Contributions à l'évaluation de systèmes biométriques embarqués

Benoît Vibert

Normandie Université

THESE

Pour obtenir le diplôme de doctorat

Spécialité Informatique

Préparée au sein de l'établissement : Université Caen Normandie

Contributions à l'évaluation de systèmes biométriques embarqués

Présentée et soutenue par
Benoît VIBERT

Thèse soutenue publiquement le 4 Mai 2017 devant le jury composé de		
Mme. Hélène LAURENT	MCF HDR à l'INSA Val de Loire Bourges	Rapporteur
M. Amine NAIT ALI	Professeur à l'Université Paris Est Créteil	Rapporteur
M. Jean-Luc DUGELAY	Professeur à EUROCOM Sophia Antipolis	Examinateur
M. Jean-Marie LE BARS	MCF HDR à l'Université de Caen Normandie	Examinateur
M. Christophe CHARRIER	MCF HDR à l'Université de Caen Normandie	Co-directeur de thèse
M. Christophe ROSENBERGER	Professeur à l'ENSICAEN	Directeur de thèse

Thèse dirigée par Christophe ROSENBERGER et co-dirigée par Christophe CHARRIER, laboratoire GREYC

UNIVERSITÉ CAEN NORMANDIE

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

MI∫IΣ

GREYC

Pour ma famille

Résumé

La biométrie suscite de plus en plus d'intérêt de la part des industriels car nous avons besoin de nouvelles méthodes d'authentification d'un individu : pour du contrôle d'accès physique, du contrôle aux frontières ou pour du paiement. Ces données non révocables et sensibles sont très souvent stockées sur des systèmes embarqués de type élément sécurisé (SE), comme par exemple une carte à puce. Ces SE embarquent aussi un module de comparaison nommé On-Card-Comparison (OCC), permettant de déterminer si le template présenté correspond bien à celui stocké sur l'élément sécurisé. Dans cette thèse, nous nous intéressons particulièrement aux empreintes digitales car c'est une modalité biométrique bien perçue par les usagers.

Nous proposons dans cette thèse différentes contributions permettant d'évaluer des systèmes biométriques embarqués. La première est une plateforme d'évaluation de systèmes biométriques nommée EVABIO. La seconde contribution, permet d'évaluer l'incidence sur les performances lors de la réduction de templates biométriques lorsqu'ils doivent être stockés sur un SE. Nous proposons des méthodes permettant de réduire la taille du template biométrique tout en gardant un taux de reconnaissance élevé, garantissant ainsi un bon niveau de performance du système biométrique complet. La dernière contribution étudie les attaques d'un système biométrique embarqué sur SE. Nous regardons quels a priori sont importants pour un imposteur : nous avons montré que le type de l'empreinte digitale est une information importante pour un attaquant. Nous avons également proposé une contre-mesure pour les systèmes embarqués.

Summary

Biometrics is sparking the interest of manufacturers and industrial compagnies because we are in need of new methods of authenticating individuals: for physical access control, border control or for payments. Non-revocable and sensitive data is very often stored on embedded systems of the secure element type (SE), such as a smart card. SEs include a comparison module called On-Card-Comparison (OCC), which determines whether the template presented corresponds to the template stored within it. In this thesis, we are particularly interested in fingerprints because it is a biometric modality that is very well perceived by the population.

We propose in this thesis different contributions to evaluate embedded biometric systems. The first is a biometric evaluation platform called EVABIO. The second contribution evaluates the impact on performance when reducing biometric templates that are to be stored on an SE. We propose methods to reduce the size of biometric templates while maintaining a high recognition rate thus, guaranteeing a good level of performance of the global biometric system. The last contribution studies attacks on a biometric system that is embedded on a SE. We look at what a priori are important for an impostor: we have shown that the type of fingerprint is an important a priori and the reason why we have also proposed a countermeasure for embedded systems.

Table des matières

Chapitre 1

Introduction

Sommaire

« Il n'y a pas de chute sans gravité. »

Isaac Newton, 1665

1.1 Contexte

Cette thèse a été financée par le biais d'un projet EUROSTAR (numéro de projet E !8324 OffPAD) portant sur l'utilisation d'un objet de confiance avec capteur d'empreinte digitale, et un élément sécurisé pour différentes applications en sécurité. On peut citer comme application par exemple la gestion décentralisée de données personnelles au sein de cet objet en possession de l'utilisateur. J'ai effectué cette thèse à Caen au sein de l'Ecole doctorale Mathématiques, Information, Ingénierie des Systèmes (MIIS), et du laboratoire Groupe de Recherche en informatique, image, automatique et instrumentation (GREYC) dans l'équipe Monétique & Biométrie depuis octobre 2013 sous la direction de Christophe Rosenberger, la co-direction de Christophe Charrier et l'encadrement de Jean-Marie Le Bars. La sécurité des transactions électroniques ainsi que la biométrie font partie des domaines de recherche

de cette équipe, c'est pourquoi j'ai effectué cette thèse dans cette équipe du laboratoire. La biométrie étant de plus en plus utilisée pour identifier un individu que ce soit pour le contrôle d'accès à un bâtiment, le contrôle aux frontières mais aussi plus récemment pour le paiement, il devient nécessaire d'étudier et d'enrichir l'évaluation et la sécurisation de ces systèmes. Ma thèse s'articule dès lors autour du thème lié à l'évaluation des systèmes biométriques embarqués.

1.2 Motivations

La biométrie suscite de plus en plus d'intérêt de la part des industriels comme moyen d'authentification forte d'un individu pour des transactions électroniques sécurisées. De plus, la biométrie est de plus en plus présente dans notre quotidien, tout comme l'utilisation de nos cartes bancaires pour du paiement.

Nous utilisons le code PIN pour valider les transactions chez un commerçant (en face à face). Celui-ci nous permet simplement de montrer que nous connaissons un secret associé à la carte et ne permet absolument pas de nous authentifier de manière sûre. C'est la raison pour laquelle la biométrie est de plus en plus utilisée pour authentifier une personne et ainsi avoir une meilleure preuve de l'identité du porteur. Depuis 2013, les téléphones portables (Iphone,...) ont été dotés de capteurs d'empreinte digitale, au départ pour déverrouiller le téléphone, puis progressivement les usages ont évolué permettant ainsi à l'utilisateur de faire des achats sur internet. Depuis 2014, Apple a lancé le service Apple Pay dans un premier temps aux Etat-Unis, puis quelques mois après au Canada. La chine a suivi très rapidement au début de l'année 2015 et le Royaume-Uni en juillet. Lorsque l'on souhaite inclure un processus d'authentification biométrique dans un élément sécurisé (SE), il doit obligatoirement comporter un module permettant de déterminer si la donnée biométrique est suffisamment similaire à celle enregistrée sur le SE lors de l'enrôlement. Ce module est communément nommé OCC (On-Card-Comparison) ou MOC (Match-On-Card). Cet OCC doit être caractérisé et certifié par un organisme agréé par le GIE Carte Bancaire pour que le système soit autorisé en France. Pour effectuer cette certification, il est nécessaire d'avoir recours à des plateformes d'évaluations certifiées et, à l'heure actuelle, aucune plateforme ne remplit ce critère de certification. Ces plateformes d'évaluation doivent caractériser les algorithmes avec des métriques de performance, des scénarii d'attaque, etc...

Cette thèse attaque trois verrous scientifiques. Le premier est inhérent aux méthodes et outils permettant de réaliser une évaluation d'un système biométrique

embarqué dans un élément sécurisé. Le second concerne la réduction d'un template biométrique lorsque ce dernier est embarqué sur un élément sécurisé. Les méthodes de l'état de l'art n'ont pas les meilleures performances en terme de taux de reconnaissance et nous proposons de nouvelles méthodes. Le troisième verrou scientifique est de connaître les a priori utiles pour un attaquant lorsqu'il souhaite compromettre un système biométrique embarqué sur un élément sécurisé.

Objectifs & contributions

Les objectifs de cette thèse sont de proposer une contribution à l'évaluation des systèmes biométriques embarqués sur des éléments sécurisés. Cet enjeu est important car les données biométriques sont sensibles et non révocables. Le fait d'utiliser un élément sécurisé permet de protéger ces données, c'est pourquoi les SE sont le plus couramment utilisés. Pour ce faire, nous proposons :

— Une plateforme d'évaluation de systèmes biométriques embarqués sur SE. La plateforme nous permet, d'effectuer des campagnes d'acquisition d'empreintes digitales avec un panel d'utilisateurs ou de fausses empreintes (spoofing, doigt mort,...). Des empreintes digitales synthétiques (générées par un logiciel) peuvent être également utilisées. Il s'agit aussi d'effectuer des analyses sécuritaires ainsi que d'évaluer les performances du système biométrique.
— Une contribution à l'authentification biométrique en proposant des méthodes de réduction de template biométrique pour qu'ils soient stockés sur un élément sécurisé. L'évaluation de cette réduction est effectuée grâce à la plateforme nous permettant ainsi de pouvoir comparer les méthodes entre elles.
— Des tests sécuritaires sur l'élément sécurisé et ainsi connaître les éléments importants pour un imposteur lui permettant d'attaquer efficacement un tel système biométrique.

1.3 Organisation du manuscrit

Le manuscrit est organisé en cinq chapitres ayant pour objectifs de présenter le contexte de cette thèse, puis les différentes contributions autour de la biométrie embarquée sur élément sécurisé, pour finir par une conclusion sur les travaux effectués ainsi qu'une présentation de différentes perspectives sur ce sujet.

Le manuscrit est articulé de la façon suivante :

— **Le chapitre 2** positionne le contexte en définissant les notions les plus importantes pour mieux appréhender les contributions de la thèse ;

— **Le chapitre 3** fait un état des lieux des différentes plateformes d'évaluation de systèmes biométriques existantes. Notre première contribution est une nouvelle plateforme d'évaluation (appelée EVABIO) plus générique que celles existantes. Les principaux avantages d'EVABIO sont mis en évidence au travers de trois illustrations d'utilisation de la plateforme. Cette plateforme est utilisée dans les différents travaux de cette thèse ;

— **Le chapitre 4** propose des méthodes permettant de réduire la taille d'un template biométrique de minuties pour être stocké sur un élément sécurisé tout en préservant les performances du système. Dans ce chapitre, différentes méthodes sont utilisées, celle de l'état de l'art ainsi que des évolutions de ces dernières, puis des méthodes plus évoluées comme celle basée sur la triangulation de Delaunay ou l'utilisation d'un algorithme génétique ;

— **Le chapitre 5** présente quant à lui des attaques que nous pouvons effectuer sur un système biométrique. Dans une première partie, nous nous intéressons plus spécifiquement aux informations importantes pour un attaquant. Par la suite, nous proposons une méthode permettant de reconnaître le type d'empreinte digitale à partir du template de minuties sans avoir accès à l'image et sans reconstruction de cette dernière. Ceci permet d'envisager une contre mesure à des attaques par force brute ;

Enfin, nous concluons ce manuscrit et donnons quelques perspectives.

Chapitre 2

Positionnement du problème

Ce chapitre présente quelques généralités sur la biométrie permettant ainsi d'avoir un aperçu des différentes modalités. Ensuite, une présentation des différentes méthodes d'évaluation d'un système biométrique sont présentées afin d'en appréhender le fonctionnement. Une présentation du fonctionnement d'un élément sécurisé est également réalisée.

Sommaire

2.1 Généralités

Depuis l'Antiquité, la biométrie est utilisée pour identifier un individu. En effet, dès 3000 avant J-C, les historiens ont trouvé des traces d'échanges commerciaux babyloniens utilisant les empreintes digitales pour la transaction de biens, en office de signature. Cela a également été mis en évidence en Chine au 7ème siècle.

Ce n'est qu'au cours du 17ème siècle, et plus particulièrement avec la découverte de la couche basale de l'épiderme par Marcello Malpighi, que les premiers travaux ont été réalisés sur les empreintes digitales. Cependant, c'est le botaniste et anthropologiste

Nehemiah Grew, qui fut le premier à décrire les dermatoglyphes, plis et crêtes épidermiques du doigt. Ses travaux furent poursuivis par Jan Evangelista, qui a découvert neuf formes élémentaires d'empreintes digitales. Cette classification est très proche de celle utilisée aujourd'hui.

Sir Francis Galton, physicien anglais réputé, réalisa des recherches sur les mensurations des hommes, tels que la taille, le poids et d'autres caractéristiques à des fins de statistiques. Il déduit de ces travaux que les figures cutanées, formant les empreintes digitales, sont le moyen d'identification le plus performant, le plus sûr et avec la marge d'erreur la plus faible. Dans sa thèse *Fingerprint* [1], il présente ses études étalées sur dix ans montrant que les empreintes digitales sont propres à chaque humain, qu'elles sont uniques et permanentes. Il estime la probabilité que deux humains aient les mêmes empreintes digitales à 1 chance sur 64 milliards. Suite aux travaux menés par Sir Francis Galton, William James Herschel a été le premier européen à scientifiquement démontrer que les empreintes digitales sont uniques et persistantes tout au long de la vie, ce qu'il put prouver en enregistrant ses empreintes digitales régulièrement au cours de son existence.

Ce fut ensuite un grand criminologue français, Alphonse Bertillon, qui contribua fortement au développement de la biométrie. C'est lorsqu'il fréquenta l'école de Médecine de Clermont Ferrand, qu'il entreprit des réflexions au sujet de l'anthropométrie, ayant pour objectif d'utiliser cette science dans l'identification de criminels par la police. Il y parviendra plus tard et ses découvertes furent rassemblées dans ce que l'on appelle le système Bertillon, qui fut expérimenté pour la première fois en 1882. Ce système permet d'avoir les mensurations osseuses de différentes parties du corps (taille, envergure, longueur du tronc) et des différents caractères propres à chaque individu comme les cicatrices ou la couleur des yeux. La figure 2.1 montre les informations permettant de créer cette fiche d'identification. C'est Edwards Henry qui popularisa et généralisa l'utilisation de la dactyloscopie (empreintes digitales) dans la criminologie durant le 20ème siècle. Ainsi, à son apogée, le système Bertillon fut utilisé par des organisations de sécurité parmi les plus importantes au monde, comme celle de la sécurité intérieure des USA. Cependant, le système Bertillon se révéla imprécis, et facilement contournable. Une simple opération chirurgicale ou un accident pouvaient en effet mettre en défaut le système.

Le Bertillonage fut aussi victime de l'expansion de l'informatique. Le système informatisé garantissant une meilleure sécurité, et ses données se révélant quasi-infalsifiables. De plus, le traitement des données est largement plus rapide. Il est cependant concurrencé par le profil ADN. Par la suite, des produits ont été commercialisés au début des années 1980 avec l'informatisation des empreintes digitales.

FIGURE 2.1 – Exemple de fiche d'identification du système Bertillon (extrait de [2]).

Ces dernières sont omniprésentes dans les systèmes de sécurité actuels. Prenons l'exemple des passeports biométriques, qui ont été introduits suite aux attentats du 11 Septembre 2001 par les différents gouvernements et influencés par les États-Unis. Maintenant, plus de 15 ans après l'introduction massive de la biométrie, cette dernière suscite toujours autant d'intérêt de la part des industriels qui souhaitent toujours bénéficier de nouvelles méthodes d'identification d'un individu. Dans notre quotidien, nous avons vu apparaître de nouveaux usages à base de biométrie que ce soit pour du contrôle d'accès physique, du contrôle aux frontières, pour déverrouiller son smartphone et plus récemment pour du paiement. La figure 2.2 montre quelques exemples d'utilisation de la biométrie actuellement.

Une information biométrique est une donnée personnelle sensible car non révocable en général (impossible de la changer comme un mot de passe). Afin de protéger une donnée biométrique, elle peut être stockée dans un élément sécurisé comme une puce à microcircuit. Il est généralement possible de réaliser la vérification d'identité d'un individu en comparant une donnée biométrique capturée avec celle stockée dans l'élément sécurisé. Ce processus de comparaison est communément nommé OCC (On-Card-Comparison).

Nous présentons dans un premier temps des généralités sur la biométrie, ensuite nous montrons comment on évalue un système biométrique. Nous présentons très succinctement les éléments sécurisés servant de support aux systèmes biométriques considérés tout au long de cette thèse.

FIGURE 2.2 – Exemples d'identification biométrique de nos jours.

2.2 La biométrie

D'après la définition du Larousse, la biométrie est « La science visant à identifier ou vérifier l'identité d'un individu à partir de caractéristiques morphologiques ou comportementales » [3].

2.2.1 Modalités

Il existe trois grandes familles de modalités biométriques permettant de vérifier ou déterminer l'identité d'un individu : (1) les modalités biologiques , (2) comportementales et (3) morphologiques.

1. Les modalités biologiques consistent en l'analyse de *données biologiques* liées à une personne, par exemple l'analyse ADN [4, 5], l'odeur [6], les signaux physiologiques [7, 8, 9].
2. Les modalités comportementales analysent les comportements d'un individu comme par exemple la dynamique de signature [10, 11], la dynamique de frappe au clavier [12, 13, 14, 15], la façon de marcher [16, 17] ou encore, la manière d'utiliser son téléphone portable [18].
3. Les modalités morphologiques consistent à identifier les traits physiques particuliers d'un individu, qui sont uniques et permanents tels que les empreintes

digitales [19, 20, 21], le visage [22, 23], la forme de la main [24, 25], l'iris [26, 27, 28].

La Figure 2.3 présente une illustration de quelques modalités biométriques.

FIGURE 2.3 – illustration de quelques modalités biométriques.

2.2.1.1 Les caractéristiques biométriques

Une modalité biométrique est considérée comme intéressante et exploitable, si la donnée biométrique utilisée satisfait différentes propriétés qui permettent d'obtenir des performances non négligeables [29] et respectant les caractéristiques suivantes [30] :

- Universalité : toutes les personnes à identifier doivent la posséder ;
- Unicité : l'information doit être aussi dissimilaire que possible entre les différentes personnes ;
- Permanence : l'information collectée doit être présente pendant toute la vie d'un individu ;
- Collectabilité : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons ;
- Acceptabilité : le système doit respecter certains critères (facilité d'acquisition, rapidité, etc.) afin d'être employé.

Modalité	*Univ*	*Unic*	*Perm*	*Coll*	*Acce*	*Perf*
Modalités biologiques						
ADN	Oui	Oui	Oui	Faible	Faible	⋆⋆⋆⋆⋆
Groupe sanguin	Oui	Non	Oui	Faible	Oui	⋆
Modalités comportementales						
Démarche	Oui	Non	Faible	Oui	Oui	⋆⋆⋆
Dynamique de frappe	Oui	Oui	Faible	Oui	Oui	⋆⋆⋆
Voix	Oui	Oui	Faible	Oui	Oui	⋆⋆⋆⋆
Modalités morphologiques						
Iris	Oui	Oui	Oui	Oui	Faible	⋆⋆⋆⋆⋆
Rétine	Oui	Oui	Oui	Oui	Faible	⋆⋆⋆⋆⋆
Visage	Oui	Non	Faible	Oui	Oui	⋆⋆⋆⋆
Géométrie de la main	Oui	Non	Oui	Oui	Oui	⋆⋆⋆⋆
Veines de la main	Oui	Oui	Oui	Oui	Oui	⋆⋆⋆⋆⋆
Oreille	Oui	Oui	Oui	Oui	Oui	⋆⋆⋆⋆⋆
Empreinte digitale	Oui	Oui	Oui	Oui	Oui	⋆⋆⋆⋆

TABLE 2.1 – Comparaison des modalités biométriques selon les propriétés suivantes : (Univ) universalité, (Unic) Unicité, (Perm) Permanence, (Coll) Collectabilité, (Acce) Acceptabilité, (Perf) Performance. Pour la performance, le nombre d'étoiles est lié à la valeur du taux d'égale erreur (EER) obtenu dans l'état de l'art (extrait de [31]).

Les caractéristiques biométriques ne possèdent pas toutes ces propriétés, ou à des degrés différents. Le tableau 2.1 extrait de [31], compare les principales modalités biométriques selon les caractéristiques précédemment décrites (universalité, unicité, performance, collectabilité, acceptabilité) et en ajoutant un critère de performance. Ce tableau montre qu'aucune caractéristique n'est idéale et qu'elles peuvent être plus ou moins adaptées à des applications particulières. Par exemple, l'analyse basée sur l'ADN est une des techniques les plus efficaces pour vérifier l'identité d'un individu ou l'identifier [32]. Néanmoins, elle ne peut pas être utilisée pour le contrôle d'accès logique ou physique pour des raisons de temps de calcul, mais aussi a fortiori parce qu'aucune personne ne serait prête à donner un peu de sang pour se faire authentifier sur un système. Le choix de la modalité est ainsi effectué selon un compromis entre la présence ou l'absence de certaines propriétés selon les besoins de chaque application. Il est important de noter que le choix de la modalité biométrique peut aussi dépendre de la culture locale de l'utilisateur.

2.2.1.2 Les modèles biométriques

Un modèle biométrique autrement appelé gabarit ou template, correspond à l'ensemble des données utilisées pour représenter un utilisateur. Lors de la phase d'ac-

quisition des données biométriques celles-ci ne sont pas enregistrées et utilisées telles quelles. Une phase de traitement est effectuée pour réduire les données biométriques brutes et ainsi produire un modèle biométrique réduit contenant des caractéristiques. La figure 2.4 illustre quelques exemples de modèles biométriques. Ces modèles peuvent être stockés à différents emplacements, comme par exemple une clé USB, une base de données centralisée, sur le capteur lui même ou dans un élément sécurisé (SE). Chacun de ces emplacements présente des avantages et des inconvénients en termes de temps de traitement, de confidentialité et de respect de la vie privée. En France, la Commission Nationale Informatique et Libertés (CNIL) proscrit l'utilisation des bases de données centralisées pour un nombre élevé d'individus [33].

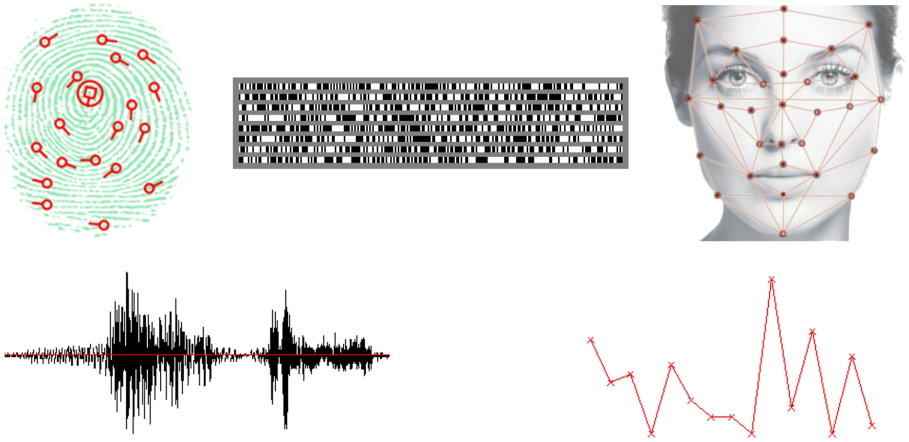


FIGURE 2.4 – Exemples de quelques modèles biométriques, avec de gauche à droite : minuties extraites d'une empreinte digitale, code d'un iris, graphe utilisant les points d'intérêt du visage, signal vocal et signaux de la dynamique de frappe au clavier.

2.2.1.3 Cadre d'utilisation

Nous pouvons observer deux types de systèmes biométriques différents proposés par Jain [29] permettant (1) l'*identification*, ou la (2) *vérification*. Ces deux types de systèmes s'appuient sur un troisième procédé (3) l'*enrôlement* permettant d'enregistrer un individu dans le système.

1. L'*identification* permet de reconnaître un individu à partir d'une donnée biométrique parmi l'ensemble des utilisateurs du système. Il s'agit d'une vérification de type "1 contre n", où l'utilisateur n'a pas besoin de fournir son identité. Le système retourne l'identité de l'individu identifié, ou une liste

d'individus potentiels, ou le rejette s'il ne correspond à aucun utilisateur du système ;

2. La *vérification* permet de vérifier si l'identité de l'individu est bien celle qu'il prétend être. Cette fois-ci, le système compare la donnée biométrique acquise avec le modèle biométrique correspondant stocké. Il s'agit d'une comparaison de type "1 contre 1". Le système retourne alors la décision d'acceptation ou de rejet de l'utilisateur ;
3. L'*enrôlement* est la première phase de tout système biométrique. Il s'agit de la toute première étape pendant laquelle un utilisateur est enregistré dans le système biométrique pour la première fois. Cette étape est commune à l'identification et à la vérification. Pendant l'enrôlement, une représentation numérique est extraite à partir de la donnée provenant d'un capteur biométrique. Cette représentation est ensuite réduite, en utilisant un algorithme d'extraction dépendant de la modalité, afin de réduire la quantité de données à stocker, et ainsi faciliter la vérification et l'identification. Suivant l'application ainsi que le niveau de sécurité, le modèle biométrique est stocké soit dans une base de données centrale soit sur un élément personnel propre à chaque individu de type SE ;

2.2.2 Système biométrique

L'architecture d'un système biométrique est normalisée et définie par la norme ISO/IEC 19795-1 [34]. Elle se compose de cinq modules comme le montre la figure 2.5 :

— Le **module de capture** consiste à acquérir des données biométriques afin d'extraire des représentations numériques. Cette représentation est ensuite utilisée pour l'enrôlement, la vérification et l'identification. Le capteur biométrique peut être de type avec ou sans contact ;
— Le **module de traitement du signal** permet de réduire la représentation numérique extraite afin d'optimiser la quantité de données à stocker lors de la phase d'enrôlement, ou pour faciliter le temps de traitement pendant la phase de vérification ou d'identification. Ce module peut avoir un test de qualité pour contrôler les données biométriques acquises ;
— Le **module de stockage** contient les modèles biométriques des utilisateurs enrôlés du système. La plupart du temps il s'agit d'une base de données centrale, mais ce module peut être inclus dans un SE pour une vérification ;
— Le **module de similarité** compare quant à lui les données biométriques extraites par le module d'extraction des caractéristiques à un ou plusieurs

modèles préalablement enregistrés. Ce module détermine ainsi le degré de similarité (ou de divergence) entre deux vecteurs biométriques ;

— Le **module de décision** détermine à partir du ou des scores de comparaison si la preuve d'identité est acceptée (mode vérification) ou la liste de candidats potentiels (mode identification).

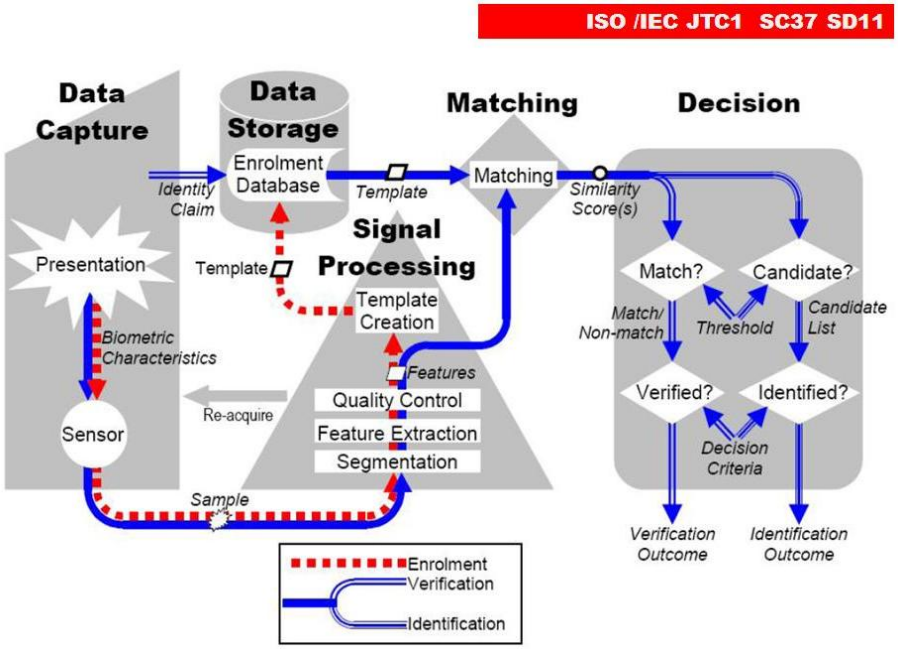


FIGURE 2.5 – Architecture générique d'un système biométrique (extrait de l'Organisation Internationale de Normalisation ISO/IEC 19795-1 [34]).

2.2.3 Les limitations des systèmes biométriques

Les systèmes biométriques ont de nombreux avantages en comparaison des systèmes d'authentification traditionnels (facilité d'usage, lien étroit entre l'authentifiant et l'individu, attaque plus complexe ...). Cependant, leur utilisation a très souvent été limitée à des applications spécifiques comme le passeport biométrique ou le contrôle d'accès à des zones sensibles. Néanmoins, depuis plusieurs années, l'authentification biométrique commence à se démocratiser avec l'arrivée des smartphones possédant des lecteurs d'empreinte digitale, permettant de déverrouiller son téléphone ainsi que de pouvoir effectuer un paiement. Ces systèmes souffrent cependant de plusieurs limitations pouvant dégrader considérablement leurs intérêts.

La première limitation se situe dans la performance. Contrairement aux systèmes classiques d'authentification, tel que le code Pin, les mots de passe, qui eux donnent

une réponse de type vrai ou faux, ceux basés sur la biométrie donnent un pourcentage de similarité lors d'une comparaison. Par exemple, le pourcentage de similarité est compris entre 0% et 100%, le 100% n'étant quasiment jamais atteint. Cette différence est due à plusieurs facteurs : la variabilité lors de la capture (*i.e.*, bruit d'acquisition, caractéristiques du capteur utilisé, *etc.*), la variabilité intra-classe (variabilité des données pour un même individu) et la similarité inter-classe (*i.e.*, similarité des données biométriques de plusieurs individus comme des jumeaux par exemple).

Une autre limitation de la biométrie est l'usage qui en est fait ainsi que la culture des individus qui l'utilisent. Par exemple, l'ADN qui est de plus en plus utilisé pour des affaires judiciaires, pour l'identification de criminels pose des problèmes d'usage. Suivant la modalité utilisée, l'acquisition de données biométriques est effectuée avec ou sans contact par le capteur. Ce contact est une source d'inquiétude et éventuellement de stress pour certains utilisateurs pour des raisons d'hygiène ou de perception. Prenons l'exemple de la reconnaissance par la rétine, cette technologie assure une très bonne fiabilité et une haute barrière contre la fraude. Malgré les avantages de cette technologie, elle est considérée comme intrusive par les utilisateurs, c'est pourquoi elle est très peu utilisée. L'utilisation de la biométrie présente également des risques en termes de respect des droits et des libertés fondamentales. En France, la CNIL, n'autorise que les applications utilisant des biométries à traces (*i.e.*, les empreintes digitales) que lorsque la base de données est chiffrée et non centralisée.

Enfin, les systèmes biométriques sont vulnérables à des attaques spécifiques. Ratha *et al.* [35] présente huit emplacements de points de compromission d'un système biométrique. Même s'il est plus difficile de falsifier un iris que de déchiffrer un mot de passe, il est possible d'attaquer un système biométrique. Les travaux présentés dans [36] montrent la facilité de reproduire des empreintes digitales en utilisant des images résiduelles sur le capteur.

2.2.4 Le cas des systèmes à base d'OCC

Le cadre applicatif des travaux menés durant cette thèse concerne un système biométrique embarqué sur un SE, pour vérifier l'identité d'un individu. Ce système est de type OCC, ce qui signifie que le stockage, la comparaison et la prise de décision sont effectués directement sur le SE, comme le montre la figure 2.6. Dans cette thèse, nous nous focalisons sur l'empreinte digitale. Dans notre cas, le template biométrique est basé sur les minuties de celle-ci. La comparaison est réalisée par comparaison de template de minuties directement sur le SE, et en général en moins de 500 ms.

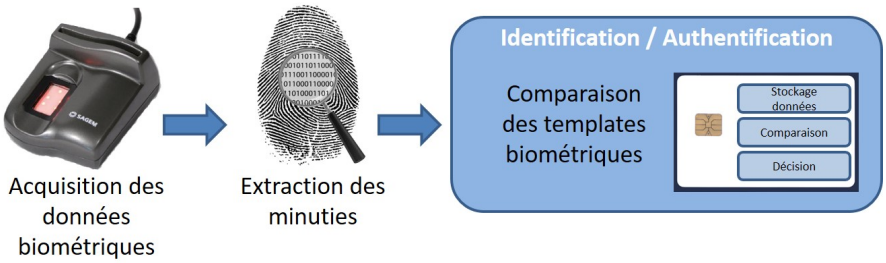


FIGURE 2.6 – Architecture d'un système biométrique embarqué sur SE basé sur l'empreinte digitale.

2.3 Élément sécurisé

Une brève présentation sur l'élément sécurisé est donnée ici, puisque nous l'utilisons comme support du système biométrique tout au long de cette thèse. Certaines notions sont donc nécessaires pour bien comprendre le fonctionnement d'un SE comme une carte à puce à microcircuit. Différentes spécifications et normes sont utiles pour communiquer avec une puce à microcircuit. Nous présentons aussi les limitations d'un SE d'un point de vue mémoire et capacité de calcul.

Un élément de sécurité ou « Secure Element » (SE) est une plateforme « inviolable » capable de stocker une ou plusieurs applications en toute sécurité ainsi que les données cryptographiques et confidentielles associées. Le SE contrôle les interactions entre les sources de confiance (émetteur de puce à microcircuit comme un établissement financier), l'application de confiance (*i.e.*, une application de paiement, ou d'authentification biométrique) stockée dans une zone sécurisée du SE et des tiers (*i.e.*, un commerçant pour le paiement et le système Parafe [37] pour le contrôle aux frontières). Le domaine de sécurité protège les informations échangées lors d'une communication entre le terminal et la carte en créant un canal sécurisé. La figure 2.7 montre une vue éclatée d'une carte à puce à microcircuit.

FIGURE 2.7 – Vue éclatée sur un SE de type carte à puce.

Il existe différents types de SE suivant l'utilisation de ce dernier. Les trois plus couramment utilisés sont :

— le SE pour mobile : Universal Integreted Circuit Card (UICC) sur les cartes SIM ;
— le SE embarqué dans une enclave sécuritaire d'un SmartPhone ;
— le SE sous forme de microSD pour des utilisations externalisées.

Ces SEs stockent actuellement de nombreuses applications de confiance dans un environnement sécurisé. D'un point du vue logiciel, les SEs sont très souvent basés sur des systèmes d'exploitation ouverts comme JavaCard [38] et répondant aux spécifications GlobalPlatform [39] pour le chargement d'applications et la communication sécurisée entre un terminal et le SE.

2.3.1 Protocoles et spécifications

Dans cette partie, nous allons présenter les différentes normes et spécifications qui sont utiles pour communiquer avec un SE. La figure 2.8 résume les différentes strates constituant un SE de type JavaCard. Chaque strate sera succinctement détaillée pour donner quelques principes et interactions.

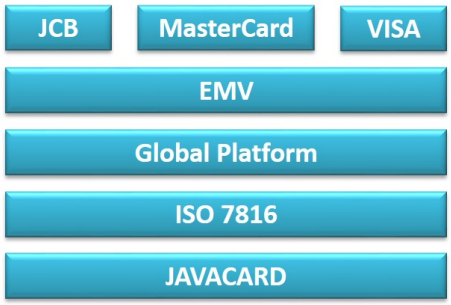


FIGURE 2.8 – les différentes strates composant un SE.

2.3.1.1 JavaCard

JavaCard est un environnement d'exécution destiné aux puces à microcircuit permettant d'écrire et d'exécuter des programmes appelé Applet avec l'approche orientée objet du Java. JavaCard a été crée par des ingénieurs de Schlumberger. Ainsi en 1997, avec Gemplus, ils fondent Java Card Forum [40]. Des fabricants de puces à microcircuit, tels que Bull ou Giesecked & Devrient viendront ensuite les rejoindre. Les principaux avantages de cet environnement sont la facilité de développement,

l'interopérabilité des applications, l'isolation entre celles-ci, la sécurité, l'indépendance au hardware et la gestion de multiples applications.

2.3.1.2 ISO7816

La norme ISO 7816 [41] permet de définir un SE de type carte à puce, elle se décompose en quatre parties :

1. 7816-1 : précise les caractéristiques physiques de la carte ;
2. 7816-2 : définit la position et le brochage des contacts de la carte à puce ;
3. 7816-3 : définit les niveaux électriques et les chronogrammes de bas niveau qui régissent le dialogue avec les cartes à puce ;
4. 7816-4 : indique les différentes commandes pour communiquer avec une puce à microcircuit.

Nous utilisons dans cette thèse essentiellement la norme 7816-4 qui nous permet d'avoir des échanges "Application Protocol Data Unit" (APDU) entre un logiciel ou terminal avec une carte à puce. Les données échangées au niveau applicatif à partir d'un terminal vers une carte à puce sont appelées commandes APDU (C-APDU). A l'inverse, les données échangées à partir de la carte à puce vers le terminal sont les réponses APDU (R-APDU). Durant tous les échanges, la carte prendra le rôle d'esclave, c'est-à-dire qu'elle ne sait que répondre à une commande APDU, elle ne peut pas initier un dialogue, elle se contente de répondre. La figure 2.9 montre une communication entre un terminal de type Terminal de paiement électronique (TPE) et une carte. Comme nous pouvons le remarquer, une commande envoyée par le terminal est obligatoirement suivie d'une réponse de la carte.

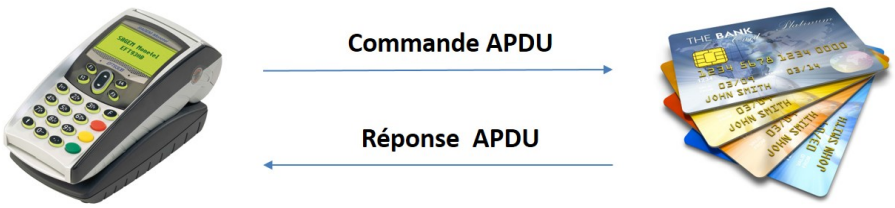


FIGURE 2.9 – Communication entre un TPE et une carte bancaire (couple commande/réponse APDU).

Sur la figure 2.10, nous pouvons observer la structure d'une commande et d'une réponse APDU d'après la norme ISO/IEC 7816 [41]. Nous n'allons pas détailler chaque champ ici, mais pour simplifier, les octets [CLA,INS,P1,P2] constituent l'entête de la commande permettant à la carte de savoir ce que souhaite obtenir le terminal. Les octets [LC,UDC] sont utilisés si des données sont transmises à la carte

et l'octet [LE] permet de dire à la carte le nombre d'octets que l'on souhaite en réponse. Les trois derniers champs [LC,UDC,LE] sont optionnels. Si le champ [LE] est présent dans la C-APDU, la R-APDU contiendra un [UDR] contenant [LE] données, ainsi que deux mots d'états nommés "Status Word" [SW1,SW2], définissant le statut de traitement de la commande par la carte.

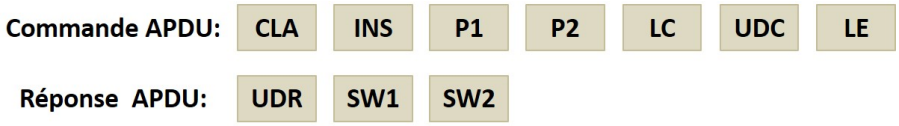


FIGURE 2.10 – Structure d'une commande et réponse APDU lors d'une communication.

2.3.1.3 Global Platform

GlobalPlarform [39] est un consortium créé en 1999 par les grandes entreprises des secteurs du paiement et des télécommunications ainsi que les structures gouvernementales. L'infrastructure globale est destinée à l'implémentation des cartes à puce commune à tous les secteurs. Les spécifications GlobalPlatform visent à gérer les cartes de façon indépendante du matériel, des vendeurs et des applications. Elles répondent efficacement aux problématiques de la gestion multi-applicatives : chargement sécurisé des applications, gestion du contenu et cycle de vie, comme le montre la figure 2.11. Cette spécification, permet d'avoir des outils permettant de sécuriser la communication entre un logiciel ou terminal avec une carte. Cela permet aussi de faire cohabiter une application biométrique et d'autres applications comme le paiement par exemple sur un même SE.

2.3.1.4 EMV

Europay Mastercard Visa (EMV) est un ensemble de spécifications pour la sécurité des paiements par cartes à puce. C'est l'organisme EMVco, composé de Mastercard, Visa, JCB et American Express, qui s'occupe de ce standard. Les points importants de ces spécifications sont l'interopérabilité internationale, la vérification et déchiffrement de la clé personnelle (PIN) par la puce. Précisons toutefois qu'EMV couvre la transaction à partir de l'émetteur jusqu'au terminal en passant par l'acquéreur. Les spécifications EMV [42] sont constituées de quatre livres disponibles librement en ligne. L'EMV offre depuis 2016 la possibilité d'utiliser la biométrie comme moyen d'authentification (en remplacement du code PIN) dans une transaction bancaire.

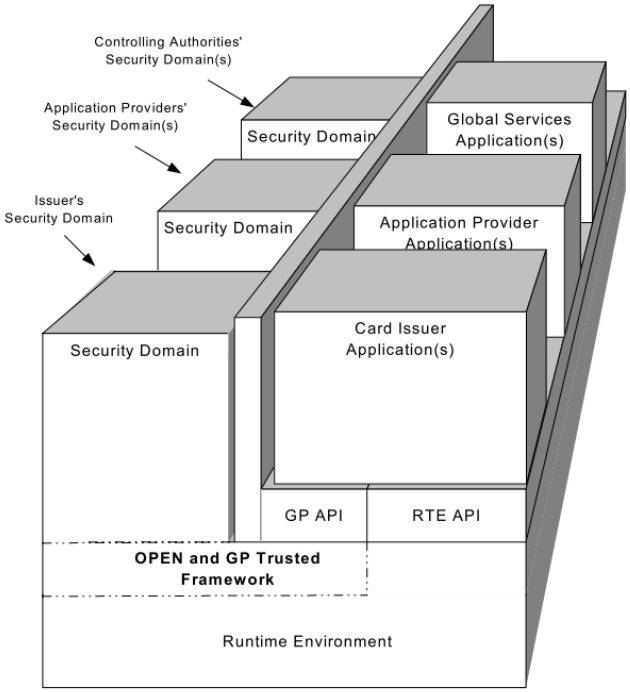


FIGURE 2.11 – Architecture d'une carte Global Platform (source : GlobalPlatform).

2.3.2 Limitations des SE

Les SE ayant une taille très réduite, le micro-processeur permet d'exécuter l'environnement d'exécution JavaCard, la communication ISO 7816, ainsi que les différentes sur-couches GlobalPlatform, EMV, Visa, MasterCard, JCB et CB. Le micro-processeur a cependant une capacité de calcul limité, c'est pourquoi certains SE ont un crypto-processeur pour effectuer toutes les opérations cryptographiques demandées lors d'une transaction bancaire. En ce qui concerne la mémoire, le SE a une capacité très faible en comparaison à un ordinateur, seulement quelques kilo-octets de mémoire sécurisée [43]. Cela limite les données que l'on peut stocker sur ce dernier. Une donnée biométrique nécessite un stockage de plusieurs dizaines de kilo-octets (pour une empreinte digitale d'environ 60 minuties). L'ISO Compact Card II [44] a été proposé pour stocker de façon efficace une empreinte digitale pour un SE.

2.4 L'empreinte digitale sur élément sécurisé

Le cas d'étude de cette thèse concerne la modalité biométrique de l'empreinte digitale embarquée sur un élément sécurisé. Étant donné que les données biométriques

extraites d'un capteur sont trop volumineuses pour être stockées sur un élément sécurisé, il convient d'extraire des minuties. Les minuties sont des représentations des points caractéristiques de l'empreinte digitale, qui sont stockées sur l'élément sécurisé.

2.4.1 Les minuties

Une image d'empreinte digitale de bonne qualité nécessite environ 100ko de stockage, c'est avec ce type d'image que nous avons les meilleurs taux de reconnaissance d'un individu sur un système biométrique. Plutôt que de travailler sur une image de plusieurs milliers de pixels, l'idée est de rechercher des points caractéristiques de l'empreinte digitale et ainsi diminuer la dimension de l'espace de recherche. Des techniques d'extractions permettent d'obtenir à partir de l'image, des points caractéristiques que l'on appelle des minuties. Il existe différents types de points caractéristiques qui sont définis par Galton [45] et illustrés par la figure 2.12. Ces minuties garantissent l'unicité d'une empreinte digitale. Les minuties sont des caractéristiques locales qui se produisent à chaque bifurcation ou fin de crêtes (voir la figure 2.12). Sur la figure 2.12, nous pouvons observer les types de minuties suivants :

— Point de fin (Endings) : le point de fin de la crête ;
— Bifurcation : le point à partir duquel la crête se sépare en deux ;
— Point (Dot) : très petite crête ;
— Ile (Island) : crête un peu plus longue qu'un point, occupant un espace intermédiaire entre deux crêtes temporairement divergentes ;
— Etang ou lac (Ponds ou Lake) : espace vide entre deux crêtes temporairement divergentes ;
— Crochet (Hook ou Spurs) : Un crochet provenant d'une crête ;
— Pont (Bridge) : petites crêtes joignant deux longues crêtes adjacentes ;
— Croisement (Crossover) : deux crêtes qui se croisent ;
— Le point Core : Le point intérieur, normalement au milieu de l'empreinte, autour duquel les spirales, les boucles, ou les arches sont centrés. Il correspond au point de courbure maximale des crêtes de l'empreinte digitale.
— Le point Delta : Le point, normalement en bas à gauche ou à droite de l'empreinte digitale suivant la main, autour duquel une série de triangle de crête est centrée.

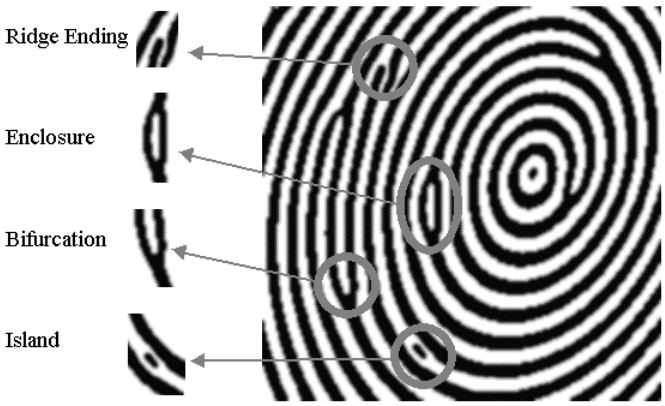


FIGURE 2.12 – Quelques types de minuties que l'on peut trouver dans une empreinte digitale, tiré de [46]

2.4.2 Standard ISO Compact Card II

Le standard ISO Compact Card II [47] permet de garantir l'interopérabilité entre les systèmes biométriques. Il est très souvent utilisé pour créer un template biométrique d'empreinte digitale et ainsi permettre de le stocker sur un SE. Ce template est composé d'un ensemble de minuties représenté par 3 octets et 4 valeurs $(x_i, y_i, T_i, \theta_i),\ i = 1 : N_j$ où les coordonnées (x_i, y_i) correspondent à la localisation de la minutie dans l'image, T_i correspond au type de minutie tel que présenté en section 2.4.1, θ_i l'orientation de la minutie (relative à la crête) et N_j le nombre de minuties pour l'échantillon j de l'utilisateur comme le montre la figure 2.13.

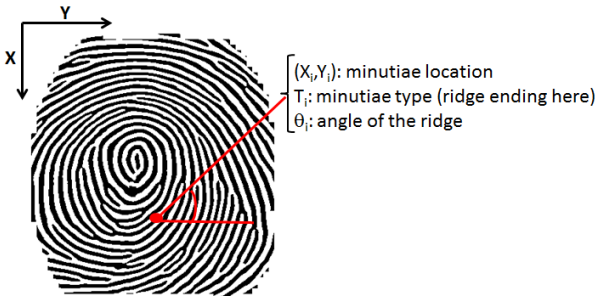


FIGURE 2.13 – Description d'un template de minutie d'une empreinte digitale

Ce format de stockage des minuties est utilisé pour tous les travaux décrits dans ce manuscrit, aussi bien pour l'évaluation des systèmes biométriques embarqués sur SE, que pour la réduction de template biométrique ou les attaques sur les éléments sécurisés. La prochaine section définit les différents aspects de l'évaluation d'un système biométrique.

2.4.3 Algorithmes de comparaison embarqués sur SE

Le système de vérification d'identité est basé sur la comparaison de deux templates de minuties, correspondant respectivement au doigt de la personne enrôlée (template de référence) et au doigt de la personne à tester (template de test). Pour déterminer si les deux templates de minuties correspondent à un même individu, il est nécessaire d'adopter un algorithme de comparaison qui soit robuste à d'éventuelles translations, rotations et déformations qui affectent systématiquement les empreintes digitales. À partir de ces deux templates de minuties, le système est capable de donner un indice de similarité ou de correspondance qui varie de :

— 0% si les empreintes sont extrêmement différentes

— à 100% si les empreintes sont identiques.

Deux templates de minuties extraits à partir de la même empreinte ne donneront jamais 100% de correspondance du fait des différences qui existent lors de l'acquisition des deux images, ils donneront cependant toujours un niveau élevé de similarité (supérieur ou égale à 95%).

Un seuil d'acceptation (ou de décision) permet, à partir de l'indice de similarité, de savoir si deux empreintes sont issues du même doigt ou non. Si l'indice de similarité est supérieur au seuil d'acceptation, la correspondance est avérée ; dans le cas contraire les empreintes digitales ne proviennent pas du même individu.

2.5 Évaluation des systèmes biométriques

L'évaluation des systèmes biométriques est un enjeu majeur pour plusieurs raisons. Premièrement, elle permet d'offrir aux chercheurs et industriels une méthodologie de test et de comparaison avec les systèmes de l'état de l'art. Deuxièmement, elle permet de prendre en considération le comportement des utilisateurs durant le processus d'évaluation, permettant ainsi d'avoir une meilleure compréhension de leurs besoins et ainsi de mieux déployer cette technologie dans la vie quotidienne. Enfin, elle permet d'identifier, pour chaque système, les applications industrielles en se basant sur divers critères tels que la performance, la qualité, la sécurité et l'usage (comme illustré dans la figure 2.14) :

1. **La performance** mesure l'efficacité d'un système biométrique en terme d'erreur tel que le taux d'erreur égale (EER) [34] ;
2. **La qualité** mesure la qualité des données biométriques acquises [48, 49, 50] ;
3. **La sécurité** mesure la résistance d'un système biométrique (capteur et algorithmes) aux attaques [51] ;

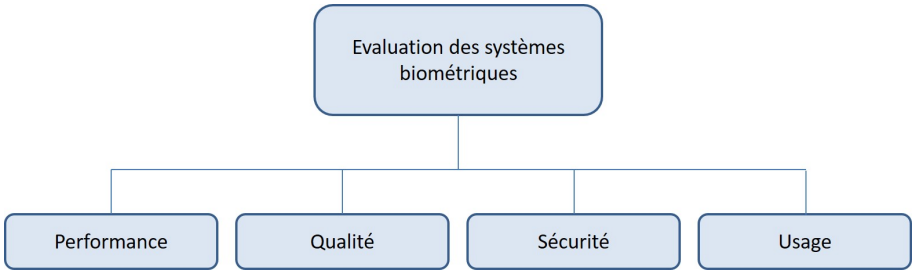


FIGURE 2.14 – Aspects de l'évaluation des systèmes biométriques

4. **L'usage** mesure l'acceptabilité et la satisfaction des utilisateurs lors de l'utilisation du système biométrique [52].

Nous détaillons chacun de ces points par la suite.

2.5.1 Performance

La performance mesure l'efficacité et la fiabilité d'un système biométrique dans un contexte d'utilisation donné. Pour quantifier la performance d'un système biométrique, plusieurs critères existent dans la littérature [53, 54, 34, 55] permettant d'estimer les mesures des taux d'erreurs, les mesures liées au temps de traitement et occupation mémoire, les courbes de performance ainsi que les points de fonctionnement associés.

2.5.1.1 Mesure des taux d'erreurs

L'Organisation Internationale de Normalisation (ISO) a défini la norme ISO/IEC 19795-1 [34] permettant de diviser les mesures de taux d'erreurs en trois classes, les taux d'erreur fondamentales, les taux d'erreur de systèmes d'authentification et les taux d'erreur de systèmes d'identification.

1. Taux d'erreur fondamentale

— Taux d'échec à l'acquisition (*failure-to-acquire rate*, FTA) : proportion des tentatives de vérification ou d'identification pour lesquels le système biométrique n'a pas pu acquérir l'information biométrique requise ;
— Taux d'échec à l'enrôlement (*failure-to-enroll rate*, FTE) : proportion des individus pour lesquels le système n'a pas pu générer le modèle biométrique durant la phase d'enrôlement. Prenons par exemple le cas des empreintes digitales, il existe certaines personnes qui n'ont pas d'empreintes digitales pour des raisons génétiques, ou des empreintes quasi-inexistantes pour des raisons médicales ou très abimées de par leur profession ;

— Taux de fausses non correspondances (*false-non-match rate*, FNMR) : proportion de faux rejets par l'algorithme de comparaison entre la donnée biométrique acquise et le modèle correspondant ;
— Taux de fausses correspondances (*false match rate*, FMR) : proportion de fausse acceptation par l'algorithme de comparaison entre la donnée biométrique acquise et le modèle correspondant à un autre individu.

2. Taux d'erreurs de systèmes d'authentification

— Taux de faux rejets (*false rejection rate*, FRR, spécifique à la vérification) : proportion des transactions des demandeurs légitimes rejetées par erreur. Pour une transaction de vérification à une seule tentative et un seuil fixé à τ (τ dépendant de l'algorithme de comparaison), le taux de faux rejets est calculé comme suit :

$$FRR(\tau) = FTA + FNMR(\tau) * (1 - FTA) \tag{2.1}$$

— Taux de fausses acceptations (*false acceptance rate*, FAR, spécifique à la vérification) : proportion des transactions des imposteurs acceptées à tort. Pour une transaction de vérification à une seule tentative et un seuil fixé à τ, le taux de fausses acceptations est calculé par :

$$FAR(\tau) = FMR(\tau) * (1 - FTA) \tag{2.2}$$

Les deux taux d'erreurs, FAR et FRR, sont liés et dépendent d'un seuil de décision qui est fixé en fonction du niveau de sécurité (haut ou bas) du système biométrique. La figure 2.15 nous donne la distribution théorique des taux de vraisemblance des utilisateurs légitimes et des imposteurs. Comme nous pouvons le constater, plus le seuil fixé sera bas, plus le taux de fausses acceptations sera élevé. Ce qui veut dire que le système biométrique acceptera des imposteurs. À l'inverse, plus le seuil est élevé plus le taux de fausses acceptations est bas. Le système biométrique sera dans ce cas robuste aux imposteurs mais rejettera beaucoup plus d'utilisateurs légitimes.

3. Taux d'erreur de systèmes d'identification

— Taux d'identification (*identification rate*, IR) : ce taux correspond à la proportion de transactions d'identification d'utilisateurs enrôlés dans le système, pour lesquels l'identifiant de l'utilisateur est présent dans les identifiants retournés ;
— Taux de faux-négatif d'identification (*fasle-negative identification-error rate*, FNIR) : proportion de transactions d'identification par des utilisateurs enrôlés

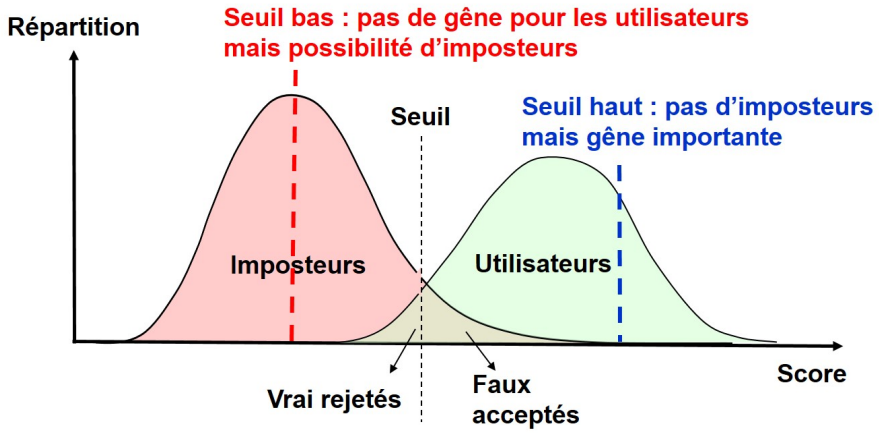


FIGURE 2.15 – Représentation du taux de vraisemblance d'utilisateurs légitimes ainsi que d'imposteurs sur un système d'authentification biométrique (dont le système de comparaison est basé sur un calcul de similarité) (extrait de [56]).

dans le système, pour lesquels l'identification de l'utilisateur ne figure pas dans la liste des identifiants retournée par le système.
Exemple : Pour une transaction d'identification à une seule tentative contre une base de données contenant N modèles, le taux de faux-négatif d'identification est calculé par :

$$FNIR(\tau) = FTA + (1 - FTA) * FNRT(\tau) \tag{2.3}$$

— Taux de faux-positif d'identification (*false-positive identification-rate*, FPIR) : proportion de transactions d'identification, par des utilisateurs non enrôlés dans le système, pour lesquels la liste des identifiants retournée est non vide.
Exemple : Pour une transaction d'identification à une seule tentative contre une base de données contenant N modèles, le taux de faux-positifs d'identification est calculé par :

$$FPIR = (1 - FTA) * (1 - (1 - FMR)^N) \tag{2.4}$$

— Erreur de l'algorithme de présélection (*pre-selection error*) : L'algorithme de présélection permet de réduire le nombre de modèles biométriques à comparer avec l'image acquise durant la phase d'identification. L'erreur se produit quand le modèle correspondant à la donnée biométrique acquise ne figure pas dans la liste des modèles retournés ;
— Taux de pénétration (*penetration rate*, PR) : mesure, en moyenne, le nombre de modèles biométriques pré-sélectionnés par rapport au nombre total de modèles.

2.5.1.2 Mesure des temps de traitement et occupation mémoire

Lors de l'évaluation de systèmes biométriques, le temps de traitement de l'information par le système, est un facteur très important. Il se compose généralement de trois temps :

- Temps moyen d'enrôlement : désigne le temps moyen pour générer les modèles biométriques des individus ;
- Temps moyen de vérification : désigne le temps moyen pour l'acquisition des données biométriques requises et la comparaison de ces données avec le modèle correspondant. Ce temps ne dépend pas du nombre de personnes dans la base de données ;
- Temps moyen d'identification : désigne le temps moyen pour l'acquisition des données biométriques requises et la comparaison de ces données avec les modèles existants dans la base. Le nombre d'utilisateurs du système a un impact très important sur cette information. Il peut être conséquent pour de grandes bases, comme par exemple la base *Aadhaar* [57] comptant à terme 1,2 milliard d'individus Indiens.

Un autre facteur important à prendre en considération lors de l'évaluation des systèmes biométriques est l'espace mémoire requis par le système. Il est principalement mesuré en *taille moyenne et maximale d'un modèle biométrique* mais aussi en *espace mémoire maximal alloué* pendant les phases d'enrôlement, de vérification et d'identification. Il faut aussi prendre en compte, par exemple, le temps de vérification d'empreintes digitales sur un SE qui est limité à 500 ms.

2.5.1.3 Les courbes de performance

La performance d'un système biométrique pour différents seuils de décision est illustrée graphiquement en utilisant des courbes spécifiques. Nous avons :

- Courbe CMC (*Cumulative Match Characteristic curve*) : Cette courbe est utilisée pour comparer la performance de systèmes d'identification biométrique. En abscisse, on trouve les valeurs des rangs d'identification et en ordonnée les probabilités d'une identification correcte ;
- Courbe RC (*Robustness Curve*) : cette courbe permet d'illustrer la robustesse du système biométrique en terme de performance face à diverses altérations comme par exemple le bruit sur une image lors de l'acquisition de données biométriques ;
- Courbe ROC (Receiver Operating Characteristic curve)[53] : cette courbe est l'une des méthodes les plus utilisées afin d'évaluer la performance globale

d'un système d'authentification biométrique. La courbe ROC représente la relation entre le taux de fausses acceptations (FAR) et le taux de faux rejets (FRR) pour différentes valeurs de seuil de décision. Le terme DET (*détection d'erreur Tradeoff*) est alors utilisé, dans ce cas le terme ROC est réservé à la représentation du taux de vrais rejets (1-FRR) au taux de fausses acceptations (FAR). La figure 2.16 illustre la représentation d'une courbe ROC. Le principal avantage de cette unique courbe est que l'on obtient une représentation compacte de la performance d'un système biométrique, ce qui permet de comparer objectivement différents systèmes biométriques.

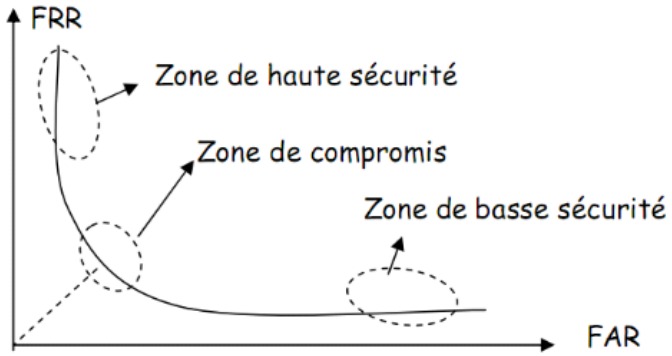


FIGURE 2.16 – Exemple de courbe ROC : Variation du FRR en fonction du FAR lorsque le seuil de décision varie.

2.5.1.4 Les points de performance

Les points de performance sont utilisés pour représenter la performance des systèmes biométriques. Dans la littérature, plusieurs métriques [34, 55] existent tel que le taux d'égale erreur (EER), le taux d'erreur pondéré (WER), le taux d'erreur moyenne (HTER), l'aire sous la courbe ROC (AUC) et la capacité. Dans la suite, seuls l'EER et l'AUC seront présentés car nous les utilisons tout au long de cette thèse.

— Taux d'égale erreur (*Equal Error Rate*, EER) : L'EER est obtenu à partir de la courbe ROC lorsque le FAR = FRR (*cf.*, figure 2.16). Cette valeur constitue le point de compromis entre la zone de haute sécurité et la zone de faible sécurité. L'EER permet d'avoir une unique valeur pour représenter la performance d'un système biométrique. De plus, ce taux d'erreur est le plus communément utilisé dans la littérature.

— Aire sous la courbe ROC (*Area Under Curve*, AUC) : cette métrique permet de quantifier la diversification de la distribution de score des utilisateurs légitimes ainsi que des imposteurs. Plusieurs méthodes permettent d'estimer l'AUC

et ont été proposées dans [58] ainsi que par Tronci *et al.* [59] se basant sur des tests statistiques de Wilconox-Mann-Whitney (WMW) [60] pour estimer l'AUC. Celle-ci est également un bon indicateur pour évaluer et comparer des systèmes biométriques. Plus la valeur de l'AUC est petite, plus l'algorithme de comparaison est performant.

2.5.1.5 Intervalle de confiance

Lorsque l'on souhaite évaluer la performance de systèmes biométriques, nous utilisons des bases de données collectées. Ces dernières ne sont cependant pas représentatives de la population globale. Ces bases ne sont qu'un sous-ensemble d'une population, souvent elles contiennent peu de personnes et surtout peu d'échantillons par personne. Lors de l'évaluation, il y a souvent une différence entre le nombre de scores des utilisateurs légitimes et imposteurs, ce qui n'est pas représentatif de la réalité. Cela est dû au découpage de la base de données (enrôlement-test) utilisé pour calculer la performance du système globale. Le fait de découper la base a aussi un impact sur les taux d'erreur EER et AUC car seul un sous-échantillon de la base de données est utilisé. Pour toutes ces raisons, il est nécessaire de calculer un intervalle de confiance à l'EER lors de la comparaison des systèmes biométriques. Cet intervalle de confiance est surtout indispensable lorsque les taux d'erreurs entre des systèmes biométriques sont similaires, cela permet d'avoir une précision supplémentaire.

Une méthode permettant d'estimer l'intervalle de confiance associé aux taux d'erreurs FAR et FRR utilise une méthode dite de *bootstrap* ayant été introduite par Bolle *et al.* [61]. Cette méthode permet de faire de l'inférence statistique avec un tirage aléatoire avec remise de M éléments de la base de données de test. Nous effectuons k tirages aléatoires de $M = N_i$ scores pour le FRR et $M = N_j$ scores pour le FAR, ce qui nous permet d'avoir une estimation du $FRR(\tau)$, $FAR(\tau)$ pour une valeur de seuil τ et ainsi une estimation de l'EER_k. Comme il a été démontré par Allano [62], 1000 tirages (k=1000) sont suffisants.

D'après la loi des grands nombres, lorsque k tend vers l'infini, la variable à estimer, dans notre cas l'EER, tend vers une variable normale. L'intervalle de confiance (IC) peut ainsi être déterminé grâce aux percentiles de la distribution normale. L'intervalle de confiance à 95% est défini par l'équation 2.5 :

$$IC = EER \pm 1.96 \times \frac{\sigma}{\sqrt{k}} \tag{2.5}$$

où l'EER est le taux d'erreur global estimé sur l'échantillon initial, k est le nombre de tirages, et σ la variance des k taux d'erreurs calculés sur les k différents tirages. L'intervalle de confiance représente ainsi une mesure de confiance sur le taux d'erreur estimé. Plus l'intervalle de confiance est petit, et plus le taux d'erreur calculé est significatif.

2.5.2 Qualité

La qualité des données biométriques est importante car c'est à partir de ces données que l'extraction des caractéristiques est effectuée. Suivant la qualité d'une image d'empreinte digitale, si la qualité est faible, des artefacts d'acquisition peuvent apparaître et ainsi perturber l'algorithme d'extraction des minuties. L'extracteur peut ainsi trouver des minuties non présentes dans l'image originale. Si nous prenons l'exemple de l'empreinte digitale, la qualité d'image de l'empreinte varie suivant plusieurs facteurs :

- la saleté des doigts ;
- niveau d'humidité ou d'assèchement ;
- aspect dégradé comme des coupures, entailles ;
- la pression exercée sur le capteur biométrique joue sur les détails à extraire de cette donnée.

Pour qu'un système biométrique soit efficace contre divers types de bruit d'acquisition, le contrôle de la qualité des données acquises est indispensable. Il a été montré par Alonso-Fernandez *et al.* [63] l'impact d'une mauvaise qualité d'image sur les performances globales des systèmes biométriques. Différentes méthodes existent pour mesurer la qualité d'empreintes digitales [64, 65, 66], mais la plus connue d'entre elles est la métrique NFIQ (Nist Fingerprint Image Quality) du NIST proposée par Tabassi et Wilson [67]. Cette métrique donne une classe de qualité d'image allant de 1 pour une qualité excellente à 5 pour une image de mauvaise qualité. Le principe de NFIQ est donné dans la figure 2.17.

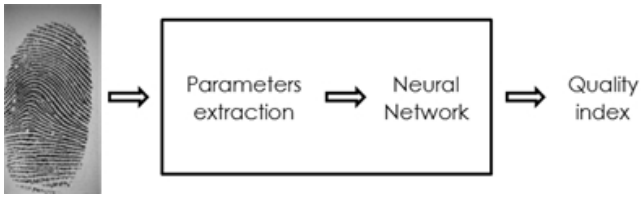


FIGURE 2.17 – Principe de fonctionnement de la métrique NFIQ (extrait de [49]).

En avril 2016, le NIST à proposé sa nouvelle métrique de qualité NFIQ 2 [68], qui retourne toujours une classe de qualité d'image allant de 1 à 5 comme pour NFIQ. Le principe de NFIQ 2 est illustré dans la figure 2.18.

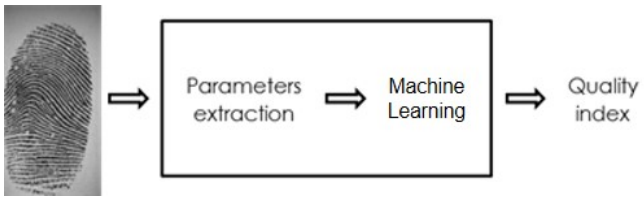


FIGURE 2.18 – Principe de fonctionnement de la métrique NFIQ 2.

Une autre métrique, développée dans le cadre de la thèse de Zhigang Yao au sein de l'équipe, nommée Q permet d'estimer la qualité d'une empreinte digitale a été proposée dans [49] et propose de meilleurs résultats que ceux obtenus avec NFIQ. Cette métrique Q est basée sur une combinaison de 11 critères de qualités d'empreinte digitale. 10 d'entre eux sont extraits de l'empreinte digitale (dont le nombre de minuties, ...) et le dernier sur la fusion des scores. La métrique Q donne une valeur variant de 0 à 100, sachant que la meilleure qualité d'image est représentée par la valeur 100. La figure 2.19 donne le principe de la métrique.

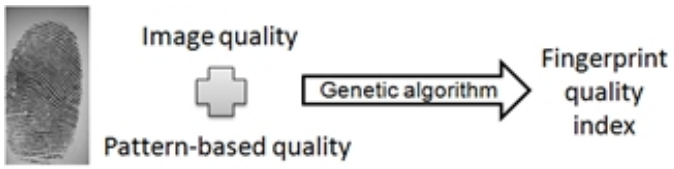


FIGURE 2.19 – Principe de fonctionnement de la métrique Q (extrait de [49]).

2.5.3 Sécurité

Les systèmes biométriques sont de plus en plus utilisés dans de nombreuses applications, pour améliorer la sécurité d'accès à des ressources physiques et logiques. Malgré les avantages de ces systèmes par rapport aux systèmes d'authentification traditionnels, ils sont toujours vulnérables à des attaques spécifiques qui peuvent dégrader considérablement leur fonctionnalité. Dans la littérature, différents travaux montrent la vulnérabilité des systèmes biométriques.

Ratha *et al.* [35] ont regroupé les attaques sur un système biométrique générique en 8 classes. Jain *et al.* [69] ont mis à jour le schéma en donnant des indications sur

les types d'attaques possibles. La figure 2.20 illustre les emplacements possibles de ces attaques dans un système biométrique générique :

Classe 1 Données biométriques falsifiées : une reproduction de la donnée biométrique utilisée sera présentée au capteur biométrique (comme la présentation d'une copie d'une signature) ;

Classe 2 Transmission de données biométriques interceptées : une ancienne donnée biométrique enregistrée est rejouée dans le système sans passer par le capteur biométrique (comme la présentation d'une ancienne copie de l'image de l'empreinte) ;

Classe 3 Attaque sur le module d'extraction de paramètres : ce module pourrait être remplacé par un cheval de Troie de manière à produire des informations choisies par l'attaquant ;

Classe 4 Altération de paramètres extraits : après l'obtention de données par le module d'extraction de paramètres, ceux-ci sont altérés voire remplacés par d'autres données définies par l'attaquant ;

Classe 5 Le module de calcul de similarité est remplacé par un module malveillant : ce module pourrait être remplacé par un cheval de Troie afin de produire artificiellement de hauts ou bas scores ;

Classe 6 Altération de la base de données : la base de modèles biométriques est disponible localement, à distance ou distribuée sur plusieurs serveurs. Dans ce type d'attaque, l'attaquant modifie un ou plusieurs modèles afin d'autoriser un imposteur (usurpation d'identité) voire d'empêcher un utilisateur légitime d'y accéder (déni de service) ;

Classe 7 Attaque sur le canal entre la base de données et le module de calcul de similarité : dans ce type d'attaque, les modèles sont altérés sur le lien de transmission reliant la base de modèles et le module de calcul de similarité ;

Classe 8 Altération des décisions (accepté ou rejeté) : ce type d'attaque altère la décision booléenne (oui ou non) pris par le module de calcul de similarité. La dangerosité de cette attaque est élevée puisque même si le système est robuste en terme de performance, il a été rendu inutile par ce type d'attaque.

2.5.4 Usage

L'usage d'un système biométrique est un élément très important, car l'interaction homme-machine n'est pas toujours intuitive surtout pour les utilisateurs inexpérimentés. Comme cela a été proposé dans [56] ainsi que dans [70, 71], il faut prendre

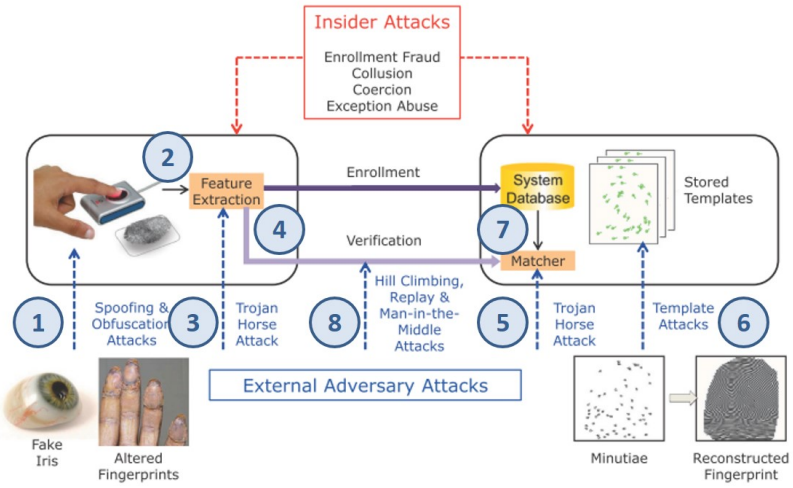


FIGURE 2.20 – Emplacement des points de compromission d'un système biométrique (extrait de [35, 69]).

en compte lors du développement du système biométrique l'interaction des individus avec le capteur. Les auteurs sont d'accord sur le fait que l'absence de cette étude entraînera une dégradation de la performance des systèmes biométriques tels que le taux d'échec à l'enrôlement (FTE), le taux d'échec à l'acquisition (FTA) ainsi que le taux de faux rejets (FRR). La complexité de conception d'un système biométrique a été représentée sur trois axes par Jain *et al.* : la performance en terme d'erreurs (FTE, FTA, EER, ...), l'usage en terme d'acceptabilité et la sécurité en terme de robustesse contre la fraude. La figure 2.21 nous montre la représentation de cette complexité. Actuellement, la majorité des systèmes ne sont évalués que sur l'un de ces trois axes, la performance, mais il ne faut pas négliger les deux autres axes (Usage et Sécurité). Si l'on prend en compte ces trois axes cela permet d'une part, d'augmenter l'acceptabilité des usagers, surtout pour des applications destinées au grand public, et d'autre part d'améliorer les performances en terme d'erreurs (FTA, FTE, ERR) [72].

Plusieurs enquêtes ont été effectuées [73, 74, 75, 52, 76, 56] montrant l'intérêt de la biométrie pour différents cas d'usage comme le contrôle aux frontières avec l'utilisation de passeports biométriques. Selon ces études, certaines modalités sont considérées comme intrusives, comme l'utilisation de l'iris ou de l'ADN. Cependant, bien que l'ADN soit considérée comme une des méthodes les plus fiables, elle n'est pas utilisée pour du contrôle d'accès physique ou logique car considéré comme trop intrusif par les usagers. Le stockage des données biométriques est souvent source d'inquiétude pour les usagers, ces dernières sont non révocables et les usagers craignent le non-respect de leur vie privée ainsi qu'une mauvaise utilisation de leurs données

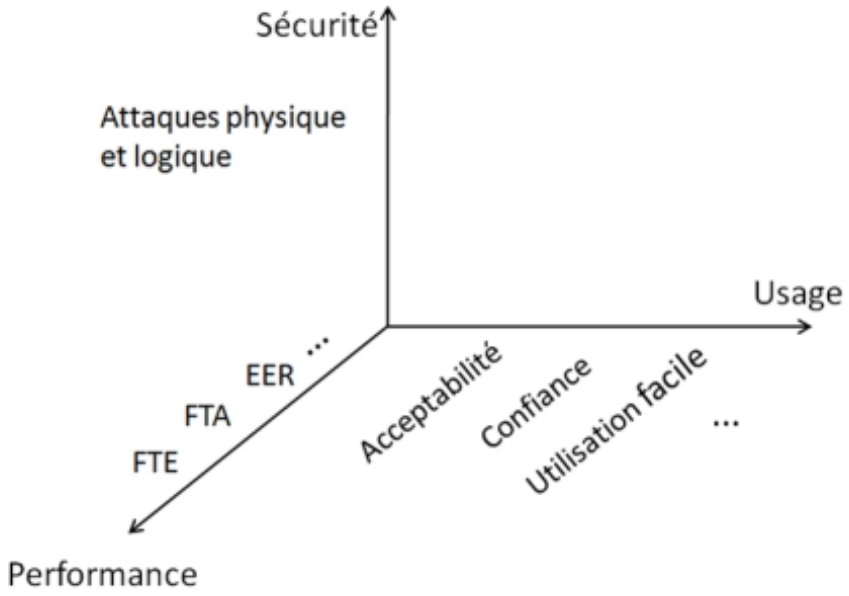


FIGURE 2.21 – Conception d'un système biométrique : performance, usage et sécurité (extrait de [71]).

biométriques.

2.6 Conclusion

Dans ce premier chapitre, après une introduction générale sur la biométrie ainsi que ses propriétés, nous avons fait une présentation des méthodes existantes permettant d'évaluer des systèmes biométriques. Ces méthodes peuvent être décomposées suivant quatre aspects que sont la performance en terme de taux d'erreur, la qualité des données acquises, l'usage en terme d'acceptabilité et la sécurité en terme de robustesse contre la fraude. Nous avons vu qu'il existe un grand nombre de métriques statistiques mises en place pour évaluer la performance des systèmes biométriques. Cependant, le processus biométrique est réalisé par une interaction homme-machine grâce à un capteur et a un impact majeur sur la performance globale du système, comme le montre l'état de l'art. Nous avons également vu que les systèmes biométriques sont vulnérables à des attaques spécifiques, qui peuvent considérablement dégrader le fonctionnement du système ainsi que l'utilité. Ces systèmes présentent également des soucis en terme de respect de la vie privée, de stockage ainsi que d'une mauvaise utilisation des données personnelles.

Le cadre applicatif de cette thèse est l'utilisation de l'empreinte digitale avec un élément sécurisé. L'empreinte digitale fait partie des modalités les plus utilisées et étudiées en biométrie. De nombreux travaux portent essentiellement sur les images des empreintes digitales. Nos contributions se focalisent sur les templates de minuties, nous considérons avoir aucun accès à l'image originale, qui vont être stockés sur un élément sécurisé. Nous souhaitons pouvoir évaluer un système biométrique utilisant un élément sécurisé de type carte à puce. Majoritairement, nous n'avons pas d'accès au code des algorithmes embarqués sur ces éléments sécurisés, c'est pourquoi nous devons effectuer des évaluations dite en *Boite Noire*, c'est-à-dire lorsque l'implémentation du système n'est pas connu et seul le résultat de la décision est disponible lors d'une vérification biométrique.

Dans le prochain chapitre, nous présentons une première contribution de cette thèse concernant la conception d'une plateforme d'évaluation d'un systèmes biométrique. Cette plateforme sera le support des contributions suivantes portant sur la réduction de template de minuties pour le stockage sur carte à puce et sur les attaques de systèmes biométriques par l'utilisation d'a priori sur l'empreinte digitale.

Chapitre 3

Plateforme d'évaluation de systèmes biométriques

Ce chapitre décrit une plateforme d'évaluation de systèmes d'une manière générale, en quoi cela est utile dans notre problématique lié à la biométrie. Une présentation des différentes plateformes d'évaluation de systèmes biométriques dans la littérature est réalisée ainsi qu'une comparaison de leurs différentes fonctionnalités. Une nouvelle plateforme est proposée pour répondre aux différents manques, elle va nous servir de support pour tous les travaux effectués durant cette thèse.

Sommaire

La première question que l'on se pose est : « qu'est-ce qu'une plateforme ? » D'après son étymologie une plateforme repose toujours, quelque soit le domaine, sur la notion de soutien voir même de fondation.

Si l'on regarde à travers le prisme de l'informatique, une plateforme est une base de travail à partir de laquelle on peut écrire, lire, développer et utiliser un ensemble de logiciels [77]. Une plateforme informatique peut être composée de matériels (processeurs,...), d'un système d'exploitation (Windows, Mac OS X, Linux,...), d'outils logiciels et/ou de développement (bibliothèque logicielle, API, framework, base de

données, serveur web / d'applications).

Il existe deux grands types de plateformes liés au domaine de l'informatique et des sciences appliquées :

1. les plateformes matérielles qui sont généralement conçues, développées, construites, mises en service et maintenues par des sociétés informatiques, ou des prestataires de services ;
2. les plateformes logicielles qui, quant à elles, sont plutôt développées et maintenues par des organismes (CNRS, INRIA, CEA, INRA) qui hébergent la base de travail et les logiciels associés.

Dans cette étude, ce sont les plateformes logicielles qui vont nous intéresser, car notre problématique se porte sur l'évaluation de systèmes biométriques embarqués sur des éléments sécurisés. Nous attendons d'une telle plateforme qu'elle puisse répondre à certaines caractéristiques primordiales :

— **Reproductibilité des résultats** : cet enjeu est le plus important car il permet de garantir qu'avec les mêmes scénarii de tests, nous obtenons les mêmes résultats. La traçabilité des résultats y compris intermédiaires est primordiale pour une plateforme d'évaluation et encore plus pour pouvoir effectuer des certifications.
— **Plateforme générique** : Cette plateforme doit permettre l'évaluation de systèmes utilisant tout type de modalité biométrique comme les empreintes digitales, la dynamique de frappe au clavier mais aussi la voix ;
— **Modularité (plugin)** : cet enjeu est important car cela permet à la plateforme de pouvoir évoluer sans avoir à tout reconstruire à chaque fois, voire de faire évoluer un module indépendamment du reste de la plateforme ;
— **Métriques de performance** : permet la visualisation des résultats de l'évaluation sur les critères définis par l'ISO de manière automatique ;
— **Métriques de qualité** : cela permet de faire des filtrages ou sélections des données biométriques à utiliser suivant les scénarii choisis. C'est un enjeu important car cela permet d'avoir des options supplémentaires lors d'une évaluation.
— **Scénarii d'évaluation** : les scénarii sont très liés à la reproductibilité des résultats, car ils permettent par exemple de toujours effectuer les mêmes tests. Plutôt que de faire évoluer un scénario, on en crée un nouveau avec une nouvelle référence.

— **Capteurs (choix / acquisition)** : la plateforme doit permettre de s'interfacer avec différents capteurs biométriques. Cet enjeu est important car il permet de pouvoir faire des sessions d'acquisition mais aussi de pouvoir comparer des capteurs entre eux suivant un ou plusieurs scénarii.
— **Analyse boîte noire** : c'est essentiel qu'une plateforme d'évaluation permette de faire des analyses en boîte noire (sans avoir accès au code source du système à tester), car peu d'industriels souhaitent donner accès à leurs codes sources contrairement aux chercheurs.
— **Attaques** : nous souhaitons que la plateforme offre la possibilité de faire des attaques sur un capteur, un algorithme de comparaison (OCC) pour mesurer l'impact de ces attaques sur le système biométrique global.
— **Cartes à puce (SE)** : notre contexte d'utilisation de la biométrie se basant sur un élément sécurisé (SE), nous souhaitons que la plateforme permette de communiquer avec des SEs.

Ces caractéristiques vont permettre de comparer, dans la section suivante, les plateformes existantes dédiées à l'évaluation des systèmes biométriques présentes dans l'état de l'art et, le cas échéant, de pouvoir sélectionner la plus adaptée à notre étude.

3.1 État de l'art

Dans la littérature, peu de plateformes existent pour l'évaluation de la performance et la sécurité des systèmes biométriques. Les plus importantes sont présentées dans la suite du manuscrit.

3.1.1 Projet MISTRAL

Le projet MISTRAL [78] s'appuie sur le projet TECHNOLANGUE AGILE/ALIZE [79] et s'est terminé en janvier 2005 (figure 3.1). Cette plateforme logicielle Open-Source est spécialisée dans l'authentification biométrique. Un des objectifs de cette plateforme est de faciliter l'accès aux technologies biométriques au monde académique (centre de recherche et d'enseignement) comme au monde industriel en fournissant une plateforme logicielle performante et modulaire. L'originalité majeure de la plateforme MISTRAL, sur le plan technologique, est de mettre en place un moteur de reconnaissance unique pour différentes modalités, essentiellement voix et visage. La plateforme offre un environnement distribué et embarqué comme les smartphones et

environnements perceptifs (« smart-rooms ») permettant des applications de sécurisation d'espace (salles de réunions, halls publics,...). L'utilisation d'un moteur de reconnaissance unique, quelle que soit la modalité visée, offre de nombreux avantages. Cela permet en premier lieu de concentrer les efforts de recherche et développement sur les aspects spécifiques de la modalité étudiée plutôt que sur le développement et le suivi de différents moteurs de reconnaissance. Il devient alors plus facile d'intégrer de nouvelles modalités en s'appuyant sur le savoir-faire acquis sur des modalités déjà étudiées. Par ailleurs, il permet d'optimiser les efforts de développement mais également de faciliter l'intégration des techniques biométriques dans des démonstrateurs ou des produits. Enfin, cette caractéristique unique facilite grandement la fusion des différentes modalités pour renforcer la sécurité et la sûreté des systèmes ou pour améliorer leur ergonomie. Ce moteur est basé sur une approche statistique, largement éprouvée pour la voix.

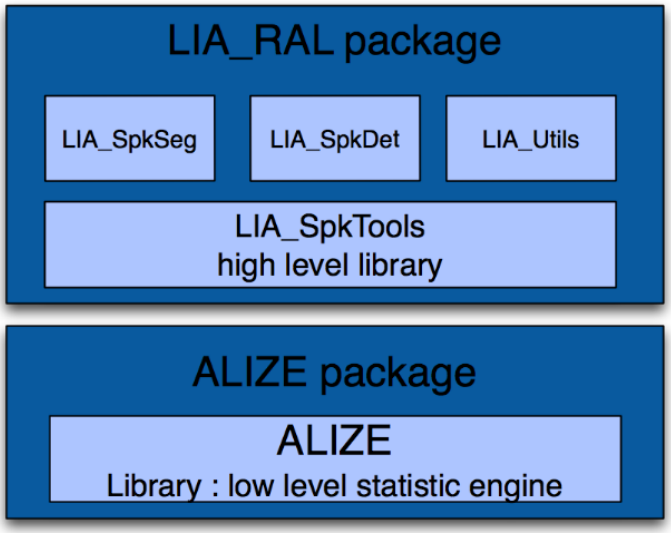


FIGURE 3.1 – Base logicielle de MISTRAL provenant d'ALIZE (Extrait de [79])

3.1.2 Plateforme Minex II

La plateforme du NIST Minex II [80] est utilisée dans de nombreuses compétitions de recherche. Elle permet aux chercheurs ainsi qu'aux entreprises, de tester leurs algorithmes de comparaison embarqués sur un SE ainsi que leurs extracteurs de minuties, en terme d'intéropérabilité. Les rapports d'évaluation du NIST donnent des informations sur le FMR (taux de fausse acceptation) et le FNMR (taux de faux rejets) pour chaque algorithme de comparaison et extracteur. Le but de cette plateforme est de faire comparer les algorithmes ou systèmes existants par un tiers

de confiance (le NIST en l'occurrence). Une mise à jour a été réalisée en 2015 avec Minex III [81]. Cette version permet d'avoir une évaluation sur une base de données plus importante et d'avoir des informations plus détaillées sur les résultats. La figure 3.2 montre un exemple de résultats d'évaluation pour différents fabriquants, seules les informations les plus importantes y sont présentes comme le taux de FNMR pour les générateurs de templates et les algorithmes de comparaison. Pour les entreprises présentes dans ce tableau, un rapport complet permet d'avoir des informations plus précises sur l'évaluation.

Top Template Generators

Organization	Code	Pooled 2 Fingers FNMR@ FMR≤10^{-2}	Native 1 Finger FNMR@ FMR≤10^{-4}	Completion Date
AA Technology Ltd.	aatec+0201	0.00039	0.0119	11/16/2015
id3 Technologies	id3tech+1250	0.00041	0.0163	02/24/2016
Innovatrics	innovatrics+0017	0.00044	0.0096	06/09/2016
AA Technology Ltd.	aatec+0300	0.00048	0.0127	03/14/2016
Neurotechnology	Neurotechnology+0105	0.00056	0.0146	08/24/2015
Neurotechnology	Neurotechnology+0106	0.00066	0.0116	07/20/2016

Top Template Matchers

Organization	Code	Pooled 2 Fingers FNMR@ FMR≤10^{-2}	Native 1 Finger FNMR@ FMR≤10^{-4}	Completion Date
Innovatrics	innovatrics+0017	0.00024	0.0096	06/09/2016
Neurotechnology	Neurotechnology+0106	0.00026	0.0116	07/20/2016
Neurotechnology	Neurotechnology+0105	0.00040	0.0146	08/24/2015
AA Technology Ltd.	aatec+0300	0.00127	0.0127	03/14/2016
AA Technology Ltd.	aatec+0201	0.00132	0.0119	11/16/2015
id3 Technologies	id3tech+1250	0.00173	0.0163	02/24/2016

FIGURE 3.2 – Exemple de résultats d'évaluation (Extrait de [82])

3.1.3 FVC-OnGoing

La plateforme FVC-OnGoing [83] est dédiée à la vérification des algorithmes de comparaison d'empreintes digitales (évolution de la compétition FVC). La plateforme offre de nombreuses bases de données regroupées en deux parties. La première intitulée "Vérification d'empreintes" quantifie à la fois le module d'enrôlement et

de vérification, tandis que la seconde "comparateur d'empreintes au format ISO" quantifie seulement le module de vérification sur des templates ISO [47] basés sur les minuties. Les métriques de performance sont : le taux de non-acquisition (FTA), le taux de non-enrôlement (FTE), le taux de faux rejets (FNMR) pour un taux de fausse acceptation (FMR) donné et vice versa, le temps moyen de l'enrôlement et la vérification, la taille maximale du template biométrique acceptée par le SE, la distribution des scores des utilisateurs légitimes et des imposteurs et la courbe ROC avec son taux d'erreur égale (EER). La figure 3.3 schématise les différentes interactions possibles avec la plateforme ainsi que les possibilités offertes. Nous remarquons que l'évaluation est très fortement supervisée.

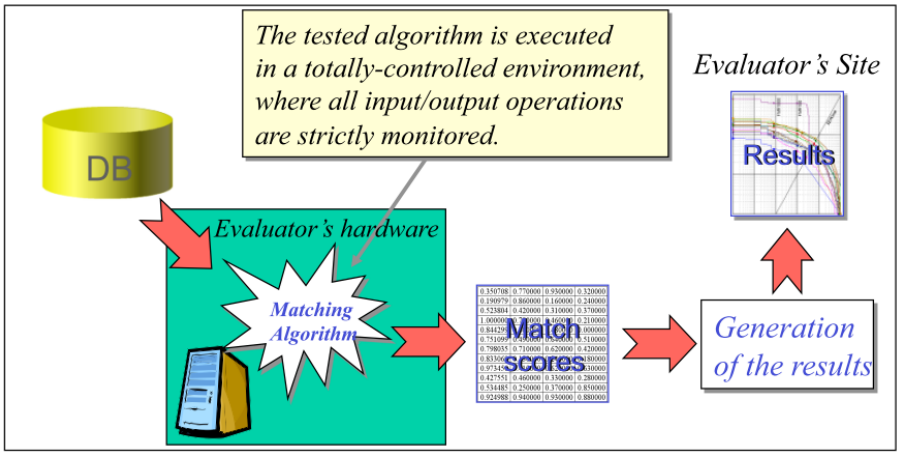


FIGURE 3.3 – Schéma de la plateforme FVC-onGoing (Extrait de [84])

3.1.4 BEAT

Une plateforme est actuellement en développement avec le projet européen BEAT (Biometric Evaluation And Testing) [85]. À la fin de ce projet, un framework sera proposé qui évaluera les performances des technologies biométriques utilisant plusieurs métriques et critères comme la performance, les vulnérabilités, le respect de la vie privée. La figure 3.4, nous montre comment l'utilisateur crée son scénario d'évaluation avec des blocs. Cette conception permet une modularité et l'ajout de fonctionnalités dans le temps. Le but de ce projet est de fournir une plateforme commune aussi bien pour les industriels que pour les chercheurs permettant ainsi d'évaluer leurs produits et avoir une certification indépendante avec des critères communs.

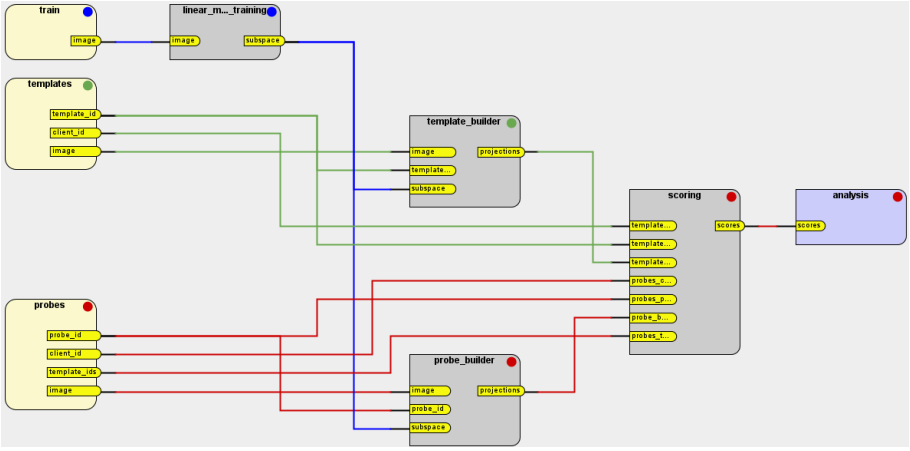


FIGURE 3.4 – Exemple de scénario d'évaluation (Extrait de [86])

3.1.5 Discussion

Par rapport à nos enjeux, la plateforme MISTRAL a des manques comme par exemple l'analyse en boîte noire, les attaques, l'utilisation des empreintes digitales. Cette plateforme ne permet pas non plus d'utiliser de vrais capteurs pour des campagnes d'acquisition. La plateforme d'évaluation est surtout utilisée pour tester et évaluer des capteurs et algorithmes pour la voix et le visage.

La plateforme du NIST a des manques comme par exemple l'analyse en boîte noire, les attaques aussi bien sur capteurs que d'algorithmes embarqués ou d'avoir une plateforme générique. Leur plateforme ne permet pas non plus d'utiliser de vrais capteurs pour des campagnes d'acquisition. La plateforme d'évaluation est surtout utilisée pour tester les algorithmes pour le standard PIV (Personal Identity Verification) [87] qui permet de garantir l'interopérabilité entre les systèmes.

Le principal inconvénient de la plateforme FVC-OnGoing est qu'il est nécessaire d'envoyer un exécutable ou le code source de l'algorithme de comparaison sur la plateforme en ligne, ce qui cause des soucis de confidentialité. La plateforme n'est pas modulaire et ne permet pas d'ajouter des modules a posteriori, ni d'effectuer des attaques ou de travailler directement sur un élément sécurisé de type carte à puce.

La plateforme BEAT n'est pas encore disponible intégralement et n'est pas orientée vers les systèmes embarqués sur SE. Elle ne permet pas l'utilisation de capteurs biométriques pour des campagnes d'acquisition ni le choix du meilleur capteur.

Nous venons de comparer les quatre plateformes de la littérature vis-à-vis de nos enjeux. D'une manière générale, les chercheurs et surtout les industriels ne souhaitent pas envoyer leur code source lors d'une évaluation. Ils sont plus enclins à envoyer une carte à puce avec un algorithme de comparaison intégré ou une librairie pour évaluer leurs algorithmes, c'est pourquoi l'analyse en boîte noire est importante pour nous. Concernant la reproductibilité des résultats de recherches, les plateformes du NIST et OnGoing le font de manière plus complexe que la plateforme BEAT qui est conçue autour de ce principe. Les possibilités et limitations des plateformes présentées précédemment sont résumées dans le tableau 3.1. Force est de constater qu'aucune plateforme ne répond pleinement aux critères définis en introduction. C'est la raison pour laquelle nous avons décidé de développer notre propre plateforme.

	MISTRAL	NIST	FVC On-Going	BEAT
Reproductibilités des résultats	✓	✓	✓	✓
Plateforme générique	✓	✓	✗	✓
Modularité	✓	✗	✗	✓
Métriques de performance	✗	✓	✓	✓
Métriques de qualité	✗	✗	✗	✓
Scénarios d'évaluation	✗	✗	✗	✓
Capteurs (choix / acquisitions)	✓	✗	✗	✗
Analyse boîte noire	✗	✗	✗	✓
Attaques	✗	✗	✗	✗
Cartes à puces	✗	✓	✗	✗

TABLE 3.1 – Comparaison des possibilités offertes par les plateformes par rapport aux enjeux

3.2 La plateforme EVABIO

La plateforme EVABIO, pour évaluation de systèmes biométriques, nous permet de répondre aux objectifs énoncés précédemment avec deux cas d'usage principaux. Le premier est de servir de support logiciel aux activités de recherche de l'équipe en biométrie pour l'évaluation d'algorithmes ou systèmes développés en recherche. Le second a pour objectif de faciliter la collaboration avec des industriels pour des prestations (caractérisation de capteurs ou d'algorithmes), ou des collaborations en recherche. La figure 3.5 illustre cette idée d'enrichissement mutuel, puisque les industriels nous permettent d'améliorer la plateforme pour répondre à leurs besoins,

de partager les résultats avec le monde académique et de susciter de nouveaux travaux de recherche suite à des problématiques énoncées par des industriels.

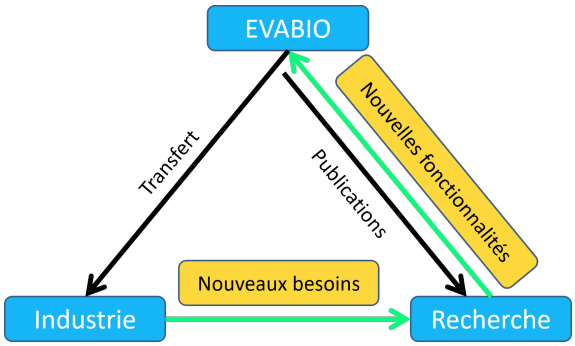


FIGURE 3.5 – Intéraction de la plateforme EVABIO avec les industriels et la recherche

3.2.1 Schéma général

La figure 3.6 montre l'architecture générale de la plateforme EVABIO [88]. Elle intègre davantage de fonctionnalités que la première plateforme précédemment développée [89], offrant ainsi plus de modules fonctionnels, tels que le module Sensor qui permet de faire des campagnes d'acquisitions, le module Quality qui intègre différentes métriques de qualité, le module Security analysis qui permet par exemple de faire des attaques et audits sur un algorithme de comparaison embarqué dans un SE. Ces nouveaux modules offrent aux développeurs ainsi qu'aux chercheurs, différentes méthodes pour choisir un capteur ou pour évaluer leurs algorithmes.

3.2.2 Les différents modules

Comme mentionné précédemment, la plateforme est composée de différents modules avec des traitements spécifiques. Tous les modules présents sont indépendants. Cette modularité nous permet de modifier et/ou ajouter des modules sans changer l'architecture générale de la plateforme. Par exemple, nous pouvons quantifier le bénéfice du contrôle de qualité durant le processus d'enrôlement. La plateforme utilise des mécanismes actifs de communication par évènements permettant un accès simultané par plusieurs modules aux données échangées entre le client applicatif et l'OCC, nous offrant ainsi une analyse "à la volée" des résultats. Tous les principaux modules tels que `Core`, `Scenario`, `Attacks`, `GUI interface`, `Sensor`, `Computing`, `Quality`, `Template reduction` et `Evaluation` ont été développés au cours de cette thèse et sont décrits ci-après.

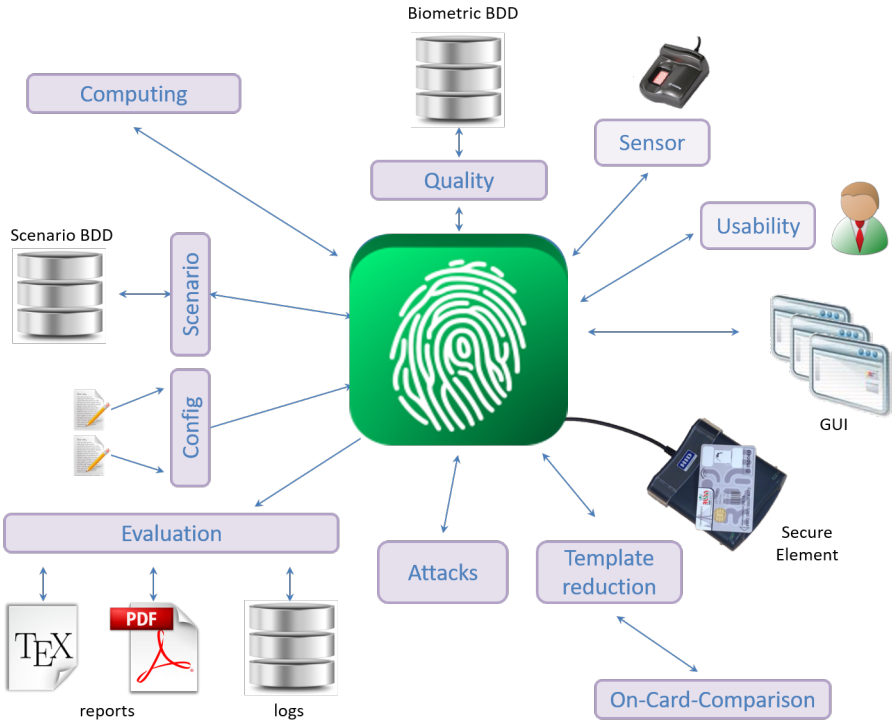


FIGURE 3.6 – Architecture générale de la plateforme EVABIO

3.2.2.1 Le module CORE

Le module `Core` (en vert) dans la figure 3.6 est le module principal connectant les autres modules. Il contrôle les interactions avec les différents modules. Il connait simplement le type de données en entrée du module et le type de données retournées par ce dernier. Par exemple, pour communiquer avec un SE, le module `Core` gère de manière transparente la connexion et la communication avec l'algorithme de comparaison (OCC). Cela est réalisé par la communication PCSC (Personal Computer/Smart Card) ou le simulateur JCOP (JavaCard OpenPlaterform) avec une librairie logicielle développée au travers de la plateforme WSCT [90]. Cette plateforme est développée au sein de notre équipe de recherche, elle a la particularité de proposer une architecture modulaire pour offrir des interactions avec un SE. Nous pouvons effectuer une transaction EMV [42] tout en voyant apparaître dans un autre plugin les commandes APDU et les réponses associées, mais aussi refaire de manière logicielle l'attaque de Cambridge [91] qui consiste à ne pas envoyer le code PIN à la carte et la transaction s'effectue de manière normale avec validation du paiement à la fin.

3.2.2.2 Module Scénario

Le module `Scenario` permet de créer ou d'utiliser un scénario d'évaluation. Il définit la base de données biométriques à interroger, le nombre d'échantillons biométriques à utiliser pour l'enrôlement ou le nombre d'utilisateurs à considérer. Cela nous permet de faire des tests reproductibles en paramétrant ces éléments. La figure 3.7, montre l'interface permettant de créer, modifier des scénarios avec les différents éléments le composant. Lorsque l'on crée un scénario, nous obtenons un fichier au format XML et un autre en JSON, la figure 3.8 montre la facilité de lecture des différentes informations .

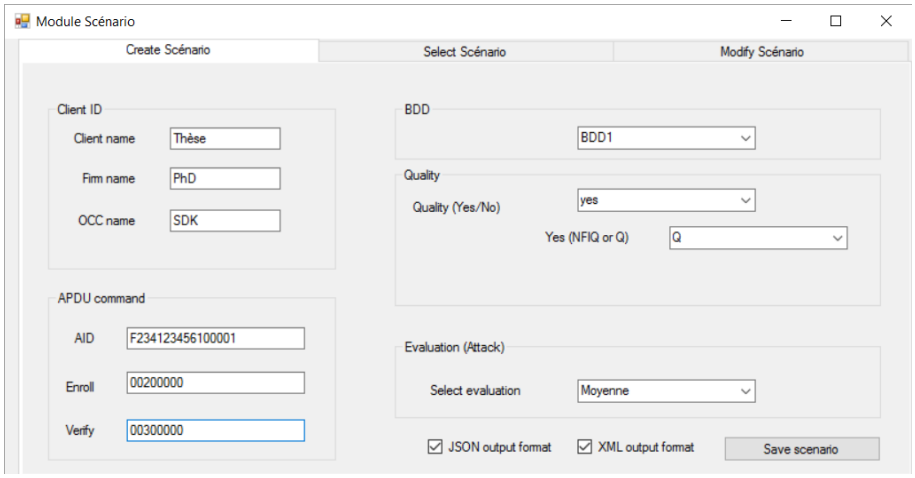


FIGURE 3.7 – Interface graphique du module Scenario de la plateforme EVABIO permettant la création, l'édition de scénarios


```
{
  "scenario": {
    "name": "scenario_Thèse_PhD_SDK",
    "infosClient": {
      "nomClient": "Thèse",
      "nomCompagnie": "PhD",
      "nomOCC": "SDK"
    },
    "bdd": "BDD1",
    "evaluation": "Moyenne",
    "quality": {
      "value": "yes",
      "yes": "Q"
    },
    "apdu": {
      "aid": "F234123456100001",
      "enroll": "00200000",
      "verify": "00300000"
    }
  }
}
```


FIGURE 3.8 – Exemple de fichier JSON obtenu avec le module scénario de la plateforme

3.2.2.3 Module Attaques

Le module `Attacks` contient différentes méthodes d'attaque sur OCC. Il est possible d'utiliser l'approche par Fuzzing [92] qui consiste à injecter de fausses données biométriques à l'algorithme de comparaison (OCC). Cela peut être un template biométrique respectant le format ISO mais contenant des données biométriques aléatoires (attaque par force brute). Il est aussi possible de tester l'interopérabilité des OCC en fournissant des modèles biométriques ISO dans lesquels des erreurs ont été injectées.

3.2.2.4 Module Interface graphique

La plateforme proposée possède une `Interface Graphique` principale qui permet de choisir le scénario de test et les métriques d'évaluation comme le montre la figure 3.9. À partir de l'interface principale, les plugins peuvent être ajoutés pour obtenir des informations à propos d'une ou plusieurs données (par exemple, le temps minimum, moyen et maximum pour un enrôlement ou une vérification). Comme mentionné précédemment, la plateforme proposée utilise des mécanismes actifs de communication par évènement. C'est pourquoi, les plugins peuvent être développés par des utilisateurs pour récupérer toutes les informations spécifiques qui ont de l'intérêt pour lui.

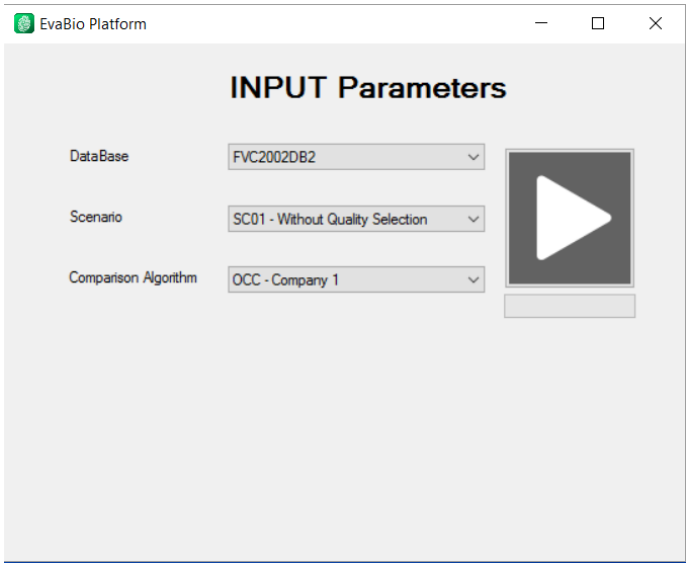


FIGURE 3.9 – Interface graphique de la plateforme EVABIO, permettant de lancer une évaluation

3.2.2.5 Module Capteur

Le module `Sensor` est une mini plateforme qui permet d'acquérir de vraies et fausses bases de données d'empreintes avec de vrais doigts et des protocoles spécifiques. Ce module est utilisé pour évaluer la performance des capteurs et pour effectuer des attaques sur ces derniers. Cette plateforme de capteurs peut-être utilisée en entrée pour le module `Core`, pour acquérir en direct une ou plusieurs empreintes digitales afin d'être comparées sur un algorithme OCC. Le module intègre aussi le logiciel SFinge [93] permettant de générer des empreintes digitales synthétiques en définissant les paramètres souhaités de l'empreinte digitale comme le montre la figure 3.10. SFinge permet, entre autres, de pouvoir choisir la résolution de l'image, le type d'empreinte digitale que l'on souhaite générer mais surtout de pouvoir créer des bases de données conséquentes avec jusqu'à 100 000 individus (cette limitation de taille de bases de données est imposée par SFinge).

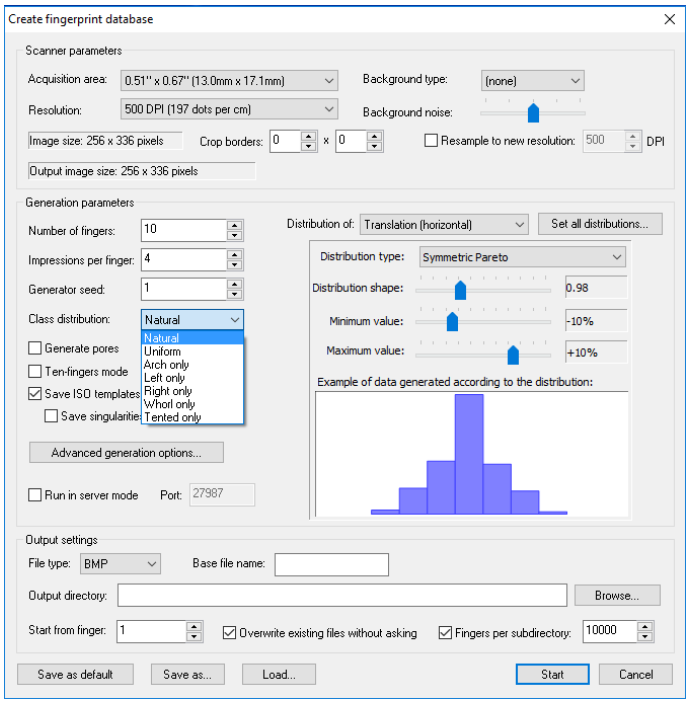


FIGURE 3.10 – Interface graphique du logiciel SFinge permettant de générer des bases d'empreintes digitales synthétiques

3.2.2.6 Le module Calcul distribué

Le module `Computing` permet d'avoir un calcul distribué pour augmenter l'efficacité de l'évaluation des algorithmes OCC. Par exemple, avec trois algorithmes

OCC sur trois cartes à puces, nous sommes capables de lancer les trois évaluations en parallèle, ce qui permet de réduire drastiquement le temps d'évaluation durant une campagne.

3.2.2.7 Module Qualité

Le module `Quality` est consacré à la métrique de qualité de données biométriques comme des images d'empreintes digitales ou des templates de minuties. Une telle métrique est très utile pour comparer différents capteurs biométriques à partir de mêmes utilisateurs et permet d'évaluer les performances de comparaison en enlevant les échantillons de mauvaise qualité [94], aussi bien pour la session d'enrôlement que de vérification. Cet objectif peut être facilement atteint parce qu'une bonne qualité d'empreinte fournit des informations plus fiables et précises. Cela a aussi une incidence bénéfique sur les opérations de comparaison sur cartes à puce, surtout quand il est nécessaire de faire une sélection de minuties (la taille du template étant limitée sur un SE). Il a été montré expérimentalement qu'un extracteur de minuties localise plus précisément les points caractéristiques à l'intérieur d'images de bonnes qualités que dans de mauvaises [65]. Par conséquent, un template de minuties réduit doit préserver autant que possible les minuties correctement détectées plutôt que les points parasites tout en assurant une performance similaire. Le module de mesure de qualité présent dans la plateforme est combiné avec un composant de validation qui permet à l'utilisateur de mesurer la performance des différentes métriques, ce qui permet de rendre une nouvelle décision et ainsi choisir la métrique appropriée. Le module dispose d'une interface qui permet de gèrer toutes les bases de données biométriques. Le module `Core` demande à l'interface la prochaine donnée biométrique filtrée par une des métriques de qualité et délègue à l'interface le traitement, la connexion et la gestion des différentes bases biométriques. Ceci permet, par exemple, de rendre indépendant le format de stockage des données biométriques dans la plateforme EVABIO.

Deux algorithmes d'évaluation de la qualité d'image sont disponibles dans le module `Quality` : 1) NFIQ [67] et 2) la métrique Q du GREYC [95]. La métrique NFIQ génère cinq niveaux de qualité de 1 à 5, sachant que la meilleure qualité est indiquée par la valeur la plus petite et le niveau maximum dénote une image de très mauvaise qualité. La métrique Q du GREYC, développée au sein de l'équipe, estime la qualité des empreintes digitales sur une échelle continue à cinq catégories, (0-20) médiocre, (20-40) mauvais, (40-60) moyen, (60-80) bon et (80-100) très bon. Le fait d'utiliser

une qualité des scores continue permet d'avoir une meilleure répartition des qualités d'échantillons que ceux utilisant uniquement quelques niveaux de qualité. A l'instar des autres modules, nous avons la possibilité d'enrichir les métriques de qualités proposées dès qu'une nouvelle méthode est disponible. La figure 3.11, nous donne un exemple d'évaluation de la qualité d'une empreinte digitale provenant d'un capteur.

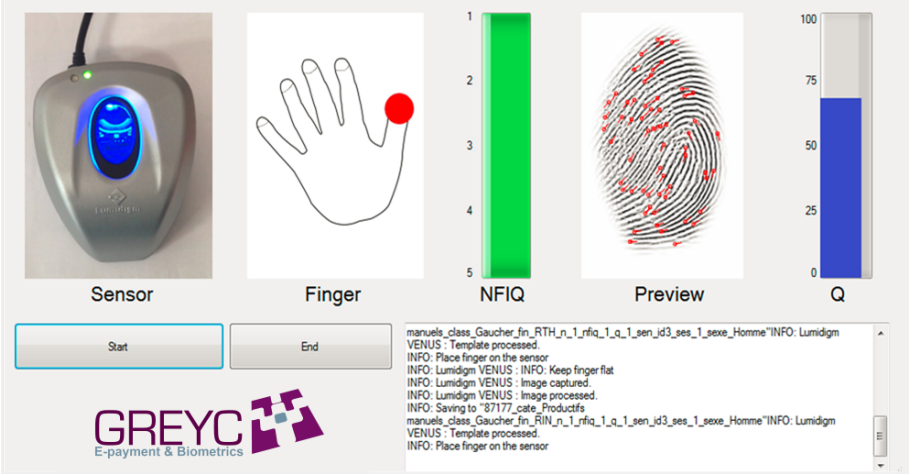


FIGURE 3.11 – Interface graphique du module Sensor permettant de visualiser les différentes métriques pour une empreinte digitale acquise.

3.2.2.8 Module Réduction de template

Le module `Template reduction` propose différentes méthodes permettant de réduire la taille d'un template biométrique. Ce module contient les méthodes de l'état de l'art ainsi que nos contributions décrites dans le chapitre 4.

3.2.2.9 Module Évaluation

Le module `Evaluation` propose différentes mesures de performance communément utilisées dans la littérature mais aussi dans l'ISO [96] dont certaines sont plus spécifiques. Nous reprenons certaines définitions présentées en section 2.5.1 mais dans le cadre d'utilisation d'un OCC :

— Le taux de fausse correspondance (False Match Rate, FMR) mesure combien de fois la donnée biométrique d'un utilisateur donne une vérification positive avec une donnée d'un autre utilisateur ;

— Le taux de faux rejets (False Non Match Rate, FNMR) mesure combien de fois la donnée biométrique d'un utilisateur donne une vérification négative avec une donnée du même utilisateur ;

— Le taux de succès d'une attaque mesure le ratio d'attaques réussies (nombre de résultats positifs sur le nombre d'essais) ;
— La mesure de l'interopérabilité quantifie le ratio de tests validés lorsque l'on vérifie un template ISO sur un OCC ;
— La courbe ROC (Receiver Operating characteristic curve)[53] décrit le comportement de l'OCC biométrique pour chaque valeur du seuil de décision (à partir de laquelle un test est positif). Cela implique qu'il est possible d'obtenir le score de comparaison fourni par l'OCC ou d'avoir la possibilité de définir le seuil de décision. Pour les OCC de recherche, cette information est toujours disponible contrairement aux OCC industriels, car cela donnerait beaucoup d'informations à un attaquant et mettrait en danger leur OCC ;
— Le temps de vérification mesure le temps nécessaire pour effectuer un enrôlement ou pour obtenir un résultat de vérification, après avoir envoyé une APDU (Application Protocol Data Unit définie dans [41]) au SE. Il est également possible de générer plusieurs statistiques sur les temps de calcul telles que l'histogramme du temps de vérification, la moyenne, le minimum, le maximum, l'écart-type,....

La figure 3.12 montre les principaux résultats provenant d'une évaluation des performances sur la dynamique de frappe au clavier. En entrée de ce module, nous devons sélectionner le fichier de logs mis en forme pour calculer et afficher les résultats de l'évaluation. Par exemple, ici, nous pouvons voir sur la courbe ROC que les performances du système ne sont pas très bonnes avec un EER à 20%. D'un simple coup d'oeil, nous pouvons aussi voir le seuil à l'EER qui est de 150, ce qui veut dire que le seuil de décision de l'OCC est fixé à cette valeur. La distribution des scores nous permet de voir s'il y a une grande disparité au niveau de l'évaluation, ce qui ici est le cas, nous avons beaucoup de valeurs inférieures à 2000 et peu sont supérieures à 2000. Ces informations sont importantes lorsque l'on fait une évaluation, c'est la raison pour laquelle ces métriques sont calculées et affichées dans l'interface graphique. Une partie de cette interface est consacrée aux calculs permettant d'obtenir la valeur du FMR pour une valeur spécifique de FNMR et l'inverse est également proposé.

Dans cette section, nous avons présenté l'architecture de la plateforme EVABIO ainsi que les différents modules, développés au cours de cette thèse, la composant. EVABIO remplit les objectifs que nous avons définis précédemment même si certains modules sont toujours en cours de développement. Le tableau 3.2 rappelle les objectifs et les possibilités offertes par les différentes plateformes.

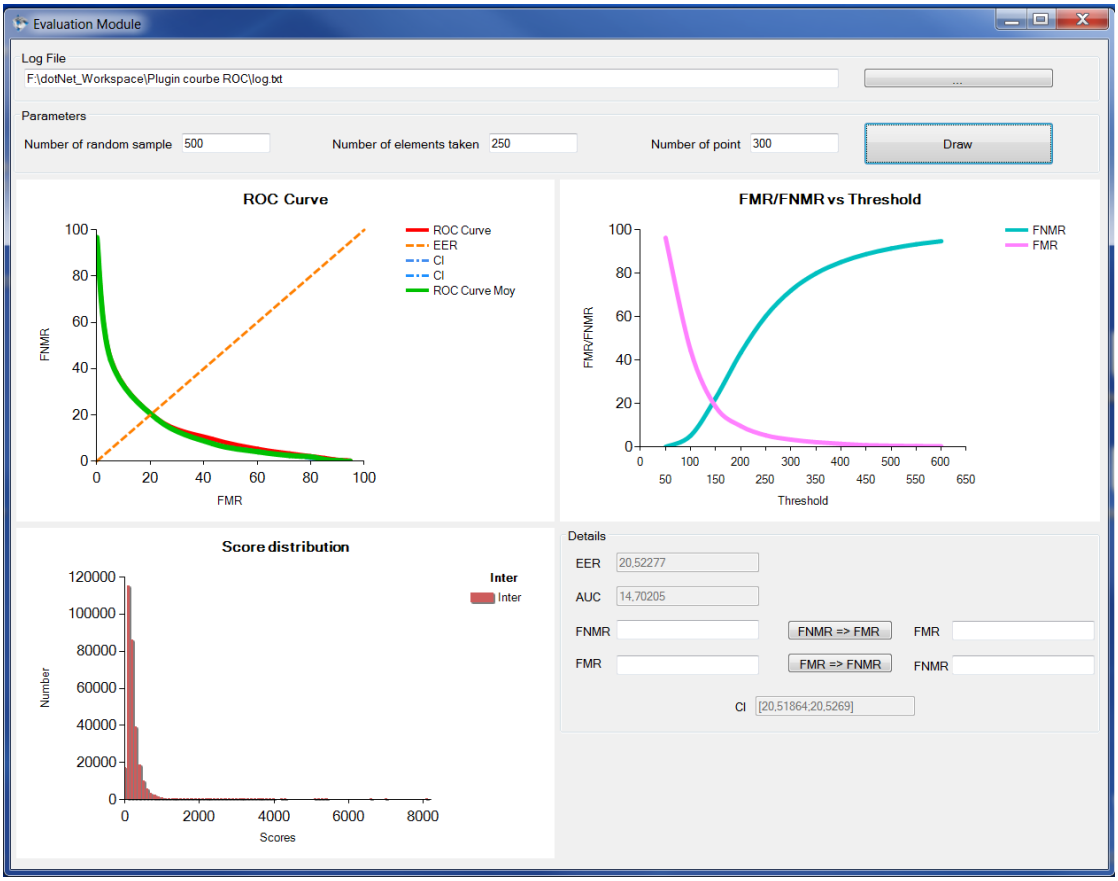


FIGURE 3.12 – Aperçu de l'interface graphique du module d'évaluation.

3.3 Cas d'usage d'EVABIO

Dans cette section, nous présentons quatre cas d'utilisation de la plateforme, à savoir le stockage et comparaison d'un Bio-Hashing dans un élément sécurisé, le contrôle de la qualité durant l'enrôlement, le module d'acquisition sur capteurs biométriques, et l'évaluation sur OCC. Ce sont quatre usages représentatifs de la plateforme car ils permettent de voir les interactions entre différents modules et le fonctionnement transparent pour l'utilisateur.

3.3.1 Algorithme de comparaison de BioCode sur SE

Comme nous l'avons vu dans la section 2.3, les données biométriques sont stockées et comparées directement sur l'élément sécurisé. Ici, nous utilisons des données biométriques provenant d'une empreinte et sécurisées grâce à une fonction de bio-hashing. Le bio-hashing est un algorithme permettant d'obtenir à partir d'une donnée biométrique de type empreinte et un secret (seed) un BioCode représentant la donnée

	MISTRAL	NIST	FVC On-Going	BEAT	EVABIO
Reproductibilités des résultats	✓	✓	✓	✓	✓
Plateforme générique	✓	✓	✗	✓	✓
Modularité	✓	✗	✗	✓	✓
Métriques de performance	✗	✓	✓	✓	✓
Métriques de qualité	✗	✗	✗	✓	✓
Scénarios d'évaluation	✗	✗	✗	✓	✓
Capteurs (choix / acquisitions)	✓	✗	✗	✗	✓
Analyse boîte noire	✗	✗	✗	✓	✓
Attaques	✗	✗	✗	✗	✓
Cartes à puces	✗	✓	✗	✗	✓

TABLE 3.2 – Comparaison des possibilités offertes par EVABIO et les autres plateformes.

biométrique. Ce Biocode est non-reversible, ce qui veut dire qu'on ne peut pas retrouver la donnée biométrique source même en connaissant le secret. La figure 3.13 illustre le principe de génération du BioCode.

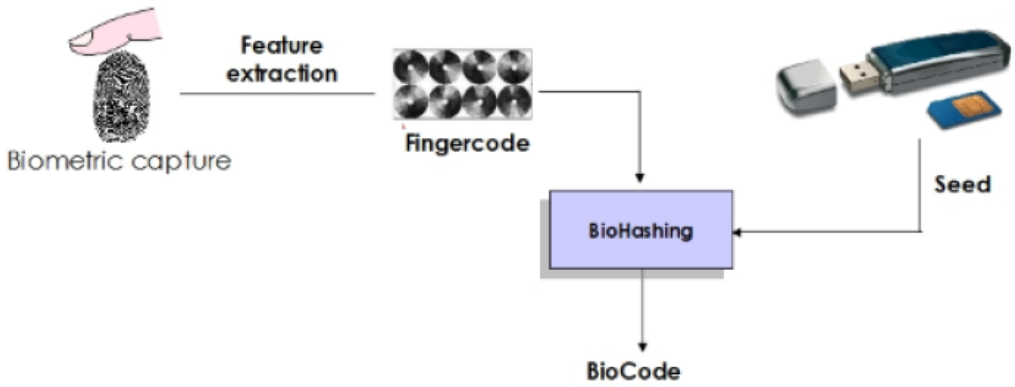


FIGURE 3.13 – Principe général de génération d'un BioCode (extrait de [97]).

Nous avons développé en Javacard, la partie stockage des données, le BioCode ainsi que le secret. De plus, un algorithme de comparaison de Biocode a été développé pour l'élément sécurisé. Pour garantir une sécurité maximale et éviter une attaque de type « homme du milieu », un canal sécurisé a été créé grâce à Global Platform, entre l'élément sécurisé et le CORE. Ce canal sécurisé a été chiffré pour avoir le moins d'informations sensibles en clair qui transitent.

Cette application nous a permis de montrer la possibilité d'avoir des données biométriques révocables stockées sur un élément sécurisé. Cela nous a aussi permis d'avoir une utilisation réelle et embarquée d'un système biométrique révocable sur

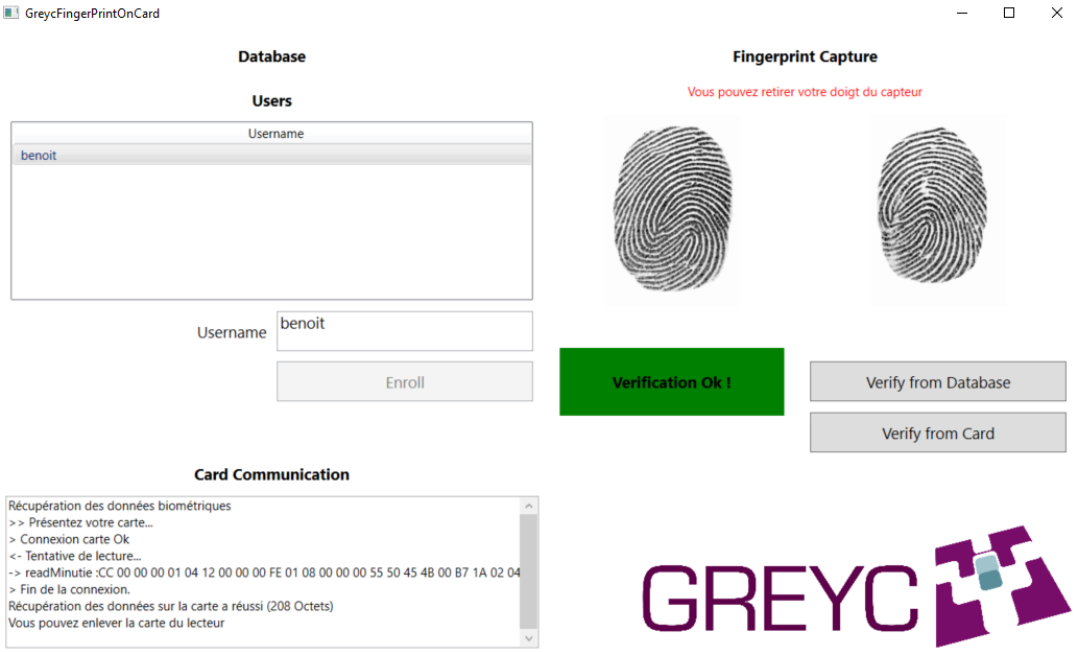


FIGURE 3.14 – Capture du logiciel FingerPrint On Card utilisant un canal sécurisé chiffré pour transférer les données biométriques au SE).

un élément sécurisé, en garantissant une sécurité maximale lors de l'échange des données.

3.3.2 Contrôle de la qualité durant l'enrôlement

Nous abordons ici le problème de la sélection du meilleur template en terme de qualité et du nombre de minuties pour l'enrôlement pour un OCC. Ce processus de sélection est effectué en utilisant à la fois la métrique NFIQ et l'indice de qualité Q du GREYC. La figure 3.15, montre la procédure utilisée pour choisir un template sans contrôle de qualité et lorsque qu'un contrôle de qualité est effectué.

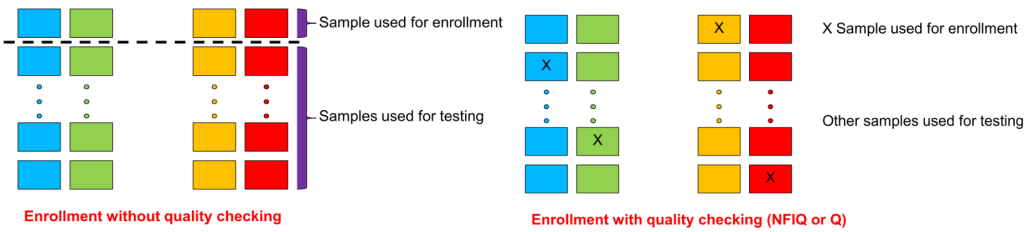


FIGURE 3.15 – Protocole de sélection du template de référence pour l'enrôlement avec et sans contrôle de la qualité, où une colonne correspond aux échantillons provenant d'un individu.

Concernant le protocole, nous utilisons des données biométriques collectées lors d'une expérimentation avec trente-neuf individus. Nous avons fait trois sessions de capture avec deux doigts : index gauche et droit, avec cinq échantillons par session et par individu. Au total, nous avons capturé 1170 images d'empreintes digitales représentées également par un template au format ISO Compact Card. Sur chaque image, nous avons calculé, grâce au module `Quality` de la plateforme EVABIO, un score de qualité en utilisant les métriques NFIQ et Q. Pour choisir le template de référence, nous avons sélectionné pour chaque personne, le template avec la meilleure qualité en considérant les deux métriques séparément ainsi que le plus grand nombre de minuties n'excédant pas le nombre maximal accepté par l'OCC.

La performance sans la sélection du template d'enrôlement est aussi calculée [89] ce qui permet d'évaluer l'impact du contrôle qualité. Le tableau 3.3 présente les résultats de l'évaluation sur un OCC commercial de la sélection du template d'enrôlement avec et sans contrôle de la qualité. D'un point de vue performance, il y a une assez bonne résistance aux impostures pour toutes les méthodes avec au maximum 0.41% de fausses acceptations, ce qui est bien mais pas assez faible pour arriver au 1/10000 communément utilisé pour garantir la même sécurité qu'un code PIN. Le FNMR est relativement bon pour la sélection avec la métrique GREYC Q comparé aux autres méthodes avec 4.75% de faux rejets comparé au 17.36% pour la méthode "sans sélection" et 14.36% pour NFIQ. Nous observons des résultats plutôt satisfaisants avec 0.41% sans filtrage de la qualité, en terme de FMR comparés à ceux publiés dans le rapport Minex2 [80] 0.0068% et une très bonne performance (gain de 50%) avec le filtrage de la qualité 0.003% avec la métrique GREYC Q. Le taux de faux rejets (FNMR) apparait trop élevé. Cependant, par sélection du template d'enrôlement, nous sommes capables de réduire le FNMR d'environ 17% avec la sélection NFIQ et 66% de plus avec la sélection Q en comparaison avec NFIQ. Ces résultats montrent un gain très significatif sur la performance, rien qu'en faisant une sélection avec les métriques de qualité du template pour l'enrôlement sans rien changer au système biométrique existant.

Pour conclure sur la performance, cette expérimentation a montré que la sélection de la qualité du template d'enrôlement est très importante pour obtenir une bonne performance sur un système biométrique. C'est pourquoi, dans la plateforme EVABIO, une métrique de qualité est utilisée comme un filtre pour choisir le template de référence pour chaque utilisateur de la base de données. Nous pouvons quantifier le gain du contrôle de qualité lors de la procédure d'enrôlement d'une

	FMR	FNMR
Sans sélection	0.41%	17.36%
NFIQ	0.05%	14.36%
Q	0.003%	4.75%

TABLE 3.3 – Performance de chaque méthode de sélection pour les métriques de qualité

manière opérationnelle. Cela nous permet aussi d'améliorer la métrique de qualité développée au GREYC, dans le cadre de la thèse de Zhigang Yao, en effectuant des expérimentations similaires sur différentes bases de données.

3.3.3 Module acquisition sur capteurs biométrique

La plateforme EVABIO propose un autre module dédié à l'acquisition de templates biométriques. Celui-ci permet de recueillir des données brutes et de les stocker dans des bases de données. Durant une campagne d'acquisition, nous utilisons différents capteurs et ce module permet de détecter sur quel capteur le doigt est placé. Chaque acquisition génère l'image de l'empreinte digitale ainsi que le template de minutie associé au format ISO. Ces données sont enregistrées avec un identifiant comprenant un numéro d'identification de l'individu, la main et le doigt utilisé ainsi que les informations du profil utilisateur. Voici un exemple d'identifiant, $10589\_G\_I\_S\_H\_R$: avec 10589 pour le numéro d'identification, G : la main gauche, I : pour l'Index, S : pour Sénior, H : pour Homme, R : pour Retraité). Le module d'acquisition avec les capteurs est présenté dans la figure 3.16. Suivant le capteur à utiliser, différents écrans sont montrés à l'utilisateur, lui indiquant la main et le doigt à utiliser pour effectuer la capture. Nous sommes aussi capables de lancer une acquisition en direct durant une évaluation sur un capteur réel, nous permettant ainsi de pouvoir tester des empreintes d'un panel d'individus réputé difficile pour l'acquisition des données.

En ce qui concerne la sécurité, un capteur biométrique présente des vulnérabilités. Ratha et *al.* [35] ont classifié les attaques d'un système biométrique générique en huit classes (tel qu'expliqué en section 2.5.3). Nous avons testé deux attaques sur le capteur biométrique, une avec de fausses empreintes digitales prises sur de vrais utilisateurs et l'autre sur des doigts morts.

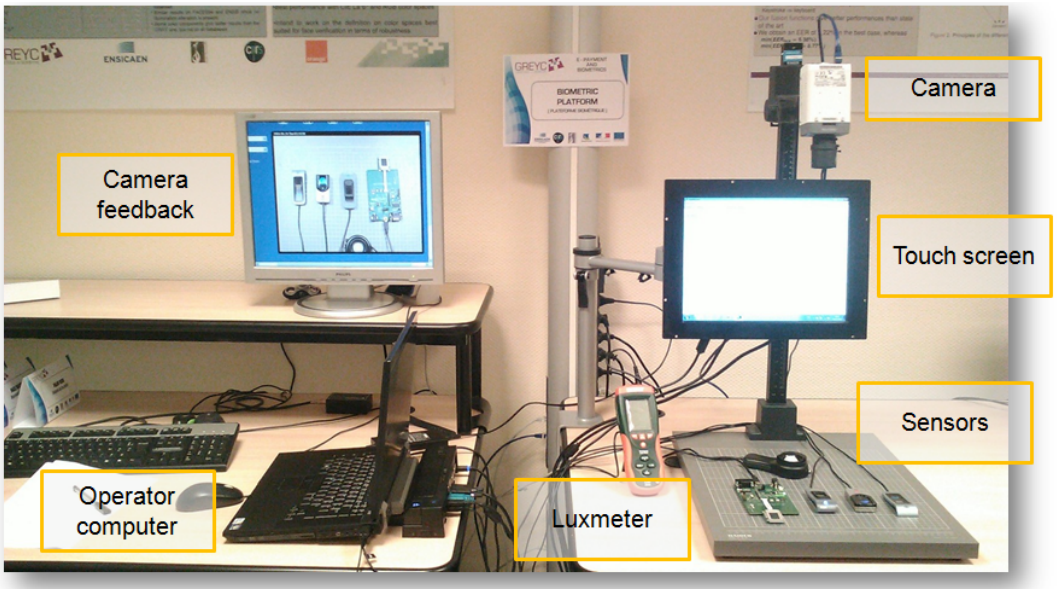


FIGURE 3.16 – Plateforme d'acquisition en fonctionnement

3.3.3.1 Fausses empreintes digitales

Une base de données de fausses empreintes digitales provenant de vrais doigts et empreintes a été créée (cf. figure 3.17). Pour construire cette base de données, nous avons utilisé de la cire et de la gélatine car ces matériaux ne sont pas épais. Ils permettent aussi de se poser facilement sur un vrai doigt et peuvent aussi être peu visible lorsque le doigt est posé sur le capteur. Pour vérifier la robustesse des capteurs, nous avons calculé le FTA et nous avons déterminé si les capteurs de tests fournissent une vérification négative ou s'ils sont capables de détecter une fausse empreinte ou une attaque par usurpation d'identité aussi nommée spoofing.

FIGURE 3.17 – Exemple de fausses empreintes

3.3.3.2 Doigts morts

Nous avons créé une base de données d'empreintes constituées uniquement de doigts morts, provenant de personnes ayant fait don de leur corps à la science. Nous sommes allés à la morgue du CHU de Caen et nous avons fait l'acquisition d'empreintes de quatre personnes décédées. Le protocole d'acquisition pour chaque personne est le suivant :

— 3 capteurs ont été utilisés
— 4 doigts (excepté le pouce) ont été utilisés
— les 2 mains ont été utilisées
— 6 captures par individu par doigt et par capteur ont été réalisées

Finalement, nous avons 144 (6*2*4*3) données (images d'empreintes digitales et le template ISO associé) par individu pour tous les capteurs. Pour les quatre individus, nous avons au total 576 (144*4) données. Nous avons calculé le FTA et nous obtenons un résultat de 36,11%, ce qui est très important, en général le FTA est inférieur à 1% [98]. Cela veut dire que les capteurs ont du mal à capturer les empreintes provenant de doigts morts.

3.3.3.3 Base de données Sénior

Une base de données séniors a été créée, respectant le même protocole que pour les doigts morts, pour avoir une base de comparaison avec les doigts morts, qui proviennent de personnes ayant un âge proche de ceux ayant fait don de leur corps à la science (voir figure 3.18).

3.3.3.4 Illustrations

Pour comparer les deux attaques, nous avons utilisé les fausses empreintes ainsi que les doigts morts sur les quatre capteurs, nous permettant ainsi de vérifier si ce type d'attaque fonctionne sur cet ensemble de capteurs. Le capteur 1 est un modèle swipe, et les autres sont optiques. Pour les fausses empreintes, nous avons un FTA à 100% pour les capteurs 1, 3 et 4. Ce qui par conséquent, nous permet d'en déduire que les attaques de type spoofing ne fonctionnent pas pour ces capteurs. Pour le capteur 2, le FTA est à 0% ce qui signifie que ce capteur n'a pas de difficulté pour acquérir une donnée biométrique. Sur 96 tests effectués, 65% ont conduit à une vérification négative et 35% à une positive. Cela veut dire que malgré le fait que le capteur arrive à capturer l'empreinte digitale, la comparaison ne fonctionne que dans un tiers des cas, ce qui n'est pas concluant. Les matériaux utilisés ne permettent

FIGURE 3.18 – Acquisition à la morgue

Résultats de la métrique Q				
	Capteur 1	Capteur 2	Capteur 3	Capteur 4
Morgue	38.3	81.9	72.3	68.3
Sénior	32.1	84	78.6	73.7

TABLE 3.4 – Valeur moyenne de la métrique Q pour des empreintes digitales provenant d'une base de données constituées de séniors et une autre de doigts morts.

pas d'avoir une précision suffisante pour que les minuties soient bien détectées par l'extracteur.

Pour les doigts morts, nous avons utilisé la métrique de qualité Q, car il a été montré dans une précédente étude [95] que cette métrique fournit une meilleure évaluation de la qualité que NFIQ. Le tableau 3.4 compare pour chaque capteur la moyenne de la métrique Q pour la base de données de doigts morts et une base de données de séniors.

Nous pouvons noter pour les capteurs 2, 3 et 4 que les doigts morts ont une qualité d'empreintes digitales inférieure à la base sénior (rappelons que plus haute est la valeur de la métrique Q, meilleure est la qualité). Pour le capteur 1 (le seul capteur swype), ce n'est pas le cas et la qualité est largement moins bonne que les trois autres. Nous pensons que cela est dû à plusieurs facteurs, le premier peut provenir de la détérioration de la peau d'un doigt mort d'autant qu'ils ont été congelés. La seconde vient de la capture, la main étant coupée et utilisée par un personnel du CHU, il est

plus dur pour cette dernière d'avoir un retour sensoriel sur la force d'appui du doigt sur le capteur lors du swype. Ces facteurs peuvent expliquer la mauvaise qualité des échantillons obtenus.

3.3.4 Évaluation sur OCC

Pour illustrer le fonctionnement de la plateforme EVABIO, nous avons évalué un OCC commercial avec une base de données biométriques acquise avec le module sensor. Cette base de données est constituée de 60 individus et nous avons acquis 6 échantillons par doigt pour chaque capteur. La base de données est donc constituée de 360 (60 x 6) templates biométriques par capteur. Lors de l'évaluation, nous calculons les scores intra et inter nous permettant d'obtenir la performance de l'algorithme de comparaison embarqué dans l'élément sécurisé. Le point de fonctionnement, qui représente la performance du système pour un seuil déterminé par le fournisseur de l'OCC commercial, est donné dans la figure 3.19 avec le taux de fausses acceptations (FMR) et le taux de faux rejets (FNMR). La distribution du FMR et du FNMR en fonction de la métrique Q du GREYC est représentée dans la figure 3.20. Nous avons aussi deux informations supplémentaires, la distribution des temps (voir figure 3.21) ainsi que la distribution de la métrique Q sur la base de donnée.

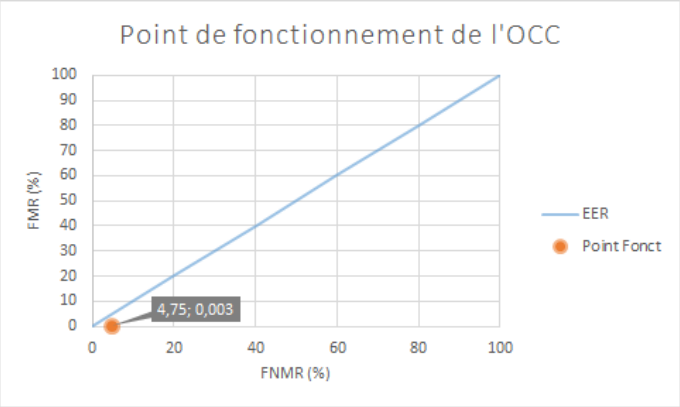


FIGURE 3.19 – Point de fonctionnement du système avec la métrique de qualité Q

Comme montré dans la figure 3.19, nous pouvons savoir si notre algorithme de comparaison est performant sur la base de données utilisée. Nous pouvons aussi en déduire, si l'algorithme se trouve dans une zone de compromis, ou de haute ou basse sécurité. Ainsi, il est plus aisé de comparer la performance d'algorithmes de comparaison pour une même base. Comme nous pouvons le constater, l'algorithme à un taux de FMR à 0.003% ce qui est très performant, à contrario le taux de faux rejets (FNMR) est de 4.75% ce qui est assez élevé pour un algorithme commercial. Cela

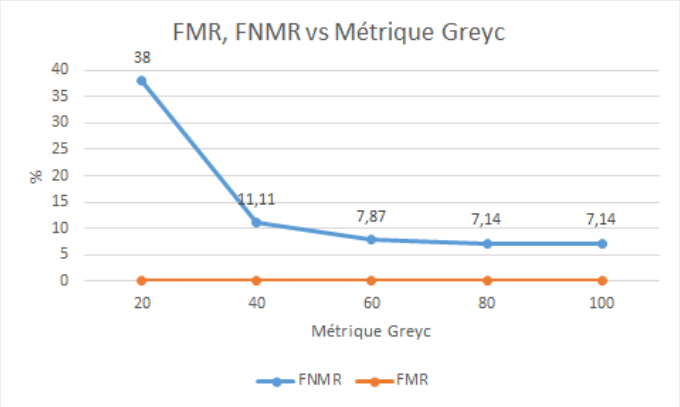


FIGURE 3.20 – FMR FNMR vs la métrique Q : plus la métrique de qualité Q est élevée plus l'échantillon est de bonne qualité et plus la valeur du FNMR est basse.

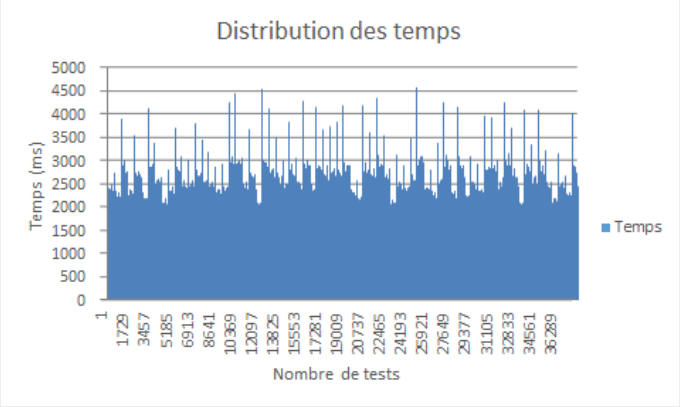


FIGURE 3.21 – Distribution des temps

induit que l'algorithme a été paramétré en mode sécurité moyenne car le taux de faux rejets est élevé. Le temps est une autre information importante car cela a un impact au niveau de l'acceptation par l'utilisateur. Sur la figure 3.21, nous remarquons que le temps varie de manière significative d'une comparaison à l'autre. Ce temps dépend totalement de l'algorithme de comparaison utilisé. Cela est dû au nombre de minuties présentes dans le template stocké ainsi que celui de test, plus nous avons de données biométriques à comparer plus le temps de comparaison augmente. Ceci peut donner une indication à un attaquant sur la taille du template stocké. Concernant l'évolution du FNMR en fonction de la qualité de l'échantillon, figure 3.20, nous constatons que lorsque la qualité de l'image est faible, la performance du système est mauvaise avec un FNMR de 38%. A contrario, plus la qualité de la donnée enrôlée est importante et plus le taux de FNMR diminue jusqu'à atteindre 7.14%. Cette information, nous permet d'observer le gain non négligeable obtenu lorsque l'on sélectionne le template

à enrôler dans notre SE. Ceci permet de visualiser très rapidement le gain obtenu suivant la métrique de qualité utilisée pour une même base. Cette information nous permet de quantifier l'importance du choix du template à considérer lors de la phase d'enrôlement pour ainsi garantir une bonne performance opérationnelle.

3.4 Conclusion

Dans ce chapitre, nous avons présenté ce qu'était une plateforme d'une manière générale puis au travers du prisme de l'informatique. Nous avons défini dans la section 3 les dix caractéristiques qui nous semblent importantes pour une plateforme d'évaluation. Nous avons ensuite présenté les différentes plateformes d'évaluation de systèmes biométriques de l'état de l'art. Nos caractéristiques nous ont permis de comparer les différentes plateformes et ainsi d'identifier les avantages et inconvénients de chacune. Aucune plateforme ne répondant à tous nos enjeux, nous avons décidé de développer EVABIO (pour évaluation biométrique) notre propre plateforme d'évaluation. L'architecture de la plateforme, ainsi que les différents modules qui la composent ont été présentés. Cette plateforme répond à nos différents enjeux, trois cas d'utilisations ont permis de montrer les différentes interactions possibles entre les modules ainsi que les avantages de cette plateforme. La plateforme EVABIO nous sert de support pour tous les travaux effectués pendant cette thèse. Cette plateforme est en constante évolution au sein de l'équipe Monétique & Biométrie du GREYC. Il est important pour nous de développer et maintenir une telle plateforme pour la communauté scientifique et les entreprises.

Pour conclure, cette plateforme répond à nos enjeux, elle a fait l'objet de deux publications en conférence internationale et d'une publication en chapitre de livre.

Dans le chapitre suivant, nous abordons la sélection de minuties au sein d'un template d'empreinte digitale lorsque ce dernier est trop volumineux pour être stocké sur un SE.

Chapitre 4

La sélection de minuties

Ce chapitre présente les différentes méthodes de sélection des minuties d'un template biométrique de l'état de l'art. Nous proposons ensuite de nouvelles méthodes pour obtenir de meilleures performances. Une proposition de méthode de sélection est présentée pour la génération du template de référence à enrôler sur l'élément sécurisé. Ensuite, une illustration de la distribution d'un template réduit de minuties pour chacune des méthodes permet d'observer la répartition de ces dernières dans le template initial.

Sommaire

4.1 Introduction

Le but de la sélection de minuties est de satisfaire la limitation de la mémoire des applications ainsi que des capacités de calculs embarquées sur un élément sécurisé. C'est-à-dire, ne conserver qu'un sous-ensemble des minuties de l'empreinte digitale. Nous commençons par présenter le contexte d'utilisation de la réduction de template, puis les méthodes disponible dans l'état de l'art. Ensuite, nous présentons

et comparons les méthodes que nous avons développées. Une méthode basée sur les algorithmes génétiques est présentée pour répondre au besoin de l'enrôlement de l'individu sur un élément sécurisé.

Nous supposons ici ne pas avoir accès à l'image de l'empreinte digitale pour cette tâche. Notre objectif est de trouver des méthodes permettant d'avoir la meilleure performance possible tout en ayant un temps de calcul rapide. Le fait de vouloir un niveau de performance élevé nous permet lors de la phase d'enrôlement, d'avoir le meilleur template stocké sur l'élément sécurisé (voir figure 4.1).

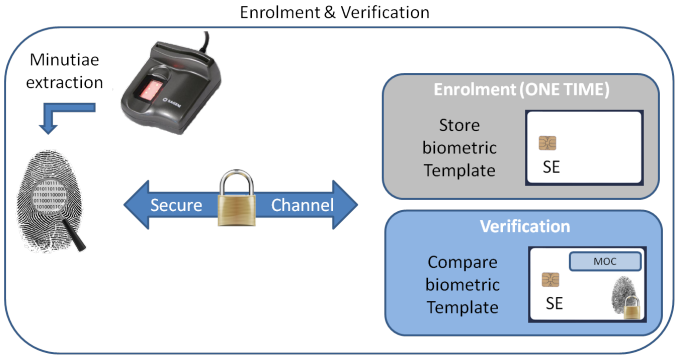


FIGURE 4.1 – Étape d'enrôlement et de vérification

Pour cette étude, nous reprenons la figure 3.6 car nous avons développé le module `Template reduction` en rouge dans la figure 4.2. Celui-ci nous permet d'effectuer les réductions de template biométrique. Dans ce chapitre, nous souhaitons déterminer dans quelle mesure la réduction de template biométrique, sans aucune connaissance de l'algorithme d'extraction de minuties ainsi que de l'algorithme de comparaison, impacte les performances lors de l'authentification biométrique. Chacune des méthodes de réduction de template présentées ici sont intégrées dans notre module `Template reduction`. Nous voyons dans la prochaine section les méthodes de la littérature utilisées dans ce contexte.

4.2 Les méthodes de l'état de l'art

Dans l'état de l'art, nous avons trouvé deux méthodes qui permettent de réduire la taille du template de minuties à partir du template ISO Compact Card. Il y en a une proposée par le standard ISO 19795-2 [47] appelé *Troncature* et une par le NIST [99] nommé *Barycentre*. Ces deux méthodes sont décrites ci-après.

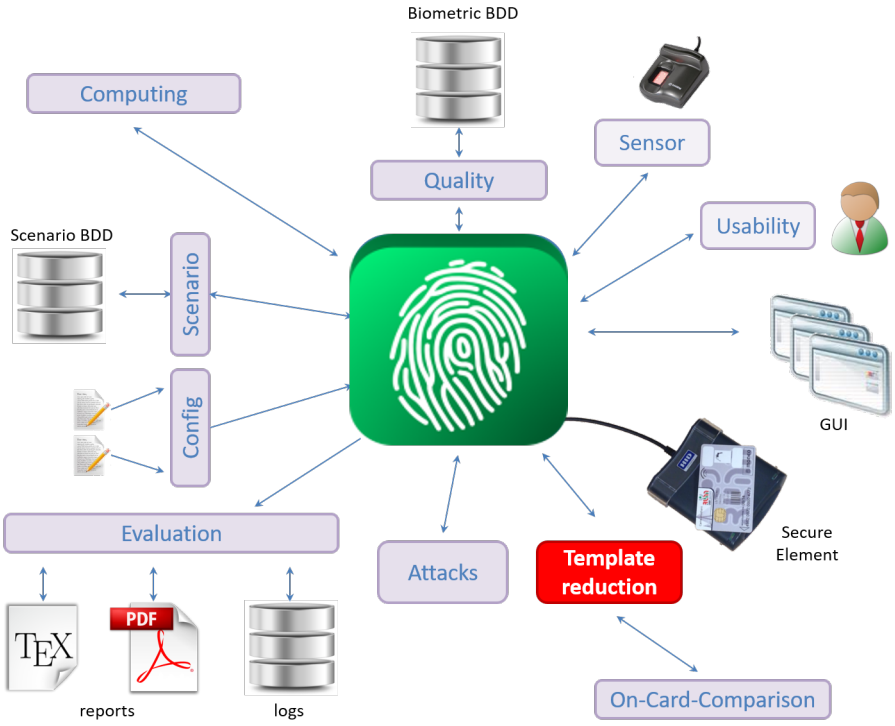


FIGURE 4.2 – Architecture générale de la plateforme EVABIO avec le module Tempalte reduction utilisé dans ce chapitre

4.2.1 Troncature

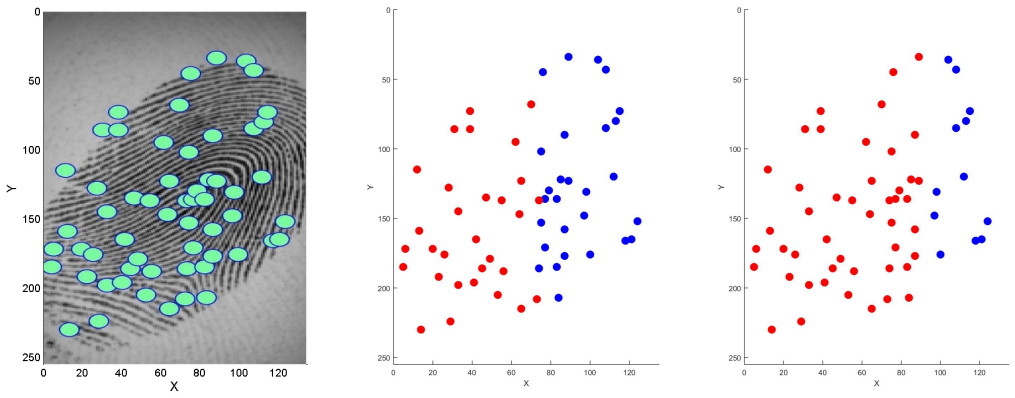
Cette méthode est basée sur une troncature simple, nous gardons simplement les N_{max} minuties du template initial. La raison pour laquelle cette approche simple peut être efficace est liée à la génération du template d'empreinte digitale. Pour de nombreux systèmes biométriques commerciaux, un template d'empreinte digitale est généré par un procédé spécifique. Il peut être généré en tenant compte de l'emplacement ascendant des minuties sur l'axe Y par exemple. Dans le cas où plusieurs captures ont été effectuées, les minuties de haute qualité (toujours présentes dans les différentes captures, par exemple) peuvent être placées au début du template. La sélection des N_{max} premières minuties pourrait être dans ce cas très simple et efficace. L'algorithme 1 nous montre les étapes pour obtenir le template réduit avec cette méthode.

Algorithm 1: Algorithme pour la méthode troncature

Result: TemplateReduit
Input : TemplateMinuties
Input : nbrMinutieAttendues

$n \leftarrow nbrMinutieAttendues$
$m \leftarrow size(TemplateMinuties)$
if $m > n$ **then**
  $TemplateReduit \leftarrow TemplateMinuties(1$ **to** $nbrMinutieAttendues)$
else
  $TemplateReduit \leftarrow TemplateMinuties$
end

La figure 4.3 montre quelques exemples de template réduit avec cette méthode :



(a) (b) (c)

FIGURE 4.3 – Exemples de réduction de template avec la méthode troncature : (a) est le template initial avec les minuties extraites de l'image, les minuties en rouge sont conservées dans le template réduit avec (b) nbrMinutieAttendues = 30 et (c) nbrMinutieAttendues = 46.

4.2.2 Barycentre

Cette méthode est basée sur un mécanisme d'élagage. Cette approche est simple et rapide (quelques millisecondes de calcul). Le NIST a observé que les minuties les plus proches du Core de l'empreinte digitale sont les plus utilisées dans le processus de comparaison [99]. Pour le template d'empreinte digitale, en général le point Core

est inconnu mais le centroïde du template de minuties en est, en général, une bonne estimation. Cette approche de sélection de minuties tend à garder les minuties les plus proches du centroïde. Nous avons cinq étapes présentées dans l'algorithme 2 pour cette méthode.

Algorithm 2: Algorithme pour la méthode barycentre

Result: TemplateReduit
Input : TemplateMinuties
Input : nbrMinutieAttendues

$n \leftarrow nbrMinutieAttendues$
$m \leftarrow size(TemplateMinuties)$
if $m > n$ **then**
  $centroide \leftarrow calculCentroide(TemplateMinuties)$
  $dist \leftarrow DistanceEuclidienne(TemplateMinuties, centroide)$
  $TemplateOrdonn \leftarrow OrdreCroissant(TemplateMinuties, dist)$
  $TemplateReduit \leftarrow TemplateOrdonne(1$ **to** $nbrMinutieAttendues)$
  $TemplateReduit \leftarrow OrdreCroissantX(TemplateReduit)$
else
  $TemplateReduit \leftarrow TemplateMinuties$
end

Concernant la méthode `calculCentroide`, l'équation 4.1 nous permet de calculer le centroïde du template de minuties contenant N_j minuties. Nous obtenons ainsi un centroïde ayant une position (X_c, Y_c).

$$(X_c, Y_c) = \frac{1}{N_j}(\sum_{i=1}^{N_j} X_i, \sum_{i=1}^{N_j} Y_i) \tag{4.1}$$

La méthode `DistanceEuclidienne` permet de calculer la distance euclidienne entre les minuties du template et le centroïde. L'équation 4.2, nous donne en retour la distance d'une minutie M_i au centroïde C.

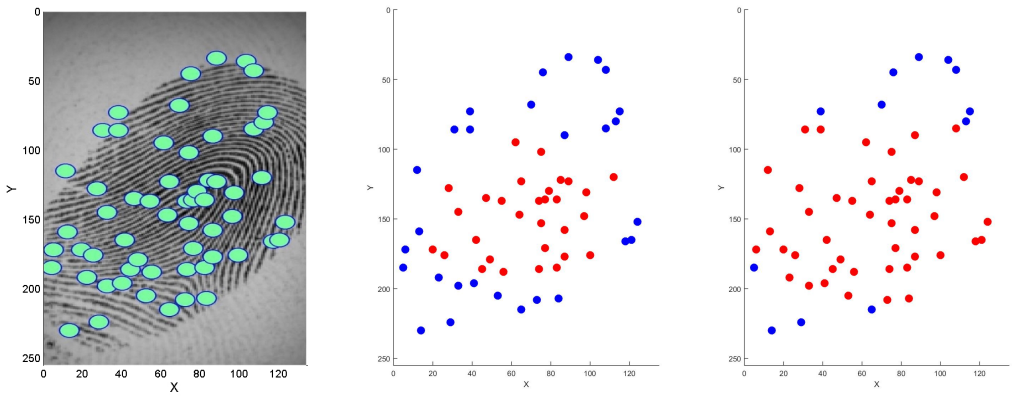
$$d_i(M_i, C) = \sqrt{(X_i - X_c)^2 + (Y_i - Y_c)^2}, \forall\ i = 1 : N_j \tag{4.2}$$

Quant à la méthode `OrdreCroissant`, elle permet d'ordonner par ordre ascendant

les minuties suivant la distance $d_i,\ i = 1 : N_j$.

La dernière méthode `OrdreCroissantX` permet de ré-ordonner les minuties suivant l'élément X, cela est nécessaire car un template ISO Compact Card II est constitué de cette manière. Elle sera utilisée pour toutes les méthodes développées et présentées ci-après.

La figure 4.4 montre quelques exemples de template réduit avec cette méthode.



(a) (b) (c)

FIGURE 4.4 – Exemples de réduction de template avec la méthode barycentre : (a) est le template initial avec les minuties extraites de l'image, les minuties en rouge sont conservées dans le template réduit avec (b) nbrMinutieAttendues = 30 et (c) nbrMinutieAttendues = 46.

Ces deux méthodes de l'état de l'art ont été testées et éprouvées, mais il est possible d'obtenir de meilleures performances.

4.3 Méthodes proposées

Nous proposons de catégoriser les nouvelles méthodes suivant leurs modes de fonctionnement répartis en quatre catégories :

— Non-incrémental avec centroïde
— Non-incrémental avec distribution
— Incrémental avec centroïde
— Incrémental avec distribution

4.3.1 Non-incrémental avec centroïde

Nous proposons une méthode non-incrémental avec centroïde nommée Median Y.

Méthode Median Y

La méthode Median Y suit le même schéma que la méthode barycentre mais en utilisant seulement l'information présente sur l'élément Y du template de minuties. L'algorithme 3 compte cinq étapes implémentant cette méthode.

Algorithm 3: Algorithme pour la méthode Median Y

Result: TemplateReduit
Input : TemplateMinuties
Input : nbrMinutieAttendues

$n \leftarrow nbrMinutieAttendues$
$m \leftarrow size(TemplateMinuties)$
if $m > n$ **then**
  $Mediane(Y_m) \leftarrow calculMediane(TemplateMinuties)$
  $dist \leftarrow DistanceEuclidienneY(TemplateMinuties, Y_m)$
  $TemplateOrdonnY \leftarrow OrdreCroissant(TemplateMinuties, dist)$
  $TemplateReduit \leftarrow TemplateOrdonneY(1$ **to** $nbrMinutieAttendues)$
  $TemplateReduit \leftarrow OrdreCroissantX(TemplateReduit)$
else
  $TemplateReduit \leftarrow TemplateMinuties$
end

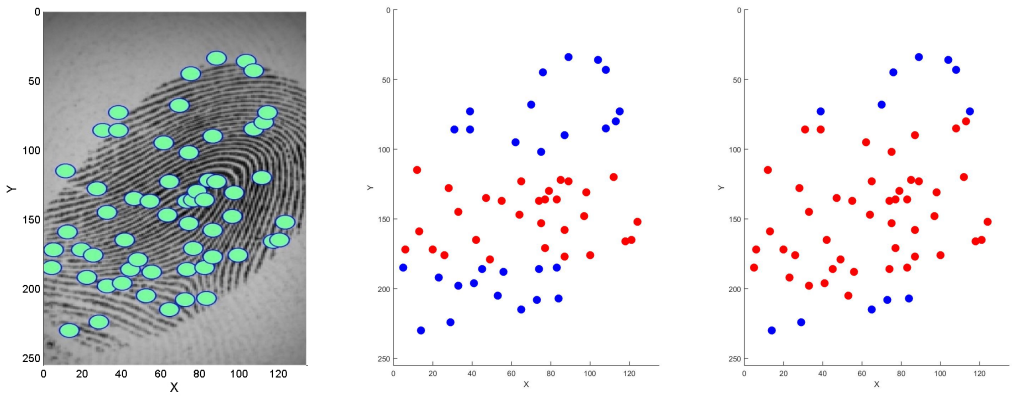
Dans la méthode `calculMediane`, l'équation 4.3 nous permet de calculer la valeur médiane du template sur l'élément Y du template initial.

$$Mediane(Y_m) = \frac{1}{N_j}(\sum_{i=1}^{N_j} Y_i) \tag{4.3}$$

La méthode `DistanceEuclidienneY` calcule grâce à l'équation 4.4 la distance euclidienne entre le template de minutie et la valeur médiane Y_m.

$$d_i(Y_i, Y_m) = \sqrt{(Y_i - Y_M)^2}, \forall\ i = 1 : N_j \tag{4.4}$$

La figure 4.5 présente quelques exemples de template réduit avec cette méthode.



(a) (b) (c)

FIGURE 4.5 – Exemples de réduction de template avec la méthode Median Y : (a) est le template initial avec les minuties extraites de l'image, les minuties en rouge sont conservées dans le template réduit avec (b) nbrMinutieAttendues = 30 et (c) nbrMinutieAttendues = 46.

4.3.2 Non-incremental avec distribution

Deux méthodes de type non-incrémental avec distribution sont proposées, la méthode Trancature Random Permutation ainsi que la méthode K-Means.

4.3.2.1 Méthode Troncature Random Permutation

Cette méthode est basée sur une permutation aléatoire du template initial et seulement les N_{max} premières minuties sont conservées. Contrairement aux méthodes précédemment présentées, qui ont toutes les minuties dans une même zone, nous souhaitons avec cette méthode, avoir une répartition des minuties dans le template initial. Nous souhaitons ainsi déterminer si le fait d'avoir des minuties à différentes places dans le template réduit est important ou non.

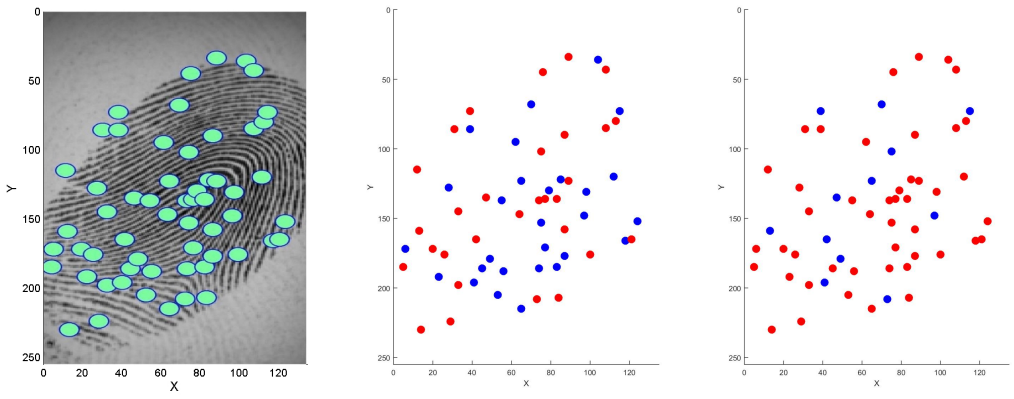
La méthode `randPerm(m)`, permet de générer m nombres aléatoires compris entre un et le nombre de minuties du template initial. Cela nous permet d'avoir un tirage de n minuties parmis m minuties du template inital. Chaque minutie possède la même probabilité d'être sélectionnée.

Algorithm 4: Algorithme pour la méthode TroncRandPerm

Result: TemplateReduit
Input : TemplateMinuties
Input : nbrMinutieAttendues

$n \leftarrow nbrMinutieAttendues$
$m \leftarrow size(TemplateMinuties)$
if $m > n$ **then**
    $random \leftarrow randPerm(m)$
    $TemplateReduit \leftarrow TemplateMinuties(random(1$ **to** $nbrMinutieAttendues))$
    $TemplateReduit \leftarrow OrdreCroissantX(TemplateReduit)$
else
    $TemplateReduit \leftarrow TemplateMinuties$
end

Voici quelques exemples de template réduit avec cette méthode :



(a) (b) (c)

FIGURE 4.6 – Exemples de réduction de template avec la méthode Troncature Random Permutation : (a) est le template initial avec les minuties extraites de l'image, les minuties en rouge sont conservées dans le template réduit avec (b) nbrMinutieAttendues = 30 et (c) nbrMinutieAttendues = 46.

4.3.2.2 Méthode K-Means

La méthode utilisée et basée sur l'exploitation de l'algorithme de Fuzzy C-Means (FCM)[100], qui est un classifieur automatique de données bien connu. Dans notre

cas d'usage, cette méthode prend en paramètres le template de minuties et le nombre de classes que l'on souhaite, c'est-à-dire, le nombre de minuties souhaité. En retour, nous avons le point central de chaque classe à partir duquel, nous cherchons la minutie la plus proche de ce point. L'algorithme 5 présente les trois étapes permettant d'effectuer cette réduction de template.

Algorithm 5: Algorithme pour la méthode K-Means

Result: TemplateReduit
Input : TemplateMinuties
Input : nbrMinutieAttendues

$n \leftarrow nbrMinutieAttendues$
$m \leftarrow size(TemplateMinuties)$
if $m > n$ **then**
    $CentroideCluster \leftarrow FCM(TemplateMinuties, n)$
    $TemplateReduit \leftarrow$
     $MinutieProcheCluster(TemplateMinuties, CentroideCluster))$
    $TemplateReduit \leftarrow OrdreCroissantX(TemplateReduit)$
else
    $TemplateReduit \leftarrow TemplateMinuties$
end

La méthode `FCM`, se décompose en deux parties, la phase d'initialisation et la phase de traitement. Trois étapes du traitement sont répétées tant que le nombre de classes n'est pas atteint.

— Initialisation

1. Prendre un point aléatoirement pour être le centroïde de la première classe $C1$
2. Prendre un autre point avec la plus grande distance du centroïde $C1$ pour qu'il devienne le centroïde de la seconde classe $C2$

— Traitement

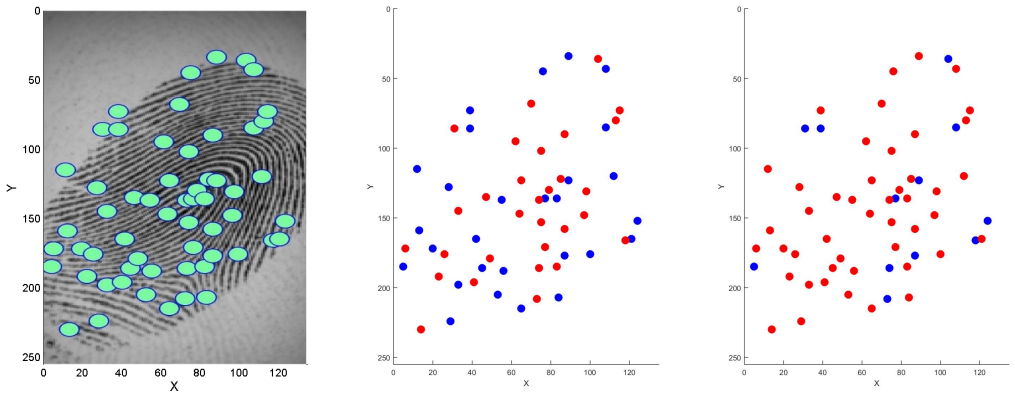
1. Calcul de la distance de chaque point avec les centroïdes des classes (ex : $C1$ et $C2$)
2. Classement dans chaque classe des points avec la plus petite distance par rapport aux centroïdes des classes.
3. Prendre un nouveau point comme nouveau centroïde Cx avec une grande distance par rapport aux autres centroïdes des classes.

4. Répéter les trois étapes jusqu'à obtenir le bon nombre de classes.

La méthode `MinutieProcheCluster` nous retourne les minuties les plus proches des centroïdes des classes retournées par la méthode `FCM`.

Nous avons essayé cette méthode car K-Means permet une bonne répartition spatiale des minuties. Nous avons de forte chance de sélectionner d'autres minuties que par les méthodes précédentes.

Voici quelques exemples de template réduit avec cette méthode présenté dans la figure 4.7.



(a) (b) (c)

FIGURE 4.7 – Exemples de réduction de template avec la méthode K-Means : (a) est le template initial avec les minuties extraites de l'image, les minuties en rouge sont conservées dans le template réduit avec (b) nbrMinutieAttendues = 30 et (c) nbrMinutieAttendues = 46.

4.3.3 Incremental avec centroïde

Une méthode incrémental avec centroïde nommée Barycentre évolutif est proposée.

Méthode Barycentre évolutif

Cette méthode est basée sur la sélection combinée avec la méthode Barycentre du NIST. L'algorithme 6 montre les différentes étapes de cette méthode.

Algorithm 6: Algorithme pour la méthode barycentre Évolutif

Result: TemplateReduit
Input : TemplateMinuties
Input : nbrMinutieAttendues

$n \leftarrow nbrMinutieAttendues$
$m \leftarrow size(TemplateMinuties)$
$temp \leftarrow TemplateMinuties$
if $m > n$ **then**
  while $taille(temp) > n$ **do**
    $centroide \leftarrow calculCentroide(temp)$
    $dist \leftarrow DistanceEuclidienne(temp, centroide)$
    $TemplateOrdonne \leftarrow OrdreCroissant(temp, dist)$
    $temp \leftarrow TemplateOrdonne(1$ **to** $size(temp) - 1)$
  end
  $TemplateReduit \leftarrow OrdreCroissantX(temp)$
else
  $TemplateReduit \leftarrow TemplateMinuties$
end

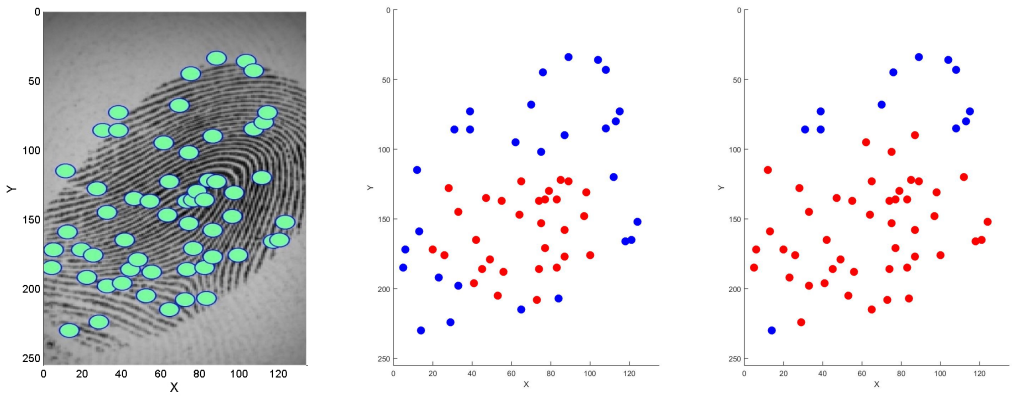
Ce sont exactement les mêmes méthodes que pour barycentre, le seul élément qui diffère est la suppression de la minutie la plus éloignée du barycentre et de répéter les différentes étapes jusqu'à obtenir la taille du template souhaité. La figure 4.8 montre quelques exemples de réduction de template avec cette méthode.

4.4 Résultats expérimentaux

Pour évaluer la performance des méthodes de réduction, nous devons effectuer certains choix concernant les bases de données biométriques, l'extracteur de minuties, les algorithmes de comparaison et les métriques d'évaluation de performance. Nous détaillons tous ces aspects dans les parties suivantes.

4.4.1 Les bases de données

Dans cette étude, nous avons utilisé trois bases de données d'empreintes digitales composées de 800 images provenant de 100 individus avec 8 échantillons pour chaque utilisateur :



(a) (b) (c)

FIGURE 4.8 – Exemples de réduction de template avec la méthode barycentre évolutif : (a) est le template initial avec les minuties extraites de l'image, les minuties en rouge sont conservées dans le template réduit avec (b) nbrMinutieAttendues = 30 et (c) nbrMinutieAttendues = 46.

— Base de données de référence FVC2002 DB2[101] : la résolution de l'image est 296 × 560 pixels avec un capteur optique "FX2000" par Biometrika. Cette base de données a été utilisée durant la compétition (Fingerprint Verification Competition) en 2002.
— Base de données de référence FVC2004 DB1[102] : la résolution de l'image est 640 × 480 pixels avec un capteur optique "V300" par CrossMatch ;
— Base de données de référence FVC2004 DB2[103] : la résolution de l'image est 328 × 364 pixels avec un capeur optique "U.are.U 4000" par Digital Persona.

La figure 4.9 présente une empreinte digitale pour chaque base de données. Cela montre aussi la diversité des empreintes utilisées dans cette étude.

(a) (b) (c)

FIGURE 4.9 – Un exemple d'empreintes digitales provenant de chaque base de données utilisée : (a) la base de données FVC2002 DB2 (b) la base de données FVC2004 DB1 et (c) la base de données FVC2004 DB2.

La figure 4.10 montre la répartition du nombres de minuties présentes dans chacun des templates biométriques constituant chacune des bases de données biométriques utilisées. Nous remarquons que le nombre de minuties n'est pas identique entre les bases, même si en moyenne elles sont proches. Sur FVC2002DB2 le nombre moyen de minuties est de 54, pour FVC2004DB1 48 et 43 pour FVC2004DB2. De plus, nous remarquons que le nombre de minuties peut être supérieur à 80 voir même 100, ce qui est supérieur à la taille maximale acceptée par l'élément sécurisé. C'est pourquoi nous devons réduire la taille de ces templates.

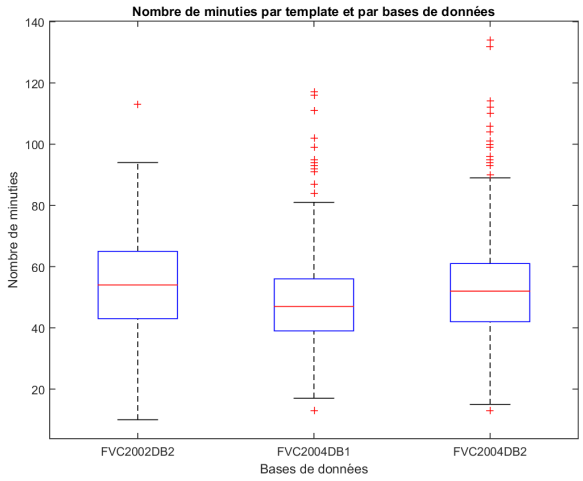


FIGURE 4.10 – Répartition du nombre de minuties présentes dans chaque template par base de données par des boîtes à moustaches

4.4.2 Extracteur de minuties

Les templates de minuties utilisés dans l'expérimentation ont été extraits à l'aide de l'outil NBIS et plus spécialement MINDTCT [104] du NIST. Nous avons utilisé cet extracteur car il est très largement utilisé dans la recherche académique.

4.4.3 Les algorithmes de comparaison

Dans cette étude, nous avons utilisé deux algorithmes de comparaison issus de la recherche et un provenant de l'industrie :

— **Bozorth3** [104] : Cet algorithme de comparaison utilise seulement les emplacements et l'orientation des minuties pour faire correspondre les empreintes digitales. Nous obtenons en sortie de l'algorithme un score de similarité.

— **Minutia Cylinder-Code (MCC) algorithm** [105] : la représentation de MCC associe une structure locale à chaque minutie. Cette structure contient les relations spatiales et directionnelles entre la minutie et son voisinage (rayon fixe). Chaque structure est invariante en translation, rotation, aux distorsions ainsi qu'aux petites erreurs d'extraction de caractéristiques. Une double mesure de similarité est calculée et consolidée pour fournir un score global de la comparaison.

— **OCC commercial** : Nous n'avons pas d'information sur le fonctionnement de cet algorithme. Nous émettons l'hypothèse qu'un OCC commercial a des performances élevées. En sortie de l'algorithme, nous n'avons pas un score mais simplement une information de type « Accepté » ou « Refusé » pour éviter des attaques.

4.4.4 Méthode de référence

La méthode de référence correspond à la pseudo-vérité terrain permettant d'avoir la performance dans le cas idéal, qui correspond à celui où l'on dispose de toutes les minuties. L'objectif étant de sélectionner les méthodes qui minimisent l'écart à cette valeur dite de référence. Tous les résultats obtenus avec les méthodes décrites précédemment sont comparés avec les résultats obtenus par cette méthode dite de référence. On émet l'hypothèse que les résultats obtenus seront moins bons que la méthode de référence, avoir plus de minuties permet de meilleurs résultats.

4.4.5 Métriques d'évaluation

Parmi toutes les méthodes présentées en section 2.5.1.4, nous avons utilisé la courbe DET (Detection Error Tradeoff) [96]. Cette courbe montre le taux de fausses acceptations (FMR), acceptation à tort d'un utilisateur, sur l'axe des abscisses en fonction du taux de faux rejets (FNMR), rejet d'un bon utilisateur, sur l'axe des ordonnées tracées de façon paramétrique en fonction du seuil de décision. La mesure associée est appelée AUC et est souvent considérée comme un critère global de performance. Nous utilisons cette valeur pour quantifier l'efficacité d'une méthode de sélection de minuties. L'intervalle de confiance (CI) sera calculé. Nous utilisons également la valeur du taux d'erreur égale (EER) pour avoir un point de fonctionnement du système.

4.4.6 Évaluation des méthodes

Pour évaluer les méthodes, nous allons utiliser deux critères qui sont le temps de réduction du template ainsi que les performances obtenues par les métriques précédentes. Dans notre contexte d'utilisation de la biométrie avec un élément sécurisé, le temps est aussi un élément important à considérer lors de l'évaluation des méthodes. Une transaction devant être réalisée en moins de 500 ms, nous devons avoir une méthode qui soit à la fois efficace et rapide.

Tous les calculs ont été fait sous Matlab avec un ordinateur de type PC ayant un processeur Intel Core I7 à 4 coeurs avec une fréquence de 2.8GHz et 16 GO de RAM.

4.4.6.1 Temps de réduction du template

Dans cette section, nous présentons le temps de traitement pour générer un template réduit pour chaque méthode. La tableau 4.1 présente les temps moyens pour chaque méthode sur toutes les bases de données. Cela permet d'observer, par exemple, que la méthode K-Means est environ 300 fois plus lente que la méthode troncature. Cet indicateur est un critère important, tout comme la performance, de sélection d'une méthode de réduction de template biométrique, tant pour les systèmes commerciaux que pour les usages.

N_{max}	30	34	38	42	46	50
Troncature	7.9 ms	7.6 ms	7.4 ms	7.2 ms	7 ms	6.8 ms
Troncat Rand Perm	20.7 ms	19.9 ms	18.9 ms	17.4 ms	16.5 ms	14.6 ms
Barycentre	476 ms	409 ms	376 ms	364 ms	301 ms	244 ms
Barycentre évolutif	5387 ms	4747 ms	3988 ms	3435 ms	2789 ms	2206 ms
K-Means	24349 ms	24047 ms	22783 ms	20569 ms	18298 ms	15473 ms
Median Y	171 ms	164 ms	193 ms	186 ms	189 ms	196 ms

TABLE 4.1 – Temps moyen pour toutes les tailles de minuties et toutes les méthodes

Si nous ne prenons que le temps en compte, il n'y a que quatre méthodes qui ont un temps de traitement inférieur à 500 ms, les deux méthodes de l'état de l'art Troncature et Barycentre ainsi que deux méthodes proposées Troncature Random Permutation et Median Y. Les méthodes Barycentre Evolutif et K-Means quant à elles sont nettement au delà des 500 ms, ce qui n'est pas acceptable pour un traitement normal. Cependant, ces méthodes peuvent être utilisées lors de la phase d'enrôlement qui, elle, permet un temps de réduction plus long.

4.4.6.2 Construction de la vérité terrain

Pour toutes les bases de données, nous calculons les valeurs de l'aire sous la courbe (AUC), l'intervalle de confiance (CI) pour chaque méthode de sélection avec N_{max} variant de 30 à 50 par pas de 4. Le tableau 4.2 présente la valeur de l'AUC pour chaque base de données pour le template original comme référence pour les comparaisons dans notre étude. Nous observons que les algorithmes de comparaison du NIST ainsi que MCC ont une bien moins bonne performance que l'OCC commercial. Ceci était attendu, les algorithmes commerciaux se doivent d'avoir de très bonnes performances car ils sont utilisés pour contrôler l'accès à des zones sécuritaires ou pour du paiement. De plus, nous constatons que la performance diffère entre la première base et les deux autres. Cela est peut-être dû à la résolution des images de la base FVC2002DB2 qui ont une taille d'image inférieure aux deux autres. Nous supposons que les extracteurs ont plus de difficultés à extraire les minuties de ces images. Mais après avoir réduit la taille des images de la base FVC2004DB1, et extrait de nouveau les minuties, nous nous sommes aperçu que les performances étaient les mêmes qu'avant la réduction. La taille de l'image n'a donc pas d'incidence dans notre cas pour expliquer les performances. Ceci montre l'incidence non négligeable de l'association entre algorithme et bases de données sur les performances du système.

Algorithme de comparaison	Bozorth	MCC	OCC commercial
FVC2002DB2	14% ± .14	10% ± .28	0.04% ± .06
FVC2004DB1	11.1% ± .18	18.4% ± .17	3.77% ± .09
FVC2004DB2	11.1% ± .09	18.9% ± .12	3.68% ± .07

TABLE 4.2 – Valeurs de l'AUC pour les trois bases de données avec Bozorth, MCC et l'OCC commercial

Les résultats sur l'algorithme MCC sont élevés en comparaison à ceux présentés dans [105] sur la base FVC2006 avec 6% d'AUC. Cette différence de performance peut être expliquée par l'évolution de la résolution des images produites par les capteurs, ainsi qu'une meilleure détection des minuties présentes sur l'image. Nous verrons dans le chapitre suivant que MCC a de très bonnes performances sur d'autres types de bases de données. Ces valeurs serviront de pseudo-vérités terrain pour comparer les différentes méthodes de réduction.

4.4.6.3 Algorithme de comparaison Bozorth

Les tableaux 4.3, 4.4 et 4.5 présentent les valeurs de l'AUC pour chaque méthode de réduction de minuties testée pour les bases de données FVC2002DB2, FVC2004DB1 et FVC2004DB2 selon différentes valeurs $N_{\max}$ du nombre de minuties

sélectionné. L'objectif étant d'avoir une valeur AUC la plus petite possible. Nous pouvons noter que la méthode de réduction K-Means donne le meilleur résultat dans la majorité des cas. Concernant la base de données FVC2002DB2, la majorité des méthodes de réduction permettent d'obtenir de meilleures performances comparées au template initial (Tableau 4.2). A l'opposé, pour la base de données FVC2004DB1 et FVC2004DB2, le template initial fournit souvent le meilleur résultat.

N_{max}	30	34	38	42	46	50
Troncature (%)	12.2±.28	12.2±.2	10.6±.14	9.84±.11	10.3±.07	11.3±.05
Troncat Rand Perm (%)	10.0±.33	10.1±.19	8.22±.14	8.06±.09	8.67±.08	**9.55**±.06
Barycentre (%)	9.1±.31	9.87±.2	10.1±.15	10.3±.10	11.1±.07	12.0±.04
Barycentre évolutif (%)	12.8±.29	12.5±.21	12.6±.16	11.4±.13	12.0±.07	12.5±.05
K-Means (%)	**7.67**±.24	**9.44**±.18	**7.86**±.11	**7.14**±.07	**7.63**±.05	10.07±.03
Median Y (%)	11.1±.30	11.3±.22	11.2±.17	10.9±.13	11±.09	11.4±.07

TABLE 4.3 – Valeurs en pourcentage de l'AUC avec l'IC pour différentes valeurs $N_{\max}$ de minuties pour FVC2002DB2 avec Bozorth

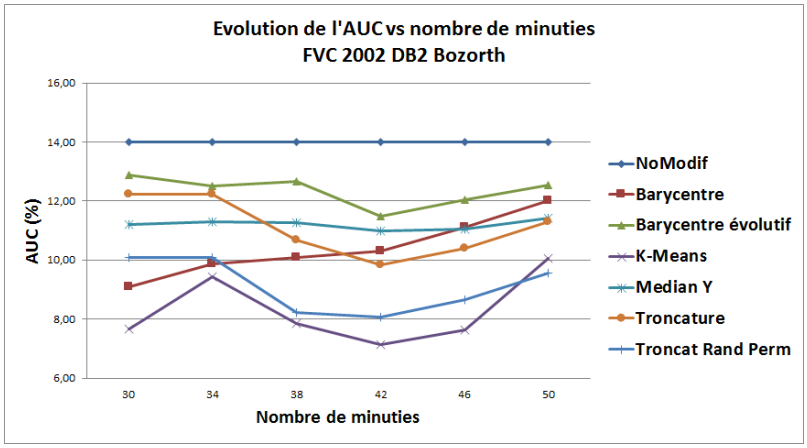
N_{max}	30	34	38	42	46	50
Troncature (%)	20.5±.24	18.8±.2	16.5±.18	15.3±.13	13.8±.09	13.1±.04
Troncat Rand Perm (%)	18±.29	16.6±.25	15.5±.21	13.2±.13	12.6±.09	12±.5
Barycentre (%)	20±.28	17.3±.22	15.5±.17	13.4±.15	12.4±.06	11.8±.04
Barycentre évolutif (%)	20.8±.26	19.4±.18	16.5±.14	14.5±.11	12.9±.07	12.2±.05
K-Means (%)	**15.7**±.20	**15.2**±.17	**14.2**±15	**12.9**±.10	**12.2**±.05	**11.4**±.03
Median Y (%)	21.3±.27	19.1±.23	16.7±.19	14.4±.16	13±.08	11.9±.05

TABLE 4.4 – Valeurs en pourcentage de l'AUC avec l'IC pour différentes valeurs $N_{\max}$ de minuties pour FVC2004DB1 avec Bozorth

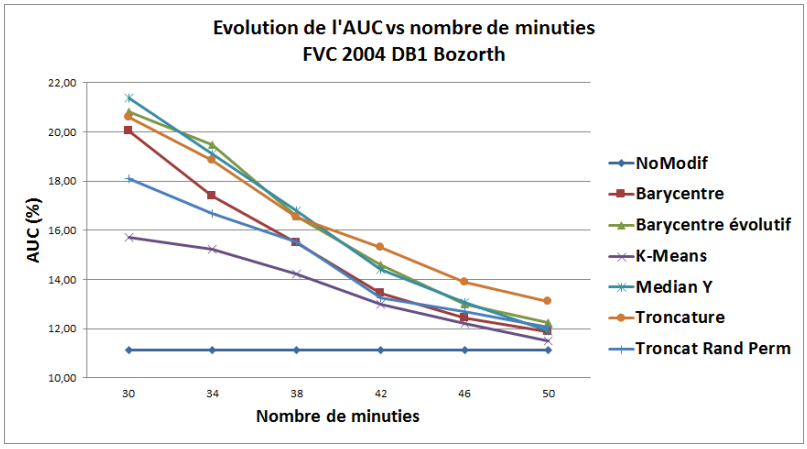
N_{max}	30	34	38	42	46	50
Troncature (%)	20.6±.20	18.7±.17	16.7±.15	15.4±.12	13.8±.09	13±.06
Troncat Rand Perm (%)	17.5±.29	16.5±.18	15.2±.13	13.6±.11	12.5±.08	11.8±.05
Barycentre (%)	19.9±.18	17.3±.15	15.4±.12	13.4±.10	12.2±.10	11.7±.08
Barycentre évolutif (%)	20.8±.19	19.3±.16	16.6±.13	14.7±.11	12.9±.09	12.1±.05
K-Means (%)	**16.7**±.16	**15**±.14	**14.4**±.11	**13.1**±.09	**12.1**±.07	**11.3**±.03
Median Y (%)	21.4±.17	18.9±.17	16.8±.16	14.5±.10	13±08	11.8±.039

TABLE 4.5 – Valeurs en pourcentage de l'AUC avec l'IC pour différentes valeurs $N_{\max}$ de minuties pour FVC2004DB2 avec Bozorth

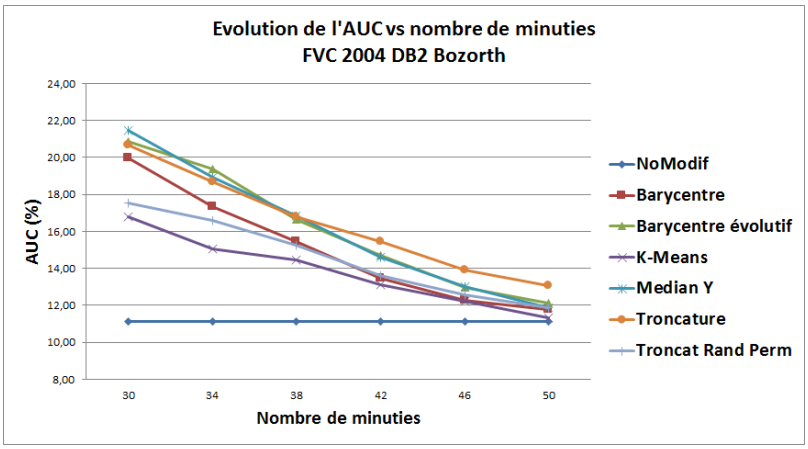
La figure 4.11(a) présente les valeurs de l'AUC pour la base de données FVC2002DB2. Dans ce cas, toutes les méthodes de réduction améliorent les performances par rapport aux performances obtenues en utilisant le template initial. La méthode de réduction K-Means quant à elle reste la meilleure quel que soit le nombre de minuties souhaité



(a) FVC2002DB2



(b) FVC2004DB1



(c) FVC2004DB2

FIGURE 4.11 – Évolution de l'AUC pour les trois bases de données en fonction de la méthode de réduction des minuties pour Bozorth

sauf pour $N_{max} = 50$. La figure 4.11(b) présente les mêmes résultats pour la base de données FVC2004DB1. Sur cette base, la meilleure performance est obtenue en utilisant le template initial. Cela montre que la réduction fait décroître les performances du système, ce qui valide notre hypothèse initiale. Les meilleures performances sont obtenues avec les méthodes K-Means, barycentre et troncature avec permutation aléatoire. Nous pouvons observer les mêmes tendances sur la figure 4.11(c) portant sur la base de données FVC2004DB2, toutes les méthodes de réduction ont une valeur AUC supérieure à celle obtenue en ne considérant que le template initial et nous observons que la méthode avec le plus bas AUC reste la méthode K-Means.

Pour essayer de comprendre les résultats obtenus sur la base FVC2002DB2, nous avons analysé les images à partir desquelles les templates de minuties sont extraits. Nous avons pu observer que les images présentent des artefacts de captures précédentes, ce qui induit en erreur l'algorithme d'extraction de minuties, qui détecte de fausses minuties. La figure 4.12 illustre ce propos, nous remarquons que des minuties sont détectées sur des artefacts de capture précédente. Pour valider nos constatations, nous avons pris un échantillon de la base FVC2002DB2, 10 individus, et nous avons retiré à la main les minuties provenant d'artefacts dans le template original. Nous avons ensuite appliqué les différentes méthodes de sélection sur ces templates « nettoyés » des artefacts. Nous avons évalué ces nouveaux templates avec la même méthodologie que précédemment et nous observons que nous avons des performances dites « normales », c'est-à-dire que les méthodes de réduction détériorent la performance du système par rapport au template initial. Le tableau 4.6 montre les résultats obtenus pour trois méthodes de réduction et la figure 4.13 illustre ces résultats.

N_{max}	30	34	38	42	46	50
NoModif (%)	10.9	10.9	10.9	10.9	10.9	10.9
Troncature (%)	10.25	12.41	10.67	9.97	9.21	9.44
Barycentre (%)	11.77	14.3	9.65	9.3	9.22	9.81
K-Means (%)	13.79	15.07	11.28	9.13	8.59	9.45

TABLE 4.6 – Valeurs en pourcentage de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2002DB2 avec Bozorth pour validation de notre hypothèse

Ces résultats valident notre hypothèse sur le comportement « anormal » de la base FVC2002DB2. Il nous faudrait appliquer ce « nettoyage » sur tous les templates de la base FVC2002DB2 et relancer l'évaluation sur toutes les méthodes et sur tous les algorithmes.

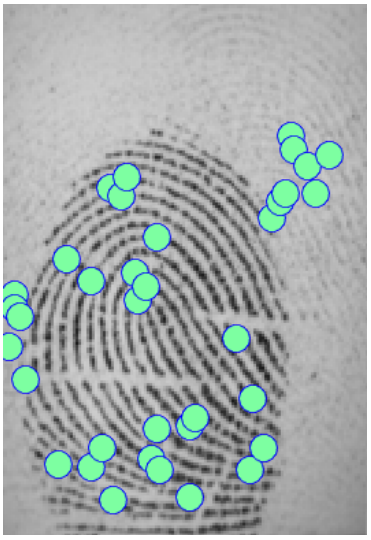


FIGURE 4.12 – Un exemple d'empreinte digitale avec des artefacts provenant de précédentes captures.

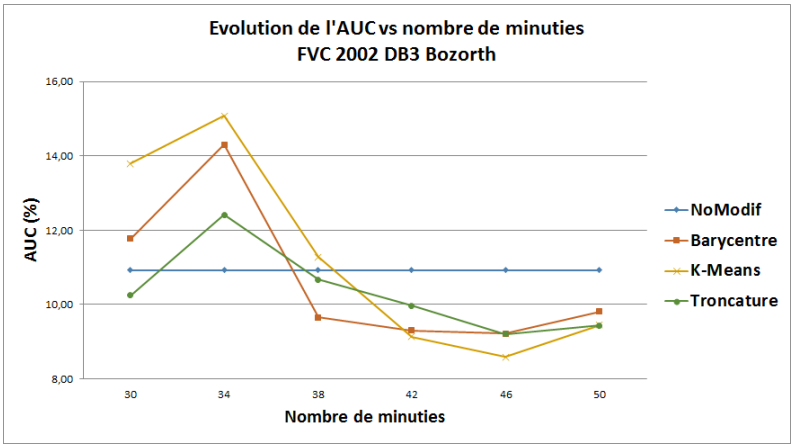


FIGURE 4.13 – Évolution de l'AUC pour les trois méthodes de réductions pour la validation de notre hypothèse pour l'algorithme Bozorth.

4.4.6.4 Algorithme de comparaison MCC

Les tableaux 4.7, 4.8 et 4.9 donnent les valeurs de l'AUC pour chaque méthode de réduction de minuties pour les bases de données FVC2002DB2, FVC2004DB1 et FVC2004DB2 pour l'algorithme MCC. Nous pouvons noter que la méthode de sélection K-Means donne le meilleur résultat dans la majorité des cas, sauf pour la base FVC2004DB2, mais les performances sont très proches des meilleures. Concernant les bases de données FVC2004DB1 et FVC2004DB2, les méthodes barycentre et troncature ont aussi de bonnes performances.

N_{max}	30	34	38	42	46	50
Troncature (%)	29.89±.48	24.51±.45	21.35±.40	17.46±.34	15.61±.32	14.34±.30
Troncat Rand Perm (%)	23.76±.46	21.15±.44	18.02±.35	16.51±.32	14.47±.26	13.43±.24
Barycentre (%)	21.7±.44	19.41±.39	17.7±.34	16.38±.32	14.81±.28	14.42±.26
Barycentre évolutif (%)	24.33±.46	22.87±.42	20.35±.38	18.73±.34	16.47±.33	16.06±.29
K-Means (%)	**19.2**±.42	**17.15**±.36	**14.82**±.34	**13.15**±.29	**13.4**±.25	**12.96**±.23
Median Y (%)	22.98±.44	20.99±.39	18.84±.36	16.11±.32	15.04±.26	15.04±.25

TABLE 4.7 – Valeurs de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2002DB2 avec l'algorithme MCC

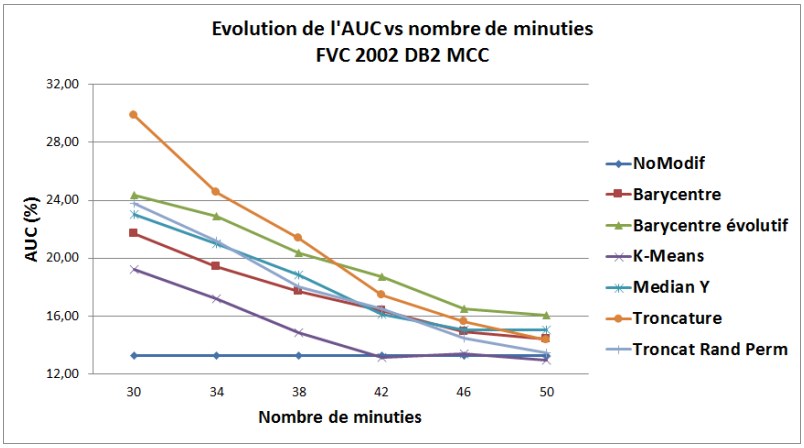
N_{max}	30	34	38	42	46	50
Troncature (%)	30.9±.44	26.6±.41	23.51±.38	21.48±.36	20.1±.35	19.33±.32
Troncat Rand Perm (%)	33.3±.38	30.13±.43	25.19±.40	24.09±.37	22.01±.34	20.7±.31
Barycentre (%)	24.04±.39	21.88±.36	19.55±.33	18.78±.33	18.49±.31	18.66±.30
Barycentre évolutif (%)	24.86±.39	21.82±.36	20.25±.34	19.69±.34	18.96±.33	18.98±.33
K-Means (%)	**23.7**±.38	**21.8**±.35	**18.85**±.33	**18.69**±.33	**18.4**±.31	**18.33**±.30
Median Y (%)	25.96±.4	23.53±.37	20.95±.35	19.18±.34	19.71±.33	19.17±.33

TABLE 4.8 – Valeurs de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2004DB1 avec l'algorithme MCC

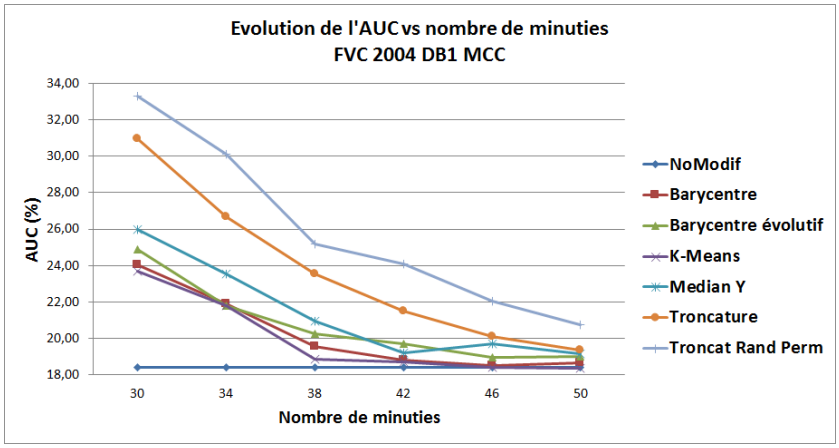
N_{max}	30	34	38	42	46	50
Troncature (%)	23.34±.43	21.85±.4	19.28±.36	19.54±.37	19.19±.36	19.5±.36
Troncat Rand Perm (%)	25.95±.46	24.67±.44	23.72±.43	21.91±.41	20.01±.4	20.6±.39
Barycentre (%)	**21.25**±.4	**20.66**±.39	19.62±.38	20.35±.39	19.93±.38	19.58±.37
Barycentre évolutif (%)	22.51±.41	21.45±.4	**19.06**±.36	**19.26**±.38	20.08±.38	19.25±.36
K-Means (%)	21.9±.4	21.22±.39	19.11±.38	19.27±.38	19.18±.36	19.08±.35
Median Y (%)	23.45±.42	21.35±.39	20.20±.39	19.29±.38	**19.03**±.36	**19.02**±.35

TABLE 4.9 – Valeurs de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2004DB2 avec l'algorithme MCC

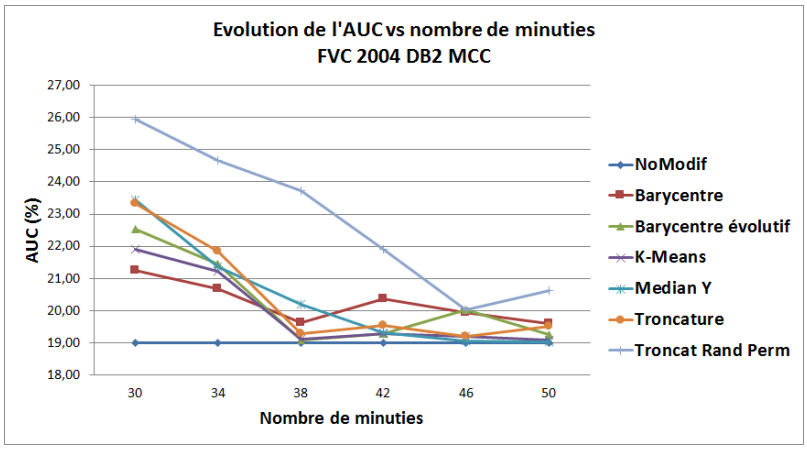
Pour toutes les bases de données, la meilleure performance est obtenue en utilisant le template initial. Cela veut dire que la réduction diminue la performance, ce qui est attendu. La figure 4.14(a) présente les valeurs de l'AUC pour la base de données FVC2002DB2. Dans ce cas, nous obtenons de bonnes performances avec une valeur d'AUC assez basse. La figure 4.14(b) présente les mêmes résultats sur la base de données FVC2004DB1. Pour ces deux bases, la méthode de sélection K-Means reste la meilleure, avec un AUC assez proche de celui obtenu avec le template initial. Par contre sur la base de données FVC2004DB2, comme le montre la figure 4.14(c), les méthodes Barycentre, Barycentre évolutif et Median Y permettent d'obtenir les meilleures performances. Toutes les méthodes de sélection produisent un AUC élevé comparé au template initial, mais nous observons d'une manière générale que la méthode avec un AUC bas est majoritairement K-Means, malgré que Barycentre et Barycentre évolutif et Median Y aient quelques bons résultats pour certains nombres



(a) FVC2002DB2



(b) FVC2004DB1



(c) FVC2004DB2

FIGURE 4.14 – Évolution de l'AUC pour les trois bases de données en fonction de la méthode de réduction des minuties pour MCC

de minuties dans le template réduit suivant la base de données utilisée.

4.4.6.5 OCC commercial

Les tableaux 4.10, 4.11 et 4.12 donnent les valeurs de l'AUC pour chaque méthode de réduction de minuties pour les bases de données FVC2002DB2, FVC2004DB1 et FVC2004DB2 pour l'algorithme OCC commercial. Une fois de plus, la méthode de sélection K-Means permet d'obtenir le meilleur résultat dans de nombreux cas, qu'importe la base de données utilisée. Cependant, sur les bases de données FVC2004DB1 et FVC2004DB2, les méthodes barycentre et barycentre évolutif ont aussi de bonnes performances avec un faible AUC.

N_{max}	30	34	38	42	46	50
Troncature (%)	2.54±.26	1.59±.23	1.36±.18	0.95±.13	0.83±.10	0.59±.09
Troncat Rand Perm (%)	3.64±.32	1.46±.21	0.77±.15	0.85±.11	0.34±.09	0.15±.05
Barycentre (%)	1.35±.22	0.84±.17	0.52±.14	0.31±.09	0.29±.08	0.28±.07
Barycentre évolutif (%)	3.99±.34	2.53±.27	1.72±.19	1.01±.15	0.55±.11	0.37±.09
K-Means (%)	**1.04**±.19	**0.61**±.15	**0.32**±.13	**0.17**±.09	**0.04**±.05	**0.08**±.03
Median Y (%)	1.72±.24	1.08±.19	0.87±.16	0.57±.10	0.46±.09	0.44±.08

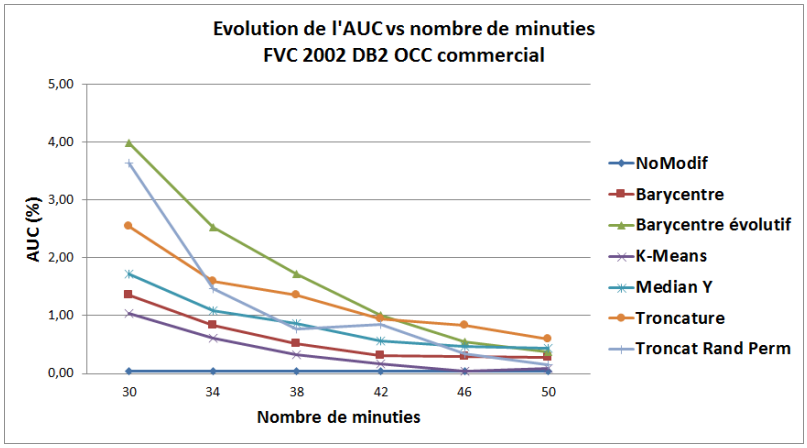
TABLE 4.10 – Valeurs de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2002DB2 avec l'OCC commercial

N_{max}	30	34	38	42	46	50
Troncature (%)	12.1±.24	9.47±.23	8.18±.21	6.61±.17	5.95±.12	5.12±.08
Troncat Rand Perm (%)	13.5±.29	11.7±.26	8.64±.17	6.22±.14	5.35±.09	5.06±.06
Barycentre (%)	7.62±.23	7.05±.21	**5.43**±.14	**4.85**±.11	4.34±.07	4.09±.04
Barycentre évolutif (%)	8.96±.24	7.28±.21	6±.18	5.16±.13	**4.19**±.07	4.19±.04
K-Means (%)	**7.21**±.22	**6.76**±.20	5.78±.15	5.12±.13	4.26±.08	**4.04**±.04
Median Y (%)	9.27±.25	7.76±.23	6.48±.19	5.46±.14	4.55±.09	4.29±.07

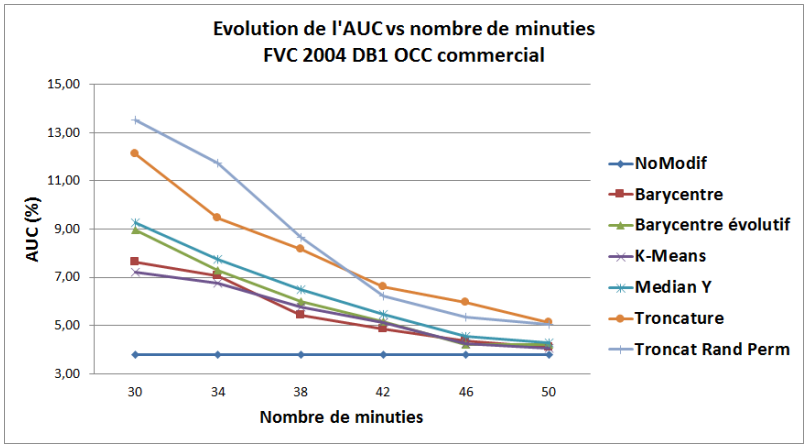
TABLE 4.11 – Valeurs de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2004DB1 avec l'OCC commercial

N_{max}	30	34	38	42	46	50
Troncature (%)	8.44±.24	7.21±.19	5.92±.13	5.28±.11	4.47±.08	4.3±.05
Troncat Rand Perm (%)	13±.29	11±.24	8.49±.18	6.51±.12	5.59±.09	4.78±.04
Barycentre (%)	**7.61**±.23	7.17±.19	**5.42**±.13	4.85±.08	4.31±.06	4.11±.03
Barycentre évolutif (%)	8.86±.24	7.45±.2	5.96±.14	5.13±.1	**4.23**±.07	4.17±.05
K-Means (%)	9.14±.28	**6.74**±.19	5.69±.14	**4.59**±.08	4.51±.06	**3.98**±.03
Median Y (%)	9.25±.26	7.89±.21	6.39±.15	5.38±.09	4.58±.04	4.23±.03

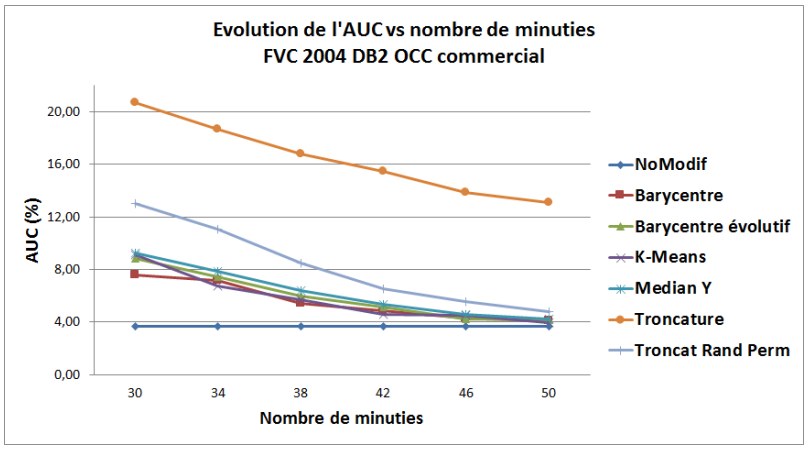
TABLE 4.12 – Valeurs de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2004DB2 avec l'OCC commercial



(a) FVC2002DB2



(b) FVC2004DB1



(c) FVC2004DB2

FIGURE 4.15 – Évolution de l'AUC pour les trois bases de données en fonction de la méthode de réduction des minuties pour l'OCC commercial

Pour toutes les bases de données, la meilleure performance est obtenue en utilisant le template initial. Comme précédemment, la réduction du template diminue la performance. La figure 4.15(a) présente les valeurs de l'AUC pour la base de données FVC2002DB2. Dans ce cas, nous obtenons de très bonnes performances avec une valeur d'AUC très basse mais nous avons un meilleur résultat avec le template intial. Sur cette base de données, qu'importe la taille de réduction, la méthode K-Means reste la meilleure avec en moyenne un AUC de 0.37%, ce qui reste assez proche de 0.04% obtenu avec le template initial. La figure 4.15(b) présente les mêmes résultats sur la base de données FVC2004DB1. Les méthodes de sélection K-Means, Barycentre et barycentre évolutif permettent d'obtenir les meilleurs résultats, avec un AUC moyen de 5.41% en comparaison au 3.77% d'AUC obtenu avec le template initial. La même tendance est constatée sur la base de données FVC2004DB2 comme le montre la figure 4.15(c). Toutes les méthodes de sélection produisent un AUC élevé comparé au template initial, mais nous observons d'une manière générale que la méthode avec un AUC bas est K-Means, bien que Barycentre et Barycentre évolutif aient quelques bons résultats pour certains nombres de minuties dans le template réduit suivant les bases de données utilisées.

4.4.7 Discussion

Nous venons d'évaluer les différentes méthodes de réduction de template biométrique en termes de temps de réduction ainsi que de performance. Nous remarquons qu'il y a un lien entre le temps de réduction et la performance. Si nous prenons l'exemple de la méthode Troncature de l'état de l'art, le temps de réduction du template est extrêmement rapide mais les performances sont moyennes quelle que soit la taille du template souhaité et pour tout algorithme de comparaison. A contrario, si l'on prend la méthode K-Means qui a un temps de réduction 3000 fois plus long que Troncature, les performances associées sont quant à elles 3 à 5% meilleures que la méthode Troncature. Nous remarquons aussi que les performances diffèrent pour les même bases de données biométriques suivant l'algorithme de comparaison utilisé ainsi que la taille du template souhaité. D'une manière générale, les performances sont les moins bonnes lorsque la réduction du template est la plus importante (30 minuties souhaitées) et augmente lorsque le template est le moins réduit, ce qui est attendu. Lorsque l'on souhaite stocker un template biométrique sur un élément sécurisé la taille moyenne constatée est de 38 minuties.

Le tableau 4.13 synthétise pour chacune des bases de données et les trois al-

	Bozorth	MCC	OCC Commercial
FVC2002DB2	K-Means	K-Means	K-Means
FVC2004DB1	K-Means	K-Means	K-Means Barycentre Barycentre évolutif
FVC2004DB2	K-Means	Barycentre Barycentre évolutif Median Y	K-Means Barycentre Barycentre évolutif

TABLE 4.13 – Résumé des meilleurs méthodes pour chacune des bases de données et chacun des algorithmes de comparaison utilisés pour toutes les valeurs de minuties.

gorithmes de comparaison la ou les meilleurs méthodes de réduction de template biométrique, d'après les résultats obtenus précédemment. Nous constatons, d'une manière générale, que la meilleure méthode est K-Means, même si les méthodes Barycentre, Barycentre évolutif et Median Y obtiennent de bonnes performances. La raison pour laquelle cette méthode est majoritairement meilleure vient sûrement du fait que K-Means permet de conserver une répartition des minuties. Les autres méthodes perdent beaucoup de minuties importantes et nécessaires pour l'algorithme de comparaison. Nous pouvons en déduire que des minuties intéressantes peuvent se situer loin du CORE. Une question reste cependant en suspend « Les méthodes proposées sont-elles loin du template réduit « optimal » ? ». La section suivante propose une méthode permettant d'approcher ce template dit « optimal ».

4.5 Réduction optimale - MRGA

Nous avons proposé la méthode MRGA (Minutiae Reduction Genetic Algorithm) permettant d'estimer la meilleure réduction possible pour un template de minuties. Étant donné un template contenant N minuties, nous souhaitons déterminer le template optimal réduit à N_{max} minuties. Pour déterminer ce template optimal, nous devrions tester $(C_{N_{max}})^N$ possibilités (nombre de combinaisons de N_{max} parmi N) ce qui n'est pas possible. A titre d'exemple, pour $N = 50$ et $N_{max} = 30$, il y a $4.7 * 10^{13}$ templates réduits possibles. La méthode proposée se base sur l'utilisation d'algorithme génétique (GA). Les algorithmes génétiques sont une méthode de recherche stochastique introduite dans les années 1970 par John Holland [106] et par Ingo Rechenberg [107]. Les algorithmes génétiques permettent de déterminer la valeur optimale d'un critère en simulant l'évolution d'une population jusqu'à la survie des meilleurs individus [108]. Les survivants sont obtenus par sélection, mutation ou croisement de la génération précédente. Nous pensons que l'utilisation des algorithmes génétiques est une bonne approche pour résoudre le problème

d'optimisation du template de minuties dans un temps raisonnable. Notre objectif est d'obtenir un template réduit ayant des performances proches du template original sur les algorithmes de comparaison.

4.5.1 Description de la méthode

Un algorithme génétique est défini par cinq éléments essentiels :

1. **Génotype** : il s'agit d'un ensemble de caractéristiques représentant chaque individu d'une population. Dans notre cas, la population initiale est constituée de 500 individus composés de N éléments, N étant le nombre de minuties souhaité dans le template biométrique réduit. Comme nous souhaitons obtenir un template avec des minuties présentes dans le template initial, la population sera constituée en effectuant des tirages aléatoires de N minuties dans le template initial contenant M minuties. La figure 4.16 nous montre sur la partie gauche le fonctionnement général d'un algorithme génétique et sur la partie droite, chaque élément le constituant.
2. **Population initiale** : elle est constituée par un ensemble d'individus tirés aléatoirement à partir du template original. Chaque individu est constitué de N éléments. Chaque élément correspond à une position unique d'une minutie présente dans le template original.
3. **Fonction d'évaluation** : Cet élément permet de mesurer la qualité d'un individu. Si nous prenons l'individu I1 pour l'évaluer par rapport au template original, nous obtenons un score S(I1). Notre fonction d'évaluation est l'algorithme de comparaison MCC, car il est rapide pour comparer deux templates biométriques et qu'il a de bonnes performances. Cet algorithme nous retourne un score de similarité entre les deux templates. Ce qui veut dire que plus le score de similarité est grand, plus l'individu testé est bon.
4. **Les opérations sur les génotypes** : les gènes de l'individu sont modifiés par l'utilisation de trois fonctionnalités :
   — sélection : les individus ne correspondant pas à l'environnement (dont le score n'est pas suffisant) ne sont pas sélectionnés. Pour ce faire, nous sélectionnons les individus nommés élites (les 5 individus ayant obtenus le meilleur score).
   — croisement : les gènes résultant du croisement de deux individus est une combinaison des gènes de ses parents. Pour obtenir l'individu résultant des individus I1 et I2, nous regardons les éléments présents chez les deux individus sans les doublons et sélectionnons de manière aléatoire les N

premiers éléments. Nous obtenons ainsi un individu (fils) mélangeant les gènes des deux individus (parents).
— mutation : une partie des gènes sont modifiés afin de s'adapter à l'environnement. Nous tirons aléatoirement un individu, puis nous croisons cet individu avec un individu élite. L'individu résultant Ir= mutation(I1) = croisement(I1,Ia) avec Ia un individu aléatoire. Ceci permet d'obtenir un individu ayant des gènes provenant d'un individu élite croisé avec des gènes d'un individu aléatoire.

5. **Terminaison** : il s'agit du critère de fin de l'évolution en fonction du score des individus ou du nombre de générations. Si un individu garde le même score durant 10 générations ou si 500 générations ont été réalisées, l'algorithme se termine.

Nous résumons ici la cinématique de l'exécution d'un algorithme génétique :

1. Définition de la population initiale
2. Évaluation des individus
3. Génération de la population suivante :
   — Sélection des 5 individus élites ;
   — 30% de la population (ici 150 individus) est obtenue par mutation des individus élites avec des individus aléatoires ;
   — 30% de la population (ici 150 individus) est obtenue par croisement des individus élites ;
   — Sélection d'individus aléatoires pour compléter la population de 500 individus.
4. Revenir à l'étape 2 si le critère d'arrêt n'est pas satisfait.

On considère une population P(t), à la génération t, est composée de 500 individus nommées Ii. La population va évoluer à la génération t+1. La figure 4.16, illustre les différentes étapes de l'algorithme génétique lors de l'utilisation de templates biométriques.

La nouvelle population est composée de nouveaux individus :
— I1 à I5 sont des individus de la génération précédente ;
— I6 à I155 sont les individus résultant de la mutation (I6 ... I155 = mutation(I2) avec m(Ii) = croisement(Ii, Ia) avec Ia un individu aléatoire) ;
— I156 à I305 sont les individus résultant du croisement (I156 ... I305 = croisement(I1,I4) ... croisement(I2,I3) ;
— I306 à I500 sont des individus aléatoires.

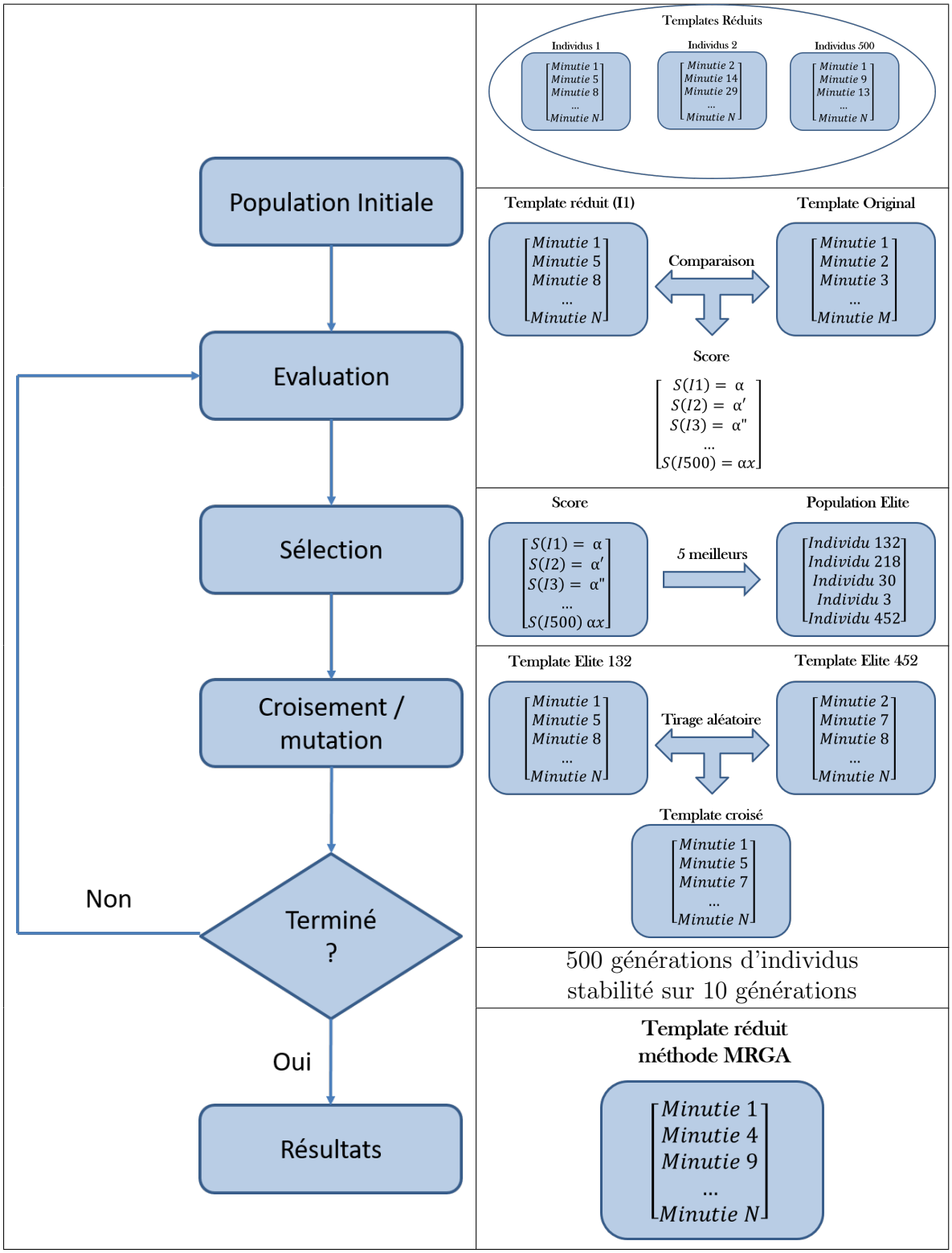


FIGURE 4.16 – Présentation du fonctionnement d'un Algorithme génétique, ainsi que les différentes étapes pour notre cas d'usage sur la réduction de template biométrique.

4.5.2 Résultats expérimentaux

L'évaluation de cette méthode suit le même protocole que précédemment. Nous allons simplement montrer les résultats sur une seule base de données FVC2004DB1 pour illustrer les performances obtenues pour les trois algorithmes Bozorth3, MCC et OCC commercial. Nous montrons les résultats obtenus avec l'algorithme MCC même s'il a été utilisé dans la fonction d'évaluation de l'algorithme génétique. Cela nous permettra d'observer si nous avons des performances proches du template initial. Les tableaux 4.14 et 4.15 ainsi que le tableau 4.16 présentent les résultats obtenus sur l'algorithme Bozoth3, MCC et OCC commercial pour la base FVC2004DB1.

N_{max}	30	34	38	42	46	50
MRGA	14%±.46	13.81%±.32	13.2%±.28	12%±.28	11.3%±.26	11.2%±.24

TABLE 4.14 – Valeurs de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2004DB1 avec la méthode MRGA avec l'algorithme Bozorth3

N_{max}	30	34	38	42	46	50
MRGA	19.2%±.17	19%±.16	18.8%±.15	18.7%±.12	18.4%±.12	18.5%±.09

TABLE 4.15 – Valeurs de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2004DB1 avec la méthode MRGA avec MCC

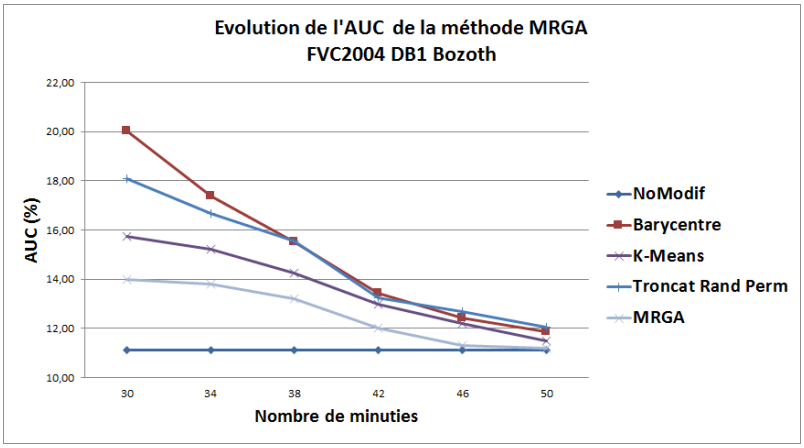
N_{max}	30	34	38	42	46	50
MRGA	5.5%±.25	4.9%±.24	4.32%±.21	3.8%±.20	3.77%±.18	3.77%±.14

TABLE 4.16 – Valeurs de l'AUC pour différentes valeurs $N_{\max}$ de minuties pour FVC2004DB1 avec la méthode MRGA avec l'OCC commercial

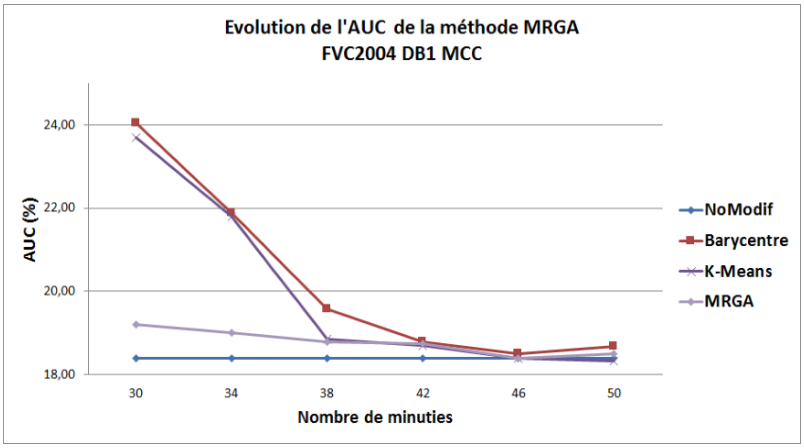
Nous observons que notre méthode MRGA, fournit des performances quasi similaires au template initial, comme nous pouvions nous y attendre. Nous pouvons en conclure que les templates obtenus avec notre méthode MRGA sont très proches des templates originaux.

4.5.3 Comparaison avec les meilleures méthodes

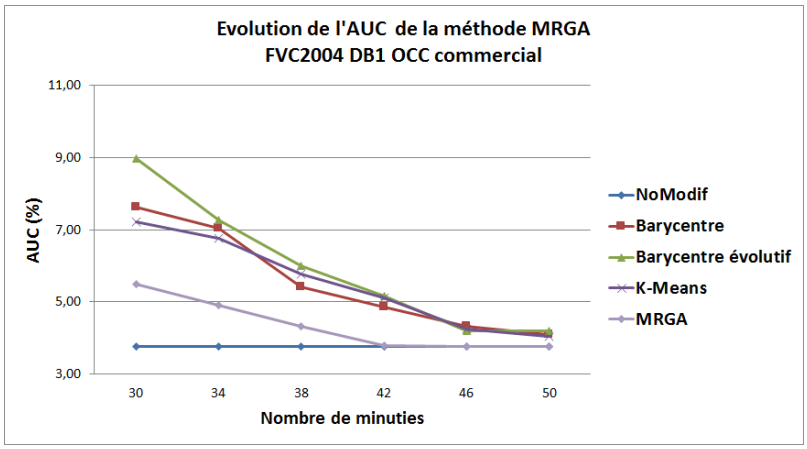
Nous souhaitons évaluer si la méthode MRGA obtient de meilleurs performances que les méthodes précédemment utilisées. La figure 4.17(a) pour l'algorithme Bozorth3, la figure 4.17(b) pour l'algorithme MCC et la figure 4.17(c) pour l'OCC commercial, illustrent cette comparaison de méthodes.



(a) Bozorth



(b) MCC



(c) OCC commercial

FIGURE 4.17 – Comparaison de la méthode optimale avec les meilleures méthodes de réduction sur la base FVC2004DB1 pour les trois algorithmes de comparaison d'empreintes digitales

Comme nous pouvons le constater, la méthode MRGA n'est pas toujours au plus proche de la performance obtenue en considérant le template initial. Les templates ayant été construits avec l'algorithme MCC, ils sont optimisés pour cet algorithme comme le montre la figure 4.17(b), Bozorth et l'OCC commercial ayant des fonctionnements de comparaison différents, nous obtenons de moins bons résultats que le template intial pour ces deux algorithmes de comparaison. Nous remarquons aussi, que les méthodes précédemment utilisées sont plus ou moins proches de la méthode MRGA. Cela nous permet de mieux appréhender si une évolution des méthodes est possible pour atteindre la meilleure réduction possible. Compte tenu de son temps de calcul, cette méthode n'est pas utilisable dans un cadre opérationnel mais uniquement à des fins de validation, ou lors de l'enrôlement de l'individu si la donnée biométrique réduite peut être envoyée ultérieurement de manière sécurisée.

Nous observons que, d'une manière générale, les meilleures méthodes de réduction de template de minuties sont celles proposant une bonne répartition spatiale de ces dernières dans le template réduit. Dans notre classification des méthodes présentée en début de chapitre, nous n'avons pas proposé de méthode de la classe « Incrémental avec distribution ». C'est pourquoi, nous proposons une étude préliminaire utilisant la triangulation de Delaunay.

4.6 Étude préliminaire - Triangulation de Delaunay

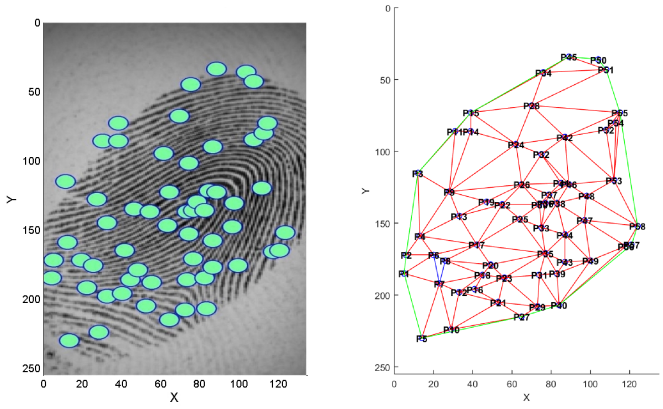
Nous avons choisi d'utiliser la triangulation de Delaunay pour conserver la géométrie du template de minuties, mais aussi pour son invariance par rotation et translation. Nous avons calculé pour chaque template la triangulation associée, comme le montre la figure 4.18, ainsi que l'enveloppe convexe. Ensuite, nous avons calculé les différents éléments pour chaque triangle comme la longueur des arêtes, les angles, l'aire. A partir de ces éléments, nous proposons deux heuristiques, la première est d'enlever du template les sommets avec les angles les plus élevés à la condition qu'ils n'appartiennent pas à l'enveloppe convexe. La seconde est d'enlever les sommets qui appartiennent à des triangles dont la somme des aires est la plus petite. Toute la partie algorithmique 7 est la même, seule l'heuristique de réduction est différente et est détaillée dans l'algorithme 8.

Algorithm 7: Algorithme pour la méthode triangulation de Delaunay basé sur une heuristique

Result: TemplateReduit
Input : TemplateMinuties
Input : nbrMinutieAttendues

$n \leftarrow nbrMinutieAttendues$
$m \leftarrow size(TemplateMinuties)$
$x \leftarrow TemplateMinuties(:, 1)$
$y \leftarrow TemplateMinuties(:, 2)$
if $m > n$ **then**
  while $taille(TemplateReduit) > n$ **do**
    $DT \leftarrow TriDelaunay(x, y)$
    $EC \leftarrow EnveloppeConvexe(DT)$
    $tri\_vois \leftarrow TriangleVoisins(m, DT)$
    $tri\_infos \leftarrow InfosTriangle(DT)$
    $temp \leftarrow$
     $heuristiqueAngle\_Max(TemplateMinuties, tri\_vois, tri\_infos, DT, EC, x, y)$
  end
  $TemplateReduit \leftarrow OrdreCroissantX(temp)$
else
  $TemplateReduit \leftarrow TemplateMinuties$
end

La méthode `TriDelaunay` nous permet de calculer la triangulation de Delaunay à partir des positions des minuties dans le template initial. Après, nous cherchons avec la méthode `EnveloppeConvexe`, les points de la triangulation appartenant à l'enveloppe convexe de la triangulation. Ensuite, avec la méthode `TriangleVoisins`, nous listons pour chacun des triangles ses voisins. La méthode `InfosTriangle`, nous permet d'avoir pour chacun des triangles, des informations complémentaires comme la longueur de chacune des arêtes, les trois angles du triangle, l'aire. La méthode `heuristique` prend toutes ces informations en paramètres et applique sa sélection, nous retournant un *TemplateReduit*. Ce template est une fois de plus remis au format ISO Compact Card II grâce à la méthode `OrdreCroissantX`.



(a) (b)

FIGURE 4.18 – Exemples de triangulation de Delaunay : (a) est l'image de l'empreinte digitale avec les minuties extraites de l'image et (b) la triangulation de Delaunay associée, calculée à partir du template de minuties.

Algorithm 8: Algorithme de l'heuristique Angle_Max

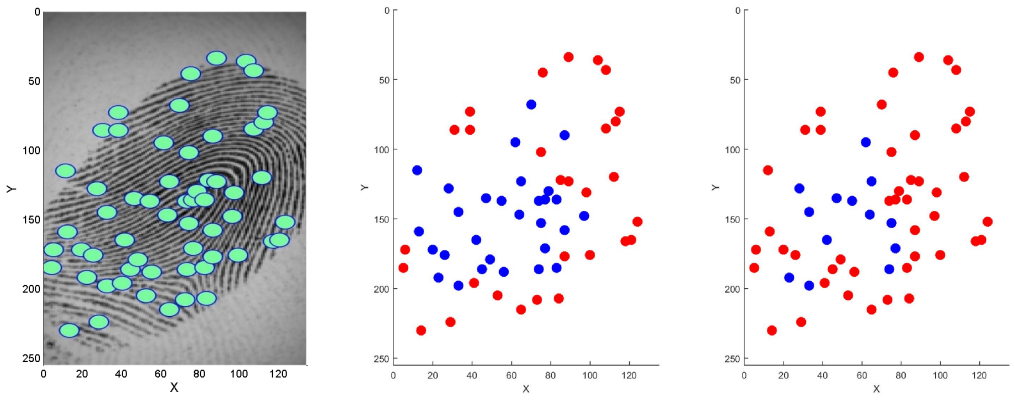
Result: TemplateReduit
Input : TemplateMinuties
Input : tri_vois
Input : tri_infos
Input : DT
Input : EC
Input : x
Input : y

1 $[ValeurMax, Index] \leftarrow TrouverAngleMaxNonEC(tri\_infos, tri\_vois)$
2 $TemplateReduit \leftarrow$
$SupprMaxAngle(TemplateMinuties, ValeurMax, Index)$

La méthode `TrouverAngleMaxNonEC`, permet de trouver une liste contenant les triangles possédant des angles obtus et n'appartenant pas à l'enveloppe convexe. La méthode `SupprMaxAngle` quant à elle, supprime l'angle le plus obtus du template de minuties.

La figure 4.19 montre quelques exemples de réduction de template avec la triangulation de Delaunay avec l'heuristique Angle_Max.

Cette étude préliminaire nous a permis d'avoir une méthode ayant une répartition



(a) (b) (c)

FIGURE 4.19 – Exemples de réduction de template avec la triangulation de Delaunay (DT) avec l'heuristique Angle_Max : (a) est le template initial avec les minuties extraites de l'image, les minuties en rouge sont conservées dans le template réduit avec (b) nbrMinutieAttendues = 30 et (c) nbrMinutieAttendues = 46.

des minuties dans le template réduit, mais les performances ne sont pas à la hauteur de nos espérances. Nous pensons cependant que cette approche a un intérêt car elle est modulaire grâce aux heuristiques.

4.7 Conclusion

Dans ce chapitre, nous avons commencé par présenter les motivations de la réduction de minuties d'un point de vue général. Nous avons ensuite présenté les méthodes de l'état de l'art qui permettent de réduire un template de minuties sans avoir accès à l'image. Nous avons proposé d'autres méthodes de réduction de template. Une étude a été effectuée pour comparer les méthodes de l'état de l'art avec les méthodes proposées. Nous avons testé sur trois bases de données biométriques bien connues et souvent utilisées dans les compétitions biométriques et sur trois algorithmes de comparaisons deux académiques (Bozorth, MCC) et un commercial. Nous avons montré que les méthodes de l'état de l'art n'étaient pas les meilleures et que nous pouvions obtenir une meilleure performance (AUC) lors de la réduction du template de minutie. La méthode ayant majoritairement les meilleurs performances sur toutes les bases et algorithmes de comparaison est K-Means. La méthode Barycentre de l'état de l'art ainsi que Barycentre évolutif ont des performances correctes mais inférieures à K-Means. Nous avons aussi proposé une méthode MRGA, qui permet

d'optimiser la réduction du template de minuties. Nous avons montré, que cette méthode est la plus performante en terme d'AUC sur tous les algorithmes de comparaison utilisés, bien que la méthode soit optimisée pour un autre algorithme de comparaison. Cette méthode MRGA est cependant extrêmement longue en temps de génération du template réduit, en comparaison à la méthode K-Means.

Dès lors que l'on se situe dans le milieu bancaire et sachant qu'une transaction doit être effectuée en moins de 500ms, la méthode retenue doit aussi être rapide. Or, K-Means est lent en comparaison avec Barycentre voire même Barycentre évolutif. La méthode la plus rapide est Troncature avec environ 7,3ms ensuite vient la méthode Barycentre avec 350ms, puis Barycentre évolutif avec 3700ms et pour finir K-Means avec 21000ms, ce qui nous donne un ratio entre Troncature et K-Means de 2682 fois plus lent en défaveur de K-Means. Donc, si nous voulons améliorer les performances du système en respectant ce plafond de 500ms, nous devons faire en sorte que ce soit le terminal de paiement qui effectue la réduction du template et non la carte. Actuellement, il n'y a que Barycentre et Troncature qui respectent la contrainte du temps d'exécution inférieur à 500ms. Il faut aussi savoir que dans notre étude aucune optimisation de code n'a été effectuée, les méthodes proposées ayant été développées sous matlab, en opposition aux méthodes de l'état de l'art qui, elles, le sont. Il faut envisager une méthode rapide qui sélectionnerait les minuties comme la méthode K-Means. Nous avons aussi montré dans ce chapitre comment les méthodes fonctionnent sur un même template, pour ainsi avoir une représentation visuelle de la sélection.

Pour conclure, nous avons proposé des méthodes permettant de réduire un template d'empreinte digitale sans avoir accès à l'image et en améliorant les performances comparées aux méthodes de l'état de l'art. Ces travaux ont fait l'objet de deux publications en conférence internationale.

Dans le prochain chapitre, nous abordons les attaques possibles sur un système biométrique embarqué sur un élément sécurisé. Nous déterminons quels éléments sont importants pour un attaquant lorsqu'il réussit à attaquer le système. Ensuite, une méthode est proposée permettant de reconnaître le type d'empreinte digitale simplement à partir du template de minutie sans accès à l'image. Plusieurs propositions d'utilisation de cette méthode sont proposées.

Chapitre 5

Les attaques d'un système biométrique

Ce chapitre présente un type d'attaque que l'on peut effectuer sur un template biométrique lorsqu'il est embarqué sur un SE. Dans un premier temps, nous étudierons les informations qui peuvent être utiles pour un attaquant. Ensuite, nous proposons une méthode permettant de reconnaître le type d'empreinte digitale à partir du template de minuties seul.

Sommaire

Nous nous intéressons dans ce chapitre à la sécurité de systèmes biométriques embarqués sur SE. La première partie concerne la proposition de nouvelles attaques et la seconde d'une contre-mesure associée. Nous proposons d'étudier dans un premier temps les informations a priori que pourrait exploiter un attaquant afin de faciliter la génération d'un template biométrique pour usurper l'identité d'un individu. Nous souhaitons déterminer si l'utilisation d'a priori, comme le fait de connaître la classe de l'empreinte digitale, le type de capteur, la résolution de l'image ou le nombre de minuties présent dans la référence biométrique de l'individu à usurper peut aider un attaquant à réussir son attaque.

5.1 Quels a priori sont utiles pour un attaquant ?

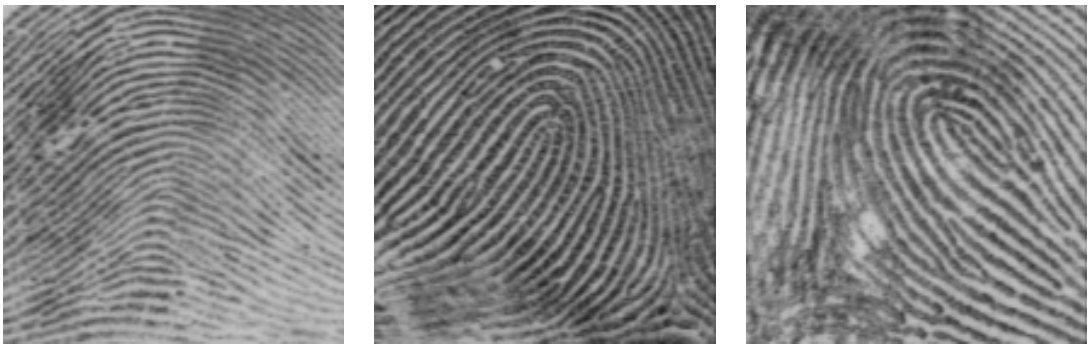
Comme il n'est pas possible de révoquer des données biométriques en cas d'attaque, ces informations sont très sensibles et doivent être protégées le mieux possible. C'est pourquoi le modèle d'empreinte digitale est souvent sauvegardé dans un élément sécurisé. En raison d'une limitation de la taille mémoire ainsi que des capacités de calcul, ce modèle biométrique n'inclut que les minuties stockées sur le SE suivant la représentation ISO Compact Card II [44]. Cette représentation est utilisée pour la mise en correspondance entre la référence et les échantillons capturés. La sécurité des systèmes biométriques embarqués sur SE est, dès lors, une exigence primordiale. L'attaque classique de ce type de système consiste à envoyer au système biométrique un template biométrique afin d'usurper l'identité d'un individu. L'attaquant doit alors générer un template biométrique pour réaliser cette attaque. Une attaque commune sur les algorithmes de comparaisons biométriques embarqué sur SE, consiste à envoyer des modèles aléatoires de minuties pour tenter de se faire passer pour un individu. Ces attaques sont nommées *force brute*, différents travaux ont portés sur ce type d'attaque [109, 110]. Un autre type d'attaque simple existe, et consiste à utiliser un template biométrique calculé à partir de sa propre donnée biométrique, cet attaque est nommé « zéro effort ». Cette attaque n'a que très peu de chance de fonctionner, mais elle peut servir de base pour des attaques plus évoluées.

Les empreintes digitales sont généralement réparties suivant la classification proposée par Henry pour laquelle cinq classes ont été identifiées : Arche, Boucle à gauche, Boucle à droite, Tente et Spirale [111, 112], illustré dans la figure 5.1. En ce qui concerne la sécurité, une comparaison biométrique embarquée (OCC) présente de nombreuses vulnérabilités. Comme présenté dans la section 2.5.3, Ratha et *al.* [35] et plus récemment Jain *et al.* [69] ont classé les attaques d'un système biométrique générique en huit catégories (résumées dans la figure 5.2). Pour chacun des points identifiés, il existe différents types d'attaques. Uludag et Jain [109], Martinez [110] et Soutar [113] considèrent les points 2 et 4 pour effectuer une attaque dite de *hill-climbing*. Cette attaque peut être réalisée par une application qui envoie des données aléatoires (perturbées itérativement) au système. L'application récupère le score de correspondance, entre la référence biométrique et l'échantillon testé, et poursuit ses perturbations seulement lorsque le score de correspondance augmente et jusqu'au moment où on atteint le seuil d'acceptation. À notre connaissance, aucune étude sur les a priori exploitables par un attaquant sur l'empreinte digitale de la personne à usurper n'a été menée. Dans cette étude, nous considérons les attaques sur les points 1 et 2. Pour effectuer une telle attaque, nous devons remplacer le

module *capteur* par notre propre mécanisme. Les informations disponibles sur un capteur biométrique sont définies ci-après, c'est pourquoi nous proposons d'étudier l'impact de ces informations en tant qu'a priori :

— Classe de l'empreinte digitale ;
— Type de capteur (utilisé à l'enrôlement) ;
— Résolution de l'image ;
— Nombre de minuties extraites.

Notre hypothèse est qu'un attaquant ait un accès logique au système et envoie de faux templates biométriques à l'élément sécurisé en exploitant ces a priori. Pour évaluer l'impact de ces a priori sur l'efficacité d'une attaque, nous utilisons la plateforme EVABIO pour caractériser son influence sur la décision de comparaison.



(a) Arche (b) Boucle à gauche (c) Boucle à droite

(d) Tente (e) Spirale

FIGURE 5.1 – Les cinq types d'empreintes définis par Henry.

5.1.1 Plateforme EVABIO - module Attaque

Dans le cadre de la plateforme EVABIO, nous avons développé un nouveau module d'attaque pour mener notre étude, décrit dans la figure 5.3. Il offre aux dévelop-

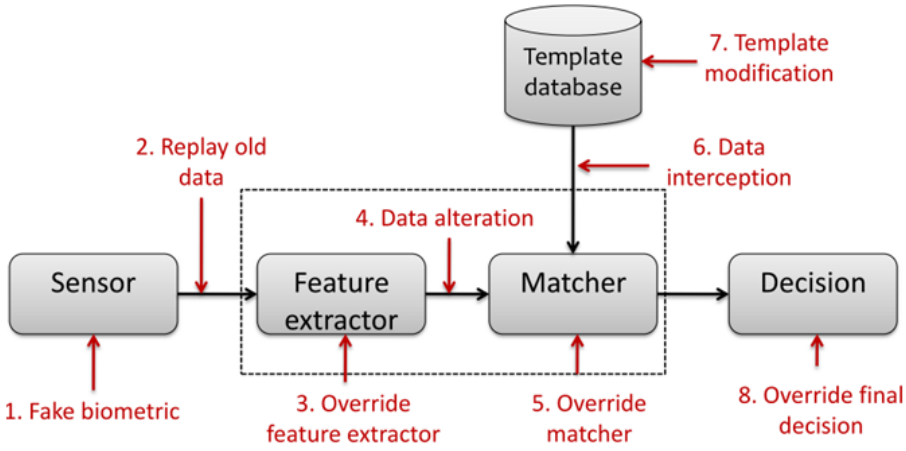


FIGURE 5.2 – Localisation des vulnérabilités sur un système biométrique (définies par [35])

peurs ainsi qu'aux chercheurs différentes méthodes d'attaque lors de la comparaison d'empreintes digitales. En outre, la plateforme permet de tester les attaques sur des algorithmes embarqués (OCC) ainsi que sur des ordinateurs. Grâce à la modularité de la plateforme EVABIO, nous avons l'avantage de pouvoir seulement modifier le module d'Attaque, pour quantifier l'avantage qu'a un attaquant à connaître la classe d'empreintes digitales afin d'usurper l'identité d'un individu. Dans cette étude, le module `Attaque` est mis à jour car il contient des méthodes permettant de tester les connaissances utiles pour un attaquant comme le type de capteur d'empreinte, la résolution de l'image extraite par le capteur, la classe de l'empreinte digitale ou bien le nombre de minuties extraites de l'image. Compte tenu de toutes ces informations, nous déterminons si ce type de connaissances est important ou non pour qu'un attaquant réussisse à usurper l'identité d'individus. Ce module contient également une méthode pour générer un template biométrique aléatoire respectant la norme ISO à l'aide du logiciel SFinge [93], qui peut être utile pour l'attaque par *force brute*. Avec cette méthode, il est possible de générer des modèles d'empreintes digitales aléatoires pour attaquer l'algorithme de comparaison embarqué.

5.1.2 Les a priori sur une empreinte digitale

Nous supposons qu'un attaquant ne peut remplacer le module de capteur que par son propre "*Faux Capteur*", lui permettant ainsi d'avoir accès aux 4 informations le constituant et réparties suivant les vulnérabilités définies dans le modèle de Ratha : 1) en modifiant la résolution de l'image fournie en sortie du capteur influençant ainsi la partie extraction des minuties, 2) en fixant la classe de l'empreinte digitale, 3)

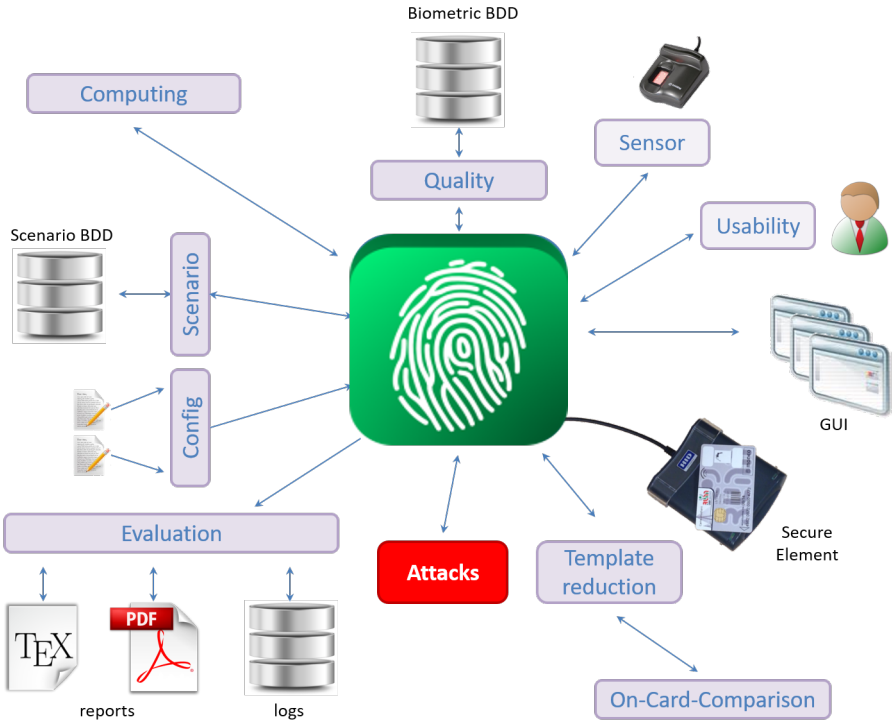


FIGURE 5.3 – Schéma général de la plateforme EvaBio (défini dans [88]) avec le module Attacks developpé

en fournissant des informations sur le type de capteur utilisé pendant le processus d'enrôlement ; 4) lorsque l'attaque est effectuée juste après le processus d'extraction des minuties, l'attaquant peut connaître le nombre de minuties extraites et sauvegardées comme référence dans le module de comparaison embarqué (OCC). Toutes les minuties extraites sont stockées dans un template, comme décrit dans la section 2.4.2.

Nous voulons quantifier dans quelle mesure la connaissance pour un attaquant des paramètres utilisés par le capteur augmente la probabilité de réussir une attaque. Cette probabilité est basée sur le taux de fausses acceptations (FAR) qui peut être interprétée comme la probabilité d'une attaque réussie. Soit b_z le modèle de référence de l'utilisateur z et D un algorithme de comparaison basé sur une distance entre une référence et un échantillon biométrique. Le succès d'une attaque par un imposteur est donné par :

$$FAR_A(\epsilon) = P[D(b_z, A_z) \leq \epsilon)] \tag{5.1}$$

où FAR_A est la probabilité d'une attaque réussie pour un seuil de décision fixé à ϵ. La requête biométrique A_z est construite par l'imposteur en prenant en compte

toutes les informations qu'il connaît sur l'utilisateur z ou sur le système biométrique. Notre but est alors d'estimer l'avantage pour un attaquant de construire A_z lorsqu'il connait la classe de l'empreinte digitale C_z, le type de capteur S_z, le nombre de minuties MN_z ou la résolution de l'image R_z de l'utilisateur z.

5.1.3 Les paramètres de l'expérimentation

Pour l'expérimentation, nous avons créé des bases de données biométriques spécifiques et nous avons utilisé Bozorth et MCC qui sont deux algorithmes de comparaison déjà étudiés dans la section 5.1.3.2.

5.1.3.1 Bases de données biométriques

Nous avons utilisé le logiciel SFinge [93] pour générer les différentes bases de données biométriques synthétiques, n'ayant pas à notre disposition de bases de données avec l'information sur les différents types de capteurs, ainsi que les différentes résolutions d'images, le nombre de minuties et surtout la classe de l'empreinte digitale. De plus, il a été démontré dans différents travaux [114, 115] que SFinge produit des empreintes digitales synthétiques avec des comportements similaires en terme de taux de reconnaissance à ceux obtenus à partir de bases de données réelles, c'est pourquoi nous l'utilisons ici.

Pour chacun des quatre a priori, deux types de bases de données sont conçus :

— **Base de données de référence** : Cette base de données simule les modèles de référence des utilisateurs. Nous avons généré un échantillon par utilisateur pour 500 individus. Cette base de données contient donc 500 empreintes digitales ;
— **Base de données d'attaque** : Nous avons généré une base de données avec 1000 échantillons d'empreintes digitales différents (un échantillon par utilisateur). Cette base de données est utilisée pour les attaques.

En utilisant SFinge, nous pouvons choisir le type de capteur parmi deux types, Capacitif et Optique. Cela induit la construction de quatre bases de données (une BDD de référence et une BDD d'attaque par type de capteur). En considérant le niveau de résolution de l'image, nous avons 3 valeurs (250dpi, 500dpi, 1000dpi) induisant 6 bases de données. En ce qui concerne le nombre de minuties, nous avons créé deux classes (nombre de minuties < 38 ou > 38) induisant 4 bases de données. Enfin,

lorsque l'on considère la classe des empreintes digitales (Arche, Boucle à gauche, Boucle à droite, Tente et Spirale), 10 bases de données sont générées (2 par classe).

Afin d'estimer le seuil de décision ϵ utilisé dans l'équation 5.1 permettant de calculer la valeur EER, nous avons généré une base de données dédiée en utilisant SFinge avec les paramètres par défaut, que nous nommons BDD_SFinge. Les seuls paramètres que nous avons fixés sont le nombre d'utilisateurs (100) ainsi que le nombre de modèles par utilisateur (8). Enfin, nous obtenons un total de 800 empreintes digitales. C'est un choix arbitraire, ce point de fonctionnement est toujours accessible pour n'importe quel algorithme de comparaison.

5.1.3.2 Les algorithmes de comparaison

Dans cette étude, nous avons utilisé deux algorithmes de comparaison issus de la recherche :

— **Bozorth3** : La valeur EER de cet algorithme a été calculée en utilisant la base de données BDD_SFinge. La valeur obtenue est égale à 1,03% pour une valeur de seuil de décision $\epsilon = 26,8$;

— **Minutia Cylinder-Code (MCC) algorithm** : La valeur de l'EER de cet algorithme a lui aussi été calculé en utilisant la base de données BDD_SFinge. La valeur obtenue est égale à 0% pour un seuil de décision $\epsilon = 0,0315$.

5.1.3.3 Protocole expérimental

Pour toute attaque, un imposteur fournit une requête pour être authentifié en tant qu'utilisateur légitime. Deux scenarii sont mis en œuvre pour simuler une attaque :

1. **Scénario 1** : Nous simulons une attaque de type *force brute*. 500 modèles sont sélectionnés aléatoirement, en suivant une distribution uniforme, dans la base de données construite par notre outil de génération aléatoire de template biométrique, ce qui constitue la base de données de référence. La base de données d'attaque est générée en construisant 1000 templates biométriques aléatoires mais respectant le format ISO, lui même provenant de notre outil de génération de templates biométriques.

2. **Scénario 2** : Pour chacun des a priori donné, une base de données de référence est générée avec le logiciel SFinge contenant 500 modèles. De plus,

pour chacun des a priori, une base de données d'attaque contenant 1000 templates biométriques est générée et sera comparée aux bases de données de référence. Par exemple, en considérant le type de capteur, nous obtenons quatre comparaisons comme représenté dans le tableau 5.1.

BDD de reference	**BDD d'attaque**
Capacitif	Capacitif
Capacitif	Optique
Optique	Capacitif
Optique	Optique

TABLE 5.1 – Exemple du scénario 2 pour le type de capteur

5.1.4 Résultats expérimentaux

Dans cette partie, nous présentons les résultats de l'expérimentation pour chaque a priori pris indépendamment.

5.1.4.1 Type de capteur

En considérant la connaissance du type de capteur utilisé pour générer la référence biométrique de l'individu, nous calculons la valeur FAR_A pour les deux scénarii décrits précédemment lorsque nous fixons la valeur du seuil de décision par rapport à l'algorithme de comparaison utilisé comme décrit dans la section 5.1.3.2.

Le tableau 5.2 donne la valeur de probabilité d'attaque réussie FAR_A pour chaque type de capteur et les deux algorithmes de comparaison. Nous pouvons clairement voir que la connaissance du type de capteur utilisé lors de l'enrôlement n'apporte pas d'aide à l'attaquant.

Algorithme de comparaison	Capacitif	Optique
Bozorth3	0.0158 %	0.016 %
MCC	0.13×10^{-3} %	0.23×10^{-3} %

TABLE 5.2 – Valeur de la probabilité d'une attaque réussie FAR_A pour chaque type de capteur pour les deux algorithmes de comparaison.

L'avantage qu'a un attaquant lorsqu'il connaît le type de capteur utilisé à l'enrôlement pour générer la référence n'est pas très importante.

5.1.4.2 Nombre de minuties extraites

Avec la connaissance de cet a priori, (le nombre de minuties dans la référence biométrique de l'individu), nous calculons la valeur FAR_A pour les deux scénarii décrits précédemment lorsque nous fixons la valeur du seuil de décision par rapport à l'algorithme de comparaison comme décrit dans la section 5.1.3.2. Les résultats obtenus montrent que pour Bozorth3, la probabilité d'une attaque réussie est égale à 0,0141% avec la méthode de type *force brute* et 0,0162% lorsque l'on connait le nombre de minuties dans la référence biométrique. Pour l'algorithme MCC, la probabilité qu'une attaque soit réussie est égale à 1.63×10^{-4}% avec l'attaque de type *brute force* et 1.6×10^{-4}% en connaissant le nombre de minuties.

On peut voir dans les deux cas que l'attaquant obtient peu de résultats avec seulement cette information. Afin d'analyser si la connaissance du nombre de minuties de la référence biométrique a un impact sur l'efficacité de cette attaque, nous appliquons le scénario suivant : nous ne considérons que les scores entre le modèle de référence et les tests ayant le même nombre de minuties.

Dans ce cas, nous avons deux séries de $4 \times 800 = 3200$ scores de correspondances. Nous pouvons calculer la valeur FAR_A pour les deux classes du nombre de minuties. Si nous considérons l'algorithme de comparaison Bozorth3, les attaques réussissent plus pour $1 < \epsilon < 35$ lorsque le nombre de minuties est supérieur à 38. Pour l'algorithme de correspondance MCC, la même remarque peut être formulée pour $0.0011 < \epsilon < 0.0023$. Le tableau 5.3 donne la valeur de la probabilité d'attaque réussie FAR_A pour chaque classe du nombre de minuties pour les deux algorithmes de comparaison. Nous pouvons voir clairement que si nous avons plus de 38 minuties, cette information aide plus l'attaquant mais elle ne suffit pas à augmenter de façon importante le succès de l'attaque.

Algorithme de comparaison	< 38	> 38
Bozorth3	0.0038 %	0.0391 %
Minutia CC	0.8×10^{-4} %	2.5×10^{-4} %

TABLE 5.3 – Valeur de la probabilité d'attaque réussie FAR_A pour les deux classes du nombre de minuties pour les deux algorithmes de comparaison.

5.1.4.3 Résolution de l'image

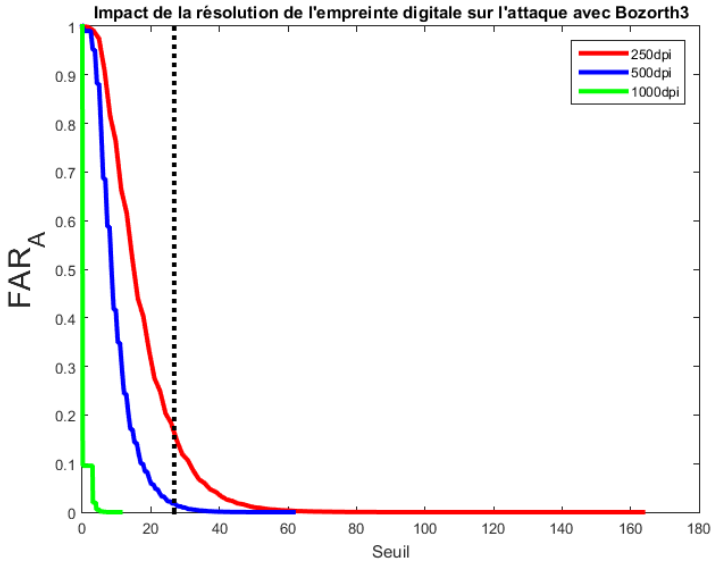
En ce qui concerne la connaissance de la résolution de l'image originale, nous calculons FAR_A pour les deux scénarii lorsque nous fixons le seuil de décision pour obtenir la valeur à l'EER. Les résultats obtenus montrent que lorsque nous utilisons l'algorithme de comparaison Bozorth3, la probabilité d'une attaque réussie est égale à 0,019% avec une attaque de type *force brute* et 0,035% connaissant la résolution de l'image originale. En considérant l'algorithme MCC, la probabilité d'attaque réussie est égale à 0,51 $\times 10^{-3}$% avec une attaque de type *brute force* et $0,8 \times 10^{-3}$% connaissant la résolution de l'image originale.

Nous pouvons voir dans les deux cas le petit avantage pour un attaquant de connaître la résolution de l'image originale extraite par le capteur. Afin d'analyser si la résolution de l'image originale a un impact sur l'efficacité de cette attaque, nous appliquons le schéma suivant : nous ne considérons que les scores entre le modèle de référence et d'attaque ayant la même résolution d'images. Dans ce cas, nous avons 3 séries de $4 \times 800 = 3200$ scores de correspondances. On peut ainsi calculer la valeur FAR_A pour chaque classe de résolution d'image, comme le montre la figure 5.4.

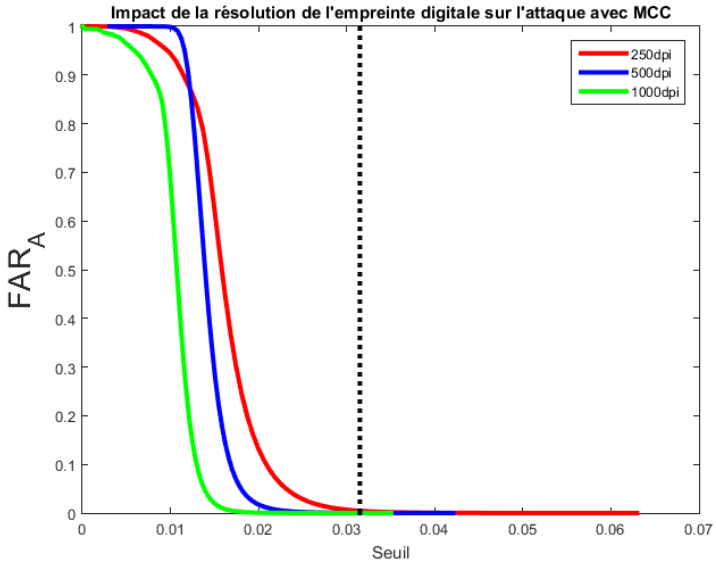
Pour l'algorithme de comparaison Bozorth3, nous pouvons voir qu'il est tout à fait impossible de réussir l'attaque avec une image de haute résolution (1000dpi), contrairement à une image de faible résolution (250dpi). La même remarque peut être formulée pour l'algorithme MCC. Le tableau 5.4 donne la valeur de la probabilité d'attaque réussie FAR_A pour chaque résolution d'image pour les deux algorithmes de comparaison. Nous pouvons clairement voir que la basse résolution aide un attaquant avec plus de 3 fois plus d'attaques réussies que la résolution moyenne (500dpi). Il faut donc éviter d'utiliser des images de faible résolution pour limiter ce type d'attaque.

Algorithme de comparaison	250dpi	500dpi	1000dpi
Bozorth3	0.165 %	0.047 %	0 %
Minutia CC	0.45×10^{-3} %	0.176×10^{-3} %	0 %

TABLE 5.4 – Valeur de la probabilité d'une attaque réussie FAR_A pour chaque résolution des images originales pour les deux algorithmes de comparaison.



(a) Impact de la résolution de l'image avec Bozorth3



(b) Impact de la résolution de l'image avec MCC

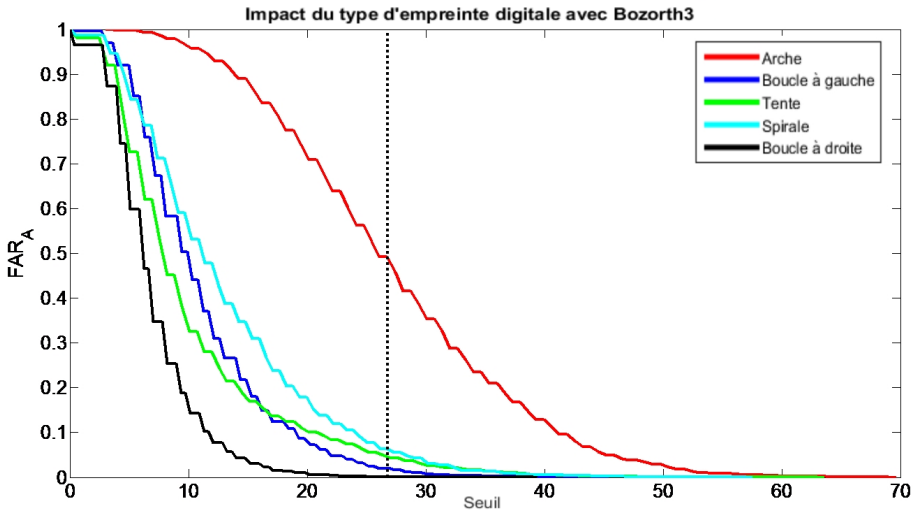
FIGURE 5.4 – Évolution de l'efficacité des attaques en tenant compte les trois résolutions du capteur pour les deux algorithmes de comparaison.

5.1.4.4 Type d'empreinte digitale

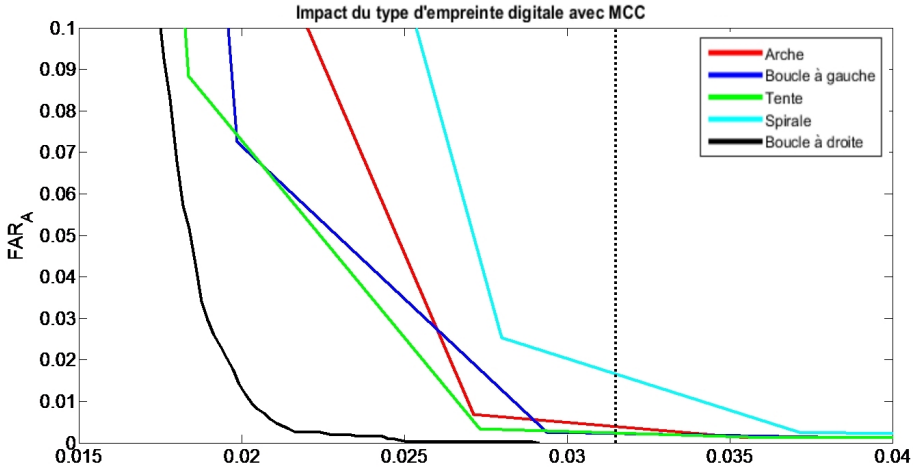
A partir de la connaissance de la classe d'empreintes digitales, nous calculons la valeur FAR_A pour les deux scénarii lorsque nous fixons la valeur du seuil de décision par rapport à l'algorithme de comparaison comme décrit dans la section 5.1.3.2. En considérant l'algorithme Bozorth3, la probabilité d'une attaque réussie est égale à 3% avec la méthode de type *brute force* et à 4,7% en connaissant la classe de l'empreinte digitale. Les résultats obtenus montrent que lorsque nous utilisons l'algorithme de comparaison MCC, la probabilité d'une attaque réussie est égale à 1,7% avec la méthode de type *brute force* et 2,6% avec la connaissance de la classe d'empreintes digitales. Nous pouvons en déduire que la connaissance de la classe d'empreintes digitales enrôlée sur l'élément sécurisé aide un attaquant à se faire authentifier sur le système. Cependant, nous devons étudier comment cette connaissance influence l'efficacité de l'attaque.

Afin d'analyser son impact, nous appliquons l'approche suivante : nous considérons uniquement les scores entre les modèles de référence et d'attaque ayant la même classe d'empreintes digitales pour calculer la valeur FAR pour chacune des classes. Dans ce cas, nous avons 5 séries de $4 \times 800 = 3200$ scores de correspondances nous permettant de calculer la valeur FAR_A.

Les résultats sont présentés dans la figure 5.5. En considérant l'algorithme de comparaison Bozorth3, la figure 5.5(a) nous permet de déduire que la classe *Arche* présente le taux d'attaque avec le succès le plus élevé alors que la classe *boucle à droite* présente le taux le plus bas. Par contre, pour l'algorithme de comparaison MCC, nous observons dans la figure 5.5(b) que la classe *Spirale* présente le taux d'attaque réussie le plus élevé contrairement à la classe *boucle à droite* ayant le plus faible taux. Une première remarque que nous pouvons formuler est que les empreintes digitales appartenant à la classe *boucle à droite* sont les moins facile à usurper. Le tableau 5.5 donne la valeur de la probabilité d'attaque réussie FAR_A pour chaque classe d'empreintes digitales pour les deux algorithmes de comparaison. Nous pouvons clairement voir que certaines classes d'empreintes digitales sont plus faciles à attaquer en fonction de l'algorithme de comparaison utilisé. Par exemple avec Bozorth3, les empreintes de la classe *Arche* peuvent être usurpées dans 50% des cas, ce qui est très important. En conclusion Bozorth ne doit pas être utilisé car il est sensible aux attaques sur les empreintes digitales de type *Arche*.



(a) Impact du type d'empreinte digitale avec Bozorth3



(b) Impact du type d'empreinte digitale avec MCC

FIGURE 5.5 – Évolution de l'efficacité des attaques en tenant compte de toutes les classes d'empreintes digitales pour les deux systèmes biométriques.

Algorithme de comparaison	Arche	Boucle à droite	Boucle à gauche	Tente	Spirale
Bozorth3	50 %	0 %	2 %	5 %	6.3 %
Minutia CC	0.6 %	0 %	0.2 %	0.2 %	2 %

TABLE 5.5 – Valeur de la probabilité FAR_A d'une attaque réussie pour chaque classe d'empreintes digitales pour les deux algorithmes de comparaison.

Discussion

Dans cette étude originale par rapport à la littérature, nous avons voulu savoir quels a priori étaient importants pour un attaquant lorsqu'il souhaite usurper l'identité de l'individu enrôlé sur l'élément sécurisé. Nous avons montré les connaissances aidant un attaquant à usurper l'identité d'un individu ou d'apporter des informations lui permettant d'augmenter ses probabilités d'attaque réussie, comme la classe d'empreintes digitales ainsi que la résolution de l'image. Nos expériences montrent que si nous connaissons la classe d'empreinte digitale pour les individus enrôlés sur le système, nous augmentons en général la probabilité d'usurper leurs identités. D'autre part, le nombre de minuties ainsi que le type de capteur (capacitif et optique) apportent peu d'aide à un attaquant. L'algorithme sur lequel nous obtenons le meilleur taux d'usurpation d'identité est Bozorth avec les empreintes digitales de type Arche. Nous émettons l'hypothèse que cet algorithme, destiné à la recherche et au public, est moins performant et non optimisé pour les empreintes de type Arche. Si l'on regarde les autres types d'empreintes pour les deux algorithmes, nous remarquons que le taux d'usurpation est assez faible ce qui est assez logique et cohérent. De plus, pour les deux algorithmes le plus haut taux d'acceptation est sur les Spirales, qui sont de surcroit le type d'empreinte digitale le plus courant [116]. D'une manière générale, nous en déduisons que le taux de réussite d'une attaque dépend quasiment exclusivement du fonctionnement de l'algorithme de comparaison.

La connaissance du type de l'empreinte digitale de l'individu à usurper est une information importante pour un imposteur. Dans la prochaine section, nous tentons de répondre à la question suivante : est il possible de reconnaitre le type d'empreinte digitale à partir de son template de minuties ? Si oui, dans quelle mesure est-il possible de contrer ce type d'attaque ?

5.2 Reconnaissance du type d'empreinte

L'empreinte digitale est devenue en quelques années une modalité biométrique très populaire. En 2013, le premier smartphone intégrant un capteur d'empreintes digitales a été déployé pour un usage public. Afin de garantir les problèmes de sécurité et de confidentialité, le traitement des empreintes digitales est réalisé sur un élément sécurisé tel qu'une carte SIM ou une carte à puce.

Parmi toutes les attaques possibles, l'une concerne plus spécialement la détection de la classe du modèle de minuties, telle que définie par Henry. Comme nous l'avons

démontré dans la section précédente ainsi que dans [117], le fait de connaître le type d'empreinte digitale aide de manière significative un attaquant à usurper l'identité d'un individu, en passant de 2% à 50% pour certains types d'empreinte digitale et suivant l'algorithme de comparaison utilisé, comme Bozorth par exemple. C'est pourquoi nous souhaitons ici proposer une méthode permettant de reconnaître le type d'empreinte digitale directement à partir du template de minuties au format ISO sans aucun accès à l'image ni reconstruction de cette dernière, afin de développer une parade à ce type d'attaque. Une façon est de considérer l'ajout d'un mécanisme de reconnaissance du type d'empreinte sur le terminal de paiement ainsi que sur le SE. La détection de la classe d'empreinte digitale sera incluse dans le résultat de vérification du porteur de carte (Cardholder Verification Result, CVR) et envoyé au terminal permettant ainsi d'effectuer l'analyse de risque (Terminal Risk Management). Cela permet de détecter si le type de l'empreinte digitale est différent de celui envoyé par le terminal à la carte à puce. De cette façon, nous étudions si la détection d'un changement de classe d'empreinte digitale entre la carte et le terminal aide à réduire le taux d'attaque réussie.

5.2.1 Positionnement par rapport à l'état de l'art

De nombreux travaux ont été réalisés pour le traitement de modèles biométriques, tels que la reconstruction du champ d'orientation [118, 119]. Ces algorithmes de comparaison [120, 121], la protection des empreintes digitales [122, 123]. Cependant, peu de travaux ont considéré la représentation ISO Compact Card II [111, 112]. Toutes les méthodes qui permettent de détecter le type d'empreintes digitales sont basées sur les images et non sur des minuties [124, 125, 126]. Différentes méthodes reconstruisent l'image à partir du template de minuties, mais cela induit beaucoup de ressources de calcul ainsi que de temps. Cela n'est pas possible dans notre cas car un SE ne dispose pas de ressources suffisantes pour reconstituer des images et appliquer ces méthodes. Notre but est donc de proposer des méthodes basées uniquement sur le template de minuties pour déterminer la classe des empreintes digitales.

5.2.2 Principe de la méthode

Nos travaux sont basés sur les templates de minuties au format ISO Compact Card II. Comme décrit dans la section 2.4.2 et résumé ici, ce template se compose de quatre informations $(x_i, y_i, T_i, \theta_i),\ i = 1 : N_j$ ou :

— Les coordonnées (x_i, y_i) correspondant à la localisation des minuties dans l'image (l'image étant bien entendu indisponible),

— T_i correspond au type de la minutie (bifurcation, fin de crête),
— θ_i est l'orientation de la minutie relative à la crête. Cette information est représentée par 6 bits, c'est-à-dire 64 valeurs différentes.
— N_j est le nombre de minuties pour l'échantillon j de l'utilisateur.

Les templates de minuties utilisés dans l'expérimentation ont été extraits à l'aide de l'outil NBIS et plus spécialement MINDTCT [104] du NIST. A partir du modèle ISO, nous avons généré un vecteur statistique appelé IsoStruct_{jk}. Pour chaque paramètre de ce vecteur, l'histogramme normalisé a été calculé avec un pas de quantification fixe. Nous avons normalisé les histogrammes pour s'affranchir du nombre de minuties présentes dans chacun des templates. On obtient alors un vecteur IsoStruct_{jk} de taille $3 \times N + 2$ en concaténant ces histogrammes, où N est le nombre de niveau de quantification dans le calcul des histogrammes et 2 correspond à l'histogramme construit sur le type de minutie qui ne contient que deux valeurs différentes.

Ce vecteur statistique IsoStruct_{jk} est alors défini comme suit :

$$\begin{aligned} \text{IsoStruct}_{jk} = \{&\text{HistoX}_{jk}, \\ &\text{HistoY}_{jk}, \text{HistoIsoAngle}_{jk}, \\ &\text{HistoType}_{jk}\} \end{aligned} \tag{5.2}$$

où $\text{HistoX}_{jk}, \text{HistoY}_{jk}, \text{HistoIsoAngle}_{jk}$ et HistoType_{jk} sont les histogrammes normalisés. Pour permettre d'avoir plusieurs niveaux de précision sur chacun des histogrammes, ils ont été générés avec un nombre variable N de niveaux de quantification.

Afin de définir un modèle pour chacune des cinq classes d'empreintes digitales, nous utilisons une technique d'apprentissage statistique.

5.2.2.1 Apprentissage par SVM

A partir de tous les schémas de classification existants, nous avons choisi la technique basée sur le Séparateur à Vaste Marge (SVM) en raison de son taux de classification élevé obtenu dans de nombreux travaux [127, 128, 129], ainsi qu'à sa capacité de généralisation élevée. Les SVM ont été développés par Vapnik et al. [130] et sont basés sur le principe de minimisation des risques structurels de la théorie de l'apprentissage statistique. Les SVM expriment des prédictions en termes de combinaison linéaire de fonctions du noyau centrées sur un sous-ensemble des

données d'apprentissage, appelées vecteur de support (SV).

Les SVM étant des classificateurs binaires, plusieurs classificateurs SVM binaires sont nécessaires pour un problème de classification multi-classes lorsque l'on utilise une technique de classification par SVM. Une décision finale est alors prise à partir de toutes les sorties des SVM binaires [128].

Le choix de la fonction du noyau est essentiel. La fonction noyau RBF (Radial Basis Function) est couramment utilisée avec le SVM. La raison principale est que les fonctions RBF fonctionnent comme des mesures de similarité entre deux exemples. Une décision finale doit être prise à partir de toutes les fonctions de décision binaires. Plusieurs stratégies de combinaison peuvent être utilisées [128]. Parmi toutes les stratégies existantes, le vote majoritaire est choisi dans notre étude pour sa simplicité de mise en oeuvre.

5.2.2.2 Protocole expérimental

Nous énumérons ici tous les éléments nécessaires pour notre expérimentation.

Bases de données SFinge : Les bases de données FVC ne fournissent aucune information sur la classe d'empreintes digitales. Nous avons donc généré cinq bases de données avec le logiciel SFinge, une pour chaque classe d'empreinte digitale décrite dans le tableau 5.6. Chaque base de données ainsi générée contient 800 échantillons biométriques.

Étiquette	Classes d'empreintes digitales
1	Arche
2	Boucle à gauche
3	Boucle à droite
4	Tente
5	Spirale

TABLE 5.6 – Étiquette pour les bases de données générées pour chaque classe d'empreintes digitales.

Afin de définir les modèles pour chacune des cinq classes d'empreintes, il est nécessaire d'entraîner les SVMs sur un ensemble d'apprentissage. Un ensemble de tests sera également impératif pour mesurer l'efficacité du classificateur généré. Pour

ce faire, plusieurs séquences d'apprentissage-test ont été exécutées. Dans chacune des séquences, la base de données d'empreintes digitales a été subdivisée en ensembles distincts d'apprentissages et de tests. Dans chaque séquence de tests, 80% de la base de données a été choisie pour l'apprentissage et 20% pour les tests et ce pour chacune des 5 bases de données. Plus précisément, chaque ensemble d'apprentissage contient 640 empreintes digitales, alors que le test contient les 260 empreintes digitales restantes. 1000 ensembles d'entraînements et de tests choisis aléatoirement, et suivant une distribution uniforme, ont été réalisés et le taux de reconnaissance des classes a été calculé sur les 1000 itérations. Nous avons utilisé la libraire libsvm [131] avec les paramètres par défaut.

5.2.2.3 Résultats expérimentaux

Un des premiers éléments que nous devons définir est le nombre de niveaux de quantification des histogrammes normalisés nécessaires par paramètre pour avoir l'impact minimal sur les performances du taux de reconnaissance. Nous avons testé différents niveaux de quantification (8, 16, 32, 64) sur la structure des caractéristiques. Les résultats sont présentés dans le tableau 5.7.

Niveau quantification	Taux de reconnaissance sur la base de test(%)
8	79.43
16	80.37
32	80.06
64	60.80

TABLE 5.7 – Tableau de reconnaissance de classe d'empreintes digitales avec le modèle ISO pour toutes les caractéristiques sur la base de test.

Nous pouvons observer que les meilleurs résultats sont obtenus avec 16 niveaux de quantifications pour la structure basée sur les caractéristiques. Ces résultats peuvent être expliqués par le fait que 64 niveaux de quantifications créent une redondance, avec beaucoup de valeurs à zéro, pour ce type d'application. Avec seulement un vecteur de caractéristiques de 50 valeurs ($50 = 3 \times 16 + 2$), nous obtenons 80,37% de reconnaissance de la classe d'empreintes digitales avec les paramètres SVM standard et aucune optimisation. Dans la suite de l'étude, nous gardons cette taille du vecteur de caractéristiques.

Le tableau 5.9 nous présente les résultats obtenus lorsque nous testons une seule classe sur notre SVM, ceci ayant pour but d'avoir un aperçu du taux de reconnaissance de chacune des classes d'empreintes digitales. Nous constatons que les classes d'empreintes digitales les mieux reconnues sont Spirale, Arche et Tente avec respectivement 87%, 85% et 80% de reconnaissance de la bonne classe. Nous remarquons que boucle à gauche et boucle à droite ont 75% de bonne classification ce qui est faible par rapport aux autres classes. Nous avons remarqué que les boucles qu'elles soient à gauche ou à droite sont souvent confondues par le SVM ce qui explique ce faible taux de 75% de bonne classification.

	Arche	Boucle à gauche	Boucle à droite	Tente	Spirale
Taux de reconnaissance (%)	85	75	75	80	87

TABLE 5.8 – Tableau de bonne classification avec le modèle ISO pour chaque base de données de tests de chacune des classes d'empreintes digitales.

Le template ISO ne contenant que quatre informations, nous souhaitons savoir lesquelles sont importantes pour la reconnaissance du type d'empreintes digitales. Le tableau 5.9 indique le taux de reconnaissance pour chaque valeur de niveau de quantification et pour chacun des paramètres présents dans le template ISO. Nous pouvons observer que le $H(Type)$ a le même taux de reconnaissance quel que soit le nombre de niveaux de quantifications utilisé. Ceci est dû aux deux valeurs possibles de ce paramètre, nous avons seulement un histogramme avec deux niveaux de quantifications en comparaison aux autres paramètres. En ce qui concerne les histogrammes sur la positions des minuties $H(X)$ et $H(Y)$, nous avons de mauvais résultats avec environ 40% de taux de reconnaissance. Ceci était prévisible, car la position des minuties dépend de l'interaction entre le doigt et le capteur, un doigt peut ainsi être posé de côté sur ce dernier et impacter fortement la reconnaissance du type d'empreinte digitale. En revanche, avec l'histogramme des angles, $H(ISO\_Angle)$, nous avons le meilleur taux de reconnaissance du type d'empreintes digitales. Ces résultats sont cohérents car les angles sont calculés à partir de la crête de l'empreinte digitale et du repère orthonormé du capteur, ce qui permet d'avoir une idée générale de la direction des différentes minuties et ainsi retrouver le type de l'empreinte plus facilement.

Nous pouvons conclure que la caractéristique $H(ISO\_Angle)$ est une information importante pour la reconnaissance de la classe d'empreintes digitales. Avec environ

	Taux de reconnaissance (%)			
Niveau quantification	H(X)	H(Y)	H(ISO_Angle)	H(Type)
8	42.87	37.52	77.85	28.13
16	43.62	38.96	80.23	28.13
32	42.25	36.51	80.24	28.13
64	40.45	36.47	78.25	28.13

TABLE 5.9 – Taux de reconnaissance pour chaque élément du template ISO CC par rapport au nombre de niveaux de quantification.

79% de taux de reconnaissance, c'est le paramètre le plus important présent dans le template initial, les trois autres paramètres n'améliorent pas la performance. Ces résultats sont satisfaisants, mais nous souhaitons avoir plus d'une information pertinente et ainsi améliorer le taux de reconnaissance des empreintes digitales.

5.2.3 Nouveaux attributs

Comme mentionné dans la section précédente, lorsque l'on utilise les histogrammes des caractéristiques provenant des templates ISO, nous avons peu d'informations pour caractériser les empreintes digitales. Les histogrammes sur la position spatiale des minuties n'aidant pas à reconnaître le type de l'empreinte, c'est pourquoi nous avons décidé d'utiliser la triangulation de Delaunay [132, 133] afin de ne pas utiliser la position spatiale des minuties. La triangulation de Delaunay est utilisée dans divers domaines, tels que la géométrie algorithmique [134] pour résoudre des problèmes, ou dans la reconstruction de surface [135, 136]. Dans notre cas, la triangulation de Delaunay permet de résoudre les problèmes de translation et de rotation du template de minuties ISO et permet également de faire une abstraction de l'emplacement des minuties dans le template. Cela nous permet de créer une structure contenant des paramètres décrivant chaque template, comme schématisé dans la figure 5.6. Cette structure de paramètres est composée d'éléments tels que la longueur des arêtes des triangles, les angles, l'aire des triangles, le périmètre.

5.2.3.1 Structure de paramètres

Pour chaque template, nous avons calculé la triangulation de Delaunay basée sur les minuties. La figure 5.7 montre un exemple de triangulation obtenue en considérant les minuties comme les sommets des triangles générés. Pour chaque triangle obtenu, nous extrayons différents paramètres :

— les trois angles,

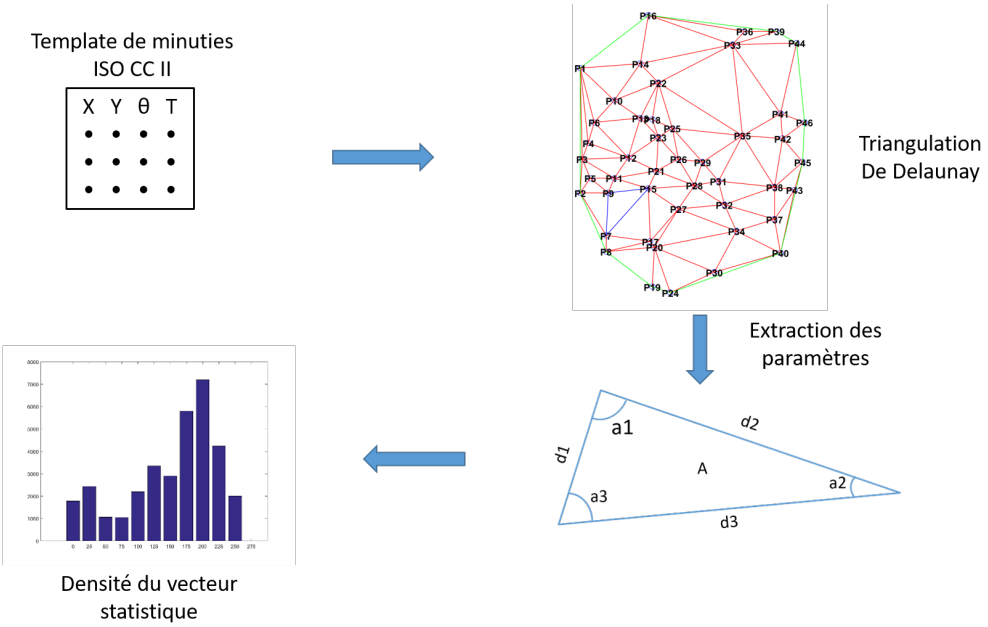


FIGURE 5.6 – Schéma général de calcul des attributs d'un template de minuties

— les trois longueurs d'arêtes,
— l'aire.

Ainsi, chaque template j d'un individu k peut être représenté par un vecteur de caractéristiques TriInf_{jk} composé de trois ensembles de paramètres :

$$\begin{aligned}\text{TriInf}_{j,k} = \{&\{\text{AngleA}_{jkl}, \text{AngleB}_{jkl}, \text{AngleC}_{jkl}\},\\ &\{\text{LengthAB}_{jkl}, \text{LengthAC}_{jkl}, \text{LengthBC}_{jkl}\},\\ &\{\text{Area}_{jkl}\}\}, \forall l \in [1; M_j],\end{aligned} \tag{5.3}$$

où $\{\text{AngleA}_{jkl}, \text{AngleB}_{jkl}, \text{Angle C}_{jkl}\}$ est le vecteur des données relatives aux valeurs des angles des triangles M_j du template j, $\{\text{LengthAB}_{jkl}, \text{LengthAC}_{jkl}, \text{LengthBC}_{jkl}\}$ représente le vecteur de données relatives aux longueurs calculées pour les triangles M_j du template j et $\{\text{Area}_{jkl}\}$ correspond au vecteur de données relatif à l'aire des triangles M_j du template j. Puisque les résultats obtenus en section 5.2.2.3 ont mis en évidence que l'orientation des minuties était une caractéristique à fort taux de discrimination, nous ajoutons ce paramètre non lié à la triangulation de Delaunay mais provenant du template original :

$$\text{IsoAngleInf}_{j,k} = \{\text{Orientation}_{jki}\}, \forall i \in [1; N_j], \tag{5.4}$$

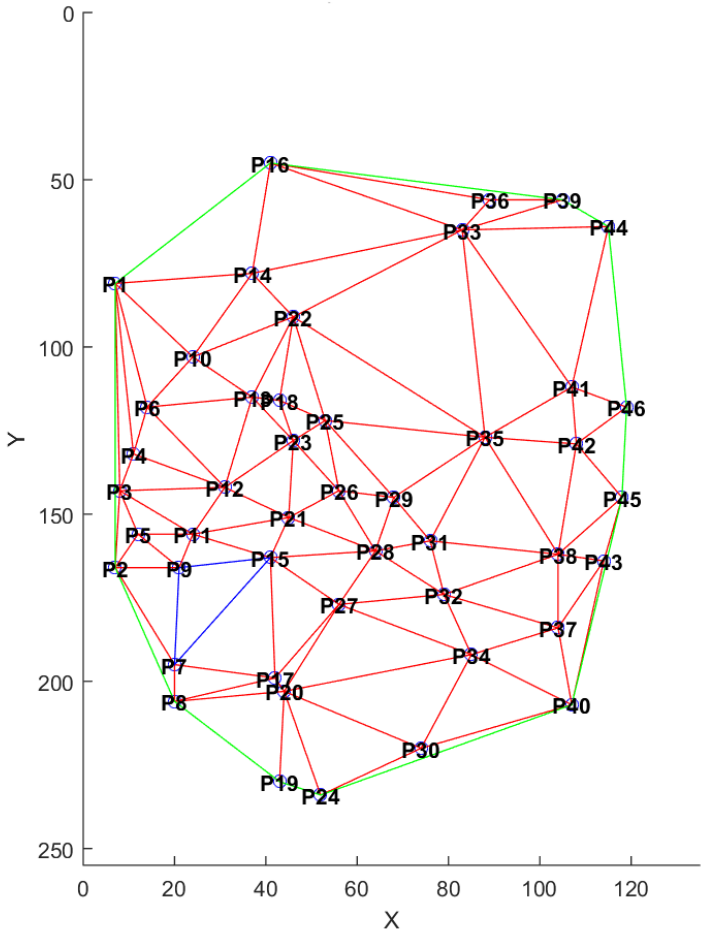


FIGURE 5.7 – Triangulation de Delaunay pour un template ISO Compact Card II

où Orientation_{jki} représente les données vectorielles contenant l'angle ISO des N_j minuties du template j.

5.2.3.2 Densité du vecteur statistique

A partir de ces deux vecteurs de caractéristiques TriInf_{jk} and IsoAngleInfo_{jk}, un nouveau vecteur de statistique est généré. Nous calculons un histogramme normalisé, pour approximer une densité de probabilité pour chaque caractéristique, n'étant pas dépendante du nombre de minuties dans le template ISO. Ces histogrammes sont calculés en considérant une valeur fixée du niveau de quantification. On obtient alors un vecteur $\text{TemplateStruct}_{jk}$ de taille $4 \times N$, où N est le nombre de niveaux de quantification dans le calcul des histogrammes. Ce vecteur statistique $\text{TemplateStruct}_{jk}$

est obtenu par une concaténation d'histogramme défini comme suit :

$$\begin{aligned}\text{TemplateStruct}_{jk} = \{&\text{HistoAngle}_{jk},\\ &\text{HistoDistance}_{jk}, \text{HistoArea}_{jk},\\ &\text{HistoISOAngle}_{jk}\}\end{aligned} \tag{5.5}$$

où $\text{HistoAngle}_{jk}, \text{HistoDistance}_{jk}, \text{HistoArea}_{jk}$ et $\text{HistoISOAngle}_{jk}$ sont des histogrammes normalisés calculés à partir de leur sous-vecteur associé TriInf_{jk} et IsoAngleInfo_{jk}. Ces histogrammes sont générés avec un nombre variable de niveaux N de quantification, permettant d'affiner la forme de l'histogramme.

5.2.3.3 Résultats expérimentaux

Nous avons utilisé le même protocole que celui défini dans la section 5.2.2.2 ainsi que le nombre de niveaux de quantifications défini dans la section 5.2.2.3 avec $N = 16$. Le tableau 5.10 nous donne les résultats de la reconnaissance du type d'empreinte pour la nouvelle sélection d'attributs. Si nous comparons les résultats seulement entre le template ISO et les nouveaux attributs, nous avons une différence d'environ 10%. Les nouveaux attributs présentent un meilleur taux de reconnaissance du type d'empreintes digitales avec 89% de bonne reconnaissance de classe d'empreintes digitales.

	Taux de reconnaissance (%)
Méthode ISO	80.37
Méthode proposée	89.12

TABLE 5.10 – Résultats de la reconnaissance du type d'empreintes digitales pour la nouvelle sélection d'attributs avec 80% d'apprentissage.

Lorsque nous effectuons la même procédure que précédemment, ne tester qu'une seule classe d'empreinte digitale sur notre SVM, nous obtenons les taux de bonne classification présentés dans le tableau 5.11. Nous constatons une fois de plus que les classes d'empreinte Spirale et Arche sont reconnues à plus de 95% par notre SVM, ces résultats sont très satisfaisants car cela montre que notre approche apporte plus d'informations et permet au SVM de mieux catégoriser nos empreintes. La classe Tente quand à elle est reconnue à 89% soit une amélioration de 9% par rapport au résultat présenté précédemment. Une fois de plus les boucles à gauche et à droite ont le taux de bonne classification le plus faible avec 82% et le SVM malgré l'ajout d'informations avec notre méthode a toujours du mal à différencier ces deux classes.

Notre méthode peut être améliorée, il faudrait envisager de prendre en compte d'autres paramètres comme par exemple les plus petits angles, les plus grands angles.

	Arche	Boucle à gauche	Boucle à droite	Tente	Spirale
Taux de reconnaissance (%)	95	82	82	89	97,8

TABLE 5.11 – Tableau de bonne classification avec la méthode proposée pour chaque bases de données de tests de chacune des classes d'empreintes digitales.

5.2.4 Discussion

Nous proposons deux cas d'utilisation de la reconnaissance du type d'empreinte digitale pour la détection d'attaque de notre système. Le premier consiste à intégrer cette reconnaissance lors d'une transaction bancaire de type EMV. La seconde s'attachera à ralentir un attaquant lorsqu'il fait un attaque de type force brute lors d'une authentification biométrique sur un service web. Ce premier cadre applicatif est très intéressant car depuis 2015, EMVco [42] permet d'utiliser des données biométriques pour la vérification porteur (*CardHolder Verification* dans la figure 5.8) de la carte bancaire en remplacement du code PIN.

Nous proposons ainsi d'intégrer notre mécanisme de reconnaissance du type d'empreinte digitale à la fois sur le terminal de paiement et la carte. Lorsqu'une transaction bancaire de type EMV est effectuée lors de la phase de vérification du porteur, un vecteur nommé CRM (Card Risk Management) est utilisé puis envoyé au terminal pour montrer quels éléments ont été vérifiés par la carte. Le terminal de son côté possède un vecteur nommé TRM (Terminal Risk Management) qu'il va comparer à celui provenant de la carte, si des éléments de ce vecteur diffèrent, la transaction peut être abandonnée ou alors partir en demande d'autorisation auprès de la banque émettrice de la carte. Nous proposons ici d'ajouter aux vecteurs CRM et TRM une information sur le type de l'empreinte digitale envoyé pour l'authentification et ainsi détecter si la donnée biométrique a été modifiée entre le terminal et la carte. On réduit ainsi les chances qu'une attaque de type homme du milieu (Man-In-The-Middle [91]) puisse être réalisée.

Dans ce second cadre applicatif, nous souhaitons intégrer notre mécanisme de reconnaissance d'empreinte digitale lorsque la base de donnée biométrique est décentralisée. Un attaquant peut essayer de se faire authentifier par le système en faisant une attaque brute force. Notre proposition consiste à détecter le type d'empreinte

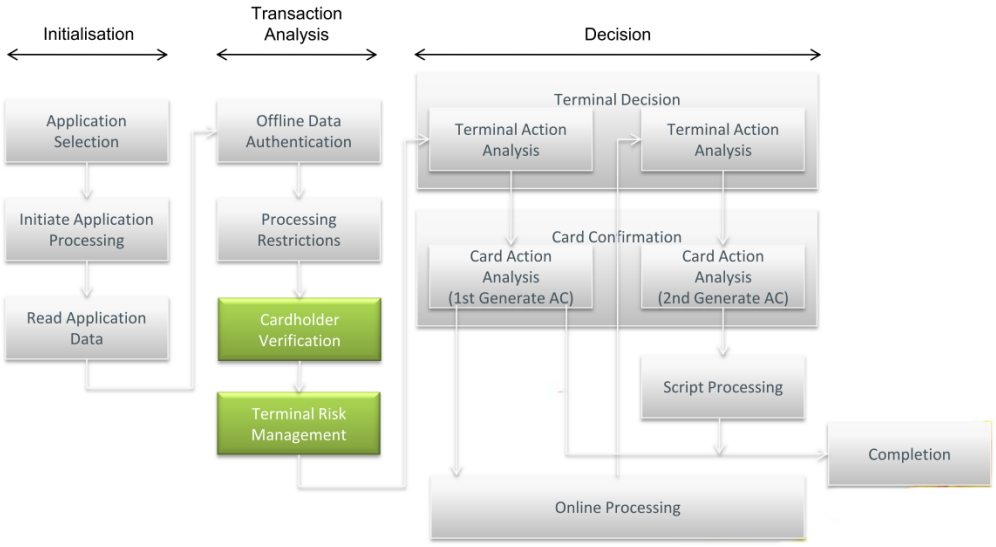


FIGURE 5.8 – Les différentes étapes d'une transaction EMV complète.

digitale reçu par le serveur et le comparer à celui attendu. Si la comparaison est négative, un temps de pénalisation proportionnel au nombre d'essais infructueux sera appliqué, permettant ainsi d'éviter des attaques par brute force. Plus un attaquant essayera d'attaquer le système et plus le temps entre chaque tentative sera long.

5.2.5 Bilan

Notre problématique est de déterminer la classe d'empreintes digitales uniquement avec les informations disponibles dans le template ISO. Nous avons proposé deux méthodes de reconnaissance du type d'empreintes digitales basées uniquement sur le template ISO et sans accès à l'image ou l'image reconstruire à partir du template. La première consiste en la création d'un vecteur contenant des histogrammes pour chacun des paramètres du template ISO. Avec ce vecteur, nous obtenons 80,37% de taux de reconnaissance, mais nous avons observé que l'attribut ISO_Angle est le paramètre permettant d'obtenir à lui seul un bon taux de reconnaissance avec 80,23%. C'est pourquoi la seconde méthode est basée sur une approche géométrique basée sur la triangulation de Delaunay, permettant d'obtenir plus de paramètres tout en gardant le paramètre ISO_Angle. Avec cette méthode, nous augmentons de 9% le taux de reconnaissance et nous obtenons 89% de bonnes classification des empreintes digitales. En comparaison, Jain *et al.* ont développé une méthode de reconnaissance du type d'empreintes digitales basée sur l'image et ont obtenu un taux de reconnaissance de 90% [137]. Notre méthode est proche du taux de reconnaissance

de référence basé sur l'image, ce qui montre que la méthode proposée est prometteuse et peut encore être améliorée.

Dans notre cas d'étude, nous avons deux approches possibles et nous devons choisir parmi l'une d'elles. La première permet d'avoir un taux de reconnaissance du type de 89% mais demande un temps de calcul plus élevé et plus de ressources. La seconde quant à elle utilise moins de ressources et une approche plus rapide basée sur le template ISO mais avec seulement 80% de reconnaissance du type d'empreintes digitales.

5.3 Conclusion

Dans ce chapitre, nous avons deux contributions majeures, la première consiste à évaluer les informations utiles, sur un système biométrique, pour un attaquant lorsque le capteur biométrique est corrompu. Sur ce type d'attaque, nous avons vu que seulement quatre paramètres sont disponibles, le type de capteur, la résolution, le nombre de minutie et le type de l'empreinte. Nous avons démontré que seulement deux d'entre elles permettent d'avoir des informations permettant de se faire accepter par le système, la résolution de l'image et, le plus important, le type de template biométrique enrôlé sur le système. C'est pourquoi, notre deuxième contribution consiste à proposer une méthode permettant de reconnaitre le type d'empreinte digitale à partir du simple template de minutie et sans aucun accès à l'image originale. Dans cette étude, nous arrivons à avoir des taux de reconnaissance du type d'empreintes digitales de l'ordre de 89%, tout comme l'image mais avec beaucoup moins d'informations.

Ces travaux nous ont permis de proposer de nouvelles attaques et méthodes de reconnaissance du type d'empreinte et ont été valorisées par une publication nationale et deux publications internationales.

Conclusions et perspectives

Bilan

Au cours de cette thèse, nous nous sommes intéressés à l'évaluation des systèmes biométriques embarqués sur des éléments sécurisés de type Carte à puce. Nous avons proposé des moyens permettant d'évaluer des systèmes biométriques embarqués en utilisant les méthodes classiques d'évaluation. Après une présentation générale de cette thèse faite dans le chapitre 1, nous avons présenté la biométrie, son cadre d'utilisation, les caractéristiques composant les modalités biométriques, ainsi que les métriques permettant l'évaluation d'un système biométrique. Nous avons aussi introduit l'aspect embarqué avec la carte à puce autrement nommé élément sécurisé (SE), en présentant des généralités sur les SE et plus spécialement sur la carte à puce, avec les possibilités offertes par le micro-processeur, les limitations en terme de taille mémoire et capacité de calcul. Nous avons aussi introduit l'aspect de transaction bancaire avec la sécurisation des communications entre une application et un SE, tout ceci est présenté dans le chapitre 2. Ces deux premiers chapitres définissent le contexte de cette thèse, ainsi que les outils préalables à notre étude. Nous avons ensuite présenté les trois contributions de cette thèse liès à l'évaluation d'un système biométrique embarqué sur élément sécurisé avec :

1. dans le chapitre 3, une plateforme d'évaluation ;
2. la réduction de template biométrique au format ISO lorsque la taille du template biométrique est supérieur à la capacité de stockage de l'élément sécurisé dans le chapitre 4 ;
3. et dans le chapitre 5, la sécurité du système biométrique lorsque l'attaquant a des a priori sur la donnée biométrique stockée sur l'élément sécurisé.

La première contribution, présentée dans le chapitre 3, concerne la proposition d'une plateforme d'évaluation de systèmes biométriques embarqués sur élément sécu-

risés (EVABIO). Cette plateforme offre la possibilité d'effectuer de manière simple et rapide des ajouts de module spécifiques pour permettre l'évaluation. Par exemple, le fait d'avoir pensé l'architecture de cette plateforme autour d'un noyau central permettant de gérer chaque module indépendamment et d'offrir des mécanismes d'échanges d'informations entre les modules sans qu'ils se connaissent. Cette plateforme offre aussi la possibilité d'effectuer des scénarios de tests, pour ainsi permettre une reproductibilité des résultats de recherche. Mais aussi de pouvoir communiquer avec un élément sécurisé de type à carte, qu'importe le support. Nous avons aussi la possibilité de constituer des bases de données en effectuant des campagnes d'acquisitions à partir de différents capteurs biométriques. La plateforme EVABIO à fait l'objet de plusieurs publications [89, 138, 139, 88]. Cette plateforme a servi de support au différents travaux menés durant cette thèse.

La deuxième contribution, présentée dans le chapitre 4, propose des méthodes de réduction de templates biométriques au format ISO, lorsque la taille de ces templates est trop importante pour être stockée sur un élément sécurisé. L'intérêt de ces méthodes est d'éviter de demander à l'utilisateur d'avoir à reposer son doigt sur le capteur pour avoir un nouveau template avec la taille désirée. Cela permet aussi d'avoir un gain d'un point de vue vitesse de traitement sachant que l'on est dans un contexte bancaire. Les méthodes ont été classées en quatre grandes familles, permettant ainsi de mieux comprendre leurs fonctionnement. Une évaluation a été effectuée avec la plateforme, permettant ainsi de comparer les méthodes entres elles, aussi bien d'un point de vue temps de réduction du template, que performance globale du système. Cette évaluation a été effectuée sur trois bases de données FVC, très souvent utilisées dans l'état de l'art, ainsi que sur trois algorithmes de comparaisons, Bozorth3 développé par le NIST et MCC par l'université de Bologne, très connu dans le milieu académique ainsi qu'un algorithme commercial. Grâce à cette évaluation, nous avons observé que la méthode K-Means reste la plus performante et la plus stable quels que soient l'algorithme de comparaison et la base de données utilisée. Cette méthode n'est pas la plus rapide mais reste la plus performante. Nous avons aussi proposé une méthode basée sur des algorithmes génétiques permettant d'avoir une estimation de la réduction optimale que l'on peut obtenir pour un algorithme de comparaison. Ceci nous permet d'avoir le template de minuties réduit le plus proche du template avant réduction, tout en ayant le moins d'impact sur la bonne reconnaissance de l'individu sur le système biométrique complet. Ces travaux ont été présentés dans [140, 141].

La troisième contribution, présentée dans le chapitre 5, est liée à l'évaluation des systèmes biométriques en terme de sécurité. Ici il s'agit de déterminer quels

a priori sont utiles pour un attaquant lorsqu'il arrive à passer outre le capteur d'empreinte pour injecter de fausses données. Nous avons donc utilisé les quatre informations présentes sur un capteur, tels que la résolution de l'image, le type de capteur biométrique, le type d'empreinte digitale, ainsi que le nombre de minuties extraites de l'image. A partir de ces informations, nous avons évalué chacune d'elles indépendamment, nous permettant ainsi de voir l'incidence de cette connaissance pour un attaquant sur le système biométrique embarqué dans l'élément sécurisé. Nous avons, de ce fait, pu démontrer que la connaissance du type de l'empreinte digitale ainsi que la résolution de l'image peuvent aider un attaquant à se faire accepter par le système. Par exemple, pour le type de l'empreinte digitale, un attaquant peut ainsi avoir un taux d'acceptation sur le système de 50%, soit une chance sur deux, avec l'algorithme Bozorth3 et une empreinte de type Arche. A contrario, sur un autre algorithme, MCC, le type d'empreinte spirale permet à l'attaquant d'être accepté environ 2% du temps. Cette contribution, nous a permis de voir que la connaissance du type de l'empreinte digitale par un attaquant est très importante. C'est pourquoi nous avons proposé une méthode permettant de reconnaitre le type de l'empreinte digitale non pas à partir de l'image mais à partir du template de minuties, et ce toujours pour un gain de temps et de ressource mémoire et calculatoire limité sur un élément sécurisé de type carte à puce. Nous avons proposé une méthode basée sur la Triangulation de Delaunay, afin de ne plus garder le lien entre la spatialité des minuties dans le repère orthonormé, nous permettant ainsi de ne se concentrer que sur la partie géométrique de l'empreinte. L'utilisation d'un SVM nous a permis de définir un modèle par classe d'empreintes digitales, et nous obtenons un taux de reconnaissance de 89% simplement avec le template de minuties. Les différents travaux effectués sur l'image obtiennent le même taux de reconnaissance avec beaucoup plus d'informations. Nous avons proposé d'utiliser cette reconnaissance du type de l'empreinte digitale dans une transaction bancaire pour éviter l'attaque présentée. Ces travaux ont été présentés dans [117, 142, 143].

Perspectives

Les perspectives de cette thèse sont nombreuses :

1. En ce qui concerne la plateforme d'évaluation, certains modules sont à améliorer pour permettre d'intégrer de nouvelles métriques de qualités d'images d'empreintes digitales, comme NFIQ 2 sortie cette année. Une première approche du module de génération de rapport d'évaluation a été faite, il reste cependant à la rendre plus stable et aboutie. Nous souhaiterions fournir de

manière libre le plugin Evaluation, qui permet, à partir d'un fichier de résultats de produire de manière automatique les courbes ROC, distribution des scores, évolution de l'EER en fonction du FAR/FRR. Ce plugin sera à destination des chercheurs et industriels en biométrie, leurs permettant ainsi d'avoir une génération homogène des résultats. Cette première étape, permettra de faire connaitre la plateforme aux chercheurs et industriels du domaine, notre perspective principale étant de faire certifier notre plateforme EVABIO pour qu'elle soit la plateforme de référence pour l'évaluation des systèmes biométriques embarqués, nous permettant ainsi de proposer la plateforme aux industriels sous forme de licence. La partie sécuritaire doit continuer à être développée pour proposer de nouvelles attaques sur un élément sécurisé de type carte à puce.

2. Pour la sélection des minuties dans un template biométrique ISO, la méthode basée sur la triangulation de Delaunay est intéressante, mais pas assez performante, nous souhaiterions la tester avec de nouveaux attributs, car nous pensons que cette approche a un très fort potentiel. Nous souhaiterions aussi développer sur l'élément de sécurité les méthodes les plus performantes pour ainsi avoir un temps réel d'exécution de ces dernières. Il faudrait aussi travailler sur l'optimisation du code des méthodes pour gagner niveau temps de traitement et ainsi respecter la contrainte d'avoir un temps d'exécution inférieur à 500ms. Dans cette thèse, nous nous sommes attardés sur le format ISO Compact Card II, mais d'autres formats sont disponibles, comme celui du NIST, proposant de nouvelles informations, comme par exemple une qualité de la minutie extraite. Ce nouveau format, nous permettra peut-être d'améliorer nos performances en terme de taux de reconnaissance lors de la réduction du template. Nous souhaitons aussi continuer nos recherches sur les méthodes de réductions de templates biométriques mais en essayant de trouver quels éléments nous permettraient de caractériser une empreinte digitale.

3. Pour finir sur la partie attaque, nous n'avons testé que deux points du système de Ratha *et al.* et nous souhaiterions proposer d'autres modules sur la plateforme permettant d'effectuer de nouvelles attaques. Dans cette thèse, nous nous sommes attardés sur la partie biométrique, mais nous pouvons aussi utiliser celles présentes dans le domaine de la carte. Dans le domaine de la carte, il existe de nombreuses attaques, que ce soit physique, par canaux cachés, par consommation de courant, ces différents éléments peuvent peut-être nous aider à faciliter une attaque lorsque la donnée biométrique

est stockée sur un élément sécurisé. En ce qui concernent la détection du type de l'empreinte digitale à partir du template de minuties, de nombreux travaux restent à faire, comme par exemple optimiser les paramètres du SVM pour augmenter encore le taux de reconnaissance. Nous pouvons aussi utiliser d'autres paramètres avec la triangulation de Delaunay, nous permettant ainsi d'avoir de nouvelles perspectives d'études. De même sur les histogrammes normalisés, nous pourrions utiliser la divergence de Rényi [144] qui permet de comparer deux histogrammes. Cette divergence est moins coûteuse en temps de calcul et ne nécessite pas l'utilisation d'un SVM.

4. Dans cette thèse, nous nous sommes aperçus que beaucoup de travaux utilisent le CORE de l'empreinte digitale pour faire l'extraction des minuties, de la réduction de template ou bien encore des algorithmes de comparaison comme MCC. Si l'on prend le format ISO Compact Card II, nous n'avons aucune information sur l'emplacement du CORE. Une perspective intéressante serait d'avoir une méthode permettant d'estimer la position de ce point en ayant simplement accès au template de minutie et non à l'image.

5. J'aimerai aussi travailler plus précisément sur l'aspect protection de la vie privé des données biométriques et plus particulièrement sur le Bio-Hashing. Ce sont des techniques permettant de transposer, dans un autre espace, les données biométriques à partir d'un secret. Ces méthodes de Bio-Hashing permettent de rendre la donnée biométrique révocable, en changeant le secret, mais surtout de ne pas pouvoir retrouver la donnée biométrique originale même en connaissant le secret. Pour moi, le fait d'utiliser des données biométriques révocables va permettre à la biométrie de prendre une place encore plus importante dans le moyen d'authentification ou d'identification d'un individu et les utilisateurs seront moins méfiants vis à vis des systèmes biométriques.

Publications de l'auteur

Chapitre de livre international

1. **Vibert, B.**, Yao, Z., Vernois, S., Le Bars, J. M., Charrier, C., & Rosenberger, C. (2015, February). Evabio a new modular platform to evaluate biometric system. In International Conference on Information Systems Security and Privacy (pp. 234-250). Springer International Publishing.

Conférences internationales avec comité de lecture et avec actes

1. **Vibert, B**, Le Bars, J. M., Charrier, C., & Rosenberger, C,. Fingerprint Class Recognition For Securing EMV Transaction. International Conference on Information Systems Security and Privacy (ICISSP), Feb 2017, Porto, Portugal.
2. **Vibert, B.**, Charrier, C., Le Bars, J. M., & Rosenberger, C. (2015, March). Comparative study of minutiae selection algorithms for iso fingerprint templates. In SPIE/IS&T Electronic Imaging (pp. 94090C-94090C). International Society for Optics and Photonics.
3. **Vibert, B.**, Rosenberger, C., & Ninassi, A. (2013, June). Security and performance evaluation platform of biometric match on card. In Computer and Information Technology (WCCIT), 2013 World Congress on (pp. 1-6). IEEE.
4. **Vibert, B.**, Lebouteiller, J., Keita, F., & Rosenberger, C. (2014). Biometric sensor and match-on-card evaluation platform. In International Biometric Performance Testing Conference (IBPC).
5. **Vibert, B.**, Yao, Z., Vernois, S., Le Bars, J. M., Charrier, C., & Rosenberger, C. (2015, February). EvaBio platform for the evaluation biometric system : Ap-

plication to the optimization of the enrollment process for fingerprints devices. In Information Systems Security and Privacy (ICISSP), 2015 International Conference on (pp. 329-335). IEEE.

6. **Vibert, B.**, Le Bars, J. M., Charrier, C., & Rosenberger, C. (2016, September). In what way is it possible to impersonate you bypassing fingerprint sensors ?. In Biometrics Special Interest Group (BIOSIG), 2016 International Conference of the (pp. 1-4). IEEE.
7. Yao, Z., **Vibert, B.**, Charrier, C., & Rosenberger, C. (2015, March). Blind minutiae selection for standard minutiae templates. In Identity, Security and Behavior Analysis (ISBA), 2015 IEEE International Conference on (pp. 1-6). IEEE.

Conférences nationales avec comité de lecture et avec actes

1. **Vibert, B.**, Le Bars, J. M., Charrier, C., & Rosenberger, C. (2016, May). Analyse d'empreintes digitales a partir de paramètres structurels calculés sur une référence réduite de l'image. In COmpression et REpre ?sentation des Signaux Audiovisuels (CORESA).
2. **Vibert, B.**, Alimi, V., & Vernois, S. (2012). Analyse de la sécurité de transactions à puce avec le framework winscard tools. In SAR-SSI 2012 (p. 8).

Bibliographie

[1] Francis Galton. *Fingerprint directories*. Macmillan and Company, 1895. [cité p. 6]

[2] Bertillon. Fiche bertillon. http ://guillotine.cultureforum.net/t3028-henri-leon-scheffer-premiere-exploitation-des-traces-papillaires. [cité p. 7, 149]

[3] Larousse. Définition. http ://www.larousse.fr/encyclopedie/divers/biométrie/27110. [cité p. 8]

[4] Masaki Hashiyada. Development of biometric dna ink for authentication security. *The Tohoku journal of experimental medicine*, 204(2) :109–117, 2004. [cité p. 8]

[5] Ranbir Soram, Memeta Khomdram, et al. Biometric dna and ecdlp-based personal authentication system : a superior posse of security. *Int. J. Comput. Sci. Netw. Secur*, 10(1) :1–9, 2010. [cité p. 8]

[6] Zhanna Korotkaya. Biometric person authentication : Odor. *Inner report in Department of Information Technology, Laboratory of Applied Mathematics, Lappeenranta University of Technology. in "Advanced Topics in Information Processing : Biometric Person Authentication"*, 2003. [cité p. 8]

[7] Koksoon Phua, Jianfeng Chen, Tran Huy Dat, and Louis Shue. Heart sound as a biometric. *Pattern Recognition*, 41(3) :906–919, 2008. [cité p. 8]

[8] Nashwa El-Bendary, Hameed Al-Qaheri, Hossam M Zawbaa, Mohamed Hamed, Aboul Ella Hassanien, Qiangfu Zhao, and Ajith Abraham. Hsas : Heart sound authentication system. In *Nature and Biologically Inspired Computing (NaBIC), 2010 Second World Congress on*, pages 351–356. IEEE, 2010. [cité p. 8]

[9] Zhidong Zhao, Qinqin Shen, and Fangqin Ren. Heart sound biometric system based on marginal spectrum analysis. *Sensors*, 13(2) :2530–2551, 2013. [cité p. 8]

[10] Thierry Artieres, J-M Marchand, Patrick Gallinari, and Bernadette Dorizzi. Multimodal segmental models for online handwriting recognition. In *Pattern Recognition, 2000. Proceedings. 15th International Conference on*, volume 2, pages 247–250. IEEE, 2000. [cité p. 8]

[11] Nesma Houmani, Sonia Garcia-Salicetti, and Bernadette Dorizzi. On assessing the robustness of pen coordinates, pen pressure and pen inclination to time variability with personal entropy. In *Biometrics : Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on*, pages 1–6. IEEE, 2009. [cité p. 8]

[12] Anil Jain, Ruud Bolle, and Sharath Pankanti. *Biometrics : personal identification in networked society*, volume 479. Springer Science & Business Media, 2006. [cité p. 8]

[13] Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. Greyc keystroke : a benchmark for keystroke dynamics biometric systems. In *Biometrics : Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on*, pages 1–6. IEEE, 2009. [cité p. 8]

[14] Marcus Karnan, Muthuramalingam Akila, and Nishara Krishnaraj. Biometric personal authentication using keystroke dynamics : A review. *Applied Soft Computing*, 11(2) :1565–1573, 2011. [cité p. 8]

[15] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, and Patrick Bours. Soft biometrics for keystroke dynamics : Profiling individuals while typing passwords. *Computers & Security*, 45 :147–155, 2014. [cité p. 8]

[16] Ju Man and Bir Bhanu. Individual recognition using gait energy image. *IEEE transactions on pattern analysis and machine intelligence*, 28(2) :316–322, 2006. [cité p. 8]

[17] Pierluigi Casale, Oriol Pujol, and Petia Radeva. Personalization and user verification in wearable systems using biometric walking patterns. *Personal and Ubiquitous Computing*, 16(5) :563–580, 2012. [cité p. 8]

[18] Gary M Weiss and Jeffrey W Lockhart. Identifying user traits by mining smart phone accelerometer data. In *Proceedings of the Fifth International Workshop on Knowledge Discovery from Sensor Data*, pages 61–69. ACM, 2011. [cité p. 8]

[19] Anil K Jain, Lin Hong, Sharath Pankanti, and Ruud Bolle. An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 85(9) :1365–1388, 1997. [cité p. 9]

[20] Yi Chen and Anil K Jain. Beyond minutiae : A fingerprint individuality model with pattern, ridge and pore features. In *International Conference on Biometrics*, pages 523–533. Springer, 2009. [cité p. 9]

[21] Ruud M Bolle, Jonathan Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. *Guide to biometrics*. Springer Science & Business Media, 2013. [cité p. 9]

[22] Anil Jain, Patrick Flynn, and Arun A Ross. *Handbook of biometrics*. Springer Science & Business Media, 2007. [cité p. 9]

[23] Esteban Vazquez-Fernandez and Daniel Gonzalez-Jimenez. Face recognition for authentication on mobile devices. *Image and Vision Computing*, 2016. [cité p. 9]

[24] Ahana Gangopadhyay, Oindrila Chatterjee, and Amitava Chatterjee. Hand shape based biometric authentication system using radon transform and collaborative representation based classification. In *Image Information Processing (ICIIP), 2013 IEEE Second International Conference on*, pages 635–639. IEEE, 2013. [cité p. 9]

[25] Ana M Bernardos, Jose M Sánchez, Javier I Portillo, Juan A Besada, and José R Casar. A contactless identification system based on hand shape features. *Procedia Computer Science*, 52 :161–168, 2015. [cité p. 9]

[26] John Daugman. New methods in iris recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, 37(5) :1167–1175, 2007. [cité p. 9]

[27] Kurt Horvath, Herbert Stögner, Georg Weinhandel, and Andreas Uhl. Experimental study on lossless compression of biometric iris data. In *Image and Signal Processing and Analysis (ISPA), 2011 7th International Symposium on*, pages 379–384. IEEE, 2011. [cité p. 9]

[28] Maria De Marsico, Michele Nappi, Daniel Riccio, and Harry Wechsler. Mobile iris challenge evaluation (miche)-i, biometric iris dataset and protocols. *Pattern Recognition Letters*, 57 :17–23, 2015. [cité p. 9]

[29] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1) :4–20, 2004. [cité p. 9, 11]

[30] Is Alice. Biometric recognition : Security and privacy concerns. *IEEE Security & Privacy*, 2003. [cité p. 9]

[31] Julien Mahier, Marc Pasquet, Christophe Rosenberger, and Felix Cuozzo. Biometric authentication. *Encyclopedia of Information Science and Technology*, 13, 2008. [cité p. 10, 153]

[32] Gustavo Stolovitzky and Isidore Rigoutsos. 1 4 dna based identification. *Biometrics : Personal Identification in Networked Society*, 479 :287, 2006. [cité p. 10]

[33] CNIL. Communication de la cnil relative à la mise en oeuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données. https ://www.cnil.fr/sites/default/files/typo/document/Communication-biometrie.pdf. [cité p. 11]

[34] ISO ISO. Iec 19795-1 : Information technology-biometric performance testing and reporting-part 1 : Principles and framework. *ISO/IEC, Editor*, 2006. [cité p. 12, 13, 22, 23, 27, 149]

[35] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems journal*, 40(3) :614–634, 2001. [cité p. 14, 30, 32, 55, 102, 104, 150, 152]

[36] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Electronic Imaging 2002*, pages 275–289. International Society for Optics and Photonics, 2002. [cité p. 14]

[37] Parafe. Parafe. http ://www.parafe.gouv.fr/. [cité p. 15]

[38] Oracle. Javacard. http ://www.oracle.com/technetwork/java/embedded/javacard/. [cité p. 16]

[39] Global Platform. https ://www.globalplatform.org/. [cité p. 16, 18]

[40] JavaCardForum. Javacardforum. https ://javacardforum.com/. [cité p. 16]

[41] ISO. *ISO/IEC 7816-1 to 15 : Identification cards - Integrated circuit(s) cards with contacts(Parts 1 to 15).* ISO/IEC, http ://www.iso.org. [cité p. 17, 50]

[42] EMVCo. EMV integrated circuit card specifications for payment systems. Technical report, EMVCo, 2008. [cité p. 18, 44, 124]

[43] ST. *NFC controller and Secure Element system-in-package.* ST. [cité p. 19]

[44] ISO/IEC 19794-2. information technology - biometric data interchange format format - part 2 : Finger minutiae data, 2011. [cité p. 19, 102]

[45] Francis Galton. *Finger prints.* Macmillan and Company, 1892. [cité p. 20]

[46] Eamonn Keogh. An overview of the science of fingerprints. *Anil Aggrawal's Internet Journal of Forensic Medicine & Toxicology*, 14(1), 2013. [cité p. 21, 149]

[47] ISO/IEC 19795-2. information technology - biometric performance testing and reporting - part 2 : Testing methodologies for technology and scenario evaluation, 2007. [cité p. 21, 40, 64]

[48] NIST. Nist fingerprint testing and standards. http ://www.nist.gov/itl/iad/ig/fingerprint.cfm, 02 2013. [cité p. 22]

[49] Mohamad El Abed, Alexandre Ninassi, Christophe Charrier, and Christophe Rosenberger. Fingerprint quality assessment using a no-reference image quality metric. In *21st European Signal Processing Conference (EUSIPCO 2013)*, pages 1–5. IEEE, 2013. [cité p. 22, 29, 30, 150]

[50] Zhigang Yao, Christophe Charrier, and Christophe Rosenberger. Utility validation of a new fingerprint quality metric. In *International Biometric Performance Testing Conference (IBPC)*, 2014. [cité p. 22]

[51] ISO. ISO/IEC fcd 19792. information technology - security techniques - security evaluation of biometrics, 2008. [cité p. 22]

[52] M Theofanos, B Stanton, and CA Wolfson. Usability & biometrics : Ensuring successful biometric systems. *National Institute of Standards and Technology (NIST)*, page 23, 2008. [cité p. 23, 32]

[53] James P Egan. Signal detection theory and {ROC} analysis. 1975. [cité p. 23, 26, 50]

[54] Alvin Martin, George Doddington, Terri Kamm, Mark Ordowski, and Mark Przybocki. The det curve in assessment of detection task performance. Technical report, DTIC Document, 1997. [cité p. 23]

[55] Jay Bhatnagar and Ajay Kumar. On estimating performance indices for biometric identification. *Pattern Recognition*, 42(9) :1803–1815, 2009. [cité p. 23, 27]

[56] Mohamad El-Abed. *Évaluation de système biométrique*. PhD thesis, Université de Caen, 2011. [cité p. 25, 31, 32, 149]

[57] Aadhaar. Aadhaar Proejct UID. https ://uidai.gov.in/beta/. [cité p. 26]

[58] David Faraggi and Benjamin Reiser. Estimation of the area under the roc curve. *Statistics in medicine*, 21(20) :3093–3106, 2002. [cité p. 28]

[59] Roberto Tronci, Giorgio Giacinto, and Fabio Roli. Designing multiple biometric systems : Measures of ensemble effectiveness. *Engineering Applications of Artificial Intelligence*, 22(1) :66–78, 2009. [cité p. 28]

[60] Henry B Mann and Donald R Whitney. On a test of whether one of two random variables is stochastically larger than the other. *The annals of mathematical statistics*, pages 50–60, 1947. [cité p. 28]

[61] Ruud M Bolle, Nalini K Ratha, and Sharath Pankanti. Error analysis of pattern recognition systems-the subsets bootstrap. *Computer Vision and Image Understanding*, 93(1) :1–33, 2004. [cité p. 28]

[62] Lorène Allano. *La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles*. PhD thesis, Evry, Institut national des télécommunications, 2009. [cité p. 28]

[63] Fernando Alonso-Fernandez, Julian Fierrez, Javier Ortega-Garcia, Joaquin Gonzalez-Rodriguez, Hartwig Fronthaler, Klaus Kollreider, and Josef Bigun. A comparative study of fingerprint image-quality estimation methods. *IEEE Transactions on Information Forensics and Security*, 2(4) :734–743, 2007. [cité p. 29]

[64] LinLin Shen, Alex Kot, and WaiMun Koo. Quality measures of fingerprint images. In *International Conference on Audio-and Video-Based Biometric Person Authentication*, pages 266–271. Springer, 2001. [cité p. 29]

[65] Yi Chen, Sarat C Dass, and Anil K Jain. Fingerprint quality indices for predicting authentication performance. In *Audio-and Video-Based Biometric Person Authentication*, pages 160–170. Springer, 2005. [cité p. 29, 48]

[66] Sanghoon Lee, Chulhan Lee, and Jaihie Kim. Model-based quality estimation of fingerprint images. In *International Conference on Biometrics*, pages 229–235. Springer, 2006. [cité p. 29]

[67] Elham Tabassi and Charles L Wilson. A novel approach to fingerprint image quality. In *Image Processing, 2005. ICIP 2005. IEEE International Conference on*, volume 2, pages II–37. IEEE, 2005. [cité p. 29, 48]

[68] Oliver Bausinger and Elham Tabassi. Fingerprint sample quality metric nfiq 2.0. In *BIOSIG*, pages 167–171, 2011. [cité p. 30]

[69] Anil K Jain, Karthik Nandakumar, and Arun Ross. 50 years of biometric research : Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 2016. [cité p. 30, 32, 102, 150]

[70] Eric P Kukula and Robert W Proctor. Human-biometric sensor interaction : Impact of training on biometric system and user performance. In *Symposium on Human Interface*, pages 168–177. Springer, 2009. [cité p. 31]

[71] Anil K Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, and Arun Ross. Biometrics : a grand challenge. In *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, volume 2, pages 935–942. IEEE, 2004. [cité p. 31, 33, 150]

[72] Eric P Kukula, Christine R Blomeke, Shimon K Modi, and Stephen J Elliott. Effect of human-biometric sensor interaction on fingerprint matching performance, image quality and minutiae count. *International Journal of Computer Applications in Technology*, 34(4) :270–277, 2009. [cité p. 32]

[73] A Westin. Public attitudes toward the uses of biometric identification technologies by government and the private sector : summary of survey findings. *Opinion Research Corporation (ORC) International*, 2002. [cité p. 32]

[74] Eric P Kukula, Mathias J Sutton, and Stephen J Elliott. The human–biometric-sensor interaction evaluation method : biometric performance and usability measurements. *IEEE Transactions on Instrumentation and Measurement*, 59(4) :784–791, 2010. [cité p. 32]

[75] Mohamad El-Abed, Romain Giot, Baptiste Hemery, and Christophe Rosenberger. A study of users' acceptance and satisfaction of biometric systems. In *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*, pages 170–178. ieee, 2010. [cité p. 32]

[76] Laurie A Jones, Annie I Antón, and Julia B Earp. Towards understanding user perceptions of authentication technologies. In *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, pages 91–98. ACM, 2007. [cité p. 32]

[77] Definition plateforme logicelle. https ://fr.wikipedia.org/wiki/Plate-forme. [cité p. 35]

[78] MISTRAL. Mistral project. http ://www.agence-nationale-recherche.fr/ ?Projet=ANR-06-TLOG-0001. [cité p. 37]

[79] ALIZE. Alize project. http ://mistral.univ-avignon.fr/. [cité p. 37, 38, 150]

[80] P Grother, W Salamon, C Watson, M Indovina, and P Flanagan. Minex ii "performance of fingerprint match-on-card algorithms" phase iv : report NIST interagency report 7477 (revision ii). 2011. [cité p. 38, 54]

[81] Patricia Flanagan. Minex iii-what's new. 2015. [cité p. 39]

[82] NIST. Minex minutiae exchange. http ://www.nist.gov/itl/iad/ig/minexiii.cfm, 2015. [cité p. 39, 150]

[83] Biolab. FVConGoing. https ://biolab.csr.unibo.it/FVCOnGoing, 2009. [cité p. 39]

[84] D Maio, D Maltoni, R Capelli, A Franco, M Ferrara, and F Turroni. Fvc-ongoing : on-line evaluation of fingerprint recognition algorithms. *URL https ://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx*, 2013. [cité p. 40, 150]

[85] BEAT Project. Beat project. https ://www.beat-eu.org/, 2013. [cité p. 40]

[86] BEAT Project. BEAT Platform. https ://www.beat-eu.org/platform/. [cité p. 41, 150]

[87] PUB FIPS. 201, personal identity verification (piv) of federal employees and contractors, march 2006. *URL : http ://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1. pdf (23.02. 2012).* [cité p. 41]

[88] B Vibert, Z Yao, Sylvain Vernois, Jm Le Bars, Christophe Charrier, and Christophe Rosenberger. Evabio platform for the evaluation biometric system : Application to the optimization of the enrollment process for fingerprint device. In *International Conference on Information Systems Security and Privacy*, 2015. [cité p. 43, 105, 128, 152]

[89] Benoit Vibert, Christophe Rosenberger, and Alexandre Ninassi. Security and performance evaluation platform of biometric match on card. In *Computer and Information Technology (WCCIT), 2013 World Congress on*, pages 1–6. IEEE, 2013. [cité p. 43, 54, 128]

[90] Benoit Vibert, Vincent Alimi, and Sylvain Vernois. Analyse de la securite de transactions a puce avec le framework winscard tools. *SAR-SSI 2012*, page 8, 2012. [cité p. 44]

[91] Steven Murdoch, Saar Drimer, Ross Anderson, and Mike Bond. Chip and PIN is broken. In David Evans and Giovanni Vigna, editors, *SSP 2010, 31st IEEE Symposium on Security & Privacy*, Piscataway, NJ, USA, May 2010. IEEE Computer Society Technical Committee on Security and Privacy/The International Association for Cryptologic Research, IEEE Computer Society. [cité p. 44, 124]

[92] Julien Lancia. Un framework de fuzzing pour cartes à puce : application aux protocoles emv. In *Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC)*, page 82, 2011. [cité p. 46]

[93] Raffaele Cappelli, D Maio, and D Maltoni. Sfinge : an approach to synthetic fingerprint generation. In *International Workshop on Biometric Technologies (BT2004)*, pages 147–154, 2004. [cité p. 47, 104, 106]

[94] P. Grother and E. Tabassi. Performance of biometric quality measures. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(4) :531–543, 2007. [cité p. 48]

[95] Mohamad El-Abed, Baptiste Hemery, Christophe Charrier, Christophe Rosenberger, et al. Evaluation de la qualité de données biométriques. *Revue des Nouvelles Technologies de l'information (RNTI)*, pages 1–22, 2011. [cité p. 48, 58]

[96] ISO. ISO/IEC 2382-37. information technology - vocabulary - part 37 : Biometrics, 2012. [cité p. 49, 77]

[97] Rima Belguechi, Adel Hafiane, Estelle Cherrier, and Christophe Rosenberger. Comparative study on texture features for fingerprint recognition : Application to the biohashing template protection scheme. [cité p. 52, 150]

[98] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008 :113, 2008. [cité p. 57]

[99] Patrick Grother and Wayne Salamon. Interoperability of the iso/iec 19794-2 compact card and 10 iso/iec 7816-11 match-on-card specifications 11. 2007. [cité p. 64, 66]

[100] Nikhil R Pal and James C Bezdek. On cluster validity for the fuzzy c-means model. *Fuzzy Systems, IEEE Transactions on*, 3(3) :370–379, 1995. [cité p. 71]

[101] Fvc2002db2. http ://bias.csr.unibo.it/fvc2002/download.asp. [cité p. 75]

[102] Fvc2004db1. http ://bias.csr.unibo.it/fvc2004/databases.asp. [cité p. 75]

[103] Davide Maltoni, Dario Maio, Anil Jain, and Salil Prabhakar. *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009. [cité p. 75]

[104] C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. Mccabe, S. Janet, and K. Ko. User's guide to nist biometric image software (nbis). Technical report, NIST, 2007. [cité p. 76, 116]

[105] Raffaele Cappelli, Matteo Ferrara, and Davide Maltoni. Minutia cylinder-code : A new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(12) :2128–2141, 2010. [cité p. 77, 79]

[106] John H Holland. *Adaptation in natural and artificial systems : an introductory analysis with applications to biology, control, and artificial intelligence.* U Michigan Press, 1975. [cité p. 89]

[107] Ingo Rechenberg. Evolutionsstrategie94. frommann-holzboog-verlag, stuttgart (germany), 1994. *German ; includes also*, 1581. [cité p. 89]

[108] Matthew Bartschi Wall. *A genetic algorithm for resource-constrained scheduling.* PhD thesis, Massachusetts Institute of Technology, 1996. [cité p. 89]

[109] Umut Uludag and Anil K Jain. Attacks on biometric systems : a case study in fingerprints. In *Electronic Imaging 2004*, pages 622–633. International Society for Optics and Photonics, 2004. [cité p. 102]

[110] Marcos Martinez-Diaz, J Fierrez-Aguilar, Fernando Alonso-Fernandez, Javier Ortega-García, and JA Siguenza. Hill-climbing and brute-force attacks on biometric systems : A case study in match-on-card fingerprint verification. In *Proceedings 2006 40th Annual IEEE International Carnahan Conferences Security Technology*, pages 151–159. IEEE, 2006. [cité p. 102]

[111] Anil K Jain, Salil Prabhakar, and Lin Hong. A multichannel approach to fingerprint classification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 21(4) :348–359, 1999. [cité p. 102, 115]

[112] Qinzhi Zhang and Hong Yan. Fingerprint classification based on extraction and analysis of singularities and pseudo ridges. *Pattern Recognition*, 37(11) :2233–2243, 2004. [cité p. 102, 115]

[113] Colin Soutar et al. Biometric system security. *White Paper, Bioscrypt, http ://www. bioscrypt. com*, 2002. [cité p. 102]

[114] Dario Maio, Davide Maltoni, Raffaele Cappelli, Jim L Wayman, and Anil K Jain. Fvc2004 : third fingerprint verification competition. In *Biometric Authentication*, pages 1–7. Springer, 2004. [cité p. 106]

[115] Julian Fiérrez-Aguilar, Loris Nanni, Javier Ortega-Garcia, Raffaele Cappelli, and Davide Maltoni. Combining multiple matchers for fingerprint verification : a case study in fvc2004. In *International Conference on Image Analysis and Processing*, pages 1035–1042. Springer, 2005. [cité p. 106]

[116] HandResearch. Fingerprints world map. http ://www.handresearch.com/news/fingerprints-world-map-whorls-loops-arches.htm. [cité p. 114]

[117] B Vibert, Charrier Christophe, Jean-Marie Le Bars, and Christophe Rosenberger. In what way is it possible to impersonate you bypassing fingerprint sensors ? In *15th International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2016. [cité p. 115, 129]

[118] Bishwa Ranjan Roy and Amit Kumar Trivedi. Construction of fingerprint orientation field from minutia points. In *Advanced Communication Control and Computing*

Technologies (ICACCCT), 2014 International Conference on, pages 1439–1442. IEEE, 2014. [cité p. 115]

[119] Lars Oehlmann, Stephan Huckemann, and Carsten Gottschlich. Performance evaluation of fingerprint orientation field reconstruction methods. In *Biometrics and Forensics (IWBF), 2015 International Workshop on*, pages 1–6. IEEE, 2015. [cité p. 115]

[120] Anil Jain and Sharath Pankanti. Fingerprint classification and matching. *Handbook for Image and Video Processing*, 2000. [cité p. 115]

[121] Manoj Kumar et al. A novel fingerprint minutiae matching using lbp. In *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on*, pages 1–4. IEEE, 2014. [cité p. 115]

[122] Umarani Jayaraman, Aman Kishore Gupta, and Phalguni Gupta. An efficient minutiae based geometric hashing for fingerprint database. *Neurocomputing*, 137 :115–126, 2014. [cité p. 115]

[123] Soosai Antony Maria Celestin Vigila, Karuppiah Muneeswaran, and William Thomas Berkin Albert Antony. Biometric security system over finite field for mobile applications. *IET Information Security*, 9(2) :119–126, 2014. [cité p. 115]

[124] Kalle Karu and Anil K Jain. Fingerprint classification. *Pattern recognition*, 29(3) :389–404, 1996. [cité p. 115]

[125] Raffaele Cappelli, Alessandra Lumini, Dario Maio, and Davide Maltoni. Fingerprint classification by directional image partitioning. *IEEE Transactions on pattern analysis and machine intelligence*, 21(5) :402–421, 1999. [cité p. 115]

[126] Sen Wang, Wei Wei Zhang, and Yang Sheng Wang. Fingerprint classification by directional fields. In *Multimodal Interfaces, 2002. Proceedings. Fourth IEEE International Conference on*, pages 395–399. IEEE, 2002. [cité p. 115]

[127] Christophe Charrier, Olivier Lézoray, and Gilles Lebrun. A machine learning regression scheme to design a fr-image quality assessment algorithm. In *Conference on Colour in Graphics, Imaging, and Vision*, volume 2012, pages 35–42. Society for Imaging Science and Technology, 2012. [cité p. 116]

[128] C-W. Hsu and C-J. Lin. A comparison of methods for multiclass support vector machines. *Neural Networks, IEEE Transactions on*, 13(3) :415–425, 2002. [cité p. 116, 117]

[129] M. Kudo and J. Sklansky. Comparison of algorithms that select features for pattern classifiers. *Pattern Recognition*, 33(1) :25–41, 2000. [cité p. 116]

[130] V. N. Vapnik. *Statistical Learning Theory*. Wiley, New York, 1998. [cité p. 116]

[131] Chih-Chung Chang and Chih-Jen Lin. Libsvm : A library for support vector machines. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2(3) :27, 2011. [cité p. 118]

[132] Franz Aurenhammer. Voronoi diagramsï¿½a survey of a fundamental geometric data structure. *ACM Computing Surveys (CSUR)*, 23(3) :345–405, 1991. [cité p. 120]

[133] Peter Su and Robert L Scot Drysdale. A comparison of sequential delaunay triangulation algorithms. In *Proceedings of the eleventh annual symposium on Computational geometry*, pages 61–70. ACM, 1995. [cité p. 120]

[134] Jonathan Richard Shewchuk. Delaunay refinement algorithms for triangular mesh generation. *Computational geometry*, 22(1) :21–74, 2002. [cité p. 120]

[135] M Gopi, Shankar Krishnan, and Cláudio T Silva. Surface reconstruction based on lower dimensional localized delaunay triangulation. In *Computer Graphics Forum*, volume 19, pages 467–478, 2000. [cité p. 120]

[136] Patrick Labatut, Jean-Philippe Pons, and Renaud Keriven. Efficient multi-view reconstruction of large-scale scenes using interest points, delaunay triangulation and graph cuts. In *Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on*, pages 1–8. IEEE, 2007. [cité p. 120]

[137] Anil K Jain, Salil Prabhakar, , and Lin Hong. A multichannel approach to fingerprint classification. In *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, volume 24, pages 248–359, 1999. [cité p. 125]

[138] Benoît Vibert, John Lebouteiller, Felix Keita, and Christophe Rosenberger. Biometric sensor and match on card evaluation platform. In *International Biometric Performance Testing Conference (IBPC)*, 2014. [cité p. 128]

[139] Benoit Vibert, Zhigang Yao, Sylvain Vernois, Jean-Marie Le Bars, Christophe Charrier, and Christophe Rosenberger. Evabio a new modular platform to evaluate biometric system. In *Information Systems Security and Privacy*, pages 234–250. Springer, 2015. [cité p. 128]

[140] Benoit Vibert, Christophe Charrier, J-M Le Bars, and Christophe Rosenberger. Comparative study of minutiae selection algorithms for iso fingerprint templates. In *SPIE/IS&T Electronic Imaging*, pages 94090C–94090C. International Society for Optics and Photonics, 2015. [cité p. 128]

[141] Z Yao, B Vibert, Christophe Charrier, and Christophe Rosenberger. Blind minutiae selection for standard minutiae templates. In *Identity, Security and Behavior Analysis (ISBA), 2015 IEEE International Conference on*, pages 1–6. IEEE, 2015. [cité p. 128]

[142] B Vibert, JM Le Bars, C Charrier, and C Rosenberger. Analyse d'empreintes digitales a partir de parametres structurels calculés sur une référence réduite de l'image. [cité p. 129]

[143] Benoît Vibert, Jean-Marie Le Bars, Christophe Charrier, and Christophe Rosenberger. Fingerprint Class Recognition For Securing EMV Transaction. In *International Conference on Information Systems Security and Privacy*, Porto, Portugal, February 2017. [cité p. 129]

[144] Alfréd Rényi et al. On measures of entropy and information. In *Proceedings of the fourth Berkeley symposium on mathematical statistics and probability*, volume 1, pages 547–561, 1961. [cité p. 131]

Liste des abréviations

APDU	Application Protocol Data Unit
AUC	Area Under Curve
EER	Error Equal Rate
EMV	Europay Mastercard Visa
FAR	False Acceptance Rate
FNMR	False Non Match Rate
FMR	False Match Rate
FRR	False Rejected Rate
FTAR	Fail To Acquire Rate
FTER	Fail To Enroll Rate
GIE	Groupement d'Intérêt Économique
ISO	International Organization Standard
JCOP	JavaCard Open-Platform
JSON	JavaScript Object Notation
NFIQ	Nist Fingerprint Image Quality
OCC	On-Card-Comparison
PIN	Personal Identifier Number
PCSC	Personal Computer Smart Card
PIV	Personal Identity Verification
ROC	Receiver Operating Characteristic
SE	Secure Element
XML	Extensible Markup Language

Table des figures

Liste des tableaux

La biométrie suscite de plus en plus d'intérêt de la part des industriels car nous avons besoin de nouvelles méthodes d'authentification d'un individu : pour du contrôle d'accès physique, du contrôle aux frontières ou pour du paiement. Ces données non révocables et sensibles sont très souvent stockées sur des systèmes embarqués de type élément sécurisé (SE), comme par exemple une carte à puce. Ces SE embarquent aussi un module de comparaison nommé On-Card-Comparison (OCC), permettant de déterminer si le template présenté correspond bien à celui stocké sur l'élément sécurisé. Dans cette thèse, nous nous intéressons particulièrement aux empreintes digitales car c'est une modalité biométrique très bien perçue par la population.

Nous proposons dans cette thèse différentes contributions permettant d'évaluer des systèmes biométriques embarqués. La première est une plateforme d'évaluation de systèmes biométriques nommé EVABIO. La seconde contribution, permet d'évaluer l'incidence sur les performances lors de la réduction de templates biométriques lorsqu'ils doivent être stockés sur un SE. Nous proposons des méthodes permettant de réduire la taille du template biométrique tout en gardant un taux de reconnaissance élevé, garantissant ainsi un bon niveau de performance du système biométrique complet. La dernière contribution étudie les attaques d'un système biométrique embarqué sur SE. Nous regardons quels a priori sont importants pour un imposteur : nous avons montré que le type de l'empreinte digitale est un a priori important. Nous avons également proposé une contre-mesure pour les systèmes embarqués.

63/5000 Contributions to the evaluation of embedded biometric systems

Biometrics is sparking the interest of manufacturers and industrial compagnies because we are in need of new methods of authenticating indivduals : for physical access control, border control or for payments. Non-revocable and sensitive data is very often stored on embedded systems of the secure element type (SE), such as a smart card. SEs include a comparison module called On-Card-Comparison (OCC), which determines whether the template presented corresponds to the template stored within it. In this thesis, we are particularly interested in fingerprints because it is a biometric modality that is very well perceived by the population.

We propose in this thesis different contributions to evaluate embedded biometric systems. The first is a biometric evaluation platform called EVABIO. The second contribution evaluates the impact on performance when reducing biometric templates that are to be stored on an SE. We propose methods to reduce the size of biometric templates while maintaining a high recognition rate thus, guaranteeing a good level of performance of the global biometric system. The last contribution studies attacks on a biometric system that is embedded on a SE. We look at what a priori are important for an impostor : we have shown that the type of fingerprint is an important a priori and the reason why we have also proposed a countermeasure for embedded systems.

Indexation Rameau : MOTS CLÉS À VOIR AVEC LA BU
Indexation libre : mots clés perso

Spécialité Informatique et applications

Laboratoire GREYC - UMR CNRS 6072 - Université de Caen Basse-Normandie - Ensicaen
6 Boulevard du Maréchal Juin - 14050 CAEN CEDEX