were placed in the input of Fresnel domains of three channels. The physical parameters of the optical system were used as keys. Due to the complex-value of output of most optical transform, the phase retrieval algorithm was applied into encryption schemes [12, 74-75]. Wang and Zhao [15], in 2011, proposed a multiple-image encryption using amplitude-truncation and phase-truncation. The phase truncated from complex-value based on Rivest-SHAMIR-

Adelman algorithm was used as public keys. Wang [76], in 2014, proposed an optical asymmetric cryptosystem using phase-truncation in Fourier transform. The decryption keys were truncated from cypher text using modified amplitude-phase retrieval algorithm. An optical image encryption algorithm using phase retrieval algorithm in diffraction domain was proposed by Chen in 2017 [12]. Verma et al., in 2019, proposed an optical encryption algorithm using the phase retrieval and phase-truncated Fourier transforms.

The optical encryption systems can be implemented not only by optical methods but also by digital cryptographic algorithms and systems based on the optical theory. Pei et al. [80-88] proposed a series of discrete domains and its computation algorithms, such as discrete fractional cosine transform (DFrCT) and discrete fractional sine transforms (DFrST), discrete fractional Hartley transform, multiple-parameter discrete fractional Fourier transform [25-28, 88-92], random discrete fractional Fourier transform, which greatly improves the development of encryption algorithms. Liu [70-71] proposed a discrete random transform based on FrFT, which inherits the properties of discrete fractional Fourier. And Liu, in 2006, proposed an encryption scheme using discrete random cosine/sine transform.

To solve inconvenience for storage, transmission, or display caused by complex-value optical transforms, the reality-preserving transform was proposed in discrete domain [28, 63, 93-95]. Zhou [28], in 2012, proposed a color image encryption using reality-preserving FrMT. Wu [63], in 2013, proposed an image encryption scheme using a reality-preserving DFrCT. A color image encryption based on reality-preserving multiple-parameter FrFT was proposed by Lang in 2015 [94]. Zhao [58] proposed an optical image encryption scheme using redefined FrHT in 2008. The value of input and output are real, which is convenient for record, transmission and print. And the implementation of optical encryption system was proposed as well.

In recent years, the logistic maps have been used in image encryption [96-104]. Pareek [104], in 2006, proposed an image encryption algorithm based on logistic maps. In the proposed encryption, two logistic maps with an external secret key of 80 bits were used to meet the requirements of security. Many novel chaotic logistic maps were designed and applied in image encryption, such as logistic map, sine map, tent map, logistic-tent map, 2D logistic-sine map, 3D logistic map etc. [105-106].

In fact, most encryption algorithms based on FrFT optical systems are linear, which have some potential security risks to some extent [28]. Consequently, some nonlinear

encryption methods were proposed [15, 25-28, 107-109]. Liu [15] proposed a nonlinear phase-truncation algorithm for image encryption. Joshi [109] proposed a nonlinear image encryption scheme for color images, using natural logarithms and FrFT. Zhou et al. proposed a series of image encryption methods based on FrMT. Besides, the image encryption technique also combines with compressive sensing and a lot of results are published [27, 98, 110-113]. From above reviews, we can know that the image encryption technique has had a lot of research results with very important practical significance.

2.2 Evaluation criterion of image encryption

It is necessary to test the encryption system's performance with statistical analyses. Those analysis methods are utilized to look for the internal relationship between the original image and the encrypted image. A good encryption algorithm can resist the statistical attacks. The common statistical analysis methods including histogram analysis, information entropy analysis, and correlation analysis. Besides statistical analyses, some other analyses are also very important for encryption systems, including the mean square error (MSE), logarithm of mean square error (LMSE), key space analysis and robustness analysis (such as noise and occlusion attacks).

2.2.1 Histogram analysis

The histogram is a very important analysis method used to describe the number of pixels in the image with different gray levels and their frequency of occurrence. The histograms of the original images usually are different, while those of cipher images obey a uniform distribution, by which the attackers cannot obtain useful information.

2.2.2 Information entropy analysis

In 1948, Shannon [114] proposed the concept of information entropy which is used to describe how random the texture of an image is. Information entropy H solves the problem of quantification of information and is defined as

$$H = \sum_{i=1}^{n} P(x_i)\log_2 P(x_i) \tag{2.4}$$

where $P(x_i)$ represents the probability of the occurrence of the pixels x_i for an n-gray level image. The value of information entropy is maximum $\log_2 n$ when the

probability of the occurrence of every gray level is equal: $P(x_1) = P(x_2) = \cdots = P(x_n) = 1/n$. For example, the maximum is 8 for the encryption of a 256-graylevel image. It is useless trying to attack the information entropy when the gray values of encryption image follow a uniform distribution.

2.2.3 Correlation analysis

There exist strong neighborhood correlations between adjacent pixels for the original images. However, to be secure and efficient, those neighborhood correlations should not exist for encrypted images. Therefore, it is necessary to perform a correlation analysis on adjacent image pixels in cipher and plain images. The correlation coefficient is defined as [115-116]

$$C = \frac{\sum_{i=1}^{N_1}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{N_1}(x_i - \bar{x})^2 (y_i - \bar{y})^2}} \tag{2.5}$$

where $\bar{x} = \frac{1}{N_1}\sum_{i=1}^{N_1} x_i$ and $\bar{y} = \frac{1}{N_1}\sum_{i=1}^{N_1} y_i$, N_1 denotes the number of adjacent pixel pairs chosen in the horizontal, vertical, and diagonal directions. The adjacent pixels have the strongest correlation when the coefficient C is equal to 1, whereas, for $C = 0$, those have no correlation. Thus, the closer the correlation coefficients of encryption images get to 0, the safer it is.

2.2.3 Mean square error and logarithm of mean square error

To measure the similarity between the original image and the decrypted image, the mean square error (MSE) and logarithm of mean square error (LMSE) are introduced to evaluate the quality of the decrypted images.

MSE is defined as [117]

$$\mathrm{MSE} = \frac{1}{M_1 M_2}\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[f(i,j) - f'(i,j)]^2 \tag{2.6}$$

where $f(i,j)$ denotes the original image pixel, $f'(i,j)$ is the pixel of the decrypted image, $M_1 \times M_2$ are the size of original and decrypted images.

LMSE is defined as

$$\mathrm{LMSE} = \log_{10}\left\{\frac{1}{M_1 M_2}\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[f(i,j) - f'(i,j)]^2\right\} \tag{2.7}$$

2.2.4 NPCR and UACI

The attackers always try to find the relationship between two encrypted images whose original images have a 1-bit pixel difference by differential attack to obtain useful information. Thus, a reliable and secure encryption algorithm should be very sensitive to small change in the plain images. The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are two commonly used quantities to test the ability of an encryption algorithm to resist differential attacks. The NPCR and the UACI are, respectively, represented as [116-117]

$$\mathrm{NPCR} = \sum_{i=1}^{M_1}\sum_{j=1}^{M_2} D(i,j) \times \frac{100\%}{M_1 \times M_2} \tag{2.8}$$

$$\mathrm{UACI} = \left[\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times \frac{100\%}{M_1 \times M_2}\right] \tag{2.9}$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j); \\ 1, & C_1(i,j) \neq C_2(i,j). \end{cases} \tag{2.10}$$

where $D(i,j)$ is a bipolar. $C_1(i,j)$ and $C_2(i,j)$ are pixel values of encrypted images of size $M_1 \times M_2$, whose original images have a 1-bit pixel difference.

For an ideal encryption system, the expected NPCR and UACI values of two arbitrary images can be obtained by the following equations:

$$\mathrm{NPCR_E} = (1 - 2^{-t}) \times 100\% \tag{2.11}$$

$$\mathrm{UACI_E} = \frac{1}{2^{2t}} \frac{\sum_{i=1}^{2^t-1} i(i+1)}{2^t} \times 100\% \tag{2.12}$$

where *t* represents the number of grayscales of the image. For an 8-bit grayscale image, the $\mathrm{NPCR_E}$ and $\mathrm{UACI_E}$ are 96.6094% and 33.4635%, respectively, which means that it is useless that the attackers analyze images by using differential attacks.

2.2.5 Robustness analysis

Robustness is used to measure a system's ability that withstands or overcomes adverse conditions. In practical, since the cipher images are easily affected by noise and data loss during transmission and processing, it is necessary to measure the robustness of the proposed image encryption algorithm, noting that noise attack and occlusion

attack are two effective assessment methods.

The image usually is polluted by noise, like Gaussian noise and salt & peppers noise, during its collection, acquisition and transmission. Thus, a good encryption system must have an ability to resist noise interference, which means that although the encryption image to some extent was polluted with noise, the main information still can be obtained and recognizable with correct keys.

It is possible that the received and decrypted image comes across data loss due to network interruption or link congestion during signal transmission process. Therefore, it is necessary to study the effect of occlusion attacks on encrypted images. The encryption system is considered as a good one if the partially cropped cipher-text can be recovered to some extent with correct keys.

2.3 Chaotic logistic maps

Chaotic phenomenon is a kind of aperiodic, random-like, chance or irregular movement in deterministic system, which widely appears in the real world. Although chaotic phenomenon can be described in a nonlinear deterministic system, its behavior shows uncertainty, not repeatability and unpredictability. Generally, chaos stems from nonlinear dynamical system and nonlinear dynamical equation. In discrete domain, chaos can be shown as follows:

$$x_{n+1} = F(x_n), n = 0, 1, \ldots \tag{2.13}$$

where F can represent the nonlinear function. This dynamical equation that is regarded as an iterative one may be performed repeatedly, in which the result of each iteration is used as the initial value for the next iteration shown as follows:

$$x_n = F_n\left(F_{n-1}\left(F_{n-2}\cdots F_0(x_0)\right)\right) \tag{2.14}$$

In some cases, the behavior of the obtained sequence $\{x_0, x_1, \cdots x_{n+1}\}$ will be extremely complex. Chaos has been widely used in information encryption systems due to its several basic features: initial value sensitivity, parameter sensitivity, inherent randomness, and boundedness.

(1) Initial value sensitivity and parameter sensitivity

The motion trajectory of chaotic system is impacted intensely by the selected initial

value or control parameter. The final result swings wildly in response to even a little change in initial value due to the magnifying effects of iteration equation.

(2) Inherent randomness

There exists pseudo randomness for inner behavior of the chaotic system, which is independent of the external environment.

(3) Boundedness

Although chaotic system is extremely unstable, its motion trajectory is always limited to a certain area. In other words, the motion trajectory is never out of system's scoped areas, no matter how drastic the internal changes are.

In image encryption systems, several commonly-adopted chaotic maps are shown as follows.

2.3.1 Logistic map

The logistic map is a simple dynamic and widely used equation to produce a numerical sequence with a complex behavior, which is defined as [98, 117]:

$$x_{l+1} = \mu x_l(1 - x_l) \tag{2.15}$$

where the iterative value x_l belongs to (0, 1), $\mu \in (0, 4]$ is system parameter. It can be seen that the logistic map is chaotic when μ is within $[3.5699456, 4]$ as shown in Fig. 2.2.

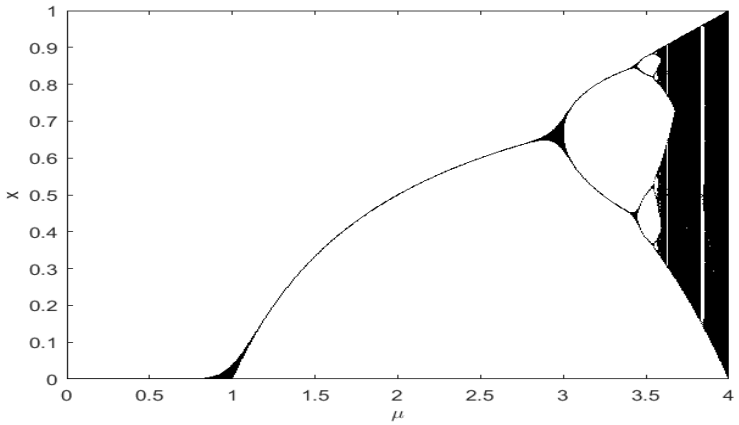


Fig. 2.2 The bifurcation diagram for the logistic map.

2.3.2 Tent map

A tent map is a common 1-D nonlinear chaotic map, which is defined as:

$$x_{n+1} = \begin{cases} \dfrac{\mu x_n}{2}, & x \le \dfrac{1}{2} \\ \dfrac{\mu(1-x_n)}{2}, & x > \dfrac{1}{2} \end{cases} \tag{2.16}$$

where the parameter $\mu \in (0, 4]$. The shape of tent map is like a tent in its bifurcation diagram as shown in Fig. 2.3 [119].

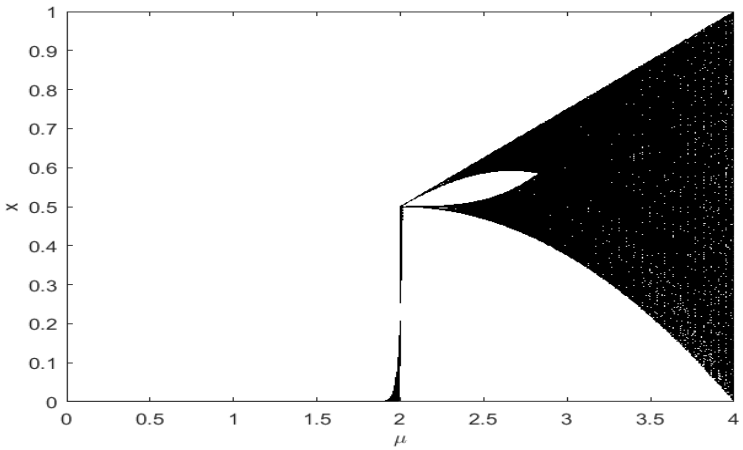


Fig. 2.3 The bifurcation diagram for the tent map.

2.3.3 Sine map

The behavior of sine system is similar with those of logistic or tent system as shown in Fig. 2.4 [105, 117]. The sine map is defined as:

$$x_{n+1} = \frac{\mu \sin(\pi x_n)}{4} \tag{2.17}$$

where the parameter $\mu \in (0, 4]$.

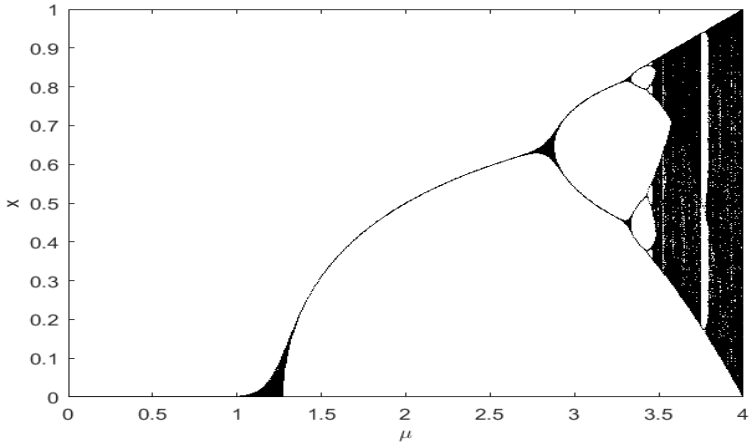


Fig. 2.4 The bifurcation diagram for the sine map.

There are two problems in logistic and tent maps: (1) the chaotic range is limited, (2) the distribution of the variant density function is non-uniform. Therefore, [120] introduces several compound chaotic systems based on multiple model with excellent performance.

2.3.4 Logistic-tent map

The logistic-tent map is derived from logistic and tent maps, and its mathematical definition is given by [120]

$$x_{n+1} = \begin{cases} \left(rx_n(1-x_n) + \dfrac{(4-\mu)x_n}{2}\right) \bmod 1, & x < 1/2 \\ \left(rx_n(1-x_n) + \dfrac{(4-\mu)(1-x_n)}{2}\right) \bmod 1, & x \geq 1/2 \end{cases} \tag{2.18}$$

where the parameter $\mu \in (0, 4]$, the operator 'mod' represents the modulo operation. The bifurcation diagram is shown in Fig. 2.5. It can be seen that its chaotic range is within (0, 4], which extends far beyond those of the logistic or tent maps. Besides, its iteration results uniformly distribute within [0, 1].

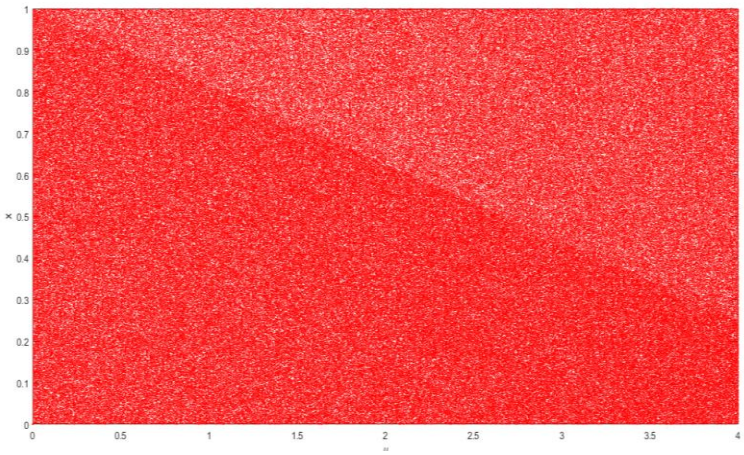


Fig. 2.5 The bifurcation diagram of the logistic-tent.

2.3.5 Logistic-sine map

The logistic-sine system is obtained by logistic map and sine map, as defined [120]:

$$x_{n+1} = \left(\mu x_n(1-x_n) + \frac{(4-\mu)\sin(\pi x_n)}{4}\right) \bmod 1 \tag{2.19}$$

where the parameter μ is within (0, 4]. Fig. 2.6 shows the bifurcation diagram of

logistic-sine, from which it can be seen that its chaotic behaviors exist within the whole range (0, 4] and the output sequences distribute within [0, 1] uniformly.

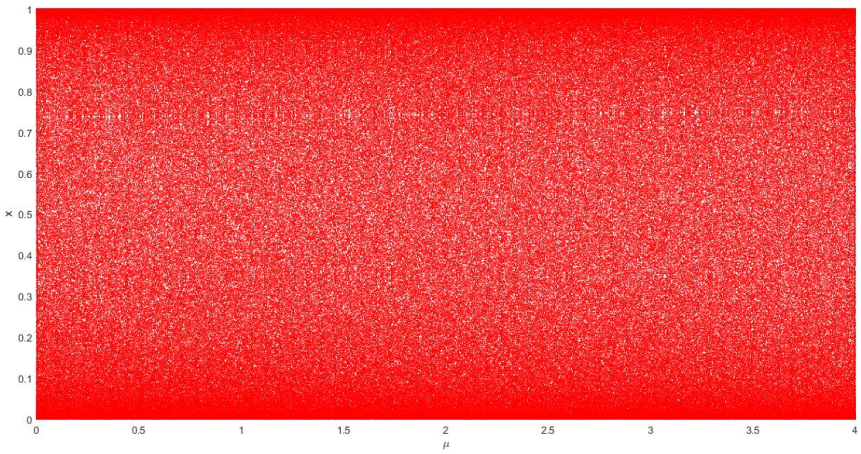


Fig. 2.6 The bifurcation diagram of the logistic-sine.

2.3.6 2D logistic map

The definition of 2D-dimensional Logistic system is as follows [121]

$$\begin{cases} x_{l+1} = \mu_l x_l(1 - x_l) + \gamma_1 y_l^2 \\ y_{l+1} = \mu_2 y_l(1 - y_l) + \gamma_2(x_l^2 + x_l y_l) \end{cases} \tag{2.20}$$

where x_l, y_l belong to (0, 1), l=0, 1, 2…, and μ_1, μ_2, γ_1, γ_2 are the system parameters. If the following conditions are met: $2.75 < \mu_1 < 3.4$, $2.75 < \mu_2 < 3.45$, $0.15 < \gamma_1 < 0.21$, $0.13 < \gamma_2 < 0.15$, then the system exhibits chaotic behavior.

2.3.7 3D logistic map

The 3D logistic system is defined as [122-123]

$$\begin{cases} x_{l+1} = \lambda x_l(1 - x_l) + \beta x_1 y_l^2 + \alpha {z_l}^3 \\ y_{l+1} = \lambda y_l(1 - y_l) + \beta y_1 z_l^2 + \alpha {x_l}^3 \\ z_{l+1} = \lambda z_l(1 - z_l) + \beta z x_l^2 + \alpha {y_l}^3 \end{cases} \tag{2.21}$$

where x_l, y_l and z_l are in the range of (0, 1), l=0, 1, 2…, and when the conditions $3.53 < \lambda < 3.81$, $0 < \beta < 0.022$, $0 < \alpha < 0.015$ are met, the system exists chaotic behavior.

2.3.8 Arnold transform

Arnold transform, a 2D chaotic map, is a widely used scrambling transformation in image encryption systems and its general form with a>0, $b > 0$ is [121]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{2.22}$$

where $[x, y]^t$ and $[x', y']^t$ are positions of an *N*-order matrix element before and after the Arnold transform, respectively, the operator 'mod' represents the modulo operation. Since maximum Lyapunov exponent of the Arnold map is $\lambda = 1 + \frac{ab+\sqrt{(ab)^2+4ab}}{2} > 1$, which makes this 2D system always exhibit chaotic behavior [121].

When a=0, $b = 1$, the transform is the common Arnold transform shown as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{2.23}$$

And its inverse transform is given as:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N \tag{2.24}$$

Arnold transform has a periodic feature, which makes the input of the transform return to its initial state after many times of iterations. Notice that the input with different size corresponds to different transformation period. For example, the period of the Arnold transform is 192 corresponding to the input with size 256×256 as shown in Table 2.1.

Table 2.1 Arnold transform period

Input size	Arnold transform period
128×128	96
256×256	192
512×512	384
1024×1024	768

2.4 Fractional Fourier transform

2.4.1 Fourier transform

The Fourier transform is a common mathematical method to analyze and synthesize signals. Any continuous sequence or signal can be expressed by superposition of sinusoidal signals with different frequencies. This method changes the signal from time domain to frequency domain. The continuous Fourier transform is defined as

$$F(\omega) = F\{f(t)\} = \int_{-\infty}^{\infty} f(t)e^{-i\omega t}\mathrm{d}t \tag{2.25}$$

where $f(t)$ and $F(\omega)$ are named the Fourier transform pair, which can describe the same physical object in different domains (the time domain or the frequency domain). The inverse Fourier transform is shown as

$$f(\omega) = F^{-1}\{f(t)\} = \frac{1}{2\pi}\int_{-\infty}^{\infty} F(\omega)e^{\mathrm{i}\omega t}\mathrm{d}\omega \tag{2.26}$$

The 2D Fourier transform is defined as

$$F(\xi,\eta) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y)\exp[-\mathrm{i}2\pi(\xi x+\eta y)]\mathrm{d}x\mathrm{d}y \tag{2.27}$$

Its inverse is

$$f(x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} F(\xi,\eta)\exp[\mathrm{i}2\pi(\xi x+\eta y)]\mathrm{d}\xi\mathrm{d}\eta \tag{2.28}$$

where x, y, ξ, η are real variables.

The discrete form of the Fourier transform can be computed quickly using a digital computer. Its fast algorithm is called fast Fourier transform (FFT). The discrete Fourier transform and its inverse for a signal with length N are defined as

$$F(k) = \frac{1}{\sqrt{N}}\sum_{n=0}^{N-1} f(n)e^{-\mathrm{i}2\pi\frac{nk}{N}}, k = 0,1,\dots,N-1 \tag{2.29}$$

$$f(n) = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} F(k)e^{\mathrm{i}2\pi\frac{nk}{N}}, n = 0,1,\dots,N-1 \tag{2.30}$$

The 2D discrete Fourier transform and its inverse for a 2D signal $f(m,n)$ are expressed as

$$F(k,l) = \frac{1}{\sqrt{M\times N}}\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} f(m,n)e^{-\mathrm{i}2\pi\left(\frac{mk}{M}+\frac{nl}{N}\right)}, k = 0,1,\dots,M-1;$$

$$l = 0,1,\dots,N-1 \tag{2.31}$$

$$f(m,n) = \frac{1}{\sqrt{M\times N}}\sum_{k=0}^{M-1}\sum_{l=0}^{N-1} F(k,l)e^{\mathrm{i}2\pi\left(\frac{mk}{M}+\frac{nl}{N}\right)}, m = 0,1,\dots,M-1;$$

$$n = 0,1,\dots,N-1 \tag{2.32}$$

The Fourier transform has linearity:

$$af_1(n) + bf_2(n) \Leftrightarrow aF_1(k) + bF_2(k) \tag{2.33}$$

The complex convolution operation can be simplified by the Fourier transform.

$$f * g = F^{-1}\{F\{f\} \cdot F\{g\}\} \tag{2.34}$$

where functions f and g are absolutely integrable.

2.4.2 Fractional Fourier transform

FrFT has found many applications in optical signal processing and encryption. The mathematical definition of FrFT was given by McBride and Kerr. Let $F^{\alpha}\{f(t)\}(u)$ denote the fractional Fourier transform of the function $f(t)$, thus the FrFT is defined as [59, 85-87]

$$F^{\alpha}\{f(t)\}(u) = \int_{-\infty}^{\infty} f(t)K_{\alpha}(u,t)\mathrm{d}t \tag{2.35}$$

where the transform kernel is given by:

$$K_{\alpha}(u,t) = \begin{cases} A_{\alpha}\exp\{\mathrm{i}\pi[(u^2+t^2)\cot\phi - 2tu\csc\phi]\}, & \phi \neq \pi, 2\pi \\ \delta(t-u), \quad \phi = 2\pi; \\ \delta(t+u), \quad \phi = \pi \end{cases} \tag{2.36}$$

and

$$A_{\alpha} = \frac{\exp\left[-\mathrm{i}(\frac{\pi\mathrm{sgn}(\phi)}{4} - \phi/2)\right]}{|\sin\phi|^{1/2}} \tag{2.37}$$

where $\phi = \alpha\pi/2$ with $0 < |\alpha| < 2$, α is the FrFT order and i is imaginary unit. If $\alpha = 1$, then Eq. (2.35) is equal to the conventional Fourier transform. Thus, FrFT can regarded as generalized Fourier transform. Since FrFT has ability to represent the signal in the spatial and frequency domains simultaneously, as the generalization of the Fourier transform, FrFT not only inherits the basic properties of the Fourier transform, but also owns the properties not available in the Fourier transform.

The 2D fractional Fourier transform with order (p_1, p_2) is [146]

$$F^{(p_1,p_2)}(u,v) = C \cdot \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y) \cdot \exp\left\{\begin{array}{c} -2\pi\mathrm{i}\left(\frac{ux}{\sin\phi_1} + \frac{vy}{\sin\phi_2}\right) \\ +\pi\mathrm{i}\left(\frac{u^2+x^2}{\tan\phi_1} + \frac{v^2+y^2}{\tan\phi_2}\right) \end{array}\right\} \mathrm{d}x\mathrm{d}y$$

(2.38)

where C is a constant, $\phi_1 = \frac{p_1\pi}{2}$, $\phi_2 = \frac{p_2\pi}{2}$. Observe that $F^{(0,0)}(u,v) = f(x,y)$, which is equal to $f(x,y)$, and $F^{(1,1)}(u,v) = F(u,v)$, which is the Fourier transform of $f(x,y)$.

The main mathematical properties of FrFT are shown as follows [125-126].

(1) Linear additivity

The linearity is a very important property for FrFT, which satisfies the superposition theorem:

$$F^{\alpha}\{c_1 f_1(t) + c_2 f_2(t)\}(u) = c_1 F^{\alpha}\{f_1(t)\} + c_2 F^{\alpha}\{f_2(t)\} \tag{2.39}$$

where c_1, c_2 are complex constants, $f_1(t)$ and $f_2(t)$ are arbitrary functions, α is the order of FrFT.

(2) Fractional order additivity

The order of FrFT is additive:

$$F^{\alpha}F^{\beta} = F^{\alpha+\beta} \tag{2.40}$$

(3) Periodicity

The period of FrFT order is 4:

$$F^{\alpha+4} = F^{\alpha} \tag{2.41}$$

(4) Reversibility

FrFT owns reversibility:

$$(F^{\alpha})^{-1} = F^{-\alpha} \tag{2.42}$$

(5) Unitarity

The fractional Fourier operators are unitary:

$$(F^{\alpha})^{-1} = (F^{\alpha})^{H} \tag{2.43}$$

where *H* represents the conjugate and the transpose.

(6) Continuity

$$F^{c_1\alpha_1+c_2\alpha_2}\{f(t)\} = F^{c_1\alpha_1}F^{c_2\alpha_2}\{f(t)\} = F^{c_2\alpha_2}F^{c_1\alpha_1}\{f(t)\} \tag{2.44}$$

where c_1, $c_2 \in R$, α_1, α_2 are the orders of FrFT.

(7) Shift properties

The time shift characteristic:

$$F^{\alpha}\{f(t-m)\}(u)=\exp\left\{im\sin\left(\frac{\alpha\pi}{2}\right)\left[u-m\cos(\frac{\alpha\pi}{4})\right]\right\}\times F^{\alpha}(u-m\cos\alpha) \tag{2.45}$$

The frequency shift characteristic:

$$F^{\alpha}\{\exp(itv)\,f(t)\}(u)=\exp\left\{-iv\cos\alpha\left[\frac{v\sin\alpha}{2}+u\right]\right\}\times F^{\alpha}(u-v\sin\alpha) \tag{2.46}$$

(8) Scale property

Changing the FrFT input signal in scale not only introduces a quadratic phase related to scale factor, but also changes the order of FrFT, as shown below:

$$F^{\alpha}\{f(ct)\}(u)=\sqrt{\frac{1-i\cot\alpha}{c^2-i\cot\alpha}}\exp\left(i\frac{u}{2}\left(1-\frac{\cos^2\beta}{c\sin^2\alpha}\right)\cot\alpha\right)\times F^{\beta}\{f(x)\}\frac{\sin\beta}{c\sin\alpha}u) \tag{2.47}$$

where $c\in R^{+}$, $\beta=\arctan(c^2\tan\alpha)$.

2.4.3 Fresnel diffraction

Namias [126] established the fractional Fourier transform in 1980 and McBride and Kerr completed its theory in 1987. In the early 1990s, FrFT has been introduced into optical field. Pierre pointed that the optical fractional Fourier transform corresponds to the mathematical expression of Fresnel diffraction, just as the standard optical Fourier transform corresponds to Fraunhofer diffraction.

Within the framework of paraxial approximation, it is generally assumed that the distance Δs and angle θ of rays from the optic axis is small. As shown in Fig. 2.7 the distance from observation point *p* to diffraction aperture point *O* is indicated as:

$$L=\sqrt{d^2+(x-x_0)^2+(y-y_0)^2}=\sqrt{d^2+\Delta s^2} \tag{2.48}$$

where *d* is the distance from the input plane to the observation plane.

The paraxial approximation will be satisfied and equation (2.49) can be obtained when $d\gg\Delta s$.

$$\begin{cases} L\approx d \\ \cos\theta\approx 1 \end{cases} \tag{2.49}$$

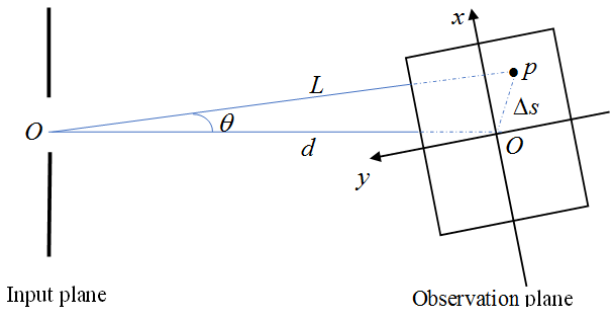


Fig. 2.7 The diffraction aperture and observation plane.

The Fresnel diffraction integral can be approximately expressed as:

$$E_1(x,y) = \frac{1}{\mathrm{i}\lambda d}\exp(\mathrm{i}kd)\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} E_0(x_0,y_0) \times \exp\left\{\mathrm{i}\frac{k}{2d}[(x-x_0)^2+(y-y_0)^2]\right\}\mathrm{d}x_0\mathrm{d}y_0 \tag{2.50}$$

where $E_0(x_0,y_0)$ and $E_1(x,y)$ are the input plane and the observation plane, respectively, λ is incidence wavelength, and $k = 2\pi/\lambda$.

Eq. (2.50) can be rewritten in the form:

$$E_1(x,y) = \frac{1}{\mathrm{i}\lambda d}\exp(\mathrm{i}kd)\exp\left(\mathrm{i}\frac{k}{2d}(x^2+y^2)\right)\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} E_0(x_0,y_0) \times \exp\left[\mathrm{i}\frac{k}{2d}(x_0^2+y_0^2)\right]\exp\left\{\mathrm{i}\frac{k}{2d}\left[x_0\frac{x}{\lambda d}+y_0\frac{y}{\lambda d}\right]\right\}\mathrm{d}x_0\mathrm{d}y_0 \tag{2.51}$$

Obviously, this Fresnel diffraction integral can be computed by following two steps:

(a) Performing fast Fourier transform (FFT) of $E_0(x_0,y_0)\times\exp\left[\mathrm{i}\frac{k}{2d}(x_0^2+y_0^2)\right]$.

(b) Then, the result of FFT is multiplied by $\frac{1}{\mathrm{i}\lambda d}\exp(\mathrm{i}kd)\exp\left(\mathrm{i}\frac{k}{2d}(x^2+y^2)\right)$.

It is can be seen from the Fresnel diffraction integral that its space frequencies are:

$$f_x = \frac{x}{\lambda d},\ f_y = \frac{y}{\lambda d}.$$

In order to find the relationship between FrFT and the Fresnel transform, the following substitution is made for Fresnel formula (2.51): A vector variable ***r*** expresses input plane coordinates (x_0,y_0) and ***s*** is also a two-dimensional variable representing observation plane (*x, y*). Then, the Fresnel diffraction integral (2.51) can be expressed as:

$$E(\boldsymbol{s}) = \frac{1}{\mathrm{i}\lambda d}\exp(\mathrm{i}kd)\exp\left(\mathrm{i}\frac{ks^2}{2d}\right)\int_{-\infty}^{\infty} E_0(\boldsymbol{r})\exp\left(\mathrm{i}\frac{kr^2}{2d}\right)\exp\left(\mathrm{i}\frac{2\pi}{\lambda d}\boldsymbol{sr}\right)\mathrm{d}\boldsymbol{r} \tag{2.52}$$

where $r = \sqrt{x_0^2 + y_0^2}$, $s = \sqrt{x^2 + y^2}$, and $\mathrm{d}\boldsymbol{r} = \mathrm{d}x_0\mathrm{d}y_0$.

Similarly, the FrFT formula (2.38) can be rewritten by two-dimensional variable:

$$F(\boldsymbol{s}) = A_s\exp\left(\mathrm{i}\frac{s^2}{2\tan\alpha}\right)\int_{-\infty}^{\infty} f(\boldsymbol{r})\exp\left(\mathrm{i}\frac{r^2}{2\tan\alpha}\right)exp\left(-\mathrm{i}\frac{\boldsymbol{s}\cdot\boldsymbol{r}}{\sin\alpha}\right)\mathrm{d}\boldsymbol{r} \tag{2.53}$$

As is known, (2.52) and (2.53) have similarities. The scaled variables for $\boldsymbol{r}$ and $\boldsymbol{s}$ are introduced

$$\begin{cases} \boldsymbol{\rho} = \mu\boldsymbol{r} = \sqrt{2\pi\tan\alpha/(\lambda d)}\boldsymbol{r} \\ \boldsymbol{\sigma} = v\boldsymbol{s} = \sqrt{2\pi\sin\alpha\cos\alpha/(\lambda d)}\boldsymbol{s} \end{cases} \tag{2.54}$$

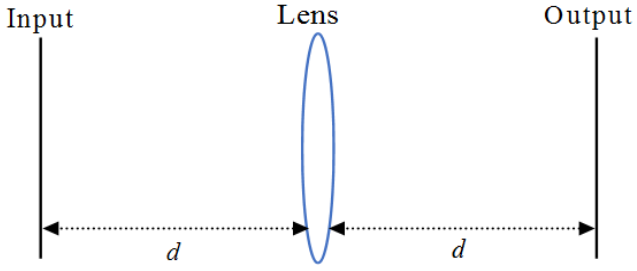
Then (2.52) becomes

$$\begin{aligned} E\left(\frac{\sigma}{v}\right) &= \frac{1}{\mathrm{i}\lambda d}\exp(\mathrm{i}kd)\exp\left(\mathrm{i}\frac{\tan\alpha}{2}\sigma^2\right)\exp\left(\mathrm{i}\frac{\sigma^2}{2\tan\alpha}\right) \\ &\quad\times\int_{-\infty}^{\infty} E_0\left(\frac{\sigma}{\mu}\right)\exp\left(\mathrm{i}\frac{\rho^2}{2\tan\alpha}\right)\exp\left(\frac{2\pi}{\lambda d}\boldsymbol{\rho\sigma}\right)\mathrm{d}\boldsymbol{\rho} \\ &= C'\exp\left(\mathrm{i}\frac{\tan\alpha}{2}\sigma^2\right)F^{\alpha}\left\{U\left(\frac{\boldsymbol{\rho}}{\mu}\right)\right\}\left(\frac{\boldsymbol{\sigma}}{\mu}\right) \end{aligned} \tag{2.55}$$

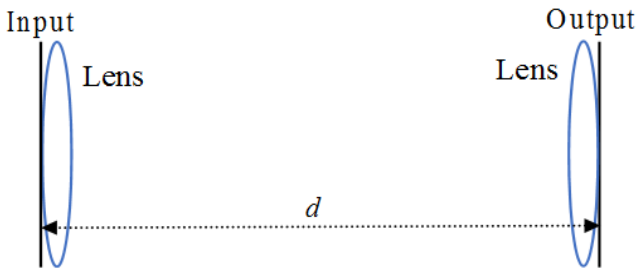
(2.55) indicates that the Fresnel diffraction distribution equals the product of the FrFT with order α and a quadratic phase factor. Notice that this quadratic phase factor has no influence on the diffraction intensity distribution. Thus, FrFT can be performed by the Fresnel diffraction.

2.4.4 Optical fractional Fourier transform with lens

Ozaktas and Mendlovic [59], in 1993, introduced FrFT into optics by using a piece of graded-index fiber of proper length to perform a Fourier transform. Lohmann [22, 128] indicated that the optical systems shown in Fig. 2.8 are capable of performing fractional Fourier transform.



(a) Lohamann I



(b) Lohamann II

Fig. 2.8 Optical systems for performing the FrFT system.

Fig. 2.8(a) shows the setup for performing FrFT by utilizing a single lens, which is named Lohmann I. d is the distance from the input plane P_1 to the lens or the lens to the output plane P_3. The focal length is f. The output function is the FrFT with order α of the input function when a combination of the following conditions is true:

$$\begin{cases} d = f_s \tan(\phi/2) \\ f = f_s / \sin\phi \end{cases} \tag{2.56}$$

where $\phi = \alpha\pi/2$, f_s is the standard focal length.

Fig. 2.8(b) gives a Lohamann II optical system with two lenses. The distance between the two lenses with focal length f is d. Lohamann II optical system is capable of performing FrFT when it meets the two following conditions:

$$\begin{cases} d = f_s \sin(\phi/2) \\ f = f_s / \tan\phi \end{cases} \tag{2.57}$$

Traditional Fresnel diffraction integral cannot be utilized directly when the space between diffraction plane and observation plane are not free. Collins indicated that the lens systems can be analyzed by use of diffraction theory and presented a diffraction integral using transform matrix ABCD for an arbitrary optical system, limited by the paraxial approximation restriction. The Collins diffraction integral can be expressed in the form

$$E_1(x,y) = \frac{1}{\mathrm{i}\lambda B}\exp(\mathrm{i}kd)\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} E_0(x_0,y_0) \times \exp\left(\mathrm{i}\frac{k}{2B}[A(x^2+y^2) - 2(xx_0+yy_0) + D(x_0^2+y_0^2)]\right)\mathrm{d}x_0\mathrm{d}y_0 \tag{2.58}$$

where A, B, C is related with the optical systems.

2.4.5 Apertured fractional Fourier transform optical system

Generally, there are no apertures in the FrFT optical systems. However, in practice, apertures always exist in most optical systems, due to the reasons such as the finite size of lens in Lohamann I, as shown in Fig. 2.9 [40].

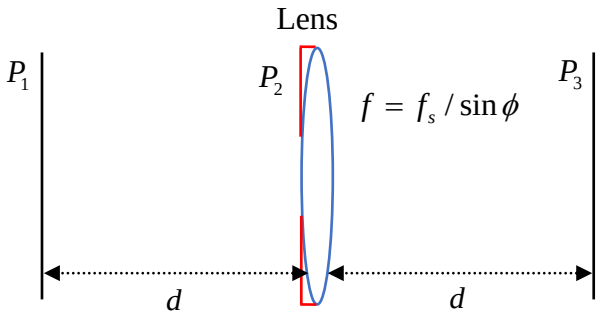


Fig. 2.9 An optical system for the apertured FrFT

A hard aperture is placed just before the lens for the apertured FrFT as shown in Fig. 2.9. Within the framework of paraxial approximation, the field of propagation of light across optical system as shown in Fig. 2.9 is divided into two ABCD optical systems in accordance with Collins diffraction integral formulas [40, 129-131]. $\{A_1, B_1, C_1, D_1\}$, $\{A_2, B_2, C_2, D_2\}$ are the elements of the transfer matrices of the two sections, respectively. The first diffraction describes the field $E(x_1, y_1)$ at P_2 before aperture, the following integral equation from P_1 to P_2 can be denoted as:

$$\begin{aligned} E_1(x,y) &= F^{(A_1,B_1,C_1,D_1)}\{f(x,y)\} \\ &= \frac{1}{\mathrm{i}\lambda B}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y) \\ &\times \exp\left(\mathrm{i}\frac{k}{2B}[A(x^2+y^2) - 2(xx_1+yy_1) + D(x_1^2+y_1^2)]\right)\mathrm{d}x\mathrm{d}y \end{aligned} \tag{2.59}$$

$$\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \tag{2.60}$$

where $F^{(A_1,B_1,C_1,D_1)}$ is Collins diffraction integral of the optical system, $f(x,y)$ is input at optical field P_1, λ is the wave length. Actually, this first diffraction is Fresnel diffraction. The second optical field describes the propagation of field $E(x_2, y_2)$ at P_3, the integral equation from aperture plane P_2 to the output plane P_3 is:

$$E_2(x_2,y_2) = F^{(A_2,B_2,C_2,D_2)}\{E_1(x_1,y_1)\} = \frac{1}{\mathrm{i}\lambda B}\int_{-b}^{+a}\int_{-b}^{+a} E_1(x_1,y_1) \times \exp\left(\mathrm{i}\frac{k}{2B}[A(x_1^2+y_1^2) - 2(x_1x_2+y_1y_2) + D(x_2^2+y_2^2)]\right)\mathrm{d}x_1\mathrm{d}y_1 \tag{2.61}$$

$$\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1/f & 1 \end{pmatrix} = \begin{pmatrix} 1-d/f & d \\ -1/f & 1 \end{pmatrix} \tag{2.62}$$

If the hard aperture before lens is rectangle, it can be represented as a rectangle function

$$K(x_1,y_1) = \begin{cases} 1, & |x_1,y_1| \le a,b \\ 0, & |x_1,y_1| > a,b \end{cases} \tag{2.63}$$

or

$$K(x_1,y_1) = \begin{cases} 1, & x_1^2+y_1^2 \le a^2 \\ 0, & x_1^2+y_1^2 > a^2 \end{cases} \tag{2.64}$$

for a circular aperture.

Collins pointed out that the limiting aperture can be removed by use of the integral derived, multiplying by the aperture function. So, Eq. (2.45) can be rewritten as:

$$E_2(x_2,y_2) = F^{(A_2,B_2,C_2,D_2)}\{E_1(x_1,y_1)\} = \frac{1}{\mathrm{i}\lambda B}\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} E_1(x_1,y_1)K(x_1,y_1) \times \exp\left(\mathrm{i}\frac{k}{2B}[A(x_1^2+y_1^2) - 2(x_1x_2+y_1y_2) + D(x_2^2+y_2^2)]\right)\mathrm{d}x_1\mathrm{d}y_1 \tag{2.65}$$

Then the apertured FrFT with a fractional order of α can be implemented through Eq. (2.59) - (2.65) by changing the distance *d* and the focal length of the lens f_s. Its inverse is calculated as [131-134]:

$$F^{D,-B,-C,A}(F^{(A,B,C,D)}\{f(t)\}) = f(t) \tag{2.66}$$

2.5 Fractional Mellin transform

2.5.1 Mellin transform

R. H. Mellin first gave a systematic formulation of Mellin transform and its inverse in 1933 [135]. Casasent and Psaltis discussed the implementation of Mellin transform in optical systems [136].

Suppose that $f(t)$ is a locally integrable function defined on the positive real axis $0 < t < \infty$, $M\{\cdot\}$ represents the operation of Mellin transform. Mellin transform is defined as:

$$M\{f(t)\} = M(s) = \int_0^{\infty} f(t)t^{s-1}\mathrm{d}t \tag{2.67}$$

In general, the integral exists only for $s = c + \mathrm{i}b$ such that $c_1 < c < c_2$ $c_1 < c < c_2$, where c_1 and c_2 depend on the function $f(t)$.
And the inverse Mellin transform can be expressed as:

$$M^{-1}\{M(s)\} = f(t) = \frac{1}{\mathrm{i}2\pi}\int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} M(s)t^{-s}\mathrm{d}s \tag{2.68}$$

Mellin transform has a close relationship with Fourier transform. By writing $s = \mathrm{i}2\pi b$, $t = e^x$ to obtain the relation to Fourier transform:

$$\begin{aligned} M(s) = \int_0^{\infty} f(t)\, t^{s-1}\mathrm{d}t &\longrightarrow \int_0^{\infty} f(e^x)e^{x(s-1)}\,\mathrm{d}e^x \\ &= \int_{-\infty}^{\infty} f(e^x)e^{x(-\mathrm{i}2\pi b)}\mathrm{d}x = \int_{-\infty}^{\infty} f(e^x)e^{-\mathrm{i}2\pi bx}\,\mathrm{d}x = F\{f(e^x)\} \end{aligned} \tag{2.69}$$

where $F\{\cdot\}$ represents Fourier transform. Hence, Mellin transform can be performed by a special Fourier transform: (1) Performing a log transform for signal $f(t)$ along axis t to obtain $f(e^x)$. (2) Mellin transform can be obtained by performing Fourier transform for signal $f(e^x)$.

There is scale invariant property in coherent optical processing using Mellin transform. The intensity of the correlation peak is independent of the input scale [136]:

$$M\{f(kt)\} = \int_0^{\infty} f(kt)t^{s-1}\mathrm{d}t = a^{-s}\int_0^{\infty} f(t)t^{s-1}\mathrm{d}t = k^{-s}M\{f(t)\}$$

(2.70)

Thus, for any scale factor k, the amplitude of Mellin transform is invariant:

$$|M\{f(kt)\}| = |M\{f(t)\}| \tag{2.71}$$

There are other properties:

Multiplication by t^a:

$$M\{t^a f(t^a)\} = \int_0^\infty f(t)t^{(s+a)-1}dt = F(s+a) \tag{2.72}$$

where $F(\cdot)$ is Fourier transform.

Inverse of independent variable:

$$M\{\ln(t)f(t)\} = F(1-s) \tag{2.73}$$

Multiplication by a power of $\ln(t)$:

$$M\{\ln(t)^k f(t)\} = \frac{d^k}{ds^k}F(s) \tag{2.74}$$

Convolution:

$$M\{f(t)g(t)\} = \frac{1}{2\pi \mathrm{i}}\int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} F(z)G(s-z)\mathrm{d}z \tag{2.75}$$

2.5.2 Fractional Mellin transform

Sazbon gave the definition of the 2D fractional Mellin transform (FrMT) of order (p_1, p_2) by [146]:

$$\begin{aligned} M^{(p_1,p_2)}(u,v) = {} & C \\ & \cdot \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{f(x,y)}{x^2+y^2} \\ & \times \exp\left(\begin{array}{c} -2\pi \mathrm{i}\left(\dfrac{u\ln\sqrt{x^2+y^2}}{\sin\phi_1} + \dfrac{v\arctan(y/x)}{\sin\phi_2}\right) \\ +\pi \mathrm{i}\left(\dfrac{u^2+\ln^2\sqrt{x^2+y^2}}{\tan\phi_1} + \dfrac{v^2+[\arctan(y/x)]^2}{\tan\phi_2}\right) \end{array}\right)\mathrm{d}x\mathrm{d}y \end{aligned} \tag{2.76}$$

where C is a constant, $\phi_1 = \frac{p_1\pi}{2}$, $\phi_2 = \frac{p_2\pi}{2}$. Let $\rho = \ln\sqrt{x^2+y^2}$, $\theta = \arctan(y/$

x), then FrMT can be expressed as:

$$M^{(p_1,p_2)}(u,v) = C \cdot \int_0^{2\pi} \int_{-\infty}^{\infty} f(\rho,\theta) \times \exp\left[\begin{matrix} -2\pi \mathrm{i}\dfrac{u\rho}{\sin\phi_1} + \dfrac{v\theta}{\sin\phi_2} + \\ \pi \mathrm{i}\left(\dfrac{u^2+\rho^2}{\tan\phi_1} + \dfrac{v^2+\theta^2}{\tan\phi_2}\right) \end{matrix}\right] \mathrm{d}\rho\mathrm{d}\theta \tag{2.77}$$

As shown in Eq. (2.77), the fractional Mellin transform can be obtained from fractional Fourier transform by a change of coordinates from plane coordinates (x, y) to polar coordinates (ρ, θ).

$$M^{(p_1,p_2)}(u,v) = F^{(p_1,p_2)}\{f(\rho,\theta)\} \tag{2.78}$$

Note that $M^{(0,0)}(u,v) = f(\rho,\theta)$, which is the input itself in log-polar coordinates, $M^{(1,1)}(u,v) = M\{f(\rho,\theta)\}$, which is the Mellin transform of the input. Since the log-polar transform is nonlinear, the relationship between the fractional Fourier transform and Mellin transform is nonlinear as well. However, the fractional Mellin transform still keeps other properties, such as periodicity and unitarity. The implementation for the fractional Mellin transform is shown as follows

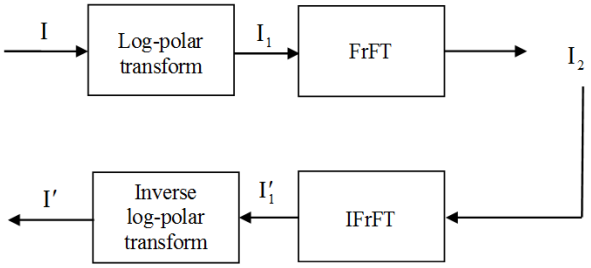


Fig. 2.10. Chart for performing FrMT and its inverse [25].

According the relationship between FrMT and FrFT, FrMT can be performed by the log-polar and the fractional Fourier transforms as shown in Fig. 2.10. First, the image I is regarded as the input of log-polar transform to obtain image I_1. And then, the image I_1 is processed by FrFT to finally obtain FrMT result I_2.

2.5.3 Log-polar transform

The log-polar transform is proposed by Schwartz to describe an active vision system [28, 137-139]. Scholars like Weiman, Tistarelli, Ferrari and Sandini et al further studied the application of log-polar in stereoscopic vision, motion targets tracking and other fields. It is necessary to build and describe the relationship between Cartesian and log-polar coordinates for images. In Cartesian coordinates, pixels are indexed by (x, y),

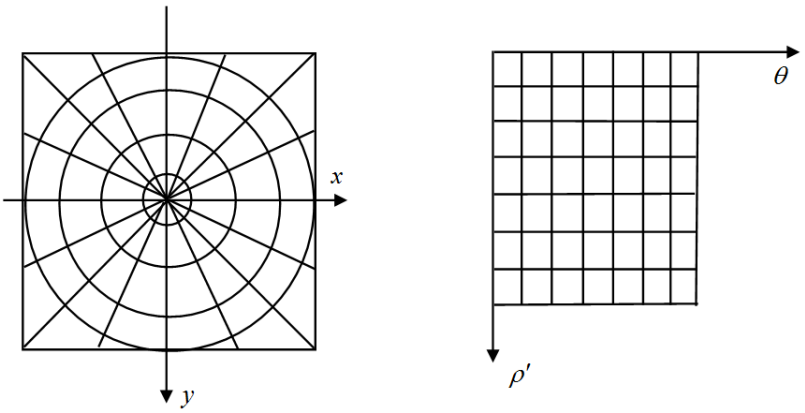
related to log-polar coordinates ring number ρ and wedge number θ by the mapping:

$$\rho = \sqrt{(x - x_c)^2 + (y - y_c)^2} \tag{2.79}$$

$$\rho' = \ln\rho \tag{2.80}$$

$$\theta = \arctan\frac{y - y_c}{x - x_c} \tag{2.81}$$

where (x_c, y_c) is the position of the geometric center of the original image, ρ' and θ represent the distance axis, angle axis as shown in Fig. 2.11(b), respectively.



(a) Polar grid (b) Log grid

Fig. 2.11. Log-polar transform: log-polar grid.

Extending ρ' by *k* times in polar coordinates, then (2.80) becomes:

$$\rho_1 = \ln k\rho' = \ln k + \ln\rho' \tag{2.82}$$

There is additivity in the angle change, then the new angle can be obtained:

$$\theta_1 = \theta + \xi \tag{2.83}$$

where ξ is the change of angle in polar coordinates. This shows that the change along the scale and angle in polar coordinates corresponds to an up-down and a right-left translation in log coordinates, respectively.

In general, the quantities of scale and angle exist decimals and have small values in range when (2.80) - (2.81) are performed. Hence, to solve this issue, the (2.80) - (2.81) are adjusted by adding parameters n_r and n_w:

$$R = \frac{(n_r - 1)(\rho - \rho_{\min})}{(\rho_{\max} - \rho_{\min})} \tag{2.84}$$

$$W = \frac{n_{w\theta}}{2\pi} \tag{2.85}$$

where n_r and n_w are the numbers of discrete sampling points along distance axis and along angle axis, respectively; $\rho_{\min}$ and $\rho_{\max}$ represent the radii of the smallest and the largest distance, respectively. The log-polar transform is invertible:

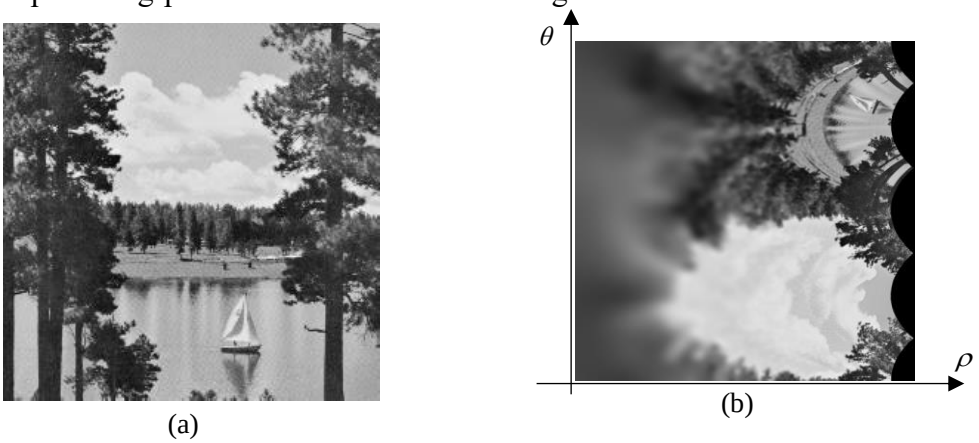
$$\begin{cases} \rho' = \dfrac{(\rho_{\max} - \rho_{\min})R}{(n_w - 1)} \\ \theta' = \dfrac{2\pi W}{n_w} \end{cases} \tag{2.86}$$

$$\begin{cases} \rho = \exp(\rho') \\ \theta = \theta' \end{cases} \tag{2.87}$$

Therefore, the Cartesian coordinates can be obtained:

$$\begin{cases} x = \rho\cos\theta + x_c \\ y = \rho\sin\theta + y_c \end{cases} \tag{2.88}$$

An example of log-polar transform is shown in Fig. 2.12.



(a) (b)

Fig. 2.12. An example to show log-polar transform: (a) An original image of size 256×256. (b) The image in the log-polar coordinates with 500 rings and 500 wedges.

2.6 Summary

This chapter first introduces the evaluation criterion of image encryption algorithm, such as statistical analyses and sensitivity analyses. Several chaotic maps and its main properties that are capable of producing the random sequences are described. And then the Fourier transform, the fractional Fourier transform and its properties, paraxial approximation, Fresnel diffraction, Collins integral formulas, the apertured fractional Fourier transform are introduced in detail. The relationships among the fractional transform, the Fresnel diffraction, the optical system with lens and the Collins integral formulas are analyzed. At last, the Mellin and the fractional Mellin transforms are

presented. The relationships between the Mellin/fractional Mellin transforms and the Fourier/fractional Fourier transforms are also analyzed. According to those relationships, the fast and convenient implementation methods of the Mellin/fractional Mellin are described, which can be performed by the log-polar transform and the fractional Fourier transform.

Chapter 3

Image encryption based on the aperture FrMT

Due to its nonlinear property, FrMT is utilized for eliminating potential insecurity in an image encryption system caused by known-plaintext and chosen-plaintext attacks. The aperture in the optical system makes it harder for attackers to collect optical signals in the transmission process. The apertured FrMT can be implemented by log-polar transform and Collins diffraction. Thus, in this chapter, an optical image encryption scheme is discussed by utilizing an apertured nonlinear fractional Mellin transform (FrMT).

3.1 Introduction

With the development of information technology, information security and encryption receive more and more attention. Image encryption is a very important field in information security. The fractional domain transforms have been widely involved in image encryption, such as fractional discrete cosine transform (FrDCT) [31-32], fractional Fourier transform (FrFT) [97], fractional Hartley transform (FrHT) [58, 60], discrete fractional angular transform (DFrAT) [140]. The FrFT based on optical system was implemented in image encryption due to its advantages of 2D parallel computation and data processing at a high speed [18]. However, the encryption system based on FrFT is a linear one which is relatively insecurity weak in comparison to nonlinear encryption systems. Consequently, some nonlinear encryption schemes, like encryption schemes based on the fractional Mellin transform (FrMT) [25-28], were proposed to reduce the security risk existing in linear encryption systems. The FrMT is implemented through the log-polar and FrFT, and the optoelectronic hybrid setup for FrMT was proposed in [25]. Consequently, image encryption systems based on FrMT not only enlarge the key space but also have the capability to overcome the drawback existing in linear FrFT system.

Generally, most of the studies and applications of FrFT and FrMT involve with optical image encryption systems without aperture. However, in practice, there are always apertures in most optical systems [40]. It is well known that the propagation of light in an optical system will be limited by the finite sized aperture in the system. And the attacker can perhaps obtain some useful information from the marginal leakage of the light in the systems. So, it is necessary and practical to analyze the performance of optical encryption systems with aperture.

In this chapter, a nonlinear optical image encryption scheme based on fractional Mellin transform with a hard aperture is proposed. The FrMT with aperture is realized through the log-polar transform and FrFT with aperture. In the image encryption process, since the FrFT is considered as a special Fresnel diffraction [11, 24, 45, 127], the apertured FrFT can be implemented by Collins formula with aperture [40]. In the proposed scheme, the side-length of the aperture is chosen to be extra private key which enlarges the key space of the proposed encryption scheme. The apertured FrMT gives good security due to its nonlinearity and the performance of encryption can be controlled by adjusting the size of the aperture.

This chapter is organized as follows. In Section 3.2, the proposed image encryption and decryption scheme is presented in detail. In Section 3.3, simulation results are discussed. Finally, conclusions are drawn in Section 3.4.

3.2 Image encryption and decryption based on the apertured FrMT

3.2.1 Proposed fractional Mellin transform with aperture

The fractional Mellin transform is a kind of nonlinear transform and can be obtained from fractional Fourier transform by a change of coordinates from plane coordinates (x, y) to polar coordinates (ρ, θ). The representation of the apertured FrMT is

$$M^{(p_1,p_2)}(u,v) = C \cdot \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{f(x,y)}{x^2+y^2} \times K(x,y) \times \exp\left\{-2\pi \mathrm{i}\left(\frac{u\ln\sqrt{x^2+y^2}}{\sin\phi_1} + \frac{v\arctan(y/x)}{\sin\phi_2}\right) + \pi \mathrm{i}\left(\frac{u^2+\ln^2\sqrt{x^2+y^2}}{\tan\phi_1} + \frac{v^2+[\arctan(y/x)]^2}{\tan\phi_2}\right)\right\} \mathrm{d}x\mathrm{d}y \tag{3.1}$$

where $K(x,y)$ is rectangular function or circular function, p_1, p_2 are the fractional orders of the apertured FrMT, $\phi_1 = \frac{p_1\pi}{2}$, $\phi_2 = \frac{p_2\pi}{2}$. Let $\rho = \ln\sqrt{x^2+y^2}$, $\theta = \arctan(y/x)$, then the apertured FrMT can be represented by log-polar transform and apertured FrFT:

$$M_a^{(p_1,p_2)}(u,v) = F_a^{(p_1,p_2)}\{f(\rho,\theta)\} \tag{3.2}$$

where $M_a^{(p_1,p_2)}$ represents the apertured FrMT.

Fig. 3.1 shows the optoelectronic hybrid setup to change coordinates from (x,y) to (ρ,θ) and to implement the apertured FrFT.

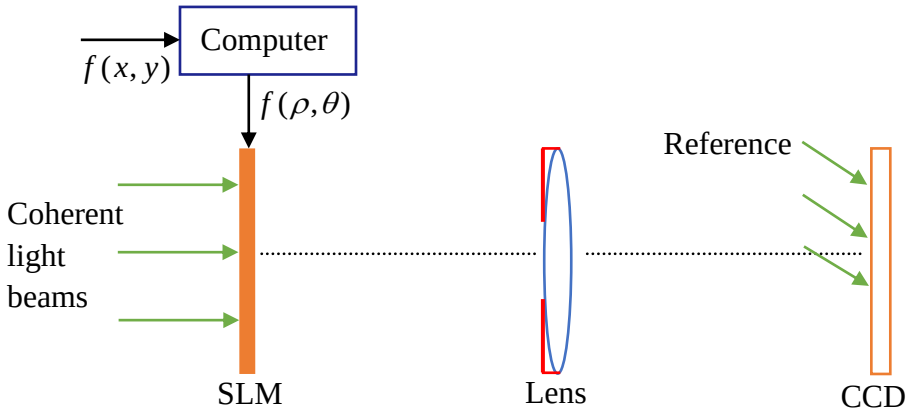


Fig. 3.1 Optoelectronic hybrid setup for apertured FrMT.

In the optoelectronic hybrid setup, the transformation of coordinates of the input image is completed through the computer. Then the processed image is used to modulate coherent light beams by means of a spatial light modulator. After that, the light beams pass through the optical system with the aperture, and the results of the apertured FrMT are captured by CCD.

The implementation of FrMT was already described in detail in [25-28]. Because FrMT is performed in an annular domain, many parameters have to be set in advance, including the center of the original image (denoted as (c_x, c_y)), the numbers of rings and wedges (denoted as n_r and n_w), and the radii of the innermost and outermost rings of the annular domain (denoted as r_{in}, r_{out}). The value ranges of r_{in} and r_{out} are $1 \le r_{\text{in}} \le r_{\text{out}} \le r_{\max}$, where $r_{\max} = \max_{x,y}(\sqrt{(x-x_c)^2+(y-y_c)^2})$. The size of the hard aperture also should be set in advance, i.e., the side-lengths *a, b*. The orders of the FrFT and apertured FrMT are denoted as q_i and $p_i, i = 1, 2, \cdots \text{N}$, respectively. The

wavelength is denoted as λ. Those parameters mentioned above are all considered as cipher keys which have a great effect on the performance of the encryption system

3.2.2 Proposed image encryption and decryption scheme

The schematic of the proposed image encryption and decryption algorithm is shown in Fig. 3.2 and the encryption process is described below:

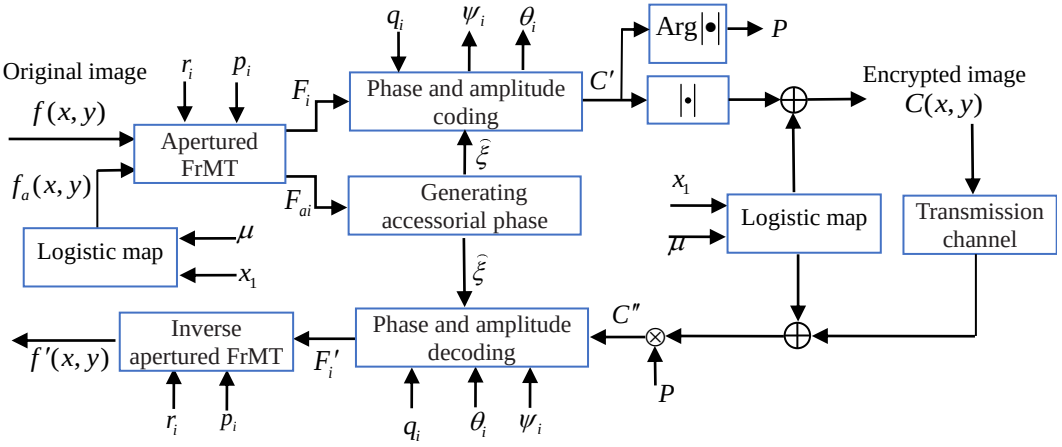


Fig. 3.2 Proposed image encryption and decryption algorithm

Step 1: As illustrated in [25], the FrMT is computed by the log-polar and fractional Fourier transforms. The original image $f(x,y)$ is first log-polar transformed to obtain the input of the apertured fractional Fourier transform. Then original image $f(x,y)$ is divided into N sub-images denoted as $f_i(\rho,\theta), i = 1,2,\cdots N$. $f_i(\rho,\theta)$ is of size $n_r \times n_w$, affinely transformed from a ring-shaped image block with inner radius r_{i-1} and outer radius r_i, $2 < i < N$.

Step 2: The N sub-images $F_i(u,v), i = 1,2,\cdots N$. are obtained by performing the apertured FrFT with the side-lengths of the hard aperture being a and b, if the hard aperture is rectangular:

$$F_i(u,v) = F_a\{f_i(\rho,\theta)\}, \qquad i = 1,2,\cdots N \tag{3.3}$$

where $F_a\{\cdot\}$ means the operation of apertured fractional Fourier transform.

Here, the apertured FrFT is computed through Collins diffraction *ABCD* integral formulas (2.61) - (2.67). The order p_i of the FrMT, the outer radius r_i, $1 < i < N$ and wavelength λ jointly constitute the cipher keys.

Step 3: The $F_i(u,v), i = 1,2,\cdots N$ are further encrypted into one encrypted image by an N-iteration process described in detail in [25], in which the amplitude and phase coding is adopted. The amplitude of the sub-images is encoded into phase restricted in

a range of $[0, 2\pi]$ and the phase is encoded into amplitude restricted in a range of $[0, 255]$. The fractional Fourier transform without aperture are adopted in the encoding process. After this iterative process, an intermediate result is obtained:

$$C'(x, y) = C_N \exp[\mathrm{i}\xi_N(x, y)] \tag{3.4}$$

where $C_N(x, y)$ and $\xi_N(x, y)$ are amplitude and phase obtained after N times iterative, respectively.

Step 4: A logistic map is applied to generate an accessorial matrix [98, 117]:

$$x_{l+1} = \mu x_l(1 - x_l) \tag{3.5}$$

where, $\mu \in (0,4]$ and $x_l \in (0,4]$.

A matrix $g(x, y)$ of size 255×255 generated by the logistic map is used as an accessorial matrix and linearly mapped into range [0, 255]. By setting $g(x, y)$ as input of the apertured FrMT and repeating the above step 1 - step 3, $D(x, y)$ can be obtained:

$$D(x, y) = O\{g(x, y)\} \tag{3.6}$$

where $O\{\cdot\}$ represents the operations of step 1 - step 3. The phase of $D(x, y)$ is extracted:

$$\hat{\xi}(x, y) = \mathrm{Arg}[D(x, y)] \tag{3.7}$$

where $\mathrm{Arg}[\cdot]$ represents phase extraction. To increase the effect of aperture on phases, ψ_i, θ_i the phases are re-calculated as

$$\psi_i' = \psi_i(x, y) + \hat{\xi}(x, y) \tag{3.8}$$

$$\theta_i' = \theta_i(x, y) + \hat{\xi}(x, y) \tag{3.9}$$

The side-lengths of aperture a, b, and the seeds of logistic map x_1, μ are regarded as keys of proposed scheme. The $\psi_i'(x, y)$ and $\theta_i'(x, y), i = 1,2, \ldots, \mathrm{N}$, are phases involved in this process and served as keys.

Step 5: Amplitude and phase of $C'(x, y)$ are extracted as

$$C_A(x, y) = |C'(x, y)| \tag{3.10}$$

$$P(x, y) = \mathrm{Arg}|C'(x, y)| \tag{3.11}$$

where $|\cdot|$ represents extracting amplitude, $P(x, y)$ denotes the phase of $C'(x, y)$ to be reserved to recover the original image.

To further scramble $C_A(x, y)$, an XOR operation is introduced:

$$C = C_A \oplus C_{ho} \tag{3.12}$$

where $\oplus$ denotes XOR operation, C_{ho} is a random matrix of size $n_r \times n_w$ generated by the logistic map with initial values x_1 and parameter μ. The value of parameter μ is related to $F_i(u, v)$ [147].

The decryption process is the inverse of encryption one, as shown in Fig. 3. First, the amplitude can be recovered by XOR operation:

$$C'_A = C \oplus C_{ho} \tag{3.13}$$

Second, the intermediate result can be obtained as:

$$C'' = C'_A \times \exp(-\mathrm{i} \times P) \tag{3.14}$$

Next, F'_i is obtained by the inverse of encoding process. Finally, the plain image $f'(x, y)$ is recovered by inverse apertured FrMT.

3.3. Simulation results and analyses

The simulation is performed using MATLAB 2016b on a computer with 3.60 GHz, CPU i7-4790 and RAM 8.00GB to evaluate the proposed encryption algorithm. Since FrMT is good at dealing with the image with odd length and width, so in the experiment, the images of size 255×255 are considered as test plain-images.

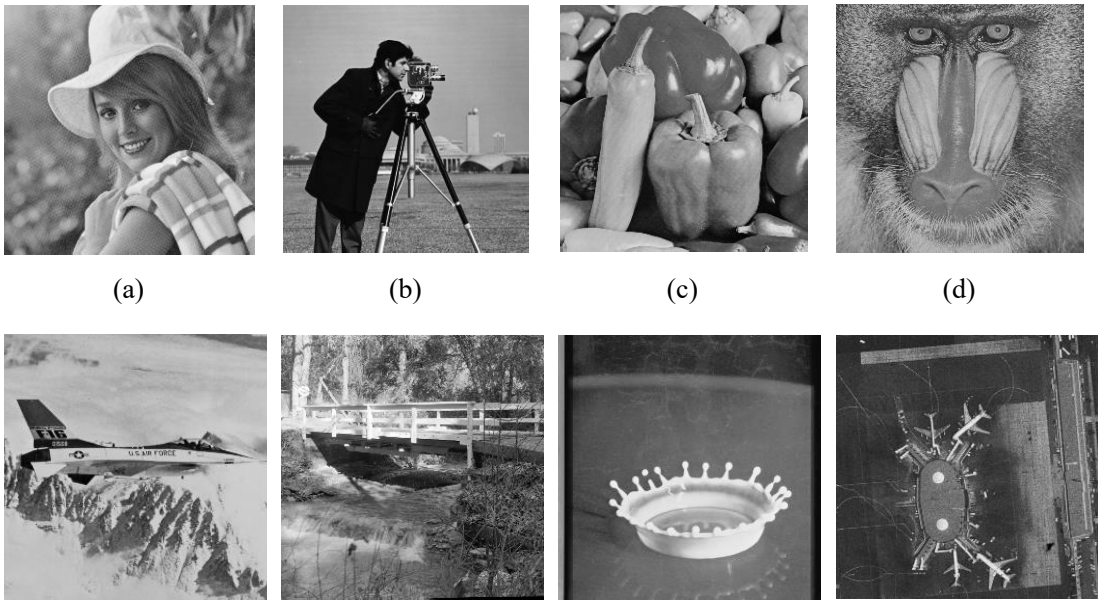
3.3.1 Parameters setup

The original image is separated into $N = 5$ sub-images before the operation of the apertured FrMT. The parameters used are chosen as follows. The geometric center of the original image $(c_x, c_y) = (128, 128)$, the outer radii of the annular domains are set to be $(r_1 = 45,\ r_2 = 80,\ r_3 = 125,\ r_4 = 160,\ r_5 = 181)$, and the rings and wedges are chosen as $n_r = 500,\ n_w = 500$. The apertured FrMT related parameters are set as: $\lambda = 632.8$ nm, $f_s = 4$ mm. For convenience, all the orders of the apertured FrMTs are set to 0.5 and the orders of FrFTs in the encoding process are set to 0.5.

3.3.2 Encrypted results and decrypted images

To test the performance of proposed algorithm, a lot of images were used in simulations. Due to the thesis limitation, partial results are shown. The encryption

results corresponding to 8 different original images as shown in Fig. 3.3, respectively, are shown in Fig. 3.4 (a1), (b1), (c1) (d1), (e1), (f1), (g1) and (h1) from which it can be seen that the cipher images are visually unrecognizable. There are 8 groups of correctly decrypted images Fig. 3.4 (a2) - (a8), (b2) - (b8), (c2) - (c8), (d2) - (d8), (e2) - (e8), (f2) - (f8), (g2) - (g8) and (h2) - (h8) with each group containing 7 decrypted images corresponding to 7 different values of aperture widths, $a = 5.2,\ 2.6, 1.3,\ 0.6\ , 0.3, 0.2,$ 0.1 mm, respectively. As is shown, the image sharpness decreases gradually when the side-length of aperture gets smaller. The images in Fig. 3.4 (a8), (b8), (c8) (d8), (e8), (f8) and (h8) are virtually indistinguishable when a reduces to 0.1 mm.



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

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

Fig. 3.3 Original images: (a) Elaine, (b) Cameraman, (c) Peppers, and (d) Baboon, (e) Airplane, (f) Bridge, (g) Milkdrop and (h) Lax

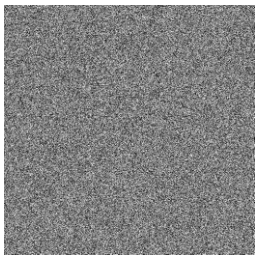
(a1) (a2) $a = 5.2$ mm (a3) $a = 2.6$ mm (a4) $a = 1.3$ mm

(a5) $a = 0.6$ mm

(a6) $a = 0.3$ mm

(a7) $a = 0.2$ mm

(a8) $a = 0.1$ mm



(b1)

(b2) $a = 5.2$ mm

(b3) $a = 2.6$ mm

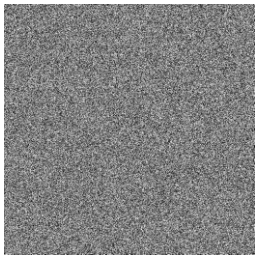
(b4) $a = 1.3$ mm

(b5) $a = 0.6$ mm

(b6) $a = 0.3$ mm

(b7) $a = 0.2$ mm

(b8) $a = 0.1$ mm



(c1)

(c2) $a = 5.2$ mm

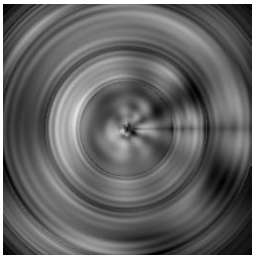
(c3) $a = 2.6$ mm

(c4) $a = 1.3$ mm

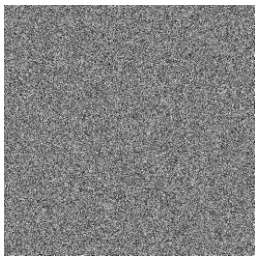
(c6) $a = 0.6$ mm

(c5) $a = 0.3$ mm

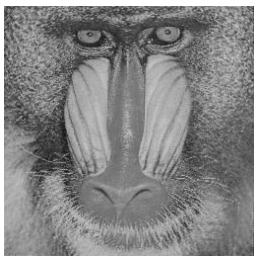
(c7) $a = 0.2$ mm



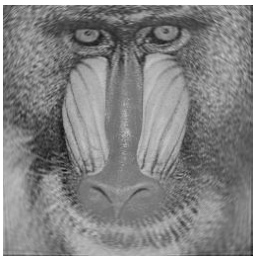
(c8) $a = 0.1$ mm



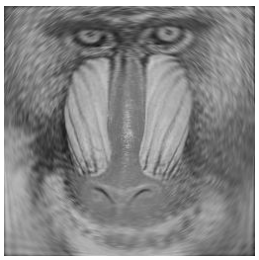
(d1)



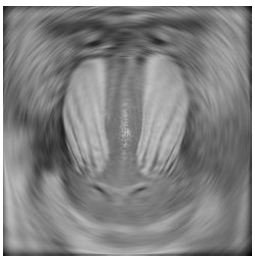
(d2) $a = 5.2$ mm



(d3) $a = 2.6$ mm



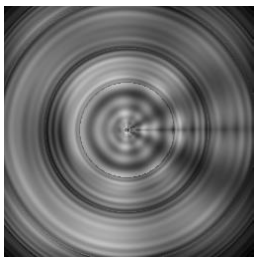
(d4) $a = 1.3$ mm



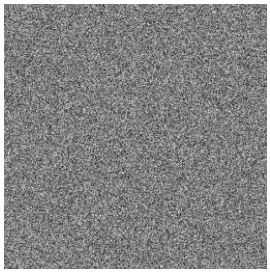
(d5) $a = 0.6$ mm

(d6) $a = 0.3$ mm

(d7) $a = 0.2$ mm



(d8) $a = 0.1$ mm

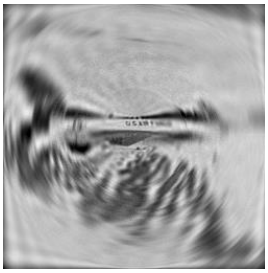


(e1)

(e2) $a = 5.2$ mm

(e3) $a = 2.6$ mm

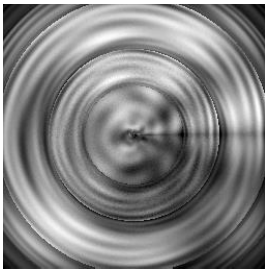
(e4) $a = 1.3$ mm



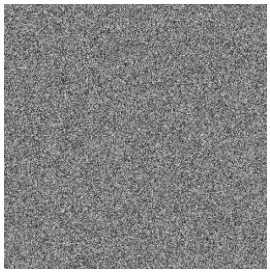
(e5) $a = 0.6$ mm

(e6) $a = 0.3$ mm

(e7) $a = 0.2$ mm



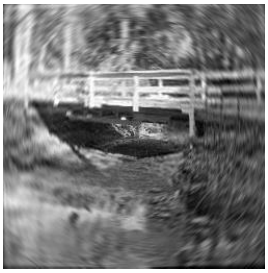
(e8) $a = 0.1$ mm



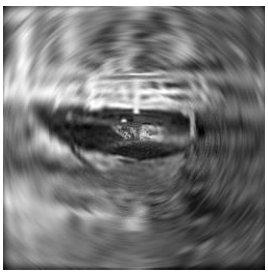
(f1)

(f2) $a = 5.2$ mm

(f3) $a = 2.6$ mm



(f4) $a = 1.3$ mm

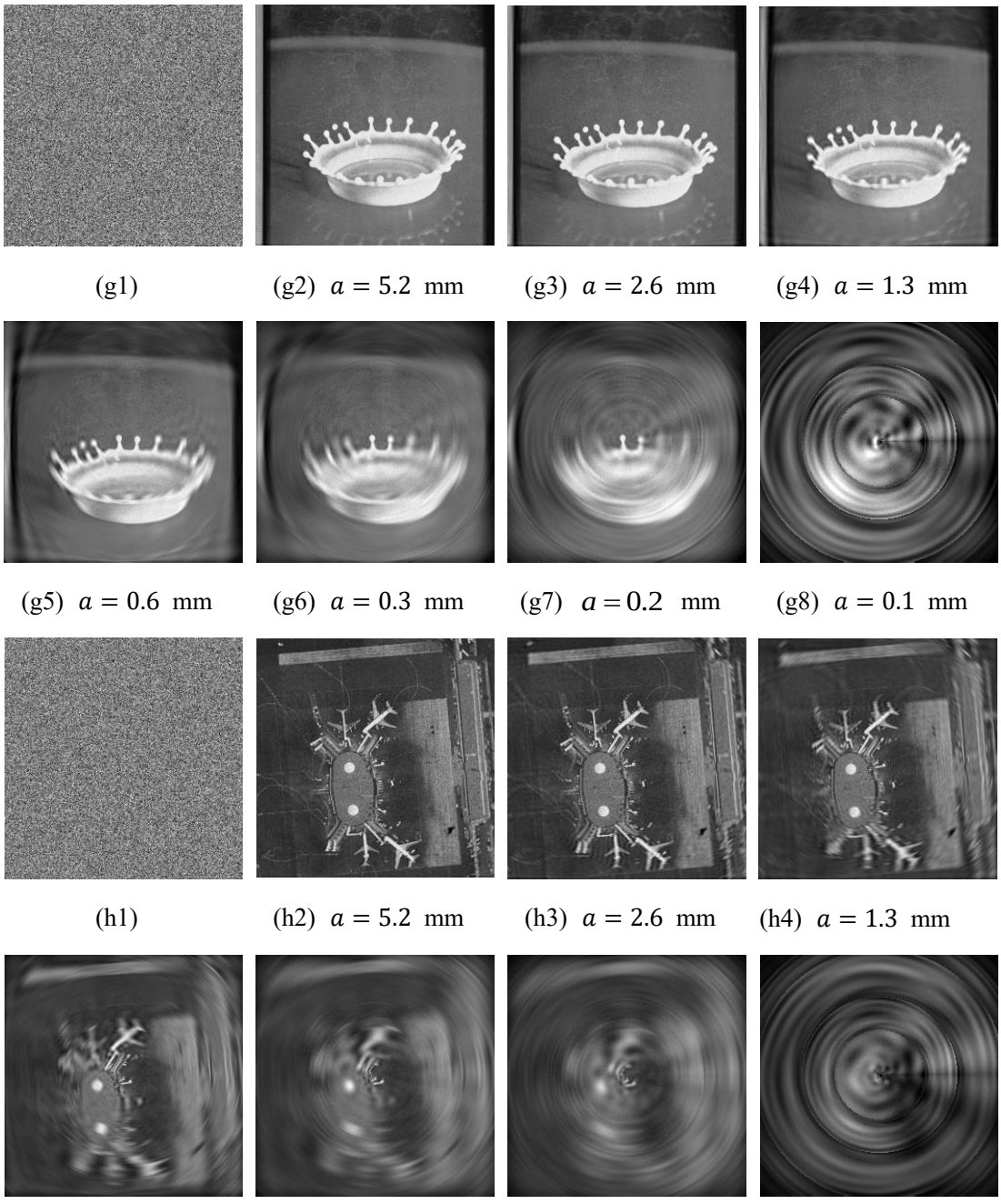


(f5) $a = 0.6$ mm

(f6) $a = 0.3$ mm

(f7) $a = 0.2$ mm

(f8) $a = 0.1$ mm



(g1) (g2) $a = 5.2$ mm (g3) $a = 2.6$ mm (g4) $a = 1.3$ mm

(g5) $a = 0.6$ mm (g6) $a = 0.3$ mm (g7) $a = 0.2$ mm (g8) $a = 0.1$ mm

(h1) (h2) $a = 5.2$ mm (h3) $a = 2.6$ mm (h4) $a = 1.3$ mm

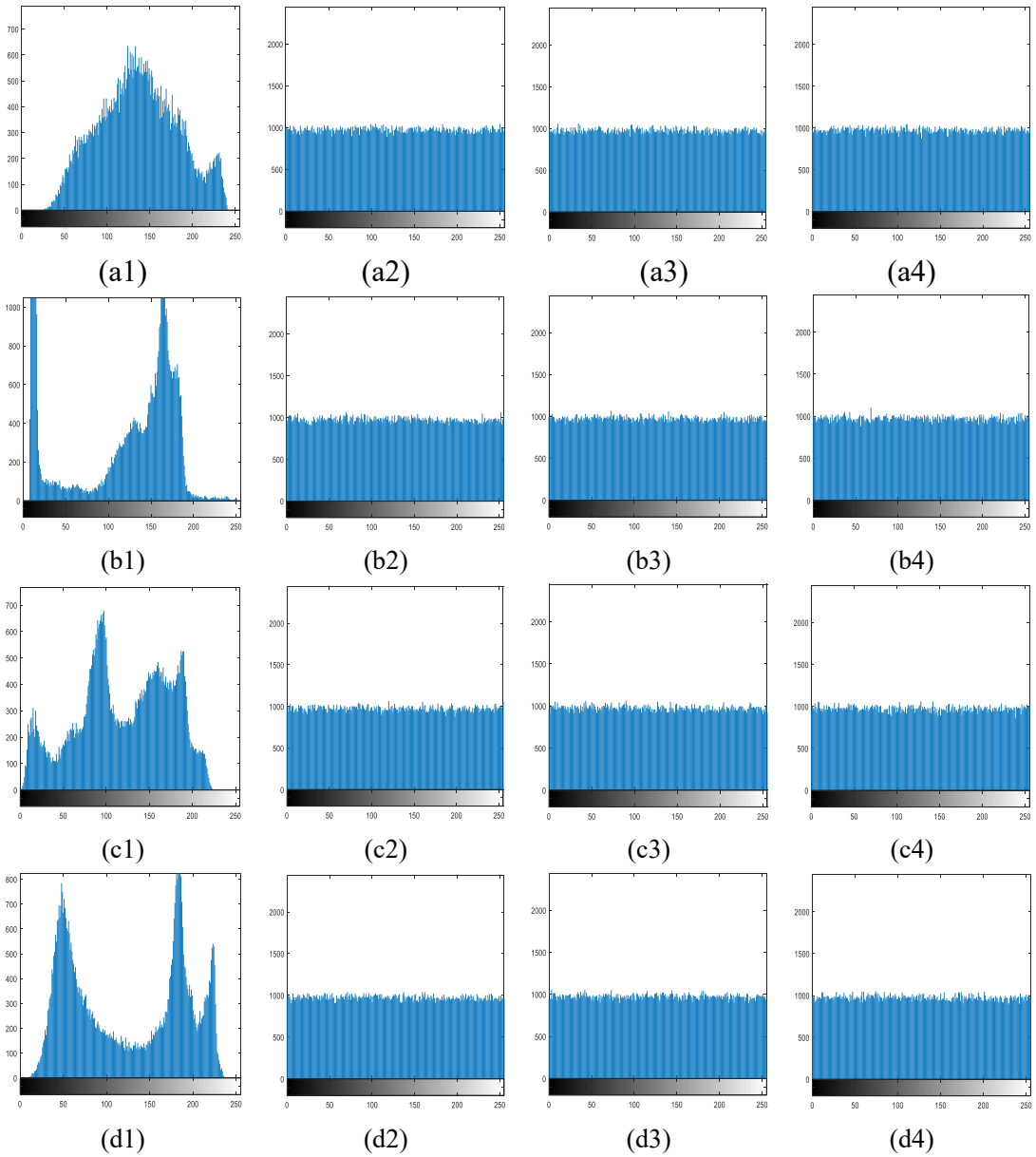
(h5) $a = 0.6$ mm (h6) $a = 0.3$ mm (h7) $a = 0.2$ mm (h8) $a = 0.1$ mm

Fig. 3.4 Encryption and decryption results for different side-lengths a, b with $a = b$: $a = 5.2$, 2.6, 1.3, 0.6 , 0.3, 0.2, 0.1 mm. (a1), (b1), (c1), (d1), (e1), (f1), (g1), (h1) encrypted results for Elaine, Cameraman, Peppers, Baboon, respectively. (a2) - (a8) decrypted Elaine, (b2) - (b8) decrypted Cameraman, (c2) - (c8) decrypted Peppers, and (d2) - (d8) decrypted Baboon, (e2) - (e8) decrypted Airplane, (f2) - (f8) decrypted Bridge, (g2) - (g8) decrypted Milkdrop, (h2) - (h8) decrypted Lax.

3.3.3 Histogram

The histograms of ciphered images should obey a fairly uniform distribution. Fig.

3.5 (a1), (b1), (c1), (d1) (e1), (f1), (g1) and (h1) shows the histograms of the original images Elaine, Cameraman, Peppers and Lake, Airplane, Bridge, Milkdrop and Lax, respectively. Histograms of the corresponding encryption results for $a = 5.2$ mm are shown in Fig. 3.4 (a2), (b2), (c2) (d2), (e2), (f2), (g2) and (h2). For other values of a, such as 2.2 mm and 1.2 mm, the histograms of the encrypted images are shown in Fig. 3.5 (a3), (b3), (c3), (d3), (e3), (f3), (g3) and (h3) and (a4), (b4), (c4), (d4), (e4), (f4), (g4) and (h4), respectively. Although the histograms of the four original images are different from each other, the histograms of ciphered images are almost the same, following a nearly uniform distribution. Thus, one believes that the attackers cannot obtain any useful information by histogram analysis.



(a1) (a2) (a3) (a4)

(b1) (b2) (b3) (b4)

(c1) (c2) (c3) (c4)

(d1) (d2) (d3) (d4)

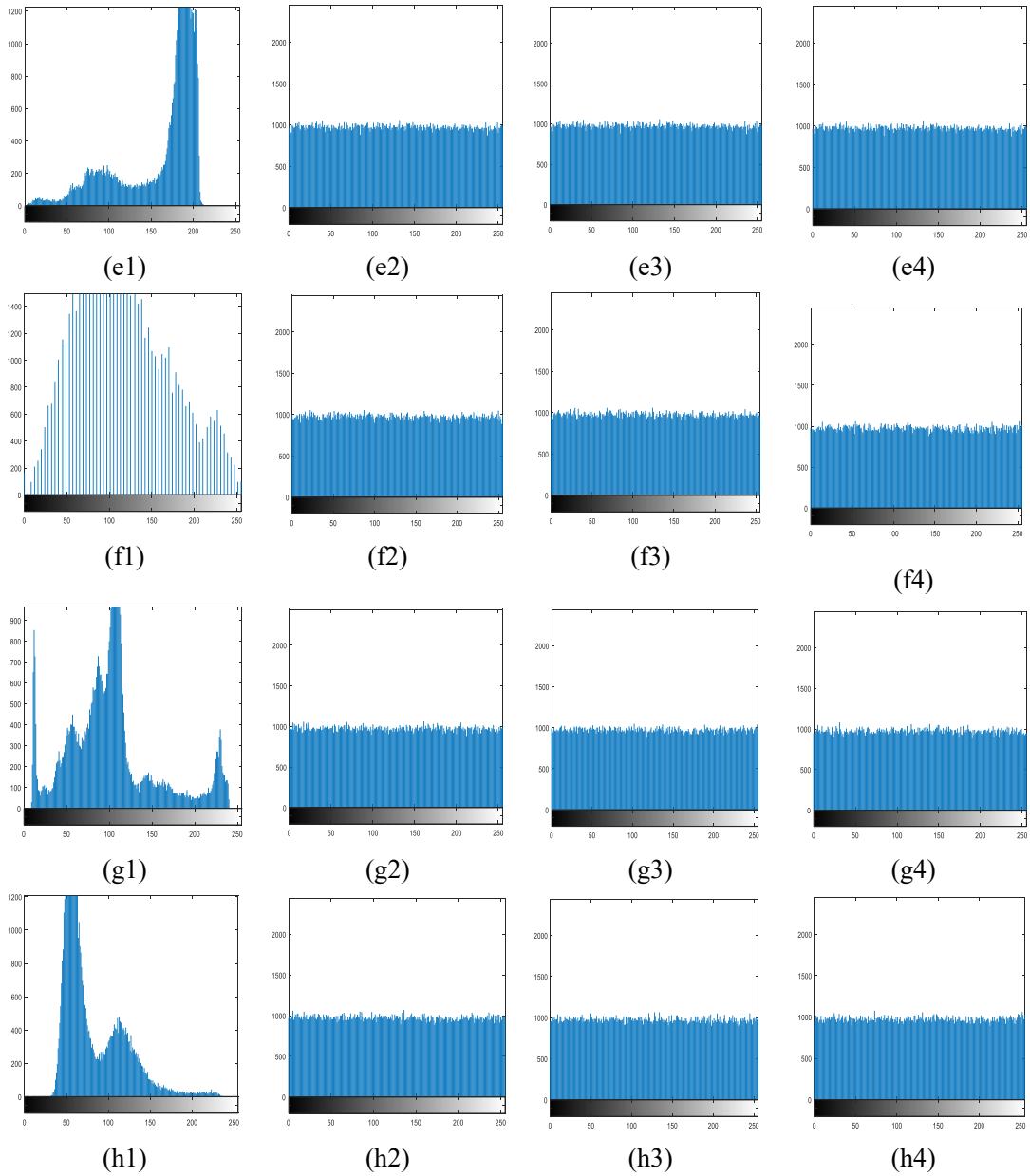


Fig. 3.5 Histograms of original images (a1) Elaine, (b1) Cameraman, (c1) Peppers, (d1) Lake, (e) Airplane, (f) Bridge, (g) Milkdrop and (h) Lax. and histograms of encrypted images for different side-lengths of hard aperture: (a2), (b2), (c2), (d2), (e2), (f2), (g2) and (h2) for $a = 5.2$ mm; (a3), (b3), (c3), (d3) (e3), (f3), (g3) and (h3) for $a = 2.2$ mm; (a4), (b4), (c4), (d4), (e4), (f4), (g4) and (h4) for $a = 1.2$ mm.

3.3.4 Correlation of adjacent pixels

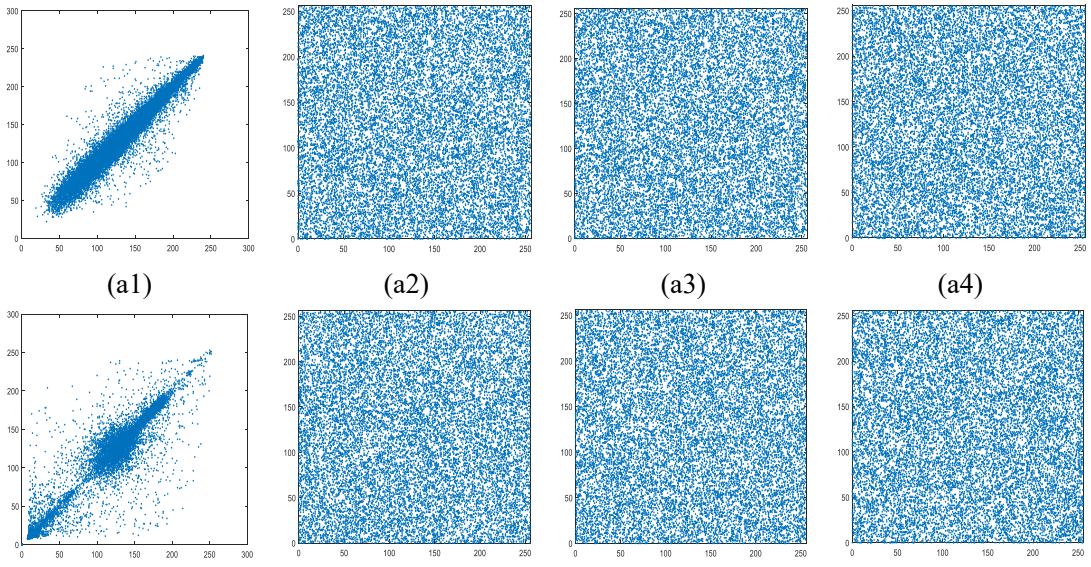
Images Elaine Cameraman, Girl, Cameraman, Car and Airplane are used to make a correlation analysis of neighborhood pixels between the cipher and plaintext images and five different values of aperture side-lengths, $a = 5.2,\ 4.2, 3.2,\ 2.2$, 1.2 mm, are selected. Table 1 shows numerically the correlation coefficients of proposed encryption algorithm and the algorithm in Ref. [25]. From Table 3.1 and Fig. 3.6, it can be seen

that the adjacent pixels of original images have a very strong correlation, while the correlation in cipher-text is very weak, hence the proposed apertured FrMT based image encryption algorithm is capable of resisting correlation analysis attack.

Table 3.1 Correlation coefficients between two adjacent pixels

Algorithm	Image	Value a (mm)	Horizontal direction	Vertical direction	Diagonal direction
Proposed algorithm	Plain Elaine		0.9589	0.9526	0.9276
	Encrypted Elaine	5.2	0.0014	–0.0101	0.0039
		4.2	0.0089	0.0078	0.0002
		3.2	0.0011	0.0021	–0.0039
		2.2	–0.0029	–0.0035	–0.0137
		1.2	0.0051	–0.0067	–0.0016
	Plain Lena		0.9594	0.9193	0.9056
	Encrypted Lena	5.2	0.0118	0.0053	–0.0087
		4.2	–0.0073	0.0078	0.0074
		3.2	0.0098	0.0028	0.0031
		2.2	0.0123	0.0046	–0.0040
		1.2	0.0105	–0.0017	–0.0013
	Plain Girl		0.9666	0.9565	0.9383
	Encrypted Girl	5.2	-0.0040	0.9691	0.9623
		4.2	-0.0055	0.0126	0.0068
		3.2	-0.0145	0.0058	-0.0079
		2.2	-0.0024	0.0030	8.8940e-04
		1.2	0.0146	0.0135	0.0050
	Plain Cameraman		0.9600	0.9394	0.9083
	Encrypted Cameraman	5.2	0.0101	–0.0117	0.0034
		4.2	0.0116	0.0008	–0.0106
		3.2	–0.0037	–0.0053	–0.0039
		2.2	0.0024	–0.0017	0.0062
		1.2	0.0080	–0.0040	0.0099
	Plain Car		0.9688	0.9846	0.9558
	Encrypted Car	5.2	-0.0028	-0.0027	-0.0017
		4.2	0.0150	0.0030	-0.0060

		3.2	-0.0086	0.0167	-0.0033
		2.2	-0.0015	-0.0058	-0.0067
		1.2	-0.0083	6.2277e-05	-0.0130
	Plain Airplane		0.9151	0.9066	0.8499
		5.2	-0.0073	--0.0073	9.6368e-04
		4.2	0.0011	0.0095	0.0149
	Encrypted	3.2	-0.0072	-0.0165	4.0915e-04
	Airplane	2.2	-0.0077	0.0032	0.0102
		1.2	-0.0034	0.0188	-3.1146e-04
Ref. [25]	Encrypted Lena		0.1089	0.0878	0.0683
	Encrypted Elaine		0.0523	0.0808	0.0481



(a1) (a2) (a3) (a4)

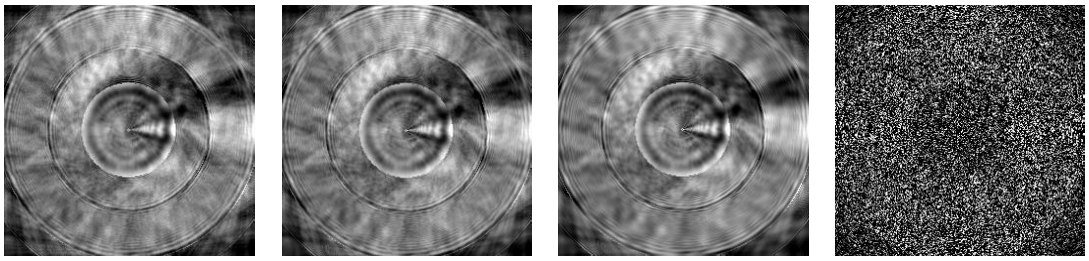
(b1) (b2) (b3) (b4)

Fig. 3.6 Graphical representation of correlations of a pair of horizontally adjacent pixels in (a1) Elaine, (a2), (a3), and (a4) encrypted Elaine with $a = 5.2$ mm, $a = 2.2$ mm, $a = 1.2$ mm, respectively (b1) Cameraman, (b2), (b3), and (b4) encrypted Cameraman with $a = 5.2$ mm, $a = 2.2$ mm, $a = 1.2$ mm, respectively.

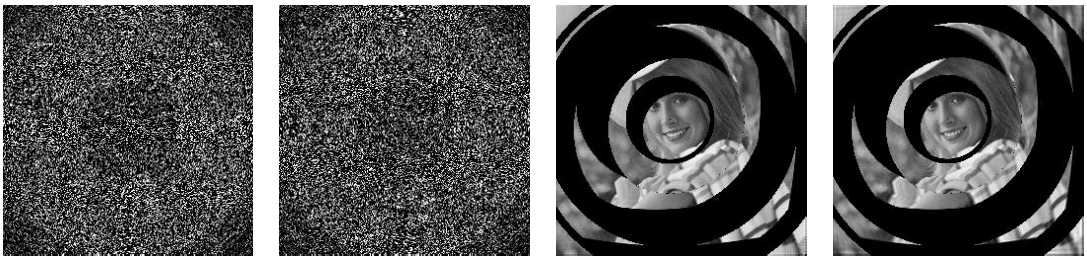
3.3.5 Key-sensitivity and key space analyses

Three different values 5.2, 2.6, 1.3 mm of aperture side-lengths are used to analyze

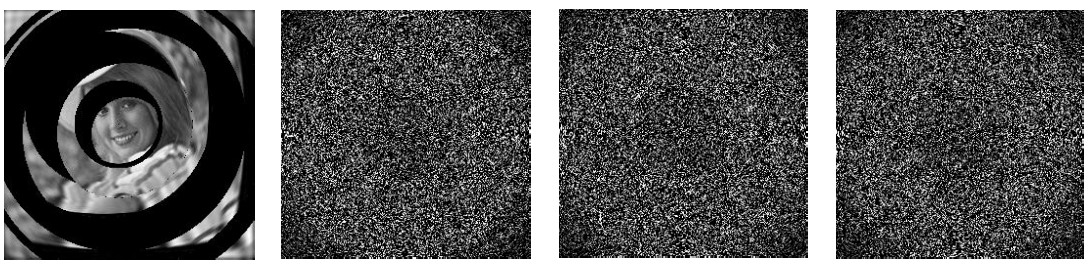
the key sensitivity. Fig. 3.7 shows the decrypted results of Elaine with incorrect keys. Fig. 3.7(a1) - (a3) illustrate the decrypted images with incorrect FrMT orders $p_i = 0.55,\ i = 1, 2, \ldots, N$, Figs. 3.7(b1) - (b3) present the decrypted images with incorrect FrFT orders $q_i = 0.55,\ i = 1, 2, \ldots, N$. The decrypted images with incorrect outer radii of the annular, $r_1 = 40,\ r_2 = 75,\ r_3 = 110,\ r_4 = 150,\ r_5 = 181$ are illustrated in Fig. 3.7(c1) - (c3). The decrypted images with interference phase $\theta_j = \theta_j + \theta_r,\ j,\ r = 1,2, \ldots, N$ are given in Fig. 3.7 (d1) - (d3), θ_r is the random phase whose value distributes in (–1, 1). Similarly, replacing another correct phase key with interference phase $\psi_j' = \psi_j + \psi_r,\ j,\ r = 1,2, \ldots, N$, the decrypted images are shown in Fig. 3.7(e1) - (e3), where ψ_r is the random phase whose value also distributes in (–1, 1). The incorrect wavelength $\lambda = 655.8$ nm is used for decrypting process and the decrypted images are shown in Fig. 3.7(f1) - (f3). Changing the side-length of aperture with $a + 0.05$ mm for decrypting process, the decrypted images are shown in Fig. 3.7 (g1) - (g3). From those results, one can see that the encrypted results change dramatically in spite of a small deviations to the keys used in decryption. It indicates that the proposed image encryption scheme is sufficiently sensitive to the keys.



(a1) $a = 5.2$ mm (a2) $a = 2.6$ mm (a3) $a = 1.3$ mm (b1) $a = 5.2$ mm



(b2) $a = 2.6$ mm (b3) $a = 1.3$ mm (c1) $a = 5.2$ mm (c2) $a = 2.6$ mm



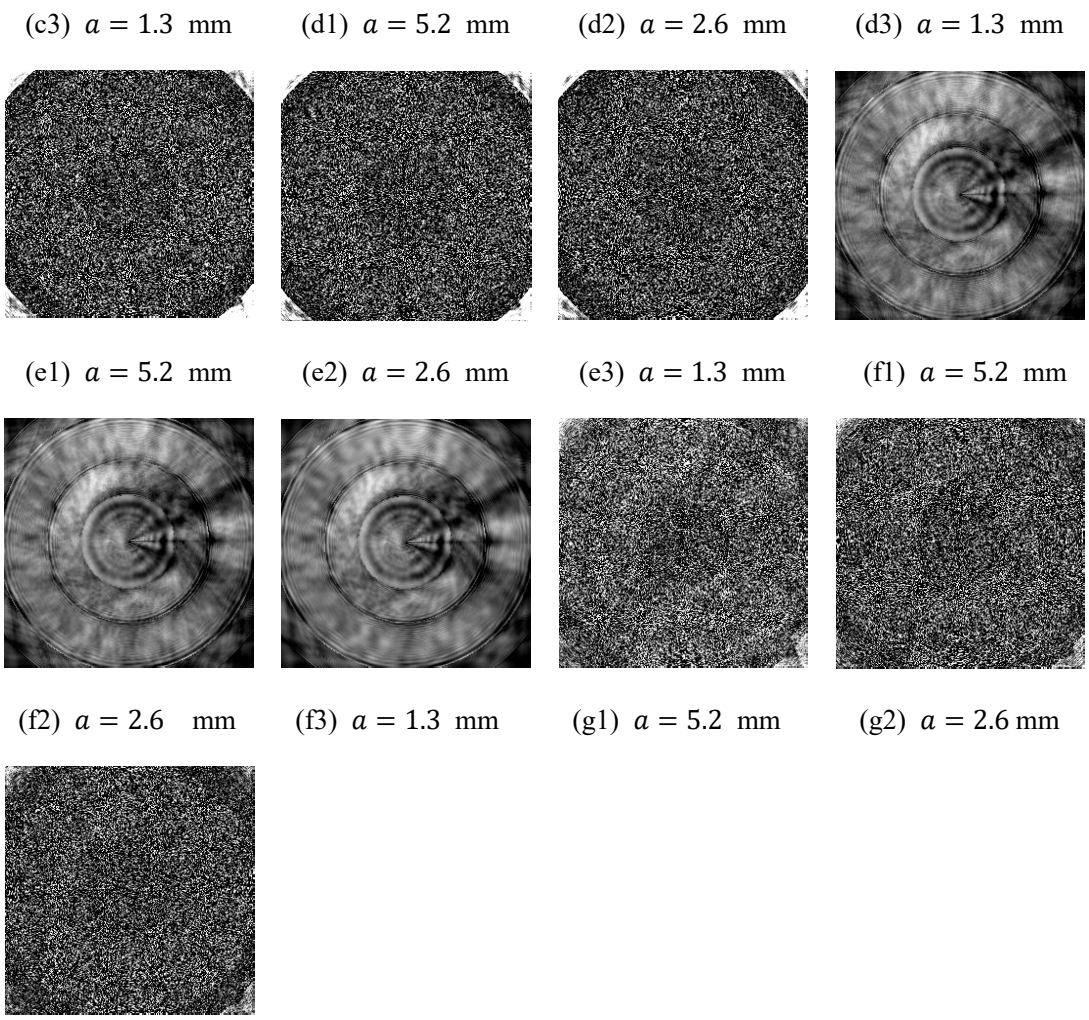
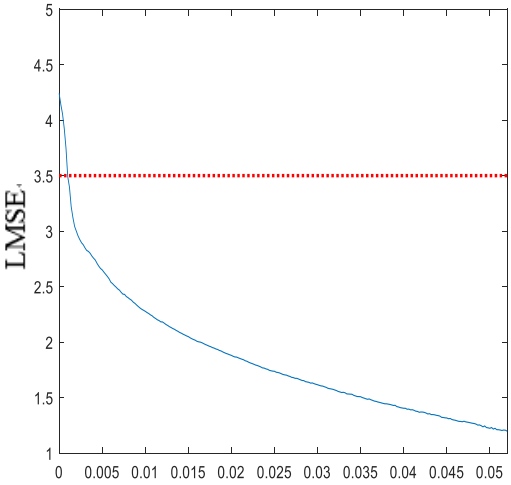
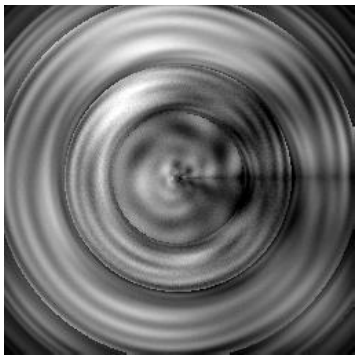


Fig. 3.7 Decrypted Elaine with incorrect keys with different side-lengths of the aperture: (a1) - (a3) wrong apertured FrMT order, (b1) - (b3) wrong FrFT order, (c1) - (c3) wrong outer radii, (d1) - (d3) wrong θ_i, (e1) - (e3) wrong ψ_i, (f1) - (f3) wrong wavelength λ, (g1) - (g3) wrong side-length a.

To analyze the key space, the logarithm of mean square error (LMSE) is introduced to evaluate the quality of the decrypted images. Fig. 3.8 demonstrates that LMSE is inversely proportional to the hard aperture side-length.



(a)



(b)

Fig. 3.8 (a) The deviations of LMSE curve of proposed scheme versus side-lengths of aperture a, (b) Decrypted image corresponding to LMSE=3.5.

To evaluate the key space of θ_i and ψ_i, $i = 1, 2, \ldots, N$ more clearly, all phases θ_i, ψ_i, $i = 1, 2, \ldots, N$ are allowed to fluctuate within certain limits. New keys θ_i' and ψ_i', $i = 1, 2, \ldots, N$ are set close to the correct keys for decrypting images denoted as:

$$\begin{cases} \theta_i' = \theta + \Delta\theta_i \\ \psi_i' = \psi + \Delta\psi_i \end{cases} \tag{3.15}$$

$$\begin{cases} \Delta\theta_i = d\theta_{Ri} \\ \Delta\psi_i = d\psi_{Ri} \end{cases} \tag{3.16}$$

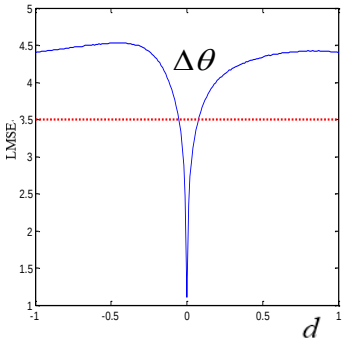
where θ_{Ri} and ψ_{Ri} $(i = 1, 2, \ldots, N)$ are random phases within the range (-1, 1), d is a coefficient ranged from $-\pi$ to π.

The deviations of LMSE versus d are shown in Fig. 3.9. The threshold of LMSE is 3.5, which is marked by a red dash line. When the LMSE is less than the threshold, the partial or total information of original image can be recovered visually [25]. Δd is

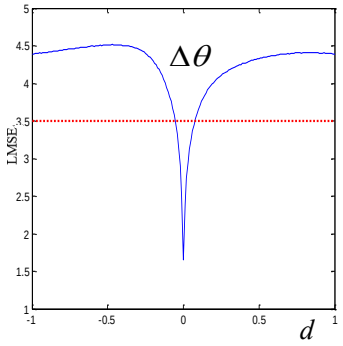
denoted as the width which the deviation of LMSE versus d is below the threshold. Because of the effective range Δd, the number of possible values of each point of the key can be calculated according to following formula:

$$k_d = \begin{cases} \dfrac{2\pi}{\Delta d}, & \text{for } \theta,\ \psi \\ \dfrac{2}{\Delta d}, & \text{for } p, q \end{cases} \tag{3.17}$$

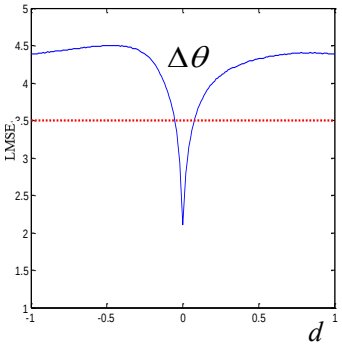
Therefore, the key space of θ, ψ, p, or q is k_d^5 (k_d's are different for different keys). The key space of θ, ψ, p and q are shown in Table 3.2.



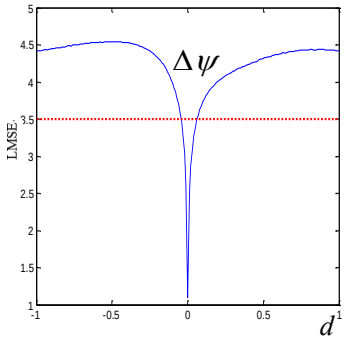
(a1) $a = 5.2$ mm



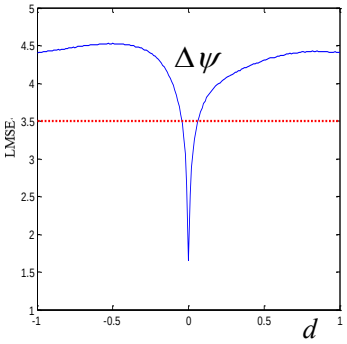
(a2) $a = 2.6$ mm



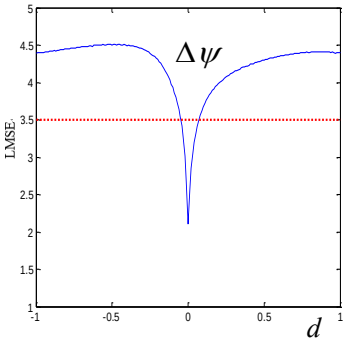
(a3) $a = 1.3$ mm



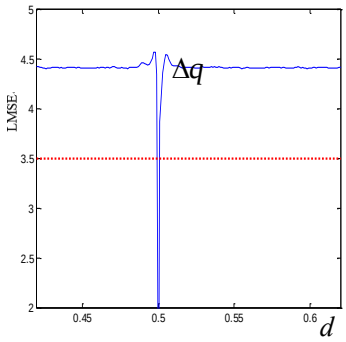
(b1) $a = 5.2$ mm



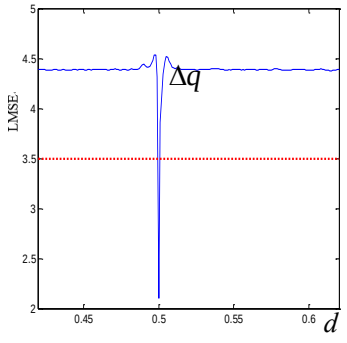
(b2) $a = 2.6$ mm



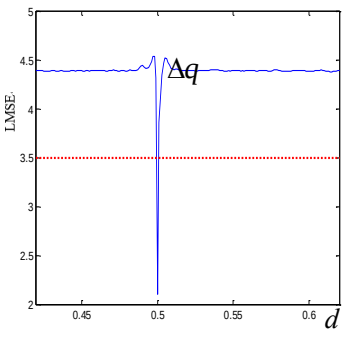
(b3) $a = 1.3$ mm



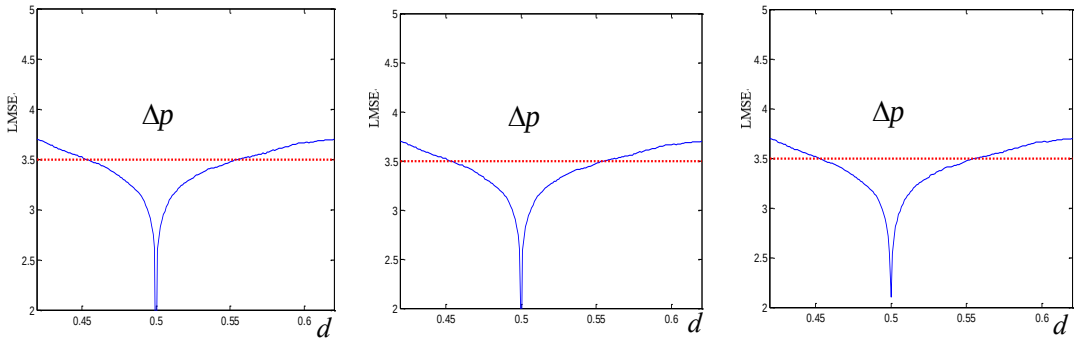
(c1) $a = 5.2$ mm



(c2) $a = 2.6$ mm



(c3) $a = 1.3$ mm



(d1) $a = 5.2$ mm (d2) $a = 2.6$ mm (d3) $a = 1.3$ mm

Fig. 3.9 LMSE curves with different aperture side-lengths for (a1) - (a3) θ, (b1) - (b3) ψ, (c1) - (c3) p, (d1) - (d3) q.

The key space of the proposed scheme is

$$K = k_\theta \times k_\psi \times k_q \times k_p \times k_x \times k_\mu \tag{3.17}$$

where k_θ, k_ψ, k_q, k_p and (k_x, k_μ) denotes the key space of the phase θ, the phase ψ, the order p of FrMT, the order q of FrFT, the seeds of logistic map, respectively . Under different conditions of size-length of aperture, $a = 5.2$, $a = 2.6$, $a = 1.3$ mm, K can be calculated by substituting the values of k_θ, k_ψ, k_q, k_p in Table 3.2 into Eq. (32) and (k_{x_1}, k_μ) with precision of 1×10^{-15}:

$$K = \begin{cases} 2.4744 \times 10^{39} \times 10^{30} = 1.2582 \times 2^{230}, \text{for } a = 5.2 \text{ mm} \\ 4.1057 \times 10^{39} \times 10^{30} = 2.6775 \times 2^{230}, \text{for } a = 2.6 \text{ mm} \\ 2.5021 \times 10^{39} \times 10^{30} = 2.1183 \times 2^{230}, \text{for } a = 1.3 \text{ mm} \end{cases} \tag{3.18}$$

Thus, the total key space of the proposed scheme is at least 2^{230}, which is large enough to resist brute-force attacks.

Besides a sufficiently large key space, the outer radii of the annular r_i, $i = 1, 2, \ldots, 5$, the side-lengths a, b and the wavelength λplay an important role and further enlarge the key space.

Table 3.2 Key space of θ, ψ, p, q

Image Lena		Side-lengths: a (mm)		
		5.2	2.6	1.3
θ	Δd_θ	0.1160	0.1153	0.1147
	k_θ	54.1654^5	54.4942^5	54.7793^5
ψ	Δd_ψ	0.1030	0.1058	0.1173
	k_ψ	61.0018^5	59.3874^5	53.5651^5
p	Δd_p	0.1028	0.1029	0.1028
	k_p	19.4553^5	19.4363^5	19.2864^5

q	Δd_q	0.0017	0.0014	0.0014
	k_p	1176.5^5	1428.5^5	1428.6^5

Table 3.3 lists the LMSEs when deviations Δp of the order of FrMT of the proposed encryption algorithm and the algorithms in [25] and [145] are 0.05. It can be seen that these values of LMSE are very close. The LMSEs versus deviation Δq at order of FrFT 0.7 are shown in Table 3.4, which reveal that the performance using FrFT in proposed algorithm is better than the one in [25] and [145].

Table 3.3 LMSE versus deviation $\Delta p = 0.05$ at order of FrMT $p = 0.3$.

Algorithm	FrMT order p
Proposed algorithm ($a = 5.2$ mm)	3.7020
Ref. [25]	3.7160
Ref. [145]	3.6990

Table 3.4 LMSE versus deviation $\Delta q = 0.05$ at order of FrFT $q = 0.7$.

Algorithm	FrFT order q
Proposed algorithm ($a = 5.2$ mm)	4.4150
Ref. [25]	3.8976
Ref. [45]	3.6990

The LMSE between the decrypted image and the original one varying with the number of incorrect outer radii of the annular domains is given in Fig. 3.10. The MSE between the decrypted images and the original image becomes higher when the incorrect radii increase.

Table 3.5 MSE versus deviation $\Delta p = 0.05$ at order of FrMT $p = 0.5$ and Run time for different N.

Number	N=2	N=3	N=4	N=5	N=6	N=7
MSE	1.7265e+03	1.7351e+03	1.8086e+03	1.8112e+03	1.7757e+03	1.7937e+03
Time (s)	43.347435	44.703182	49.2094	54.719876	72.070509	77.467377

Table 3.5 shows the performance of proposed algorithm caused by different N. The MSE versus deviation $\Delta p = 0.05$ for different N is shown in table 3.5. However, with

the increase of N, the run time of simulation gets longer on a same computer platform.

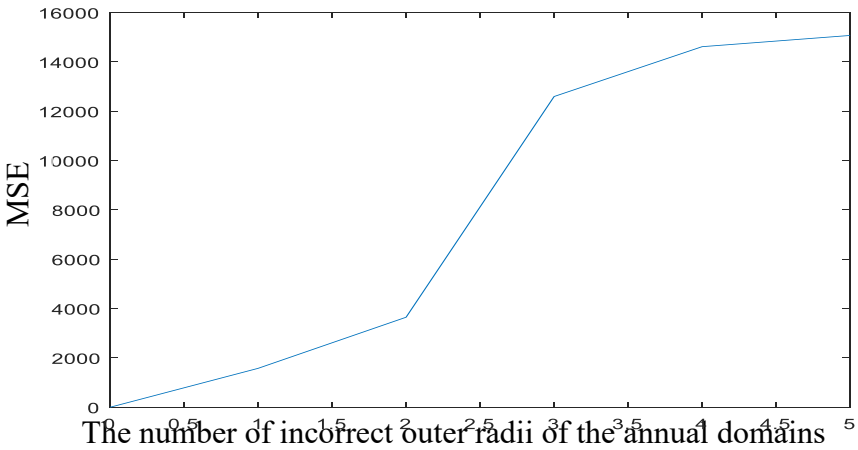


Fig. 3.10. LMSE curve for the number N of incorrect outer radii of the annular domains.

3.3.6. Information entropy analysis

Information entropy is a quantitative measurement that makes sure how random the texture of an image is. Table 3.6 indicates the entropies of proposed algorithm and the one of Ref. [25]. The results shown in Table 3.6 prove that the entropies of the encrypted image for different aperture side-lengths are close to expected value 8. Hence, the proposed scheme is capable of resisting entropy analysis attacks.

Table 3.6 Entropies of encrypted images for the proposed algorithm for different side-lengths (mm).

Algorithm	Image	Original	Encrypted				
			$a = 5.2$	$a = 4.2$	$a = 3.2$	$a = 2.2$	Average
Proposed algorithm	Cameraman	7.0030	7.9992	7.9993	7.9993	7.9994	7.99933
	Peppers	7.3656	7.9992	7.9993	7.9992	7.9992	7.99923
	Lake	7.4893	7.9994	7.9992	7.9992	7.9992	7.99925
	Lena	7.2157	7.9993	7.9993	7.9993	7.9993	7.99930
	Girl	7.0782	7.9993	7.9993	7.9992	7.9992	7.99925
	Car	3.1232	7.9992	7.9993	7.9993	7.9993	7.99924
	Airplane	6.7111	7.9993	7.9992	7.9992	7.9992	7.99923
Ref. [25]	Cameraman	7.0030					7.86270
	Peppers	7.3656					7.85630
	Lake	7.4893					7.85660
	Lena	7.2157					7.71550

3.3.7. Differential attacks

The experimental NPCR and UACI results are listed in Table 3.7 and Table 3.8, respectively, from which it can be seen that all of the NPCRs are very close to the expected value 99.6054% and the UACIs are very close to the expected value 33.4635%. As a result, the proposed scheme is believed to be insensitive to plain-text changes.

Table 3.7 The NPCR of encrypted images for proposed algorithms for different side-length (mm).

Image	$a = 5.2$	$a = 4.2$	$a = 3.2$	$a = 2.2$	$a = 1.2$
Elaine	99.5964%	99.6236%	99.6112%	99.5940%	99.6020%
Cameraman	99.5804%	99.5932%	99.6176%	99.6196%	99.6164%
Peppers	99.6096%	99.5960%	99.6208%	99.6292%	99.6008%
Lake	99.6104%	99.6060%	99.6180%	99.5968%	99.5984%
Girl	99.6168%	99.6088%	99.6084%	99.6208%	99.5992%
Car	99.5792%	99.5924%	99.6172%	99.6108%	99.5896%
Airplane	99.6068%	99.6044%	99.5988%	99.6148%	99.6248%

Table 3.8 The UACI of encrypted images for proposed algorithms for different side-length (mm).

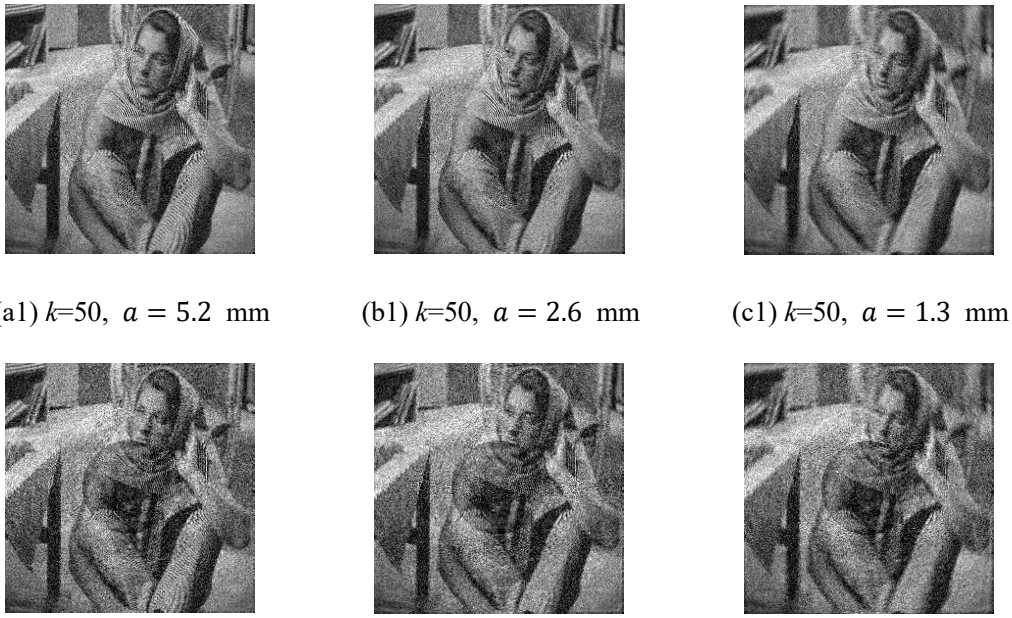
Image	$a = 5.2$	$a = 4.2$	$a = 3.2$	$a = 2.2$	$a = 1.2$
Elaine	33.4586%	33.5034%	33.4265%	33.3623%	33.4124%
Cameraman	33.4684%	33.4142%	33.5138%	33.4068%	33.5124%
Peppers	33.4855%	33.4568%	33.4886%	33.4634%	33.5207%
Lake	33.3645%	33.5368%	33.5171%	33.4769%	33.4417%
Girl	33.5190%	33.5041%	33.3501%	33.4908%	33.4156%
Car	33.4833%	33.4805%	33.3953%	33.4192%	33.4181%
Airplane	33.4578%	33.4844%	33.4530%	33.4819%	33.5102%

3.3.8 Noise attack and robustness analysis

The Gaussian noise is added into the encrypted image to test the ability of this proposed scheme to resist noise attacks:

$$C' = C + kG \tag{3.19}$$

where C' and C are encrypted image with and without noise, respectively, k indicates the strength of the Gaussian noise G with zero-mean and unit standard deviation. The major information of the decrypted images is still visible within a certain range of noise as shown in Fig. 3.11 and Table 3.9, although the decrypted image becomes blurrier. It is shown that the proposed scheme can resist the noise attacks to a certain extend.



(a1) k=50, $a = 5.2$ mm (b1) k=50, $a = 2.6$ mm (c1) k=50, $a = 1.3$ mm

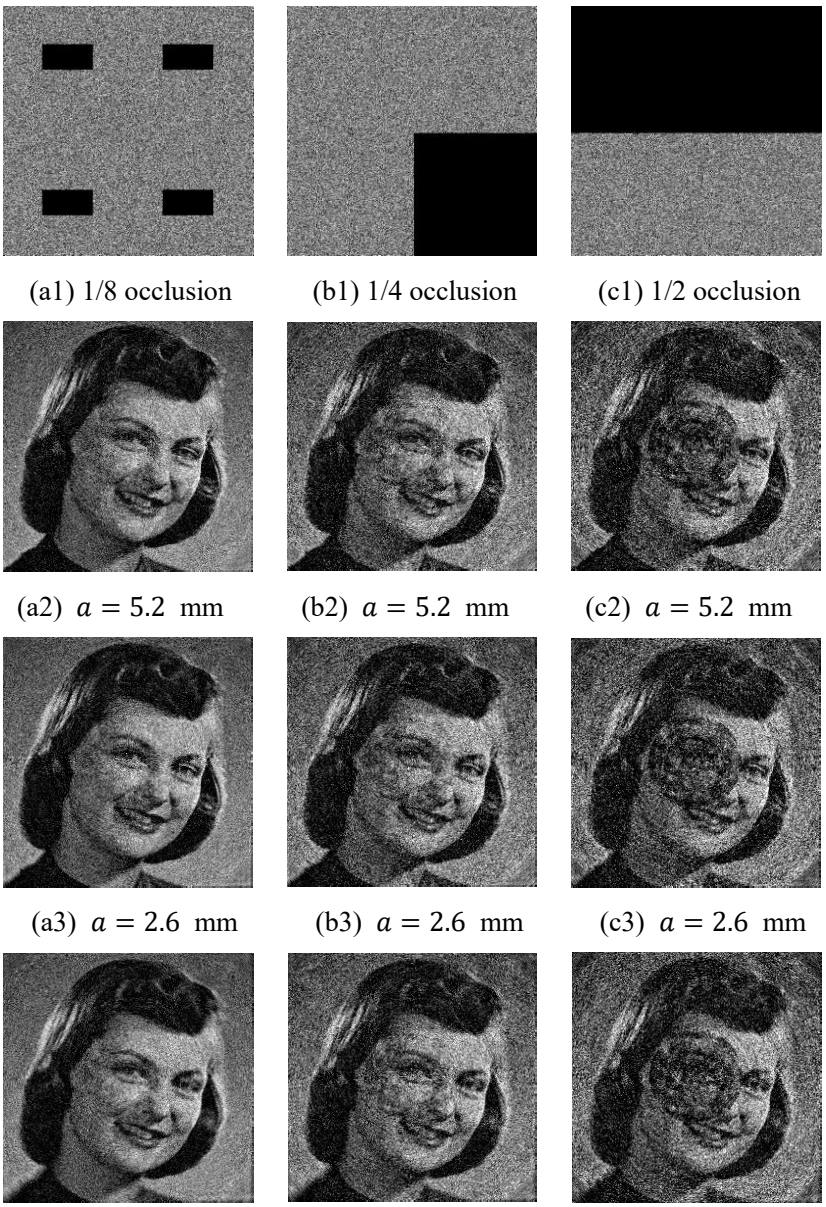
(a2) k=100, $a = 5.2$ mm (b2) k=100, $a = 2.6$ mm (c2) k=100, $a = 1.3$ mm

Fig. 3.11 Results of noise attack: (a1) k=50, $a = 5.2$ mm, (a2) k=100, $a = 5.2$ mm, (b1) k=50, $a = 2.6$ mm, (b2) k=100, $a = 2.6$ mm, (c1) k=50, $a = 1.3$ mm, (c2) k=100, $a = 1.3$ mm.

Table 3.9 LMSE for noise attacks for different side-length (mm).

Noise	$a = 5.2$	$a = 2.6$	$a = 1.3$
K=50	2.6243	2.7074	2.7935
K=100	2.9425	2.9789	3.0161

The capability for resisting the occlusion of the encrypted image is analyzed. The decrypted results for encrypted images with 1/4, 1/2 and 1/8 occlusions are shown in Fig. 3.12(a1), (b1) and (c1), respectively. The corresponding decrypted images under different aperture side-lengths are shown in Figs. 3.11(a2) - (a4), (b2) - (b4) and (c2) - (c4), respectively. From Fig. 3.12 and Table 3.10, one can observe that although the decrypted images are cut off to different degrees, the main information of the original image remains with correct keys.



(a1) 1/8 occlusion (b1) 1/4 occlusion (c1) 1/2 occlusion

(a2) $a = 5.2$ mm (b2) $a = 5.2$ mm (c2) $a = 5.2$ mm

(a3) $a = 2.6$ mm (b3) $a = 2.6$ mm (c3) $a = 2.6$ mm

(a4) $a = 1.3$ mm (b4) $a = 1.3$ mm (c4) $a = 1.3$ mm

Fig. 3.12 Results for occlusion of encrypted data. Encrypted images with (a1) 1/4, (b1) 1/2, (c1) 1/8 occlusion. Under the different values of aperture widths, decrypted images for (a2), (a3), (a4) with 1/4 occlusion, decrypted images for (b2), (b3), (b4) with 1/2 occlusion, decrypted images for (c2), (c3), (c4) with 1/8 occlusion.

Table 3.10 LMSE for 1/8, 1/4 and 1/2 occlusion for different side-length (mm).

Occlusion	$a = 5.2$	$a = 2.6$	$a = 1.3$
1/8	3.0798	3.0804	3.0938
1/4	3.2867	3.2885	3.2928
1/2	3.3726	3.3701	3.3750

3.4 Summary

An optical image encryption scheme based on a fractional Mellin transform with a hard aperture is presented. The amount of light passing the lens can be controlled and adjusted by the size of the hard aperture. This proposed scheme can effectively reduce light leakage at the edge of the lens, which resists the direct attack for optical information to some extent. Furthermore, in practice the application scenario of the proposed image encryption scheme is close to actual situation where a marginal leakage of light is often unavoidable. According to simulation, it is known that the size of the hard aperture has an influence to the key space. In addition, the sufficiently large key space of the encryption system is huge to resist common attacks, such as statistical analysis attacks, noise attacks occlusion attacks. Furthermore, the performances of the encryption system is insensitive to plain-text changes, i.e., capable of resisting differential attacks. It is worth noting that the nonlinearity of FrMTs guarantees that the proposed encryption scheme is a nonlinear one and capable of resisting known plain-text and chosen plain-text attacks.

Chapter 4

Image encryption based on a reality-preserving Gaussian apertured FrMT

In chapter 3, an image encryption scheme based on apertured FrMT is discussed. Although the nonlinearity of the apertured FrMT guarantees that the proposed encryption scheme is a nonlinear one and capable of resisting known plain-text and chosen plain-text attacks, the obtained cipher-text is complex value which is inconvenient for display, transmission and storage. Thus, an image encryption scheme based on a Gaussian apertured reality-preserving FrMT (GARPFrMT) is proposed. The GARPFrMT was realized in the diffraction domain. The Gaussian aperture, like a soft aperture, improved the amount of light that passed through the lens compared to a hard aperture and reduced the light leakage at the edge of the lens, assisting to some extent in resisting direct attacks. In the proposed scheme, the reality-preserving transform was constructed in the diffraction domain to ensure that the cipher-text is real. The GARPFrMT is a nonlinear transformation used for eliminating potential insecurity existing in the linear image encryption system. In order to further enhance the security of the encryption system, an Arnold transform, and a bitwise XOR operation were employed for permutation and scrambling in the encryption process. Simulation results and theoretical analysis show that the proposed algorithm is feasible and capable of withstanding several common attacks.

4.1 Introduction

Sheridan also indicated that FrFT is a linear transformation, which rotates the signal through any arbitrary angle into a mixed frequency-space domain. However, to some extent, the linear FrFT-based encryption system has some potential security risks [42, 52]. To avoid the disadvantages stemming from the linearity of classical DRPE, Wang [15] proposed an encryption algorithm based on nonlinear amplitude-truncation and

phase-truncation in the Fourier domain. Joshi et al. [109] proposed a nonlinear image encryption scheme for color images, using natural logarithms and FrFT, which showed better anti-attack performance than linear image encryption methods.

Zhou [25-28] proposed a series of nonlinear image encryption algorithms based on fractional Mellin transform (FrMT). FrMT itself is a nonlinear transform that makes the nonlinearity of the encryption system convenient and useful. Because of those proposed nonlinear encryption systems, high robustness and sensitivity to the cipher keys are achieved. To simplify encryption process and enhance the sensitivity for fractional orders of FrMT, Zhou [26] proposed an improved encryption algorithm based on a multi-order discrete fractional Mellin transform. However, the aforementioned encryption algorithms based on FrMT [25-27] finally obtained complex-valued cipher-text. In general, complex-values have some inconvenience in display, transmission and storage. Consequently, Zhou [28] proposed an image encryption algorithm based on a reality-preserving fractional Mellin transform (RPFrMT), whose cipher-text is real-valued data. Lang [93] proposed an image encryption algorithm using the reality-preserving multiple-parameter FrFT and chaos permutation. Lang [94] applied the reality-preserving method in color image. A reality-preserving image encryption scheme with the generalized Hilbert transform was given by Li [95]. Wu [63] proposed a reality-preserving encryption method based on fractional discrete cosine transform.

This chapter proposes an image encryption scheme based on a Gaussian apertured reality-preserving FrMT. The apertured FrMT is realized through the log-polar transform and apertured FrFT. Since the lens with Gaussian apertures is variable and non-uniform, such as a soft aperture edge diaphragm, the intensity distributions of the output laser are improved, which facilitates resistance to possible attacks for obtaining some useful information from the marginal leakage of light in the optical encryption systems. Thus, the Gaussian aperture is chosen to construct the apertured FrMT. Within the framework of paraxial approximation, the apertured FrFT can be implemented using the Collins diffraction integral formula. To obtain the real-valued encrypted data, the Gaussian apertured reality-preserving FrMT (GARPFrMT) is constructed.

The rest of this chapter is arranged as follows: In Section 4.2, the Gaussian apertured FrFT optical system is introduced. In Section 4.3, an encryption algorithm for gray image based on RPGAFrMT is presented in detail. In Section 4.4, simulations and analyses are given. The encryption scheme on color image is described in Section 4.5. The experimental results and analyses are demonstrated in Section 4.6. The conclusions

are drawn in Section 4.7.

4.2 Gaussian apertured FrFT optical system

Gaussian apertured FrFT can be performed in the diffraction domain in an optical system, as shown in Fig. 4.1. The lens is a Gaussian lens, f is the focal length with respect to the standard focal length f_s, and $d = f_s \tan(\phi/2)$ is the transmission distance, where $\phi = p \times \pi/2$, p is the fractional order of the Gaussian apertured FrFT.

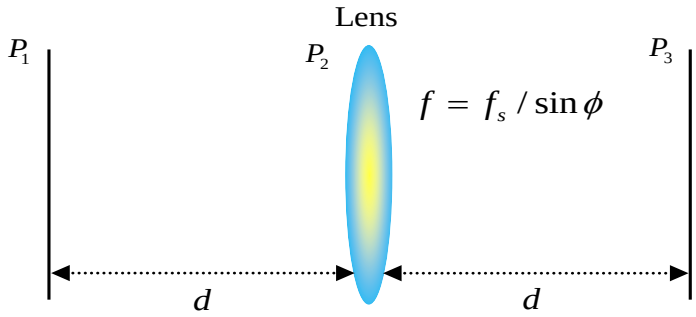


Fig. 4.1 An optical system for the Gaussian apertured FrFT

Within the framework of the paraxial approximation, the field of light propagation across the optical system as shown in Fig. 4.1 is divided into two ABCD optical systems in accordance with the Collins diffraction integral formula [40]. $\{A_1, B_1, C_1, D_1\}$ and $\{A_2, B_2, C_2, D_2\}$ are respectively the elements of the transfer matrices of the two sections:

$$\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \tag{4.1}$$

$$\begin{pmatrix} A_2 & B_2 \\ C_2 & D_2 \end{pmatrix} = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1/f & 1 \end{pmatrix} = \begin{pmatrix} 1 - d/f & d \\ -1/f & 1 \end{pmatrix} \tag{4.2}$$

For the optical field $E(x_1, y_1)$ at P_2, the following integral equation from P_1 to P_2 can be computed as:

$$\begin{aligned} E_1(x,y) &= F^{(A_1,B_1,C_1,D_1)}\{f(x,y)\} \\ &= \frac{1}{\mathrm{i}\lambda B} \iint_{-\infty}^{\infty} f(x,y) \\ &\times \exp\left(\mathrm{i}\frac{2\pi}{2\lambda B}[A(x^2+y^2) - 2(xx_1+yy_1) + D(x_1^2+y_1^2)]\right)\mathrm{d}x\mathrm{d}y \end{aligned} \tag{4.3}$$

where $F^{(A_1,B_1,C_1,D_1)}$ is the two-dimensional Collins diffraction transform with the

incidence wavelength λ and $f(x,y)$ is the optical field at P_1.

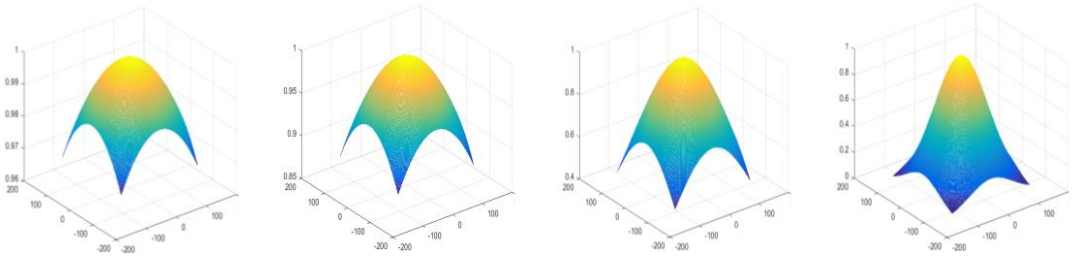
For the optical field $E(x_2,y_2)$ at P_3, the integral equation from the lens plane P_2 to the output plane P_3 is:

$$\begin{aligned} E_2(x_2,y_2) &= F^{(A_2,B_2,C_2,D_2)}\{E_1(x_1,y_1)\} \\ &= \frac{1}{\mathrm{i}\lambda B}\iint_{-\infty}^{+\infty} E_1(x_1,y_1)K(x_1,y_1) \\ &\times \exp\left(\mathrm{i}\frac{2\pi}{2\lambda B}[A(x_1^2+y_1^2)-2(x_1x_2+y_1y_2)+D(x_2^2+y_2^2)]\right)\mathrm{d}x_1\mathrm{d}y_1 \end{aligned} \tag{4.4}$$

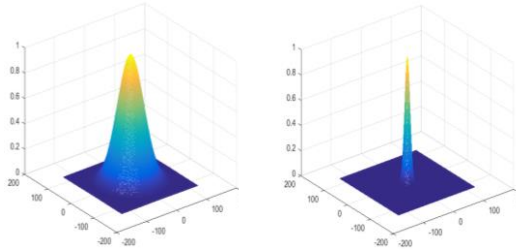
where $K(x_1,y_1)$ represents the Gaussian aperture shown in Fig. 4.2, which can be rewritten as

$$K(x_1,y_1) = e^{(-x_1^2/\sigma^2)} \times e^{(-y_1^2/\sigma^2)} \tag{4.5}$$

Then, the Gaussian apertured FrFT can be implemented through formulas (1) - (5) by changing the distance d and focal length of the lens f_s.



(a1) $\sigma = 1000$ (a2) $\sigma = 500$ (a3) $\sigma = 200$ (a4) $\sigma = 100$



(a5) $\sigma = 50$ (a6) $\sigma = 10$

Fig. 4.2 Normalized intensity distributions of Gaussian function for different standard deviations σ: $\sigma = 1000,\ 500,\ 200,\ 100,\ 50,\ 10$, respectively.

4.3. Image encryption based on a Gaussian apertured reality-preserving FrMT

4.3.1 Gaussian apertured fractional Mellin transform

The definition of Gaussian fractional Mellin transform is given as follows:

$$M^{(p_1,p_2)}(u,v) = C \cdot \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{f(x,y)}{x^2+y^2} \times K(x,y) \times \exp\left(-2\pi \mathrm{i}\left(\frac{u\ln\sqrt{x^2+y^2}}{\sin\phi_1} + \frac{v\arctan(y/x)}{\sin\phi_2}\right) + \pi \mathrm{i}\left(\frac{u^2+\ln^2\sqrt{x^2+y^2}}{\tan\phi_1} + \frac{v^2+[\arctan(y/x)]^2}{\tan\phi_2}\right)\right) \mathrm{d}x\mathrm{d}y \tag{4.6}$$

where $K(x,y) = e^{(-x^2/\sigma^2)} \times e^{(-y^2/\sigma^2)}$ is Gaussian aperture.

The GAFrMT can be obtained from fractional Fourier transform with aperture by a change of coordinates from rectangular Cartesian coordinates (x,y) to polar coordinates (ρ,θ). By letting $\rho = \ln\sqrt{x^2+y^2}$ and $\theta = \arctan(y/x)$, the relationship between the two-dimensional fractional Mellin transform and fractional Fourier transform is that the GAFrMT can be represented by log-polar transform and Gaussian apertured FrFT, i.e.,

$$M_G^{(p_1,p_2)}(u,v) = F_G^{(p_1,p_2)}\{f(\rho,\theta)\} \tag{4.7}$$

where the operators $M_G^{(p_1,p_2)}(\cdot)$ and $F_G^{(p_1,p_2)}(\cdot)$ represent Gaussian apertured FrMT and Gaussian apertured FrFT with same orders (p_1,p_2), respectively. Fig. 4.3 shows the optoelectronic hybrid setup to transform coordinates from (x,y) to (ρ,θ) and to implement the Gaussian apertured FrFT.

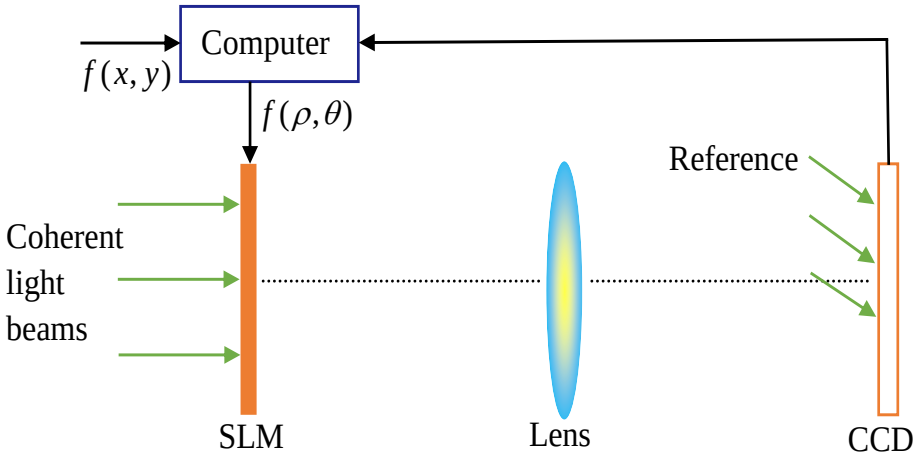


Fig. 4.3 Optoelectronic hybrid setup for apertured FrMT.

4.3.2 reality-preservation of fractional transform

I Venturini et al. [141] proposed a methodology to obtain reality-preserving forms of fractional transforms. Based on this methodology, Zhou et al. [28] gave a reality-preserving fractional Mellin transform. The reality-preserving fractional transform is reviewed briefly. If $x = \{x_1, x_2, \ldots, x_1\}^T$ is a real one-dimensional signal, then the signal is constructed into a complex vector $\hat{x}$ with length $N/2$, N, which is even:

$$\hat{x} = \left\{x_1 + \mathrm{i}x_{\frac{N}{2}+1},\ x_2 + \mathrm{i}x_{\frac{N}{2}+2}, \ldots,\ x_{\frac{N}{2}} + \mathrm{i}x_N\right\}^T \tag{4.8}$$

where i is the imaginary unit. Then, the following calculation is performed:

$$\hat{Y} = \begin{bmatrix} \mathrm{Re}(M_p) & -\mathrm{Im}(M_p) \\ \mathrm{Im}(M_p) & \mathrm{Re}(M_p) \end{bmatrix} \hat{x} = B_p \hat{x} \tag{4.9}$$

where $\mathrm{Re}(\cdot)$ and $\mathrm{Im}(\cdot)$ represent the real part and the imaginary part, respectively, M_p is the complex-valued discrete-fractional Mellin transform matrix with order p, size $(N/2) \times (N/2)$ [29]. The reality-preserving result of FrMT can be obtained:

$$Y = (\mathrm{Re}(\hat{Y}), \mathrm{Im}(\hat{Y}))^T \tag{4.10}$$

This paper proposes a reality-preserving transform suitable for Gaussian apertured FrMT in the diffraction domain. The details of the reality-preserving transform are as follows:

(1) If A is a real square matrix with size $N \times N$, then a real square matrix A is used to construct a complex matrix B with size $N \times N/2$:

$$B(i,j) = A(i,j) + \mathrm{i}A(i, N/2 + j) \tag{4.11}$$

where $1 \le i \le N, 1 \le j \le N/2$.

(2) Then the $\hat{Y}$ can be obtained:

$$\begin{aligned}\hat{Y} &= \left[\mathrm{Re}\left(M_{Gp}\right) + \mathrm{iIm}\left(M_{Gp}\right)\right][\mathrm{Re}(B) + \mathrm{iIm}(B)] \\ &= \left[\mathrm{Re}\left(M_{Gp}\right)\mathrm{Re}(B) - \mathrm{Im}\left(M_{Gp}\right)\mathrm{Im}(B)\right] \\ &+ \mathrm{i}\left[\mathrm{Im}\left(M_{Gp}\right)\mathrm{Re}(\mathrm{B}) + \mathrm{Re}\left(M_{Gp}\right)\mathrm{Im}(B)\right] \\ &= \left[\mathrm{Re}\left(M_{Gp}(\mathrm{Re}(B))\right) - \mathrm{Im}\left(M_{Gp}(\mathrm{Im}(B))\right)\right] \\ &+ \mathrm{i}\left[\mathrm{Im}\left(M_{Gp}(\mathrm{Re}(B))\right) + \mathrm{Re}\left(M_{Gp}(\mathrm{Im}(B))\right)\right]\end{aligned} \tag{4.12}$$

where M_{Gp} is the Gaussian apertured fractional Mellin transform with order p in the diffraction domain with size $N \times N/2$.

(3) Finally, the reality-preserving result Y with size $N \times N$ is obtained:

$$Y = (\mathrm{Re}(\hat{Y}), \mathrm{Im}(\hat{Y}))^T \tag{4.13}$$

4.3.3 Proposed image encryption and decryption scheme

The schematic of the proposed image encryption and decryption algorithm is shown in Fig. 4.4, and the encryption process is described as follows:

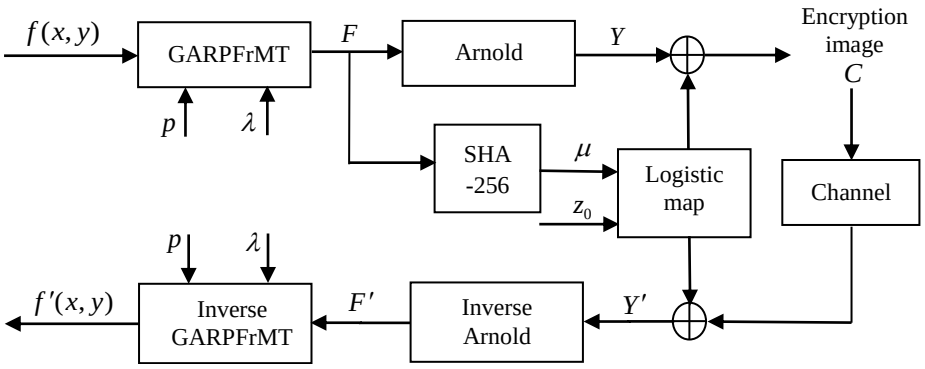


Fig. 4.4 Block diagram of the encryption and decryption process.

Step 1: Since the GARPFrMT is realized by the log-polar and the Gaussian apertured reality-preserving fractional Fourier transforms, the original image $f(x, y)$ is first log-polar transformed into $f(\rho, \theta)$ of size $n_r \times n_w$ from Cartesian coordinates (x, y) to polar coordinates (ρ, θ), as described in detail in [26].

Step 2: Then, $f(\rho, \theta)$ is regarded as the input of the reality-preserving Gaussian apertured FrFT with order p and parameter σ. Finally, the output $F(u, v)$ of the GARPFrMT can be obtained. The order p and incidence wavelength λ are regarded as cipher keys.

Step 3: The output $F(u, v)$ of the GARPFrMT is further permuted by the Arnold transform to generate a new encryption image named by $Y(u, v)$.

Step 4: Logistic map with initial values μ and parameter z_0 is iterated to obtain a

random sequence $z' = [z'_1, z'_2, \ldots, z'_P]$, where $P = n_r \times n_w$. The sequence z' is used to perform the bitwise XOR operation to diffuse the encrypted image $Y(u,v)$ and finally obtain the cipher-text C. The cipher key μ used in the logistic map is generated using the SHA-256 algorithm [142, 143], which is related to the output $F(u,v)$ of the GARPFrMT. The values μ and z_0 are used as cipher keys.

4.3.4 Decryption process

The decryption process is the inverse of the encryption shown in Fig. 4.4. First, the inverse bitwise XOR operation with cipher keys μ and z_0 is utilized to decrypt the cipher-text C. Secondly, the inverse Arnold transform is employed to recover the image $F'(u,v)$. Finally, the decrypted image $f'(x,y)$ can be recovered by performing an inverse GARPFrMT.

4.4 Simulation results and security analyses

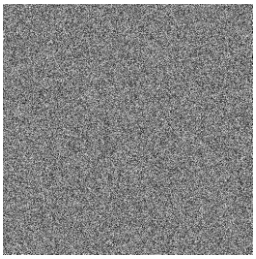
4.4.1 Parameters setup

The grayscale images of Elaine, Peppers and Cameraman with size 255×255, as shown in Fig. 4.5, were selected as test plain images. The geometric center of the original image (c_x, c_x) is set as $(128,128)$, the outer radii of the annular domain is $r_{\max} = 181$. The rings and wedges were chosen as $n_r = 500, n_w = 500$. The GARPFrMT-related parameters are set as: $\lambda = 632.8$ nm, $f_s = 4$ mm, and the order p is set to 0.5. The initial value of the logistic map z_0 is equal to 0.32, and the parameter μ is obtained using the SHA-256 algorithm.

4.4.2 Encryption results and decryption images

The simulation-encrypted results corresponding to the three different original images are shown in Fig. 4.5 (a2), (b2), (c2), (d2), (e2) and (f2) respectively, from which it can be seen that the cipher images are visually unrecognizable. There are three groups of correctly decrypted images (a3) - (a8), (b3) - (b8), (c3) - (c8), (d3)-(d8), (e3)-(e8) and (f3)-(f8) with each group containing six decryption images corresponding to six different values σ, $\sigma = 1000,\ 500,\ 200,\ 100,\ 50,\ 10$. As shown in Fig. 4.5, the decrypted images become blurred around the edges of the images as the value σ gradually decreases.


(a1) Original image


(a2) Encrypted image

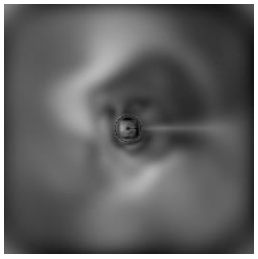

(a3) $\sigma = 1000$


(a4) $\sigma = 500$

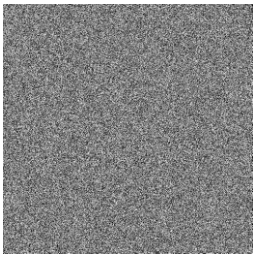

(a5) $\sigma = 200$


(a6) $\sigma = 100$


(a7) $\sigma = 50$


(a8) $\sigma = 10$


(b1)Original image


(b2) Encrypted image


(b3) $\sigma = 1000$


(b4) $\sigma = 500$

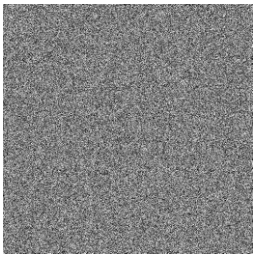

(b5) $\sigma = 200$


(b6) $\sigma = 100$


(b7) $\sigma = 50$


(b8) $\sigma = 10$

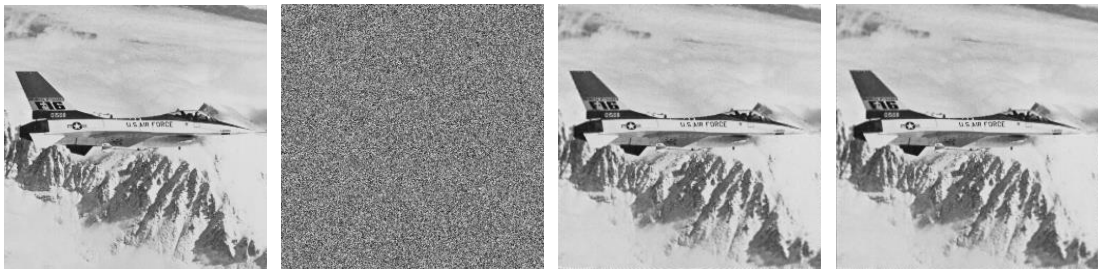

(c1) Original image


(c2) Encrypted image

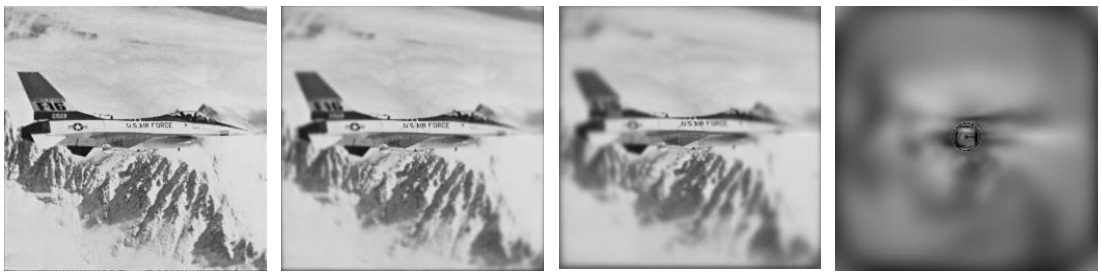

(c3) $\sigma = 1000$


(c4) $\sigma = 500$

(c5) $\sigma = 200$ (c6) $\sigma = 100$ (c7) $\sigma = 50$ (c8) $\sigma = 10$



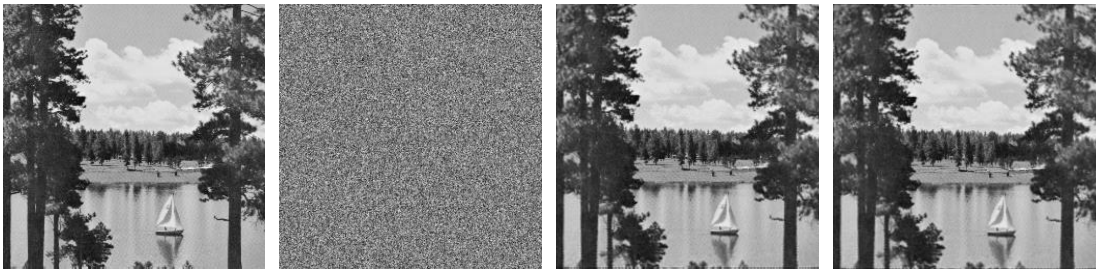
(d1) Original image (d2) Encrypted image (d3) $\sigma = 1000$ (d4) $\sigma = 500$



(d5) $\sigma = 200$ (d6) $\sigma = 100$ (d7) $\sigma = 50$ (d8) $\sigma = 10$

(e1) Original image (e2) Encrypted image (e3) $\sigma = 1000$ (e4) $\sigma = 500$

(e5) $\sigma = 200$ (e6) $\sigma = 100$ (e7) $\sigma = 50$ (e8) $\sigma = 10$



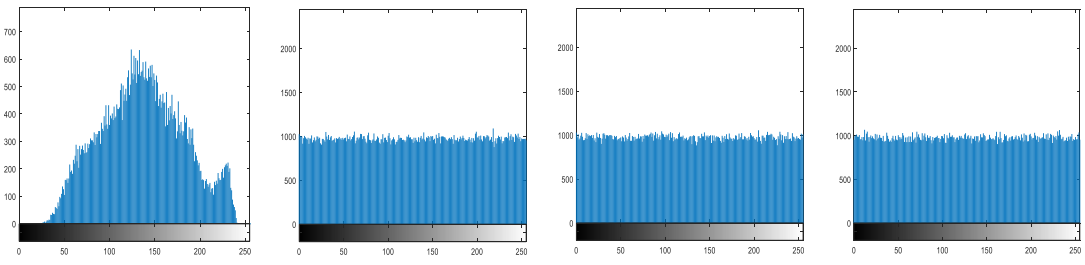
(f1) Original image (f2) Encrypted image (f3) $\sigma = 1000$ (f4) $\sigma = 500$

(f5) $\sigma = 200$ (f6) $\sigma = 100$ (f7) $\sigma = 50$ (f8) $\sigma = 10$

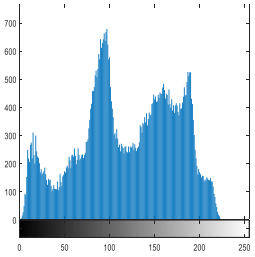
Fig. 4.5 Encrypted and decrypted results for different values σ: $\sigma = 1000, 500, 200, 100, 50, 10$; (a1), (b1), and (c1) are the original images: Elaine, Peppers, and Cameraman, Airplane, Lane and Lake respectively. (a2), (b2), and (c2) are the encrypted images. (a3) - (a8) are decrypted Elaine, (b3) - (b8) are decrypted Peppers, (c3) - (c8) are decrypted Cameraman, (d3) - (d8) are decrypted Airplane, (e3) - (e8) are decrypted Lane and (f3) - (f8) are decrypted Lake.

4.4.3 Histogram analysis

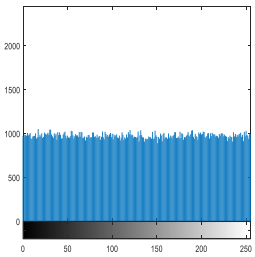
The histogram describes the number of pixels in the image with different gray levels and their frequency of occurrence. The histograms of cipher images should obey a fairly uniform distribution. Fig. 4.6 (a1), (b1), (c1), (d1), (e1) and (f1) show the histograms of plain images. Fig. 4.6 (a2) - (a3), (b2) - (b3), (c2) - (c3), (d2) - (d3), (e2) - (e3) and (f2) - (f3) show the histograms of cipher images for the different values σ, such as 1000, 500, 100. Obviously, the histograms of cipher images are nearly identical and almost uniformly distributed. Thus, there are reasons to believe that histograms of cipher images are no longer useful for attackers.



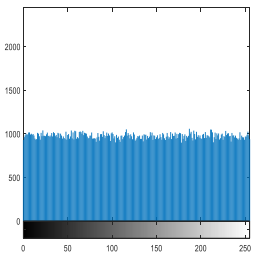
(a1) Elaine (a2) $\sigma = 1000$ (a3) $\sigma = 500$ (a4) $\sigma = 100$



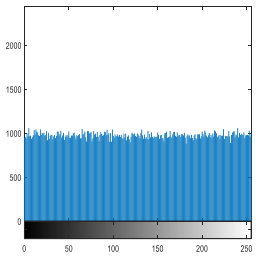
(b1) Pepper



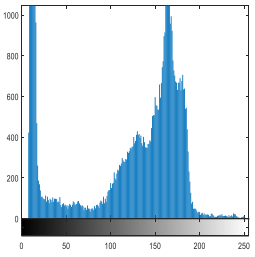
(b2) $\sigma = 1000$



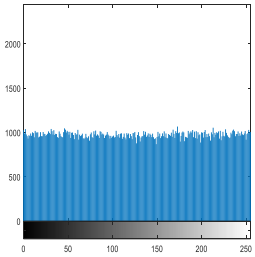
(b3) $\sigma = 500$



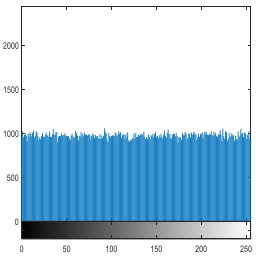
(b4) $\sigma = 100$



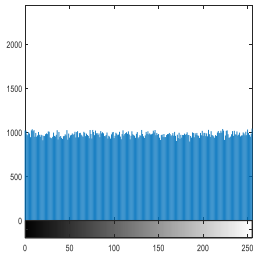
(c1) Cameraman



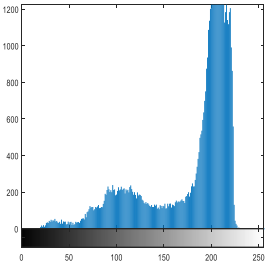
(c2) $\sigma = 1000$



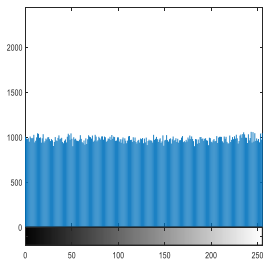
(c3) $\sigma = 500$



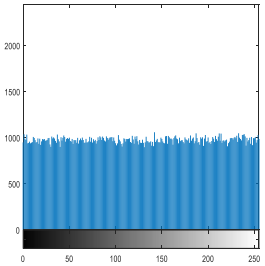
(c4) $\sigma = 100$



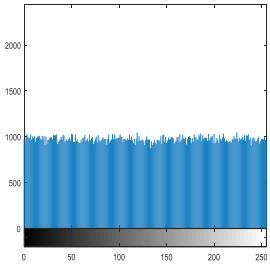
(d1) Airplane



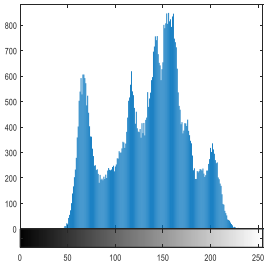
(d2) $\sigma = 1000$



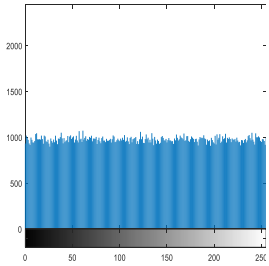
(d3) $\sigma = 500$



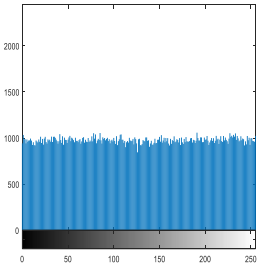
(d4) $\sigma = 100$



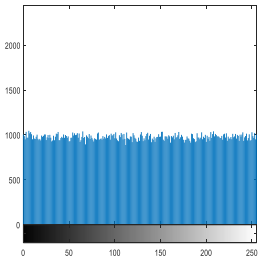
(e1) Lane



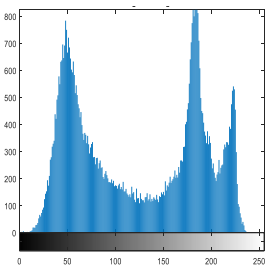
(e2) $\sigma = 1000$

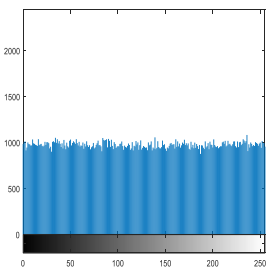


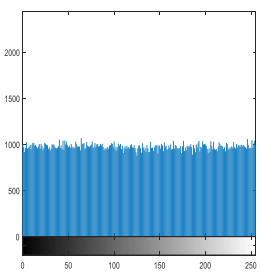
(e3) $\sigma = 500$

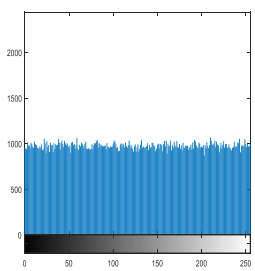


(e4) $\sigma = 100$









(f1) Lake (f2) $\sigma = 1000$ (f3) $\sigma = 500$ (f4) $\sigma = 100$

Fig. 4.6. Histograms of original images (a1) Elaine, (b1) Peppers, (c1) Cameraman, (d1) Airplane, (e1) Lena, (f1) Lake and histograms of encrypted images for different values σ. (a2), (b2) , (c2), (e2) and (f2) for value $\sigma = 1000$; (a3), (b3) (c3), (d3), (e3) and (f3) for value $\sigma = 500$; (a4), (b4) (c4), (d4), (e4) and (f4)for value $\sigma = 100$.

4.4.4 Correlation of adjacent pixels

As shown in Table 1 and Fig. 4.7, there exist strong neighborhood correlations between adjacent pixels for the original images. However, to be secured and efficient, those neighborhood correlations should not exist for encrypted images. Therefore, it is necessary to perform a correlation analysis on adjacent image pixels in cipher and plain images.

Table 4.1 and Fig. 4.7 show that the adjacent pixels of the original images have a strong correlation, whereas those in the ciphered images for different values σ are very weak. Therefore, the proposed image encryption algorithm based on GARPFrMT is secured against correlation analysis attack.

Table 4.1 Correlation between two adjacent pixels

Image	σ	**Horizontal direction**	**Vertical direction**	**Diagonal direction**
Plain Elaine		0.9589	0.9526	0.9276
	1000	–0.0085	0.0055	0.0071
	500	0.0013	0.0117	0.0098
Encrypted Elaine	200	0.0071	–0.0080	0.0066
	100	0.0012	0.0156	0.0015
	50	–0.0051	–0.0004	0.0028
Plain Peppers		0.9600	0.9394	0.9083
	1000	–0.0060	–0.0065	0.0046
	500	0.0071	0.0087	0.0092
Encrypted Peppers	200	–0.0027	–0.0028	–0.0115
	100	–0.0034	–0.0007	0.0088
	50	0.00003	–0.0038	0.0035
Plain Airplane		0.9136	0.9014	0.8464

Encrypted Airplane	1000	-0.0190	0.0157	8.8267e-04
	500	-0.0130	0.0185	-0.0023
	200	-0.0157	0.0048	0.0058
	100	-0.0051	0.0102	-0.0087
	50	-0.0032	0.0091	-0.0035
Plain Lena		0.9548	0.9196	0.8975
Encrypted Lena	1000	-0.0017	0.0026	0.0090
	500	-0.0055	-0.0018	0.0011
	200	-0.0163	0.0066	0.0025
	100	-0.0054	-0.0018	0.0046
	50	-0.0121	-0.0048	-0.0081
Plain Lake		0.9383	0.9457	0.9047
Encrypted Lake	1000	0.0148	-0.0077	0.0049
	500	-0.0091	-0.0119	0.0077
	200	0.0087	0.0097	-0.0121
	100	5.9092e-04	0.0207	-0.0033
	50	1.9748e-04	0.0049	0.0077

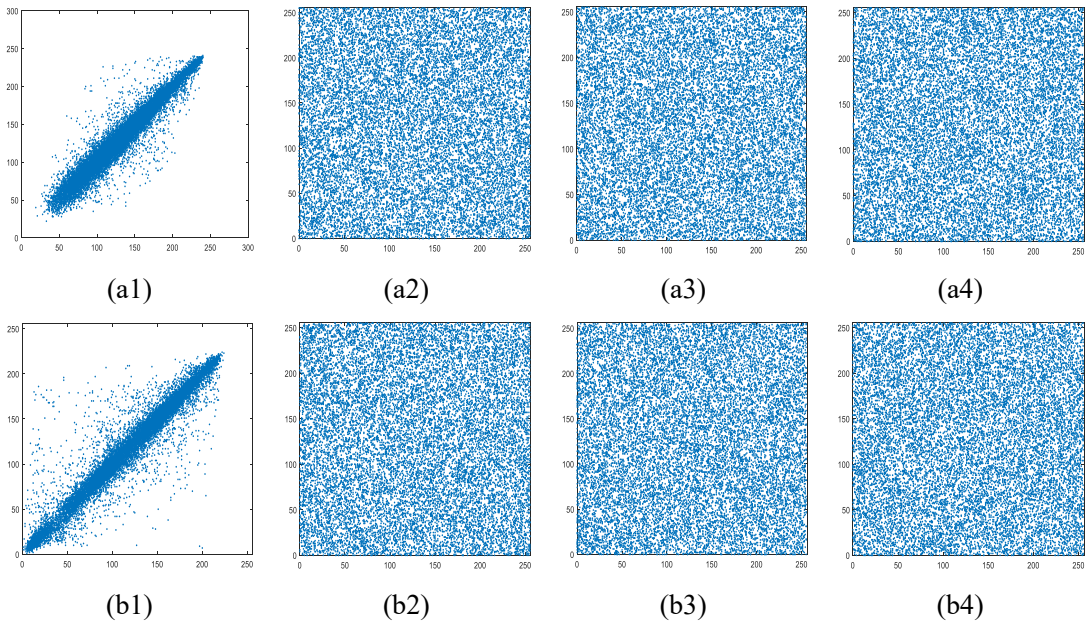
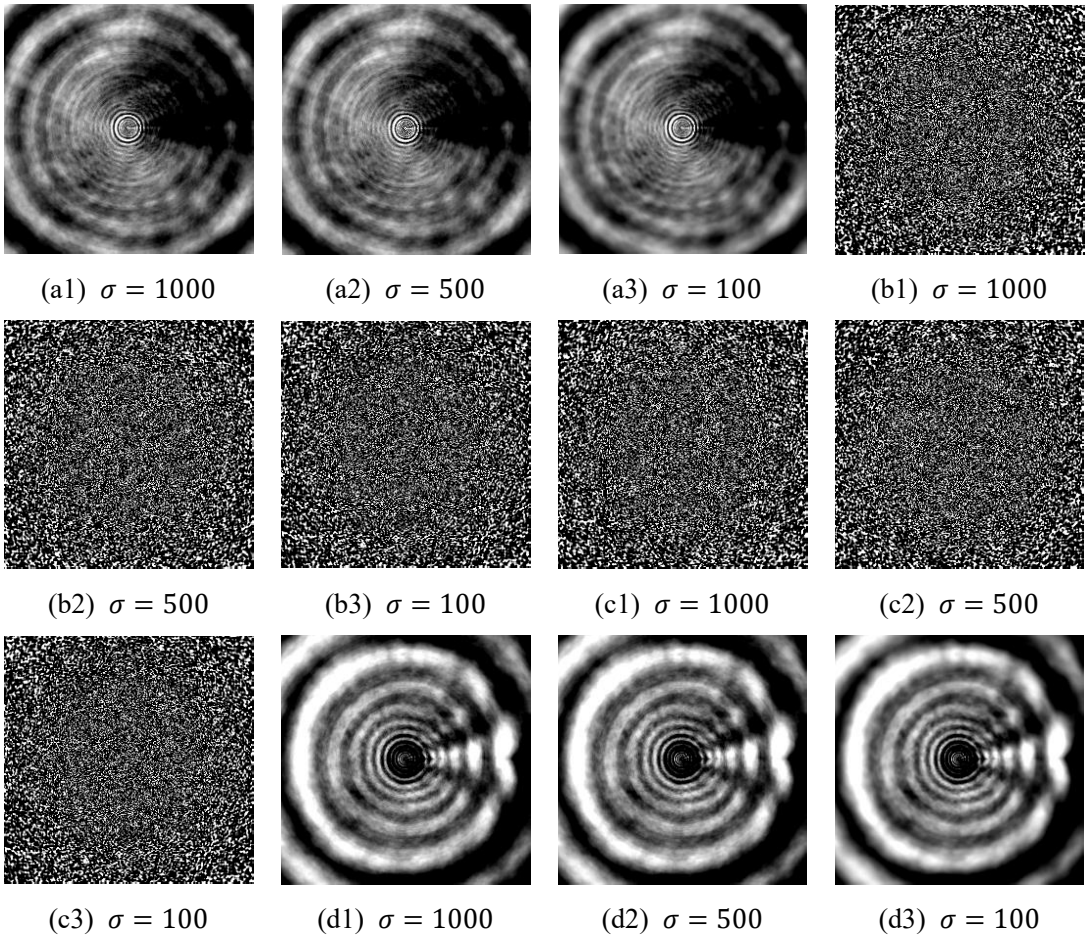


Fig. 4.7 Graphical representation of correlations in horizontally adjacent pixels in (a1) Elaine, (a2),

(a3) and (a4) encrypted Elaine with $\sigma = 1000,\ 500,\ 100$, respectively, (b1) Peppers, (b2), (b3) and (b4) encrypted Peppers with $\sigma = 1000,\ 500,\ 100$, respectively.

4.4.5 Key-sensitivity and key space analyses

In the experiments, three different control parameters $\sigma = 1000, 500, 100$ of Gaussian aperture were used to analyze the cipher key sensitivity. Fig. 4.8 shows the decrypted results of Elaine with incorrect keys. Fig. 4.8(a1) - (a3) illustrates the decrypted images with an incorrect GAPRFrMT order p=0.6. Fig. 4.8(b1) - (b3) presents the decrypted images with a wrong initial value for logistic map $\mathrm{z}'\colon z' = z_0 + 10^{-15}$. The decrypted results with a wrong parameter for logistic map $\mu'\colon \mu' = \mu + 10^{-15}$. are given in Fig. 4.8(c1) - (c3). The incorrect incidence wavelength $\lambda'\colon \lambda' = \lambda_0 + 10^{-7}$ is used for the decryption process, the decrypted images are shown in Fig. 4.8(d1) - (d3).



(a1) $\sigma = 1000$ (a2) $\sigma = 500$ (a3) $\sigma = 100$ (b1) $\sigma = 1000$

(b2) $\sigma = 500$ (b3) $\sigma = 100$ (c1) $\sigma = 1000$ (c2) $\sigma = 500$

(c3) $\sigma = 100$ (d1) $\sigma = 1000$ (d2) $\sigma = 500$ (d3) $\sigma = 100$

Fig. 4.8. Decrypted Elaine using incorrect cipher keys with different values σ: $\sigma = 1000$, 500, 100. (a1) -(a5) incorrect GARPFrMT order of 0.6, (b1) - (b3) wrong initial value for logistic map $z'\colon z' = z_0 + 10^{-15}$, (c1) - (c3) wrong parameter for logistic map parameter $\mu'\colon \mu' = \mu_0 + 10^{-15}$,

(d1) - (d3) wrong incidence wavelength λ': $\lambda' = \lambda_0 + 10^{-7}$.

To measure the similarity between the original image and the decrypted image, the mean square error (MSE) and logarithm of mean square error (LMSE) are introduced to evaluate the quality of the decrypted images.

Alvarez and Li [110] indicated that the encryption scheme is secure when its cipher key space is at least up to 2^{100}. As can be seen from Fig. 4.8 and Fig. 4.9, the double-precision of the parameters z_0, μ_0 of the logistic map is approximately 10^{-15}, then the value of those cipher key spaces is 10^{30}. The cipher key space for the incidence wavelength λ is 10^7. Since the incorrect wavelength only effects on GARPFrMT, the curve of LMSE don't make a large difference for different parameters σ in Fig. 4.9(d). The period of the Arnold transform is 751 when the output size of GARPFrMT is 500×500. Therefore, the total key space is at least 10^{39}, which is greater than 2^{100}. This means that the key space is large enough to resist brute-force attacks.

In addition to a sufficiently large key space, the order p of GARPFrMT further expands the cipher key space.

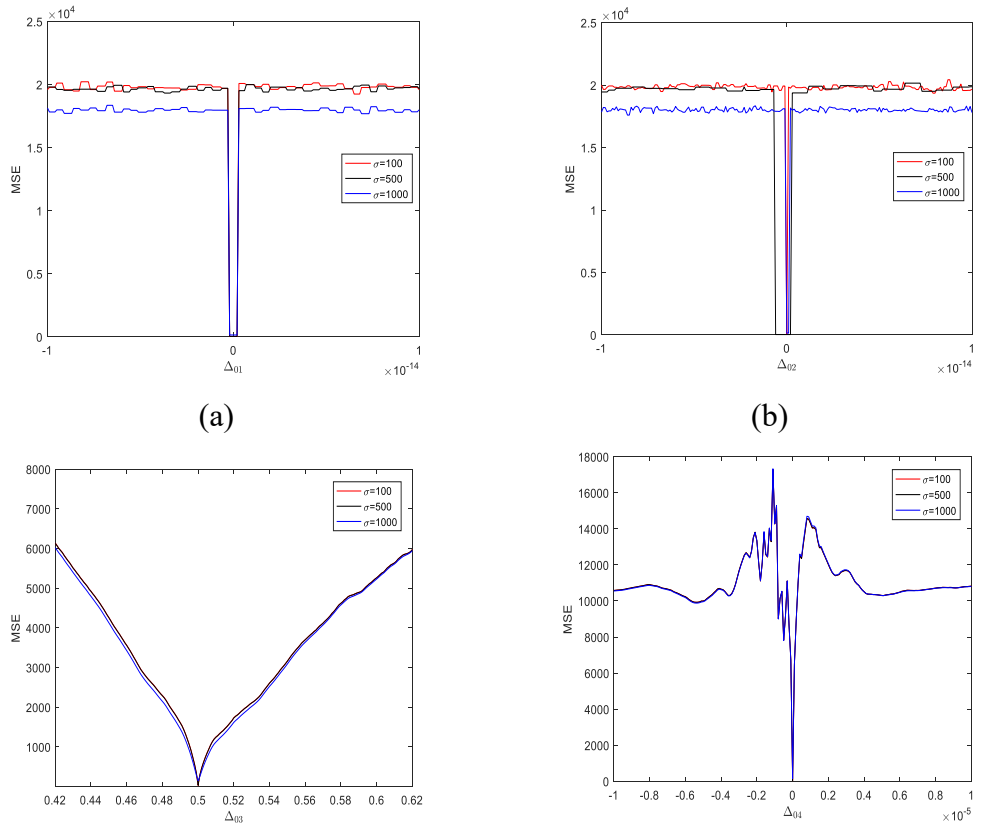


Fig. 4.9 MSE curves for (a) parameter $\mu + \Delta_{01}$, (b) initial value $z_0 + \Delta_{02}$, (c) GARPFrMT order $p + \Delta_{03}$, (d) incidence wavelength $\lambda + \Delta_{04}$.

4.4.6 Information entropy analysis

Information entropy is used to describe the randomness of image textures. The results shown in Table 4.2 indicate that the entropies of the encrypted images for different values σ are very close to 8. Therefore, the proposed scheme has the ability to resist information entropy attacks.

Table 4.2 Comparison of entropies of original and encrypted images for different values σ

Images	Original	Encryption image				
		$\sigma = 1000$	$\sigma = 500$	$\sigma = 200$	$\sigma = 100$	$\sigma = 50$
Elaine	7.5036	7.9993	7.9993	7.9992	7.9993	7.9993
Cameraman	7.0030	7.9992	7.9992	7.9993	7.9994	7.9993
Peppers	7.3656	7.9992	7.9993	7.9992	7.9994	7.9992
Airplane	6.7092	7.9993	7.9993	7.9993	7.9993	7.9992
Lena	7.2157	7.9993	7.9993	7.9992	7.9993	7.9993
Lake	7.4893	7. 9992	7.9992	7.9992	7.9991	7.9993

4.4.7 Differential attacks

The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are two commonly used quantities to test the ability of an encryption algorithm to resist differential attacks.

The experimental NPCR and UACI are shown in Tables 4.3 and 4.4, respectively, from which it can be known that all the NPCRs and UACIs are very close to the expected values of 99.6054% and 33.4635%, respectively. The results indicate that the proposed scheme is sensitive to plain-text changes.

Table 4.3 NPCR (%) values of encrypted images for different values σ

Image	$\sigma = 1000$	$\sigma = 500$	$\sigma = 200$	$\sigma = 100$	$\sigma = 50$
Elaine	99.6136	99.6396	99.6056	99.6192	99.6156
Cameraman	99.5832	99.5832	99.5816	99.5956	99.6112
Peppers	99.5952	99.6176	99.5912	99.6168	99.6272
Airplane	99.6068	99.6212	99.5984	99.6152	99.6104
Lena	99.6168	99.6076	99.6160	99.6088	99.5916
Lake	99.6000	99.6044	99.6244	99.6392	99.6232

Table 4.4 UACI (%) values of encrypted images for different values σ

Image	$\sigma = 1000$	$\sigma = 500$	$\sigma = 200$	$\sigma = 100$	$\sigma = 50$

Elaine	33.5040	33.5050	33.5107	33.4867	33.5570
Cameraman	33.5654	33.5294	33.4850	33.5044	33.4988
Peppers	33.4638	33.4272	33.5354	33.5366	33.5836
Airplane	33.4271	33.5150	33.4777	33.4889	33.5577
Lena	33.5383	33.5471	33.5458	33.5046	33.5323
Lake	33.4234	33.5421	33.4904	33.5697	33.4240

4.4.8 Robustness analysis

Since the cipher images are easily affected by noise and data loss during transmission and processing, it is necessary to measure the robustness of the proposed image encryption algorithm, noting that noise attack and occlusion attack are two effective assessment methods. Salt and pepper noise with different intensities is used to alter the decrypted images generated at different values of σ. Fig. 4.10 shows the deviation of MSE versus noise intensity k. Fig. 4.11 shows the decrypted images of Cameraman when k is equal to 0.01, 0.5, 0.1, respectively. It can be seen that the major information of the original image is still visually perceptible even with a certain amount of noise added to the encrypted images.

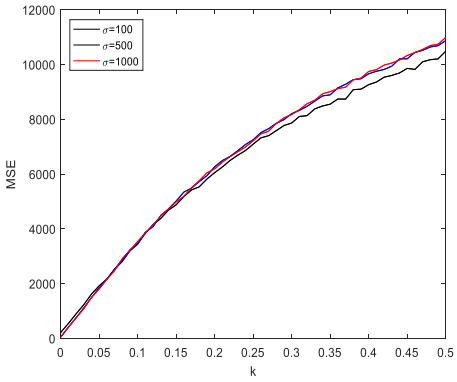


Fig. 4.10 Results of noise attack: The MSE curve for GARPFrMT with different values σ

(a1) $\sigma = 1000, k = 0.01$

(a2) $\sigma = 1000, k = 0.05$

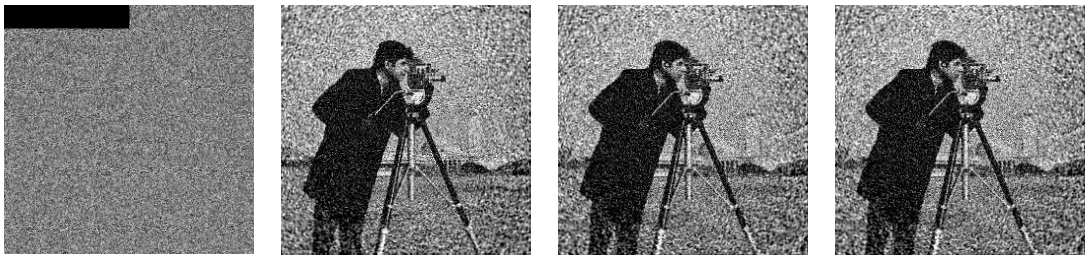
(a3) $\sigma = 1000, k = 0.1$

(b1) $\sigma = 500, k = 0.01$ (b2) $\sigma = 500, k = 0.05$ (b3) $\sigma = 500, k = 0.1$

(c1) $\sigma = 100, k = 0.01$ (c2) $\sigma = 100, k = 0.05$ (c3) $\sigma = 100, k = 0.1$

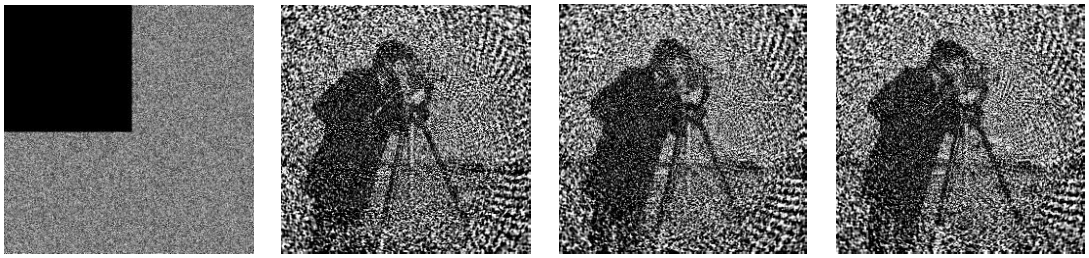
Fig. 4.11 Decrypted Cameraman with various intensities of salt and pepper noises. At the different values σ, decrypted images for (a1), (b1) and (c1) with $k = 0.01$, decrypted images for (a2), (b2) and (c2) with $k = 0.05$, decrypted images for (a3), (b3) and (c3) with $k = 0.1$.

The robustness on resisting occlusion attack was analyzed with an occlusion ratio of 1/16, 1/8, 1/4, as shown in Fig. 4.12(a1), (b1), and (c1), respectively. The corresponding decrypted results at different values σ are presented in Fig. 4.12(a2) - (a4), (b2) - (b4) and (c2) - (c4), respectively. As shown in Fig. 4.12, it is observed that the decrypted images remain visible, although the degree of data loss is different. It can be seen that the proposed scheme has a certain degree of robustness against noise and occlusion attacks.



(a1) (a2) $\sigma = 1000$ (a3) $\sigma = 500$ (a4) $\sigma = 100$

(b1) (b2) $\sigma = 1000$ (b3) $\sigma = 500$ (b4) $\sigma = 100$



(c1) (c2) $\sigma = 1000$ (c3) $\sigma = 500$ (c4) $\sigma = 100$

Fig. 4.12 Decrypted Cameraman with various occlusion ratios. Encrypted images with (a1) 1/16, (b1) 1/8, and (c1) 1/4 occlusion. At the different values σ, decrypted images for (a2), (a3), and (a4) with 1/16 occlusion, decrypted images for (b2), (b3), and (b4) with 1/8 occlusion, and decrypted images for (c2), (c3), and (c4) with 1/16 occlusion.

4.5 Color image encryption algorithm based on reality-preserving Gaussian FrMT

4.5.1 Color space rotation

Human visual perception can be described through color categories, with names such as white, black, red, green, yellow, blue, brown, purple, pink, orange and gray. Color images are easily recognizable, extractable from a scene and capable of carrying more image information such as color shades and intensities, compared with grayscale images. RGB (red, green, blue) color model is a color specification with name three primary colors, which is utilized to create most any color in the visible spectrum by combining in proportion.

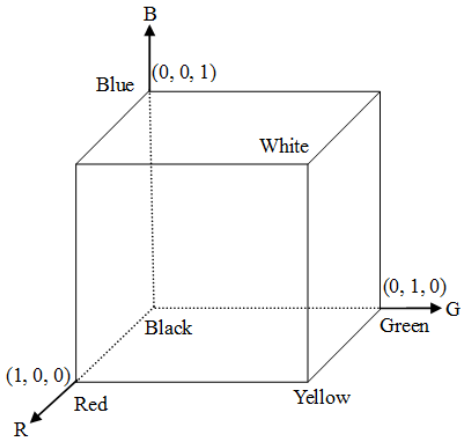


Fig. 4.13 Schematic of the RGB color cube [144].

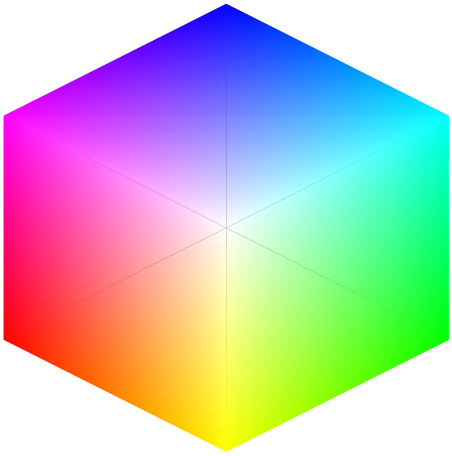


Fig. 4.14 RGB color cube

The RGB model is based on a Cartesian coordinate system as shown in Fig. 4.13 and Fig. 4.14. The three primary colors normalized in the RGB cube are at three corners, respectively, and different colors determined by vectors starting from the origin are points on or inside the cube [144]. To hide the color information that is very important for color images, the color information of an original image is scrambled by rotating the RGB color space with different rotation angles about the *x, y* and *z* axes to a new color space with name R′G′B′ color space. The transition relations around the *x, y* and *z* axes between RGB color space and R′G′B′ color space are shown as follows:

$$R_x(\alpha) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{bmatrix} \tag{4.14}$$

$$R_y(\beta) = \begin{bmatrix} \cos\beta & 0 & \sin\beta \\ 0 & 1 & 0 \\ -\sin\beta & 0 & \cos\beta \end{bmatrix} \tag{4.15}$$

$$R_z(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{4.16}$$

where α, β, θ are the rotation angles around the x, y and z axes, respectively. The new three color pixel $R'(x,y)$, $G'(x,y)$ and $B'(x,y)$ are obtained by the following transformation matrix $T(\alpha, \beta, \theta)$

$$\begin{bmatrix} R'(x,y) \\ G'(x,y) \\ B'(x,y) \end{bmatrix} = R_x(\alpha) \cdot R_y(\beta) \cdot R_z(\theta) \begin{bmatrix} R(x,y) \\ G(x,y) \\ B(x,y) \end{bmatrix} = T(\alpha, \beta, \theta) \begin{bmatrix} R(x,y) \\ G(x,y) \\ B(x,y) \end{bmatrix} \tag{4.17}$$

It is easy to prove that the matrix $T(\alpha,\beta,\theta)$ is reversible because $R(x,y)$, $G(x,y)$ and $B(x,y)$ are regarded as orthogonal. Thus, the color information of original image can be recovered by using the reversible matrix $T'(\alpha,\beta,\theta)$

$$\begin{bmatrix} R(x,y) \\ G(x,y) \\ B(x,y) \end{bmatrix} = T'(\alpha,\beta,\theta) \begin{bmatrix} R'(x,y) \\ G'(x,y) \\ B'(x,y) \end{bmatrix} \tag{4.18}$$

where $T^{-1}(\alpha,\beta,\theta) = R_z^{-1}(\theta) \cdot R_y^{-1}(\beta) \cdot R_x^{-1}(\alpha)$. As shown in Fig. 15, although the original image information can't be disturbed, there exists image distortion resulting from color space transform.

(a) (b)

Fig. 4.15 (a) The original image Lena, (b) The rotated image with rotation angles $\alpha = \pi/3,\ \beta = \pi/5,\ \theta = \pi/6$.

4.5.2 Color image encryption algorithm based on RPGAFrMT

The schematic of the color image encryption and decryption scheme is shown in Fig. 4.16. The encryption process includes color space rotation, reality-preserving Gauassian apertured FrMT, 3D scrambling, and operation of Xor. The encryption and decryption process are described below:

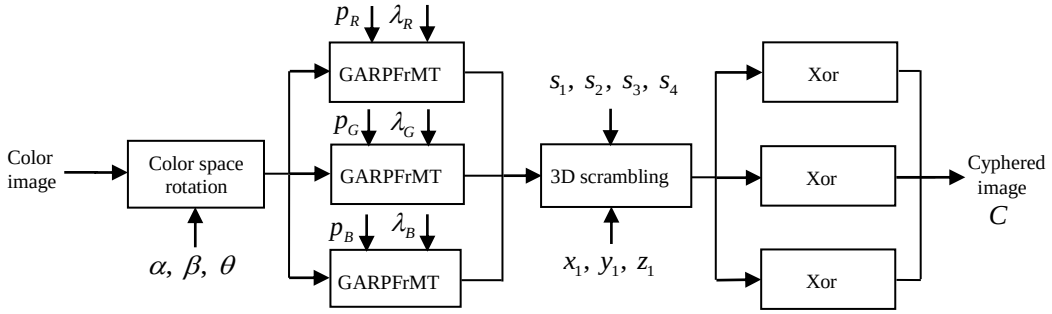


Fig. 4.16 The schematic of the color image encryption algorithm.

Step 1: The original color image of size $M \times N \times 3$ is transformed from RGB color space to a new $\mathrm{R'G'B'}$ space with transformation matrix $T(\alpha, \beta, \theta)$, and three new color components $R'(x,y)$, $G'(x,y)$ and $B'(x,y)$ are obtained. The rotation angles α, β, θ serve as keys.

Step 2: The new color components $R'(x,y)$, $G'(x,y)$ and $B'(x,y)$ are used as inputs of three GARPFrMTs with orders $p_i, (\, i = R, G, B)$, respectively, and transformed to $R'(u,v)$, $G'(u,v)$ and $B'(u,v)$ in the GARPFrMT domain. The fractional orders $p_i, (\, i = R, G, B)$ and the incidence wavelengths $\lambda_i, (\, i = R, G, B)$ corresponding to three different GARPFrMTs, respectively, are used as cipher keys.

Step 3: The security of the proposed algorithm is improved by introducing scrambling operation for $R'(u,v)$, $G'(u,v)$ and $B'(u,v)$. First, three components are scrambled, respectively. Then the scrambled components are combined to form a new 2D matrix E, which is scrambled again to mix the three components. The scrambling process is described in detail as follows:

(a) The 3D-logistic map with three initial values x_1, y_1, z_1 and the seeds s_1, s_2, s_3 is iterated to obtain three $P \times 1$ random sequences $x = [x_1, x_2, \dots, x_P\,]^T$, $y = [y_1, y_2, \dots, y_P\,]^T$, $z = [z_1, z_2, \dots, z_P\,]^T$, where $P = M_1 \times N_1$, $M_1 \times N_1$ is the size of $R'(u,v)$. Sort the sequences x, y and z to obtain index sequences a_x, a_y and a_z. The components of $R'(u,v)$, $G'(u,v)$ and $B'(u,v)$ can be expressed as 2D matrices $\mathrm{R'}$, $\mathrm{G'}$ and $\mathrm{B'}$, and the three matrices are reshaped to the sequences r', g', and b' with length $P \times 1$. Map the pixel with index $a_x(i)$, $a_y(i)$ and $a_z(i)$ in the sequences r', g', and b' to the position with index i in the sequences r'', g'', and b'', respectively. The seeds s_1, s_2, s_3 serve as cipher keys.

(b) The sequences r'', g'', and b'' are respectively reshaped to three 2D matrices $\mathrm{R''}$, $\mathrm{G''}$ and $\mathrm{B''}$, and the three 2D matrices are combined to a matrix E with size $N_1 \times 3M_1$, where $\mathrm{E} = [\mathrm{R''}, \mathrm{G''}, \mathrm{B''}]$. The logistic-sine map with an initial value x_2 and seed s_4 is used to generate sequences q_0 with length N_1 and N_1 sequence q_l of length $3M_1$ $(1 \le l \le N_1)$, which are sorted to obtained index sequences a_0 and a_l, respectively. The pixel with coordinate $\left(a_0(i), a_y(j)\right)$ in matrix E is mapped to the position with coordinate (i,j) in the matrix $\mathrm{E'}$ of size $N_1 \times 3M_1$. The seed s_4 generated with SHA-256 algorithm serve key. The SHA-256 algorithm is related to the mean value of the components

$R'(u,v)$, $G'(u,v)$ and $B'(u,v)$.

Step 4: The matrix E' is divided into three components with the same size $M_1 \times N_1$: E'_R, E'_G and E'_B, and the three components are mapped into an integer range $[0, 255]$. The sequence q' of size $1 \times M_1 N_1$ is generated by the logistic-sine map with the initial value x_2 and seed s_4. The sequence q' is reshaped into three matrices with size $M_1 \times N_1$, denoted as D, and this matrix is mapped into integer range $[0, 255]$ as well. The components E'_{R}, E'_{G} and E'_{B} are diffused by the bitwise Xor operation with D, respectively, to generate cypher image C with three encrypted components R_0, G_0 and B_0.

The decryption process is shown in Fig. 4.17. The bitwise Xor operation and the inverse pixel 3D scrambling method with correct keys (s_1, s_2, s_3, s_4) are successively utilized to decrypt the image C. The inverse GARPFrMT with correct keys $(p_R, p_G, p_B, \lambda_R, \lambda_G, \lambda_B)$ is employed to recover the color components $\mathrm{R}'', \mathrm{G}''$, and B''. Finally, the inverse color space rotation with correct keys (α, β, θ) is adopted to obtain the decrypted image.

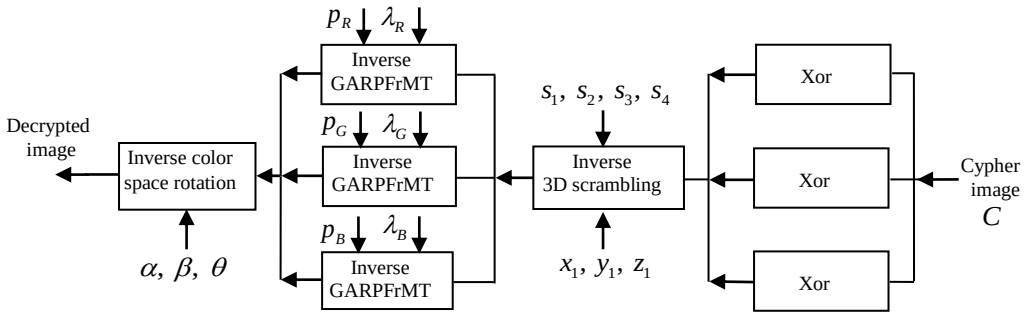


Fig. 4.17 The schematic of the color image decryption algorithm.

4.6 Experimental results and security analyses

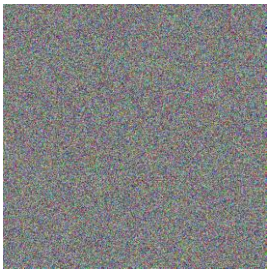
4.6.1 Parameters setup

The color image of Peppers with size $255 \times 255 \times 3$ was select as the plain image as shown in Fig. 4.18. The orders were set as $p_R = 0.5$, $p_G = 0.5$ and $p_B = 0.5$ respectively. The incidence wavelengths were chosen as $\lambda_R = 632.8$nm, $\lambda_G = 546.1$ nm, and $\lambda_B = 700$nm, respectively, and $f_s = 4$ mm. The color rotation angles were set as $\alpha = \pi/3$, $\beta = \pi/5$, and $\theta = \pi/6$. Several different parameters of Gaussian aperture were selected as test parameters $\sigma = 1000$, 500, 100, 50. The channel 1,

channel 2 and channel 3 were corresponding to red, green and blue components, respectively. The initial values and the seeds of the 3D logistic map were set as $x_1 = 0.2350$, $y_1 = 0.2350$, $z_1 = 0.7350$, $s_1 = 0.0125$, $s_2 = 0.0157$, $s_3 = 3.7700$, and the initial value and the seed logistic-sine map were set as $x_2 = 0.3200$, $s_4 = 3.9400 + x_{\text{hash}} \times 10^{-5}$, where x_{hash} is generated with SHA-256 algorithm related to the mean value of the components $R'(u,v)$, $G'(u,v)$ and $B'(u,v)$.

4.6.2 Encrypted results and decrypted images

(a) Original image



(b) Encrypted image

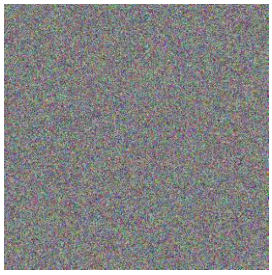
(c) $\sigma = 1000$

(d) $\sigma = 500$

(e) $\sigma = 100$

(f) $\sigma = 50$

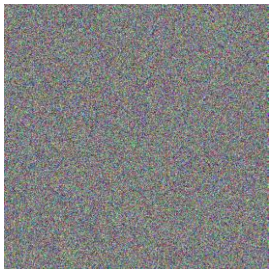
(a2) Original image



(b2) Encrypted image

(c2) $\sigma = 1000$

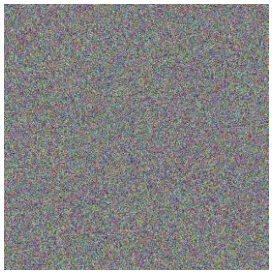
(d2) $\sigma = 500$ (e2) $\sigma = 100$ (f2) $\sigma = 50$

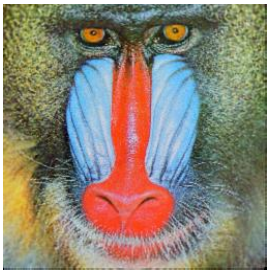

(a3) Original image (b3) Encrypted image (c3) $\sigma = 1000$



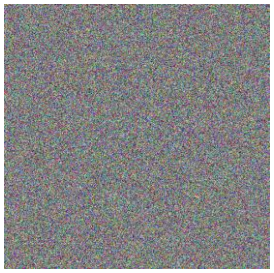
(d3) $\sigma = 500$ (e3) $\sigma = 100$ (f3) $\sigma = 50$


(a4) Original image (b4) Encrypted image (c4) $\sigma = 1000$



(d4) $\sigma = 500$ (e4) $\sigma = 100$ (f4) $\sigma = 50$

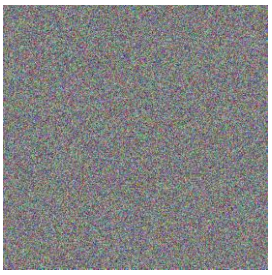

(a5) Original image (b5) Encrypted image (c5) $\sigma = 1000$

(d5) $\sigma = 500$

(e5) $\sigma = 100$

(f5) $\sigma = 50$

(a6) Original image



(b6) Encrypted image

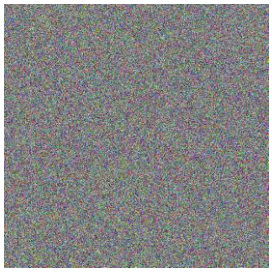
(c6) $\sigma = 1000$

(d6) $\sigma = 500$

(e6) $\sigma = 100$

(f6) $\sigma = 50$

(a7) Original image



(b7) Encrypted image

(c7) $\sigma = 1000$

(d7) $\sigma = 500$

(e7) $\sigma = 100$

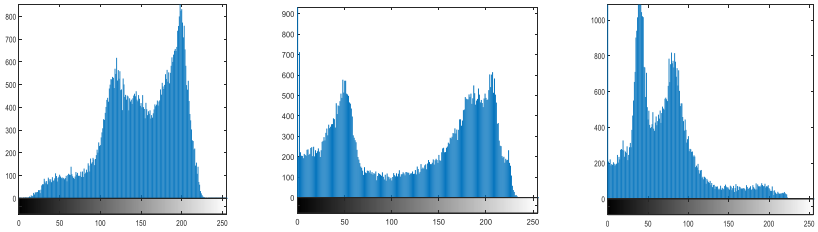
(f7) $\sigma = 50$

Fig. 4.18 Color image encryption and decryption results: (a1)-(a2) Original image Peppers, House, Cartoon, Baboon, Couple and Girl, (b)-(b7) encrypted image, (c)-(c7), (d)-(d7), (e)-(e7), (f)-(f7) decrypted images with correct keys for different values σ.

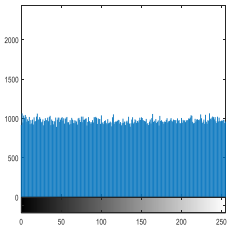
The original image of color Peppers, House, Cartoon, Baboon, Couple and Girl are shown in Fig. 4.18(a)-(a2), and Fig. 18(b)-(b7) show the corresponding encrypted image. Figs. 4.18(c)-(c7), (d)-(d7), (e)-(e7), (f)-(f7) show the decrypted color images with correct keys for four different values σ, $\sigma = 1000, 500, 100, 50$, respectively. It can be seen that there is no significant differences between original image and the decrypted image at the parameter $\sigma = 1000$. Although the decrypted images get blurred around the edges of the images as the parameter σ decreases gradually, the content of the decrypted images are still visually recognizable.

4.6.3 Histogram analysis

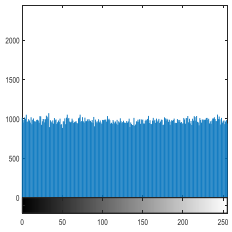
The color images Peppers, Lena, House, Cartoon, Baboon, Couple and Girl are used for performing the test on histogram analysis of the proposed encryption algorithm. Figs. 4.19 (a1), (a2), (a3), (a4), (a5), (a6) and (a7) R; (b1) (b2), (b3), (b4), (b5) and (b6) and (b7) G; (c1) (c2) , (c3), (c4), (c5), (c6) and (c7) B show that the histograms for three channels of the same plain image are entirely different, while the ciphertext's histograms of R, G, B components are similar and almost uniformly distributed, and the histograms of three components of different original images are nearly identical too, as shown in Figs. 4.19(d1), (d2), (d3), (d4), (d5), (d6) and (d7) R; (e1), (e2), (e3), (e4), (e5), (e6) and (e7) G; (f1), (f2), (f3), (f4), (f5), (f6) and (f7) B. Thus, it demonstrates that the histogram analysis cannot provide with valuable information about encryption systems for the attackers.



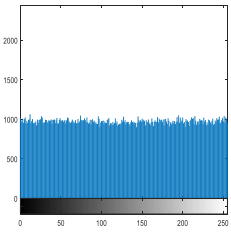
(a1) (b1) (c1)



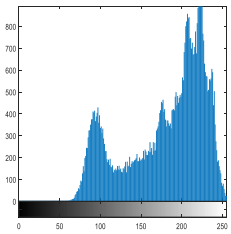
(d1)



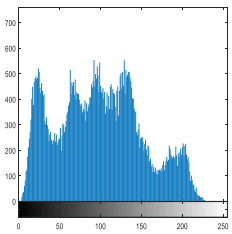
(e1)



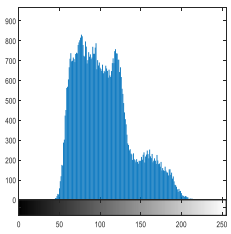
(f1)



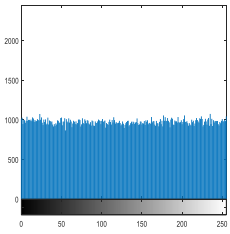
(a2)



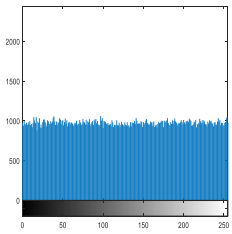
(b2)



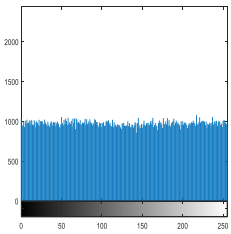
(c2)



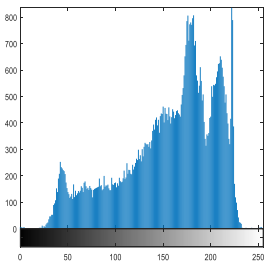
(d2)



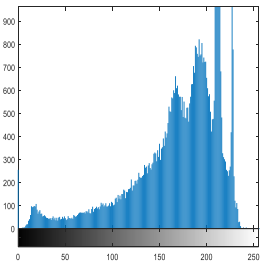
(e2)



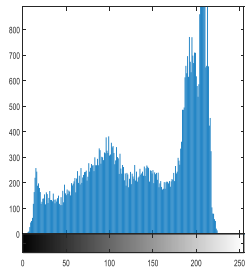
(f2)



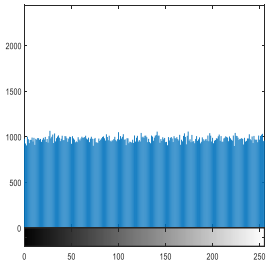
(a3)



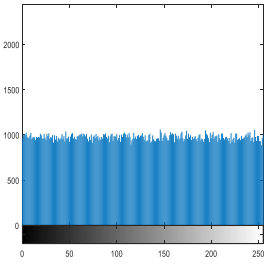
(b3)



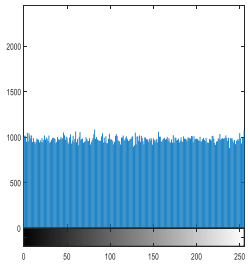
(c2)



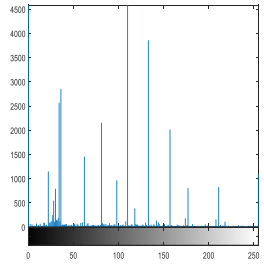
(d3)



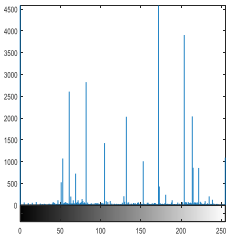
(e3)



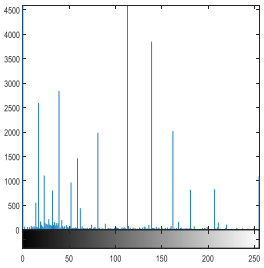
(f3)



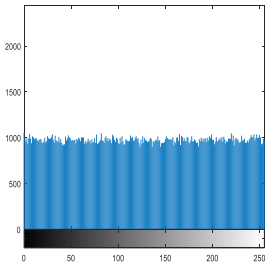
(a4)



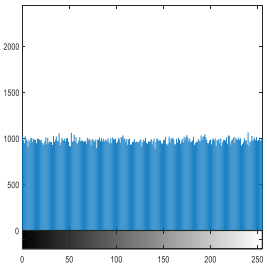
(b4)



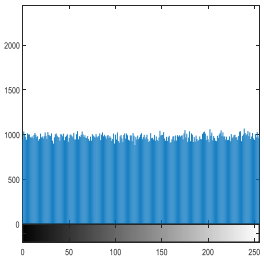
(c4)



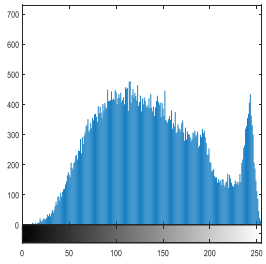
(d4)



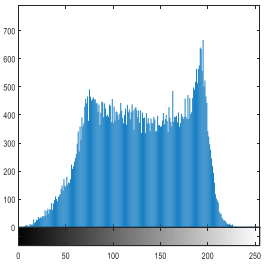
(e4)



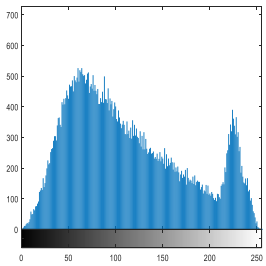
(f4)



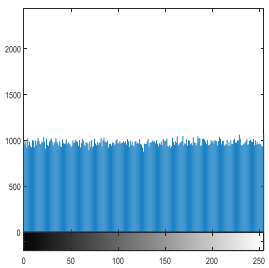
(a5)



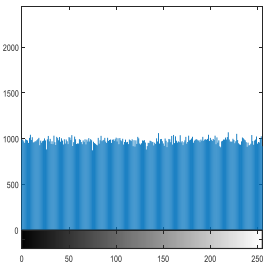
(b5)



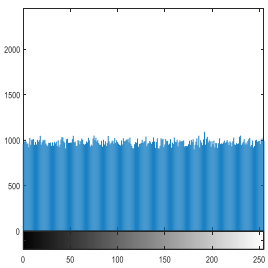
(c5)



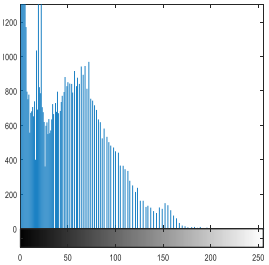
(d5)



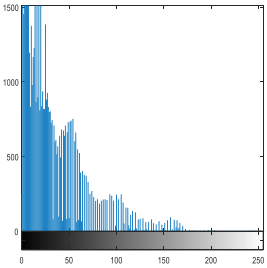
(e5)



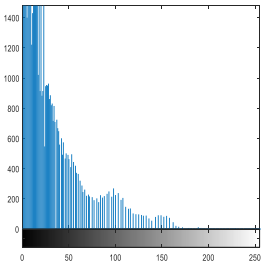
(f5)



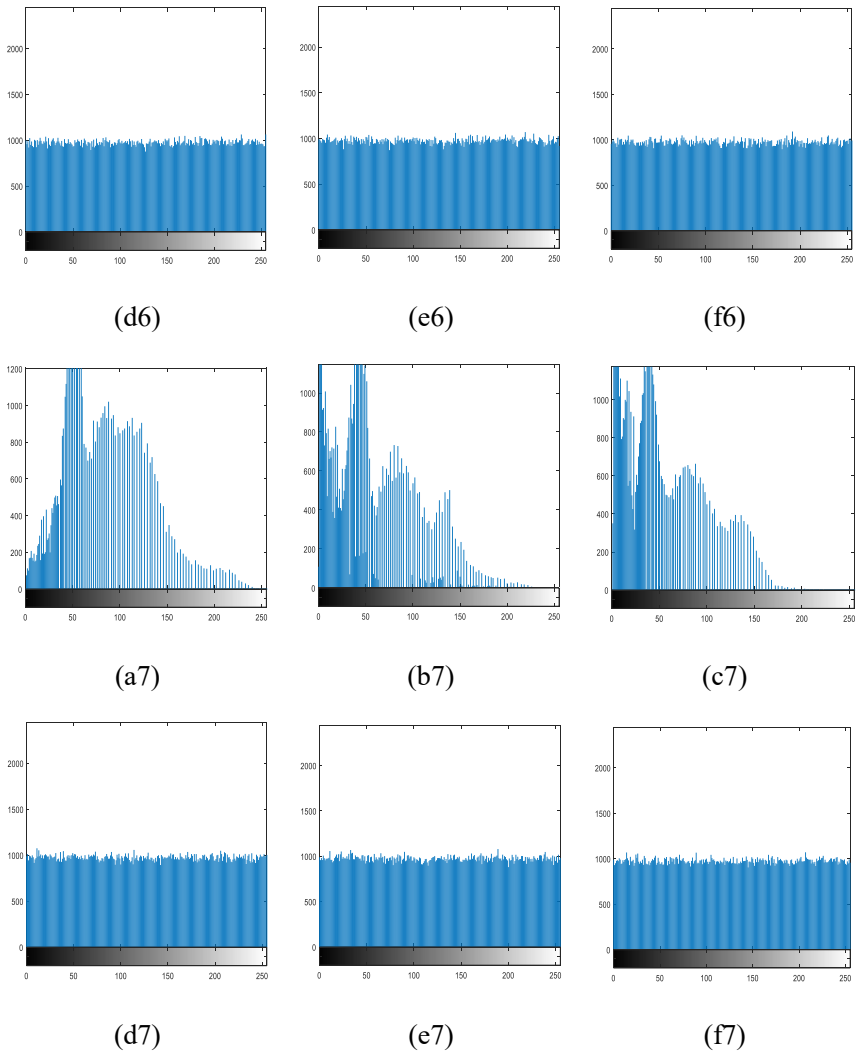
(a6)



(b6)



(c6)



(d6) (e6) (f6)

(a7) (b7) (c7)

(d7) (e7) (f7)

Fig. 4.19 Histograms of the original and encrypted images at $\sigma = 1000$: (a1) - (f1) Peppers, (a2) - (f2) Lena, (a3) - (f3) House, (a4) - (f4) Cartoon, (a5) - (f5) Baboon, (a6) - (f6) Couple and (a7) - (f7) Girl. Histograms of the original images in (a1), (a2), (a3), (a4), (a5), (a6) and (a7) R; (b1) (b2), (b3), (b4), (b5) and (b6) and (b7) G; (c1) (c2) , (c3), (c4), (c5), (c6) and (c7) B components, and its histograms of encrypted images (d1), (d2), (d3), (d4), (d5), (d6) and (d7) R; (e1), (e2), (e3), (e4), (e5), (e6) and (e7) G; (f1), (f2), (f3), (f4), (f5), (f6) and (f7) B.

4.6.4 Correlation of adjacent pixels

Figs. 4.20(a), (b) and (c) are respectively the self-correlations of R, G and B components for the color images Lena and Peppers, while Figs. 4.20(d), (e) and (f) are respectively the self-correlations of the three channels for encrypted image. Tables 4.5-4.7 show respectively the correlation coefficients of R, G and B components in horizontal, vertical and diagonal directions for Lena and encrypted Lena. From Fig.

4.20 and Tables. 4.5-4.7, we can see that there exist strong neighborhood correlations between adjacent pixels of each channel of the original image, whereas those in encrypted image for different values σ are very weak. Consequently, the proposed algorithm can realize effectively the confusion and diffusion for image information, which shows an ability against correlation analysis attack.

Table 4.5. Correlation between two adjacent pixels for R component of color images.

Image	σ	Horizontal direction	Vertical direction	Diagonal direction
Plain Lena		0.9693	0.9433	0.9202
Encrypted Lena	1000	–0.0203	0.0047	0.0001
	500	0.0004	0.0016	0.0009
	100	0.0002	–0.0003	0.0106
	50	0.0051	–0.0004	0.0028
Plain Peppers		0.9474	0.9030	0.9631
Encrypted Peppers	1000	0.0025	0.0077	0.0036
	500	0.0046	0.0070	0.0012
	100	0.0053	0.0071	0.0086
	50	0.0011	0.0082	0.0064
Plain Couple		0.9558	0.9482	0.9155
Encrypted Couple	1000	-0.0040	3.1671e-04	0.0048
	500	-0.0097	-0.0109	0.0064
	100	-0.0045	-0.0108	0.0038
	50	-0.0011	0.0013	-0.0047
Plain Airplane		0.9484	0.9749	0.9396
Encrypted Airplane	1000	-0.0017	-0.0222	0.0013
	500	0.0163	-0.0054	0.0050
	100	0.0023	-0.0032	-0.0124
	50	0.0166	-0.0068	-0.0118
Plain Baboon		0.8229	0.8594	0.8115
Encrypted Baboon	1000	0.0043	8.5483e-04	1.9894e-04
	500	0.0022	3.2248e-05	-0.0157

	100	0.0016	-0.0019	-5.1887e-04
	50	0.0014	0.0038	-0.0143
Plain Girl		0.9581	0.9712	0.9456
	1000	-0.0120	-0.0060	0.0023
Encrypted Girl	500	0.0015	-0.0049	0.0127
	100	-5.6444e-04	0.0118	-0.0071
	50	-0.0012	0.0115	-0.0070
Plain House		0.8229	0.8594	0.8115
	1000	4.3704e-04	-0.0020	-0.0115
Encrypted House	500	-0.0077	-0.0166	-0.0063
	100	-0.0122	-9.1049e-04	0.0101
	50	9.7845e-04	0.0088	-0.0155

Table 4.6. Correlation between two adjacent pixels for G component of color image.

Image	σ	Horizontal direction	Vertical direction	Diagonal direction
Plain Lena		0.9693	0.9433	0.9202
	1000	–0.0120	0.0033	0.0069
Encrypted Lena	500	0.0013	0.0005	0.0037
	100	0.0014	–0.0134	0.0069
	50	0.0033	–0.0086	0.0094
Plain Peppers		0.9450	0.9631	0.9343
	1000	0.0005	0.0047	0.0015
Encrypted Peppers	500	0.0070	0.0033	0.0122
	100	0.0056	0.0003	0.0003
	50	0.0074	0.0083	0.0189
Plain Couple		0.9544	0.9295	0.8896
	1000	0.0106	-0.0133	0.0153
Encrypted Couple	500	-5.5602e-04	-0.0117	-0.0072
	100	-0.0013	6.0187e-05	-0.0122

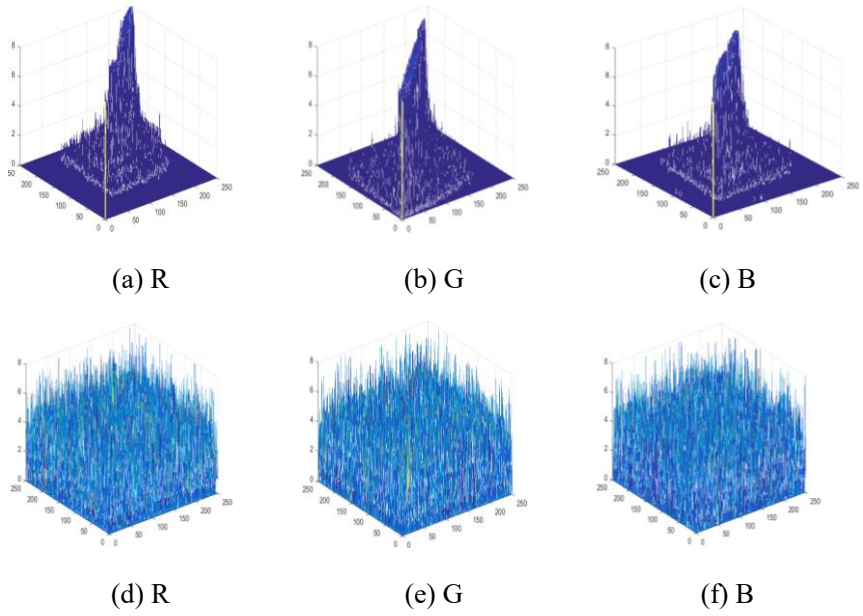
	50	0.0013	0.0025	0.0016
Plain Airplane		0.9682	0.9574	0.9350
Encrypted Airplane	1000	0.0147	0.0106	4.4701e-04
	500	0.0033	-0.0013	-0.0070
	100	0.0047	-0.0076	0.0080
	50	0.0139	-0.0079	-0.0122
Plain Baboon		0.6658	0.7246	0.6383
Encrypted Baboon	1000	3.7679e-04	0.0181	-0.0071
	500	9.3123e-04	0.0100	-0.0062
	100	0.0030	0.0029	-0.0034
	50	0.0163	-0.0173	0.0042
Plain Girl		0.9623	0.9727	0.9498
Encrypted Girl	1000	-0.0076	0.0071	0.0081
	500	0.0077	-0.0025	-0.0106
	100	0.0085	-0.0019	-0.0138
	50	7.9088e-04	-2.2175e-05	0.0011
Plain House		0.8229	0.8594	0.8115
Encrypted House	1000	0.0151	-0.0121	-0.0060
	500	0.0056	-0.0034	-0.0159
	100	-0.0086	0.0115	0.0045
	50	-0.0035	-0.0062	-0.0019

Table 4.7. Correlation between two adjacent pixels for B component of color image.

Image	σ	Horizontal direction	Vertical direction	Diagonal direction
Plain Lena		0.9693	0.9433	0.9202
Encrypted Lena	1000	–0.0015	0.0027	0.0155
	500	0.0009	0.0078	0.0005
	100	0.0016	–0.0067	0.0060

	50	0.0052	–0.0068	0.0050
Plain Peppers		0.9030	0.9280	0.8930
Encrypted Peppers	1000	0.0005	0.0047	0.08930
	500	0.0048	0.0042	0.0023
	100	0.0018	0.0003	0.0127
	50	0.0137	0.0050	0.0129
Plain Couple		0.9406	0.9190	0.8804
Encrypted Couple	1000	-0.0081	-0.0106	-0.0044
	500	0.0103	-0.0102	0.0090
	100	-0.0088	0.0072	1.2100e-04
	50	-0.0011	-0.0033	-0.0087
Plain Airplane		0.9643	0.9744	0.9471
Encrypted Airplane	1000	-9.2010e-04	0.0208	-0.0051
	500	0.0014	-2.4470e-04	-0.0071
	100	-0.0068	0.0092	-0.0119
	50	-0.0058	-0.0015	0.0026
Plain Baboon		0.8148	0.8100	0.7833
Encrypted Baboon	1000	0.0040	0.0084	0.0050
	500	0.0061	0.0094	-0.0127
	100	-0.0014	-0.0144	-0.0055
	50	-0.0033	-0.0070	-0.0079
Plain Girl		0.9516	0.9582	0.9413
Encrypted Girl	1000	-0.0015	-0.0024	-0.0043
	500	0.0012	0.0059	0.0090
	100	-0.0096	-0.0015	-0.0120
	50	0.0097	0.0027	-0.0016
Plain House		0.8229	0.8594	0.8115
Encrypted House	1000	0.0115	-0.0094	-0.0057
	500	0.0020	-2.0144e-05	0.0100
	100	-0.0078	0.0031	0.0107

	50	0.0011	0.0040	0.0057



(a) R (b) G (c) B

(d) R (e) G (f) B

Fig. 4.20 Self-correlations. Original image Lena: (a) R, (b) G, (c) B, encrypted image: (d) R, (e) G, (f) B.

4.6.5 Information entropy analysis

The results in Table 4.8 show that the entropies of R. G and B components of the original Lena and Peppers are about 7, whereas those of encrypted images for different σ values are very close to 8. Therefore, the proposed scheme is enough to resist against the entropy attacks.

Table 4.8 Comparison of entropies of R. G and B components of original and encrypted images for different values σ.

Original images			**Encryption images**			
			$\sigma = 1000$	$\sigma = 500$	$\sigma = 100$	$\sigma = 50$
Lena	R	7.2507	7.9993	7.9992	7.9993	7.9992
	G	7.5941	7.9993	7.9993	7.9992	7.9992
	B	6.9663	7.9992	7.9992	7.9991	7.9993
Peppers	R	7.3430	7.9992	7.9992	7.9993	7.9993
	G	7.5017	7.9993	7.9992	7.9993	7.9993
	B	7.0535	7.9993	7.9991	7.9993	7.9994

	R	6.2477	7.9993	7.9993	7.9992	7.9991
Couple	G	6.0596	7.9994	7.9992	7.9992	7.9992
	B	5.9281	7.9991	7.9993	7.9991	7.9992
	R	6.4224	7.9993	7.9991	7.9994	7.9992
Airplane	G	6.4308	7.9993	7.9993	7.9994	7.9993
	B	5.7474	7.9993	7.9992	7.9993	7.9993
	R	7.6958	7.9993	7.9991	7.9994	7.9992
Baboon	G	7.4656	7.9994	7.9992	7.9992	7.9993
	B	7.7457	7.9993	7.9993	7.9992	7.9993
	R	6.4144	7.9993	7.9992	7.9992	7.9993
Girl	G	6.5693	7.9993	7.9993	7.9992	7.9993
	B	6.3790	7.9993	7.9993	7.9992	7.9993
	R	6.4224	7.9993	7.9992	7.9992	7.9993
House	G	6.4308	7.9992	7.9993	7.9991	7.9993
	B	5.7474	7.9992	7.9993	7.9992	7.9992

4.6.6 Differential attacks

Table 4.9 and Table 4.10 list the NPCR and UACI values for R, G and B components of the decrypted images at different values σ, respectively, from which we can know that the NPCR and UACI values are close to the expected values of 99.6054% and 33.4635%, respectively. It is proved that the proposed algorithm persists the ability to resist differential attacks.

Table 4.9 NPCR (%) values of three channels of encrypted images for different values σ.

Image	channel	$\sigma = 1000$	$\sigma = 500$	$\sigma = 100$	$\sigma = 50$
	R	99.6040	99.6164	99.6072	99.6292
Lena	G	99.6040	99.6164	99.6072	99.6292
	B	99.6040	99.6164	99.6072	99.6292
	R	99.5924	99.5996	99.6108	99.6156
Peppers	G	99.5924	99.5996	99.6108	99.6156
	B	99.5924	99.5996	99.6108	99.6156
	R	99.6192	99.6004	99.6084	99.5920
Couple	G	99.6192	99.6004	99.6084	99.5920

	B	99.6192	99.6004	99.6084	99.5920
Airplane	R	99.6024	99.6196	99.6112	99.6124
	G	99.6024	99.6196	99.6112	99.6124
	B	99.6024	99.6196	99.6112	99.6124
Baboon	R	99.6124	99.6148	99.6096	99.5924
	G	99.6124	99.6148	99.6096	99.5924
	B	99.6124	99.6148	99.6096	99.5924
Girl	R	99.6028	99.5980	99.6140	99.6128
	G	99.6028	99.5980	99.6140	99.6128
	B	99.6028	99.5980	99.6140	99.6128
House	R	99.5900	99.6228	99.6136	99.5724
	G	99.5900	99.6228	99.6136	99.5724
	B	99.5900	99.6228	99.6136	99.5724

Table 4.10. UACI (%) values of three channels of encrypted images for different values σ

Image	channel	$\sigma = 1000$	$\sigma = 500$	$\sigma = 100$	$\sigma = 50$
Lena	R	33.5006	33.5800	33.5220	33.5498
	G	33.4810	33.5517	33.5638	33.5276
	B	33.5342	33.5776	33.5629	33.5249
Peppers	R	33.5326	33.5083	33.5482	33.4805
	G	33.5316	33.5230	33.6002	33.4964
	B	33.5628	33.5026	33.5294	33.4691
Couple	R	33.4483	33.4512	33.4541	33.4915
	G	33.4435	33.4365	33.4996	33.4579
	B	33.4104	33.4644	33.4946	33.4771
Airplane	R	33.4939	33.4811	33.4456	33.4864
	G	33.5242	33.4823	33.4547	33.4488
	B	33.5251	33.4595	33.4268	33.4312
Girl	R	33.5482	33.4921	33.5643	33.5605
	G	33.5345	33.4318	33.5350	33.5358
	B	33.5065	33.4622	33.5774	33.5411
House	R	33.4527	33.4517	33.5200	33.4755
	G	33.4238	33.4543	33.5513	33.5110

B	33.4666	33.4736	33.4995	33.4710

4.6.7 Key-sensitivity and key space analyses

The cipher keys of this proposed algorithm for color image include the fractional orders (p_R, p_G, p_B), the incidence wavelengths $(\lambda_R, \lambda_G, \lambda_B)$, the rotation angles (α, β, θ) and the seeds of logistic maps s_1, s_2, s_3, s_4.

Fig. 4.21(a), (b) and (c) illustrate the decrypted images with one incorrect rotation angles α, and the corresponding deviation of the angles are $\mathrm{d}\alpha = \pi/180$, $\mathrm{d}\alpha = \pi/15$ and $\mathrm{d}\alpha = \pi/2$, respectively. Fig. 4.21(d), (e) and (f) gives the decrypted images with one incorrect angles β, and the deviation of the angles are $\mathrm{d}\beta = \pi/180$, $\mathrm{d}\beta = \pi/15$ and $\mathrm{d}\beta = \pi/2$, respectively. The Fig. 4.21(g), (h) and (i) show the decrypted image with three deviation of the angles $\mathrm{d}\alpha = \mathrm{d}\beta = \mathrm{d}\theta = \pi/180$, $\mathrm{d}\alpha = \mathrm{d}\beta = \mathrm{d}\theta = \pi/15$ and $\mathrm{d}\alpha = \mathrm{d}\beta = \mathrm{d}\theta = \pi/2$. From the Fig. 4.21, it is can be seen that the distortion level of the image color information becomes larger with the increase of the deviation of the rotation angles.

(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Fig. 4.21. The decrypted images with incorrect rotation angles. (a) $\mathrm{d}\alpha = \pi/180$, (b) $\mathrm{d}\alpha = \pi/15$, (c) $\mathrm{d}\alpha = \pi/2$, (d) $\mathrm{d}\beta = \pi/180$, (e) $\mathrm{d}\beta = \pi/15$, (f) $\mathrm{d}\beta = \pi/2$, (g) $\mathrm{d}\alpha = \mathrm{d}\beta = \mathrm{d}\theta = \pi/180$, (h) $\mathrm{d}\alpha = \mathrm{d}\beta = \mathrm{d}\theta = \pi/15$, (i) $\mathrm{d}\alpha = \mathrm{d}\beta = \mathrm{d}\theta = \pi/2$.

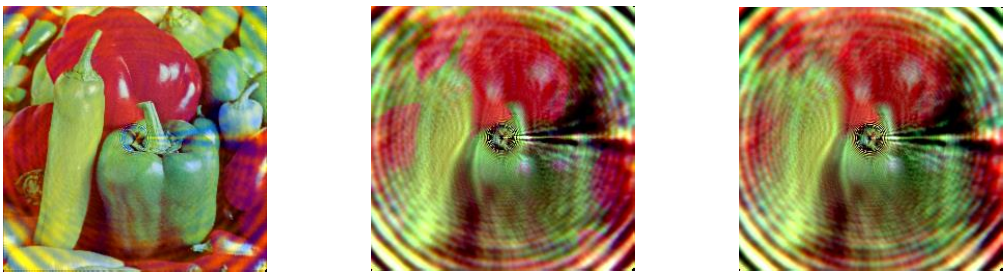
Fig. 4.22 gives decrypted images with incorrect fractional orders. Fig. 4.22(a) shows the decrypted image with only one incorrect fractional order $p_R = 0.55$ while other keys are correct, and we can see that the main information of the decrypted result is kept. Fig. 4.22(b) illustrates the decrypted image with two incorrect fractional orders $p_R = 0.55$ and $p_G = 0.55$, and the decrypted image becomes very blurry. Fig. 4.22(c) shows the decrypted image with three incorrect orders, and we can't recognize what the image looks like. Therefore, the original image can't be recovered unless two correct fractional orders at least are known.

(a) (b) (c)

Fig. 4.22 Decrypted images with (a) only one incorrect fractional order $p_R = 0.55$, (b) two incorrect fractional orders $p_R = 0.55$, $p_G = 0.55$, (c) three incorrect fractional orders $p_R = 0.55$, $p_G = 0.55$, $p_B = 0.55$.

Fig. 4.23 shows the encrypted images with incorrect wavelengths. Fig. 4.23(a) gives the decrypted image with one incorrect wavelength $\lambda_R' = \lambda_R + 5 \times 10^{-7}$. Fig. 4.23(b) illustrates the decrypted image with two incorrect wavelengths $\lambda_R' = \lambda_R + 5 \times 10^{-7}$ and $\lambda_G' = \lambda_G + 5 \times 10^{-7}$, and Fig. 4.23(c) shows the decrypted result with three incorrect wavelengths. From the simulation results as shown in Fig. 4.23(b) - (c), we

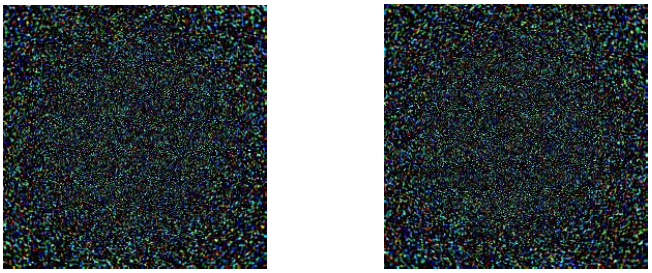
can know that the decrypted image can't be recognized with only one correct wavelength.



(a) (b) (c)

Fig. 4.23. Decrypted images with (a) only one incorrect wavelength $\lambda'_R = \lambda_R + 5 \times 10^{-7}$, (b) two incorrect wavelengths, $\lambda'_R = \lambda_R + 5 \times 10^{-7}$, $\lambda'_G = \lambda_G + 5 \times 10^{-7}$, (c) three incorrect wavelengths, $\lambda'_R = \lambda_R + 5 \times 10^{-7}$, $\lambda'_G = \lambda_G + 5 \times 10^{-7}$, $\lambda'_B = \lambda_B + 5 \times 10^{-7}$.

In the experiment, the key sensitivities for the four seeds of logistic maps are given. Figs. 4.24 shows the decrypted results with incorrect keys and MSE for the deviations of s_1, s_2, s_3 and s_4. Figs. 4.24 (a) - (c) show respectively the decrypted images with incorrect keys s_1, s_2 and s_3 used in 3D logistic map for scrambling (their deviations δ of incorrect value from correct one are 1×10^{-15}). As shown in those results, we can't get any information of the original image at all, since each seed of 3D logistic map will greatly affect the each of components of the image. The decrypted result with a wrong seed s_4 (the deviation δ is 1×10^{-15}) are given in Figs. 4.24(d), and the information of original image still can't be derived. Fig. 4.24(e) - (h) illustrate the MSE for the deviations of those four seeds s_1, s_2, s_3 and s_4 for RGB components, respectively. Therefore, the experimental results indicates that there exists strongly coupling between the keys in different channel. No matter which channel the key is wrong, the decrypted image will have a massive distortion, even cause decryption to fail completely.



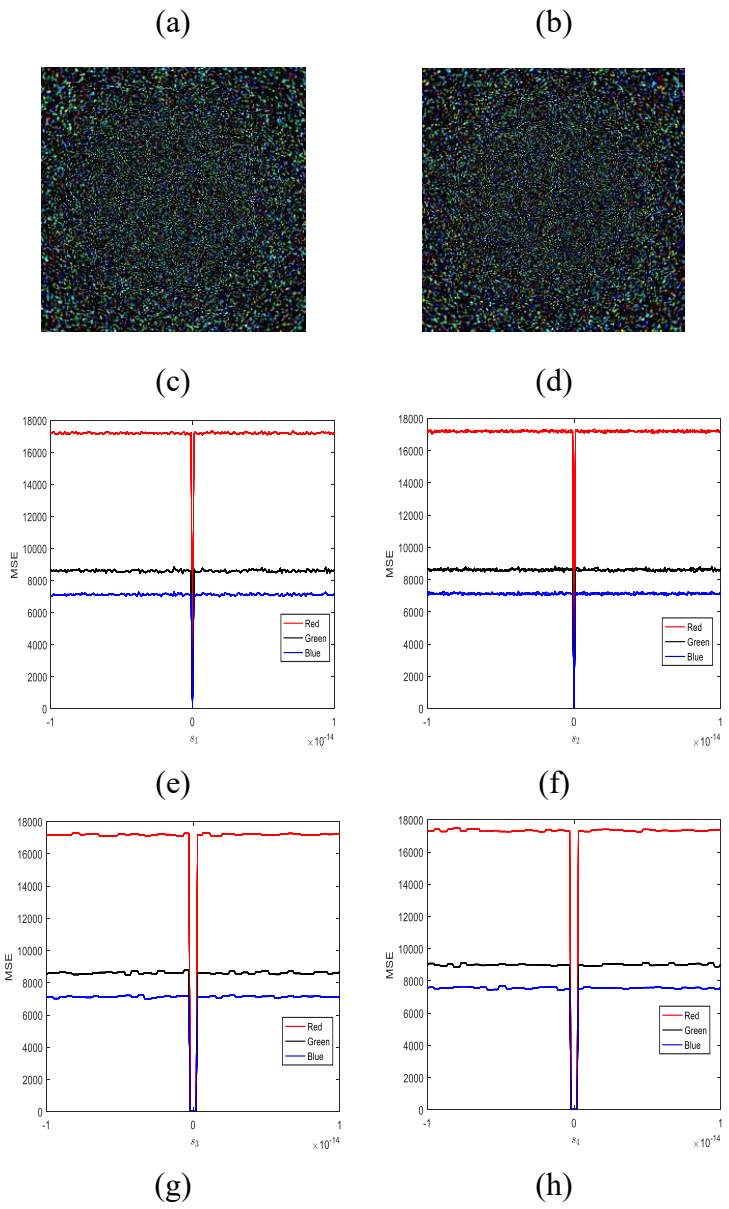


Fig. 4.24 Results decrypted images with incorrect s_1, s_2, s_3 and s_4. (a) incorrect s_1 ($\delta = 1 \times 10^{-15}$), (b) incorrect s_2 ($\delta = 1 \times 10^{-15}$), (c) incorrect s_3 ($\delta = 1 \times 10^{-15}$), (d) incorrect s_4 ($\delta = 1 \times 10^{-15}$); and MSE for the deviations of (e) s_1, (f) s_2, (g) s_3 and (h) s_4 for R, G, B components.

In generally, to ensure the security of encryption algorithm, the key space of the proposed algorithm should be at last up to 10^{30}. The key space of four seeds can be expressed as:

$$S = S_1 \times S_2 \times S_3 \times S_4 \tag{4.6}$$

where S_i represent the key space of the *i*-th seed.

Fig. 4.22 shows that the key space of S_i is 1×10^{-15}. Therefore, the total key space S is 10^{60}, which is greater than 10^{30}. Besides, the key space is further increased by

other keys including the fractional orders (p_R, p_G, p_B), the incidence wavelengths $(\lambda_R, \lambda_G, \lambda_B)$ and the rotation angles (α, β, θ). The GARPFrMT inherits the nonlinearity from the FrMT, which strengthens the security of the image encryption.

4.6.8 Robustness analysis

Salt and peppers noise with different intensity are added into encrypted images to simulate the scenes which the ciphertexts are disturbed by different degree of noise. Fig. 4.25 shows the deviation of MSE versus noise intensity k for R, G and B components. The decrypted images with noise intensity 0.01, 0.1 and 0.2 are illustrated in Fig. 4.26. The experimental results present that the main information of the original image is still recognizable.

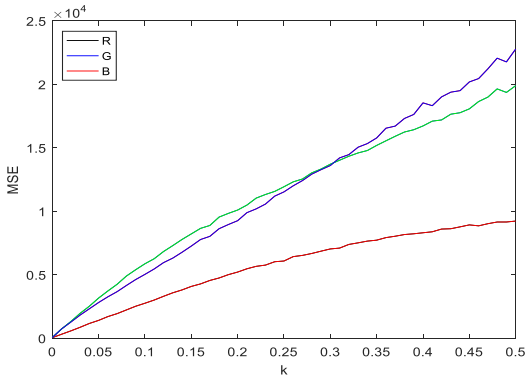
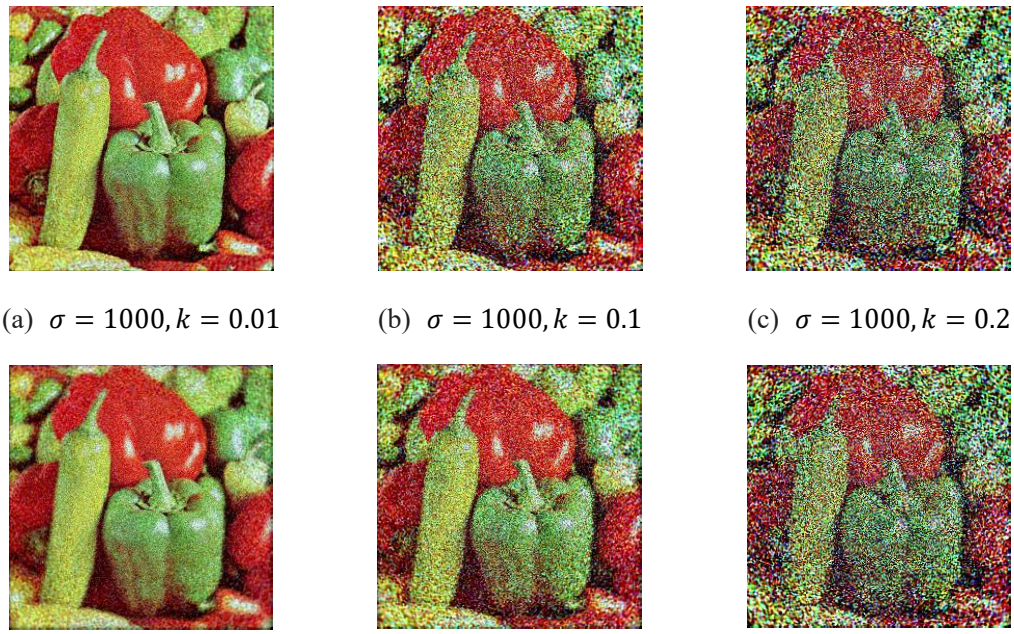


Fig. 4.25 Results of noise attack: The MSE curves for the three channels.



(a) $\sigma = 1000, k = 0.01$ (b) $\sigma = 1000, k = 0.1$ (c) $\sigma = 1000, k = 0.2$

(d) $\sigma = 100, k = 0.01$ (e) $\sigma = 100, k = 0.1$ (f) $\sigma = 100, k = 0.2$

Fig. 4.26 Decrypted images with various intensity of salt and peppers noises. At different values

σ, decrypted images for (a) and (d) $k = 0.01$, decrypted images for (b) and (d) $k = 0.1$, decrypted images for (c) and (f) $k = 0.2$.

The robustness analysis also includes the resistance to occlusion attack. The Fig. 4.27(a) and (f) show the encrypted images with occlusion ratios of 1/16, 1/8 and 1/4 respectively, and the corresponding decrypted images at different values σ are shown in Fig. 4.27(b) - (c), (e) - (f) and (g) - (i), respectively. From the Fig. 4.27, it can be seen that the quality of the decrypted images become lower gradually as the occlusion size increasing. Though the decrypted images are blurred to some extent, the decrypted results are still distinguishable visually. As a consequence, the proposed algorithm has a certain degree of noise against and robustness against.

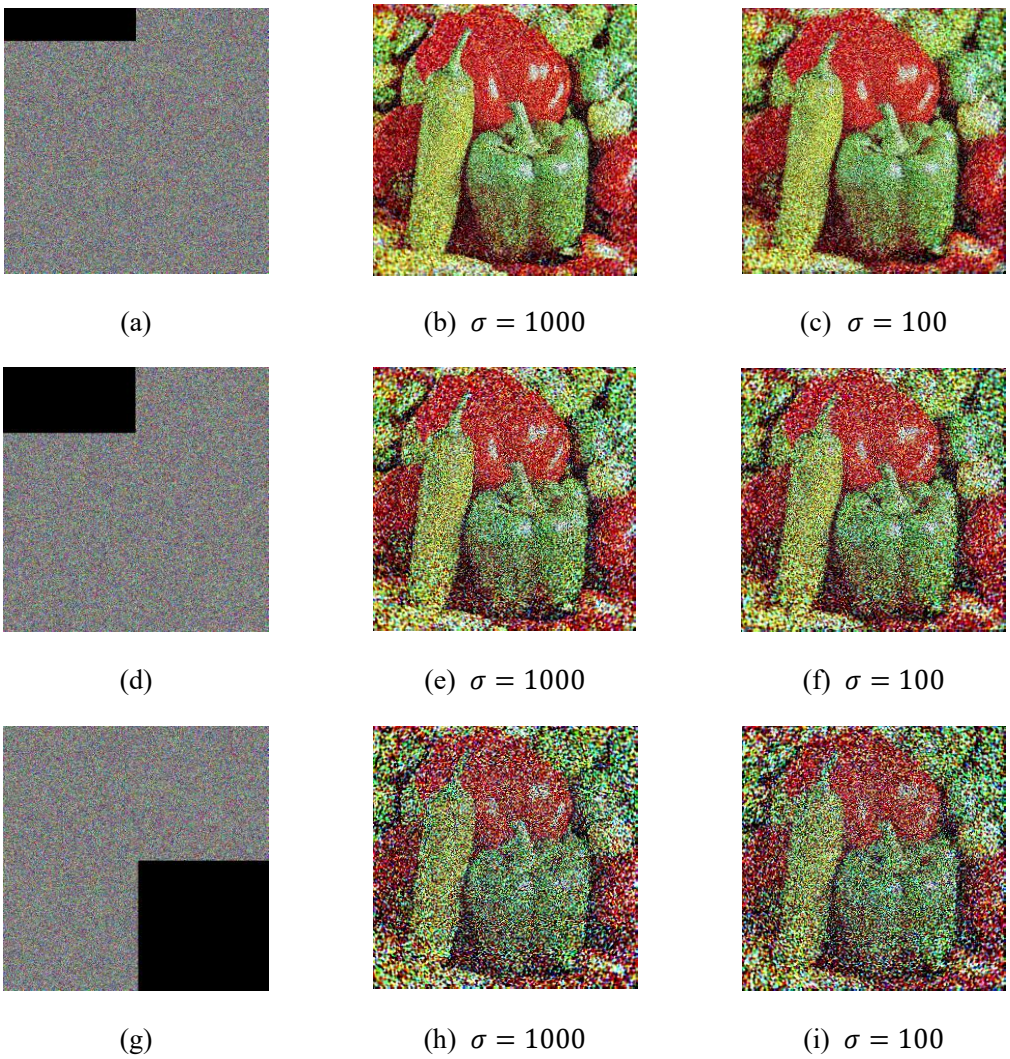


Fig. 4.27 Decrypted Peppers with various occlusion ratios. Encrypted images with (a) 1/16, (d) 1/8, (g) 1/4 occlusion. At the different values σ, decrypted image for (b) and (c) with 1/16 occlusion, decrypted image for (e) and (f) decrypted image with 1/8 occlusion, decrypted image for (h) and (i) with 1/4 occlusion.

4.7 Summary

In this chapter, two image encryption schemes based on the Gaussian apertured reality-preserving fractional Mellin transform are presented.

The first encryption scheme based on a reality-preserving transform with Gaussian apertured is designed for gray image. To further enhance the security of the encryption system, the Arnold transform and the bitwise XOR operation are adopted to encrypt the output of GARPFrMT. The simulation results demonstrate that the Gaussian aperture parameter σ influences the performance of the optical encryption system. In addition, the encryption algorithm is sensitive enough to the cipher keys, and the key space is large enough against brute-force attacks.

The second encryption algorithm using reality-preserving transform with Gaussian aperture is designed to test its implementation for color image. The 3D Logistic map is used to scramble the three channels. The experimental results show that the GARPFrMT is suitable for color image encryption system. The proposed algorithm increases the coupling between channels.

Furthermore, the simulation results of both encryption schemes have shown that the encryption system is capable of resisting different attacks, such as known-plaintext attack, chosen-plaintext attack, and statistical analysis attacks. Besides its high security, the proposed scheme is, to some extent, robust with noise and occlusion attacks.

Chapter 5

Conclusion and perspective

5.1 Summary of thesis

In the mobile internet era, image encryption is a field with great social significance. Thus, this thesis proposes apertured FrMTs in diffraction domain and applies them into optical image encryptions. The encryption schemes are analyzed and verified by a series of numerical simulations. The main contributions are as follows:

Firstly, within the framework of paraxial approximation, the new idea of introducing hard aperture to FrMT is proposed based on apertured FrFT. And the apertured FrMT is applied into a new optical image encryption algorithm for a grayscale image. The hard aperture is used not only to control the amount of light passing the lens by adjusting the size of hard aperture, but also to reduce the leakage of light, which enhances the robustness against the direct attacks to some extent. The size of the aperture is designed as a cipher key to enhance the key space further. The nonlinearity of apertured FrMT can reduce the potential insecurity in an image encryption existing in caused by linear encryption algorithms. The simulation results verify the performance of this image encryption algorithm.

Secondly, the Gaussian lens is introduced into apertured FrMT. The proposed Gaussian apertured reality-preserving FrMT algorithm in diffraction domain ensures that the cipher-text is real, which is convenient for display, transmission and storage. A new encryption scheme for gray images based on GARPFrMT is designed. In this encryption scheme, the Arnold transform and the bitwise XOR operation are also adopted to encrypt the image to enhance the security. As a soft aperture, the Gaussian aperture can improve the intensity distributions of output laser. The feasibility has been verified with a series of numerical simulations.

Thirdly, a new color image encryption scheme based on GAPRFrMT is designed, which ensures that the outputs of three channels are real. The experimental results show

that the GARPFrMT is suitable for color image encryption system, and the proposed algorithm increases the coupling between channels that the decrypted image Furthermore, the simulation results of the encryption scheme have shown that the encryption systems are capable of resisting different attacks, such as known-plaintext attack, chosen-plaintext attack, and statistical analysis attacks. Besides its high security, the proposed scheme is, to some extent, robust with noise and occlusion attacks.

5.2 Future research

In this thesis, the apertured FrMT in diffraction domain and its reality-preserving algorithm are investigated and applied into optical image encryption schemes. However, the discussion and application of apertured FrMT in optical image encryption or other fields have been relatively few so far. Therefore, in this final chapter, we suggest that the following research ideas or directions deserve further exploration.

1. Introducing the hard apertures with irregular polygonal shapes to the implementation apertured FrMT. Besides the size of aperture, its shape can also be designed as the secret key, which improves the security and increases the key space of encryption.

2. Multi-image encryption based on apertured FrMT. Actually, the size of aperture can be used to adjust cut-off frequency of space wave field. Thus, apertured FrMT could be utilized to segment and reassemble images in frequency domain, which could be introduced into multi-image encryption.

3. Introducing the aperture into other optical transforms. The idea of aperture transform can also be used in encryptions based on other optical transforms, such as fractional Hartley transform, the fractional cosine/sine transform.

4. The application of apertured optical transform in image watermarking technique. The special information can be hided in normal images in frequency domain by using the ability of adjusting the frequency bands.

5. Verify the performance by real optical implementation in the future.

References

[1] Z. J. Tang, X. Q. Zhang. Secure image encryption without size limitation using Arnold transform and random strategies [J]. Journal of Multimedia, 2001, 6(2): 202–206.

[2] Richard Spillman. Classical and contemporary cryptology [M]. Prentice Hall, 2005.

[3] X. Peng, H. Z. Wei, P. Zhang. Introduction to Optical Information Security [M]. Beijing: Science press, 2008.

[4] W. Chen, B. Javidi, X. Chen. Advances in optical security systems [J]. Advances in Optics and Photonics, 2014, 6(2): 120–155.

[5] O. Matoba, B. Javidi. Secure holographic memory by double-random polarization encryption [J]. Applied Optics, 2004, 43: 2915–2919.

[6] O. Matoba, B. Javidi. Encrypted optical memory systems based on multidimensional keys for secure data storage and communications [J]. IEEE Circuits Devices Mag. 2000, 16(5): 8–15.

[7] J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini. Multiplexing encrypted data by using polarized light [J]. Optics Communications. 2006, 260: 109–112.

[8] O. Matoba, B. Javidi. Encrypted optical storage with wavelength-key and random phase codes [J]. Applied Optics. 1999, 38: 6785–6790.

[9] P. Refregier, B. Javidi. Optical image encryption based on input plane and Fourier plane random encoding [J]. Optical Letters, 1995, 20: 767–769.

[10] X. Tan, O. Matoba, T. Shimura, K. Kuroda, and B. Javidi. Secure optical storage that uses fully phase encryption [J]. Applied Optics, 2000, 39: 6689–6694.

[11] G. H. Situ, J. J. Zhang. Double random-phase encoding in the Fresnel domain [J]. Optics Letters, 2004, 29(14): 1854–1856.

[12] L. F. Chen, G. J. Chang, B. Y. He, H. D. Mao, D. M. Zhao. Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition [J]. Optics and Lasers in Engineering, 2017, 88: 221–232.

[13] Javidi B. Securing information with optical technologies [J]. Physics Today, 1997, 50: 27–32.

[14] R. Kumar, J. T. Sheridan, B. Bhaduri. Nonlinear double image encryption using 2D non-separable linear canonical transform and phase retrieval algorithm [J]. Optics and Laser Technology, 2018, 107: 353–360.

[15] X. G. Wang, D. M. Zhao. Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain [J]. 2011. 284: 148–152.

[16] B. Zhu, S. Liu, Q. Ran. Optical image encryption based on multi-fractional Fourier transforms [J]. Optics Letters, 2000, 25: 1159–1166.

[17] G. Unnikrishnan, J. Joseph, K. Singh. Optical encryption by double-random phase encoding in the fractional Fourier domain [J]. Optics Letters, 2000, 25: 887–899.

[18] B. M. Hennelly, J. T. Sheridan. Image encryption and the fractional Fourier transform [J]. Optik, 2003, 114(6): 251–265.

[19] H. M. Ozaktas, M. P. Kutay, Zalevsky. The fractional Fourier transform with applications in optics and signal processing [M]. 2001, England: Wiley.

[20] Sui L, Xin M, Tian A, Jin H. Single-channel color image encryption using phase retrieve algorithm in fractional Fourier domain [J]. Optics and Lasers in Engineering, 2013, 51: 1297–1309.

[21] R. G. Dorsch, A. W. Lohmann. Fractional Fourier transform used for a lens-design problem [J]. Applied Optics, 1995, 34(20): 4111–4112.

[22] A. W. Lohmann. Image rotation, Wigner rotation, and the fractional Fourier transform [J]. Journal of the Optical Society of America A, 1993, 10(10): 2181–2186.

[23] J. W. Goodman. Introduction to Fourier optics [M]. 1996, United State, 2nd ed.

McGrawHill.

[24] H. E. Hwang. Optical color image encryption based on the wavelength multiplexing using cascaded phase-only masks in Fresnel transform domain [J]. Optics Communications, 2012, 285: 567–573.

[25] N. R. Zhou, Y. X. Wang, L. Gong. Novel optical image encryption scheme based on fractional Mellin transform [J]. Optics Communications, 2011, 284(13): 3234–3242.

[26] N. R. Zhou, Y. X. Wang, J. H. Wu. Image encryption algorithm based on the multi-order discrete fractional Mellin transform [J]. Optics Communications 2011, 284: 5588–5597.

[27] N. R. Zhou, H. Li, D. Wang, S. Pan, Z. Zhou. Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform [J]. Optics Communications, 2015, 343: 10–21.

[28] N. R. Zhou, Y. X. Wang, L. Gong, X. Chen, Y. Yang. Novel color image encryption algorithm based on the reality preserving fractional Mellin transform [J]. Optics and Laser Technology, 2012, 44(7): 2270–2281.

[29] L. H. Gong, C. Z. Deng, S. M. Pan, N. R. Zhou. Image compression-encryption algorithms by combining hyper chaotic system with discrete fractional random transform [J], Optics and Laser Technology, 2018, 103: 48–58.

[30] N. Singh, A. Sinha. Chaos based multiple image encryption using multiple canonical transforms [J]. Optics and Laser Technology, 2010, 42: 724–731.

[31] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, S. T. Liu. Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains [J]. Optics Communication, 2011, 284: 123–128.

[32] Abuturab MR. Color information security system using discrete cosine transform in gyrator transform domain radial-Hilbert phase encoding [J]. Optics and Lasers in Engineering, 2012, 50: 1209–1216.

[33] Y. R. Liang, G. Liu., N. R. Zhou, J. H. Wu. Image encryption combining multiple generating sequences controlled fractional dct with dependent scrambling and diffusion [J]. Journal of Modern Optics, 2015, 62(4): 251-264.

[34] L. Zhang, J. Wu, N. R. Zhou. Image Encryption with Discrete Fractional Cosine Transform and Chaos [C]. 2009, Fifth International Conference on Information Assurance & Security. IEEE Computer Society.

[35] S. Kumar, B. Panna, R. K. Jha, Medical image encryption using fractional discrete cosine transform with chaotic function [J]. Medical and Biological Engineering and Computing, 2019: 1–17

[36] L. Chen, D. M. Zhao. Optical image encryption based on fractional wavelet transform [J]. Optics communications, 2005, 254(4–6): 361–367.

[37] J. A. Rodrigo, T. Alieva, M. L. Calvo. Experimental implementation of the gyrator transform [J]. Journal of the Optical Society of America A, 2007, 24(10): 3135–3139.

[38] M. R. Abuturab. Noise-free recovery of color information using a joint-extended gyrator transform correlator [J]. Optics and Lasers in Engineering, 2013, 51: 230–239.

[39] J. A. Rodrigo, T. Alieva, M. L. Calvo. Application of gyrator transform for image processing [J]. Optics Communications, 2007, 278: 279–284.

[40] K. L. Wang, C. Zhao. Analytical solution for an anomalous hollow beam in a fractional Fourier transforming optical system with a hard aperture [J]. Optics and Laser Technology, 2012, 44(5): 1232–1239.

[41] X. Peng, P. Zhang, H. Wei, B. Yu. Known-plaintext attack on optical encryption based on double random phase keys [J]. Optical Letters, 2006, 31: 1044–1046.

[42] Y. Frauel, A. Castro, T. J. Naughton, B. Javidi. Resistance of the double random phase encryption against various attacks [J]. Optics Express, 2007, 15(16): 10253–10265.

[43] B. Javidi, G. Zhang, J. Li. Encrypted optical memory using double random phase encoding [J]. Applied optics, 1996, 36(5): 1054–1058.

[44] F. Goudail, F. Bollaro, B. Javidi, R. Philippe.. Influence of a perturbation in a double phase-encoding system [J]. Journal of the Optical Society of America A, 1998, 15(10): 2629–2638.

[45] O. Matoba, B. Javidi. Encrypted optical memory system using three-dimensional

keys in the Fresnel domain [J]. Optics Letters, 1999, 24(11): 762–764.

[46] B. Javidi, T. Nomura. Securing information by use of digital holography [J]. Optics Letters, 2000, 25(1): 28–30.

[47] E. Tajahuerce, O. Matoba, S. C.Verrall and B. Javidi. Optoelectronic information encryption with phase-shifting interferometry [J]. Applied Optics, 2000, 39(14): 2313–2320.

[48] Z. J. Liu, Q. Guo, L. Xu, M. A. Ahmad, S. Liu. Double image encryption by using iterative random binary encoding in gyrator domains [J]. Optics Express, 2010, 18: 12033–12043.

[49] L. Chen, D. Zhao. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms [J]. Optics Express, 2006, 14: 8552–8560

[50] J. H. Wu, L. Y. Zhang, N. R. Zhou. Image encryption based on the multiple-order discrete fractional cosine transform [J]. Optics Communications. 2010, 283(9): 1720–1725.

[51] X. Peng, H. Wei, P. Zhang. Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain [J]. Optics Letters. 2006, 31(22): 3261–3263.

[52] A. Biryukov. Known plaintext attack [M]. Encyclopedia of Cryptography and Security. 2005.

[53] W. Liu, G. Yang, H. Xie. A hybrid heuristic algorithm to improve known-plaintext attack on Fourier plane encryption [J]. Optics Express, 2009 17(16): 13928–13938.

[54] Y. Sheng, Z. Xin, M. S. Alam, L. Xi, L. Xiao-Feng. Information hiding based on double random-phase encoding and public-key cryptography [J]. Optics Express 2009, 17(5): 3270–3284.

[55] N. R. Zhu, Y. X. Wang, J. Liu, J. Xie, H. Zhang. Optical image encryption based on interference of polarized light [J]. Optics Express. 2009, 17(16): 13418–13424.

[56] S. Liu, L. Yu, B. Zhu. Optical image encryption by cascaded fractional Fourier transforms with random phase filtering [J]. Optics Communications, 2001, 187(1-3): 57–63.

[57] Han, Jong-Wook. Optical image encryption based on XOR operations [J]. Optical

Engineering, 1999, 38(1): 47–54.

[58] D. Zhao, X. Li, L. Chen. Optical image encryption with redefined fractional Hartley transform [J]. Optics Communications, 2008, 281(21): 5326–5329.

[59] Ozaktas, M. H., D. Mendlovic. Fractional Fourier transforms and their optical implementation II [J]. Journal of the Optical Society of America A, 1993, 10(12): 2522–2531.

[60] N. Singh, A. Sinha. Optical image encryption using Hartley transform and logistic map [J]. Optics Communications, 2009, 282(6): 1104–1109.

[61] H. M. Ozaktas, D. Mendlovic, L. Onural, B. Barshan. Convolution, filtering, and multiplexing in fractional Fourier domains and their relation to chirp and wavelet transforms [J]. Journal of the Optical Society of America A, 1994, 11(2): 547–559.

[62] D. Mendlovic, Z. Zalevsky, D. Mas, G. Javier, C. Ferreira. Fractional wavelet transform [J]. Applied Optics, 1997, 36(20): 4801–4806.

[63] J. H. Wu, F. F. Guo, P. Zeng, N. R. Zhou. Image encryption based on a reality-preserving fractional discrete cosine transform and a chaos-based generating sequence [J]. Journal of Modern Optics, 2013, 60(20): 1760–1771.

[64] X. Z. Luo, N. R. Zhou, Q. M. Zhao, J. H. Wu. Color image encryption based on the multiple-order discrete fractional cosine transform and chaos in ycbcr space [J]. Applied Mechanics and Materials, 2012, 182-183: 1839-1843.

[65] C. Niu, X. Wang, N. Lv, Z. Zhou, X. Li. An encryption method with multiple encrypted keys based on interference principle [J]. Optics Express, 2010, 18: 7827–7834.

[66] J. Cai, X. Shen, M. Lei, C. Lin, S. Dou. Asymmetric optical cryptosystem based on coherent superposition and equal modulus decomposition [J]. Optics Letters, 2015, 40: 475–478.

[67] L Chen, J. Liu, J. Wen, H. Mao, F. Ge, D. Zhao. Pseudo color image encryption based on three-beams interference principle and common vector composition [J]. Optics Communications, 2015, 338: 110–116.

[68] L. Chen, J. Liu, J. Wen, X. Gao, H. Mao, X. Shi, Q. Qu. A new optical image encryption method based on multi-beams interference and vector composition [J].

Optics Laser Technology, 2015, 69: 80–86.

[69] Q. Wang. Optical image encryption with silhouette removal based on interference and phase blend processing [J]. Optics Communication 2012, 285: 4294–4301.

[70] Z. Liu, C. Guo, J. Tan, W. Liu, J. Wu, Q. Wu, L. Pan, S. Liu. Securing color image by using phase-only encoding in Fresnel domains [J]. Optics Lasers in Engineering 2015, 68: 87–92.

[71] Z. Liu, H. Zhao, S. Liu. A discrete fractional random transform [J]. Optics Communications, 2005, 255(4-6): 357-365.

[72] Z. Liu, Q. Guo, S. Liu. The discrete fractional random cosine and sine transforms [J]. Optics Communications, 2006, 265(1): 100-105.

[73] Y. Zhang, D. Xiao. Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform [J]. Optics and Lasers in Engineering, 2013, 51(4): 472-480.

[74] X. Wang, Y. Chen, C. Dai, D. Zhao. Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform [J]. Applied Optics, 2014, 53: 208–213

[75] Deng X, Zhao D. Multiple-image encryption using phase retrieve algorithm and intermodulation in Fourier domain [J]. Optics Laser Technology. 2012, 44: 374–377.

[76] X. G. Wang, W. Chen, X. Chen. Optical Encryption and Authentication Based on Phase Retrieval and Sparsity Constraints [J]. IEEE Photonics Journal, 2017, 7(2): 1-10.

[77] L. Sui, M. Xu, A. Tian. Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain [J]. Optics and Lasers in Engineering, 2017, 91: 106-114.

[78] Q. Liu, Y. Wang, J. Wang, Q. H. Wang. Optical image encryption using chaos-based compressed sensing and phase-shifting interference in fractional wavelet domain [J]. Optical Review, 2018, 25(1): 46-55.

[79] P. Singh, A. K. Yadav, K. Singh, I. Saini. Optical image encryption in the fractional Hartley domain, using Arnold transform and singular value decomposition [J].

2017.

[80] S. C. Pei, M. H. Yeh. The discrete fractional cosine and sine transforms [J]. IEEE Transactions on Signal Processing, 2001, 49(6): 1198-1207.

[81] S. C. Pei, C. C. Tseng, M. H. Yeh, J. J. Shyu. Discrete fractional Hartley and Fourier transforms [J]. IEEE Transactions on Circuits & Systems II Analog & Digital Signal Processing, 1998, 45(6): 665-675.

[82] S. C. Pei, W. L. Hsue. The multiple-parameter discrete fractional Fourier transform [J]. IEEE Signal Processing Letters, 2006, 13(6): 329-332.

[83] W. L. Hsue, S. C. Pei. The multiple-parameter discrete fractional Fourier transform and its application [C]. IEEE International Conference on Acoustics. 2006.

[84] S. C. Pei, J. J. Ding. Eigenfunctions of the offset Fourier, fractional Fourier, and linear canonical transforms [J]. Journal of the Optical Society of America A, 2003, 20(3): 522-532.

[85] S. C. Pei, J. J. Ding. Fractional, canonical, and simplified fractional cosine transforms [C]. IEEE International Conference on Acoustics. 2001.

[86] M. H. Yeh, S. C. Pei. A method for the discrete fractional Fourier transform computation [M]. 2003.

[87] S. C. Pei, M. H. Yeh, T. L. Luo. Discrete fractional Fourier transform [C]. IEEE International Symposium on Circuits & Systems. 1996.

[88] W. L. Hsue, S. C. Pei. Random Discrete Fractional Fourier Transform [J]. IEEE Signal Processing Letters, 2009, 16(12): 1015-1018.

[89] Z. Moghaddasi, H. A. Jalab, Noor R M. Image splicing forgery detection based on low-dimensional singular value decomposition of discrete cosine transform coefficients [J]. Neural Computing & Applications, 2018, (1): 1-11.

[90] K. K. Hasan, S. S. Saleh, M. U. Barrak. Reserved Discrete Cosine Transform Coefficients Effects on Image Compression [J]. IOP Conference Series Materials Science and Engineering, 2018, 454(1): 012071.

[91] G. U. Fan, C. Tang, G. Yong, S. U., J. Cheng, Y. Bi, I. L., Z. Lei. Image encryption based on discrete cosine transform and Ushiki map [J]. Optical Technique, 2017,

43(4): 319-322 and 328.

[92] Z. Zhong, H. Qin, L. Liu, Y. Zhang, M. Shan. Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain [J]. Optics Express, 2017, 25(6): 6974–6982.

[93] J. Lang. Image encryption based on the reality-preserving multiple-parameter fractional Fourier transform and chaos permutation [J]. Optics and Lasers in Engineering, 2012, 285(10-11): 2584–2590.

[94] J. Lang. Color image encryption based on color blend and chaos permutation in the reality-preserving multiple-parameter fractional Fourier transform domain [J]. Optics Communications, 2015, 338(338): 181-192.

[95] X. M. Li, R. Tao, L. L. Dai, Y. Yang. Reality-preserving image encryption associated with the generalized Hilbert transform [C]. IEEE International Symposium on Industrial Electronics. 2009.

[96] J. Fridrich. Symmetric ciphers based on two-dimensional chaotic maps [J]. International Journal of Bifurcation and Chaos. 1998, 8(6): 1259–1284.

[97] T. Habutsu, Y. Nishio, I. Sasase, S. Mori. A secret key cryptosystem by iterating a chaotic map [C]. in: D. Davies (Ed.), Advances in Cryptology - EUROCRYPT'91, Lecture Notes in Computer Science, 547, Springer Berlin Heidelberg, 1991, pp. 127–140.

[98] N. R. Zhou, H. Jiang, L. H. Gong, X. W. Xie. Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging [J]. Optics and Lasers in Engineering. 2018, 110: 72–79.

[99] X. Li, D. Xiao, Q. H. Wang. Error-free holographic frames encryption with ca pixel-permutation encoding algorithm [J]. Optics and Lasers in Engineering. 2018, a100: 200–207.

[100] L. Xu, Z. Li, J. Li, W. Hua. A novel bit-level image encryption algorithm based on chaotic maps [J]. Optics and Lasers in Engineering. 2016, 78: 17–25.

[101] W. Liu, K. Sun, C. Zhu. A fast image encryption algorithm based on chaotic map [J]. Optics and Lasers in Engineering. 2016, 84: 26–36

[102] Y. Zhou, L. Bao, C.L.P. Chen. A new 1D chaotic system for image encryption

[J]. Signal Processing. 2014, 97: 172–182.

[103] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems [J]. International Journal of Bifurcation and Chaos. 2006, 16(8): 2129–2151.

[104] N. K. Pareek, V. Patidar, K. K. Sud. Image encryption using chaotic logistic map [J]. Image and Vision Computing, 2006, 24(9):926–934.

[105] Z. Y. Hua, Y. C. Zhou. Image encryption using 2D Logistic-adjusted-Sine map [J]. Information Sciences, 2016, 339: 237–253.

[106] Z. Y. Hua, F. Jin. B. X. Xu, H. J. Huang. 2D Logistic-Sine-coupling map for image encryption [J]. Signal processing, 2018, 149: 148–161.

[107] X. Wang, D. Zhao. Simultaneous nonlinear encryption of grayscale and color images based on phase-truncated fractional Fourier transform and optical superposition principle [J]. Applied Optics, 2013, 52(25): 6170–6178.

[108] A. Jacobo, M. C. Soriano, C. R. Mirasso, P. Colet. Chaos-Based Optical Communications: Encryption Versus Nonlinear Filtering [J]. IEEE Journal of Quantum Electronics, 2010, 46(4): 499–505.

[109] M. Joshi, C. Shakher, K. Singh. Logarithms-based RGB. Image encryption in the fractional Fourier domain: A non-linear approach [J]. Optics and Lasers in Engineering 2009, 47: 721–727.

[110] N. R. Zhou, A. Zhang, F. Zheng, L. H. Gong. Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing [J]. Optics and Laser Technology, 2014, 62(10): 152–160.

[111] R. Huang, K. H. Rhee, S. Uchida. A parallel image encryption method based on compressive sensing [J]. Multimedia Tools and Applications, 2014, 72(1): 71–93.

[112] L. Pei, Z. Xu, Xi L, X. Liu. Digital image information encryption based on Compressive Sensing and double random-phase encoding technique [J]. Optik - International Journal for Light and Electron Optics, 2013, 124(16): 2514–2518.

[113] X. Liu, W. Mei, H. Du. Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain [J]. Journal of Modern Optics,

2014, 61(19): 1570–1577.

[114] C. E. Shannon. Communication theory of secrecy systems. 1945 [J]. Bell System Technical Journal, 1949, 28(4): 656–715.

[115] M. Zhang, X. Tong. A new chaotic map based image encryption schemes for several image formats [J]. Journal of Systems and Software, 2014, 98: 460–154.

[116] Z. Liu, L. Xu, J. Dai, S. Liu. Image encryption by using local random phase encoding in fractional Fourier transform domains [J]. Optik - International Journal for Light and Electron Optics, 2012, 123(5):428–432.

[117] R. Zahmoul, R. Ejbali, M. Zaied. Image encryption based on new Beta chaotic maps [J]. Optics and Lasers in Engineering, 2017, 96: 39–49.

[118] X. Y. Wang, F. Chen, T. Wang. A new compound mode of confusion and diffusion for block encryption of image based on chaos [J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15(9): 2479–2485.

[119] M. A. Alzain, O. S. Faragallah. Efficient Chaotic Tent Map-based image cryptosystem [J]. International Journal of Computer Applications, 2017, 167: 12–17

[120] L. C. Chiun, A. Mandangan, A. Daud, C. Hussin. Image encryption and decryption by using logistic-sine chaotic system and logistic-tent chaotic system [C]. 4th International Conference on Mathematical Sciences. AIP Publishing LLC, 2017.

[121] X. Huang, G. Ye. An efficient self-adaptive model for chaotic image encryption algorithm [J]. Communications in Nonlinear Science and Numerical Simulation, 2014, 19(12): 4094–4104.

[122] Y. Li, X. Li, X. Jin, et al. An Image Encryption Algorithm based on zigzag transformation and 3-Dimension chaotic logistic map [C]. International Conference on Applications and Techniques in Information Security. Springer Berlin Heidelberg, 2015.

[123] G. Ye, K. Jiao, C. Pan, X. L. Huang. An effective framework for chaotic image encryption based on 3D logistic map [J]. Security and Communication Networks, 2018, 2018:1–11.

[124] D. Dragoman, M. Dragoman. Temporal implementation of Fourier-related transforms [J]. Optics Communications, 1998, 145(1-6): 33–37.

[125] A. C. Mcbride, F. H. Kerr. On Namias fractional Fourier transforms [J]. IMA Journal of Applied Mathematics, 1987, 39(2): 159–175.

[126] Namias, Victor. The fractional order Fourier transform and its application to quantum mechanics [J]. Geoderma, 1980, 25(3): 241–265.

[127] Pellat-Finet P. Fresnel diffraction and the fractional-order Fourier transform [J]. Optics Letters, 1994, 19(18):1388–1390.

[128] R. G. Dorsch, A. W. Lohmann. Fractional Fourier transform used for a lens design problem [J], Applied Optics, 1995, 34(20): 4111–4112.

[129] H. T. Yura, S. G. Hanson, T. P. Grum. Speckle: Statistics and interfere of metric decorrelation effects in complex ABCD optical systems [J], Journal of the Optical Society of America A, 1993, 10(2): 316–322.

[130] M. Santarsiero. Propagation of generalized Bessel-Gauss beams through ABCD optical systems [J], Optics Communications, 1996, 132(1-2): 1–7.

[131] S. C. Pei, J. J. Ding. Closed-form discrete fractional and affine Fourier transforms [J], IEEE Transactions on Signal Processing, 2000, 48(5): 1338–1353.

[132] H. M. Ozaktas, O. Arikan, M. A. Kutay, G. Bozdagt. Digital computation of the fractional Fourier transform [J], IEEE Transactions on Signal Processing, 1996, 44(9): 2141–2150.

[133] García Javier, D. Mas, R. G. Dorsch. Fractional-Fourier-transform calculation through the fast-Fourier-transform algorithm [J], Applied Optics, 1996, 35(35): 7013–7018.

[134] Almeida, L. B. The fractional Fourier transform and time-frequency representations [J], IEEE Transactions on Signal Processing, 1994, 42(11): 3084–3091.

[135] A. Kilicman, M. Omran. Note on fractional Mellin transform and applications [J]. SpringerPlus, 2016, 5(1): 100.

[136] D. Casasent, D. Psaltis. Scale invariant optical correlation using Mellin

transforms [J]. Optics Communications, 1976, 17(1):59-63.

[137] D. Young. Straight lines and circles in the log-polar image [C], Proceedings of the British Machine Vision Conference 2000, Bristol, UK, September 2000, 11–14.

[138] K. Schindler. Geometry and construction of straight lines in log-polar images [J], Computer Vision and Image Understanding, 2006, 103(3): 196–207.

[139] Li YJ, Zhang K. Vision bionics image guidance technique and application, National [M]. Beijing: Defense Industry Press; 2006.

[140] Z. J. Liu, M. Gong, Y. K. Dou, F. Liu, S. Lin, M. A. Ahmad, J. M. Dai, Liu. S. T.. Double image encryption by using Arnold transform and discrete fractional angular transform [J]. Optics and Lasers in Engineering 2012, 50(2): 248-255.

[141] I. Venturini, P. Duhamel. Reality preserving fractional transforms [signal processing applications] [C]. IEEE International Conference on Acoustics. 2004.

[142] Y. Xin, R. Tao, Y. Wang. Real-value encryption of digital image utilizing fractional Fourier transform [J]. Optical Technology 2008, 34: 498–508.

[143] Y. Zhang, Y. J. Tang. A plaintext-related image encryption algorithm based on chaos [J]. Multimedia Tools and Applications, 2018, 77: 6647–6669.

[144] R. C. Gonzalez, R. E. Woods. Digital Image Processing (3rd Edition) [M]. Prentice-Hall, Inc. 2007.

[145] S. Vashisth, H. Singh, A.K.Yadav, K. Singh. Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval [J]. Optik. 125 (2014): 5309–5315.

[146] D. Sazbon, Z. Zalevsky, E. Rivlin, D. Mendlovic. Using Fourier/Mellin-based correlators and their fractional versions in navigational tasks [J]. Pattern Recognition, 2002, 35(12), 2993–2999.

[147] H. Wang, D. Xiao, X. Chen, H. Y. Huang. Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map [J]. Signal Processing 2018, 144: 444-452.