REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE LARBI TEBESSI - TEBESSA
FACULTE DES SCIENCES EXACTES ET SCIENCES DE LA NATURE ET DE VIE
DEPARTEMENT DE MATHEMATIQUE ET INFORMATIQUE

MEMOIRE

DE FIN D'ETUDES POUR L'OBTENTION DU DIPLOME DE MASTER EN

INFORMATIQUE

SPECIALITE : SYSTEME D'INFORMATION

THEME

Protéger l'échange d'information via un système crypto-biométrique

Présenté par : Bendjenna Riadh

Devant le jury :

- Laouar Mohamed Ridha	**Professeur**	**Président**
- Betouil Ali Abdelatif	**MCA**	**Examinateur**
- Laimeche Lakhdar	**MCA**	**Encadreur**
- Abdallah Meraoumia	**MCA**	**Co-Encadreur**

Année Universitaire 2020/ 2021

Remerciement

Je tiens avant tout à remercier mes encadreurs, M. Laimeche lakhdar et M. Meraoumia Abdallah qui m'ont aider de commencer après une rupture de 20 ans des études. Je les remercie également pour leurs temps et son investissement dans tous les aspects de mon travail.

Je tiens également à remercier les membres du Jury :

M. Laouar Mohamed Redha et M. Betouil Ali Abdelatif.

Je remercie également les étudiants du Master 2 que j'ai eu le plaisir d'étudier avec et mes collègues au travail.

Je remercie toutes les personnes que j'ai pu rencontrer et avec lesquelles j'ai pu échanger.

Ces remerciements ne seraient pas complets sans remercier tous mes enseignants de l'année scolaire 2020/2021.

Merci a toute ma famille.

R. Bendjenna

Résumé : *Ce projet présente un cryptosystème biométrique basé sur un nouveau descripteur de texture nommé fonction d'images statistiques binaires orientées sécurité (S-BSIF) basée sur le descripteur de texture BSIF. Dans cette méthode d'extraction de caractéristiques, nous avons ajouté deux couches, une pour la transformation des gabarits et l'autre pour le cryptage des gabarits afin de fournir des caractéristiques biométriques profonde et révocables. D'autre part, notre méthode est basée sur un système chaotique pour produire les éléments de transformation en raison de son extrême sensibilité aux conditions initiales. Nous avons testé le cryptosystème biométrique proposé sur une base de données de 300 personnes, nous avons constaté une amélioration significative du taux d'identification (100%) avec notre méthode d'extraction de caractéristiques (S-BSIF). La méthode proposée a également montré un niveau de sécurité élevé (protection des templates) qui dépasse en réalité* 10^{180}.

Mots clés : *Sécurité, Biométries, Empreinte palmaire multi-spectral, BSIF, S-BSIF, cartes chaotiques.*

Abstract: *Biometrics,*

This project present a biometric cryptosystem based on a novel palmprint texture descriptor named, Security-oriented Binarized Statistical Image Features (S-BSIF) which based on BSIF texture descriptor. In this feature extraction method, we have added two layers, one for the transformation of the templates and the other for the encryption of the templates to obtain a deep and revocable template. In addition, our method is based on chaotic system to produce the transformation elements due to its extreme sensitivity to initial conditions. We tested the proposed system on a database of 300 people; we found a significant improvement in the identification rate (100%) with our feature extraction method (S-BSIF). The proposed method has also shown a high level of security (template protection) which actually exceeds 10^{180}.

Index term*: Security, Biometrics, Multispectral palmprint, BSIF, S-BISF, Chaotic Map*

ملخص يقدم هذا المشروع نظام تشفير بيومتري يعتمد على طريقة جديدة تسمى (S-BSIF). قمنا في هذه الطريقة (استخراج الميزات) بإضافة طبقتين : إحداهما لتحويل ميزات الصور البيومترية والأخرى لتشفيرها و هذا من اجل توفير ميزات بيومترية عميقة وقابلة للإلغاء. من ناحية أخرى ، تعتمد هذه الطريقة على نظام فوضوي لإنتاج عناصر التحويل نظرًا لحساسيتها الشديدة للقيم الأولية للمعطيات. اختبرنا نظام التشفير البيومتري المقترح على قاعدة بيانات تضم 300 شخص، ووجدنا تحسنًا كبيرًا في معدل تحديد الهوية (100٪) من خلال طريقة استخراج الميزات (S-BSIF). كما أظهرت الطريقة المقترحة أيضًا مستوى عالٍ من الأمان (حماية الميزات) والذي يتجاوز فعليًا 10^{180}

الكلمات المفتاحية : *الحماية, البيومتري, بصمة كف اليد متعددة الأطياف, S-BSIF, BSIF, الخرائط الفوضوية.*

Table des Matières

Liste des Figures

Liste des tableaux

Glossaire

Les termes suivants, classés dans l'ordre alphabétique, sont utilisés dans le texte.

EER **:** Taux d'erreurs égales - Equal Error Rate.

FAR **:** Taux de Fausses Acceptations - False Acceptance Rate.

FRR **:** Taux de Faux Rejets - False Reject Rate.

GAR **:** Taux d'acceptation des clients - Genuine Acceptance Rate.

RGB **:** Espace des couleurs RGB-R : rouge, G : vert et B : blue.

ROC **:** Courbe représentant les taux d'erreur - Receiver Operating.

ROI **:** Région d'intérêt - Region Of Interest.

Introduction

La reconnaissance biométrique est une technologie qui permette de vérifier l'identité des individus en fonction de leurs traits physiologiques (par exemple, empreinte digitale, visage) ou comportementaux (par exemple, signature). Au cours de l'authentification, les traits biométriques d'une personne sont comparés aux templates biométriques stockées de l'identité désirée dont l'accès est accordé s'il y a une correspondance suffisante. Les systèmes biométriques sont connus en tant qu'une alternative plus fiable qu'aux systèmes de sécurité basés sur des mots de passe, vu que les modalités biométriques ne peuvent pas être volées et difficile de les copier. La biométrie fournit également la non-répudiation (un utilisateur authentifié ne peut pas nier l'avoir fait) dans une certaine mesure en raison de la difficulté de copier ou de voler les données biométriques de quelqu'un.

L'une des tâches les plus importantes dans les systèmes biométriques est la protection fiable des templates biométriques. En utilisant une template biométrique mal protégée ou non protégée, un attaquant peut compromettre le système d'authentification biométrique, récupérer les données biométriques d'origine et extraire des informations privées.

Bien que de nombreuses méthodes aient été proposées pour la protection des modèles biométriques, selon les auteurs Soutar et al. [21], la plupart des techniques de protection des templates disponibles ne répondent pas à toutes les exigences souhaitées d'un système biométrique pratique comme la révocabilité, la sécurité, confidentialité et précision de correspondance élevée.

Cette conclusion est tout à fait vraie pour les systèmes de reconnaissance biométriques, qui sont les plus largement utilisés dans la pratique. Un cryptosystème biométrique est la technique la plus encourageante pour la protection des modèles biométriques [14]. Les cryptosystèmes biométriques offrent des solutions pour la protection de modèles ou la libération de clés cryptographiques en liant une clé à ou en générant une clé à partir d'un échantillon biométrique. Les performances des systèmes cryptographiques biométriques existants sont nettement inférieures à celles des systèmes biométriques ordinaires. Il existe un besoin nécessaire de développer des systèmes cryptographiques biométriques à hautes performances pour des applications pratiques. Les performances des cryptosystèmes biométriques existants sont fortement affectées par des facteurs tels que l'extraction de caractéristiques, la représentation des caractéristiques, la base de données biométrique et le nombre d'échantillons d'entraînement et de test [13].

Hormis les limites des cryptosystème biométrique, l'objectif principal de notre travail consiste non seulement à sécuriser les systèmes biométriques mais aussi à protéger ses données lors de leurs transmission à travers un réseau informatique, afin de réaliser une identification biométrique à distance. Alors que notre travail s'inscrit dans le cadre de l'intersection de deux axes de recherche à savoir : la cryptographie et la biométrie. Il présente une solution de compromis qui se révèle alors dans l'association entre ces deux systèmes, profitant des avantages des uns pour compenser les inconvénients des autres.

Dans ce projet de fin d'étude, nous avons proposée un cryptosystème biométrique pour protéger les templates biométriques basé sur une approche hybride qui combine à la fois la transformation et/ou le cryptage des templates. Dans cette approche, nous avons reconstruit la méthode d'extraction de caractéristiques BSIF pour pouvoir extraire un gabarit précis et révocable. Nous avons ajouté deux couches à cette méthode, une pour la transformation des gabarits et l'autre pour le cryptage des gabarits affin d'améliorer sa protection. Notre méthode repose aussi sur des systèmes chaotiques pour produire les éléments de transformation en raison de son extrême sensibilité aux conditions initiales. Ces systèmes sont récemment révélés très efficaces dans les systèmes de sécurité de l'information.

Nous allons essayer d'atteindre notre objectif à travers trois chapitres :

- Dans le premier chapitre, nous allons présenter des concepts généraux sur la biométrie à savoir les différentes modalités, l'architecture générale d'un système biométrique ainsi que ses différents modes de fonctionnement et leurs applications.

- Dans le deuxième chapitre, nous allons présenter les différentes menaces et vulnérabilités des systèmes biométriques. Puis, les approches de protections des systèmes biométriques à savoir les cryptosystèmes et qui sont basées sur les méthodes de transformations sont détaillées. Un état de l'art sur les différentes techniques de protection des systèmes biométriques est ensuite présenté.
- Dans le dernier chapitre, nous présentons la méthode proposée ainsi que les résultats expérimentaux. Dans une première étape, des prérequis théoriques à savoir les systèmes chaotiques et la méthode BSIF, sur lesquelles repose notre système proposé, sont détaillés. Ensuite, un nouveau système biométrique révocable est proposé. L'originalité de notre système réside dans la médication de la méthode d'extraction de caractéristique BSIF. Dans une deuxième étape, les résultats expérimentaux sont détaillés et discutés. Finalement, Nous clôturons ce mémoire par une conclusion générale, ainsi que les perspectives visées.

Chapitre 1

Sécurité d'information et biométrie

Résumé

La biométrie est aujourd'hui intégrée à de nombreux actes de la vie quotidienne nécessitant une authentification des personnes. Dans un contexte professionnel, il peut s'agir du contrôle d'accès à des locaux, à des ordinateurs, ou à des applications. La biométrie est souvent présentée dans ces cas comme une alternative plus ergonomique et plus fiable que le port de badges encombrants et que l'on peut oublier. Dans ce chapitre nous allons présenter les notions de base de la biométrie, les différentes techniques biométriques et leurs applications. Ensuite, nous allons présenter l'architecture générale d'un système biométrique et les différentes phases de son fonctionnement. Les limitations et l'évaluation des systèmes biométriques ainsi que la protection des systèmes biométriques sont aussi présentées.

Introduction

La biométrie est le moyen le plus approprié pour identifier et authentifier les individus de manière fiable et rapide grâce à des caractéristiques biologiques uniques. Dans ce chapitre nous allons présenter les notions de base de la biométrie, les différentes techniques biométriques et leurs applications. Ensuite, nous allons présenter l'architecture d'un système biométrique ainsi les différentes phases de son fonctionnement. La biométrique multimodal basée sur différents types de fusion appliquée à la biométrie, les différents niveaux de fusion ainsi la notion de normalisation des scores sera présentée. Finalement, quelques domaines d'application de la biométrie ainsi que ses limites sont présentées.

I.1 Nécessitée de la biométrie

La biométrie est un élément constitutif de la sécurité. La technologie rend les choses plus confortables, mais les progrès rapides s'accompagnent de nouveaux défauts et défis. Cela fait de la sécurité une préoccupation majeure. La protection des données contre l'usurpation d'identité, le vol de données ou encore de ressources informatiques est appelée cybersécurité. À mesure que la technologie progresse, ils tirent également parti des nouveaux outils et compétences et mettent en place des systèmes de sécurité, rendant les mots de passe inefficaces en tant que mécanisme de protection. Pour ces raisons, la sécurité biométrique gagne rapidement en popularité parmi les entreprises, les organisations et les particuliers comme moyen privilégié de protéger le cyberespace contre les pirates et autres individus malveillants.

I.2 Définition de la biométrie

La biométrie recense nos caractères physiques et comportementaux (voir figure I.1) les plus uniques, qui peuvent être captés par des instruments et interprétés par des ordinateurs de façon à être utilisés comme des représentants de nos personnes physiques dans le monde numérique. Ainsi, nous pouvons associer à notre identité des données numériques permanentes, régulières et dénuées de toute ambiguïté, et récupérer ces données rapidement et automatiquement à l'aide d'un ordinateur." [1].

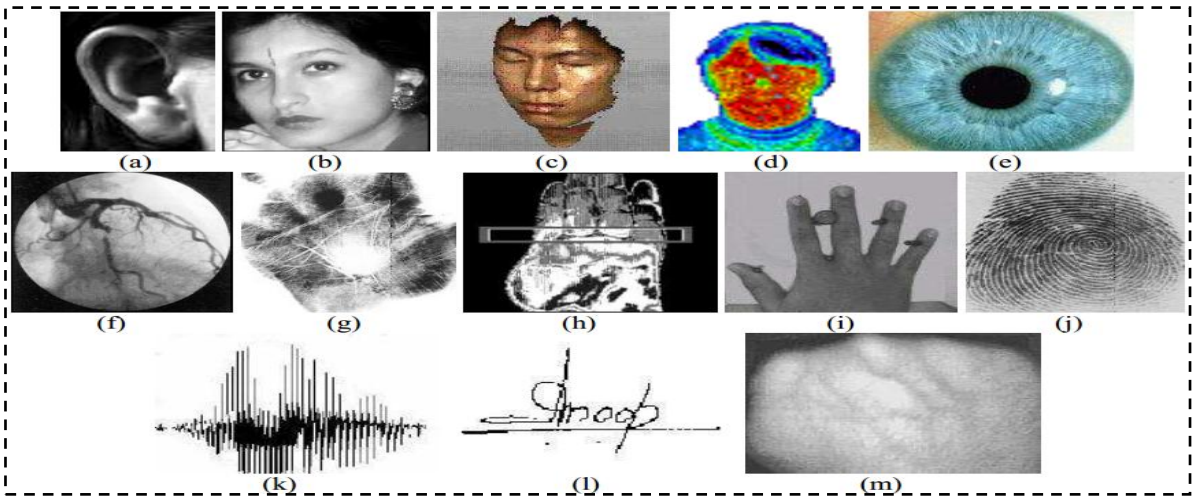


Fig. I.1 : Exemple des traits biométriques utilisé pour l'identification [2].

I.3 Types de modalités

Il existe différents types de modalités biométriques qui peuvent être classées en trois grandes catégories (voir figure I.2).

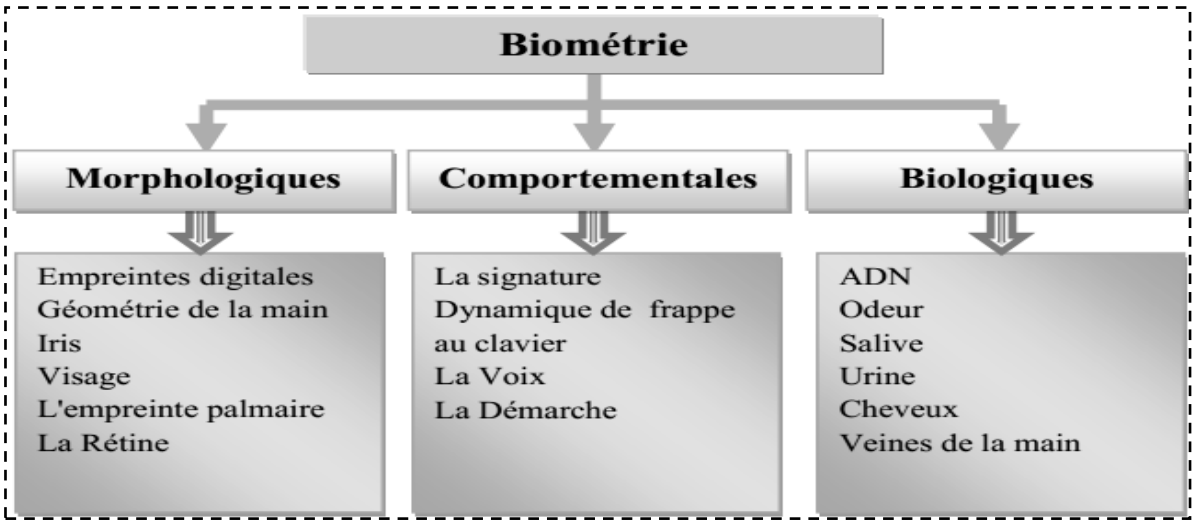


Fig.I.2. : Classification d'un certain nombre de modalités biométriques [3]

I.3.1 Modalités morphologiques (physiologiques): Les modalités biométrique de cette catégorie sont les plus utilisées. Elles sont basées sur les traits physiques qui sont uniques et permanents. Cette catégorie regroupe l'empreinte digitale, l'empreinte palmaire, la géométrie de la main, l'iris, le visage, le réseau veineux de la rétine, la géométrie de l'oreille, etc.

I.3.2 Modalités comportementale: Les modalités biométriques comportementales sont basées sur l'analyse de certains comportements d'une personne. Cette catégorie regroupe la reconnaissance vocale, la dynamique de frappe au clavier, la signature manuscrite, l'analyse de la démarche, …etc. Elle reste encore assez peu utilisée mais dont l'usage à tendance à se développer.

I.3.3 Modalités biologiques: La dernière catégorie consiste à l'étude des traces biologiques. Elle regroupe des caractéristiques telles que les veines de la main, le DNA, la thermographie faciale, l'odeur, le sang, et la salive, … etc.

I.3.4 Autres modalités biométrique: Il existe d'autre techniques biologiques qui sont qualifiées d'être biométriques mais elles ne sont pas pratiquement utilisées telles que l'odeur et la salive.

I.4 Comparaison entre les différentes modalités biométriques

La comparaison entre les différentes modalités biométriques permet de choisir une modalité en fonction des contraintes liées à l'application. En effet, chaque caractéristique (ou modalité) biométrique a ses forces et ses faiblesses, et faire correspondre un système biométrique spécifique à une application dépend du mode opérationnel de l'application et des caractéristiques biométriques choisies. En France le Club de la Sécurité des Systèmes d'Information Français [4] a proposé une comparaison (avantages / inconvénients) des principales modalités biométriques en se basant sur la facilité ou l'ergonomie d'utilisation, la vulnérabilité aux attaques, aux contournements, la fiabilité relative à la précision et à l'efficacité de la reconnaissance (voir tableau I.1).

Tableau I.1 : Avantages et inconvénients des modalités biométriques [4].

Modalité	Avantages	Inconvénients
Empreintes digitales	Coût, ergonomie moyenne, facilité de mise en place, taille du capteur	Fiabilité des appareils de mesure, acceptabilité, moyenne, possibilité d'attaques (rémanence de l'empreinte,...)
Forme de la main	Très ergonomique, bonne acceptabilité	Système encombrant, coût, perturbation possible par des blessures et l'authentification des membres d'une même famille, permanence des données
Visage 2D	Coût, peu encombrant, bonne acceptabilité	Jumeaux, psychologie, déguisement, vulnérabilité aux attaques
Rétine	Fiabilité, pérennité	Coût, acceptabilité faible, installation difficile
Iris	Fiabilité	Acceptabilité très faible, contrainte d'éclairage
Voix	Fiabilité	Vulnérable aux attaques
Signature	Ergonomie	Dépendant de l'état émotionnel de la personne, fiabilité
Frappe au clavier	Ergonomie	Dépendant de l'état physique de la personne

Aucune modalité biométrique n'est optimale. La correspondance entre une modalité biométrique et une application dépend du mode opérationnel de l'application et des propriétés de la modalité biométrique (voir tableau I.2).

Tableau I.2 : Etude comparative entre les modalités biométriques [5]

Modalités biométriques	Universalité	Distinctif	Permanence	Mesurabilité	Acceptabilité
Empreinte digitale	Moyenne	Haute	Haute	Moyenne	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Haute
Iris	Haute	Haute	Haute	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Faible
ADN	Haute	Haute	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Haute
Démarche	Moyenne	Faible	Faible	Haute	Haute
Frappe clavier	Faible	Faible	Faible	Moyenne	Moyenne
Géométrie de la main	Moyenne	Moyenne	Moyenne	Haute	Haute
Veines main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne

I.5 Système biométrique

Les systèmes biométriques s'appuient sur plusieurs processus distincts : enregistrement, capture directe, extraction de modèle et comparaison de modèle (voir figure I.3).

- L'objectif de l'enregistrement consiste à collecter des échantillons biométriques, et à générer des modèles numériques pour des comparaisons ultérieures. Nous pouvons distinguer la "capture directe" de l'enregistrement en la définissant comme le processus visant à collecter des échantillons biométriques en direct lors d'une tentative d'accès ou d'identification, puis à les comparer à une "galerie" de modèles précédemment enregistrés.
- L'extraction de modèle nécessite un traitement du signal des échantillons biométriques bruts (ex : images ou échantillons audio) afin d'obtenir un modèle numérique. Les modèles sont habituellement générés et stockés lors de l'enregistrement pour gagner du temps lors du traitement des comparaisons ultérieures. La comparaison de deux échantillons biométriques applique des calculs algorithmiques destinés à évaluer leur similarité.
- Lors de la comparaison, un score de correspondance est attribué. S'il est supérieur à un seuil donné, les modèles sont considérés comme identiques. En règle générale, les algorithmes d'extraction de modèle biométrique et de comparaison sont propriétaires (différents et secrets), aussi ne peuvent-ils pas être utilisés au sein d'un même système avec ceux d'autres fournisseurs (ex : pour comparer des modèles générés par différents produits, ou pour utiliser un algorithme de recherche de correspondance d'une société afin de comparer des modèles générés par les algorithmes d'une autre société).

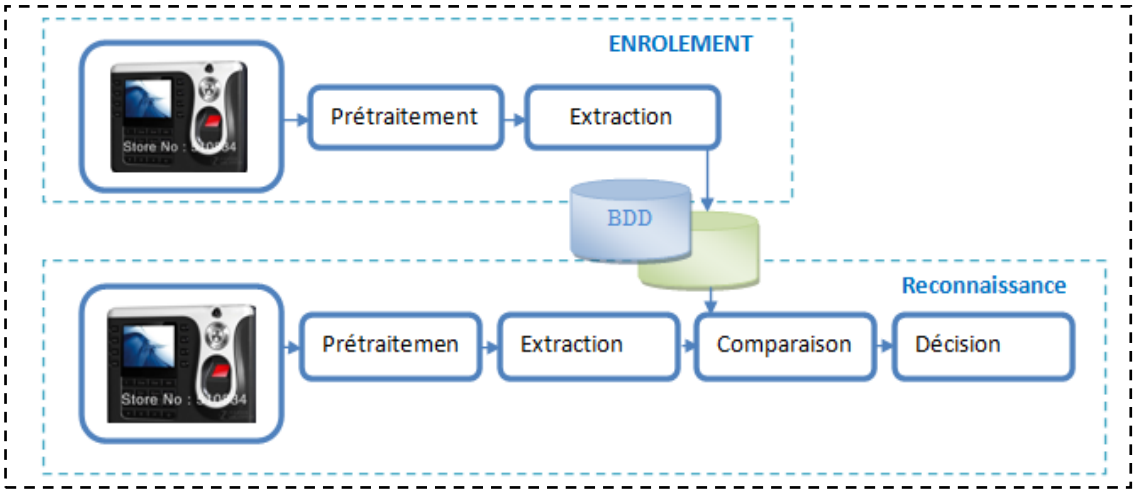


Fig. I.3 : Système de reconnaissance biométrique

I.5.1 Modes de fonctionnement d'un système biométrique

I.5.1.1 Phase d'enrôlement: C'est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. Plusieurs campagnes d'acquisitions de données peuvent être réalisées afin d'assurer une certaine robustesse au système de reconnaissance aux variations temporelles des données. Dans cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numérique (signatures), et enfin stockées dans la base de données [6].

I.5.1.2 Phase de reconnaissance: C'est la phase de vérification ou d'identification d'identité de la personne qui veut accéder au système, elle est primordiale dans le fonctionnement de la biométrie, Au cours de cette phase le système effectue une saisie de la donnée biométrique puis un ensemble de paramètres sera extrait comme dans la phase de l'enrôlement. Le capteur utilisé dans la phase de reconnaissance doit être aussi proche de celui utilisé dans la phase d'enrôlement.

Selon le fonctionnement du système, il existe deux modes de reconnaissance:

- **Mode de vérification :** c'est la comparaison 1-à-1, entre les données biométriques capturées (modèle de test) et les données stockées dans sa propre base (modèle d'apprentissage). Dans un tel système, un individu qui désire être identifié réclame une identité, habituellement par l'intermédiaire d'un PIN (numéro d'identification personnelle), d'un nom d'utilisateur, d'une carte d'identité, etc. Le système doit alors répondre à la question suivante "*Suis-je réellement la personne que suis-je entrain de proclamer ?*" [6].
- **Mode d'identification :** nommée aussi mode d'authentification, le système identifie un individu en cherchant les signatures (Template) de tous les utilisateurs dans la base de données. Par conséquent, le système conduit plusieurs comparaisons 1-à-N pour établir l'identité d'un individu [7]. En résumé, un système biométrique opérant en mode identification répond à la question "*Suis-je bien connu du système ?*".

I.5.2 Système en ligne et système hors ligne

Les systèmes de reconnaissances biométriques sont classifiés en deux catégories :

- **Système hors ligne** : un système biométrique hors ligne traite les images capturées précédemment. Par exemple, des images obtenues a partir des doigts des mains encrées digitalisées par un scanner numérique. Ces approches peuvent fournir des images à

haute résolution et conviennent aux méthodes qui exigent des images de résolution fine pour extraire des lignes, des points caractéristiques et des minuties. Cependant, ces méthodes ne sont pas appropriées aux systèmes de sécurité en ligne car deux étapes sont nécessaires : encrer les doigts pour obtenir les images de modalité sur des papiers et puis les scanner pour obtenir des images numériques.

- **Système en ligne** : dans ce système, un dispositif de capture spécifique pour chaque modalité (ex : appareil photo numérique) pour capturer des images de la modalité, est utilisé. Les images numériques acquises sont traités en temps réel. Par exemple, la signature en ligne est numérisé directement par un dispositif qui permet d'échantillonnés d'une signature en ligne nécessite un capteur spécifique. Une tablette à digitaliser ou un écran tactile suffisant pour cette tâche.

I.6 Biométrie multimodale

Le système biométrique multimodal consiste à combiner plusieurs modalités biométriques différentes ainsi que la consolidation d'informations présentées par les différentes modalités peut permettre une authentification précise de l'identité e améliorer les performances de reconnaissance afin de diminuer les tentatives de fraudes. Lors de l'augmentation de la quantité d'informations discriminantes de chaque personne, on souhaite augmenter le pouvoir de reconnaissance du système (vérification ou identification), et diminuer le taux d'erreur.

I.6.1 Scénarios de combinaisons

Les systèmes biométriques multimodaux améliorent les performances des systèmes biométriques monomodaux en combinant plusieurs systèmes. On peut différencier 5 types de systèmes multimodaux selon les systèmes qu'ils combinent (voir figure I.4):

- **multi-capteurs :** lorsqu'ils associent plusieurs capteurs pour acquérir la même modalité, par exemple un capteur optique et un capteur capacitif pour l'acquisition de l'empreinte digitale.
- **multi-instances :** lorsqu'ils associent plusieurs instances de la même biométrie, par exemple l'acquisition de plusieurs images de visage avec des changements de pose, d'expression ou d'illumination.
- **multi-algorithmes :** lorsque plusieurs algorithmes traitent la même image acquise, cette multiplicité des algorithmes peut intervenir dans le module d'extraction en considérant

plusieurs ensembles de caractéristiques et/ou dans le module de comparaison en utilisant plusieurs algorithmes de comparaison.

- **multi-échantillons :** lorsqu'ils associent plusieurs échantillons différents de la même modalité, par exemple deux empreintes digitales de doigts différents ou les deux iris. Dans ce cas les données sont traitées par le même algorithme mais nécessitent des références différentes à l'enregistrement contrairement aux systèmes multi-instances qui ne nécessitent qu'une seule référence.
- **multi-biométries :** lorsque l'on considère plusieurs biométries différentes, par exemple visage et empreinte digitale. Un système multimodal peut bien sûr combiner ces différents types d'associations, par exemple l'utilisation du visage et de l'empreinte mais en utilisant plusieurs doigts.

Tous ces types de systèmes peuvent pallier à des problèmes différents et ont chacun leurs avantages et inconvénients. Les quatre premiers systèmes combinent des informations issues d'une seule et même modalité ce qui ne permet pas de traiter le problème de la non-universalité de certaines biométries ainsi que la résistance aux fraudes, contrairement aux systèmes "multi-biométries". En effet, les systèmes combinant plusieurs informations issues de la même biométrie permettent d'améliorer les performances en reconnaissance en réduisant l'effet de la variabilité intra-classe. Mais ils ne permettent pas de traiter efficacement tous les problèmes des systèmes monomodaux. C'est pour cette raison que les systèmes multi-biométries ont reçu beaucoup d'attention de la part des chercheurs.

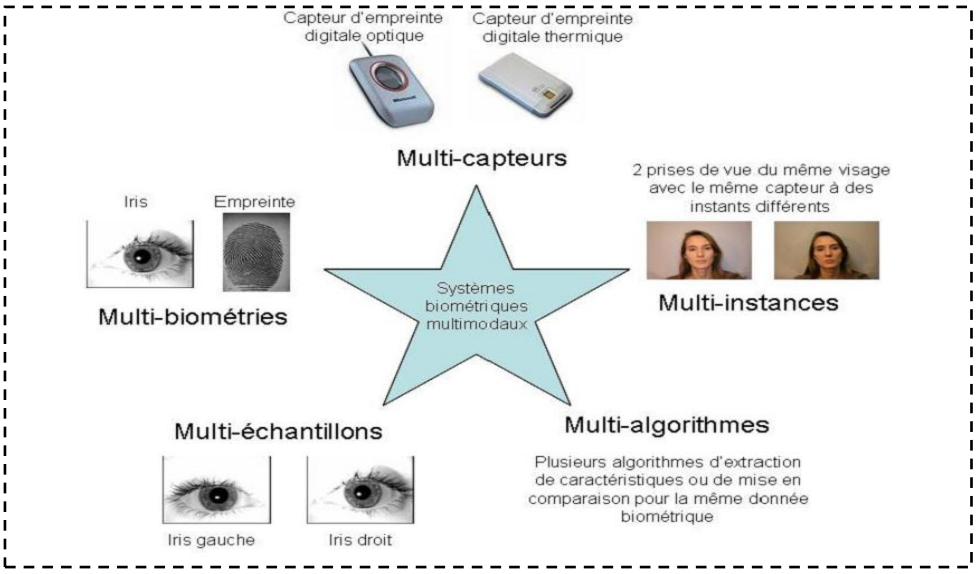


Fig. I.4 : Différents systèmes multimodaux

I.6.2 Technologies de fusion

La fusion dans un système biométrique multimodal peut se faire à quatre niveaux différents : au niveau des capteurs, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau du module de décision (voir figure I.5). Ces derniers peuvent être classés en deux sous ensembles : La fusion pré-classification (avant la comparaison) et la fusion post-classification (après la comparaison).

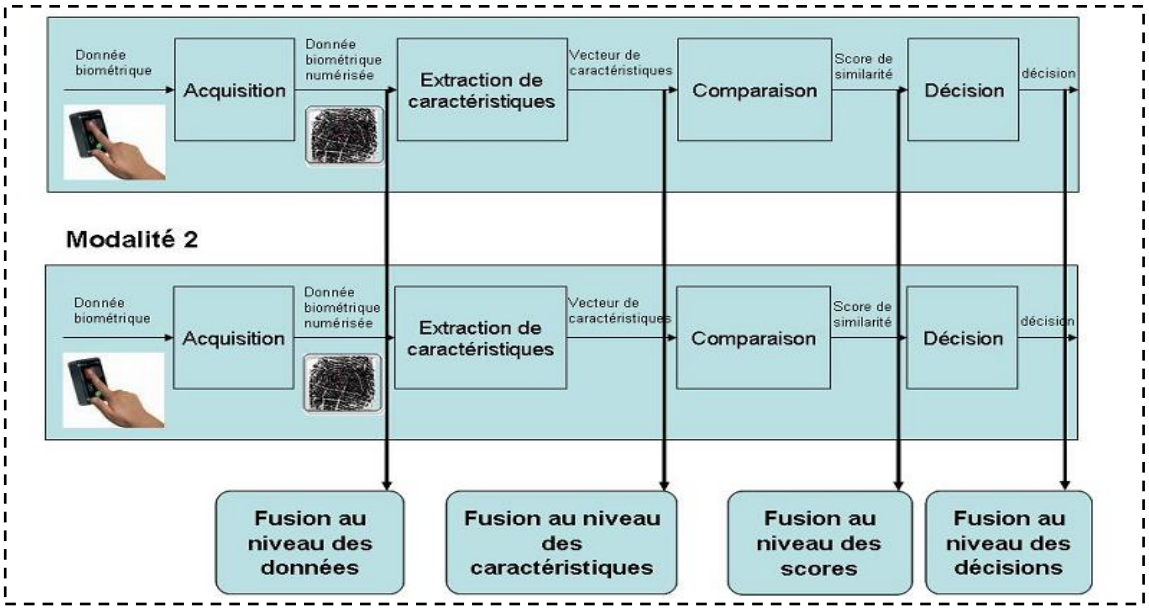


Fig. I.5. Différents niveaux de fusion.

- **La fusion au niveau du capteur:** Appelé aussi fusion niveau données, correspond généralement à algorithmes multi-capteurs ou multi-échantillons, où les données sont combinées immédiatement après son acquisition. Autrement dit, la fusion de données est effectuée avant l'extraction des caractéristiques, directement sur les données brutes. Dans le cas d'un module de reconnaissance faciale, cela correspond à une combinaison au niveau des pixels d'images de visage capturées à partir d'un appareil photo. Par exemple, plusieurs visages peuvent être capturés avec des variations de pose.
- **La fusion au niveau des caractéristiques**: Appelé niveau intermédiaire, la combinaison des caractéristiques extraites après la phase de prétraitement des données acquises qui sont obtenus à partir de : plusieurs capteurs du même descripteur biométrique, plusieurs algorithmes du même descripteur biométrique, ou encore plusieurs descripteurs biométriques. Lorsque les vecteurs de caractéristiques sont homogènes (de même taille), un unique vecteur de caractéristiques résultant (a la même

taille que les deux vecteurs individuels) peut être calculé comme une somme pondérée des vecteurs de caractéristiques individuels. Le vecteur résultant. Néanmoins, quand les vecteurs de caractéristiques sont hétérogènes (de différentes tailles), le vecteur résultant se constitue de la concaténation des vecteurs de caractéristiques individuels.

- **La fusion au niveau du score:** La combinaison des scores individuels après la comparaison. C'est le type de fusion le plus utilisé à cause de sa simplicité et son efficacité. En effet, une opération de normalisation des scores est nécessaire si ces derniers ne sont pas homogènes (mesure de distance et mesure de proximité) ou n'inclus pas dans le même intervalle. La normalisation des scores consiste à changer la valeur du score issu de chaque sous-système individuel, de manière à ce que les scores de différents sous-systèmes soient transformés dans un domaine commun afin d'éviter les influences des facteurs d'échelle quand les données varient dans des intervalles différents.
- **La fusion au niveau de décision:** Appelé haut niveau, elle consiste à combiner les décisions obtenues à partir de chaque sous-système. La fusion au niveau des décisions est souvent utilisée pour sa simplicité. En effet, chaque système fournit une décision binaire sous la forme OUI ou NON que l'on peut représenter par 0 et 1, et le système de fusion de décisions consiste à prendre une décision finale en fonction de cette série de 0 et de 1. Les méthodes les plus utilisées sont des méthodes à base de votes telles que OU (si un système a décidé 1 alors OUI), le ET (si tous les systèmes ont décidé 1 alors OUI) ou le vote à la majorité (si la majorité des systèmes ont décidé 1 alors OUI), On peut également utiliser des méthodes plus complexes qui pondèrent les décisions de chaque sous-système. Ces méthodes de fusion au niveau des décisions sont très simples mais utilisent très peu d'information (0 ou 1).

1.7. Domaine d'applications

La biométrie s'est rapidement distinguée comme la technologie la plus pertinente qui répond à une exigence de sécurité où il est nécessaire de connaître l'identité des personnes. De ce fait, de nombreuses applications font appel à la biométrie. Ces applications sont de quatre grands types :

- **Contrôle d'accès:** Le contrôle d'accès peut être lui-même subdivisé en deux sous catégories : le contrôle d'accès physique et le contrôle d'accès logique. On parle de contrôle d'accès physique lorsqu'une personne cherche à accéder à un lieu sécurisé (salle, bâtiment, …etc.). On parle de contrôle d'accès logique dans le cas où une personne cherche à accéder à un terminal, un réseau informatique, un service, ou une information (ordinateur, réseau privé, site web, base de données …etc.). Longtemps, l'accès à des lieux sécurisés s'est fait à l'aide de clés ou badges. Une garde était chargé de la vérification des badges qui sont munis d'une photo. Cependant, grâce à la biométrie, la même opération peut être effectuée automatiquement de nos jours. Traditionnellement, l'accès logique est sécurisé par des systèmes basés sur une connaissance (mot de passe). Néanmoins, les applications biométriques devraient connaître une popularité croissante à cause de leur fiabilité et la diminution des prix des appareils d'acquisition.

- **Transactions commerciales et bancaires :**L'authentification des transactions englobe le retrait d'argent au guichet des banques, les paiements par cartes bancaires et les paiements effectués à distance sur internet, . . . etc.

- **Identification judiciaire :** Dès le début du $20^{ème}$ siècle, la biométrie est acceptée comme moyen d'identification formelle d'une personne. L'utilisation de la biométrie s'est rapidement répandue. Elle est utilisée pour la première fois dans le domaine judiciaire. Les modalités biométriques utilisées sont l'empreinte digitale et l'empreinte génétique. Les empreintes digitales sont utilisées depuis longtemps pour prouver certains faits relatifs à des infractions criminelles, dont la présence de l'accusé en un lieu, le fait qu'il ait touché un objet ou une personne,...etc. L'ADN est extrait des cellules de criminel qui sont trouvées sur le lieu du crime. Ces cellules peuvent être des taches de sang, des cellules buccales déposées par de la salive, des cheveux ou encore des cellules coincé sous les ongles de la victime. Il est possible de disculper ou de confondre un suspect avec une très grande sûreté, en identifiant certaines séquences d'ADN propres à un individu et en les comparants à celles présentes dans l'ADN trouvées dans le lieu d'un crime par son auteur. Encore que la recherche criminelle, la vérification des signatures est utilisée dans les contrats afin d'éliminer de les falsifier.

De plus, la biométrie est utilisée dans d'autres applications juridiques telles que l'identification de cadavre, l'identification de terroriste, l'identification des enfants disparus, etc.

- **Service public :** La biométrie est utilisée dans une certaines applications d'ordre gouvernemental telles que le contrôle des frontières et le contrôle des passeports et visas. Ainsi, elle est introduite dans plusieurs cartes à savoir les cartes d'assurance sociale, les cartes d'identité nationale et les permis de conduire, ce qui facilite la vérification de l'identité de leur propriétaire.

I.8 Limitations des systèmes biométriques

Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut garantir actuellement un excellent taux de reconnaissance avec des systèmes biométriques unimodaux, basés sur une unique signature biométrique. De plus, ces systèmes sont souvent affectés par les problèmes suivants [8] :

- **Bruit introduit par le capteur :** du bruit peut être présent dans les données biométriques acquises, ceci étant principalement dû à un capteur défaillant ou mal entretenu.
- **Non-universalité :** Cependant, toutes les modalités biométriques ne sont pas vraiment universelles. Le *National Institute of Standards and Technologies* (NIST) a rapporté qu'il n'était pas possible d'obtenir une bonne qualité d'empreinte digitale pour environ 2% de la population (personnes avec des handicaps liés à la main, individus effectuant de nombreux travaux manuels répétés, etc.). La non-universalité entraîne des erreurs d'enrôlement dans un système biométrique,
- **Manque d'individualité :** Par exemple, une certaine partie de la population peut avoir une apparence faciale pratiquement identique due à des facteurs génétiques (père et fils, vrais jumeaux, etc.). Ce manque d'unicité augmente le taux de fausse acceptation,
- **Sensibilité aux attaques :** bien qu'il semble très difficile de voler les modalités biométriques d'une personne, il est toujours possible de contourner un système biométrique en utilisant des modalités biométriques usurpées. Les études dans [18, 19] ont montrés qu'il était possible de fabriquer de fausses empreintes digitales en gomme et de les utiliser pour contrer un système biométrique.

1.9 Conclusion

De nos jours la protection des droits d'auteur est réaliser à l'aide des données biométriques car elle est le moyen de sécurité le plus utilisé grâce à la variabilité des données biométriques est ses avantages. Dans ce chapitre, nous avons, dans une première étape, présenté les différentes modalités biométriques, leurs caractéristiques et une comparaison entre elles. Ensuite, nous avons présenté les systèmes biométriques unimodaux et multimodaux avec les divers types de combinaisons des modalités possibles, les architectures et les niveaux de fusion qui peuvent être utilisés. Finalement, nous avons terminé ce chapitre par la présentation de quelques techniques de tatouage numérique basées sur les données biométrique pour la protection des droits d'auteur.

Chapitre 2

Systèmes biométrique: menaces et sécurité

Résumé

Récemment, des discussions sur la sécurité des systèmes biométriques ont émergé. Le stockage des données de référence pose de sérieux problèmes de sécurité et d'invasion de vie privée : manipulation d'informations sensibles, reconstruction de la biométrie d'origine à partir du modèle stocké, construction d'un échantillon biométrique falsifié, utilisation secondaire des informations biométriques (surveillance, discrimination, etc.) ou l'impossibilité de révoquer l'identifiant biométrique lorsqu'un vol d'identité à eu lieu. Dans ce chapitre, nous présentons les vulnérabilités et menaces ainsi que les schémas de protection des gabarits biométriques (cryptosystèmes biométriques et transformations révocables). L'objectif principal de ces schémas de protection se base sur la fusion des deux vastes domaines a savoir la cryptographie et les fonctions de transformations affin de garantir un niveau acceptable de sécurité. Les travaux connexes son ensuite présentés.

Introduction

Les systèmes biométriques ont un potentiel puissant pour assurer la sécurité d'une variété d'applications, les systèmes sont aujourd'hui introduits dans de nombreuses applications et ont déjà été déployés pour protéger les ordinateurs personnels, les guichets automatiques, les cartes de crédit, les transactions électroniques, les aéroports, les institutions de haute sécurité comme les installations nucléaires, l'armée Bases et autres applications telles que le contrôle des frontières, le contrôle d'accès, la protection des données sensibles et les systèmes de suivi en ligne. Alors que la biométrie peut améliorer la sécurité dans des environnements différents et servir à de nombreuses fins, les systèmes biométriques, comme tout autre système de sécurité, présentent des vulnérabilités et sont sensibles aux menaces. Ils sont sensibles aux vulnérabilités externes des systèmes biométriques afin que leurs faiblesses puissent être trouvées et que des contre-mesures utiles contre les attaques prévisibles puissent être développées. L'utilisation de plus en plus répandue de la biométrie à des fins de sécurité a suscité un nouvel intérêt pour la recherche et l'exploration de méthodes d'attaque des systèmes biométriques.

Dans ce chapitre, nous présentons les vulnérabilités et menaces ainsi que les schémas de protection des gabarits biométriques (crypto systèmes biométriques et transformations révocables). L'objectif principal de ces schémas de protection se base sur la fusion des deux vastes domaines à savoir la cryptographie et les fonctions de transformations afin de garantir un niveau acceptable de sécurité. Les travaux connexes son ensuite présentées.

II.1 Vulnérabilités et menaces d'un système biométrique

Un système biométrique est soumis à de nombreuses attaques malveillantes qui peuvent être effectuées par diverses formes de menaces. Les attaques malveillantes sur une système biométrique sont un problème de sécurité et dégradent les performances du système. Le système biométrique a diverses limitations telles que les attaques par usurpation, les données bruitées, les variations interclasses et la similitude interclasse, etc.

C'est la raison pour la quelle tout système biométrique doit être analysé, et des contre-mesures doivent être prises lors de la conception du système biométrique. Les différentes attaques dans les systèmes biométriques sont les suivantes :

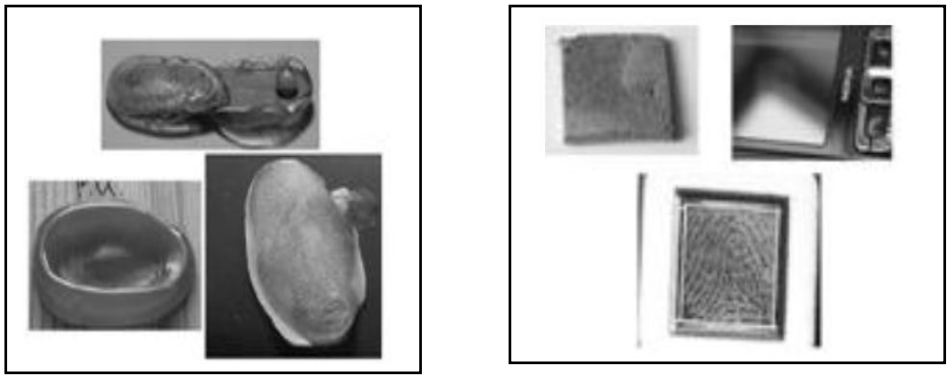
II.1.1 Faux biométrie

C'est le point de vulnérabilité qui a la plus grande importance lorsque les systèmes biométriques sont discutés, est l'usurpation ou la fourniture d'une fausse biométrie physique conçue pour contourner le système biométrique. Cette attaque peut être menée relativement facilement car peu ou pas de connaissances techniques du système sont nécessaires. Les matériaux pour la création de fausses données biométriques sont généralement existants et faciles à obtenir. Un autre facteur est que ces attaques sont menées au point d'entrée du système, de sorte que de nombreux mécanismes de protection numérique, tels que le cryptage et l'utilisation de signatures numériques, ne sont pas efficaces. De nombreuses données biométriques (y compris les empreintes digitales, la main et l'iris) sont soumises à cette forme d'attaque. La biométrie originale peut être obtenue relativement facilement à partir de nombreuses sources, avec ou sans la permission et la coopération du propriétaire de cette biométrie. Nous laissons des traces biométriques étendues, telles que des empreintes digitales et des empreintes de mains, sur les bureaux, les portes, les ustensiles et de nombreuses autres surfaces. Les faux masques faciaux, les fausses empreintes digitales en silicone, la lentille sur un iris, etc. sont quelques-unes de ces attaques malveillantes contre le capteur.

II.1.2 Attaque par rejoue

Un attaquant peut présenter une photographie ou lire une vidéo du visage, par exemple, d'un vrai client au capteur, ou à la caméra électronique, du système d'authentification. Ce point est le plus vulnérable dans le système d'authentification car dans un système entièrement automatisé, la possibilité de présenter une photographie est toujours accessible à un attaquant sauf si l'espace physique devant la caméra est supervisé par un observateur humain ou par une seconde modalité biométrique en plus de la caméra d'image faciale. Si un attaquant peut

accéder à l'intérieur de la caméra ou à la connexion entre la caméra et l'arrière du système, l'attaquant n'a pas besoin de montrer» une photographie ou une vidéo physique à l'appareil photo, mais peut injecter directement dans le système un signal électronique approprié qui correspond à l'image du visage du client.



(a) (b)

Fig. II.1. Attaque par rejoue : (a) Empreintes digitales en plastique (gélatine, silicone, moule en plastique), (b) Fausse empreinte digitale, une empreinte latente sur téléphone portable [8-9].

II.1.3 Transmission de données biométriques interceptées

Ici, l'attaquant rejoue une ancienne donnée biométrique stockée dans le système sans passer par le capteur biométrique. C'est le cas de la présentation d'une ancienne copie de l'image de l'empreinte digitale. Étant donné que l'attaquant contourne le capteur biométrique en fournissant au système une ancienne donnée enregistrée, les métadonnées n'auront aucun effet contre cette forme d'attaque.

II.1.4 Attaque sur le module d'extraction de caractéristiques

Ce module pourrait être remplacé par le virus cheval de Troie afin de produire des informations choisies par l'attaquant. L'utilisateur légitime ne se rend pas compte que ce module a été corrompu et a fourni des informations conformément aux instructions du pirate. Le module d'extraction de caractéristiques étant compromis par le hacker, les métadonnées ne seront pas efficaces contre ce genre d'attaque.

II.1.5 Altération des caractéristiques extraites

Une fois les données obtenues par le module d'extraction de caractéristiques, elles sont altérées voire remplacées par d'autres données définies par l'attaquant. Pour les attaques d'infrastructure non sécurisées, nous sommes dans des situations où le système biométrique est corrompu et ne fournira des réponses qu'en fonction de l'intention du pirate. Les métadonnées ne seront pas efficaces dans ces contextes.

II.1.6 Remplacement du module du correspondant par un module malveillant

Ce module pourrait être remplacé par un cheval de Troie pour produire artificiellement des scores élevés ou faibles.

II.1.7 Corruption de la base de données

La base de données des modèles biométriques est disponible localement, à distance ou distribuée sur plusieurs serveurs. Dans ce type d'attaque, l'attaquant modifie un ou plusieurs modèles pour permettre à un imposteur voire empêcher un utilisateur légitime d'y accéder.

II.2 Protection des systèmes biométriques

Tel que précisé par Jainet al dans [10] il existe principalement deux classes pour les méthodes de protection du modèle biométrique que sont : es cryptosystèmes biométriques et les approches par transformation.

II.2.1 Crypto systèmes biométriques

Pour résoudre les problèmes mentionnés ci-dessus, nous présentons dans cette section les cryptosystèmes biométrique. Fondamentalement, la combinaison de la cryptographie et de d'un système biométrique est connue sous le nom de cryptosystème biométrique. En utilisant cette technique, la cryptographie fournira un niveau de sécurité élevé et la biométrie aidera à éviter de se souvenir des mots de passe. De plus, les clés cryptographiques sont générées à partir des modèles biométriques de l'utilisateur. À moins que la même personne ne participe à nouveau, le système ne révélera pas les clés précédemment stockées pour la vérification [11]. Il existe deux types de cryptosystèmes biométriques, selon sur la façon dont les données auxiliaires sont dérivées : systèmes de liaison de clé et systèmes de génération de clés [12].

II.2.1.1 Crypto systèmes de liaison de clé

Dans ce schéma, des données auxiliaires sont obtenues en liant une clé cryptographique choisie à un modèle biométrique. À la suite du processus de liaison, une fusion de la clé secrète et du modèle biométrique est stockée en tant que données auxiliaires. En appliquant un algorithme de récupération de clé approprié, les clés sont obtenues à partir des données auxiliaires lors de l'authentification. Étant donné que les clés cryptographiques sont indépendantes des références biométriques, elles sont révocables, tandis qu'une mise à jour de la clé nécessite généralement un réenregistrement afin de générer de nouvelles données auxiliaires. Le mode de fonctionnement général d'un schéma de liaison de clé est illustré sur la figure II.2.

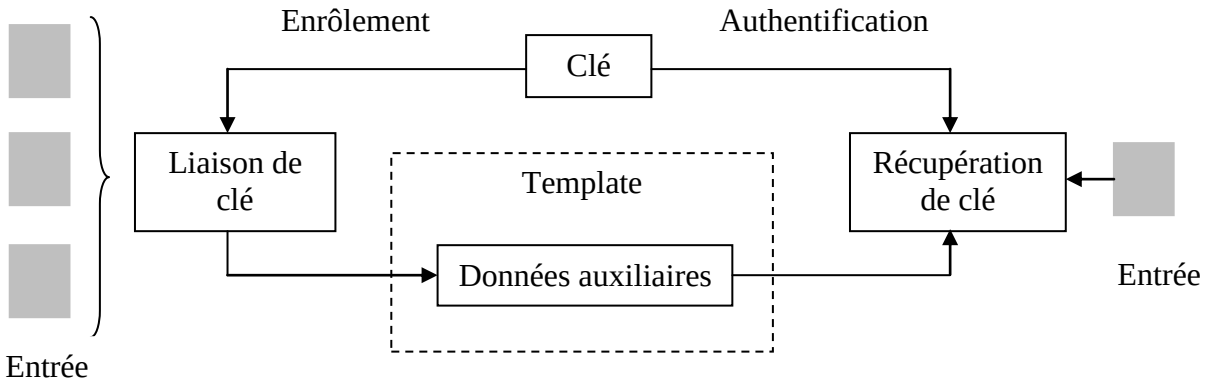


Fig. II.2. Mode de fonctionnement général d'un schéma de liaison de clé

II.2.1.2 Schémas de génération de clés

Les données auxiliaires sont dérivées uniquement du modèle biométrique. Les clés sont directement générées à partir des données auxiliaires et de modèle biométrique donné [13]. Bien que le stockage des données auxiliaires ne soit pas obligatoire, la majorité des schémas de génération de clés proposés stockent des données auxiliaires (si les schémas de génération de clés extraient des clés sans utiliser de données d'assistance, celles-ci ne peuvent pas être mises à jour en cas de compromission. Le mode de fonctionnement général d'un schéma de génération de clé est illustré sur la figure II.3.

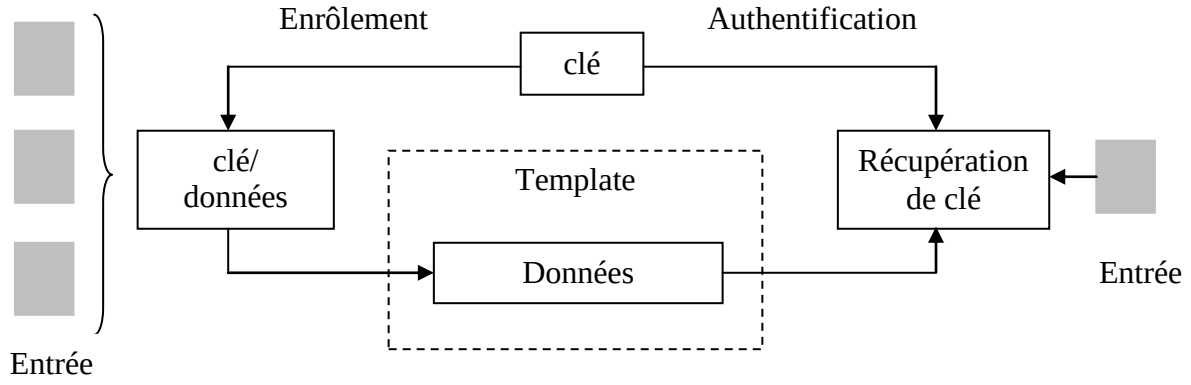


Fig. II.3. Mode de fonctionnement général d'un schéma de génération de clé

II.2.2 Transformations révocables

Les approches de cette famille n'utilisent pas de données auxiliaires pour compenser la variabilité du signal biométrique, ce qui signifie que la comparaison est effectuée dans le domaine de la transformation directement entre les modèles transformés. Supposons que **X** sera transformé en données codées **T** lors de l'enrôlement par l'utilisation d'une fonction **F**. Pour la vérification, la requête biométrique **Y** sera transformée en **T'** toujours en utilisant la

fonction **F** et l'authentification réussira si **T** est proche de **T'** en utilisant une certaine mesure de similarité. Pour assurer la révocabilité du système, une donnée aléatoire **S** sous forme d'une clé est attribuée à chaque utilisateur **U**. La clé **S** est alors considérée comme un paramètre d'entrée de la fonction de transformation **F.** La révocation consiste au remplacement direct de cette clé utilisateur. La figure II.4 résume le fonctionnement des transformations révocables.

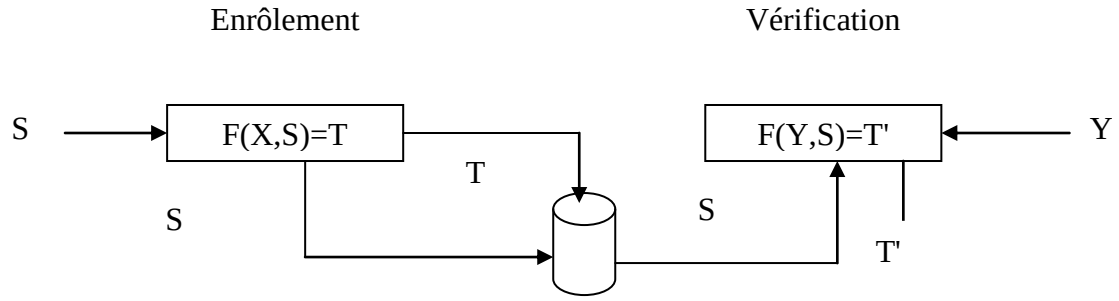


Fig. II.4. Fonctionnement générique des transformations révocable

II.2.3 Techniques hybrides

Dans les systèmes hybrides, les deux méthodes de protection; transformation des caractéristiques et les cryptosystèmes biométriques sont combinées pour construire un système robuste. Le but principal de faire cette combinaison de différentes approches est d'exploiter les avantages des deux techniques tout en évitant leurs des avantages. Feng et al. [14] ont proposé une approche hybride basée sur la reconnaissance faciale en utilisant premièrement une projection aléatoire puis la méthode des cryptosystèmes biométriques Fuzzy Commitment [15]. Autres techniques d'hybridation sont basées sur l'utilisation de mots de passe pour renforcer la sécurité des cryptosystèmes. Dans leur travail [16], Nandakumar et al ont utilisé un mot de passe pour transformer les caractéristiques des empreintes digitales en se basant sur la méthode des cryptosystèmes FuzzyVault [17]. Ari et al. [18] ont proposé une méthode hybride basée sur la génération de la clé secrète durant l'enrôlement a partir des données biométriques en appliquant le hachage discret.

II.2.4 Avantages des cryptosystèmes biométriques

Les cryptosystèmes biométriques offrent plusieurs avantages par rapport aux systèmes biométriques [19] conventionnels. Les principaux avantages peuvent être résumés comme suit:

- **Protection du gabarit** : dans les systèmes cryptographiques biométriques, le gabarit biométrique d'origine est masqué de sorte qu'une reconstruction est difficilement réalisable.
- **Libération de clé dépendante de la biométrie** : les cryptosystèmes biométriques fournissent des mécanismes de libération de clé basés sur la présentation de données biométriques.
- **Révocabilité des modèles biométriques** : plusieurs instances de modèles sécurisés peuvent être générées en liant ou en générant différentes clés.
- **Sécurité accrue** : les cryptosystèmes biométriques empêchent plusieurs types traditionnels d'attaques contre les systèmes biométriques (par exemple, les attaques de substitution).
- **Meilleure acceptation sociale** : en raison des avantages de sécurité mentionnés ci-dessus, l'acceptation sociale des applications biométriques devrait augmenter.

II.3 Travaux connexes

Il y a eu un certain nombre d'efforts de recherche visant à résoudre les problèmes liés aux cryptosystèmes biométriques. L'un des premiers cryptosystèmes biométriques implémentant la liaison de clé a été proposé par Soutar et al. [20]. Dans cette méthode, un algorithme de liaison de clé dans un système de correspondance d'empreintes digitales basé sur la corrélation optique est proposé. Cet algorithme lie une clé cryptographique aux images d'empreintes digitales de l'utilisateur au moment de l'inscription. La clé n'est ensuite récupérée qu'après une authentification réussie. L'algorithme crée d'abord une fonction de filtre de corrélation qui à la fois les composantes d'amplitude et de phase. Les critères de conception pour cette fonction incluent à la fois la tolérance à la distorsion et la discriminabilité. L'algorithme calcule également une sortie qui est obtenue par convolution/corrélation des images d'empreintes digitales d'apprentissage avec la fonction de filtre de corrélation. Ensuite, le conjugué complexe de la composante de phase de la fonction de filtre de corrélation est multiplié par un réseau de phase uniquement généré aléatoirement de la même taille. Alam et al. [21] a proposé un cryptosystème biométrique, qui intègre la transformée de Fourier discrète (DFT) et une technique révocable basée sur la projection aléatoire pour renforcer la sécurité. Dans le système proposé, les caractéristiques d'empreintes digitales basées sur une grille polaire sont transformées en utilisant la DFT et la projection aléatoire, créant un modèle non inversible. En outre, une stratégie de basculement de bits est utilisée pour injecter du bruit dans le modèle généré, afin de renforcer davantage la sécurité du modèle. Sarkar et Singh [22] ont proposé la génération de clés cryptographiques à partir de modèles d'empreintes digitales.

Différentes clés d'une longueur de 128 bits peuvent être générées en annulant et en rééditant différents modèles d'empreintes digitales. Cela réduit le risque potentiel que la même clé secrète qui existait avec le récepteur et l'expéditeur puisse être divulguée après négociation. Dans [23], Liu et Zhao ont utilisé la minimisation l1 pour protéger les modèles d'empreintes digitales et les stocker sous forme de texte chiffré. La correspondance d'empreintes digitales est effectuée dans le domaine crypté et l'authentification n'est réussie que lorsque l'empreinte digitale de la requête est suffisamment proche de l'empreinte digitale modèle. Comme le modèle est généré à partir du Minutia CylinderCode (MCC) [24] avec la conception appropriée de l'algorithme sécurisé, le système proposé atteint une sécurité et une précision de reconnaissance élevées. Xi et al. [25] ont proposés un extracteur flou utilisant une structure locale bicouche. Dans ce système, les extracteurs flous sont basés sur des codes correcteurs d'erreurs. Une clé cryptographique est codée avec un code de contrôle d'erreur, puis la séquence codée de bits s'intègre aux caractéristiques biométriques qui sont calculées à l'aide des données de l'échantillon d'apprentissage. Ce processus génère une chaîne ouverte. Alors que la personne authentifiée présente les données biométriques, les données sont calculées avec la chaîne ouverte en utilisant XOR. Le processus aboutit à une libération de clé avec des bits erronés corrigés. Li et al. [26] a proposé un schéma de voûte floue, qui combine deux structures locales, le descripteur de minutie et la structure locale de minutie. En utilisant trois approches de fusion, les deux structures locales invariantes par transformation sont intégrées dans le schéma proposé. Lifang Wu et.al [27] ont développé un cryptosystème biométrique basé sur la biométrie faciale. Pendant le cryptage, le vecteur de caractéristiques de l'analyse en composantes principales (ACP) à 128 dimensions est initialement obtenu à partir de l'image du visage. Par la suite, un vecteur binaire de 128 bits est obtenu par seuillage. Ensuite, l'auteur a sélectionné des bits distinguables pour générer une bio-clé. De plus, un code de correction d'erreur est produit à l'aide de l'algorithme de Reed-Solomon. Afin de fournir un décodage de correction d'erreur plus précis dans un schéma d'engagement flou basé sur l'iris, qui se rapproche d'une borne théorique obtenue par Bringer et al. [28], les auteurs appliquent un décodage mini-sum itératif bidimensionnel. Dans leur approche, une matrice est créée où les lignes ainsi que les colonnes sont formées par deux codes binaires différents de Reed-Muller.

Des approches hybrides qui utilisent à la fois des schémas de génération de clés et des concepts de liaison de clés ont également été proposées. Dans [29], les auteurs proposent une approche hybride qui tire parti à la fois de l'approche du cryptosystème biométrique et de l'approche basée sur la transformation. Un algorithme hybride en trois étapes est conçu et développé sur la base d'une projection aléatoire, d'une transformation préservant la

discriminabilité (DP) et d'un schéma d'engagement flou. La projection aléatoire est utilisée pour fournir l'annulation. La transformation DP est développée pour convertir des modèles annulables à valeur réelle en modèles binaires tandis que la discriminabilité est préservée, de sorte qu'elle puisse être facilement chiffrée dans le schéma d'engagement flou.

II.4 Conclusion

Dans ce chapitre, après avoir présenté les vulnérabilités et menaces des systèmes biométriques, nous avons pu voir deux grandes familles de solutions. Principalement, des solutions basées sur la cryptographie connues par les cryptosystèmes biométriques et des solutions basées sur les transformations révocables appelées systèmes biométriques révocables. Ensuite, qu'il s'agisse de cryptosystèmes biométriques ou de transformations révocables, les récents travaux connexes sont présentés.

Chapitre 3

Résultats Expérimentaux

Résumé

L'étape d'extraction de caractéristiques dans un système de reconnaissance de formes est l'une des étapes les plus importantes du système. D'un point de vue sécuritaire, cette étape doit fournir une nouvelle représentation à la fois unique pour distinguer différentes personnes et révocable en cas de piratage. Ce chapitre se concentre sur l'évaluation de la méthode d'extraction de caractéristiques proposée (S-BSIF) des deux aspects, la précision du système d'identification et la robustesse contre les tentatives de piratage. Tous les tests ont été réalisés à l'aide d'un système d'identification biométrique, en utilisant une base de données biométrique connue et disponible.

Introduction

Les systèmes de reconnaissance biométrique sont susceptibles de fournir un degré plus élevé de sécurité et de fiabilité, mais des préoccupations subsistent quant au risque que des templates biométriques soient volés et réutilisés illégalement. Dans ce chapitre, nous proposerons un système biométrique basé sur les réseaux veineux de la main, capable de générer des templates biométriques révocables en cas de falsification. La méthode proposée pour protéger ces templates biométriques est basée sur une approche hybride qui combine à la fois la transformation et/ou le cryptage des templates. Les performances du système biométrique proposé seront évaluées sous deux aspects: en précision et en sécurité à l'aide d'une base de données connue et disponible.

III.1 Système proposé

La Fig. III.1 montre l'architecture proposée pour un système d'identification biométrique basé sur l'empreinte du réseau veineux. Lors des phases d'enrôlement et d'identification, une étape de prétraitement est nécessaire pour localiser puis extraire la région d'intérêt (Region Of Interest : ROI). Ensuite, un vecteur de caractéristiques (Template) est extrait pour chaque ROI en utilisant une nouvelle méthode appelée fonction d'image statistique binarisée orientée sécurité (Security-oriented Binarized Statistical Image Features : S-BSIF) capable de fournir des templates révocables. Cette méthode utilise une clé secrète qui peut être changé en cas de piratage, de sorte que les templates produits par l'ancienne clé ne soient pas autorisés à accéder au système (utilisateur illégal). Pour la phase d'enrôlement, ce template est stocké

dans la base de données système (par stockage direct ou par apprentissage automatique), tandis qu'à l'étape d'identification, ce template fait l'objet d'une étape de mise en correspondance (comparaison) pour décider d'accepter ou de rejeter la personne en question dans l'étape de décision.

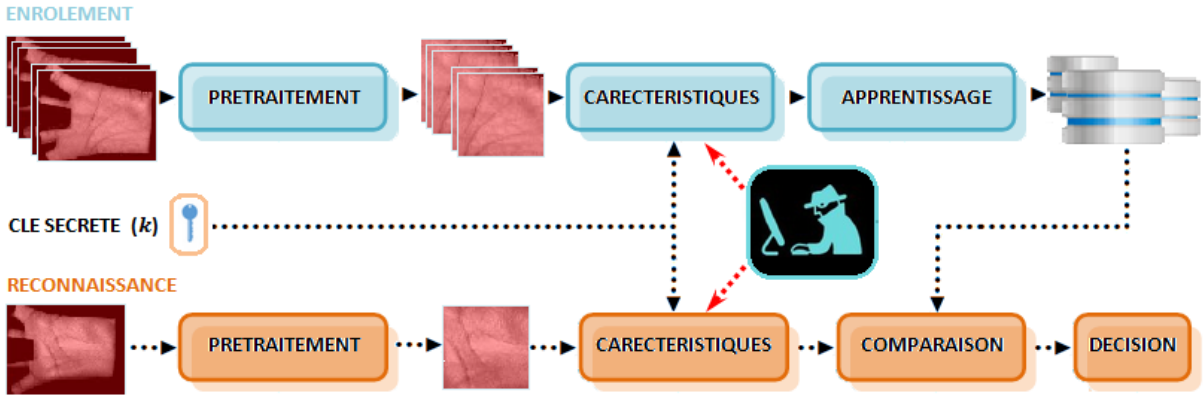


Fig. III.1. Système biométrique proposé basé sur l'empreinte du réseau veineux

III.2 BSIF orientée sécurité

Afin de bien représenter les caractéristiques biométriques de l'image, les données biométriques acquises par le module de capture sont généralement traitées par une fonction d'extraction de caractéristiques. Elle consiste en une représentation sous forme de vecteur que l'on cherche à être à la fois représentatif des données et discriminant par rapport aux autres données (d'autres personnes). Idéalement, cette nouvelle représentation est supposée unique pour chaque personne et relativement invariante aux variations intra-classes. Dans cette section, nous allons essayer d'améliorer la méthode BSIF afin d'avoir une représentation discriminante et efficace contre les tentatives d'attaque.

III.2.1 Fonction d'image statistique binarisée (BSIF): En 2012, Kannala et E. Rahtu [32] ont proposé une nouvelle méthode d'analyse de la texture d'une image capable de fournir des descripteurs ou des caractéristiques. Cette méthode est inspirée des méthodologies: motifs binaires locaux (Local Binary Pattern: LBP) et quantification de la phase locale (Local Phase Quantization : LPQ). Dans cette méthode, des patchs locaux de l'image sont projetés sur un sous-espace préalablement obtenu, puis le code binaire de chaque pixel est calculé par la binarisation de tous les résultats de projection. Pour obtenir le descripteur d'image, le code binaire de chaque pixel est d'abord converti en une valeur décimale, puis la valeur de pixel d'origine est remplacée par la valeur décimale calculée. Le descripteur d'image peut être utilisé pour obtenir le vecteur de caractéristiques de l'image analysée. Il est important de

mentionner que le sous-espace de la projection est obtenu en appliquant la méthode d'analyse en composants indépendants (Independent Component Analysais: ICA) à un ensemble d'images naturelles.

III.2.2 Fonction d'image statistique binarisée orientée sécurité (S-BSIF) : La méthode d'extraction de caractéristiques S-BSIF conserve la simplicité de BSIF, mais avec la possibilité de produire à la fois des caractéristiques biométriques révocables (annulables) et cryptées, grâce à deux couches supplémentaires : Projection et Disguise. Ces couches rendent le modèle extrait plus sécurisé contre toute attaque ou intrusion. La figure ci-dessous (Fig. III.2) montre notre structure proposée de S-BSIF qui se compose de deux parties : *Transformation* et *Déguisement*.

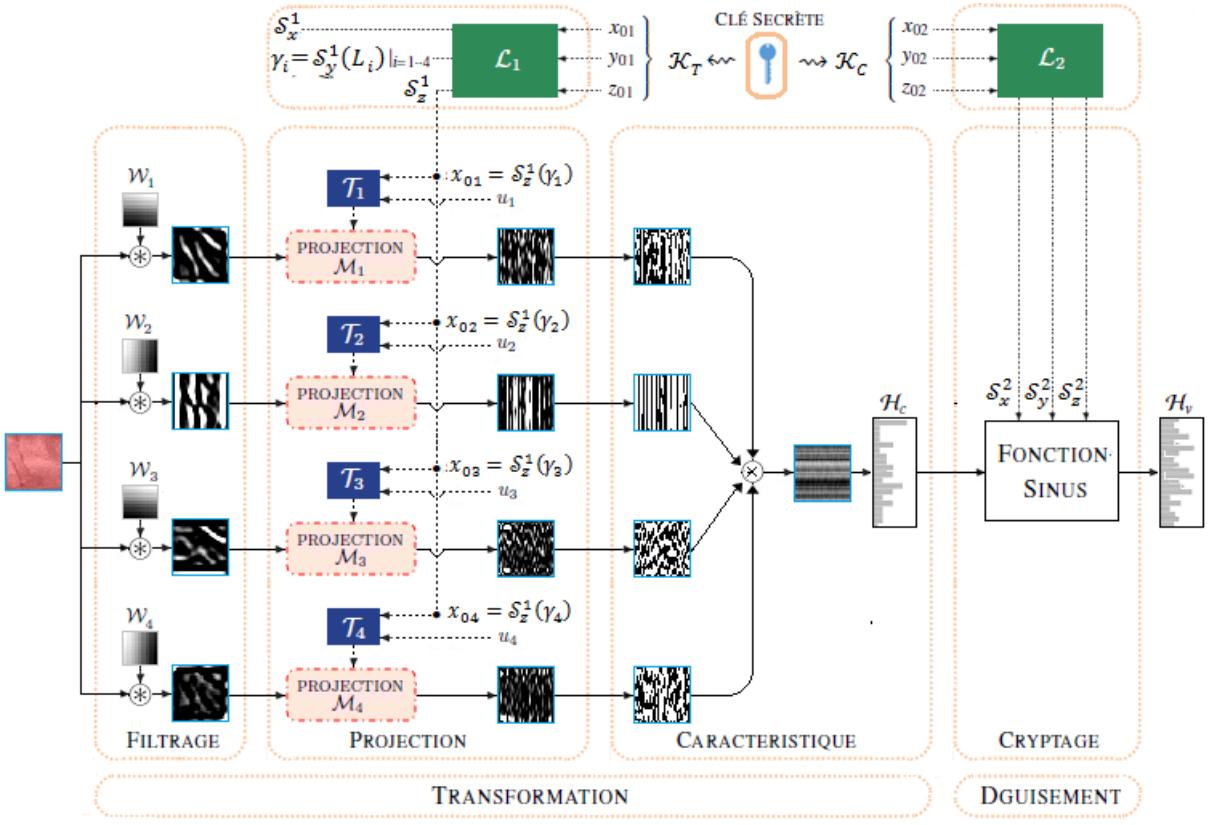


Fig. III.2. Schéma fonctionnel de la méthode d'extraction de caractéristiques révocables basée sur les cartes chaotiques. Un exemple de structure S-BSIF avec 4 filtres de convolution.

En général, cette structure peut être divisée en quatre étapes principales : *filtrage*, *projection*, *extraction de caractéristiques* (hachage binaire et histogramme par bloc) et *cryptage*.

☑ **Transformation :** Dans cette partie et afin de garantir la propriété de révocabilité, nous avons ajouté une couche qui permet de transformer le vecteur en cas de besoin. Le processus de transformation repose sur la projection d'images filtrées dans des espaces orthogonaux générés par une clé secrète qui contrôle un ensemble de systèmes chaotiques. De plus, nous avons changé la méthode d'extraction des vecteurs de l'histogramme classique vers l'histogramme des gradients orientés (Histogram of Oriented Gradients: HOG) en raison de l'efficacité de ce dernier. Cette partie comprend essentiellement trois étapes: filtrage, projection, extraction de caractéristiques.

- **Etape 1: Filtrage :** L'objectif principal de l'étape de filtrage (convolution) est de filtrer les caractéristiques inutiles de l'image d'entrée. En pratique, ce processus utilise des filtres prédéfinis et chaque filtre est convolé avec l'image d'entrée.

Afin de décrire le cadre du système, supposons que nous ayons une image d'entrée de taille $h \times w$ et que la taille du patch, c'est-à-dire la taille du filtre de convolution (2D), soit :

$$W_i = k_1 \times k_2, \quad i = 1,2,\cdots \ell \qquad (1)$$

Où ℓ désigne le nombre de filtres dans la couche de convolution. Il est important de noter que $k_j|_{j=1,2}$ est un nombre entier impair satisfaisant les conditions suivantes : $k_j \leq h$ et $k_j \leq w$.

Les sorties de cette étape sont obtenues en filtrant l'image d'entrée (I^o) par les filtres W_i:

$$I_s^i = I_o \circledast W_i, \quad i = 1,2,\cdots,\ell \qquad (2)$$

Où $\circledast$ désigne un processus de convolution 2D. Il est important de noter que pour obtenir des images filtrées de même taille que I_o, une interpolation de frontière (traitement des bords par remplissage avec des zéros) est appliquée. Enfin, en utilisant les L filtres, nous pouvons obtenir *L* images filtrées pour chaque image d'entrée.

- **Etape 2: Projection :** En tant que solution de sécurité, cette étape masque les templates biométriques afin qu'ils puissent être annulés et remplacés par un autre à tout moment. Ainsi, les templates résultants changent avec le changement de clé secrète tout en préservant, dans la mesure du possible, les performances du système biométrique. Dans notre système, nous avons adopté le principe de la projection de templates dans un espace orthogonal. Cette étape contient deux processus, à savoir la génération de l'espace de projection (matrice) et la projection dans l'espace généré.

✍ ***Processus de génération de matrices:*** L'étape de projection commence par générer les matrices de projection pour chaque sortie de l'opération de filtrage (couche de convolution).

Ainsi, notre système utilise plusieurs systèmes chaotiques (**voir Annexe C**), dont l'un est principal (clés secrètes) et les autres (qui servent à générer les matrices de projection) changent en fonction du nombre de filtres (ℓ) dans la couche de convolution. Il est important de souligner que la clé secrète ($\mathcal{K}$) de notre système peut être représentée par une valeur réelle ou entière codée en hexadécimal. Dans la sous-section suivante, nous donnerons un exemple de clé secrète représentée sous forme de valeur entière.

Premièrement, utiliser la clé secrète ($\mathcal{K}_T$) et le principal système chaotique,$\mathcal{L}_1$, (le système chaotique utilisé est le système dynamique de ***Lorenz***) pour générer trois séquences ($\mathcal{S}_x^1, \mathcal{S}_y^1$ et $\mathcal{S}_z^1$) qui sont utilisées pour contrôler les systèmes chaotiques auxiliaires (les systèmes chaotiques utilisés sont le système dynamique de ***Tent***). Soit $\mathcal{K}_T$ une clé secrète (pour la partie de transformation) représentée par :

$$\mathcal{K}_T = \biguplus_{j=0}^{2} \widetilde{\mathcal{K}}_{Tj} = \widetilde{\mathcal{K}}_{T0} \widetilde{\mathcal{K}}_{T1} \widetilde{\mathcal{K}}_{T2} \qquad (3)$$

Où $\widetilde{\mathcal{K}}_{Ti}$ est une valeur hexadécimale codée sur *M-bits* (dans notre travail *M = 16*) et $\biguplus$ est une fonction de concaténation qui permet à une nouvelle valeur de rejoindre la chaîne hexadécimale. Ainsi, les paramètres de système principal ($\mathcal{L}_1$) sont définis comme suit:

$$\begin{cases} x_{01} = \frac{\mathcal{K}_{T0}}{2^{16}} \\ y_{01} = \frac{\mathcal{K}_{T1}}{2^{16}} \\ z_{01} = \frac{\mathcal{K}_{T2}}{2^{16}} \end{cases} \qquad (4)$$

Où $\mathcal{K}_{Ti}|_{i=0,1,2}$ est la représentation décimale de la valeur hexadécimale $\widetilde{\mathcal{K}}_{Ti}|_{i=0,1,2}$. Cette représentation est choisie pour que le système chaotique de ***Lorenz*** conserve toujours leur comportement chaotique. L'objectif de système chaotique $\mathcal{L}_1$ est de générer trois séquences ($\mathcal{S}_x^1, \mathcal{S}_y^1$ et $\mathcal{S}_z^1$) afin de déterminer de déterminer les états initiaux ($x_{0i}^{\mathcal{T}}|_{i=1,2,..,\ell}$) et les paramètres de contrôle ($u_{0i}^{\mathcal{T}}|_{i=1,2,..,\ell}$) des systèmes chaotiques auxiliaires ($\mathcal{T}_i|_{i=1,2,..,\ell}$).

$$\begin{cases} x_{0i}^{\mathcal{T}} = \mathcal{S}_z^1(\gamma_i), \quad \text{avec } \gamma_i = \mathcal{S}_y^1(L_i) \\ u_i^{\mathcal{T}} = \alpha + \beta \cdot \mathcal{S}_x^1(\ell + L_i) \end{cases} \qquad (5)$$

Où la paire (α, β) est égale à (1.41, 0,58) pour la carte tente et elles sont choisies pour que le système chaotique conserve toujours leur comportement chaotique. $L_i|_{i=1,2,..,\ell}$ sont des valeurs entières prédéfinies par le système et peuvent être modifiées selon les besoins. A partir de ces équations, il est clair que $\mathcal{S}_x^1$ et $\mathcal{S}_z^1$ sont des séquences à coefficients réels (afin de les utiliser pour déterminer les états initiaux et les paramètres de contrôle) et $\mathcal{S}_y^1$ est une séquence entière qui détermine les coordonnées des valeurs de $x_{0i}^{\mathcal{T}}$ et $u_i^{\mathcal{T}}$ dans les séquences $\mathcal{S}_x^1$ et $\mathcal{S}_z^1$. Les

éléments de $\mathcal{S}_y^1$ doivent donc être quantifiés pour être entiers. En effet, la séquence $\mathcal{S}_y^1$ est normalisée dans l'intervalle [1, 100], comme suit :

$$\mathcal{S}_y^1 = 1 + \lfloor 10^5 \cdot \mathcal{S}_y^1 \rfloor (mod\ 100)\ \in [1\ \cdot\cdot 100] \quad (6)$$

Où $\lfloor \bullet \rfloor$ désigne la partie entière. Enfin, chaque système chaotique auxiliaires ($\mathcal{T}_i|_{i=1,2,..,\ell}$). génère une séquence de longueur $h \cdot w$:

$$\mathcal{S}_i^{\mathcal{T}} = \mathcal{T}_i(x_{0i}, u_i) = \{s_j\}_{j=1}^{h \cdot w} \qquad i = 1,2,\cdot\cdot\ \ell \quad (7)$$

Chaque séquence ($\mathcal{S}_i^{\mathcal{T}}$) est ensuite réorganisée pour former une matrice ($\mathcal{M}_i$) de même taille que l'image d'entrée :

$$\mathcal{M}_i = F_{h,w}\left(\mathcal{S}_i^{\mathcal{T}}\right) \in \mathbb{R}^{h \times w} \quad i = 1,2,\cdot\cdot\ \ell \quad (8)$$

Où $F_{h,w}$est une fonction qui réorganise le vecteur $\mathcal{S}_i^{\mathcal{T}} \epsilon\, R^{1 \times h \cdot w}$ en une matrice $\mathcal{M}_i\, \epsilon\, R^{h \times w}$. Une fois les différentes matrices ($\mathcal{M}_i$) sont générées et pour garantir des sorties de projection non corrélées, une opération de factorisation est appliquée à chaque matrice. Pour ce faire, nous avons utilisé la factorisation *QR* qui est l'une des opérations importantes de l'analyse matricielle dans le traitement du signal / image et les statistiques.

Soit $\mathcal{M}_i$ une matrice composée des différentes colonnes v_i définies comme suit:

$$\mathcal{M}_i = \left[v_0^i, v_1^i, v_2^i, \cdot\cdot\ v_w^i\right] \quad (9)$$

La factorisation *QR* effectue la décomposition orthogonale-triangulaire de la matrice $\mathcal{M}_i$, où cette matrice est décomposée en deux matrices, dont l'une est une matrice unitaire réelle ($\mathcal{Q}$) et l'autre est une matrice triangulaire supérieure ($\mathcal{R}$).

$$\mathcal{M}_i = \mathcal{Q}_i \cdot \mathcal{R}_i,\ \ \mathcal{R}_i \in \mathbb{R}^{w \times w},\ \mathcal{Q}_i \in \mathbb{R}^{h \times w} \quad (10)$$

La matrice résultante $\mathcal{Q}_i$ a la même dimension que $\mathcal{M}_i$ mais avec des colonnes orthogonales. Enfin, ces matrices orthogonales ($\mathcal{M}_i|_{i=1}^{\ell}$) sont utilisées pour transformer les sorties de la couche de convolution (filtrage) dans un autre espace pour leur permettre d'être cachées.

✍ ***Processus de projection*:** A l'aide des matrices $\mathcal{Q}_i$, on peut projeter les différentes images filtrées comme suit :

$$\hat{I}_s^i = I_s^i \cdot \mathcal{Q}_i \in \mathbb{R}^{h \times w},\ i = 1,\cdot\cdot\ \ell \quad (11)$$

Où $\hat{I}_s^i$ désigne la sortie de l'étape de projection.

- **Etape 3: Représentation de caractéristiques :** Cette étape permet d'extraire les caractéristiques de l'image projetée. Il se compose de deux processus principaux, à savoir le hachage binaire et l'histogramme.

✍ ***Hachage binaire*** **:** La condition la plus importante pour le système biométrique révocable est la non-réversibilité du vecteur caractéristique biométrique résultant. Heureusement, cette couche permet de vérifier cette condition, dans laquelle les images projetées ($\hat{I}_s^i|_{i=1}^{\ell}$) sont binarisées. Dans cette couche, les ℓ sorties pour l'image d'entrée, sont converties en une image à valeur entière en utilisant la quantification binaire et la conversion binaire en décimal.

Le processus de quantification binaire transforme une valeur réelle en valeur binaire. En fait, le principe de seuillage est appliqué, comme suit:

$$I_s^{b,i} = \begin{cases} 1 & \text{if } \hat{I}_s^i \geq \tau_0 \\ 0 & \text{if } \hat{I}_s^i < \tau_0 \end{cases}, \qquad i = 1,2,\cdots \ell \tag{12}$$

Où τ_0 est le seuil de binarisation. En pratique, ce seuil est choisi égal à 0 ($\tau_0 = 0$) car les résultats de la projection ont la même probabilité d'être négatifs ou positifs.

Dans l'étape de conversion binaire, la chaîne de binaires (ℓ-bits) autour de chaque pixel est convertie en valeur entière. Pour cela nous utilisons le polynôme de décodage suivant :

$$I_s^h = \sum_{i=1}^{\ell} I_s^{b,i} \cdot 2^i , \qquad i = 1,\cdots \ell \tag{13}$$

Où I_s^h est le descripteur de l'image d'entrée.

- **Histogramme:** Afin d'extraire le vecteur de caractéristiques de l'image d'entrée, la méthode d'extraction de caractéristiques basée sur le HOG est utilisée comme opération de regroupement. Ainsi, l'histogramme de l'image descripteur I_s^h est calculé par bloc pour une forte discrimination. Pour cela, nous partitionnons d'abord le descripteur I_s^h en blocs. Ainsi, en supposant que la taille du bloc utilisé ($\mathcal{B}$) est $b_1 \times b_2$ avec un taux de chevauchement *o*, chaque image est partitionnée en $\mathcal{N}_B$ blocs comme suit:

$$\mathcal{N}_B = \left\lfloor \frac{h - b_1}{o} + 1 \right\rfloor \times \left\lfloor \frac{w - b_2}{o} \right\rfloor \tag{14}$$

Pour toute image, on obtient un ensemble de blocs ψ définis comme suit :

$$\psi = \{\mathcal{B}_1, \mathcal{B}_2, \cdots \mathcal{B}_{\mathcal{N}_B}\} \epsilon \mathbb{R}^{(b_1 \times b_2) \times \mathcal{N}_B} \ \ avec \ \ \mathcal{B} \epsilon \mathbb{R}^{b_1 \times b_2} \tag{15}$$

Où $\mathcal{B}_c$ désigne le c^{th} bloc. Dans le processus d'histogramme, chaque bloc ($\mathcal{B}_c$) est représenté par un vecteur qui est extrait par la technique HOG [33].

$$\mathcal{H}_c = \mathcal{F}_{HOG}(\mathcal{B}_c), \qquad c = 1,2,..,\mathcal{N}_B \tag{16}$$

Tous les histogrammes calculés sont donc concaténés en un seul vecteur pour obtenir le vecteur de caractéristiques biométriques (Template biométrique) de l'image d'entrée (I_o):

$$\mathcal{V}_o = [\mathcal{H}_1, \mathcal{H}_2, \cdots \mathcal{H}_{\mathcal{N}_B}] \tag{17}$$

Il est important de noter que la longueur et la précision du vecteur ($\mathcal{V}_o$), de chaque image d'entrée, change selon à la taille du bloc ($b_1 \times b_2$) et le taux de chevauchement (*o*).

☑ **Déguisement:** Dans cette étape et afin de mieux protéger le gabarit biométrique, on le déguise en utilisant la technique de la cryptographie. Ce processus est contrôlé par le deuxième système chaotique principal ($\mathcal{L}_2$ pour le système de ***Lorenz***). Dans notre travail, la technique retenue est la transformation sinusoïdale [34]. Avant de décrire notre méthodologie, nous présentons brièvement la transformation sinus.

- **Transformation sinus :** Comme toutes les techniques de cryptage, cette technique permet de crypter l'image à l'aide d'une clé secrète. Avant de commencer à le décrire, nous allons d'abord présenter quelques notations qui sont utilisées dans cette section.

$\mathcal{V}_o$: Un vecteur de caractéristiques biométriques extraites de la modalité biométrique.

$$\mathcal{V}_o = [x_1, x_2, x_3, \cdots, x_n] \quad (18)$$

$\mathcal{Y}_o$: Un vecteur transformé après transformation sinusoïdale appliquée sur $\mathcal{V}_o$.

$$\mathcal{Y}_o = [y_1, y_2, y_3, \cdots, y_n] \quad (19)$$

$\mathcal{E}_o$: Un vecteur aléatoire, dans lequel e_1 est choisi aléatoirement entre $[-1, 1]$.

$$\mathcal{E}_o = [e_1, e_2, e, \cdots, e_n] \quad (20)$$

$\mathcal{P}$: une chaîne de nombre de période dans les éléments de $\mathcal{V}_o$.

$$\mathcal{P} = p_1, p_2, p_3, \cdots, p_n \quad (21)$$

Ce processus fonctionne en deux étapes : Extraction de la période et la transformation.

✍ ***Extraction de la période*:** Puisque nous utilisons la fonction sinus qui est périodique avec la période de 2π, nous devons savoir à quelle période x_i appartient. Pour chaque x_i de $\mathcal{V}_o$, on a

$$x_i = \alpha_i + p_i \cdot 2\pi \quad (22)$$

Par conséquent, nous calculons p_i par l'équation suivante :

$$p_i = \left\lfloor \frac{x_i}{2\pi} \right\rfloor \quad (23)$$

Où p_i est le nombre de période de x_i. Après cela, toutes les données de période p_i du vecteur de caractéristique $\mathcal{V}_o$ sont stockées dans la base de données pour une vérification ultérieure.

✍ ***Transformation*:** Lorsque l'étape d'extraction de caractéristiques est terminée, le vecteur de caractéristiques (Template) $\mathcal{V}_o$ d'un utilisateur sera transformé en vecteur $\mathcal{Y}_o$. Pour chaque élément x_i dans $\mathcal{V}_o$

$$\sin(x_i + y_i) = e_i \quad (24)$$

Ainsi, nous pouvons écrire $y_i = f(x_i)$ comme suit :

$$y_i = \arcsin(e_i) - \alpha_i \quad (25)$$

Parce que $\arcsin(e_i) \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ et $\alpha_i \in [0, 2\pi]$, donc la valeur de y_i est comprise entre $[-\frac{5\pi}{2}, \frac{\pi}{2}]$. La figure ci-contre (**Fig. III.3**) illustre bien l'opération de transformation.

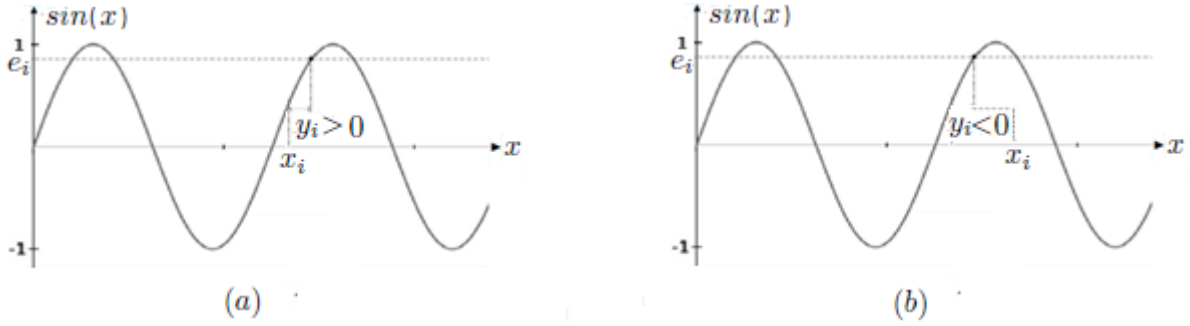


Fig. III.3. Cryptage de x_i basée sur la transformation sinus *(a)* Transformation sinus avec $y_i > 0$, et *(b)* Transformation sinus avec $y_i < 0$

En raison de la propriété périodique du sinus, pour chaque valeur de x_i, nous trouverons exactement une valeur y_i. Cependant, étant donné une valeur de yi, nous ne pouvons pas dériver exactement x_i, car il existe de nombreuses valeurs correspondant à ce y_i. En d'autres termes, cette fonction de transformation est non inversible. On peut aussi choisir une autre fonction périodique ayant la même caractéristique avec la fonction sinus (comme la fonction cosinus).

☑ **Méthodologie :** Dans le processus de cryptage, nous avons utilisé une autre clé secrète ($\mathcal{K}_C$) pour contrôler le deuxième système chaotique de ***Lorenz***, $\mathcal{L}_2$. Ce système génère également trois séquences ($\mathcal{S}_x^2, \mathcal{S}_y^2$ et $\mathcal{S}_z^2$) qui permettent : *i)* de réorganiser les éléments de x_i, *ii)* de pondérer les éléments x_i et *iii)* de déterminer les valeurs aléatoires e_i pour chaque x_i.

Soit $\mathcal{K}_C$ une clé secrète (pour la partie de cryptage) représentée par :

$$\mathcal{K}_C = \biguplus_{j=0}^{2} \widetilde{\mathcal{K}}_{Cj} = \widetilde{\mathcal{K}}_{C0}\widetilde{\mathcal{K}}_{C1}\widetilde{\mathcal{K}}_{C2} \qquad (26)$$

Où $\widetilde{\mathcal{K}}_{Ci}$ est une valeur hexadécimale codée sur *M-bits* (dans notre travail *M = 16*). Ainsi, les paramètres de système principal ($\mathcal{L}_2$) sont définis comme suit:

$$\begin{cases} x_{02} = \frac{\mathcal{K}_{C0}}{2^{16}} \\ y_{02} = \frac{\mathcal{K}_{C1}}{2^{16}} \\ z_{02} = \frac{\mathcal{K}_{C2}}{2^{16}} \end{cases} \qquad (27)$$

Où $\mathcal{K}_{Ci}|_{i=0,1,2}$ est la représentation décimale de la valeur hexadécimale $\widetilde{\mathcal{K}}_{Ci}|_{i=0,1,2}$. Avant l'opération de cryptage, le template biométrique ($\mathcal{V}_o$) est d'abord réorganisé par la séquence $\mathcal{S}_x^2$. Soit $\mathcal{S}_x^{2b}$ une séquence de composantes entières, produite à partir de la séquence $\mathcal{S}_x^2$:

$$\mathcal{S}_x^{2b} = 1 + \lfloor 10^5 \cdot \mathcal{S}_x^2 \rfloor (mod\ \eta_v) \in [1 \cdots \eta_v] \qquad (28)$$

Où η_v est la longueur de template $\mathcal{V}_0$. Nous divisons la séquence $\mathcal{S}_x^{2b}$ en deux sous-séquences ($\mathcal{S}_{x1}^{2b}$ et $\mathcal{S}_{x2}^{2b}$) comme :

$$\begin{cases} \mathcal{S}_{x1}^{2b} = \{c_i^1\}_{i=1,3,5,\dots,\eta_v} \\ \mathcal{S}_{x2}^{2b} = \{c_i^2\}_{i=2,4,6,\dots,\eta_v} \end{cases} \quad (29)$$

Ensuite, une simple permutation entre les composantes de $\mathcal{V}_o$ est appliquée :

$$\mathcal{V}_o(\mathcal{S}_{x1}^{2b}(i)) \leftrightarrows \mathcal{V}_o(\mathcal{S}_{x2}^{2b}(i)) \Leftrightarrow \mathcal{V}_o(c_i^1) \leftrightarrows \mathcal{V}_o(c_i^2) \quad (30)$$

Ensuite, le template réorganisé ($\mathcal{V}_0^z$) est pondéré par la séquence $\mathcal{S}_y^2$:

$$\mathcal{V}_0^{\mathrm{P}}(\mathrm{i}) = \mathcal{V}_0^z(\mathrm{i}) \cdot \mathcal{S}_{\mathrm{y}}^2(\mathrm{i}), \ \ \mathrm{i} = 1,2,3,\cdot\cdot,\eta_{\mathrm{v}} \quad (31)$$

Il est important de noter que tous les éléments de la séquence $\mathcal{S}_y^2$ qui sont nuls sont remplacés par 1 afin d'éviter de perdre la valeur d'origine de $\mathcal{V}_0^P$ ($\mathcal{V}_0^P(\mathrm{i})|_{i=1,2,3,\cdot\cdot,\eta_v}$).

Enfin, en utilisant la séquence $\mathcal{S}_z^2$, nous appliquons la transformation sinus au modèle pondéré $\mathcal{V}_0^P$. Comme l'amplitude de la fonction sinus varie de -1 à 1, les éléments de la séquence $\mathcal{S}_z^2$ doivent également appartenir à l'intervalle [-1,1]. Ces éléments sont à l'origine positifs, pour cela une opération de normalisation est appliquée à $\mathcal{S}_z^2$ afin de produire une séquence qui contient à la fois des éléments positifs et négatifs. En fait, pour normaliser la séquence $\mathcal{S}_z^2$, il suffit de supprimer leur valeur moyenne :

$$\mathcal{S}_z^N = \mathcal{S}_z^2 - \rho_Z \quad (32)$$

Où ρ_Z est la valeur moyenne de $\mathcal{S}_z^2$. La séquence $\mathcal{S}_z^2$ est alors utilisée comme vecteur aléatoire $\mathcal{E}_o$:

$$\mathcal{E}_o(i) = \mathcal{S}_z^N(i) \quad (33)$$

Le processus de cryptage est appliqué comme nous l'avons déjà vu précédemment. Finalement, il est à noter que notre méthode proposée peut fonctionner selon quatre configurations de base, comme le montre le tableau suivant:

Tableau 1 : Moyen de protection de Template biométrique

Etapes				**Moyen de protection de Template biométrique**
Filtrage	**Projection**	**Caractéristiques**	**Cryptage**	
x		**x**		Non-sécurisé
x	**x**	**x**		Sécurisé : Biométrie révocable
x		**x**	**x**	Sécurisé : Crypto-biométrique
x	**x**	**x**	**x**	Sécurisé : Hybride

Il ressort clairement de ce tableau que notre méthode inclut déjà la version originale du BSIF. De plus, il peut produire des templates biométriques très sécurisés qui vont de moyen à plus sécurisé (par exemple un système hybride).

III.3 Résultats expérimentaux

L'évaluation d'un système d'identification biométrique revient à déterminer, par des tests, les différents paramètres du système (dans notre cas, le nombre et la taille des filtres de la méthode S-BSIF, et le seuil de décision du système) avec laquelle une personne (enregistrée ou non dans la base de références du système) est correctement reconnue. La présente section porte sur différentes expérimentations réalisées dans le but d'évaluer la performance et la robustesse de la méthode développée.

III.3.1 Base d'images multi-spectrales : Pour l'évaluation de notre système, nous avons utilisé une base de données d'empreintes palmaires créée par l'Université polytechnique de Hong Kong (PolyU) [35]. Cette base de données a été obtenue en collectant des images d'empreintes palmaires multispectrales de 300 individus à l'aide d'un dispositif de capture d'empreintes palmaires multispectrales. Les personnes inscrites dans cette base de données sont les étudiants et les travailleurs de PolyU. Dans cette base de données, 195 personnes sont mâles et les restes sont des femelles, et la répartition par âge se situe entre 20 et 60 ans. Les personnes ont été invitées en deux sessions pour fournir environ 12 images (six images dans chaque session). L'intervalle moyen entre la première et la deuxième session est de 9 jours. Toutes les images ont été fournies sous différentes conditions d'éclairage. Cette base de données (PolyU) contient 3600 images de quatre bandes spectrales différentes : Rouge (R), Vert (V), Bleu (B) et *proche infrarouge (N)* (total des bandes égal à 14400). Toutes les images originales ont une taille de 352x288 pixels et une résolution de <100 dpi. Dans nos tests, nous n'avons utilisé que la bande proche infrarouge qui elle-même représente une biométrie appelée empreinte des réseaux veineux.

III.3.2 Protocole de tests : Dans le cadre de l'expérimentation menée dans la phase d'identification, nous avons utilisé une base de données contenant 300 personnes (12 images pour chaque personne, donc 3600 images). Cette base est similaire au nombre d'employés des petites et moyennes entreprises. Trois images pour chaque personne, soit 900 images, sont utilisées pour l'enrôlement et le reste, 1700 images pour tester le système. Pour la mesure des performances, les distributions imposteurs et clients sont générées par 403650 et 2700 comparaisons, respectivement.

III.3.3 Evaluation de performance: Les résultats expérimentaux que nous allons présenter dans ce travail sont divisés en quatre parties. Nous donnerons dans un premier temps les résultats obtenus concernant la sélection des meilleurs paramètres de la méthode BSIF (nombre et taille des filtres). Ensuite, dans la deuxième partie, nous présentons les résultats des tests des systèmes biométriques qui sont basés sur la méthode BSIF (système non protégé). La troisième partie des résultats se concentre en particulier sur le système protégé en exploitant notre méthode proposée S-BSIF. La dernière partie porte sur le niveau de sécurité de notre méthode.

☑ **Tests préliminaires:** Habituellement, dans tous les systèmes biométriques, une série de tests empiriques est effectuée afin de sélectionner les paramètres optimaux de la méthode d'extraction de caractéristiques. Par conséquent, avant de commencer à évaluer notre méthode proposée (S-BSIF), qui dépend principalement de la méthode du BSIF, nous devons d'abord sélectionner la meilleure configuration du BSIF en choisissant ses paramètres optimaux, qui ont un impact significatif sur la performance du système biométrique. Puisque l'efficacité du BSIF dépend non seulement du nombre de filtres (ℓ) mais aussi de la taille des filtres ($k_1 \times k_2$), nous pouvons effectuer une série d'expériences pour sélectionner efficacement les paramètres appropriés. Ainsi, la variation de ces paramètres permet de donner plusieurs vecteurs de caractéristiques biométriques (templates), et il est donc possible de choisir expérimentalement et empiriquement les paramètres appropriés, ce qui peut effectivement améliorer la précision du système d'identification biométrique en ajustant ces paramètres et choisissez le meilleur.

Dans notre travail, nous essayerons de sélectionner le nombre de filtres (ℓ) parmi huit nombres prédéfinis (5, 6, 7, 8, 9, 10, 11, 12). De plus, la taille des filtres de convolution ($k_1 \times k_2$) sera choisie parmi sept tailles prédéfinies (5×5, 7×7, 9×9, 11×11, 13×13, 15×15, 17×17). Il est à noter que ces filtres sont construits à partir d'une base de données d'images naturelles et qu'ils se sont avérés efficaces notamment dans le domaine biométrique. Pour examiner l'effet de ces paramètres sur la précision du système d'identification biométrique (en mode ensemble ouvert), nous illustrons, pour les deux classifiers (*k* plus proches voisins (k Nearest Neighbors : KNN) et machine à vecteurs de support (Support Vector Machine : SVM)), les performances du système sous forme de taux d'erreur égales (Equal Error Rate: EER) et Intervalle de Confiance (IC) et les résultats obtenus sont présentés dans les Figures III.4 et III.5 pour le KNN et le SVM, respectivement. Ainsi, à partir des courbes de la figure III.4, nous pouvons tirer deux remarques importantes:

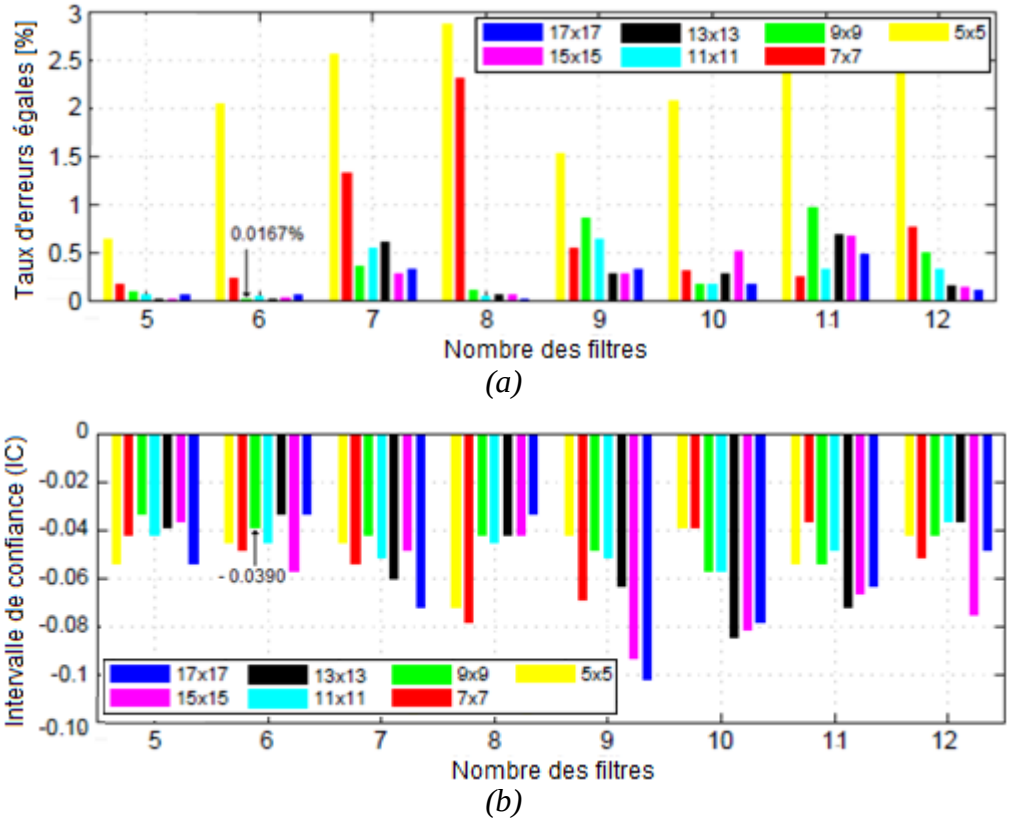


Fig. III.4. Sélection des paramètres de BSIF d'un système basé sur KNN. *(a)* Taux d'erreurs égales (EER) et *(b)* Intervalle de confiance (IC)

- Avec l'utilisation du classifier KNN, le système biométrique n'atteint pas des performances parfaites (il y a toujours un chevauchement des deux distributions, imposteur et clients (EER ≠ 0 et IC < 0)). Par conséquent, en peut changer le classifier, et réexaminer le système biométrique.
- Les performances s'améliorent presque toujours dans le cas de grandes tailles de filtres et augmentent dans le cas d'un petit nombre de filtres et dans la plupart de ces paramètres, le système peut fonctionner avec des performances élevées pouvant dépasser (EER < 0.500% et taux des clients acceptés (GAR) = 99,5%).

A partir de la Fig. III.4.*(b)*, on observe qu'en général, l'intervalle de confiance devient négatif pour tous les nombres de filtres (chevauchement des deux distributions). Lorsque nous utilisons 5 ou 6 filtres, la taille du filtre de convolution de $k_1 \times k_2 = 9 \times 9$ donne la meilleure performance (EER = 0.0167% et un seuil T_o = 0.7370). Ainsi, un acceptable IC = - 0.0390) est obtenu dans le cas de six filtres de convolution ($\ell = 6$). Dans ce cas, le système fonctionne avec un taux des clients acceptés (GAR) maximum égal à 99,9833%. Il est important de noter que tous les scores obtenus dans le système d'identification biométrique basé sur le PLM sont normalisés à l'intervalle [0,1] en le divisant par un facteur de 1500.

Contrairement au système basé sur KNN, le SVM a donné des performances parfaites. A partir des courbes de la Fig. III.5, on peut noter :

- Le système maintient la propriété qu'un petit nombre de grandes tailles des filtres offrent les meilleures performances;
- Les filtres de petite taille donnent des performances médiocres comme le cas de 5x5 ;
- Séparation complète de deux distributions (et donc EER nulle) dans de nombreux cas (11×11, 13×13, 15×15 et 17×17).

Si l'on considère la plus grande valeur de IC, cinq filtres de convolution d'une taille de 17×17 offrent les meilleures performances dans le système biométrique basé sur SVM (voir Fig. III.5.*(a)*). Dans cette configuration, le système fonctionne parfaitement avec une valeur IC acceptable de 0,0510 (voir Fig. III.5.*(b)*) et un GAR idéal à un seuil (T_o) égal à 0,6961.

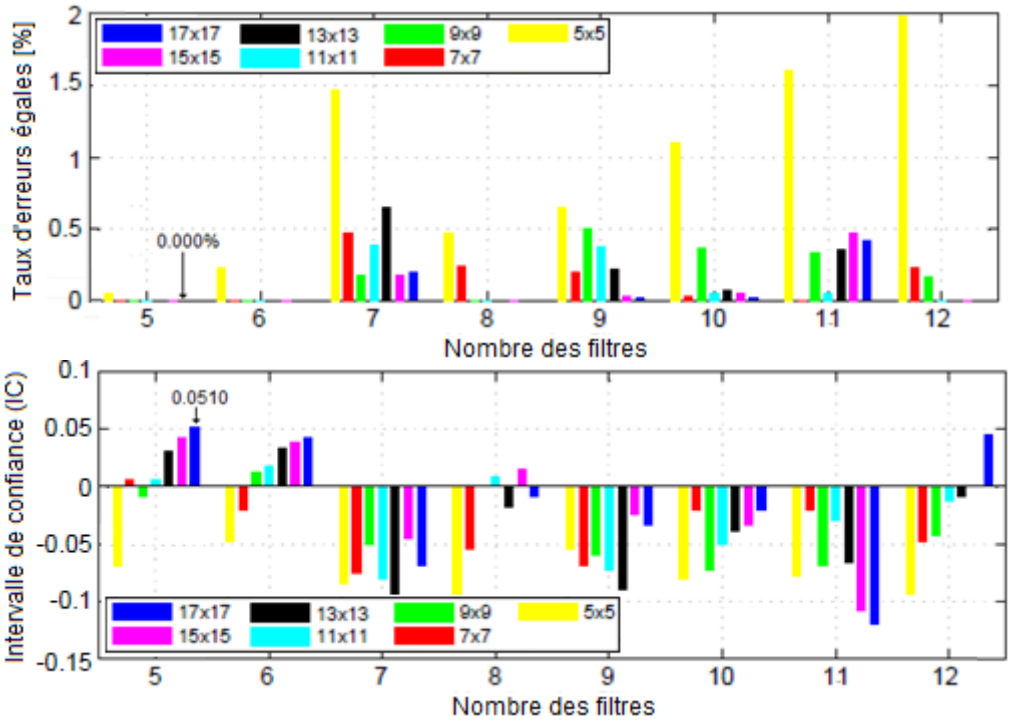


Fig. III.5. Sélection des paramètres de BSIF d'un système basé sur SVM. *(a)* Taux d'erreurs égales (EER) et *(b)* Intervalle de confiance (IC)

A partir de ces tests, on peut remarquer que :

i) Une performance très acceptable peut être obtenue avec toutes les combinaisons possibles de n et k où un taux d'identification effectif (GAR) supérieur à 97,00% a déjà été obtenu.

ii) En général, plus le nombre de filtres est petit, plus le taux d'identification est élevé, de sorte que les meilleurs résultats ont été obtenus avec 5 filtres, ce qui est meilleur que les performances obtenues avec 12 filtres.

iii) En général, plus la taille des filtres est grande, plus le taux d'identification est élevé. Les meilleurs résultats ont été obtenus avec une taille de filtre de 17×17, ce qui est mieux qu'un filtre de taille 5×5.

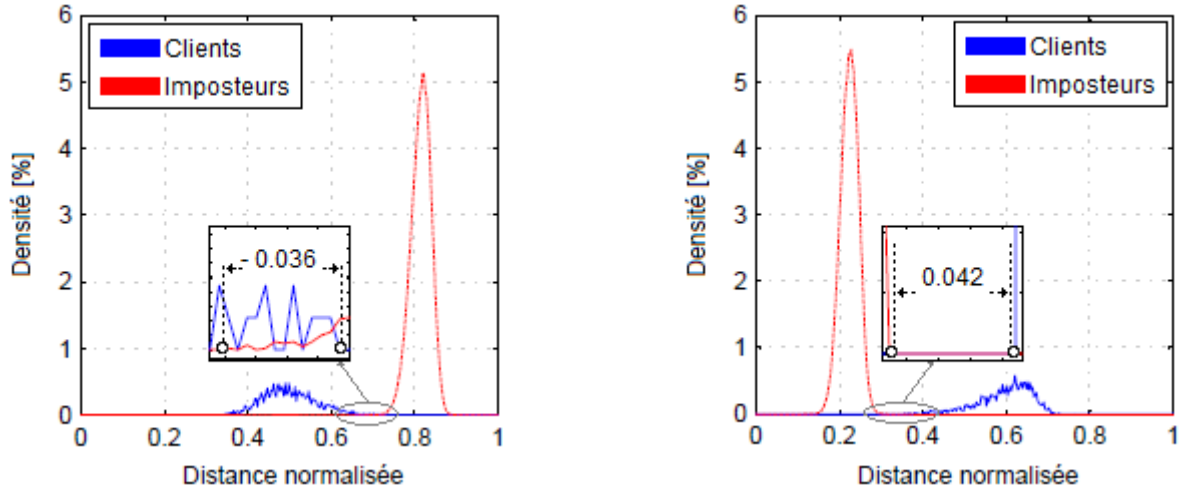
iv) En comparaison avec le classifier KNN, les performances du système peuvent être améliorées avec le classifier SVM, à partir duquel des performances optimales sont obtenues.

☑ **Performance de système biométrique :** Dans cette sous-section, nous évaluerons les performances du système dans deux cas : un système non sécurisé (template non protégé : BSIF) et un système sécurisé (template protégé : S-BSIF). D'après les résultats précédents, le système fonctionne parfaitement dans le cas de 5 filtres d'une taille de 17×17 (EER = 0,00 et IC = 0,052) utilisant le classifier SVM. Pour le classifier KNN, nous avons choisi les meilleurs paramètres (5 filtres d'une taille de 15×15) qui donnent un petit IC (-0,0330) et maintiennent l'efficacité du classifier SVM (EER = 0,000 et IC = 0,0420). Dans ce cas, le système basé sur KNN fonctionne avec un EER = 0,0231% (T_0 = 0,7157).

✍ **Système non-protégé:** Le système biométrique non protégé est un système basé sur la méthode d'extraction de caractéristiques BSIF (template biométrique non révocable). Dans ce système, le niveau de sécurité est très faible, car le système est menacé si le template biométrique est perdu. Dans les systèmes de reconnaissance de formes, le choix d'une méthode d'extraction de caractéristiques est essentiel et cette méthode est souvent efficace si les distributions des clients et imposteurs ne se chevauchent pas, ce qui signifie que le système peut facilement identifier le template s'il s'agit d'un client ou d'un imposteur. De plus, plus la distance entre les deux distributions (l'intervalle de confiance) est grande, plus les performances du système sont élevées, ce qui donne à son tour la flexibilité de choisir la matrice de transformation dans les systèmes protégés.

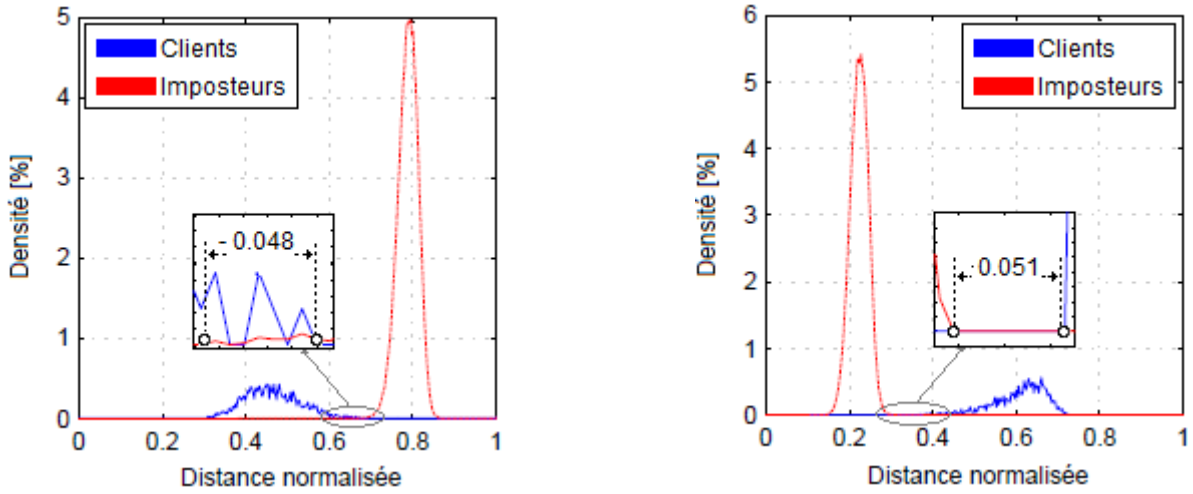
Cette partie consiste à étudier l'effet de deux filtres choisis (15×15 et 17×17) sur la performance du système d'identification. Pour ce faire, les distributions des clients et imposteurs de système biométrique, dans les deux cas (système basé sur KNN et système basé sur SVM), ont été mesurés et les résultats sont illustrés dans les figures III.6 (pour un filtre de 15×15) et III.7 (pour un filtre de 17×17). Pour 5 filtres de taille 15×15 et comme le montre la Fig. III.6, le système fonctionne efficacement en utilisant le classifier SVM. Le taux d'erreur dans cette configuration est nul (EER = 0,000% avec un seuil T_o = 0,3360) avec un intervalle de confiance assez large (IC = 0,0420). Les performances du système biométrique diminuent si le classifier KNN est utilisé (EER = 0,0231% avec un seuil T_o = 0,7157) avec un IC = -

0.0360, mais malgré cela, le taux d'erreur reste très acceptable, surtout si l'on prend la taille de la base de données qui contient 300 personnes.



(a) *(b)*

Fig. III.6. Comportement du système d'identification biométrique basé sur 5 filtres de taille 15×15. *(a)* Système basé sur le classifier KNN et *(b)* Système basé sur le classifier KNN.



(a) *(b)*

Fig. III.7. Comportement du système d'identification biométrique basé sur 5 filtres de taille 17×17. *(a)* Système basé sur le classifier KNN et *(b)* Système basé sur le classifier KNN.

L'observation de la Fig. III.7 nous montre que 5 filtres de taille 17×17 donnent une erreur d'identification parfaite égale à 0,000% et un seuil de 0,3435 avec un grand IC qui est égal à 0,052 toujours dans le cas de la classifier SVM. Une dégradation importante égale à 132,490% est obtenue (EER = 0.0537% et un seuil T_o = 0.6961) en utilisant le filtre 17×17 au lieu du filtre 15×15 dans le cas de la classification KNN. Dans les figures Fig. III.8. *(a)* et Fig. III.8. *(b)*, nous présentons une comparaison des performances du système d'identification biométrique entre les deux classifiers KNN et SVM pour les deux tailles de filtres examinées.

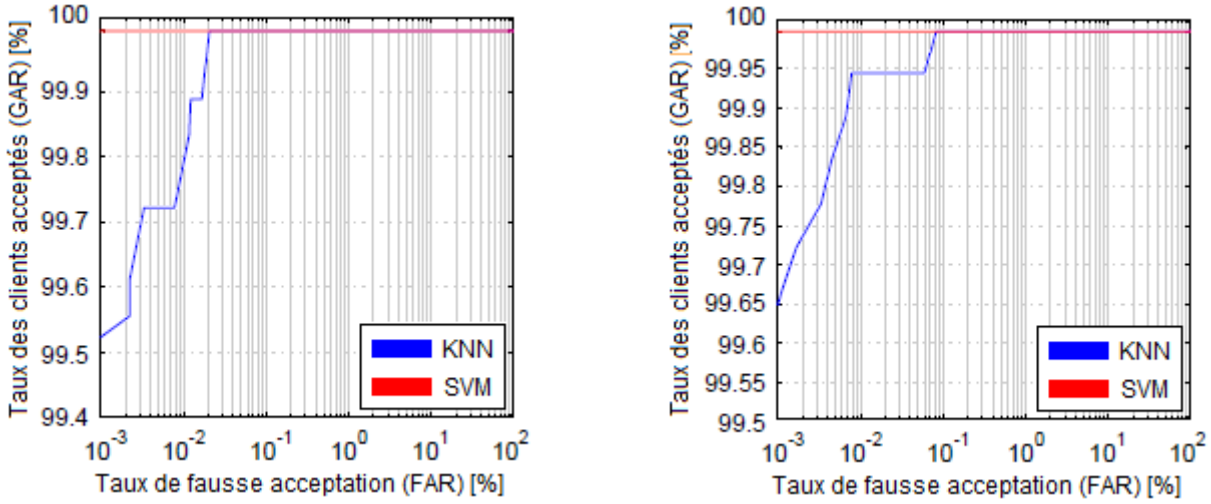


Fig. III.8. Comparaison des performances de système biométrique. *(a)* 5 filtres de taille 15×15 et *(b)* 5 filtres de taille 17×17.

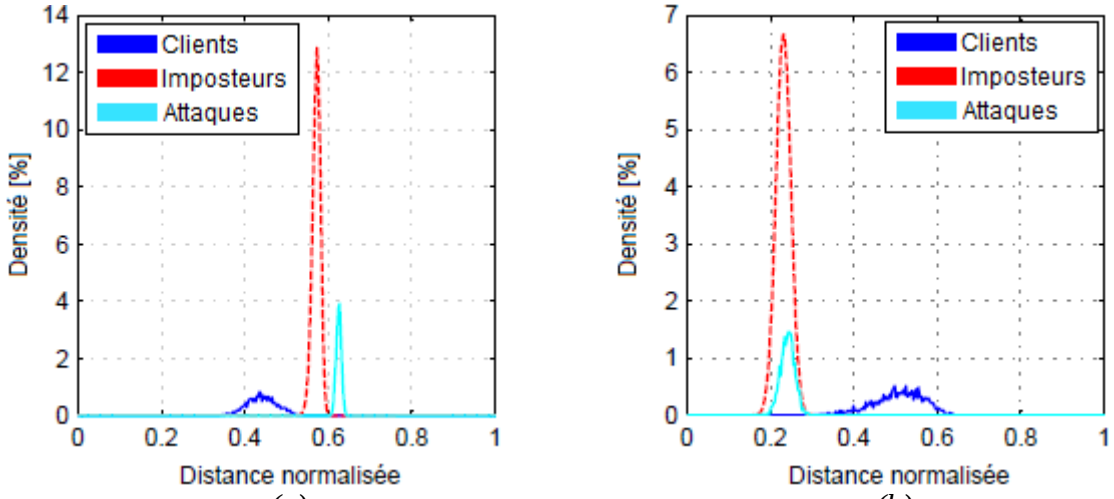
Ces figures indiquent clairement que le classifier SVM surpasse le classifier KNN en termes de GAR et de taux de fausse acceptation (False accepted rate : FAR). En conclusion, les deux tailles de filtres utilisées sont suffisantes pour obtenir une bonne précision, mais ceux basés sur le classifier SVM permettent d'atteindre efficacement le degré de sécurité souhaité (contrôle d'accès hautement sécurisé).

✍ **Système protégé:** Dans cette partie et afin d'évaluer sérieusement le système biométrique révocable proposé, deux points principaux liés à son comportement doivent être examinés.

i) Les scores trouvés par le système biométrique basé sur S-BSIF devraient présenter des distributions clients et imposteurs presque similaires à celles présentées par le système biométrique basé sur BSIF.

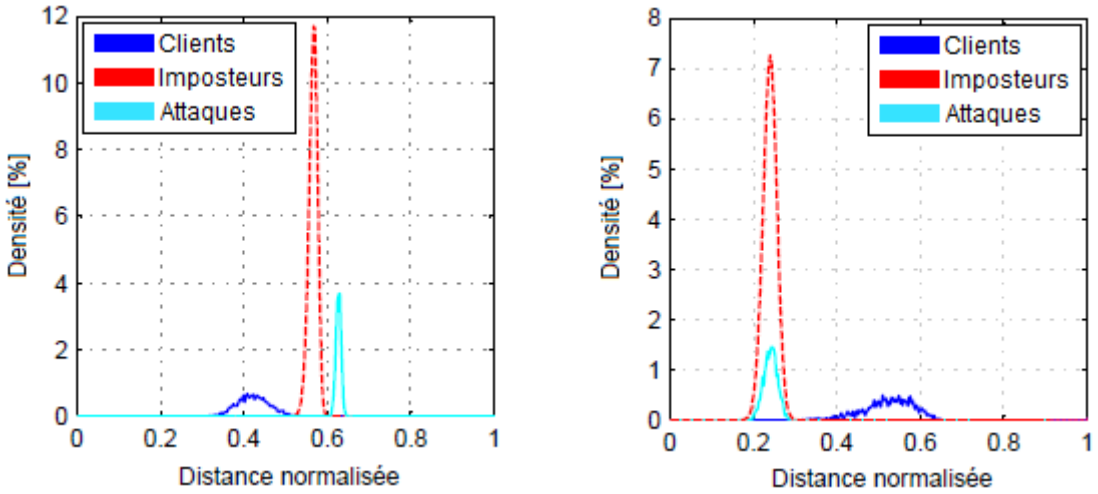
ii) Un changement soudain des scores des clients à la même position que les scores des imposteurs lors de l'utilisation d'une fausse clé de sécurité (tentative d'attaque). Le meilleur cas est lorsque tous les scores d'attaque sont inférieurs (SVM) ou supérieurs (KNN) au seuil de sécurité (T_o).

Pour le premier point, nous avons tracé les performances de S-BSIF avec clé correcte et S-BSIF avec clé incorrecte pour les deux tailles de filtre (15×15 et 17×17) afin de voir le changement qui peut se produire dans le comportement de BSIF lorsque la couche de sécurité ou transformation est intégrée (voir Fig. III.9 et Fig. III.10 pour les tailles de filtre 15×15 et 17×17, respectivement). A partir de ces figures, on peut clairement voir que le comportement général du système BSIF après l'intégration de cette n'a pas changé.



(a) *(b)*

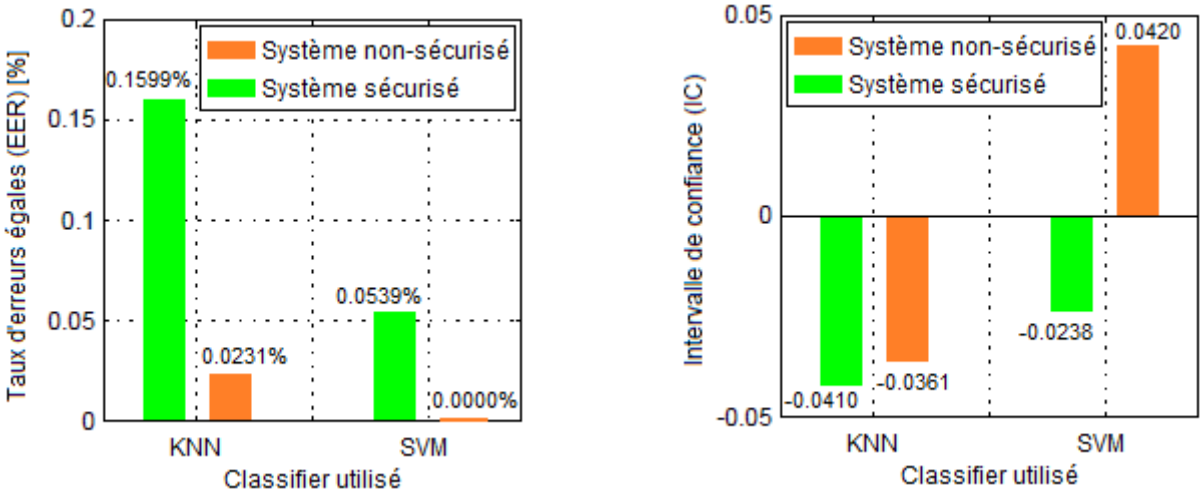
Fig. III.9. Comparaison des performances des systèmes protégés avec correcte clé et systèmes protégés avec incorrecte clé (5 filtres de 15×15). *(a)* Système basé sur le classifier KNN et *(b)* Système basé sur le classifier KNN.



(a) *(b)*

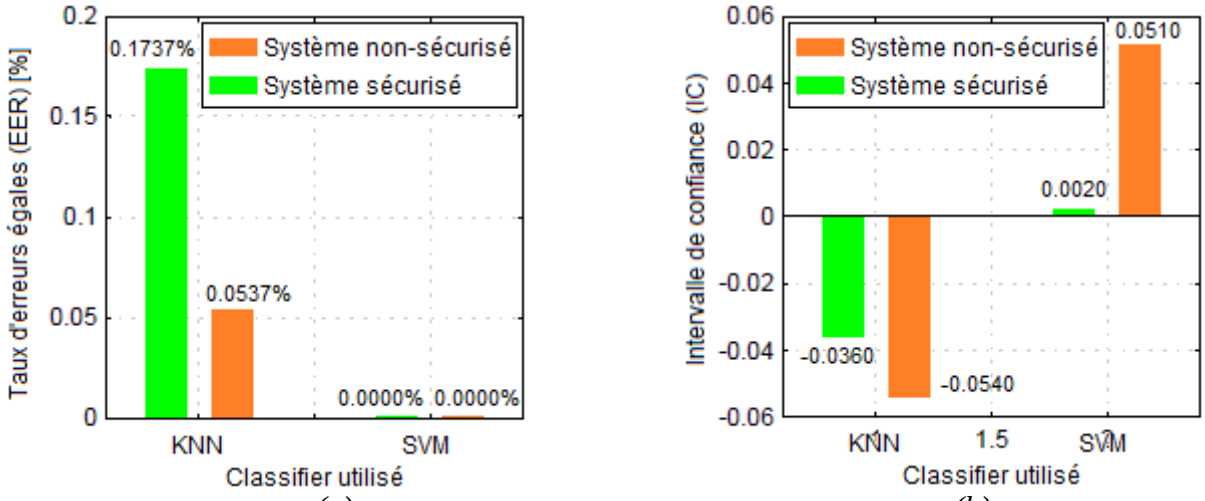
Fig. III.10. Comparaison des performances des systèmes protégés avec correcte clé et systèmes protégés avec incorrecte clé (5 filtres de 17×17). *(a)* Système basé sur le classifier KNN et *(b)* Système basé sur le classifier KNN.

Afin d'examiner le comportement du système lors de l'intégration de la couche de sécurité, nous avons calculé la précision du système dans les deux cas (15×15 et 17×17 avec KNN et SVM) et l'avons comparé au système non protégé et les résultats sont illustré dans les Fig. III.11 et Fig. III.12 pour les tailles de filtre 15×15 et 17×17, respectivement. Les résultats expérimentaux présentés dans toutes ces figures montrent que les performances du système biométrique sont généralement dégradées, ce qui est très normal car le template biométrique a été soumis à un processus de transformation.



(a) *(b)*

Fig. III.11. Comparaison des performances des systèmes non-protégés et systèmes protégés avec correcte clé (5 filtres de 15×15). *(a)* Taux d'erreurs égales (EER) et *(b)* Intervalle de confiance (IC)



(a) *(b)*

Fig. III.12. Comparaison des performances des systèmes non-protégés et systèmes protégés avec correcte clé (5 filtres de 17×17). *(a)* Taux d'erreurs égales (EER) et *(b)* Intervalle de confiance (IC)

Heureusement, le classifier SVM a maintenu son efficacité avec une erreur nulle dans le cas de la taille de filtre 17x17, mais l'intervalle de confiance s'est détérioré jusqu'à une très petite valeur de 0,0020. Dans le tableau 2, nous montrons les performances du système dans les cas étudiés (tailles de filtre 15×15 et 17×17 avec le classifier KNN et SVM).

Tableau 2 : Moyen de protection de Template biométrique

Taille de Filtre	**15x15**		**17X17**	
Classifier	**EER**	T_o	**EER**	T_o
KNN	0.1599	0.5386	0.1737	0.5306
SVM	0.0539	0.2909	**0.0000**	**0.3180**

Dans le deuxième point, nous cherchons à examiner le comportement de S-BSIF lors d'une attaque. Ainsi, dans nos tests, tous les utilisateurs sont enregistrés dans la base de données par $\mathcal{K}_{T1}$ et dans le test d'identification nous utilisons d'autres clés ($\mathcal{K}_{T2}$). Ainsi, pour voir les performances des systèmes d'identification (en mode ensemble ouvert) vis-à-vis des attaques, sur la Fig. III.9 et la Fig. III.10, nous illustrons les résultats des cas examinés. Dans ces figures, il est clair que tous les scores d'attaque sont complètement décalés en dessous/dessus du seuil de sécurité, ce qui reflète l'efficacité et la robustesse de notre système contre toute attaque éventuelle. Enfin, il convient de mentionner que le processus de cryptage n'affecte pas les performances du système biométrique, et donc le système fonctionne avec les mêmes performances, que le template soit crypté ou non.

☑ **Analyse de sécurité:** L'objectif principal de notre système est de protéger les templates biométriques, dans cette partie nous effectuerons une analyse de sécurité pour tester la robustesse de cette méthode face aux attaques potentielles. En règle générale, pour garantir la sécurité, deux points de la conception du système doivent être vérifiés, à savoir ***i)*** L'impossibilité de trouver des templates biométriques à travers une recherche exhaustive, donc l'espace de clés doit être très grande et ***ii)*** Un petit changement dans la clé sécrète produit des templates biométriques complètement différents.

Tout d'abord, avant de commencer à analyser la sécurité, il convient de noter que notre système biométrique révocable fonctionne avec deux systèmes chaotiques principaux ($\mathcal{L}_1 \; et \; \mathcal{L}_2$) et ℓ systèmes chaotiques auxiliaires ($\mathcal{T}_i|_{i=1}^{\ell}$). En général, les paramètres qui contrôlent la sécurité de notre système sont les états initiaux de $\mathcal{L}_1 \; et \; \mathcal{L}_2$ ainsi que les paramètres de contrôle de $\mathcal{T}_i \; |_{i=1}^{\xi}$.

✍ **Analyse de l'espace clé : L**'espace de tentative d'attaque est calculé en utilisant toutes les erreurs absolues moyennes entre deux séquences générées par deux clés secrètes voisins [RR]. L'erreur absolue moyenne $\varepsilon_\ell|_{\ell=\{x,u\}}$ pour le système chaotique est définie comme suit :

$$\varepsilon_\ell(\mathcal{S}, \tilde{\mathcal{S}}) = \frac{1}{\ell}\sum_{j=1}^{\ell}\left|\mathcal{S}(j) - \tilde{\mathcal{S}}(j)\right| \qquad (34)$$

Dans notre travail, nous avons utilisé deux systèmes chaotiques principaux ($\mathcal{R}_1$ pour transformation et R_2 pour déguisement), pour cela, nous allons calculer séparément l'espace des clés secrètes pour chaque système. Pour les deux systèmes chaotiques, nous utilisons les conditions suivantes : La longueur des séquences (SQ) est égal à 300 et les états initiaux de chaque paramètre ($\varrho_0 \equiv \{x_0, y_0, z_0\}$) sont définis à 0,1. Après simulation, les résultats suivants ont été obtenus :

$$(S_x, S_y, S_z) = (0.1750 \cdot 10^{18}, 0.2230 \cdot 10^{17}, 0.3110 \cdot 10^{18}) \quad (35)$$

L'espace total des clés secrètes est alors égal à :

$$S_r(R_1) \simeq S_r(R_1) = S_x \cdot S_y \cdot S_z = 0{,}129 \cdot 10^{52} \quad (36)$$

Pour ℓ systèmes chaotiques auxiliaires ($\mathcal{T}_i|_{i=1}^{\ell}$), on $S_u = 0.2418 \cdot 10^{16}$, et l'espace total des clés secrètes est alors égal à :

$$S^{\mathcal{T}} = \prod_{i=1}^{\ell} S_u = (0.2418)^{\ell} \cdot 10^{16\ell} \quad (37)$$

$$\ell = 5 \Rightarrow S^{\mathcal{T}} = (0.2418)^5 \cdot 10^{16\times 5} = 0.8266 \cdot 10^{77} \quad (38)$$

Nous avons calculé l'espace total des clés secrètes du système sous toutes les configurations possibles, et les résultats obtenus sont :

Transformation : $S_t = 0{,}129 \cdot 10^{52} \cdot 0.8266 \cdot 10^{77} = 0.1066 \cdot 10^{129}$

Déguisement: $S_d = 0{,}129 \cdot 10^{52}$

Hybride : $S_h = 0.1066 \cdot 10^{152} \cdot 0{,}129 \cdot 10^{52} = 0.1375 \cdot 10^{181}$

✍ **Sensibilité des clés:** Dans cette partie, nous avons examiné le vecteur de caractéristique résultant de plusieurs clés secrètes les plus proches pour tester la sensibilité de notre système à une légère variation de clé. Par conséquent, nous avons utilisé trois clés différentes : une clé correcte (K_c) et deux clés incorrectes plus proches de la clé correcte par $d_x = 10^{-16}$ ($\widetilde{K}_c^1$) et $d_u = 10^{-16}$ ($\tilde{k}_c^2$). Pour examiner les vecteurs de caractéristiques obtenus, nous avons calculé la corrélation entre ces vecteurs, qui est définie comme suit:

$$\rho_c[\%] = 100 \cdot \frac{C_{ij}}{\sigma_i \sigma_j} \quad (39)$$

Où C_{ij} est la covariance entre les vecteurs de caractéristiques $\mathcal{V}_i$ et $\mathcal{V}_j$, qui ont des écarts-types de σ_i et σ_j. De plus, pour une comparaison équitable, nous avons sélectionné aléatoirement deux personnes différentes (i et j) dans la base de données. Après avoir extrait le vecteur de caractéristique de la première personne (i) en utilisant la bonne clé, nous avons extrait les vecteurs de caractéristiques des deux personnes (i et j) en utilisant toutes les clés, puis nous avons calculé la corrélation entre tous les vecteurs de caractéristiques obtenus et les résultats obtenus sont présentés dans le tableau 3.

Tableau 3 : Corrélation entre les vecteurs caractéristiques produits par deux personnes

		Personne i			Personne j		
		$\mathcal{K}_c$	$\widetilde{\mathcal{K}}_c^1$	$\widetilde{\mathcal{K}}_c^2$	$\mathcal{K}_c$	$\widetilde{\mathcal{K}}_c^1$	$\widetilde{\mathcal{K}}_c^2$
Personne i	$\mathcal{K}_c$	100.00	3. 820	4.510	26.801	2.666	3.012

De ce tableau, on peut clairement extraire deux remarques importantes: Premièrement, l'utilisation de la même clé (clé secrète correcte) donne une corrélation totale pour une même personne, cette corrélation devient un peu considérable pour deux personnes différentes du fait de la similitude des traits biométriques de l'empreinte pour les deux personnes, mais bien sûr, le système biométrique capable de différencier ces deux templates. Deuxièmement, une légère modification d'un paramètre du système chaotique provoque une divergence notable entre les templates soit pour la même personne, soit pour deux personnes.

III.4. Conclusion

L'identification biométrique s'est avérée supérieure aux moyens traditionnels d'authentification. Malheureusement, ces systèmes sont vulnérables à une variété d'attaques, dont peut-être la plus grave est l'attaque du template biométrique stocké ou transmis, ce qui rend la protection de ce template plus importante dans la conception des systèmes biométriques. Ce travail suggère donc une méthode d'extraction de caractéristiques efficace qui peut fournir un template biométrique précis et révocable. Dans ce contexte, nous testons notre système proposé en utilisant deux classifiers. Les tests dans ce chapitre comprenaient la précision du système biométrique et le niveau de sécurité. En validant le système sur une base de données de 300 personnes, nous avons dégagé une amélioration considérable du taux d'identification (100%) avec notre méthode d’extraction des caractéristiques (S-BSIF). La méthode proposée a également montré un niveau de sécurité élevé (protection des templates) qui dépasse en réalité 10^{180}.

Conclusion

Les performances des systèmes de reconnaissance de formes sont toujours liées à la méthode d'extraction des caractéristiques. En fait, le système biométrique représente l'un des systèmes les plus importants dans le domaine de la reconnaissance des formes, dont l'efficacité peut être jugée par deux critères principaux, à savoir sa précision dans l'identification des personnes et son niveau de sécurité. Ainsi, avec une recherche bibliographique dans ce domaine, on constate que les travaux les plus récents portent sur ces deux critères principaux. La tendance générale de la recherche sur la précision des systèmes est axée sur les techniques d'apprentissage en profondeur, tandis que pour la sécurité des systèmes biométriques, les techniques de transformation de gabarit sont attirées l'attention des chercheurs en raison de leur haute sécurité par rapport à celles basée sur des techniques de cryptage. Dans ces techniques, la récupération illégale de la clé cryptographique peut conduire à la perte du gabarit biométrique une fois pour toutes, et donc compromettre la vie privée de la personne. Dans ce travail, nous avons reconstruit la méthode d'extraction de caractéristiques basée sur le deep learning (BSIF) pour pouvoir extraire un gabarit précis et révocable. Nous avons donc ajouté deux couches à cette méthode, une pour la transformation des gabarits et l'autre pour le cryptage des gabarits affin d'améliorer sa protection. Notre méthode repose sur des systèmes chaotiques pour produire les éléments de transformation en raison de son extrême sensibilité aux conditions initiales. Ces systèmes sont récemment révélés tries efficaces dans les systèmes de sécurité de l'information.

Les expériences ont été réalisées sur une base de données moyenne contenant 300 personnes représentées par des images d'empreintes palmaires multispectrales

De plus, pour la classification, nous avons utilisé deux classifieurs célèbres, à savoir KNN et SVM. Les résultats expérimentaux ont montré un taux d'identification élevé, qui peut également être amélioré en augmentant le nombre de stages de notre méthode. Les travaux futurs de cette étude se concentreront sur l'utilisation d'autres techniques d'apprentissage en profondeur comme DCTNet et ICANet et leur utilisation potentielle dans l'Internet des objets (IoT) ainsi que dans les applications mobiles basées sur le Cloud.

Annexe A

Evaluation des performances

L'évaluation des performances d'un système est une phase importante dans le processus de sa conception et de sa mise en œuvre dans la mesure où elle permet de savoir si le système est suffisamment performant pour l'application visée. Elle permet aussi de comparer les systèmes entre eux. Cette performance peut se mesurer principalement à l'aide de trois critères [36]: sa *précision*, son *efficacité* (vitesse d'exécution) et le *volume* de données qui doit être stocké pour chaque personne.

A.1 Mesures des taux d'erreur

Les erreurs de classification correspondent aux erreurs de décision des systèmes. Ces erreurs de décision sont de deux types [36]:

☑ **Taux de Fausses Acceptations** (*FAR*: False Acceptance Rate) : si le système déclare l'individu comme étant le client alors que c'est un imposteur. Il est égal au nombre de fausses acceptations divisé par le nombre de tests imposteur dans la base des données.

$$FAR = \frac{nombre\ de\ faux\ accepter}{nombre\ de\ imposteres} \qquad (1)$$

☑ **Taux de Faux Rejets** (*FRR* : False Rejection Rate) : si le système rejette l'individu alors que c'est le client. Il est égal au nombre de faux rejets divisé par le nombre de tests client dans la base des données.

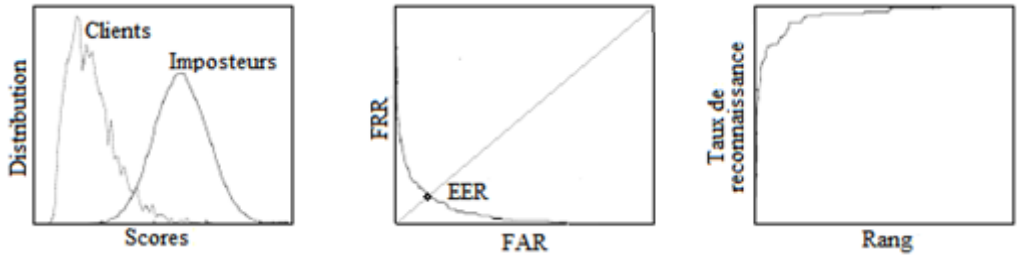
$$FRR = \frac{nombre\ de\ Faux\ rejet}{nombre\ de\ client} \qquad (2)$$

☑ **Taux des clients acceptés** (*GAR* : Genuine Acceptance Rate**) :** C'est le taux des personnes clients autorisées qui sont acceptées par le système biométrique, ce taux est important car elle représente le sucées de système. Il est exprimé par la relation suivant :

$$GAR = 1 - FRR \qquad (3)$$

A.2 Courbes de performance

Les courbes de performances permettent de représenter les performances pour toutes les valeurs du seuil sans fixer un seuil a priori [37]. Par exemple on peut représenter l'évolution des deux taux d'erreurs (*FAR* et *FRR*) lorsque le seuil varie pour les distributions de scores Client et Imposteur (cette distribution est représentée sur la Fig. III.1. *(a)).* Comme les taux d'erreurs *FAR* et *FRR* dépendent tous les deux du même seuil de décision, on peut également représenter sur une courbe la variation du *FRR* en fonction de *FAR* lorsque le seuil varie. Ces courbes s'appellent des courbes *ROC* (Receiver Operating Characteristic), représentées sur la Fig. III. 1. *(b).* Touts ces courbes concernant les deux modes des fonctionnements (vérification et identification ensemble ouvert). Dans le cas de l'identification ensemble fermé, la performance du système est représentée par le *CMC* (Cumulative Match Curve) représentés sur la Fig. III. 1. *(c).*



(a) *(b)* *(c)*

Fig.A.1 : Courbes de performance. *(a)* distributions des scores, *(c)* courbe *ROC* et *(b)* courbe *CMC*.

A.3 Point de fonctionnement

Le point de fonctionnement qui définit le choix du seuil dans le module de décision dépend de l'application visée [38]. En général lorsqu'il n'y a pas d'application définie mais qu'il s'agit d'un test de performance sur une base de données préenregistrée, on utilise le plus souvent l'*EER* (Equal Error Rate) (c'est-à-dire les deux taux d'erreurs égaux) car c'est un point de fonctionnement assez neutre qui ne favorise aucun des deux types d'erreurs. Le seuil du point *EER* correspond au seuil pour lequel les deux taux d'erreurs, *FAR* et *FRR*, sont égaux, il correspondant à l'intersection des deux courbes sur la Fig. III.1. *(b).*

Annexe B

Prétraitement

Dans les deux sous-systèmes (basé sur la TCD-2D et basé sur la TFD-2D), une tache de prétraitements (Extraction de la région d'intérêt (ROI : Region Of Interest)) permettant de préparer l'image originale à la phase de l'extraction des caractéristiques. La méthode appliquée dans notre système est basée sur l'algorithme décrit dans [38].

B.1 Filtrage : dans cette étape on applique un filtre passe bas (Gaussien) a l'image original pour faire le lissage de l'image, le but du filtrage est de réduire le bruit (voir **figure B.1**).

Figure B.1 : Image originale filtrée

B.2 Seuillage : Un seuil T_P est appliqué, pour convertir l'image original à une image binaire, cette image et nécessaire pour l'application de l'algorithme (bug flowing) (voir **figure B.2**).

Figure B.2 : Image binaire

B.3 Points des références: Obtenir le contour extérieur de l'image binaire et les deux points des références F_1 et F_2. L'algorithme utilisé pour l'extraction de contour extérieur est l'algorithme de *bug flowing*. Les deux points F_1 et F_2 sont nécessaires pour localiser la région d'intérêt ROI (voir **figure B.3**).

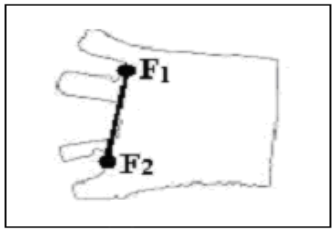


Figure B.3 : Contour extérieur

B.4 Angle d'orientation : Calculer l'angle entre le segment F_1F_2 et l'axe verticale, ensuite tourner l'image par l'angle correspondant pour que le segment F_1F_2 soit perpendiculaire (Voir la **figure B.4**).

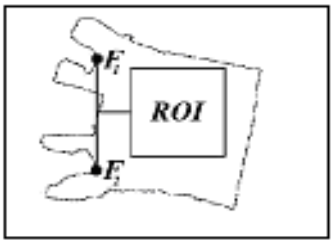


Figure B.4 : Image tourné

B.5 Rotation : Tourner l'image (originale) avec l'angle calculé précédemment puis localiser la région d'intérêt (voir **figure B.5**).

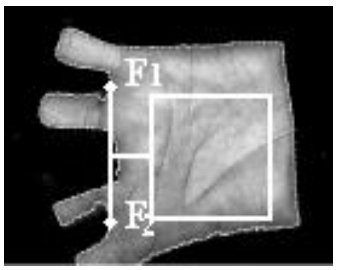


Figure B.5 : Sélection de la région d'intérêt

B.6 Extraction : Extraction de la région d'intérêt. La région d'intérêt (ROI) à une dimension fixe (128 x 128 pixels), de sorte que toutes les régions seront conformes à une même dimension (voir **figure B.6**).

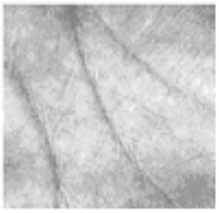


Figure B.6 : Région d'intérêt ROI

Annexe C

Systèmes chaotiques

☑ **Systèmes chaotiques :** Ces dernières années, le comportement dynamique des systèmes non linéaires a suscité un grand intérêt pratique dans de nombreuses applications en raison de leur simplicité, complexité et richesse [39]. Les systèmes chaotiques sont parmi les plus importants de ces systèmes, qui se caractérisent par leur extrême sensibilité aux conditions initiales, leur périodicité, leur comportement pseudo-aléatoire et leur grande complexité. En effet, dans un système chaotique, la sensibilité aux conditions initiales est sans aucun doute la caractéristique essentielle d'un comportement chaotique dont l'évolution est imprévisible sur le long terme. Il est donc sensible à une très faible perturbation de la condition initiale (état initial). Même si les points de départ sont presque identiques, les trajectoires se séparent rapidement.

Un système chaotique en temps discret est défini par l'équation suivante:

$$x_{n+1} = \Gamma(x_n)\,, \quad n = 0,1,2\ldots \qquad (9)$$

Où $x_n \in R^n$ est appelés état, et Γ trace l'état suivant x_{n+1}. A partir d'un état initial x_0, l'application répétée de cette fonction (Γ) provoque une séquence de N points $(\{x_n\}_{n=0}^{N})$ appelée orbite du système à temps discret.

Sans aucun doute, ces systèmes ont été utilisés avec succès dans des applications de sécurité de l'information, pour la génération de clés secrètes dynamiques dans des algorithmes de cryptage, de stéganographie et de tatouage numérique. Les cartes chaotiques sont l'un des systèmes les plus simples à utiliser pour générer une séquence chaotique. Dans la littérature, plusieurs cartes chaotiques à une dimension (1-D), deux dimensions (2-D) et trois dimensions (3-D) sont proposées. Dans cette sous-section, nous décrirons brièvement quelques cartes chaotiques, telles que la logistique et le tente.

- **Cartes des tentes:** La carte de tente [40] est un système dynamique caractérisé par deux lignes simples, ce qui rend son analyse simple par rapport aux systèmes non linéaires. Son comportement peut être défini par l'équation récurrente suivante:

$$\begin{aligned} x_{n+1} &= \Gamma_t(x_n, u) \\ &= \mu \min(x_n, 1 - x_n), \quad \mu \epsilon [0,2], \quad x_n \epsilon [0,1] \end{aligned} \tag{11}$$

Où x_n est l'état du système pour n = 0, 1, 2, · · · et μ est le paramètre de contrôle. Heureusement, malgré la simplicité et la linéarité de cette équation, pour certains paramètres, ce système peut fournir des comportements très complexes et des phénomènes chaotiques. Cependant, en fonction des valeurs de μ et de la valeur initiale x_0, ce système présente des comportements très différents:

- μ *<1*: les états de Γ_t convergeront vers zéro, quelle que soit la valeur initiale (x_0);
- μ *= 1*: les états de Γ_t convergeront a chaque valeur de $0 \leq x \leq 0.5$, quelle que soit la valeur initiale (x_0);
- *1* $\leq \mu <$ $\sqrt{2}$*:* les états de Γ_t apparaissent périodiquement;
- $\sqrt{2}$: $\leq \mu <2$: les états de Γ_t deviennent un système chaotique avec une périodicité disparue;
- μ*> 2*: les états de Γ_t divergent presque pour toutes les valeurs initiales.

- **Carte Lorenz** : Les cartes de Lorenz, également appelées système dynamique de Lorenz ou oscillateur de Lorenz, est une modélisation simplifiée des phénomènes météorologiques basée sur la mécanique des fluides. La carte de Lorenz est un système dynamique tridimensionnel qui génère un comportement chaotique dans certaines conditions. Ce système est défini par les équations suivantes [41]:

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{pmatrix} = \Gamma_S \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \sigma(y - x) \\ \rho x - y - xz \\ xy - \beta z \end{pmatrix} \tag{12}$$

Dans ces équations σ, ρ, et β sont trois paramètres réels strictement positifs et les variables dynamiques x, y et z représentent l'état du système a tout moment. La carte de Lorenz est un système non périodique qui montre comment les différentes variables du système dynamique croissent au fil du temps dans une trajectoire non périodique. Nous fixons souvent σ = 10, β = 8/3 et ρ variable restante.

Bibliographies

[1] Son, B., Ahn, J.-H., Park, J.-h., Lee, Y.: Identification of Humans Using Robust Biometric Features, *Lecture Notes in Computer Science*, **2004**.

[2] A. Kumar, D. Wong, H. Shen, and A.Jain, : Personal verification using palmprint and hand geometry biometric, Audio and Video based biometric Person Authentification, LNCS 1688, **2003**.

[3] Cardinaux F, Sanderson C, Bengio S, : Face verification using adapted generative models , The 6th IEEE International Conference Automatic Face and Gesture Recognition-AFGR, Seoul, 2004.

[4] Julian Ashbourn, « Guide To Biometrics For Large-Scale Systems », Springer **2011**.

[5] C.Tisse, L.Martin, L. Torres and M. Robert, « Person identification technique using human iris recognition », Proc. Of Vision Interface, **2002**.

[6] Jain, A. K., Griess, F.D. and Connell, S.D, « On-line signature verification », *Pattern Recognition*, **2002**.

[7] Suman Senapati, Goutam Saha, « Speaker Identification by Joint Statistical Charactcterization in the Log-Gabor Wavelet Domain », *Inernational Journal of Intelligent Systems and Technologies*, winter, **2007**.

[8] R. Rak, Biometrics and identity of people: the forensic and commercial applications, BEN, Prague, **2008**. ISBN 978-80-247-2365-5.

[9] Fingerprint structure imaging based on an ultrasound camera, **2012**. http://www.optel.pl/article/english/article.htm

[10] K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. EURASIP Journal on Advances in Signal Processing, pages 1–17, **2008**.

[11] A. Jagadeesan and K. Duraiswamy, "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris," in International Journal of Computer Science and Information Security, **2010**.

[12] .R. Seshadri and T. Raghu Trivedi, "Efiicient Cryptographic Key Generation Using Biometrics," in Int.J.Comp.Tech.AppL.

[13] Lafkih M., Lacharme P., Rosenberger C., Mikram M., Ghouzali S., and Haziti M., “Vulnerabilities of Fuzzy Vault Schemes Using Biometric Data with Traces,” in Proceedings of IEEE International Wireless Communications and Mobile Computing Conference, Dubrovnik, pp. 822-827, **2015**.

[14] Menezes A. J., Van Oorschot P. C., and Vanstone S. A. \Handbook of Applied Cryptography", In: Boca Raton, FL : CRC Press, **1996**.

[15] Sujitha V. and Chitra D. \A Novel Technique for Multi Biometric Cryptosystem Using Fuzzy Vault", In: International Journal of Medical Systems, **2019**, vol. 43, no 112.

[16] Jindal A.K., Chalamala S., Jami S.K. \Face Template Protection using Deep Convolutional Neural Network", In : IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), **2018**.

[17] Karthik Nandakumar, Abhishek Nagar, and Anil K Jain. Hardening Fingerprint fuzzy vault using password. In Advances in biometrics, pages 927-937. Springer, **2007**.

[18] Ari Juels and Madhu Sudan. A fuzzy vault scheme. Designs, Codes and Cryptography, 38(2) :237-257, **2006**.

[19] Yi Cheng Feng, Pong C Yuen, and Anil K Jain. A hybrid approach for genera- ting secure and discriminating face template. IEEE Transactions on Information Forensics and Security, 5(1) :103-117, **2010**.

[20] Kaur M. and Sofat S., "Fuzzy Vault Template Protection For Multimodal Biometric system," in Proceedings of International Conference on Computing, Communication and Automation, Greater Noida, pp. 1131-1135, **2017**.

[21] Soutar C., Roberge D., Stoianov A., Gilroy R., Kumar B. V. Biometric encryption: enrollment and verification procedures. In Proceedings of SPIE, Optical Pattern Recognition IX 3386, PP. 2435, **1998**.

[22] Alam B., Jin Z., Yap W.S., Goi B.M. An alignment-free cancelable fingerprint template for bio-cryptosystems. J. Network. Computer. Appl., Vol. 115, PP. 20–32, **2018**.

[23] Sarkar A., Singh B.K., Cryptographic key generation from fingerprint templates. In Proceedings of the 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, India, 15–17 March, pp. 1–6, **2018**.

[24] Liu, E., Zhao, Q. Encrypted domain matching of fingerprint minutia cylinder-code (MCC) with I1minimization. Neuro computing, Vol. 259, pp. 3–13, **2017**.

[25] Cappelli, R., Ferrara, M., Maltoni, D. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. IEEE Trans. Pattern Anal. Mach. Intell., Vol. 32, PP. 2128–2141, **2010**.

[26] Xi, K.; Hu, J.; Han, F. An alignment free fingerprint fuzzy extractor using near-equivalent Dual Layer Structure Check (NeDLSC) algorithm. In Proceedings of the 6th IEEE Conference on Industrial Electronics and Applications (ICIEA), Beijing, China, 21–23 June, pp. 1040–1045, **2011**.

[27] Li, P., Yang, X., Cao, K., Tao, X.,Wang, R., Tian, J. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. J. Network. Computer. Appl. Vol. 33, PP. 207–220, **2010**.

[28] [R9] Lifang W., Xingsheng L., Songlong Y. and Peng X., A Novel key generation cryptosystem based on face features, IEEE 10th IC on Signal Processing, pp:1675-1678, **2010**.

[29] Bringer, J., Chabanne, H., Cohen, G., Kindarji, B. & Zémor, G. Theoretical and practical boundaries of binary secure sketches, IEEE Transactions on Information Forensics and Security Vol. 3: PP. 673–683, **2008**.

[30] Yi C. F., Pong C. Y., A Hybrid Approach for Generating Secure and Discriminating Face Template, In IEEE transactions on information Forensics and security, Vol. 5, N°. 1, **2010**.

[31] Griffin, L.D., Lillholm, M., Crosier, M., van Sande, J.: Basic image features (bifs) arising from approximate symmetry type. In: International Conference on Scale Space and Variational Methods in Computer Vision. pp. 343{355. Springer, **2009**

[32] Kannala, J.; Rahtu, E. Bsif: Binarized statistical image features. In Proceedings of the 2012 21st International Conference on Pattern Recognition (ICPR), Tsukuba, Japan, 11–15 November **2012**; pp. 1363–1366.

[33] N. Dalal and B. Triggs. Histograms of oriented gradients for human detection. In IEEE Computer Society Conference on Computer Vision and Pattern Recognition, volume 1, pages 886–893, June **2005**.

[34] Tran K. D., Quynh C. T., Thu T. B. L., Hai T., Cancellable fuzzy vault with periodic transformation for biometric template protection, IET biometrics journal, Volume5, Issue3, September 2016

[35] The Hong Kong Polytechnic University, PolyU FKP Database, http ://www.comp.polyu.edu.hk/sbiometrics/FKP/polyudb.htm.

[36] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, \Handbook of Fingerprint Recognition", Second Edition, Springer, **2009**.

[37] V. Nalwa. "Automatic on-line signature verification ", Proceedings of the IEEE, Vol. 85(2), pp. 215-239, 1997.

[38] Meraoumia, A. Modèle de Markov cachée applique à la multi-biométrie, Thèse de doctorat en science, Université des sciences et de la technologie Houari Boumediene **2014**.

[39] Nada Hamad, Mizanur Rahman, Saiful Islam.. \Novel remote authentication pro- tocol using heart-signals with chaos cryptography", In : International Conference on Informatics, Health & Technology (ICIHT), **2017**, Riyadh, Saudi Arabia, pp. 1-7.

[40] Xiaolin Wu, Bin Zhu, Yutong Hu, Yamei Ran. \A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps", In : EEE Access, Vol. 5, pp. 6429-6436.

[41] Chong Fu, Wen-Jing Li, Zhao-Yu Meng, Tao Wang, PeiXuan Li. \A Symmetric Image Encryption Scheme Using Chaotic Baker Map and Lorenz System", In : Ninth International Conference on Computational Intelligence and Security, **2013**, Leshan, China.