République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Larbi Tébessi –Tébessa-

Faculté des Science Exactes et des Sciences de la Nature et de la Vie

Département : Mathématiques et Informatique

MEMOIRE DE MASTER

Domaine : Mathématiques et informatique

Filière: Informatique

Option: Réseaux et sécurité informatique

Thème :

# Identification à distance basée sur les crypto systèmes biométriques

Présenté par :

Boudraa Mohammed Lazhar

Devant le jury

| | | | |
|---|---|---|---|
| Hakim Bendjenna | Prof | Université de Tébessa | Président |
| Fatima Bouakkaz | MAA | Université de Tébessa | Examinateur |
| Lakhdar Laimeche | MCA | Université de Tébessa | Encadreur |
| Abdallah Meraoumia | MCA | Université de Tébessa | Co-Encadreur |

Date de soutenance: 2019 - 2020

Note: Mention:

*À ma très chére mère*

*Quoi que he fasse ou que je dise, je ne saurai point te remercier comme il se doit. Ton affection me couvre, ta bienveillance me guide et ta présence à mes côtés a toujours été ma source de force pour affronter les différents obstacles.*

*À la mémoire de mon père*

*Ce travail est dédié à mon père, décédé trop tôt, qui m'a toujours poussé et motivé dans mes études.*
*J'espère que, du monde qui est sien maintenant, il apprécie cet humble geste comme preuve de reconnaissance de la part d'un fils qui a toujours prié pour la paix à son âme.*

*À toute ma famille et mes amis pour leur soutien tout au long de mon parcours universitaire.*

*Merci d'être toujours là pour moi*

BOUDRAA M. L.

# *Remerciements*

*En préambule à ce modeste mémoire nous remerciant « ALLAH » qui nous aide et nous avoir donné le courage, la volonté et la patience d'aller jusqu'au bout de nos rêves.*

*Nos remerciements et nos profondes gratitudes vont à mes encadrants M.**Lakhdar LAIMECHE** et M.**Abdallah MERAOUMIA**, pour leur disponibilité et surtout leurs judicieux conseils, leur écoute et leur soutien tout au long de la réalisation de notre travail.*

*Plus vifs remerciements s'adressent également aux membres de jury Mr BENDJENNA Hakim et Mme BOUAKKAZ Fatima qui nous font l'honneur d'accepter de juger notre travail et pour leur précieux temps accordé à l'étude de notre mémoire.*

*Nous souhaitons adresser nos remerciements les plus sincères aux professeurs et enseignants de département Mathématiques et Informatique qui ont contribués par leur savoir et leurs encouragements le long de nos parcours.*

*Enfin, nous adressons nos plus sincères remerciements à nos Ami(e)s et nos collègues et tous ceux qui ont contribués de près ou de loin.*

# ملخص

إن تطور تكنولوجيا المعلومات دفع الباحثين إلى إنشاء العديد من الحلول الأمنية الجديدة للتطبيقات الإلكترونية الآمنة، وخاصة على الإنترنت. من بينها، يفضل مسؤولو الأمن أنظمة المصادقة لتحديد هوية المستخدم. في الواقع ، أثبتت المصادقة البيومترية أنها متفوقة في كثير من النواحي مقارنة بوسائل المصادقة التقليدية. لسوء الحظ ، فإن هذه الأنظمة عرضة لمجموعة متنوعة من الهجمات ، وربما يكون أخطرها الهجوم على النموذج المخزن أو المنقول ، مما يجعل أمان هذا النموذج أكثر أهمية في تصميم أنظمة القياسات الحيوية. لذلك، يقترح هذا البحث طريقة فعالة لاستخراج الميزات التي يمكن أن توفر ميزة بيومترية عميقة وقابلة للإلغاء. في هذه الدراسة ، يتم الجمع بين التعلم العميق والأنظمة الفوضوية لاستخراج ميزات بصمة الكف \ عروق الكف القابلة للإلغاء.

**الكلمات المفتاحية** : القياسات الحيوية القابلة للإلغاء ، التعلم العميق ، شبكة تحويل جيب التمام المنفصلة ، الخرائط الفوضوية ، بصمة الكف، عروق الكف.

# Résumé

L'évolution des technologies de l'information a incité les chercheurs de créer une multitude de nouvelles solutions de sécurité pour des applications électroniques sécurisées, notamment sur Internet. Parmi eux, les responsables de la sécurité préfèrent les systèmes d'authentification pour l'identité des utilisateurs. En effet, l'authentification biométrique s'est avérée supérieure à bien des égards par rapport aux moyens d'authentification traditionnels. Malheureusement, ces systèmes sont vulnérables à une variété d'attaques, dont la plus grave est peut-être l'attaque du gabarit stocké ou transmis, ce qui rend la sécurité de ce gabarit plus importante dans la conception des systèmes biométriques. Cette recherche suggère donc une méthode d'extraction de caractéristiques efficace qui peut fournir une caractéristique biométrique profonde et révocable. Dans cette étude, l'apprentissage en profondeur DCTNet est combiné avec des systèmes chaotiques pour extraire des caractéristiques révocables d'empreinte palmaire / veines de palme.

**Mots clés :** biométrie révocable, caractéristiques profondes, DCTNet, cartes chaotiques, empreinte palmaire, veines de palme.

# Abstract

The proliferation of information technology has prompted researchers to create a multitude of new security solutions for secure electronic applications, especially on the Internet. Among them, security officials prefer authentication systems for user's identity identification. Indeed, biometric authentication has proved to be superior in many respects compared to the traditional authentication means. Unfortunately, these systems are vulnerable to a variety of attacks, the most serious of which is perhaps the attack on the stored or transmitted template, which makes the safety of this template more important in the design of the biometric systems. This research, therefore, suggests an effective feature extraction method that can provide a deep and cancelable biometric feature. In this study, DCTNet deep learning is combined with chaotic systems to extract revocable palmprint/palm-vein features.

**Keywords :** Cancelable Biometric, Deep feature DCTNet, Chaotic maps, Palmprint, Palm-vein.

# Abréviation

ADN : Acide Désoxyribo Nucléique

CMC : Cumulative Match Curve

DCT : Discrete Cosine Transform

EER : Equal Error Rate

FA : Fausses Acceptations.

FAR : False Acceptance Rate

FR : Faux Rejet

FRR : False Rejection Rate

GAR : Gunnies Accept Rate

KNN : K- Nearest Neighbor

ROC : Receveur Operating Curve

ROR : Rank One Recognition

RPR : Rank of Perfect Recognition

SVM : Support Vector Machine

# Table des matières

# Table des figures

# Liste des tableaux

# Introduction Générale

La transformation numérique peut être définie comme une évolution par les activités de numérisation qui impactent tous les acteurs. Le boom numérique a permis de développer les différents outils, que ce soit par des moyens (ordinateurs, tablettes, objets connectés), des espaces (internet, cloud, site Web, réseaux sociaux), l'analyse des données (big data) ou sécurité (applications en ligne telles que le paiement électronique , le vote électronique et commerce électronique ) [2]. Par conséquent, l'intégration massive de ces outils a eu un impact majeur sur notre vie moderne à travers laquelle les anciennes activités ont été renforcées et de nouvelles activités ont été créées, ce qui a conduit au développement du mode de vie à tous les niveaux. Les conséquences de l'insécurité insuffisante dans ces applications ont été toujours parmi les préoccupations les plus importantes dans les organisations humaines, surtout s'ils concernent la vie privée des individus, y compris la publication des informations confidentielles telles que les coordonnées bancaires, codes confidentiels, etc. [1]. La sécurité des données personnelles est soumise aux obligations légales régies par la loi sur la protection des données. Aujourd'hui, il est généralement admis que la sécurité ne peut être pleinement et idéalement garantie, et donc souvent nécessite l'utilisation d'un ensemble de mesures pour réduire les risques de compromettre des systèmes d'information [3].

Récemment, même les pays les plus faibles ont adopté la transformation numérique dans de nombreux secteurs comme une solution pour le développement de leur économie, industrie, santé, services, etc. En fait, il n'y a pas d'autre solution que d'adopter un tel progrès technologique pour suivre le rythme des pays développés. Dans le monde, de nombreux réseaux de communications électroniques, publics et privés, se sont réunis dans un grand consortium international de réseaux, connu sous le nom d'Internet. Ce réseau est actuellement le plus populaire, le plus accessible et transporte plus d'informations parmi tous les autres réseaux informatiques publics ou privés. Étant donné que la plupart des données de ce réseau sont vulnérables au vol ou à la fraude, l'aspect fondamental et réel de la majorité des services en ligne est lié à la confiance des utilisateurs, qui est un élément très nécessaire. La sécurité de l'information est donc un élément clé de cette confiance. Pour cette raison, les fondateurs de services étaient intéressés par des méthodes qui sécurisent les informations, en introduisant de nouvelles

approches, qui utilisent des méthodes biométriques pour l'authentification d'identité, plutôt que des méthodes traditionnelles basées sur les connaissances (mots de passe) ou basées sur des jetons (cartes d'identité) [4] .

Avec le développement rapide d'Internet et des appareils mobiles, une variété de dispositifs d'authentification pour vérifier l'identité des utilisateurs sont utilisés aujourd'hui pour le contrôle d'accès logique / physique. Les méthodes d'authentification des utilisateurs les plus courantes sont basées sur des mots de passe, un paradigme peu coûteux et familier pris en charge par la plupart des systèmes d'exploitation. Cependant, lorsque les utilisateurs ont de plus en plus de comptes, la gestion des mots de passe devient pratiquement difficile, car il est normalement difficile de mémoriser différents mots de passe pour différents accès au système, en particulier ceux avec différents niveaux de haute sécurité. De plus, les mots de passe ne sont pas souvent suffisamment protégés contre les pirates [5]. Afin de résoudre ce problème, la biométrie a été utilisée pour améliorer ou renforcer les techniques d'authentification par mot de passe existantes. La biométrie est déjà reconnue comme un élément essentiel du processus d'authentification de l'identité des utilisateurs, c'est pourquoi elle est effectivement utilisée pour accroître la confiance dans la capacité d'authentification du système. Le système d'authentification biométrique est défini comme la reconnaissance automatisée des individus sur la base de leurs caractéristiques morphologiques ou comportementales [6]. Le visage, les empreintes digitales, l'iris sont les données biométriques les plus couramment utilisées en raison de leur caractère unique chez chaque individu. Cependant, la nature unique de la biométrie est également son défaut. Les données biométriques peuvent fournir un moyen d'identifier les personnes avec un haut degré de précision, mais une fois volées, rien ne permet de les sécuriser à nouveau. Étant donné que de nombreuses applications peuvent utiliser les mêmes données biométriques pour une personne, une fois les données biométriques volées dans une application, cela peut rendre différentes applications vulnérables aux attaques [7]. Malheureusement, les modalités biométriques comme le visage, les empreintes digitales, la voix, etc. sont déjà exposés et peuvent être volés à l'insu des personnes.

Pour ces raisons, un système biométrique sécurisé doit non seulement authentifier précisément l'utilisateur, mais il doit également stocker les gabarits biométriques de manière sécurisée. Contrairement aux codes PIN ou aux mots de passe, qui peuvent être modifiés s'ils sont compromis, les modalités biométriques d'une personne ne peuvent pas être modifiés en cas de vol [8]. Par conséquent, la protection du gabarit biométrique est le problème le plus important dans la conception d'un système biométrique sécurisé [9]. Pour surmonter le problème de la biométrie volée, les chercheurs ont développé plusieurs schémas de protection des gabarits biométriques, qui sont principalement di-

visés en deux catégories : les cryptosystèmes biométriques et la biométrie révocable [10]. Dans le cryptosystème biométrique, les données biométriques sont cryptées avant d'être stockées dans la base de données, et qui sont décryptées lors de l'authentification pour faire une comparaison. Alors que la biométrie révocable consiste à des distorsions intentionnelles et reproductibles des signaux biométriques qui fournissent une comparaison des gabarits biométriques dans le domaine transformé [11].

Les cryptosystèmes biométriques révèlent généralement une diminution significative de la sécurité du système, car si la clé de cryptage est volée, le gabarit biométrique d'origine sera volé, ce qui pose un problème majeur en raison du lien naturel du gabarit avec la personne [7]. Heureusement, dans la deuxième approche, même si le gabarit biométrique a été perdu ou compromis, il est difficile pour les intrus de reconstruire le gabarit d'origine à partir du gabarit transformé. De plus, si le gabarit biométrique est compromis, la version transformée peut simplement être modifiée pour créer une nouvelle variante de réinscription. Cependant, il n'est pas facile de concevoir une telle fonction en raison des caractéristiques limitantes du gabarit biométrique. Après une transformation irréversible des gabarits, les performances du système biométrique peuvent être dégradées en utilisant les nouvelles images des modèles [12]. Les travaux de recherche présentés dans ce mémoire s'inscrivent dans le cadre général de la protection de la confidentialité et de la vie privée des individus et plus particulièrement dans le cadre de la sécurité des gabarits biométriques sur des réseaux de communication numériques ouverts ou des supports de stockage. Concrètement, notre travail couvre plusieurs aspects transactionnels sur Internet et touche de près les concepts liés aux applications électroniques.

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 transformée DCT , sur lesquelles repose notre système proposé, sont détaillés. Ensuite, un nouveau système biométrique révocable est proposée. L'originalité de notre système réside dans la modification de la méthode d'extraction de

caractéristique profondes DCTNet. Notre méthode, appelée Security-Oriented Discrete Cosine Transform Network (S-DCTNet)), extrait des gabarits biométriques profonds et révocable pour garantir a la fois des performances élevées et une sécurité renforcée. Dans une deuxième étape, les résultats expérimentaux sont détaillés et discutés.
Enfin, Nous clôturons ce mémoire par une conclusion générale, ainsi que les perspectives visées.

# Chapitre 1

# Sécurité d'information et biométrie

## 1.1 Introduction

Au fil du temps, et avec le développement des applications et l'assistant d'Internet, l'authentification des individus devient de plus en plus importante dans diverses pratiques quotidiennes, et pour cela la présence de la sécurité doit être obligatoire.

À ce jour, les méthodes d'identification d'un individu dans un système sont basées sur ce que connait la personne comme un mot de passe, un code, ou sur ce que possède une personne comme un badge ou une carte d'identité, ces derniers posent un grand problème de sécurité car ils peuvent être facilement rompue. Donc pour toutes ses raisons, il est indispensable d'utiliser une nouvelle technologie d'authentification, c'est le cas des systèmes biométriques.

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.

## 1.2 Nécessité de la biométrie

La sécurité de l'information est l'une des préoccupations majeures de nos sociétés actuelles. Cette préoccupation est d'autant une partie intégrante de notre vie quotidienne et à la base des infrastructures économiques, sociales et institutionnelles. Elle est devenue une nécessité et sa vulnérabilité est un problème majeur. La nécessité de protéger la vie privée d'une part et la lutte contre les fraudes et les crimes d'autre part, placent au centre un dispositif sécuritaire pour de nombreux domaines d'application

comme par exemple le transport, le contrôle d'accès, la surveillance des frontières, le secteur bancaire, les services publics, etc. En effet, la reconnaissance de l'identité des personnes en utilisant la biométrie est l'un des moyens les plus efficaces par rapport aux méthodes de contrôle d'accès traditionnelles

Le Tableau 1.1 présente une comparaison entre les différents outils d'identification. Il est clair que la biométrie est une véritable alternative aux clés, badges et autres identifiants. Elle permet de vérifier que l'usager (la personne en question) est bien la personne qu'il prétend être.

| MÉTHODES | COPIER | VOLER | OUBLIER | PERDRE |
|---|---|---|---|---|
| CLÉ | ✓ | ✓ | ✓ | ✓ |
| BADGE | - | ✓ | ✓ | ✓ |
| CODE | ✓ | - | ✓ | - |
| BIOMÉTRIE | - | - | - | - |

TABLE 1.1 – Comparaison entre les différentes outils de sécurité.

## 1.3 Définition de la biométrie

La biométrie est la reconnaissance automatique d'une personne à l'aide de l'un ou plusieurs caractéristiques physiques, qui doivent être plus fiable et unique et aussi non falsifiable pour pouvoir représenter un et un seul individu.

Le terme biométrie vient du grec ancien *"bio"* = "vie" et *"métrique"* = "mesure". Bien que la technologie biométrique ait plusieurs utilisations, son objectif principal est de fournir une alternative plus sécurisée aux systèmes de contrôle d'accès traditionnels (les numéros d'identification (ID), les clefs) utilisés pour protéger les actifs personnels ou professionnels[13,18]. Les techniques biométriques permettent aussi de filtrer les accès aux applications utilisant des réseaux d'ordinateurs telle que : Internet, transactions financières, e-commerce, etc...[14].

Une modalité biométrique idéale devrait respecter les propriétés suivantes [15,18] :

- **Universalité** : chaque personne devrait posséder ces modalités.
- **Unicité** : deux personnes ne devrait être identique en termes de modalités biométriques.

- **Permanence (stabilité)** : les modalités doivent être invariantes dans le temps et une stabilité pour chaque personne.
- **Mesurabilité** : les modalités doivent être mesurées quantitativement et que l'obtention des modalités doit être facile.
- **Performance** : un système biométrique pratique doit avoir une précision acceptable et une vitesse de reconnaissance raisonnable vis-à-vise des ressources requises.
- **Acceptabilité** : Cela indique dans quelle mesure les gens sont disposés à accepter le système biométrique.
- **Contournement** : il s'agit de la difficulté à tromper le système par des techniques frauduleuses.

## 1.4 Intérêt biométrique

Plusieurs raisons peuvent motiver l'usage de la biométrie [16,17] :

*1)* **Haute sécurité** : combiné à d'autres technologies comme le cryptage ou la carte à puce, certains systèmes rendent très compliquée toute tentative de fraude.

*2)* **Confort** : en remplaçant juste les méthodes traditionnelles, exemple un mot de passe, la biométrie permet de respecter les règles de base de la sécurité. Et quand ces règles sont respectées, la biométrie évite aux administrateurs d'avoir à répondre aux nombreuses demandes de changement de mot de passe.

*3)* **Sécurité/Psychologie** : Dans certains cas, particulièrement pour le commerce électronique, l'usager n'a pas confiance. Il est indispensable pour les acteurs du commerce électronique de convaincre le consommateur de faire des transactions. Un moyen d'authentification biométrique pourrait faire changer le comportement des consommateurs.

Cette complémentarité permet d'imaginer des systèmes performants, intégrés et fortement dissuasifs. S'il est techniquement aisé de découvrir un mot de passe ou de se procurer de manière frauduleuse un badge d'accès ou une carte magnétique, il est presque impossible de modifier, voler ou copier une modalité physiologique ou comportementale humaine.

## 1.5 types de modalités

Il existe plusieurs modalités biométriques utilisées dans divers secteurs, on peut distinguer trois catégories[18] :

### 1.5.1 Modalités morphologiques (physiologiques)

Les modalités morphologiques sont basées sur les traits physiques de chaque individu dont les principaux sont :

**1) Empreinte digitale :** L'empreinte digitale [19] représente les différents types de traits d'un doigt, dont les principaux sont les arcs, les boucles et les tourbillons (voir figure 1.1). Les traits mineurs (ou minuties), quant à eux, sont formés par la position des extrémités et des nœuds des traces. Chaque doigt porte entre 50 et 200 traits mineurs, ce qui fournit un grand nombre de données pour l'extraction de caractéristiques.

FIGURE 1.1 – Empreinte digitale.

L'empreinte digitale est la modalité la plus utilisée dans de nombreux systèmes d'identification biométrique dont l'acquisition de cette modalité nécessite que l'utilisateur pose son doigt sur un capteur d'empreinte spécifique.

• **Avantages** : La technologie la plus éprouvée techniquement et la plus connue du grand public, petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones portables, PC), facile à mettre en œuvre, très discriminante, technique pas chère, peu vulnérable, grande précision et peuvant être installée dans divers milieux.

• **Inconvénients** : L'enregistrement se fait par contact, ce qui peut entraîner des réticences d'ordre psychologique ou hygiénique, besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur) et exige un environnement propre.

• **Applications** : Toutes les applications d'identification et de vérification peuvent utiliser les empreintes digitales. Par exemple, le contrôle d'accès physique (locaux,

machines) et le contrôle d'accès logique (systèmes d'information).

**2) Géométrie de la main :** Les techniques biométriques basées sur la géométrie de la main se basent sur la détermination des caractéristiques de la main : les dimensions des doigts, les caractéristiques des articulations de la paume et la forme de la main (voir figure 1.2). Les systèmes de reconnaissance de la géométrie de la main sont simples à utiliser. Dans une première étape, une personne doit poser sa main sur une platine, les doigts doivent être correctement placés. Une caméra à infrarouge prend alors une image sous deux angles différents de sorte à obtenir une reproduction en trois dimensions de la main. Cette biométrie est toutefois sujette aux modifications de la forme de la main liées au vieillissement.

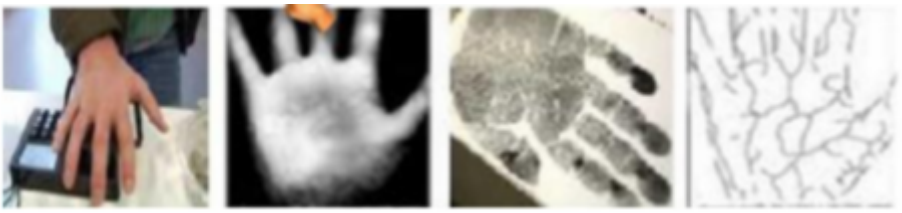


FIGURE 1.2 – géométrie des main.

•**Avantages** : bonne acceptation des usages, très simple à utiliser, le résultat est indépendant de l'humidité et de l'état de propreté des doigts, fichier à petite taille (espace de stockage faible), cette technologie peut offrir une fiabilité élevée et un temps de traitement rapide.

• **Inconvénients** : trop encombrant pour un usage sur le bureau ou voiture, risque de faute pour des jumeaux ou des membres d'une même famille, technique peu discriminante et sensible aux modifications ou altérations naturelles de la main (accident, vieillissement, arthrose), précision restreinte, difficile à utiliser pour les personnes souffrant d'arthrite.

• **Applications** : contrôle d'accès à des locaux, parloirs de prison et accès à des bâtiments prives non stratégiques tels que des entreprises, des écoles et des établissements.

**3) Empreinte palmaire :** une empreinte palmaire [20] est définie comme une empreinte sur une paume. Les empreintes palmaires contiennent plus d'information que les empreintes digitales, ainsi elles sont plus discriminantes. Elles contiennent des caractéristiques distinctives additionnelles telles que les lignes principales et les ridules,

qui peuvent être extraites à partir des images à basse résolution (voir figure 1.3).

• **Avantages** : elles contiennent plusieurs informations qui peuvent être extraites à partir des images à basse résolution, ainsi elles sont plus discriminantes ; les sources de capture d'empreintes palmaires sont beaucoup moins chères que celles de capture des iris. En combinant toutes les caractéristiques d'une paume, telles que les caractéristiques des ridules ou des plis, et des lignes principales, il est possible d'établir un système biométrique robuste.

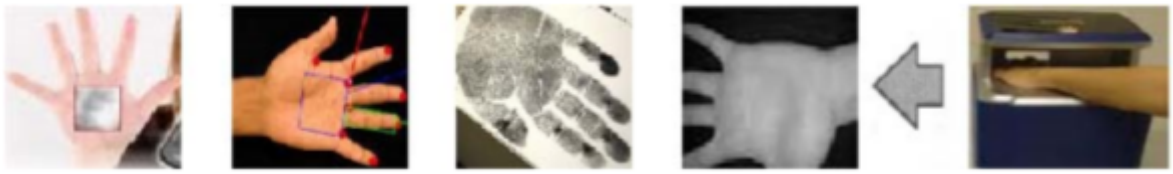


FIGURE 1.3 – Empreinte palmaire.

• **Inconvénients** : une exécution plus lente que celle d'empreinte digitale en raison de l'information supplémentaire stockée dans une empreinte palmaire.

• **Applications** : elle est utilisée typiquement dans des applications légales criminelles. Plusieurs études montrent que l'identification d'empreinte palmaire est sans doute le prochain grand domaine d'investigation dans le cadre des lois sur la sécurité.

**4) Empreinte des articulations des doigts :** la surface extérieure du doigt contient des caractéristiques distinctives, surtout au voisinage des articulations, telles que les lignes principales, les lignes secondaires et les crêtes, qui peuvent être extraites à partir des images à basse résolution.

FIGURE 1.4 – Empreinte des articulations des doigts.

Ces dernières années, un nouveau descripteur biométrique (nouvelle technologie biométrique) basé sur la surface extérieure du doigt, appelé empreinte de l'articulation du doigt [21], est exploité (voir figure 1.4). La main contient plusieurs doigts, pour cela, plusieurs travaux montrent que l'empreinte de l'articulation du doigt peut être

utilisée dans le domaine d'identification des personnes pour une reconnaissance robuste et précise, si on utilise la combinaison ou la fusion de l'information prise de chaque doigt.

• **Avantages** : bonne acceptation, très simple à utiliser. En combinant tous les doigts de la main, il est possible d'établir un système biométrique robuste et précise.

• **Inconvénients** : risque de fausse acceptation pour des jumeaux. Besoin de la co-opération de l'utilisateur (la pose correcte du doigt sur le lecteur).

• **Applications** : ce système reste expérimental.

**5) Iris :** l'iris [22] est la région annulaire située entre la pupille et le blanc de l'œil (partie colorée qui entoure la pupille noire), voir figure 1.5. Elle est constituée d'un réseau de tubes fins dont le diamètre est inférieur à celui d'un cheveu. Les iris sont uniques et les deux iris d'un même individu sont différents. Leurs formes ne varie que très peu durant la vie de l'individu.

FIGURE 1.5 – Iris.

L'image de l'iris comporte de nombreuses caractéristiques physiques différentes. Ce sont les caractéristiques recherchées lorsqu'une personne utilise ce type de système biométrique. Cette image est lue par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l'appareil. La reconnaissance de l'iris est une technologie plus récente puisqu'elle ne s'est véritablement développée que dans les années 80.

• **Avantages** : potentiel de très grande précision, les structures de l'iris restent stables durant toute la vie, la texture de l'iris est parfaitement stable au cours du temps, grande quantité d'information contenue dans l'iris, les vrais jumeaux non confondus.

• **Inconvénients** : l'acquisition des images crée un certain inconfort chez l'utilisateur, ce qui peut empêcher l'enrôlement de certaines personnes. L'acquisition des images exige une certaine formation et de la pratique. Le matériel est plus couteux avec exigences

sur l'éclairage. La fiabilité diminue proportionnellement à la distance entre l'œil et la caméra. L'enregistrement assez contraignant car il impose de ne pas bouger pendant quelques secondes face à la caméra, ce qui rebute certains utilisateurs. Enfin , les gens ont du mal à accepter cette biométrie.

• **Applications** : distributeurs de billets de banque, contrôle d'accès physique et logique.

**6) Visage :** le visage [23] est certainement la caractéristique biométrique que les humains utilisent le plus naturellement pour s'identifier entre eux, ce qui peut expliquer pourquoi elle est en générale très bien acceptée par les utilisateurs. Utiliser une caméra permet d'acquérir la forme du visage d'un individu et puis retirer certaines caractéristiques tels que l'écart entre les yeux, la forme de la bouche, le tour du visage, la position des oreilles, etc (voir figure 1.6). On évitera d'autre part les types de coiffures, les zones occupées par des cheveux en général ou toute zone sujette à modification durant la vie de la personne. Le système de reconnaissance doit être capable d'identifier un individu malgré différents artifices physiques (moustache, barbe, lunettes). Le visage est une biométrie relativement peu sure.

FIGURE 1.6 – Visage.

En effet, le signal acquis est sujet à des variations beaucoup plus élevées que d'autres caractéristiques. Ces variations peuvent être causées, entre autres, par le maquillage, la présence ou l'absence de lunettes, moustache et barbe, le vieillissement et l'expression d'une émotion.

• **Avantages** : simple et capable de fonctionner sans la collaboration de la personne (Ne demande aucune action de l'usager). Technique peu coûteuse et peut s'appuyer sur l'équipement d'acquisition des images actuel. Cette technique est très bien acceptée par le public.

• **Inconvénients** : les changements physiques peuvent tromper le système. Les vrais

jumeaux ne sont pas différenciés. Cette technique est trop sensible au changement d'éclairage et l'angle de l'appareil-photo et aux fortes préoccupations relatives au respect de la vie privée.

• **Applications** : contrôle d'accès à faible niveau de sécurité. Technologie pouvant être associée avec une autre technologie pour la compléter. Cette technique est appliquée dans les aéroports et certains grands magasins.

**7) Rétine :** la rétine [24] est la couche sensorielle située au fond de l'œil. Elle est la paroi interne et opposée de l'œil sur laquelle se projettent les images que nous voyons. Elle est parcourue par de nombreux vaisseaux sanguins (Voir figure 1.7) dont la disposition ne change pas au cours du temps et diffère d'un individu à l'autre, même s'ils sont jumeaux. De plus l'empreinte rétinienne est peu exposée aux blessures et la position respective des vaisseaux reste inchangée durant toute la vie de l'individu. Elles ne peuvent être affectées que par certaines maladies. La reconnaissance de la rétine est actuellement considérée comme une des méthodes

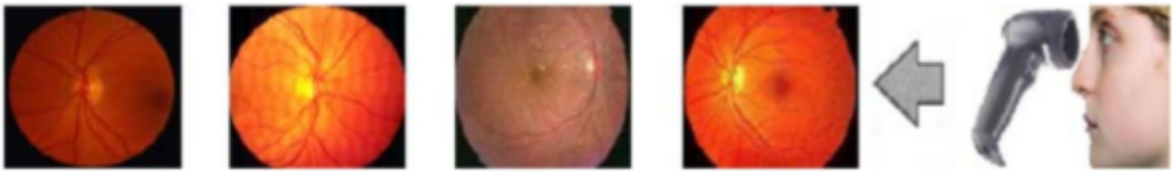


FIGURE 1.7 – Rétine.

biométriques les plus sûres. L'utilisateur doit placer son œil à quelques centimètres d'un orifice de capture situé sur le lecteur de rétine. Il ne doit pas bouger et doit fixer un point vert lumineux qui effectue des rotations. À ce moment, un faisceau lumineux traverse l'œil jusqu'aux vaisseaux sanguins capillaires de la rétine.

• **Avantages** : technique extrêmement précise, très discriminante et extrêmement difficile à frauder car la rétine est un élément interne du corps (la partie du l'œil exploitée n'est pas apparente). L'empreinte rétinienne est peu exposée aux blessures (coupure, brûlure).

• **Inconvénients** : relativement difficile à utiliser. Pas largement distribuée sur le marché. De plus, elle est moins acceptée par le public et un diabète modifie le réseau veineux rétinien.

• **Applications** : technique réservée aux applications relevant de la haute sécurité.

Applications militaires ou nucléaires, contrôle d'accès à des locaux très sensibles.

### 1.5.2 Modalités comportementale

Les techniques comportementales sont basées sur une action entreprise par une personne. D'autre part, la biométrie comportementale est basée sur des mesures et des données dérivées d'une action et mesure indirectement des caractéristiques du corps humain. Voici des exemples de modalités biométriques basées sur des caractéristiques comportementales :

**1) Analyse de la marche :** c'est la façon dont on marche et c'est une biométrique spatio-temporelle complexe. La démarche n'est pas censée être très distinctive, mais elle est suffisamment discriminatoire pour permettre la vérification dans certaines applications à faible sécurité [25].

**2) Signature manuscrite :** la façon dont une personne signe son nom est connue pour être une caractéristique de cette personne. Les signatures changent avec le temps et sont influencées par les conditions physiques et émotionnelles des signataires [26].

**3) Voix :** les systèmes de reconnaissance vocale utilisent les caractéristiques de la voix pour reconnaître une personne. La partie comportementale du discours d'une personne change avec le temps en raison de l'âge, des conditions médicales, de l'état émotionnel, etc. Par conséquent, la voix n'est pas très distinctive et peut ne pas être appropriée pour une identification à grande échelle [27].

**4) Frappe dynamique sur le clavier :** on suppose que chaque personne tape sur un clavier d'une manière caractéristique. Il n'est pas propre à chaque individu, mais il offre suffisamment d'informations discriminatoires pour permettre la vérification d'identité[28].

### 1.5.3 Modalités biologiques

Il s'agit des techniques d'identification à partir des caractéristiques comme le sang, la salive, l'urine, l'odeur ou encore l'ADN. Ces méthodes sont difficiles à mettre en œuvre pour une utilisation courante [29].

### 1.5.4 Autres Modalités

Comme l'iris, le visage ou la voix, d'autres techniques ont été développées ces dernières années dans le but spécifique d'effectuer la vérification ou l'identification fiable d'une personne. Ces recherches ont permis de mettre sur le marché des dispositifs de reconnaissance de la rétine, de la signature, ou encore de la dynamique de frappe au clavier. Mais d'autres champs restent à explorer et certaines de nos caractéristiques sont encore à l'étude dans divers laboratoires. Parmi ces caractéristiques à étudier on peut citer : la géométrie de l'oreille [30], qui peut être utilisé par la police pour identifier un individu à partir d'une photo prise sur le lieu d'un délit, la denture [31], le dessin des lèvres [32], l'odeur corporelle [33], les battements du cœur [34], l'analyse des pores de la peau [35], la salive [36], l'irrigation sanguine [37] et bien d'autres. Les recherches dans le domaine de la biométrie ne sont donc pas encore terminées. Toutefois, il est encore trop difficile de leur prédire lesquelles de ces technologies auront un usage industriel[17].

## 1.6 Domaine d'application

Aujourd'hui les principales applications de la biométrie sont la protection d'identité des personnes, le contrôle d'accès, le contrôle des frontières, l'accès aux réseaux, systèmes d'information et stations de travail, le paiement électronique, la signature numérique et même le chiffrement de données... etc. alors on peut trouver la biométrie partout on cite quelques domaines [38,18] :

### Service public

- Contrôle et sécurité des bâtiments gouvernementaux frontières.
- Contrôle des immigrants qui entrent et sortent du pays.
- Utilisés dans les aéroports et la santé.

### Pouvoir judiciaire

- L'utilisation des empreintes digitales pour prouver certains faits concernant les infractions pénales.
- L'utilisation de l'ADN extrait du sang ou des cheveux dans la scène du crime pour obtenir le criminel.

### Secteurs des banques

- Les transactions bancaires(retraits en espèces, les cartes bancaires,paiement par le téléphone et Internet).

- La réduction de la proportion de la fraude grâce à l'intégration des cartes à puce avec la reconnaissance des empreintes digitales.

### Accès physique et logique

- Ceci se rapporte au contrôle d'accès physique comme la sécurisation des lieux (bâtiment ou une pièce) ou le contrôle d'accès logique comme la sécurisation d'une session informatique (ordinateur ou base de données).

## 1.7 Système biométrique

Un système biométrique est un système basé sur la reconnaissance de forme d'un individu, sur la base de caractères physiologiques ou de traits comportementaux automatiquement reconnaissable et vérifiable [39,18].

### 1.7.1 Principe de fonctionnement d'un système biométrique

Un système biométrique fonctionne selon au moins deux phases : la phase d'apprentissage (Learning phase) qui sert à constituer une base de données de références. La seconde phase est celle de la reconnaissance (Recognition phase) qui sert comme son nom l'indique à identifier et/ou authentifier la personne [40,18].

#### • Phase d'apprentissage (enrôlement)

Est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données [41,18]. (voir la figure 1.8).

#### • Phase d'authentification(reconnaissance)

Dans cette phase, la modalité biométrique est capturée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de pré-traitements supplémentaires pour limiter la dégradation des performances [42,18]. La suite de la reconnaissance sera différente suivant le mode opératoire du système :

1. **Vérification**

   La vérification d'identité consiste à contrôler si l'individu utilisant le système est bien la personne qu'il prétend être. Dans ce cas le système doit répondre à une question de type : «Suis-je bien la personne que je prétends être ?» et renvoie uniquement une décision binaire(oui ou non)[42]. Il suffit donc de comparer le signal avec un seul des gabarits présents dans la base de données (on parle de test 1 :1).

2. **Identification**

   le système doit deviner l'identité d'un individu inconnu. Il répond donc à une question de type : «Qui suis je ?». Dans ce mode, le système compare le signal mesuré avec les différents gabarits contenus dans la base de données (on parle de test 1 :N) [42].

   — **l'identification en mode ensemble fermé :** la sortie du système biométrique est constituée par l'identité de la personne dont le gabarit (référence) possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée.[17]

   — **l'identification en mode ensemble ouvert :** si la plus grande similarité entre l'échantillon biométrique et tous les gabarits est inférieure (ou supérieure) à un seuil de sécurité fixé, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système biométrique. Dans le cas contraire, la personne est acceptée.[17]

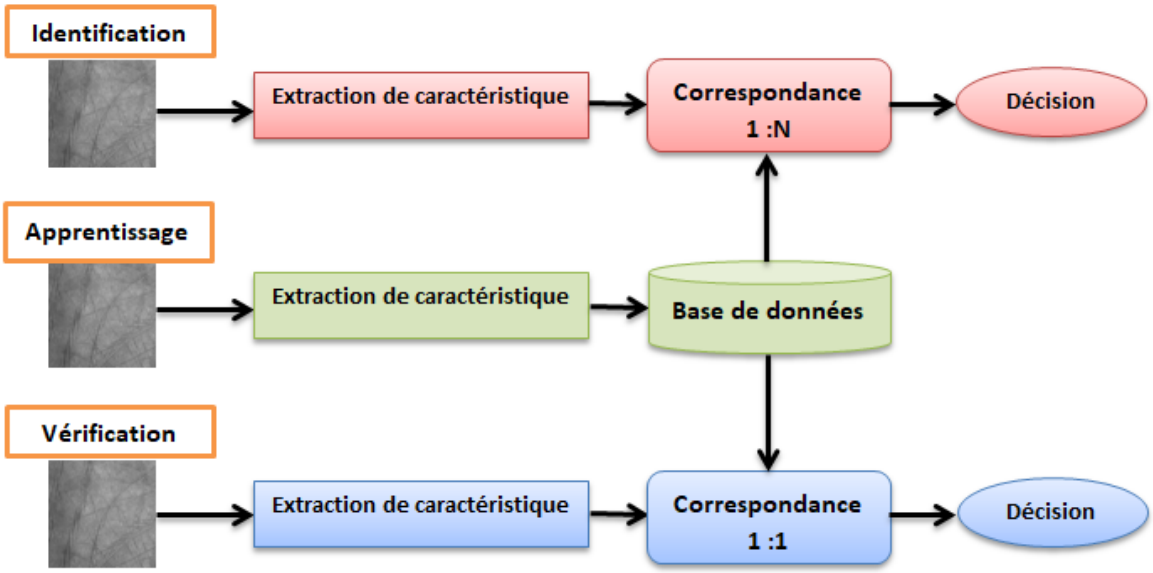



FIGURE 1.8 – Etapes de fonctionnement d'un système biométrique.

### 1.7.2 modules des systèmes biométriques

Un système biométrique est constitué de plusieurs modules [43,18] :

• **module de capture** : consiste à acquérir les données biométriques d'un individu afin d'extraire une représentation numérique (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, ...etc.).

• **module d'extraction de caractéristiques** : prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Généralement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classes (présentation sous forme d'un vecteur "template ou gabarit biométrique").

• **module de correspondance** : consiste à comparer l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de donnée du système et détermine le degré de similitude (ou de divergence) entre les deux vecteurs biométriques.

• **module de décision** : permet de vérifier l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et les gabarits enregistrés.

### 1.7.3 Système en ligne et système hors ligne

En plus du procédé de sélection des caractéristiques, la méthode d'acquisition des images est un autre facteur à prendre en compte [44]. Les systèmes de reconnaissance biométriques sont alors classifies en deux catégories : reconnaissance *en ligne* et reconnaissance *hors ligne*.

✓ **Système hors ligne** : Ce type de système traite les images de chaque modalité précédemment capturée par un scanner numérique. Ces méthodes fournissent des images à haute résolution, mais ne conviennent pas aux systèmes de sécurité en temps réel [38].

✓ **Système en ligne** :Dans ce type de systèmes, les images de modalités sont capturées par un appareil de capture spécifique et ces images numériques acquises sont traitées en temps réel [38].

### 1.7.4 Limitations des systèmes biométriques

Les systèmes biométriques sont meilleurs par rapport aux systèmes traditionnels (badge, mots de passe,...). Mais, ils doivent face à de nombreux problèmes [45,18], citons par exemple :
**La non-universalité :** malgré l'efficacité des modalités biométriques, on ne peut pas dire qu'un système biométrique est universelle parce qu'il est possible pour un sous-ensemble des utilisateurs de ne pas posséder un biométrique particulier. Par exemple (voir figure 1.9), certaines personnes peuvent avoir les empreintes digitales ou palmaires inutilisables à cause d'un accident ou d'un travail manuel prolongé. Une personne muette ne peut utiliser la reconnaissance par la voix ou une personne handicapée ne peut signer. De la même manière, des personnes ayant des maladies oculaires (comme certains glaucomes et cataractes) ne peuvent fournir des images d'iris, ou de rétine, de bonne qualité pour une reconnaissance automatique. Pour toutes ces personnes, certains systèmes biométriques ne sont pas accessibles et ceci risque alors de les exclure de certaines utilisations si aucune alternative ne leur est proposée.

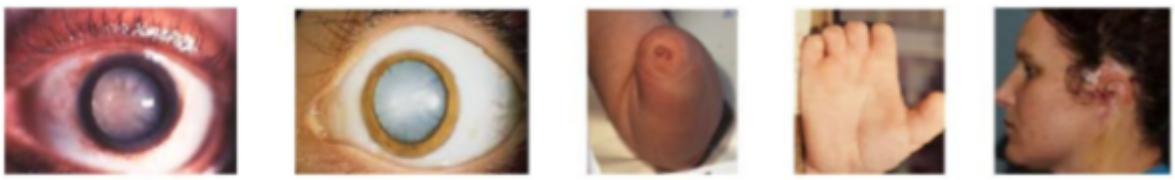


FIGURE 1.9 – Malformations des doigts, main, oreille et de l'iris.

**La non-unicité :** Dans certain type du système biométrique uni-modal on peut tom-

ber sur des résultats similaires, par exemple l'apparence faciale de quelques individus (vrai jumeaux, père fils,...).
**La variabilité lors de la capture :** est le résultat de plusieurs facteurs : le bruit, la déformation physique de la capture, les erreurs de numérotation... Ces variations causent des problèmes lors de la reconnaissance car ils donnent des fausses résultats (même utilisateur mais le système ne l'accepte pas).
**La possibilité de fraude :** parmi les limitations des systèmes uni-modaux, la sécurité contre les attaques, exemple les signatures, la voix. Ces modalités sont facile a reproduire aussi il est possible de fraudé l'empreinte digitale.

## 1.8 Conclusion

Dans ce chapitre, nous avons présenté les concepts de base des technologies biométriques dans lesquels nous avons définir leurs nécessité, leurs intérêt, les différentes modalités biométriques. Ensuite nous avons introduit leur fonctionnement, leur domaine d'utilisation et les limitations des systèmes biométriques

L'attaque sur un gabarit biométrique peut être très préjudiciable car elle implique l'exposition d'une information personnelle et sensible ainsi que le vol d'identité. Dans le chapitre suivant nous discutons les vulnérabilités et menaces d'un système biométrique ainsi que les deux grandes familles de protection des gabarits biométriques : *cryptosystèmes Biométriques et transformation révocable.*

# Chapitre 2

# Systèmes biométrique : menaces et sécurité

## 2.1 Introduction

Les gabarits biométriques sont vulnérables à plusieurs types d'attaques où un attaquant peut récupérer l'image originale de l'utilisateur en utilisant le modèle stocké dans la base de données. D'autre part, l'accès au gabarit est considéré l'une des menaces importantes en terme de sécurité et de la vie privée de l'utilisateur. Pour ces raisons, il est nécessaire de développer des mécanismes robustes pour la protection des gabarits biométriques, ces mécanismes se basent sur l'application d'une clé secrète sur les caractéristiques biométriques pour générer une donnée auxiliaire qui sera ensuite utilisée pour extraire la clé durant l'authentification.

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 afin de garantir un niveau acceptable de sécurité. Les travaux connexes son ensuite présentés.

## 2.2 Vulnérabilités et menaces d'un système biométrique

Un système biométrique appliqué dans une application donnée doit remplir les conditions requises par les clients et les prestataires de services. Fondamentalement, les fournisseurs exigent que le système autorise uniquement les clients à accéder à leurs services, tandis que les clients exigent que leurs sessions soient sécurisées. Par conséquent, pour les prestataires de services, le système biométrique conçu doit être

exploité avec une grande précision dans les deux modes d'identification (ouvert pour ne donner l'autorisation d'accès qu'aux clients et fermé pour identifier exactement l'identité de la personne). Pour les clients, leurs gabarits biométriques doivent être manipulés en toute sécurité (être protégés).

### 2.2.1 Contre-usurpation

Le succès croissant des systèmes biométriques pour garantir la sécurité de l'accès logique / physique a conduit à leur utilisation dans de nombreuses applications vitales. Par conséquent, cette utilisation accrue a conduit à son tour à de nouveaux intérêts dans la recherche et l'exploration de nouvelles méthodes d'attaque de ces systèmes. En effet, de nombreuses recherches ont montré que l'utilisation de la biométrie a créé de nouveaux problèmes et défis liés à la confidentialité et à la vie privée d'un individu. Ces nouveaux problèmes sont plus complexes que ceux rencontrés par les systèmes traditionnels [46] :

*i) Problème de non-confidentialité* : bien que les modalités biométriques garantissent l'unicité, elles ne fournissent pas de secret qui peut être imité ou pris sans connaissance ni consentement. Par exemple, chaque personne a ses propres empreintes digitales, mais cette personne peut laisser ses empreintes digitales sur n'importe quelle surface touchée.

*ii) Problème de non-révocabilité* : chaque personne est définie dans un système biométrique par un gabarit d'entité. Si ce gabarit est volé, la sécurité du système sera sérieusement vulnérable car il n'est pas possible pour un utilisateur légitime de révoquer ses gabarits biométriques et de les remplacer par un autre ensemble d'identifiants. Cela peut également empêcher l'utilisateur de se réinscrire dans le système.

*iii) Problème d'utilisation multiple* : les applications biométriques sont conçues spécifiquement pour des problèmes de sécurité mais peuvent être utilisées très différemment dans d'autres applications. Par exemple, un permis de conduire est conçu pour prouver l'identité et la légitimité de la conduite, mais il peut être utilisé de différentes manières pour prouver l'âge, le nom et même la citoyenneté dans d'autres applications. Un autre aspect de ce problème est une atteinte à la vie privée. Si une personne utilise le même gabarit biométrique dans plusieurs applications, elle peut être facilement suivie dans certaines situations, ce qui peut présenter une violation critique de sa vie privée.

En effet, tous ces problèmes sont liés à la sécurité du gabarit biométrique, qui a incité les chercheurs à développer des moyens de le protéger contre le vol et / ou l'usurpation d'identité. En fait, la plupart des approches de protection des gabarits

biométriques innovantes reposent sur deux approches principales : la cryptographie et la transformation. Dans la première approche, le gabarit biométrique est crypté, tandis que dans la seconde, un gabarit biométrique révocable est produit. De nombreux chercheurs ont prouvé l'efficacité de la seconde approche par rapport à la première. Dans ce travail, ces deux approches seront combinées pour construire un système capable d'extraire un gabarit biométrique profond et sécurisé.

### 2.2.2 Les points de vulnérabilités

En général, une attaque présente la possibilité qu'un adversaire (inscrit ou non inscrit dans le système) de contourner un système sans conscience de ses administrateurs / concepteurs. Les adversaires exploitent la structure des systèmes biométriques pour lancer des attaques spécifiques à un ou plusieurs modules / interfaces.

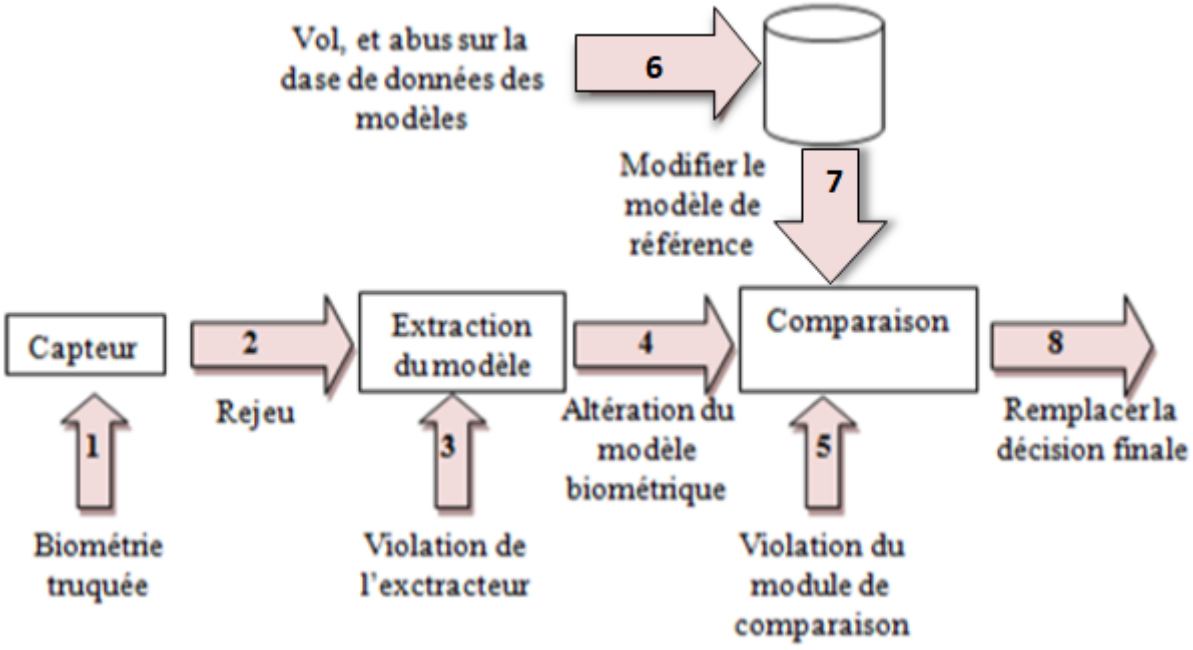



FIGURE 2.1 – Les points de vulnérabilités d'un système biométrique suivant le modèle de *Ratha et al.*[47]

Nous détaillons les points d'attaques de Ratha et al. [47] illustrées dans la figure 2.1 :

— **Point 1 :** dans ce mode d'attaque, une reproduction possible du modalité biométrique est présentée en entrée du système. Les exemples incluent un faux doigt, une copie d'un signature, ou un masque facial.

— **Point 2 :** dans ce mode d'attaque, un signal enregistré est rejoué au système, en contournant le capteur. Les exemples incluent la présentation d'une ancienne

copie d'une image d'empreinte digitale ou de la présentation d'un signal audio précédemment enregistré.

— **Point 3 :** l'extracteur de caractéristiques est attaqué à l'aide d'un cheval de Troie par exemple, afin qu'il produise des ensembles de caractéristiques présélectionnés par l'intrus.

— **Point 4 :** les caractéristiques extraites du l'image d'entrée sont remplacées par un ensemble de caractéristiques frauduleux différent. Cependant, si des minuties sont transmises à un correcteur distant (disons, sur Internet), cette menace est bien réelle. On pourrait «fouiner» sur le TCP / IP empiler et modifier certains paquets.

— **Point 5 :** le module de correspondance est attaqué et corrompu de sorte qu'il produise des scores de correspondance.

— **Point 6 :** la base de données des gabarits stockée peut être local ou distant. Les données peuvent être réparties sur plusieurs serveurs. Ici, l'attaquant pourrait essayer d'en modifier un ou plus de gabarits dans la base de données, qui pourraient aboutir soit à autoriser une personne frauduleuse, soit à refuser le service aux personnes associées avec le gabarit corrompu. Un système d'authentification par carte à puce où se trouve le modèle stocké dans la carte à puce et présenté au système d'authentification, est particulièrement vulnérable à ce type d'attaque.

— **Point 7 :** les gabarits stockés sont envoyés au module de correspondance via un canal de communication. Les données transitant par ce canal pourrait être interceptées et modifiées.

— **Point 8 :** dans ce mode d'attaque, même si le système biométrique a des excellentes caractéristiques de performance, il a été rendu inutile par le simple exercice de remplacer le résultat du module de correspondance.

## 2.3 Protection des systèmes biométriques

Comme nous avons cité précédemment, malgré les avantages des systèmes biométriques, ces systèmes ne sont pas infaillibles et un gabarit stocké peut être compromis par un imposteur. Par conséquent, une parodie des modalités biométriques peut être crée pour obtenir un accès illégitime aux systèmes qui utilisent la même modalité biométrique de l'utilisateur. Un schéma de protection du gabarit idéal devrait réunir les propriétés suivantes [48] :

- **Diversité :** le gabarit sécurisé ne doit pas permettre la compatibilité croisée sur des bases de données, assurant ainsi la confidentialité de l'utilisateur.

- **Révocabilité :** il devrait être simple de révoquer un gabarit compromise et relancez un nouveau gabarit basé sur les mêmes données biométriques.
- **Irréversibilité :** il doit être difficile d'obtenir des calculs du gabarit biométrique d'origine à partir du gabarit sécurisé. Cette propriété empêche un adversaire de créer une parodie physique de la modalité biométrique à partir d'un gabarit volé.
- **Performance :** le programme de protection de gabarit biométrique ne devrait pas dégrader les performances de reconnaissance (FAR et FRR) du système biométrique.

Deux grandes catégories de solutions sont proposées dans la littérature pour protéger les gabarits biométriques :(i) les transformation révocables, et (ii) les cryptosystèmes biométriques (Figure 2.2).

Le point commun à toutes ces solutions réside dans le fait de ne pas stocker directement dans la base les données biométriques brutes : elles sont soit stockées sur un support externe (carte à puce, token), soit stockées après une transformation [49].

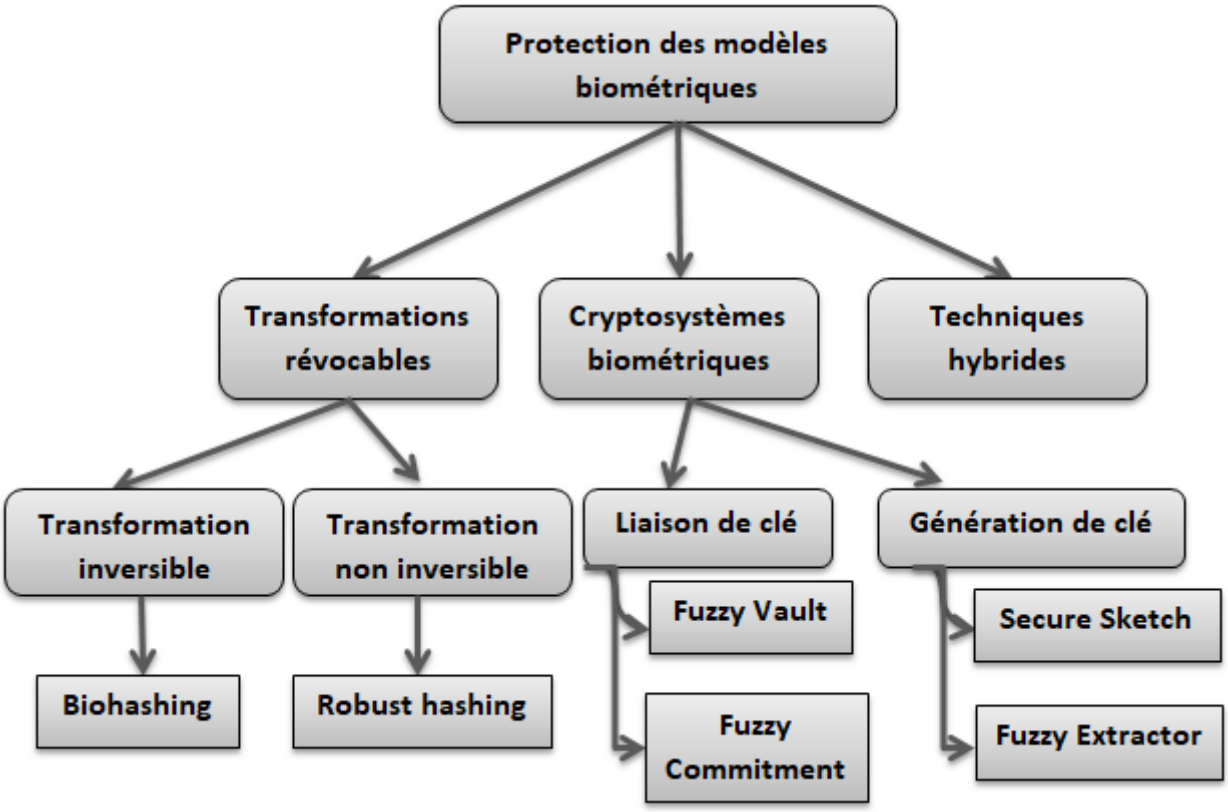



FIGURE 2.2 – Techniques de protection des gabarits biométriques.

### 2.3.1 Cryptosystèmes biométriques

Un cryptosystème biométrique est la combinaison entre les deux technologies de sécurité de l'information à savoir la cryptographie et la biométrie. L'objectif principal de développement de ces cryptosystèmes biométriques est d'améliorer la sécurité des systèmes d'authentification personnelle basés sur la biométrie. Le fonctionnement général de la plupart des cryptosystèmes biométriques est comme suit : durant l'inscription, on utilise un gabarit biométrique $\boldsymbol{O}$ et une clé $\boldsymbol{K}$ pour construire l'ensemble des données auxiliaires $\boldsymbol{H}$ (i.e. helper data), les données auxiliaire ne doivent pas révéler aucune information sur les caractéristiques biométriques ni sur la clé secrète [50]. Au moment de l'authentification, on récupère les éléments d'identification biométriques enrôlés $\boldsymbol{O}$ ou la clé secrète $\boldsymbol{K}$ à partir des caractéristiques biométriques de la requête $\boldsymbol{R}$ (le gabarit de test) et les données auxiliaires $\boldsymbol{H}$ (Figure 2.3).

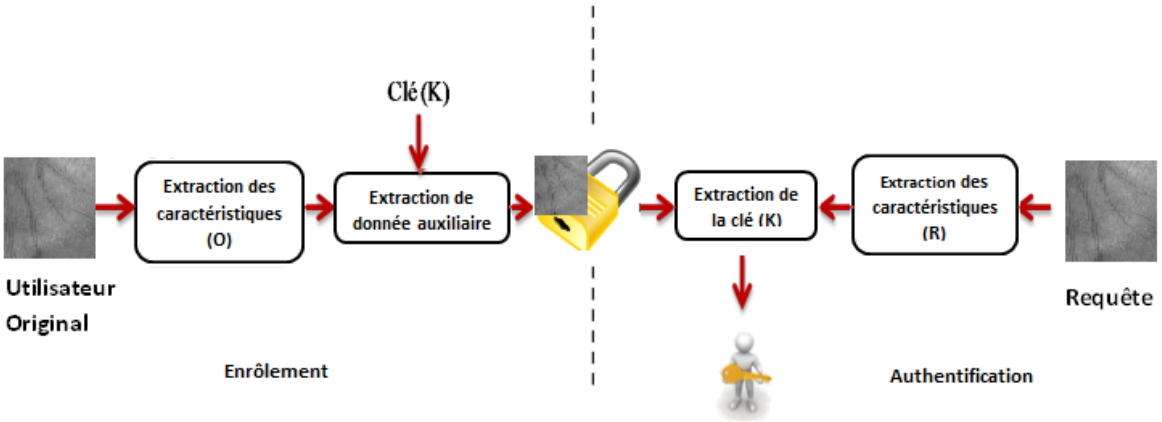



FIGURE 2.3 – Principe de fonctionnement d'un cryptosystème biométrique.

Les approches des cryptosystèmes biométriques sont divisées en deux classes : les cryptosystèmes de type "*Key Binding*" et les cryptosystèmes de type "*Key Generation*" [51].

Lorsque les données auxiliaires sont obtenues en utilisant une clé qui est indépendante des caractéristiques biométriques, il s'agit d'un cryptosystème de type *key-binding*. Si les données auxiliaires sont dérivées seulement à partir du gabarit biométrique et la clé est générée directement à partir des caractéristiques biométriques, il s'agit d'un cryptosystèmes de type *key-generation* [52].

Les approches les plus populaires de type "liaison de la clé" (i.e. : key-binding) sont les systèmes connus sous les nominations : *Fuzzy Commitment* [53] et *Fuzzy Vault* [54,55].

Fuzzy Commitment est une approche proposée par Juels et Wattenberg [56]. Durant l'enrôlement, un mot de code est dérivé d'une clé secrète. Ensuite une donnée auxiliaire est dérivée à partir des caractéristiques biométriques $\boldsymbol{x}$ et du mot de code $\boldsymbol{c}$. Le couple

qui contient la donnée auxiliaire et le mot de code haché $\boldsymbol{h}$ sera alors enregistré dans la base de données. Durant la phase d'authentification, la clé $\boldsymbol{c'}$ doit être dérivée à partir de la donnée auxiliaire stockée dans la base et les caractéristiques biométriques de la requête, L'authentification a réussi si suite $\boldsymbol{h\ (c') = h(c)}$.

Fuzzy vault est une amélioration de fuzzy commitment. Le principe du fonctionnement général de fuzzy vault est que durant l'enrôlement, une clé utilisateur $\boldsymbol{K}$ est utilisée pour construire un polynôme $\boldsymbol{P}^1$ . Ensuite, on calcule la projection polynômiale $\boldsymbol{P(T)}$ du gabarit biométrique de référence $\boldsymbol{T}$. Enfin, on ajoute un peu de bruit à $\boldsymbol{P(T)}$ pour générer la donnée auxiliaire $\boldsymbol{H}$ de fuzzy vault. Au moment de l'authentification/vérification, on utilise le gabarit de test $\boldsymbol{Q}$ et la donnée auxiliaire $\boldsymbol{H}$ pour reconstruire le polynôme $\boldsymbol{P}$ et récupérer ainsi la clé $\boldsymbol{K}$ [55].

Pour les cryptosystèmes biométriques de type "génération de la clé" (i.e. : key-generation), la clé est dérivée directement de la donnée biométrique (Figure 2.3). L'authentification est réussie si la clé est récupérée. Durant la phase d'authentification, la donnée biométrique ne peut pas être reproduite exactement. A cet effet une donnée dérivée du gabarit (la donnée auxiliaire) est aussi enregistrée dans la base de données. Les cryptosystèmes biométriques de type "*Key Generation*" peuvent suivre deux principes. Le premier principe nommé Fuzzy Extractor [57] où une chaine uniformément aléatoire est extraite à partir des données biométriques pour construire une clé. Une donnée auxiliaire est générée ensuite et stockée dans la base de données. Cette donnée est utilisée ensuite pour extraire la clé durant l'authentification. Le deuxième principe référencé par Secure Sketch [58] a pour but d'utiliser la donnée auxiliaire pour régénérer les caractéristiques biométriques originales lors de l'authentification si le gabarit courant et celui enregistré dans la base de données sont proches [58].

### 2.3.2 Transformations révocables

L'idée de base des approches de transformation révocable est de convertir un gabarit biométrique non protégé en un gabarit protégé en utilisant une fonction de transformation [47,59]. La fonction de transformation peut prendre plusieurs formes, selon le système et la modalité visée, et elle peut nécessiter aussi l'utilisation de certains paramètres de transformation (par exemple une clef utilisateur). Dans le cas où les gabarits biométriques transformés sont volés ou compromis, les paramètres de transformation sont modifiés pour mettre à jour le gabarit biométrique protégé. Pour empêcher les imposteurs de suivre les utilisateurs légitimes inscrits dans plusieurs systèmes, et protéger la vie privée par conséquent, il faut appliquer des paramètres de transformation différents ou même des fonctions de transformation différentes pour chaque application[55].

Durant la phase d'enrôlement, une clé secrète $\boldsymbol{K}$ est utilisée avec une fonction de transformation $\boldsymbol{T}$ pour protéger les caractéristiques originales $\boldsymbol{O}$. La transformation

du gabarit ***T(K, O)*** est ensuite stockée dans la base de données. Durant la phase d'authentification, la transformation ***T*** est aussi appliquée sur les caractéristiques de la requête ***R*** pour construire un gabarit transformé ***T(K, R)***. Enfin les deux gabarits transformés ***T(K, O)*** et ***T(K, R)*** sont comparés pour accepter ou refuser l'utilisateur. Le schéma ci-dessous (Figure 2.4) illustre le fonctionnement de l'approche basée sur la transformation révocable [60]. Selon la fonction de transformation, les techniques de transformation sont divisées en deux types : 1) *la transformation inversible* et 2) *la transformation non inversible* [50] [61].

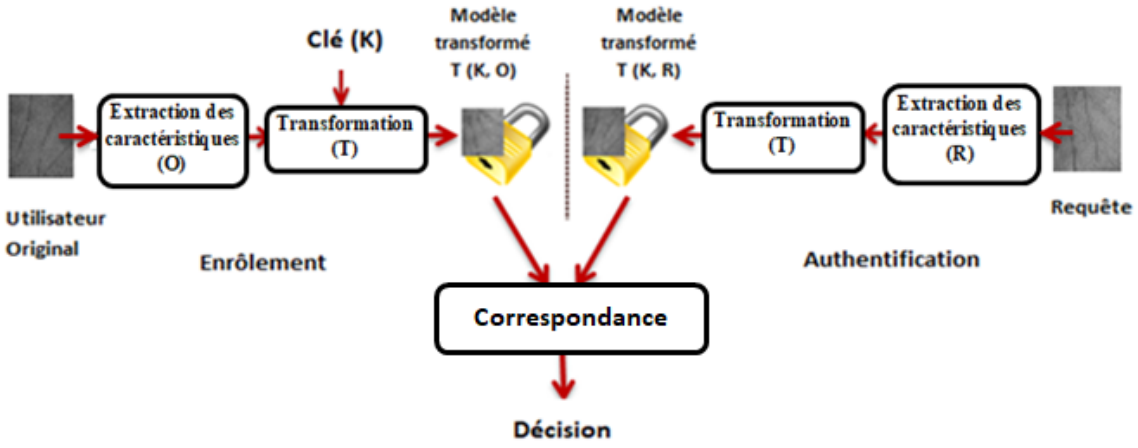



FIGURE 2.4 – Principe de fonctionnement d'un système biométrique basé sur la transformation révocable.

### 2.3.3 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 désavantages. *Feng et al.* [62] ont proposé une approche hybride basée sur la reconnaissance faciale en utilisant premièrement une projection aléatoire puis la méthode des cryptosystèmes biométriques *Fuzzy Commitment* [56].

Autres techniques d'hybridation sont basées sur l'utilisation des mots de passe pour renforcer la sécurité des cryptosystèmes. Dans leur travail [64], *Nandakumar et al.* ont utilisé un mot de passe pour transformer les caractéristiques des empreintes digitales en se basant sur la méthode des cryptosystèmes *Fuzzy Vault* [63]. *Song et al.* [65] ont proposé une méthode hybride basée sur la génération de la clé secrète durant l'enrôlement à partir des données biométriques en appliquant le hachage discret.

## 2.4 Travaux connexes

Afin de démarrer nos travaux et de cibler correctement les lacunes et les besoins dans ce domaine, nous avons commencé notre recherche par une étude bibliographique des moyens de protection des modalités biométriques via Internet ou lors du stockage. Cette vue d'ensemble de ces moyens nous a permis de voir quelles sont leurs principales caractéristiques, leurs avantages et inconvénients respectifs et de démontrer la nécessité de répondre à un nouveau système de sécurité et de confidentialité.

Il existe un consensus sur le fait que la biométrie offre un caractère unique dans les systèmes d'authentification d'identité d'une personne car ils y sont plus étroitement liés, et cela est considéré comme un atout majeur de la technologie biométrique. Cependant, ces dernières années, un certain nombre de critiques ont été formulées concernant la sécurité de ces systèmes par la communauté des chercheurs en sécurité, en particulier celles liées aux attaques contre les modèles biométriques stockés dans la base de données du système. Dans cet aperçu, nous n'exposerons que les travaux les plus importants qui tournent autour du chiffrement de modèles biométriques et des systèmes biométriques révocables qui utilisent des techniques d'apprentissage approfondi.

*1) Cryptage du modèle biométrique* : Premièrement, un cryptosystème biométrique combine la biométrie avec une clé cryptographique et fusionne ses avantages. Actuellement, de nombreux algorithmes de cryptage ont été proposés, y compris des techniques de cryptage conventionnelles telles que AES, RSA ou IDEA [66]. Cependant, ces techniques de chiffrement ne semblent pas idéales pour les images biométriques, principalement en raison des différences importantes entre le texte et les données biométriques, y compris la forte corrélation des images biométriques, la capacité et la redondance élevée [67]. Ces dernières années, des techniques d'apprentissage approfondi et un cryptage basé sur le chaos ont été progressivement développés, ce qui améliore toutes les exigences et démontre la supériorité sur les schémas de cryptage conventionnels.

Dans [68], un schéma de chiffrement chaotique est proposé pour améliorer la sécurité des images biométriques lors de la transmission. Le schéma proposé est basé sur la transformation de paquets d'ondelettes fractionnaires (FrWPT), la carte chaotique et la décomposition de Hessenberg. L'idée principale est de mélanger les images biométriques en utilisant la transformation affine suivie de la transformation dans le domaine FrWPT avec des ordres de transformation générés chaotiquement. Dans une autre approche [69], *Jindal et al.* ont proposé une méthode de protection de modèle de visage basée sur le réseau neuronal convolutionnel profond (CNN) et le hachage cryptographique SHA3-512. L'idée principale de cette méthode est de générer des codes binaires uniques avec une entropie maximale. Chaque utilisateur inscrit se voit alors attribuer un code binaire unique. Ces codes binaires sont utilisés en interne pour former le CNN profond pendant la phase d'inscription. Un hachage cryptographique du

code binaire unique attribué à un utilisateur, représentant le modèle de visage sécurisé de l'utilisateur, est calculé et stocké dans la base de données. Dans la méthode proposée présentée dans [70], l'algorithme de cryptage d'image de l'iris basé sur le deep learning effectue d'abord une normalisation, un autre prétraitement sur le jeu de données d'image de l'iris collecté, puis utilise le modèle Deep Learning Neural Network (DNN) pour extraire les caractéristiques de l'iris image. Le vecteur de caractéristiques extrait est utilisé pour la génération de clés, et enfin, l'opération XOR est effectuée sur la clé et la valeur de pixel de l'image d'origine. *Hsiao et al.* [71] ont proposé une nouvelle méthode de chiffrement pour promouvoir la sécurité des images d'empreintes digitales, un filtre adaptatif non linéaire à modèle d'amplitude chaotique en fréquence (APFM). Leur schéma a une résistance élevée contre une attaque exhaustive avec des combinaisons très élevées et la séquence chaotique présente une distribution uniforme. *2) Biométrie révocable* : L'idée de base des systèmes biométriques révocables est de convertir le gabarit d'origine en une version différente en utilisant une fonction de transformation non inversible dans la phase d'inscription. La fonction de transformation peut prendre plusieurs formes, selon le système et la modalité, et elle peut également nécessiter l'utilisation de certains paramètres de transformation.

*Abdellatef et al* [72], ont proposé une méthode de reconnaissance faciale multibiométrique révocable qui utilise plusieurs CNN pour extraire des traits profonds de différentes régions du visage. Une bio-convolution avec des noyaux aléatoires est appliquée à la génération de modèles biométriques révocables. Dans cette méthode, une séquence transformée est obtenue en utilisant une séquence originale par convolution avec un noyau aléatoire. Dans une autre approche, *Jang et al.* [73] ont proposé un système biométrique révocable pour l'authentification faciale en exploitant le système de récupération d'images faciales basé sur CNN. Pour la biométrie révocable, un schéma de hachage basé sur table profonde (DTH) qui code les fonctionnalités basées sur CNN dans le code binaire à l'aide de l'index de table de hachage est utilisé. Ensuite, ils utilisent l'intégration du bruit et l'intranormalisation qui déforme les données biométriques, ce qui améliore la non-inversibilité. *Liu et al.* [74] ont présenté un schéma sécurisé et efficace pour générer des modèles biométriques sécurisés, efficaces et révocables. Les auteurs de cette méthode utilisent Deep Belief Networks (DBN) et des projections aléatoires (FVR-DLRP) pour générer un modèle sécurisé et renouvelable. Le schéma FVRDLRP proposé transforme les modèles de haute dimension en un espace de dimension relativement basse avec une règle selon laquelle la distance entre les points doit être fixée sous un seuil satisfaisant. *Talreja et al.* [75] ont développé un système multibiométrique sécurisé qui utilise le DNN et le codage à correction d'erreur. Dans cette méthode, les vecteurs de caractéristiques de sortie par Face-CNN et IrisCNN sont fusionnés dans deux architectures différentes pour la couche de représentation conjointe : architecture entièrement connectée (FCA) et architecture bi-linéaire

(BLA). Dans FCA, les sorties de Face-CNN et Iris-CNN sont concaténées verticalement et passées à travers une couche entièrement connectée pour fusionner les caractéristiques de l'iris et du visage. Dans BLA, les sorties de Face-CNN et Iris-CNN sont combinées en utilisant le produit externe de matrice des vecteurs de caractéristiques face et iris. La sortie de la couche de représentation conjointe est un vecteur d'entités multimodales partagées à valeur réelle pour la biométrie du visage et de l'iris. Ce vecteur de représentation partagé est binarisé et un vecteur de bits fiable spécifique à l'utilisateur forme le modèle révocable. *Rathgeb et al.* [76] ont proposé un schéma générique pour générer une représentation irréversible de plusieurs modèles biométriques basés sur des filtres Bloom adaptatifs. Dans ce travail, les filtres Bloom sont utilisés pour obtenir une représentation irréversible du visage binaire et des caractéristiques de l'iris. Ensuite, les vecteurs de caractéristiques binaires sont disposés dans une matrice bidimensionnelle de largeur WF (WI) et de hauteur HF (HI). Chaque code binaire bidimensionnel est ensuite divisé en blocs de taille égale où les modèles protégés sont générés selon deux mots de code différents. *Ratha et al.* [47] ont proposé une génération de modèle biométrique révocable pour un système biométrique multimodal (visage et oreille) utilisant une projection aléatoire. Ils ont divisé le schéma biométrique révocable proposé en trois parties. Tout d'abord, la transformation est effectuée à l'aide d'une projection aléatoire double. Ensuite, les entités transformées sont projetées par les composants principaux (PC), et les entités doubles sont fusionnées par regroupement k-means. Enfin, la variabilité inter-classe est améliorée à l'aide de l'analyse linéaire discriminante (LDA).

## 2.5 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.

Le système hybride est un enjeu majeur a l'heure actuelle. Dans le chapitre suivant, nous présentons notre méthode proposée basée sur la combinaison des deux solution de protection des systèmes biométriques : la cryptographie et la transformation révocable, dans le but de répondre efficacement à tous les impératifs de sécurité souhaités.

# Chapitre 3

# Conception et réalisation d'un système biométrique sécurisé

## 3.1 Introduction

Après avoir présenté les différentes approches utilisées pour la sécurité des systèmes biométriques , un nouveau système biométrique révocable est proposé dans le présent chapitre. Notre système proposé est basé sur une nouvelle méthode, appelée Security-Oriented Discrete Cosine Transform Network (S-DCTNet)), qui extrait un ensemble de caractéristiques profondes et révocable pour garantir à la fois des performances élevées et renforcée la sécurité du système biométrique. Afin d'évaluer le système proposé, nous utilisons les modalités biométriques à savoir l'empreinte palmaire et la veine palmaire comme sujets. Les résultats expérimentaux ont montrés que le système proposé offre un niveau de sécurité très élevé et protège le système biométrique tout au long du processus de transformation. De plus, une couche de déguisement est également utilisée pour limiter et contrôler l'accès au système, tandis que l'authentification des utilisateurs est sécurisée a l'aide des gabarits révocables.

Dans le reste de ce chapitre nous présentons, dans une première étape, les prérequis théoriques sur lesquelles repose le système proposé. Dans cette section la transformée DCT ainsi que les cartes chaotiques utilisées dans notre système sont présentés. Un aperçu de l'architecture de système biométrique révocable est ensuite détaillé. Nous conclurons le présent chapitre par une analyse et discussion des résultats expérimentaux obtenus.

## 3.2 Prérequis théoriques

Essentiellement, tous les problèmes liées à la conception finale d'un système de reconnaissance de formes sont généralement liées à l'étape d'extraction de caractéristiques. Dans cette section, nous essayons de donner les prérequis théoriques concernant la transformation discrète en cosinus (DCT) et les cartes chaotiques sur lesquels est basé le système biométrique révocable proposé.

### 3.2.1 Transformée en cosinus discrète

Discrete Cosine Transform (DCT) [77] est un procédé très connu dans le domaine du traitement d'image qui permet de passer de la représentation spatiale d'un signal à sa représentation spectrale. L'application de la transformée DCT à une image, qui a des coefficients réels, décorrèle les pixels de l'image et concentre les informations dans les coefficients de basse fréquence (côté supérieur gauche). Pour une analyse rapprochée, cette transformation est généralement appliquée aux blocs d'une image au lieu de l'image entière.

La matrice de transformation 1D-DCT pour les entrées carrées de taille B × B est donnée par[95] :

$$\varphi_{ij} = \begin{cases} \frac{1}{\sqrt{B}} & i = 0, \quad 0 \leq j \leq B-1 \\ \sqrt{\frac{2}{B}} \cos\left[\frac{\pi(2j+1)i}{2B}\right] & 1 \leq i \leq B-1 \\ & 0 \leq j \leq B-1 \end{cases} \qquad (1)$$

La 2D-DCT n'est qu'un produit d'une base verticale et d'une base horizontale de 1D-DCT. Ainsi, en utilisant l'équation 1, nous générons la matrice de taille B × B ,($\varphi$) qui est utilisée pour créer la transformée DCT $p \times p$ ($p = B \cdot B$)[95] :

$$\varphi = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1B} \\ a_{21} & a_{22} & \cdots & a_{2B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{B1} & a_{B2} & \cdots & a_{BB} \end{pmatrix} = \begin{pmatrix} \nu_1 \\ \nu_2 \\ \vdots \\ \nu_B \end{pmatrix} \in \mathbb{R}^{B \times B} \qquad (2)$$

Afin de créer la 2D-DCT, les composants de chaque ligne de la matrice $\varphi$ sont utilisés comme poids pour toutes les lignes de la même matrice, comme le montre l'équation suivante[95] :

$$\begin{aligned} &\mathcal{M}_k = \nu_i^T \cdot \nu_j \in \mathbb{R}^{B \times B} \\ &\quad i, j = 1, 2, \cdots, B \\ &\quad k = 1, 2, \cdots, \rho \end{aligned} \qquad (3)$$

Le calcul de $M_k|_{k=1}^{p}$ peut être facilement compris par l'exemple suivant[95] :

$$\begin{aligned}\mathcal{M}_1 = \nu_1^T \cdot \nu_1 &= \begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1B} \end{pmatrix} \times (a_{11}, a_{12}, \cdots, a_{1B}) \\ &= \begin{pmatrix} a_{11}(a_{11}, a_{12}, \cdots, a_{1B}) \\ a_{12}(a_{11}, a_{12}, \cdots, a_{1B}) \\ \vdots \\ a_{1B}(a_{11}, a_{12}, \cdots, a_{1B}) \end{pmatrix} \in \mathbb{R}^{B \times B}\end{aligned} \tag{4}$$

Ensuite, chaque matrice obtenue ($M_k$) est transformée en un vecteur unidimensionnel ($V_k$)[95] :

$$\mathcal{V}_k = \mathcal{F}_{\rho \times 1}(\mathcal{M}_k) \in \mathbb{R}^{\rho \times 1} \tag{5}$$

Où $F_{p\times1}$ est une fonction qui mappe la matrice $M_k \in \mathbb{R}^{B\times B}$ à un vecteur $V_k \in \mathbb{R}^{p\times1}$. Les vecteurs obtenus ($V_k|_{k=1}^{p}$) sont ensuite concaténés en un seul vecteur (V)[95] :

$$\mathcal{V} = [\mathcal{V}_1, \mathcal{V}_2, \cdots, \mathcal{V}_\rho] \in \mathbb{R}^{\rho \times \rho} \tag{6}$$

Maintenant, nous utilisons la technique d'ordre de balayage en *zig-zag* (direction principale de fréquence horizontale) pour réorganiser les composants de ce vecteur[95] :

$$\widehat{\mathcal{V}} = \mathcal{F}_z(\mathcal{V}) = [\widetilde{\mathcal{V}}_1, \widetilde{\mathcal{V}}_2, \cdots, \widetilde{\mathcal{V}}_\rho] \in \mathbb{R}^{\rho \times \rho} \tag{7}$$

La technique du *zig-zag* est utilisée pour réorganiser les composants du vecteur ($\widehat{V}$) selon leur importance (basse fréquence à haute fréquence), dans laquelle les composants importants sont placés au début du vecteur. Enfin, il est important de noter que le premier vecteur ($\widetilde{V}$) (première colonne de $\widehat{V}$) représente la valeur moyenne qui est appelée la composante DC.

### 3.2.2 Les cartes chaotiques

L'avantage des systèmes chaotiques réside dans l'extrême sensibilité à tout changement des conditions initiales qui sont les états initiaux et les paramètres de contrôle. En effet, si deux systèmes chaotiques identiques ont très peu de différence dans leurs états initiaux et / ou dans leurs paramètres de contrôle, les orbites chaotiques de ces systèmes seront très différentes. Ce comportement d'hypersensibilité rend leur utilisation très intéressante pour la sécurité de l'information.

**Carte Logistique**

En 1845, *Pierre Verhulst* propose la carte logistique [78], qui est une carte dynamique non linéaire et qui est considérée comme l'une des cartes chaotiques les plus populaires. La carte logistique est un système chaotique dont le comportement complexe peut provenir d'équations dynamiques non linéaires très simples données par l'équation de récurrence suivante :

$$\begin{aligned} x_{n+1} &= \Gamma_L(x_n, \mu) \\ &= \mu x_n(1 - x_n),\ \mu \in [0, 4],\ x_n \in [0, 1] \end{aligned} \tag{8}$$

où $x_n$ est l'état du système pour n = 0, 1, 2, $\cdots$ et $\mu$ est le paramètre de contrôle. Itérativement, ce système génère une séquence à partir de $x_0 \in [0, 1]$ appelée l'état initial. En fonction des valeurs de $\mu$, $\Gamma_l$ peut être une séquence convergente, une séquence oscillante ou une séquence chaotique. Ainsi, ce système est considéré chaotique si $\mu \in [3.75, 4]$ et purement chaotique si $\mu \cong 4$ comme le montre le diagramme de bifurcation de Hopf [79]. Généralement, dans un système de sécurité de l'information, l'état initial et le paramètre de contrôle du système chaotique peuvent être utilisés comme clés secrètes $k \equiv \{x0, \mu\}$ .

**Carte Tent**

Dans l'étude des systèmes dynamiques discrets, la carte des tentes [80] est un candidat bien connu qui montre des orbites chaotiques et d'autres comportements dynamiques typiques. Mathématiquement, la carte des tentes est une fonction de valeur réelle $\Gamma_t(\mu)$ définie par :

$$\begin{aligned} x_{n+1} &= \Gamma_T(x_n, \mu) \\ &= \mu\ \min(x_n, 1 - x_n),\ \mu \in [0, 2],\ x_n \in [0, 1] \end{aligned} \tag{9}$$

où $x_n$ est l'état du système pour n = 0, 1, 2, $\cdots$ et $\mu$ est le paramètre de contrôle. Selon les valeurs de $\mu$, ce système présente des comportements très différents mais il devient un système chaotique lorsque $\sqrt{2} \leq \mu < 2$. De plus, dans ce cas, l'état initial $x_0$ et le paramètre de contrôle $\mu$ sont utilisés pour former la clé secrète ($k \equiv \{x0, \mu\}$).

**Carte Rössler**

Ce système a été proposé par le biochimiste allemand *Otto Rössler* en 1976, afin d'étudier l'écoulement des fluides. L'article original de *Rössler* indique que son système est similaire au système de *Lorenz*, mais il est facile à analyser car il ne contient qu'une seule spirale. La carte chaotique de *Rössler* [81] est définie par les équations suivantes :

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{pmatrix} = \Gamma_R \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -y - z \\ x + \alpha y \\ \beta - \gamma z + xz \end{pmatrix} \tag{10}$$

où les paramètres $\alpha$ , $\beta$ et $\gamma$ sont des constantes. *Rössler* a étudié le système chaotique avec $\alpha = \beta = 0{,}2$, et $\gamma = 5{,}7$, mais les propriétés de $\alpha = \beta = 0{,}1$, et $\gamma = 14$ sont aujourd'hui plus étudiées.

**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 [82] :

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{pmatrix} = \Gamma_S \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \sigma(y - x) \\ \rho x - y - xz \\ xy - \beta z \end{pmatrix} \tag{11}$$

Dans ces équations $\sigma$, $\rho$ et $\beta$ sont trois paramètres réels strictement positifs et les variables dynamiques x, y et z représentent l'état du système à 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 $\sigma = 10$, $\beta = 8/3$ et $\rho$ variable restante.

## 3.3 S-DCTNet framework

La méthode d'extraction de caractéristiques en profondeur basée sur S-DCTNet conserve la simplicité de DCTNet, mais avec la possibilité de produire des caractéristiques biométriques sécurisées (en utilisant le cryptage) et révocables (en utilisant la transformation), grâce à deux couches supplémentaires, ce qui le rend plus protégé contre toute attaque ou usurpation d'identité.

Dans ce système et avant la phase d'extraction des caractéristiques, le système forme d'abord les filtres de convolution (en utilisant la transformée DCT). Pour cela, avant d'expliquer comment le système extrait les caractéristiques profondes et révocables, nous présenterons tout d'abord la construction de ces filtres de convolution.

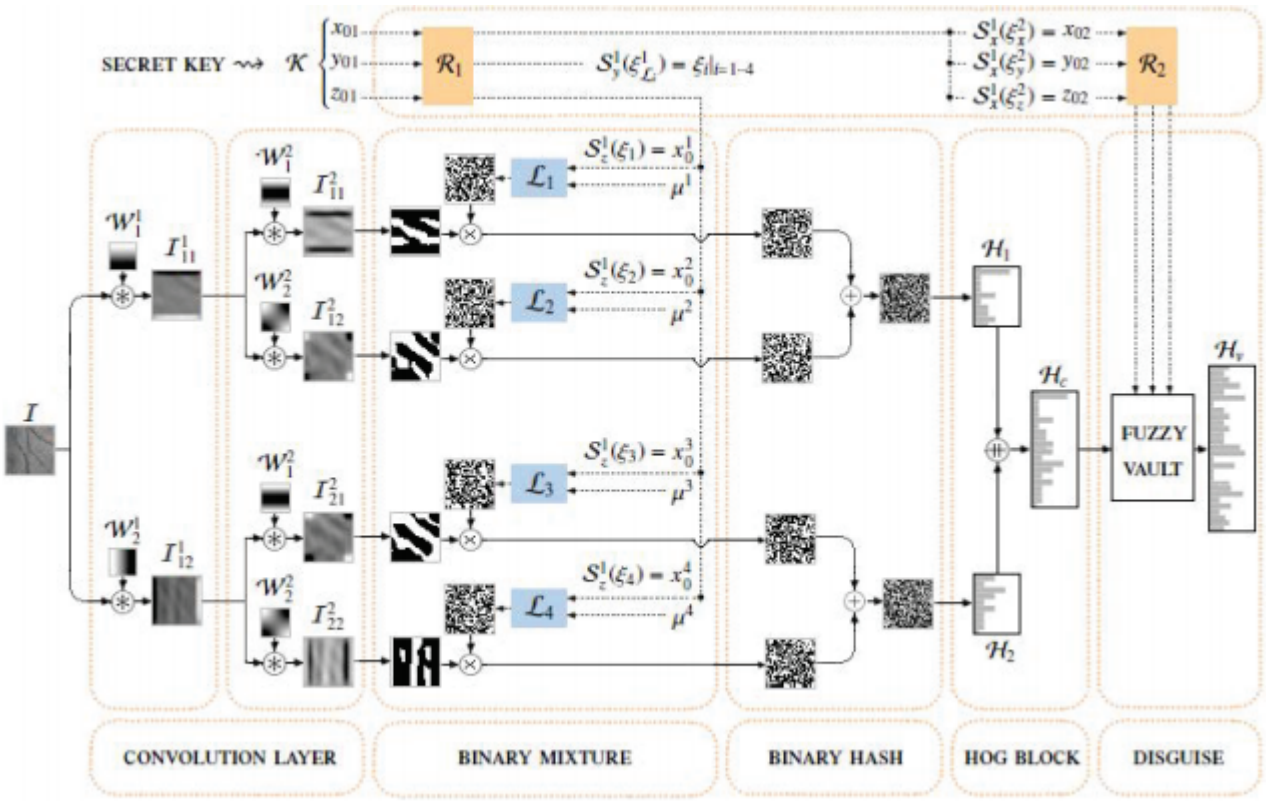



FIGURE 3.1 – Proposition d'un ensemble de caractéristiques profondes sécurisées et révocables basée sur les cartes chaotiques (S-DCTNet). Un exemple de S-DCTNet à 2 stages avec 2 filtres de convolution à chaque stage.

### 3.3.1 Formulation des filtres

Le système DCTNet est similaire au système PCANet, la différence fondamentale entre eux réside dans la façon dont les filtres sont formés : le premier système utilise la technique PCA, tandis que le second utilise la technique DCT. Ainsi, dans cette sous-section, nous présenterons la méthode utilisée dans le système DCTNet pour sélectionner les filtres convolutionnels à partir de la transformée DCT.

Tout d'abord, comme dans le système PCANet, l'image dans le système DCTNet est analysée par blocs. *Cong Jie Ng et al* dans [83], démontre la forte similitude entre les vecteurs propres des blocs (filtres) et la transformée DCT. En effet, selon les auteurs, si la corrélation entre les blocs est très élevée, les vecteurs propres PCA de la matrice de covariance des blocs s'approcheront de la transformée DCT. De plus, ils démontrent qu'une grande valeur propre de PCA correspond à une basse fréquence dans la DCT et vice versa. Cette propriété est vitale pour la sélection de la base DCT pour DCTNet (sélection des filtres), qui suit le PCA en classant l'importance du vecteur propre en fonction de la valeur propre respective.

Soit $\eta$ le nombre de filtres de taille $k_1 \times k_2$ utilisés à un stade donné (en général, des filtres carrés et impairs sont utilisés, donc ($k_1 = k_2$). Les filtres convolutionnels

sont choisis parmi le vecteur 2D-DCT ($\widehat{\mathcal{V}}$) prouvé par l'équation 7 (voir sous-section 4.1). Avant de spécifier ces filtres, il convient de noter que dans un système DCTNet, la composante DC (valeur moyenne) n'est pas considérée comme un filtre, comme indiqué par PCANet, la suppression de la moyenne de chaque patch donne de meilleures performances. La sélection de base commence donc de 2 à $\eta + 1$.

$$\mathcal{V}_F = \widehat{\mathcal{V}}(i)|_{i=2}^{\eta+1} \in \mathbb{R}^{\rho \times \eta}, \quad \rho = k_1 \times k_2 \tag{12}$$

Enfin, l'ensemble des filtres est obtenu comme suit :

$$\mathcal{W}_j = \mathcal{F}_{k_1 \times k_2}[\mathcal{V}_F(j)] \in \mathbb{R}^{k_1 \times k_2}, \quad j = 1, 2, \cdots, \eta \tag{13}$$

Où $\mathcal{W}_j$ désigne le filtre $j$ et $\mathcal{F}_{k1 \times k2}$ est une fonction qui mappe le vecteur $\mathcal{V}_F(\mathrm{j})|_{j=1,\eta}$ $\in \mathbb{R}^{\rho \times 1}$ à une matrice $\mathcal{W}_j \in \mathbb{R}^{k_1 \times k_2}$.

### 3.3.2 Architecture fonctionnelle

Dans la Fig. 3.1, nous présentons la structure S-DCTNet proposée qui se compose de deux stages. En général, cette structure peut être divisée en cinq étapes principales : étape de convolution (deux stages), étape de mélange binaire, étape de hachage binaire, étape d'extraction de caractéristiques HOG basées sur des blocs et étape de déguisement. Afin de décrire le schéma du système, nous supposerons que les images d'entrée sont de la taille $H \times W$ et que la taille du patch, c'est-à-dire la taille du filtre convolutionnel 2D, pour l'étape $l$ est :

$$\mathcal{W}_i^\ell = k_1^\ell \times k_2^\ell, \quad i \in [1 \cdot \cdot L_\ell], \quad \ell \in [1 \cdot \cdot S_\ell] \tag{14}$$

où $\mathrm{L}_l$ désigne le nombre de filtres dans la couche convolutionnelle $l$ et $\mathrm{S}_l$ est le nombre de couches convolutionnelles. Il est important de noter que $k_j^l|_{j=1,2}$ est un nombre entier impair satisfaisant aux conditions $k_j^l \leq H$ & $k_j^l \leq W$.

#### *Couche de convolution*

La méthode d'extraction de caractéristiques profondes DCTNet est inclue dans la catégorie des techniques d'apprentissage en profondeur par convolution telles que CNN. Ainsi, dans ces techniques, nous faisons d'abord convoluer l'image d'entrée avec plusieurs filtres et après l'étape de regroupement (réduction des données), les caractéristiques sont formées. La couche de convolution peut être réalisée à plusieurs stages différents en termes de taille de filtre et de nombre de filtres. Il est important de noter que contrairement au PCANet, la DCTNet ne contient pas une phase d'apprentissage pour former les filtres de convolution car il utilise directement la transformée DCT

comme filtres.

*1) Premier stage de convolution* : Dans cette étape, tout d'abord, nous utilisons l'équation 7 pour former la transformée DCT (avec B = $k_1^1 = k_2^1$), dont le vecteur résultant $\widehat{\mathcal{V}}$ est utilisé pour créer les filtres convolutionnels $L_1$ :

$$\mathcal{V}_F = \widehat{\mathcal{V}}(i)|_{i=2}^{L_1+1} \in \mathbb{R}^{\rho \times L_1}, \quad \rho = k_1^1 \times k_2^1 \tag{15}$$

L'ensemble des filtres de ce stage est obtenu comme suit :

$$\mathcal{W}_i^1 = \mathcal{F}_{k_1^1 \times k_2^1}[\mathcal{V}_F(i)] \in \mathbb{R}^{k_1^1 \times k_2^1}, \quad i = 1, 2, \cdots, L_1 \tag{16}$$

Les sorties de ce stage sont obtenues en filtrant l'image d'entrée ($\mathcal{I}$) par les filtres $\mathcal{W}_i^1|_{i=1}^{L_1}$ , où des images filtrées $L_1$ peuvent être obtenues :

$$\mathcal{I}_i^1 = \mathcal{I} \circledast \mathcal{W}_i^1, \quad i = 1, 2, \cdots L_1 \tag{17}$$

où le symbole $\circledast$ indique un processus de convolution 2D et $\mathcal{I}_i^1$ sont les images filtrées en sortie de stage 1. Il est important de noter que pour obtenir des images filtrées de même taille que $\mathcal{I}$ ($H \times W$), une interpolation de limite à remplissage nul est appliquée .

*2) Deuxième stage de convolution* : Comme le premier stage, les mêmes opérations sont effectuées dans le deuxième stage sur toutes les sorties du premier stage. De même, à ce stage, nous utilisons l'équation 7 pour former la transformée DCT (avec B = $k_1^2 = k_2^2$ ), où le vecteur résultant $\widehat{\mathcal{V}}$ est utilisé pour créer les filtres convolutionnels $L_2$ :

$$\mathcal{V}_F = \widehat{\mathcal{V}}(i)|_{i=2}^{L_2+1} \in \mathbb{R}^{\rho \times L_2}, \quad \rho = k_1^2 \times k_2^2 \tag{18}$$

Les filtres de convolution à ce stage sont donnés comme suit :

$$\mathcal{W}_j^2 = \mathcal{F}_{k_1^2 \times k_2^2}[\mathcal{V}_F(j)] \in \mathbb{R}^{k_1^2 \times k_2^2}, \quad j = 1, 2, \cdots, L_2 \tag{19}$$

Les sorties du deuxième stage sont obtenues en filtrant toutes les images ($\mathcal{I}_i^1|_{i=1}^{L_1}$) par les filtres $\mathcal{W}_j^2|_{j=1}^{L_2}$ :

$$\mathcal{I}_{ij}^2 = \mathcal{I}_i \circledast \mathcal{W}_j^2, \quad i = 1, 2, \cdots L_1, \quad j = 1, 2, \cdots L_2 \tag{20}$$

Enfin, en utilisant $L_2$ filtres, nous pouvons obtenir $L_2$ image filtrées pour chaque image d'entrée, donc pour chaque image, nous obtenons des images filtrées $L_1 \cdot L_2$ à la sortie du deuxième stage.

***Couche de mélange binaire***

Pour des raisons de sécurité, cette couche combine le gabarit biométrique avec une matrice produite afin que le gabarit puisse être révocable et remplaçable à tout moment. Par conséquent, le gabarit résultant change en fonction de la clé secrète tout en préservant les performances du système biométrique.

*1) Génération de matrices de dissimulation* : la première étape dans cette couche consiste à produire les matrices de dissimulation pour chaque sortie de la dernière étape de convolution (dans notre système, le deuxième stage). Notre système utilise de nombreux systèmes chaotiques, dont deux sont les principaux (utilisés comme clés secrètes) et les autres (sont utilisés pour créer des matrices de dissimulation) changent en fonction du nombre de filtres dans le premier et deuxième stage.

Premièrement, en utilisant la clé secrète $\{ \mathcal{K} = (x_{01},\ y_{01},\ z_{01}) \in [0 \cdot \cdot\ 1]^3\}$ et le premier système chaotique principal ($\mathcal{R}_1$ pour le système Rössler ou $\mathcal{Z}_1$ pour le système Lorenz) pour générer trois séquences ($\mathcal{S}_x^1$, $\mathcal{S}_y^1$ et $\mathcal{S}_z^1$), dans lequel $\mathcal{S}_y^1$ et $\mathcal{S}_z^1$ sont utilisés pour contrôler les systèmes auxiliaires chaotiques (qui sont des systèmes logistiques $(\mathcal{L}_i|_{i=1}^{L_1L_2})$ ou des systèmes de tentes $(\mathcal{T}_i|_{i=1}^{L_1L_2})$ et $\mathcal{S}_x^1$ est utilisé plus tard pour contrôler le deuxième système chaotique principal (cryptage de modèle).

Pour chaque sortie du deuxième stage (chaque image filtrée), les deux séquences ($\mathcal{S}_y^1$ et $\mathcal{S}_z^1$) sont utilisées pour déterminer les états initiaux $(x_0^i|\ {}_{i=1}^{L_1L_2})$ des systèmes auxiliaires chaotiques. Ces séquences ont $\epsilon$ éléments et sont définies comme suit :

$$\Gamma_R \begin{pmatrix} x_{01} \\ y_{01} \\ z_{01} \end{pmatrix} = \begin{cases} \mathcal{S}_x^1 \equiv \{x_i\}_{i=1}^{\epsilon-1} \\ \mathcal{S}_y^1 \equiv \{y_i\}_{i=1}^{\epsilon-1} \\ \mathcal{S}_z^1 \equiv \{z_i\}_{i=1}^{\epsilon-1} \end{cases} \tag{21}$$

Les éléments de $\mathcal{S}_y^1$ (générés par $\mathcal{R}_1$) étant utilisés comme coordonnées dans $\mathcal{S}_z^1$, ils doivent donc devenir des entiers. En effet, la séquence $\mathcal{S}_y^1$ est normalisée dans l'intervalle $[1,\ \epsilon]$, comme suit :

$$\mathcal{S}_y^1 = 1 + \lfloor 10^5 \cdot \mathcal{S}_y^1 \rfloor (\text{mod } \epsilon) \quad \mathcal{S}_y^1(i) \in [1 \cdot \cdot \epsilon] \tag{22}$$

Où $\lfloor \bullet \rfloor$ désigne la partie entière. Pour déterminer les états initiaux des systèmes chaotiques auxiliaires $(\mathcal{L}_i|\ {}_{i=1}^{L_1L_2})$, la séquence $\mathcal{S}_z^1$ est utilisée :

$$\begin{cases} x_0^i = \mathcal{S}_z^1(\xi_i) \\ \xi_i = \mathcal{S}_y^1(\xi_{\mathcal{L}_i}) \end{cases} \qquad i = 1, 2, \cdot \cdot\ L_1L_2 \tag{23}$$

$\{\xi_{\mathcal{L}i}\}_{i=1,2,L_1L_2}$ sont des valeurs entières prédéfinies utilisées comme coordonnées dans $\mathcal{S}_y^1$, dans lesquelles elles peuvent également être utilisées comme clé secrète. De

plus, les paramètres de contrôle des systèmes chaotiques auxiliaires ($\mathcal{L}_i|_{i=1}^{L_1L_2}$ ou $\mathcal{T}_i|_{i=1}^{L_1L_2}$) sont définis comme suit :

$$\mu^i = \alpha + \beta\varrho_i \quad i = 1, 2, \cdot\cdot L_1L_2 \tag{24}$$

Où $\varrho_i \in [0 \cdot\cdot 1]$ et la paire ($\alpha$, $\beta$) est égale à (3,57, 0,43) et (1,41, 0,58) pour, respectivement, le système logistique ($\mathcal{L}$) et le système de tente ($\mathcal{T}$). Ces valeurs sont choisies pour que les deux systèmes conservent toujours leur comportement chaotique. Il est important de noter qu'une méthode d'optimisation (par exemple l'algorithme génétique (GA)) est utilisée pour sélectionner les différents $\varrho_i$ (donc $\mu_i$) afin de maximiser le taux d'identification du système biométrique.

Maintenant, chaque système chaotique auxiliaire ($\mathcal{L}_i|_{i=1}^{L_1L_2}$) génère une séquence de longueur $H \cdot W$ :

$$\mathcal{S}_i = \Gamma_L(x_0^i, \mu^i) = \{s_j\}_{j=1}^{H\cdot W} \quad i = 1, 2, \cdot\cdot L_1L_2 \tag{25}$$

Chaque séquence ($\mathcal{S}_i$) est ensuite remodelée pour former une matrice ($\mathcal{M}_i$) de la même taille que l'image d'entrée :

$$\mathcal{M}_i = \mathcal{F}_{H,W}(\mathcal{S}_i) \in \mathbb{R}^{H\times W} \quad i = 1, 2, \cdot\cdot L_1L_2 \tag{26}$$

Une fois les différentes matrices ($\mathcal{M}_i$) générées, une opération de factorisation est appliquée à chaque matrice. Pour ce faire, nous avons utilisé la factorisation $QR$ [84] qui est l'un des processus importants de l'analyse matricielle dans le traitement du signal / image et les statistiques.

Soit $\mathcal{M}_i$ une matrice composée de $\nu^i$ colonnes définies comme suit :

$$\mathcal{M}_i = [\nu_0^i, \nu_1^i, \nu_2^i, \cdot\cdot \nu_W^i] \tag{27}$$

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

$$\mathcal{M}_i = Q_i \cdot R_i, \quad R_i \in \mathbb{R}^{W\times W}, \quad Q_i \in \mathbb{R}^{H\times W} \tag{28}$$

La matrice résultante $Q_i$ a la même dimension que $\mathcal{M}_i$ mais avec des colonnes orthogonales. Ces matrices orthogonales ($Q_i|_{i=1}^{L_1L_2}$) sont utilisées pour créer des matrices binaires $L_1L_2$. Le processus de quantification binaire transforme une valeur réelle en valeur binaire. En fait, un principe de seuillage est appliqué, comme suit :

$$\mathcal{M}_i^b(n,m) = \begin{cases} 0 & \text{if } Q_i(n,m) < 0 \\ 1 & \text{if } Q_i(n,m) \geq 0 \end{cases} \quad i = 1, \cdot\cdot L_1 L_2 \quad (29)$$

Enfin, les matrices binaires obtenues sont ensuite utilisées pour transformer les sorties du dernier stage de convolution dans un autre espace pour leur permettre d'être cachées.

*2) Processus XORing* : Dans cette étape, les sorties de la dernière étape de convolution de chaque image sont masquées. Pour ce faire, chaque sortie est binarisée puis *XORing* avec le $\mathcal{M}_i^b$ correspondant.

$$\mathcal{I}_{ij}^{2b}(n,m) = \begin{cases} 0 & \text{if } \mathcal{I}_{ij}^{2}(n,m) < 0 \\ 1 & \text{if } \mathcal{I}_{ij}^{2} \geq 0 \end{cases} \quad (30)$$
$$i = 1, 2, \cdots L_1, \quad j = 1, 2, \cdots L_2$$

Après avoir converti toutes les sorties de dernier stage, nous appliquons l'opération *XOR* entre chaque sortie et le $\mathcal{M}^b$ correspondant comme suit :

$$\widehat{\mathcal{I}}_{ij}^{2b} = \mathcal{I}_{ij}^{2b} \otimes \mathcal{M}_k^b \qquad \begin{matrix} k = (i-1)L_1 + j \\ i = 1, \cdot\cdot, L_1, \quad j = 1, \cdot\cdot, L_2 \end{matrix} \quad (31)$$

Après cette étape et dans l'étape d'histogramme, il devient impossible de récupérer les données d'origine car l'étape d'histogramme est un processus irréversible et la condition de révocabilité la plus importante est donc vérifiée dans notre système.

***Couche de hachage binaire***

Cette étape réduit la quantité de données, dans laquelle les images binarisées $L_2$ sont converties en une image à valeur entière. Ainsi, la chaîne de bits binaires $L_2$ autour de chaque pixel est convertie à l'aide du polynôme de décodage suivant (processus de conversion binaire en décimal) :

$$\mathcal{I}_i^3 = \sum_{j=0}^{L_2-1} \widehat{\mathcal{I}}_{ij}^{2b} \cdot 2^j, \quad i = 1, \cdots, L_1 \quad (32)$$

Comme dans PCANet, le nombre de sorties de cette étape dans DCTNet est égal au nombre de filtres utilisés dans le premier stage de convolution. Ainsi, après décodage de chaque groupe $L_2$ séparément, nous obtenons un ensemble d'images à valeur entière égal à $L_1$.

***Couche d'histogramme***

Cette étape réduit également la taille de la fonctionnalité de chaque image. Ainsi, l'histogramme de chaque image parmi les images $L_1$ est calculé et tous ces histogrammes sont concaténés pour former le vecteur caractéristique. Contrairement au DCTNet, notre S-DCTNet proposé utilise l'histogramme des gradients orientés (HOG).

*1) Partition de blocs* : Pour obtenir le vecteur caractéristique de chaque image d'entrée, nous partitionnons d'abord chaque image $\mathcal{I}_i^3|_{i=1}^{L_1}$ en plusieurs blocs ($\mathcal{B}$). Ainsi, chaque image est partitionnée en $N_b$ blocs comme suit :

$$\mathcal{N}_b = \lfloor \frac{h - b_1}{o} + 1 \rfloor \times \lfloor \frac{w - b_2}{o} + 1 \rfloor \tag{33}$$

Où $o$ désigne le chevauchement horizontal / vertical entre deux blocs adjacents, $b_1$ $\times$ $b_2$ est la taille du bloc d'analyse et $\lfloor \bullet \rfloor$ est la partie entière de la valeur. Pour chaque image ($\mathcal{I}_i^3|_{i=1}^{L_1}$), on obtient un ensemble de blocs $\Phi_i$ définis comme suit :

$$\begin{aligned} \Phi_i &= \{\mathcal{B}_1^i, \mathcal{B}_2^i, \cdot\cdot \mathcal{B}_{\mathcal{N}_b}^i\} \in \mathbb{R}^{(b_1 \times b_2) \times \mathcal{N}_b} \\ & B_j^i|_{j=1}^{\mathcal{N}_b} \in \mathbb{R}^{b_1 \times b_2}, \quad i = 1, 2, \cdot\cdot, L_1 \end{aligned} \tag{34}$$

où $B_j^i$ désigne le $i^{me}$bloc pour l'image $\mathcal{I}_i^3$.

*2) Vecteur caractéristique HOG* : Dans cette étape, un histogramme HOG pour chaque bloc ($\mathrm{B}_j^i$) est calculé et tous les vecteurs résultants pour les images $L_1$ sont ensuite concaténés pour former le vecteur caractéristique final pour l'image examinée.

Dans la technique HOG, l'image d'entrée est analysée par fenêtre ($\mathcal{W}_{HOG}$), dans laquelle chaque fenêtre ($\mathcal{W}_{HOG}$) est divisée en cellules ne se chevauchant pas. Ensuite, l'orientation et la magnitude du gradient sont calculées pour chaque pixel. Un histogramme de ces orientations est formé pour chaque cellule. L'amplitude du gradient est utilisée comme poids de vote. Les histogrammes des cellules de chaque fenêtre sont concaténés pour former le descripteur HOG. Ainsi, en utilisant la technique HOG, nous pouvons extraire les caractéristiques de chaque bloc comme :

$$\begin{aligned} \mathcal{H}_j^i &= \mathcal{F}_{\mathrm{HOG}}(B_j^i) \in \mathbb{R}^{\lambda \times 1} \\ & j = 1, 2, \cdot\cdot, \mathcal{N}_b, \quad i = 1, 2, \cdot\cdot, L_1 \end{aligned} \tag{35}$$

où $\mathcal{F}_{HOG}$ désigne le processus d'extraction de caractéristique HOG et $\lambda$ est la longueur de l'histogramme de bloc. Cette valeur ($\lambda$) est en fonction du nombre de fenêtres HOG ($\eta_w$) et du nombre de cases d'histogramme ($\eta_b$). Pour chaque image

$\mathcal{I}_i^3|_{i=1}^{L_1}$, les vecteurs de caractéristiques HOG extraits de tous les blocs sont concaténés en un seul vecteur $(v_i)$ :

$$\vartheta_i = [\mathcal{H}_1^i, \mathcal{H}_2^i, \cdot\cdot \mathcal{H}_{\mathcal{N}_b}^i] \in \mathbb{R}^{(\mathcal{N}_b\lambda)\times 1}, \quad i = 1, 2, \cdot\cdot, L_1 \quad (36)$$

Enfin, le vecteur caractéristique de l'image d'entrée est obtenu comme suit :

$$\mathcal{V}_T = [\vartheta_1, \vartheta_2, \cdot\cdot \vartheta_{L_1}] \in \mathbb{R}^{(\mathcal{N}_b\lambda L_1)\times 1} \quad (37)$$

Il est important de noter que la longueur et la précision du vecteur $(\mathcal{V}_T)$, de chaque image d'entrée, changent en fonction de la taille du bloc $(b_1 \times b_2)$ et du taux de recouvrement $(o)$.

***Couche de déguisement***

Dans cette étape et afin de mieux protéger le gabarit biométrique, nous le déguisons en utilisant un concept quelque peu similaire à le *Fuzzy Vault*. Ce processus est contrôlé par le deuxième système chaotique principal ($\mathcal{R}_2$ pour le système Rössler ou $\mathcal{Z}_2$ pour le système Lorenz).

$$\begin{cases} x_{02} = \mathcal{S}_x^1(\xi_x^2) \\ y_{02} = \mathcal{S}_x^1(\xi_y^2) \\ z_{02} = \mathcal{S}_x^1(\xi_z^2) \end{cases} \quad (38)$$

Où $\{\xi_x^2, \xi_y^2, \xi_z^2\} \in [1 \cdot\cdot \epsilon]$ sont trois valeurs entières prédéfinies utilisées comme coordonnées dans $\mathcal{S}_x^1$. Ce système génère trois séquences, où :

*i)* Les composants de la première séquence $(\mathcal{S}_x^2)$ sont utilisés comme un ensemble de chaff points, la taille de cette séquence est égale à la taille du gabarit biométrique :

$$\mathcal{S}_x^2 = \{x_i\}_{i=1}^{\mathcal{N}_b\lambda L_1} \quad (39)$$

Les composants de cette séquence sont normalisés entre le maximum et le minimum du gabarit biométrique $(\mathcal{V}_T)$. Pour ce faire, nous normalisons d'abord $\mathcal{S}_x^2$ dans $[0 \cdot\cdot 1]$ :

$$\mathcal{S'}_x^2 = \frac{\mathcal{S}_x^2 - \min(\mathcal{S}_x^2)}{\max(\mathcal{S}_x^2) - \min(\mathcal{S}_x^2)} \quad (40)$$

Ensuite, nous normalisons $\mathcal{S}_x'^2$ en [min $(\mathcal{V}_T)$, max $(\mathcal{V}_T)$] en utilisant la formule suivante :

$$\widehat{\mathcal{S}}_x^2 = \mathcal{S'}_x^2 \left[\max(\mathcal{V}_T) - \min(\mathcal{V}_T)\right] + \min(\mathcal{V}_T) \tag{41}$$

*ii)* La deuxième séquence ($\mathcal{S}_y^2$) est utilisée pour mélanger le gabarit biométrique. Soit $\widehat{\mathcal{S}}_y^2$ la séquence, à composantes entières, produite à l'aide de la deuxième séquence.

$$\widehat{\mathcal{S}}_y^2 = 1 + \lfloor 10^5 \cdot \mathcal{S}_y^2 \rfloor (\text{mod } \mathcal{N}_b \lambda L_1) \quad \mathcal{S}_y^1(i) \in [1 \cdot \cdot \epsilon] \tag{42}$$

Nous divisons cette séquence en deux sous-séquences ($\widehat{\mathcal{S}}_{y1}^2$ et $\widehat{\mathcal{S}}_{y2}^2$) comme :

$$\begin{aligned} \widehat{\mathcal{S}}_{y1}^2 &= \{y_i^1\}_{i=1,3,5,\cdot\cdot,\mathcal{N}_b\lambda L_1 - 1} \\ \widehat{\mathcal{S}}_{y2}^2 &= \{y_i^2\}_{i=2,4,6,\cdot\cdot,\mathcal{N}_b\lambda L_1} \end{aligned} \tag{43}$$

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

$$\begin{aligned} \mathcal{V}_T(\widehat{\mathcal{S}}_{y1}^2(i)) \leftrightarrows \mathcal{V}_T(\widehat{\mathcal{S}}_{y2}^2(i)) \Leftrightarrow \mathcal{V}_T(y_i^1) \leftrightarrows \mathcal{V}_T(y_i^2) \\ i = 1, 2, 3, \cdot\cdot\cdot, \frac{\mathcal{N}_b\lambda L_1}{2} \end{aligned} \tag{44}$$

*ii)* La troisième séquence ($\mathcal{S}_z^2$) est utilisée pour créer les coordonnées utilisées pour insérer les chaff points. Nous utilisons également l'équation 42 pour produire une séquence (de longueur $\mathcal{N}_b\lambda L_1$) avec des composantes entières.

$$\widehat{\mathcal{S}}_z^2 = 1 + \lfloor 10^5 \cdot \mathcal{S}_z^2 \rfloor (\text{mod } 2\mathcal{N}_b\lambda L_1) \tag{45}$$

Les composants de cette séquence ne doivent pas être répétés, pour cela, une phase de prétraitement doit être appliquée pour supprimer toutes les coordonnées redondantes et générer une séquence contenant différents composants. Le gabarit biométrique déguisé final ($\widehat{\mathcal{V}}_T$) est défini comme suit :

$$\begin{cases} \widehat{\mathcal{V}}_T(\widehat{\mathcal{S}}_z^2(i)) = \widehat{\mathcal{S}}_x^2(i), & i = 1 \cdot \cdot \mathcal{N}_b\lambda L_1 \\ \widehat{\mathcal{V}}_T(j) = \mathcal{V}_T(i), & j \neq i \end{cases} \tag{46}$$

Contrairement à la cryptographie basée sur le *Fuzzy Vault*, dans laquelle le *Fuzzy Vault* a sécurisé la clé secrète, dans notre méthode, nous l'utilisons pour sécuriser le gabarit biométrique.

## 3.4 Résultats expérimentaux et discussions

Le but de cette section est d'évaluer les performances de la méthode proposée, nous avons donc implémenté notre méthode dans un système d'identification biométrique à base de palmprint / palm-vein. Les expériences ont été menées sur un ensemble de données public et disponible de deux modalités biométriques fournies par Hong Kong Polytechnic University (PolyU) [85]. Cet ensemble de données contient des images multispectrales de la paume des mains, nous avons donc utilisé les bandes spectrales *rouge, verte et bleue* pour représenter l'empreinte palmaire (PLM), tandis que la bande proche infrarouge est utilisée pour la modalité palm-veine (PLV). Dans cet ensemble de données, chaque personne dispose de douze échantillons pour chaque modalité biométrique. Dans nos expériences, nous avons utilisé une base de données de 400 personnes, ce qui est similaire à un certain nombre d'employés dans une petite ou moyenne entreprise. Comme le système biométrique comprend deux phases : l'inscription et l'identification, nous avons divisé l'ensemble de données en deux galeries. Dans la galerie d'inscription, nous avons utilisé au hasard quatre échantillons de la modalité biométrique pour chaque personne, soit $400 \times 4 = 1600$ échantillons, tandis que les neuf autres échantillons ont été utilisés pour l'évaluation des performances du système, soit $400 \times 8 = 3200$ échantillons. En utilisant toutes les images de test, 641600 scores correspondants ont été obtenus, dont 3200 scores pour des expériences authentiques et 638400 scores pour des expériences d'imposteurs.

Dans ce travail, nous avons mené plusieurs expériences, que nous pouvons organiser en deux parties principales. Dans la première partie, nous présenterons des expériences pour évaluer les performances du système biométrique. Le but de cette partie est de choisir les paramètres optimaux de notre méthode proposée et d'évaluer sa robustesse face à un changement de clé secrète. La deuxième partie se concentre sur l'évaluation du niveau de sécurité du système biométrique contre les attaques.

### 3.4.1 Analyse de précision du système biométrique

Étant donné que la méthode de protection du modèle proposée est intégrée dans deux couches différentes, notre système biométrique peut donc utiliser l'une de ces deux couches ou les deux ensemble. Par conséquent, dans cette partie, nous avons divisé l'ensemble de test en deux sous-parties. En effet, étant donné que le cryptosystème biométrique n'affecte pas les performances du système biométrique, nous évaluerons ces performances dans la première sous-partie sans la protection du modèle (système biométrique basé sur DCTNet). Contrairement au cryptosystème biométrique, le processus de transformation du modèle biométrique (modèle biométrique révocable) affecte considérablement les performances du système biométrique, de sorte que ces performances doivent être réévaluées à nouveau (système biométrique basé sur S-DCTNet)

dans la deuxième sous-partie.

***Résultats des tests du système basés sur DCTNet***

Étant donné que la représentation finale des caractéristiques de l'image a un impact significatif sur le taux de reconnaissance du système et que la méthode d'extraction des caractéristiques (DCTNet) dépend de plusieurs paramètres, nous avons effectué un test empirique pour choisir les meilleurs paramètres qui pourraient améliorer la précision du système. Il convient de noter que l'effet du nombre et de la taille des filtres sur le taux de reconnaissance a été étudié à l'aide d'un système à un stage. Ces tests ont été réalisés en utilisant deux modalités biométriques (PLM et PLV) et deux classifieurs principaux utilisés, à savoir KNN et SVM. Ainsi, dans ces tests préliminaires, nous tentons de choisir le nombre de filtres ($\eta$) ainsi que leur taille ($k_1^1 \times k_2^1$ avec $k_1^1 = k_2^1$) parmi les valeurs des ensembles {2, 4, 6, 8, 10} et {9 , 11, 13, 15, 17}, respectivement. Ainsi, afin de voir l'effet de ces paramètres ($\eta$, $k_1^1$) sur les performances du système biométrique, nous illustrons clairement, sur la figure 3.2, les résultats du système d'identification à système ouvert (taux d'acceptation véritable (GAR) contre $\eta$ par rapport à $k_1$), qui utilise les deux méthodes biométriques (PLM et PLV) et fonctionne avec les deux classifieurs (KNN et SVM). Ainsi, à partir de différentes courbes de la figure 3.2, nous pouvons extraire quatre remarques importantes :
*1)* 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 97,5% a déjà été obtenu.
*2)* En général, plus le nombre de filtres est élevé, plus le taux d'identification est élevé, de sorte que les meilleurs résultats ont été obtenus avec 10 filtres, ce qui est meilleur que les performances obtenues avec 2 filtres.
*3)* Par rapport au classifieur KNN, les performances du système peuvent être améliorées avec le classifieur SVM, à partir duquel des performances optimales sont obtenues.
*4)* Enfin, l'utilisation de la modalité PLM, au lieu de la modalité PLV, peut améliorer efficacement les performances du système.

Pour la modalité PLM, d'après la figure 3.2. *(a)*, il est clair que la combinaison ($\eta$, $k_1^1$) = (10, 17) offre de meilleurs résultats en termes de GAR. Dans ce cas, le système d'identification peut atteindre un taux d'erreur égal (EER) de 0,0197% à un seuil $T_o$ = 0,7053. Une amélioration de 100% peut être obtenue en utilisant le classifieur SVM avec ($\eta$, $k_1^1$) = (10.11) (voir Fig. 3.2. *(b)*) et le seuil peut être choisi dans l'intervalle [0,252 -0,405]. La figure 3.2. *(c)* montre clairement l'efficacité du classifieur SVM par rapport au classifieur KNN. Le système biométrique conserve le même comportement dans le mode d'identification en ensemble fermé, il fonctionne avec une reconnaissance de rang un (ROR) égale à 94,281% à un rang de reconnaissance parfaite (RPR) égal à

59. Ces performances sont effectivement améliorées lors de l'utilisation classifieur SVM (ROR = 100,00% à RPR = 1).

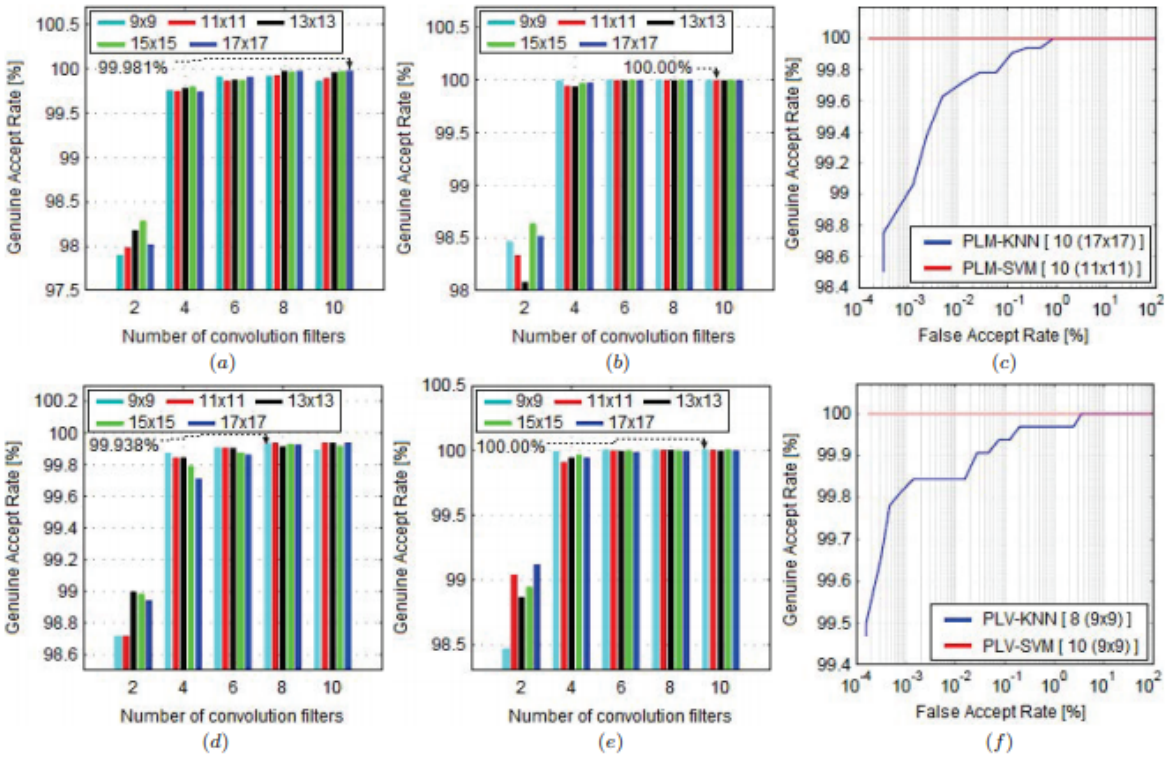



FIGURE 3.2 – Performances du système biométrique ouvert basé sur DCTNet. *(a), (b), (c)* Système biométrique basé sur PLM utilisant KNN et SVM et leur comparaison, et *(d), (e), (f)* Système biométrique basé sur PLV utilisant KNN et SVM et leur comparaison.

Pour la Modalité PLV, huit filtres à convolution de taille $9 \times 9$ offrent les meilleures performances dans un système biométrique basé sur KNN (voir Fig. 3.2. *(d)*). Dans cette configuration, le système fonctionne avec un EER acceptable égal à 0,0625% ($T_o$ = 0,6865). De plus, une performance parfaite peut être obtenue en utilisant SVM avec dix filtres de convolution de taille $9 \times 9$ (EER = 0,000% ($T_o$ = [0,216-0,279]), voir Fig.3.2. *(e)*. Enfin, dans la Fig.3.2 *(f)*, nous comparons les performances de ce système sous les deux classifieurs. Nous avons également examiné le mode d'identification en modalité, le système fonctionne toujours mal avec le classifieur KNN par rapport à SVM, dans lequel un ROR égal à 99,969% (RPR = 2) est obtenu. À partir de ces résultats, nous pouvons clairement voir que la modalité PLM peut améliorer les performances du système avec 68,480% par rapport à la modalité PLV, et cette supériorité est justifiée par la richesse de la modalité PLM avec des caractéristiques intrinsèques telles que les lignes principales et les rides.

Bien que le système biométrique unimodal donne un résultat utile, il n'exclut pas la possibilité d'accepter un utilisateur non autorisé ou de refuser un consommateur

autorisé. Heureusement, la biométrie multimodale [86] peut réduire les erreurs de reconnaissance, puis améliorer l'efficacité du système. Dans nos résultats précédents, le classifieur KNN donne de mauvais résultats d'identification ; pour cela, les résultats obtenus en utilisant ce classifieur pour les deux modalités biométriques sont fusionnés au niveau du score de correspondance [87] en utilisant le principe de fusion de score basé sur des règles. Dans notre travail et pour plus de simplicité, nous avons utilisé cinq règles de fusion différentes, qui sont le score maximum et minimum (MIN et MAX), la somme et la somme des scores pondérés (SUM et WHT) et les scores de produit (MUL). D'après les résultats expérimentaux obtenus, illustrés dans le tableau 3.1, il est clair que les performances du système biométrique ouvert / fermé sont parfaitement améliorées lorsque la règle WHT est utilisée (EER = 0,000% ( $T_o$ = 0,3780)). Enfin, les résultats expérimentaux obtenus sont très satisfaisants car, du fait de la simplicité, de la facilité d'utilisation et de l'acceptabilité élevée de ces deux modalités biométriques, ils peuvent également être combinés avec la clé secrète pour augmenter le niveau de sécurité d'une application électronique particulière.

| | EER | | FAR at FRR = 0 | | FRR at FAR = 0 | | ROR | |
|---|---|---|---|---|---|---|---|---|
| RÈGLES DE FUSION | $T_o$ | EER | $T_o$ | FAR | $T_o$ | FRR | ROR | RPR |
| SUM | 0.3372 | 0.015 | 0.3331 | 0.017 | 0.3960 | 0.094 | 100.00 | 1 |
| WHT | 0.3780 | 0.000 | 0.3779 | 0.000 | 0.3870 | 0.000 | 100.00 | 1 |
| MAX | 0.3563 | 0.019 | 0.3515 | 0.025 | 0.4049 | 0.188 | 100.00 | 1 |
| MIN | 0.3546 | 0.075 | 0.2970 | 1.165 | 0.4680 | 0.375 | 100.00 | 1 |
| MUL | 0.2085 | 0.031 | 0.1890 | 0.124 | 0.2789 | 0.125 | 100.00 | 1 |

TABLE 3.1 – Résultats du test d'identification biométrique multimodale (à l'aide du classifieur KNN).

### *Résultats des tests du système basés sur S-DCTNet*

Étant donné que l'incorporation de la transformation du modèle biométrique affecte les performances du système, dans cette section, nous réévaluerons ces performances pour étudier le comportement du nouveau système capable de fonctionner avec des modèles biométriques révocables. Il est important de noter que, contrairement à notre système proposé, tous les systèmes développés dans la littérature ne discutent que le mode d'identification en ensemble fermé, c'est pourquoi la force de notre système réside dans sa validité à la fois dans les modes d'identification en ensemble fermé / en ensemble ouvert. De plus, l'un des avantages les plus importants de notre méthode (S-DCTNet) est qu'elle contient également la méthode originale (DCTNet). Il suffit donc de mettre toutes les matrices XORing ( $\mathcal{M}_k^b|_{k=1..L_1L_2}$) à zéro pour atteindre la méthode d'origine :

$$\mathcal{M}_k^b(i,j)|_{k=1,\cdots,L_1L_2} \to 0, \quad \forall \ \ i,j \\ \Rightarrow \ \text{S-DCTNet} \to \text{DCTNet} \tag{47}$$

Pour réduire le nombre de tests, nous avons utilisé uniquement la modalité PLM et nous avons adopté le même protocole de test que dans la partie précédente. En effet, afin d'évaluer sérieusement le système biométrique révocable proposé, deux points clés concernant son comportement doivent être examinés. Le premier, bien sûr, est la précision du système, et le second est le niveau de sécurité du système, ce qui signifie que si la clé secrète est modifiée, tous les anciens gabarits biométriques du client sont annulés et sont donc considérés comme des gabarits biométriques non autorisés. Il convient de noter que dans cet ensemble de tests, nous ajoutons uniquement la couche de transformation sans changer la méthode d'apprentissage du gabarit biométrique final, qui dépend de la technique d'histogramme par blocs. Toutes les distributions de résultats et de scores de notre système d'identification biométrique révocable (S-DCTNet) ont été obtenues sous deux clés secrètes, l'une est correcte {vraie clé $\equiv \mathcal{K}_T$ = ($x_{01}$, $y_{01}$, $z_{01}$) = (0,0156, 0,8915, 0,1474)} et l'autre est incorrect {fausse clé $\equiv \mathcal{K}_F$ = ($x_{01}$, $y_{01}$, $z_{01}$) = (0,0344, 0,1187, 0,2361)}. Premièrement, nous évaluons les performances du système avec la vraie clé secrète ($\mathcal{K}_T$) afin de resélectionner les meilleurs paramètres de notre méthode, et ce lorsque le système utilise les classifieurs KNN et SVM. Ainsi, pour évaluer le système biométrique ouvert sous les paramètres à examiner ($\eta$, $k_1^1$), nous illustrons, pour les deux classifieurs utilisés (KNN et SVM), les performances sous forme de GAR et les résultats sont présentés dans la Fig. 3.3. Ainsi, grâce à l'observation et à l'évaluation de cette figure, nous pouvons tirer trois conclusions provisoires sur la méthode proposée : *i)* les performances du système se sont légèrement détériorées par rapport au système originale (DCTNet), en particulier lors de l'utilisation du classifieur SVM, mais ils sont généralement très acceptables, *ii)* les performances du système s'améliorent toujours lorsque nous augmentons le nombre de filtres de convolution, et *iii)* le niveau de sécurité du système est quelque peu faible.

D'après la figure 3.3. *(a)*, il est clair que le système d'identification en ensemble ouvert a conservé les mêmes paramètres ($\eta = 10$, $k_1^1 = 17$) que le système basé sur le classifieur KNN (DCTNet) avec un taux d'erreur (EER) de 0,090% à un seuil $T_o$ = 0,8703 pour le classifieur KNN. Bien que cette erreur soit très acceptable, malheureusement, les performances du système, dans ce cas, ont été très dégradées par rapport au système originale, où l'EER a presque quadruplé (0,090% au lieu de 0, 0190%). De même, cette dégradation inclut également le mode d'identification en ensemble fermé où le nouveau système a donné un taux d'identification (ROR) égal à 99,9347% (RPR = 99) au lieu de 100,00% (RPR = 1) dans le système DCTNet.

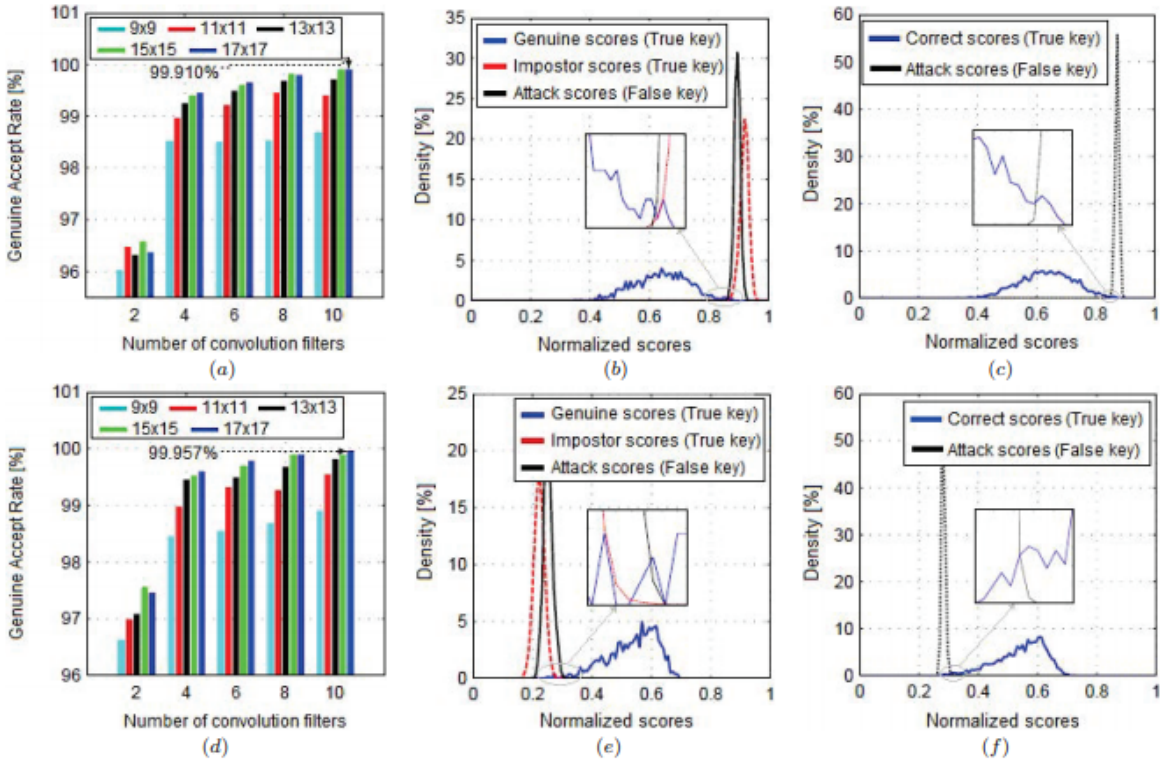



FIGURE 3.3 – Performances du système biométrique ouvert basé sur S-DCTNet (fonction de Block-wise histogram). *(a), (b), (c)* Système biométrique basé sur PLM utilisant un classifieur KNN, et *(d), (e), (f)* Système biométrique basé sur PLM utilisant un classifieur SVM.

Outre cette dégradation des performances, le niveau de sécurité n'est pas très satisfaisant. Pour clarifier cela, nous avons évalué les performances du système avec une fausse clé secrète, et tous les résultats obtenus, selon les deux modes d'identification, sont présentés dans la figure 3.3. *(b)* et la figure 3.3. *(c)*. Ces figures montrent les distributions de scores obtenues avec une clé secrète correcte ($\mathcal{K}_T$) et une autre incorrecte ($\mathcal{K}_F$). Sur la figure 3.3. *(b)*, nous pouvons clairement voir le chevauchement entre les deux distributions (distribution des scores clients obtenus par $\mathcal{K}_T$ et distribution des scores d'attaques obtenus par $\mathcal{K}_F$), ce qui explique notre jugement sur le niveau de sécurité du système. Le système étant dans ce cas destiné à fonctionner en mode d'identification à ensemble ouvert, l'acceptation ou le rejet d'un utilisateur dépend du seuil de sécurité du système ($T_o$). Par conséquent, afin de ne pas accepter les gabarits annulés, le $T_o$ doit être choisi inférieur à tous les scores d'attaque, ce qui, comme le montre la figure 3.3. *(b)*, affecte le taux d'identification du système.

| | ASR at EER | | | ASR at FAR = 0 | | | ASR at FRR = 0 | | |
|---|---|---|---|---|---|---|---|---|---|
| CLASSIFIEURS | $T_o$ | EER | ASR | $T_o$ | FRR | ASR | $T_o$ | FAR | ASR |
| KNN | 0.7030 | 0.090 | 1.273 | 0.8303 | 1.563 | 0.000 | 0.8905 | 8.461 | 17.462 |
| SVM | 0.2756 | 0.043 | 0.406 | 0.3280 | 1.438 | 0.000 | 0.2505 | 2.603 | 7.672 |

TABLE 3.2 – Performance du système biométrique ouvert à base de S-DCTNet (Caractéristique de Block-wise histogram).

Les résultats du tableau 3.2 donnent le taux de réussite d'attaque (ASR) aux trois points de fonctionnement. A partir de ce tableau, on peut remarquer que le système peut fonctionner avec un ASR de 1,273% à EER égal à 0,090% ($T_{EER}$ = 0,7030). Malheureusement, ce taux n'est pas acceptable, en particulier pour les applications qui nécessitent un haut niveau de sécurité et qui contiennent un grand nombre de clients. Au seuil $T_{FAR=0}$ = 0,8303, le système devient très sécurisé et ne peut accepter aucun gabarit déjà annulé, mais dans ce cas, le FRR augmente, ce qui affecte négativement les performances du système. Dans un système tolérant, à $T_{FRR=0}$ = 0,8905, FAR et ASR ont augmenté de manière significative et sont devenus respectivement 17,462% et 8,461%.

Dans un mode d'identification à ensemble fermé, le système non sécurisé n'a pas besoin d'un seuil pour identifier les personnes, mais parce que notre système est sécurisé, il doit donc distinguer les gabarits autorisés des gabarits annulés, et cela peut être fait facilement en utilisant un seuil de sécurité ($T_o$). Ainsi, la figure 3.3. *(c)* montre clairement le chevauchement entre les deux distributions résultant de la clé correcte et de la clé incorrecte. Dans notre système, la sélection d'un seuil égal à 0,8825 rend le ROR égal à 100,00% tandis que l'ASR devient très important à 81,125%. Pour un système hautement sécurisé, le seuil peut être choisi égal à 0,8370, dans ce cas, le ROR sera de 98,783% (ASR = 0,000%).

Nous avons également effectué un scénario d'identification en ensemble ouvert / fermé en appliquant toutes les valeurs des paramètres de $\eta$ et $k_1^1$ à l'aide du classifieur SVM, voir Fig. 3.3. A partir de la Fig. 3.3. *(d)*, la meilleure configuration est obtenue, comme dans KNN, avec dix filtres à convolution de taille 17 × 17, dans lesquels un EER de 0,043% ($T_o$ = 0,2756) a été produit. Un examen simple de la Fig. 3.3. *(e)* et du Tableau 3.2 montre que presque le même comportement envers les attaques a été maintenu dans ce système, qui fonctionne en mode d'identification ouvert. En fait, un ASR de 0,406% a été obtenu à un seuil de 0,2756%, auquel cas il s'agissait d'un EER égal à 0,043. Le système peut fonctionner avec zéro ASR au seuil de 0,3280 où EER est de 1,438%. En mode d'identification fermé (voir Fig. 3.3. *(f)*), le système fonctionne avec un ROR égal à 100,00% à un seuil $T_o$ = 0,261, mais dans ce cas, tous les modèles non autorisés ont été acceptés (ASR = 100,00% ), en raison de son chevauchement de

100%. Heureusement, un seuil égal à 0,323 permet au système de fonctionner avec un ASR nul et un ROR égal à 99,819%, ce qui est efficace par rapport à celle trouvée dans le système KNN.

On peut dire que ces résultats sont satisfaisants, mais le risque d'accepter un gabarit non autorisé (succès de l'attaque) reste possible car il n'y a pas un grand intervalle de confiance qui sépare les scores de l'attaque et celui des clients. Ainsi, la prochaine série d'expériences est utilisée pour examiner les performances du système, qui utilise la méthode HOG au lieu de l'histogramme par blocs pour former le modèle final. Dans cet ensemble d'expériences, nous utiliserons toujours le même protocole afin de choisir les meilleurs paramètres S-DCTNet. À cette fin, nous avons examiné les performances du système dans les deux modes d'identification, et les résultats obtenus sont présentés sur la figure 3.4. Il convient de noter que ces résultats peuvent changer en raison de la modification des paramètres de la méthode HOG. Dans notre travail, nous avons prédéfini ces paramètres comme 20, 0,25, 13 et 9, pour la taille du macrobloc ($b$), le taux de chevauchement des blocs ($o$), la taille des fenêtres HOG ($n_w$) et le nombre de cases d'histogramme ($n_b$), respectivement.

Un examen plus approfondi de cette figure conduit à trois points principaux : *i)* Contrairement au système précédent, l'utilisation de HOG au lieu de l'histogramme par blocs améliore considérablement les performances du système de sorte qu'il est devenu élevé pour la plupart des configurations et, dans le pire des cas, dépasse 99%, *ii)* peu de filtres peuvent donner des performances élevées, ce qui réduit le temps de traitement, et *iii)* des filtres de taille moyenne peuvent donner de meilleurs résultats. Ainsi, à partir de la figure 3.4. *(a)*, pour le système basé sur KNN, une dégradation considérable est observée par rapport au système précédent, qui utilise un histogramme par blocs. Ainsi, le système peut donner un EER de 0,216% ($T_o$ = 0,6737) au lieu de 0,090 ($T_o$ = 0,8703). Mais, d'une manière très efficace, il a réussi à séparer complètement les deux distributions (de clés secrètes correctes et incorrectes) dans les deux modes d'identification (voir Fig. 3.4. *(b)*, Fig. 3.4. *(c)*). En mode d'identification ouvert (voir Fig. 3.4. *(b)*), l'intervalle de confiance obtenu est suffisamment grand pour assurer une sécurité élevée, il est égal à 0,200. Comme le montre clairement le tableau 3.3, le système peut fonctionner avec un ASR égal à 0,000% avec un seuil $T_o \in [0{,}712 \cdot \cdot\ 0{,}9120]$. Nous resterons toujours dans le système basé sur KNN, mais maintenant nous examinerons le mode d'identification en ensemble fermé dont les distributions sont montrées sur la figure 3.4. *(c)*. Ce chiffre montre clairement que l'intervalle de confiance est légèrement abaissé à 0,1602, mais conserve toujours l'avantage d'être très sécurisé. Dans ce cas, le système peut rejeter tous les gabarits d'attaque en utilisant un seuil $T_o \in [0{,}711 \cdot \cdot\ 0{,}873]$.

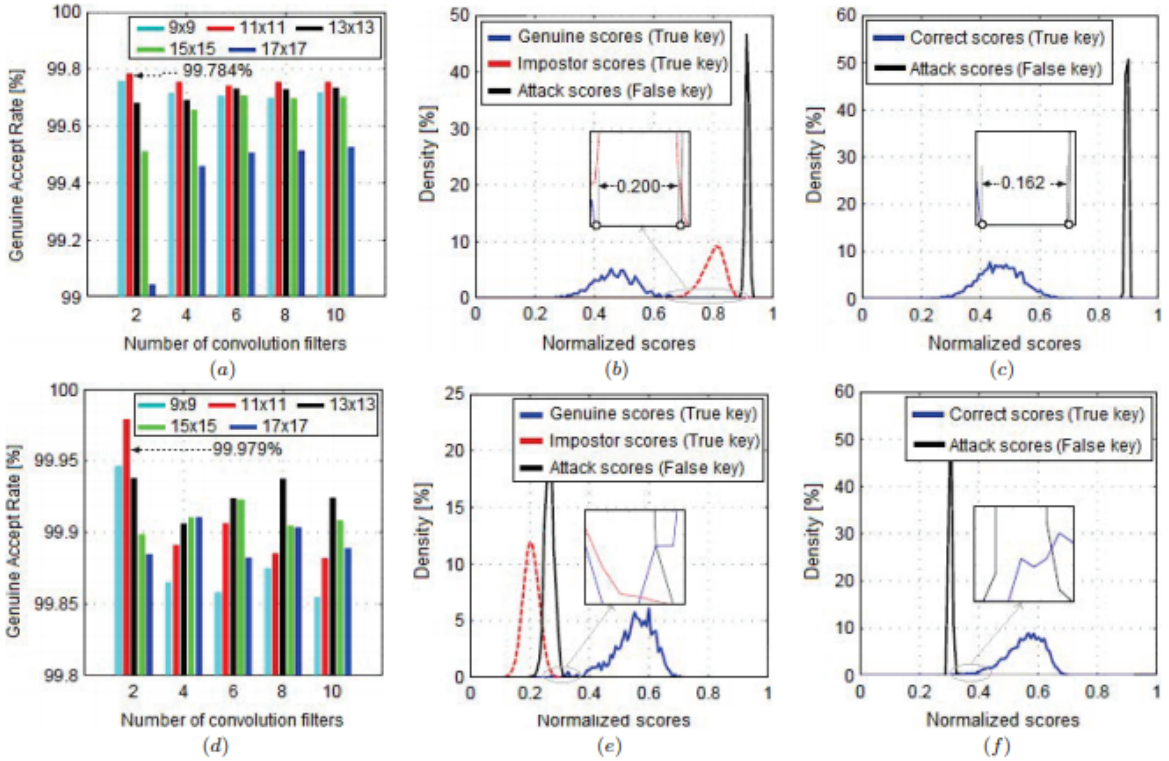



FIGURE 3.4 – Performances du système biométrique ouvert basé sur S-DCTNet (fonction de HOG). *(a), (b), (c)* Système biométrique basé sur PLM utilisant un classifieur KNN, et *(d), (e), (f)* Système biométrique basé sur PLM utilisant un classifieur SVM.

Le test final se concentrera sur le système basé sur SVM qui utilise l'algorithme HOG, dont les résultats sont illustrés dans la figure 3.4. *(d)*. La première observation très importante dans cette figure est que cette configuration peut vraiment améliorer les performances du système (EER = 0,0210 à $T_o$ = 0,2987) de 51,160% par rapport au meilleur système qui utilise un block-wise histogram. Malgré que cette configuration a réussi à améliorer les performances du système, mais une détérioration du niveau de sécurité, par rapport au système basé sur KNN, est remarquée, ce qui est clairement illustré en 3.4. *(e)* et 3.4. *(f)*. À partir du tableau 3.3, dans le point EER, le système d'identification en ensemble ouvert peut fonctionner avec un ASR égal à 1,147%, mais nous pouvons définir un autre seuil ($T_o$ égal à 0,360) afin d'atteindre un ASR nul, mais dans ce cas, le système fonctionne avec un FRR égal à 1,063%. Dans le système d'identification en ensemble fermé, une détérioration du niveau de sécurité du système a également été observée (ROR = 100,00% et ASR = 99,845% avec $T_o$ = 0,2970). Cependant, le système peut identifier presque toutes les personnes (ROR = 99,844%) à un seuil de 0,3415 avec un ASR égal à 0,000%.

| CLASSIFIEURS | ASR at EER | | | ASR at FAR = 0 | | | ASR at FRR = 0 | | |
|---|---|---|---|---|---|---|---|---|---|
| | $T_o$ | EER | ASR | $T_o$ | FRR | ASR | $T_o$ | FAR | ASR |
| KNN | 0.6737 | 0.216 | 0.000 | 0.6020 | 3.813 | 0.000 | 0.7200 | 2.782 | 0.000 |
| SVM | 0.2987 | 0.021 | 1.471 | 0.3600 | 1.063 | 0.000 | 0.2705 | 1.121 | 46.887 |

TABLE 3.3 – Performance du système biométrique ouvert à base de S-DCTNet (Caractéristique de HOG).

Toutes ces expériences peuvent être résumées comme suit :

- Premier système (SVM-S-DCTNet) : le système basé sur SVM utilisant la fonction HOG (avec $\eta = 2$, $k_1^1 = 11$) a donné de bons résultats d'identification en ensemble ouvert / fermé.
- Deuxième système (KNN-S-DCTNet) : le système basé sur KNN utilisant la fonction HOG (avec $\eta = 2$, $k_1^1 = 11$) fonctionnait bien avec un haut niveau de sécurité.

Pour cela, nous pouvons facilement utiliser le premier système pour identifier la personne, le deuxième système est utilisé pour vérifier le modèle biométrique, s'il ne s'agit pas d'un modèle annulé.

Enfin, il ne reste plus qu'à appliquer ces deux configurations à la modalité PLV pour évaluer les performances du système. Les résultats obtenus sont très proches de ceux obtenus dans le PLM, et le plus important est que le comportement du système face à l'attaque n'a pas changé dans les deux modes d'identification. Dans la même configuration, notre système d'identification à base ouverte KNN fonctionne à un taux d'erreur (EER) égal à 0,278% ($T_o = 0{,}5929$). Dans ce cas, les deux distributions sont complètement séparées et l'intervalle de confiance devient 0,187, ce qui est proche de celui de la modalité PLM. De plus, dans le mode d'identification en circuit fermé basé sur KNN, le système fonctionne avec un ROR égal à 99,844% et un RPR = 3, avec un intervalle de confiance de 1,594. Enfin, dans le système d'identification basé sur SVM, un EER de 0,062% ($T_o = 0{,}2996$) et un ROR de 99,844% ont été obtenus, respectivement pour le mode d'identification ouvert et fermé. Il convient de noter que dans ces expériences, nous avons également essayé d'améliorer le système biométrique en fusionnant les deux modalités biométriques (PLM et PLV) au niveau du score de correspondance (système multibiométrique) et les deux algorithmes (résultats KNN et SVM, ou multi- système algorithmique), mais malheureusement, tous les résultats obtenus étaient pires que le deuxième système (SVM-S-DCTNet) et cela semble logique étant donné la grande similitude entre les deux modalités biométriques (PLM et PLV) et l'énorme écart entre les taux donnés par les classifieurs KNN et SVM.

### 3.4.2 Analyse de sécurité du système biométrique

Dans la sous-partie précédente, notre système a montré des résultats très satisfaisants en ce qui concerne sa précision dans l'identification des personnes, et parce que ce système est spécifiquement conçu pour sécuriser les gabarits biométriques, dans cette sous-partie, nous effectuerons une analyse de sécurité pour évaluer sa robustesse par rapport à attaques potentielles. Il est à noter que dans notre système, connaître la clé secrète ne signifie pas récupérer le modèle d'origine (transformation irréversible), et il suffit donc d'assurer deux points importants pour assurer un niveau de sécurité élevé :

— La possibilité de générer un très grand nombre de gabarits biométriques pour la même personne tout en conservant les performances du système biométrique, et cela est lié à l'espace des clés secrètes.

— Une grande différence dans les gabarits produits pour la même personne, même si les deux clés secrètes sont très proches, et cela est lié à la sensibilité des clés secrètes.

Avant de commencer à analyser la sécurité du système, nous devons nous rappeler que notre système contient deux couches de sécurité : la couche de transformation irréversible et la couche de déguisement. Par conséquent, nous pouvons utiliser un ou les deux ensemble en tenant compte du fait que l'utilisation de la couche de déguisement seule est dangereuse si la clé secrète est récupérée. Chacune de ces deux couches est contrôlée par deux systèmes chaotiques principaux. Si nous utilisons uniquement la couche de déguisement, le système chaotique ($\mathcal{R}_2$ ou $\mathcal{Z}_2$) devient le système principal, tandis que si nous utilisons les deux couches ensemble, le système chaotique ($\mathcal{R}_1$ ou $\mathcal{Z}_1$) devient le système principal. Dans l'ensemble, la sécurité dans la couche de déguisement est assurée par le système ($\mathcal{R}_2$ ou $\mathcal{Z}_2$), tandis que la sécurité dans la couche de transformation est liée au système chaotique ($\mathcal{R}_1$ ou $\mathcal{Z}_1$) et aux systèmes chaotiques auxiliaires $L_1L_2$ ($\mathcal{L}_i|_{i=1}^{L_1L_2}$). Dans ce qui suit, nous discuterons le niveau de sécurité du système dans le cas de l'utilisation d'une couche ou des deux ensemble. En général, les paramètres qui contrôlent la sécurité de notre système sont les états initiaux de $\mathcal{R}_1$ et $\mathcal{R}_2$ ($\{x_{0i}, y_{0i}, z_{0i}\}_{i=1}^{2}$), les paramètres de contrôle de $\mathcal{L}_i$ ($\mu^i|_{i=1}^{L_1L_2}$) et ($L_1L_2$+3) valeurs entières ($\xi_x^2$, $\xi_y^2$, $\xi_z^2$ et $\xi_{\mathcal{L}_i}^1|_{i=1}^{L_1L_2}$).

#### Analyse de l'espace de clé

Nous allons essayer, dans cette sous-partie, de calculer l'espace des clés secrètes, ce qui permet à un attaquant de récupérer le gabarit biométrique. Ainsi, nous calculons séparément l'espace des clés secrètes pour chaque système chaotique afin de l'utiliser pour calculer l'espace total des clés secrètes pour le système.

| configuration | système chaotique | couche de protection | espace de clé pour | |
|---|---|---|---|---|
| | | | $\eta$=2 | $\eta$=8 |
| 1 | $\mathcal{R}_2$ | déguisement | $0.5900{\cdot}10^{50}$ | $0.5900{\cdot}10^{50}$ |
| 2 | $\mathcal{Z}_2$ | | $0.1174{\cdot}10^{48}$ | $0.1174{\cdot}10^{48}$ |
| 3 | $\mathcal{R}_1$, $\mathcal{L}_i$ | transformation | $0.8584{\cdot}10^{85}$ | $1.3508{\cdot}10^{175}$ |
| 4 | $\mathcal{R}_1$, $\mathcal{T}_i$ | | $2.6448{\cdot}10^{80}$ | $6.8265{\cdot}10^{179}$ |
| 5 | $\mathcal{Z}_1$, $\mathcal{L}_i$ | | $3.6980{\cdot}10^{82}$ | $2.6879{\cdot}10^{172}$ |
| 6 | $\mathcal{Z}_1$, $\mathcal{T}_i$ | | $5.5446{\cdot}10^{83}$ | $1.3584{\cdot}10^{177}$ |
| 7 | $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{L}_i$ | déguisement & transformation | $3.2113{\cdot}10^{91}$ | $7.9697{\cdot}10^{224}$ |
| 8 | $\mathcal{R}_1$, $\mathcal{R}_2$, $\mathcal{T}_i$ | | $4.5702{\cdot}10^{86}$ | $4.0276.10^{229}$ |
| 9 | $\mathcal{Z}_1$, $\mathcal{Z}_2$, $\mathcal{L}_i$ | | $6.3901{\cdot}10^{88}$ | $3.1556{\cdot}10^{219}$ |
| 10 | $\mathcal{Z}_1$, $\mathcal{Z}_2$, $\mathcal{T}_i$ | | $9.5811{\cdot}10^{89}$ | $1.5947{\cdot}10^{224}$ |

TABLE 3.4 – Espace des clés secrètes du système sous toutes les configurations possibles.

Puisque nos clés sont des valeurs réelles, l'espace des clés secrètes est calculé en utilisant toutes les erreurs absolues moyennes ($\mathcal{E}$) [88] entre deux séquences générées par deux clés secrètes proches. Soit $\mathcal{S}^{\varrho}$ et $\widetilde{\mathcal{S}}^{\varrho}$ ($\varrho \equiv$ {x, y, z}) deux séquences créées par le même système chaotique ($\mathcal{R}_i|_{i=1}^{2}$), où $\mathcal{S}^{\varrho}$ est créé par l'état initial $\varrho_0$ et $\widetilde{\mathcal{S}}^{\varrho}$ par l'initiale état $\varrho_0$ + d, où d est une légère différence. L'erreur absolue moyenne ($\mathcal{E}_{\varrho}|_{\varrho=\{x,y,z\}}$) pour le système chaotique est définie comme suit :

$$\mathcal{E}_{\varrho}(\mathcal{S}^{\varrho}, \widetilde{\mathcal{S}}^{\varrho}) = \frac{1}{L^{\varrho}} \sum_{j=1}^{L^{\varrho}} |\mathcal{S}^{\varrho}(j) - \widetilde{\mathcal{S}}^{\varrho}(j)| \qquad (48)$$

où $L^{\varrho}$ désigne la longueur de la séquence $\mathcal{S}^{\varrho}$. L'espace clé pour chaque valeur initiale ($\varrho_0$), appelé $s_{\varrho}$, est égal à $1/d_{\varrho}$, où $d_{\varrho}$ est la valeur de $d$ pour laquelle $\mathcal{E}_{\varrho} = 0$.

*1) Espace des clés secrètes pour le système principal :* Dans notre travail, nous avons utilisé deux systèmes chaotiques principaux ($\mathcal{R}_i$ pour Rössler et $\mathcal{Z}_i$ pour Lorenz), pour cela, nous calculerons séparément l'espace des clés secrètes pour chaque système : Pour les deux systèmes chaotiques, nous utilisons les conditions suivantes : La longueur des séquences ($\mathcal{S}^{\varrho}$) est égale à 120 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 :

- *Système Rössler ($\mathcal{R}_i$) :*

($s_x$, $s_y$, $s_z$) = (0,3020·$10^{17}$, 0,1479·$10^{18}$, 0,1318·$10^{17}$)

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

$$S^{r}(\mathcal{R}_i) = s_x \cdot s_y \cdot s_z = 0.5900 \cdot 10^{50} \qquad (49)$$

- *Système Lorenz ($\mathcal{R}_i$) :*

$(s_x,\ s_y,\ s_z) = (0.8317{\cdot}10^{14},\ 0.1445{\cdot}10^{18},\ 0.9772{\cdot}10^{16})$
L'espace total des clés secrètes est alors égal à :

$$S^z(\mathcal{Z}_i) = s_x \cdot s_y \cdot s_z = 0.1174 \cdot 10^{48} \tag{50}$$

*2) Espace des clés secrètes pour les systèmes chaotiques auxiliaires :* L'espace des clés secrètes dans les systèmes chaotiques $\{\mathcal{L}_i,\ \mathcal{T}_i\}|_{i=1}^{L_1L_2}$ peut être calculé de la même manière. Les états initiaux des systèmes logistiques auxiliaires étant contrôlés par le premier système principal, son espace clé secret ne concerne donc que leurs paramètres de contrôle $(\mu_i|_{i=1}^{L_1L_2})$. Pour les deux systèmes, les résultats suivants ont été calculés par des séquences de longueur 16384 et des états initiaux égaux à $x_{0i}|_{i=1}^{L_1L_2}$.

- *Système logistique ($\mathcal{L}_i$) :* $s_u^i = 0.4677{\cdot}10^{16}$

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

$$S^l(\mathcal{L}_i) = \Pi_{i=1}^{L_1L_2} s_u^i = (0.4677)^{L_1L_2} \cdot 10^{16L_1L_2} \tag{51}$$

- *Système Tent ($\mathcal{T}_i$) :* $s_u^i = 0.1811{\cdot}10^{17}$

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

$$S^l(\mathcal{L}_i) = \Pi_{i=1}^{L_1L_2} s_u^i = (0.1811)^{L_1L_2} \cdot 10^{17L_1L_2} \tag{52}$$

Après cela, nous avons calculé l'espace total des clés secrètes du système sous toutes les configurations possibles, et les résultats obtenus sont présentés dans le tableau 3.4. Il convient de noter que nous avons utilisé le meilleur cas trouvé dans l'évaluation des performances de la biométrie système, qui est $\eta = L_1L_2 = 2$ filtres de convolution. Ce tableau montre clairement l'efficacité de notre système, afin qu'il puisse fonctionner avec de grands espaces clés ($\simeq 10^{91}$) qui le rendent très sécurisé. Bien entendu, l'utilisation de deux couches de protection augmente efficacement la sécurité du système, qui peut être multipliée en augmentant le nombre de filtres et le nombre de stages du système.

comme nous l'avons dit, nous avons utilisés le meilleur cas trouvé dans l'évaluation des performances qui est $\eta = L_1L_2 = 2$ filtres de convolution, au lieu de cela, nous pouvons utiliser ($\eta = L_1L_2 = 8$, $k_1^1 = 13$) avec un EER = 0,613% en ensemble ouvert et ROR = 99.844% (RPR = 4) en ensemble fermé pour SVM et un EER = 0,27% en ensemble ouvert et ROR = 99.844% (RPR = 5) en ensemble fermé pour KNN afin d'augmenter la sécurité du système avec des espaces clés énormes ($\simeq 10^{229}$) et en même temps les performances du système encore très acceptables pour l'identification des personnes.La même chose pour le PLV, les résultats obtenus sont très proches de ceux obtenu dans le PLM avec les mêmes paramètres ($\eta = L_1L_2 = 8$, $k_1^1 = 13$).

***Analyse de sensibilité de clé***

Afin de tester la sensibilité du système aux légères variations de la clé, nous testons dans cette sous-partie le comportement du système résultant de nombreuses clés secrètes les plus proches. Par conséquent, nous avons utilisé trois clés différentes : une clé correcte ($\mathcal{K}$) et deux clés incorrectes plus proches de la bonne clé par $d_\varrho = 10^{-16}$ ($\mathcal{K}_1$) et $d_u = 10^{-16}$ ($\mathcal{K}_2$). Afin d'évaluer le niveau de sécurité, nous avons inscrit toutes les personnes avec la bonne clé ($\mathcal{K}$), puis nous avons testé l'identification en ensemble ouvert / fermé, en utilisant la modalité PLM, avec les trois clés ($\mathcal{K}$, $\mathcal{K}_1$ et $\mathcal{K}_2$). Les performances du système sous les trois touches sont illustrées sur la figure 3.5.

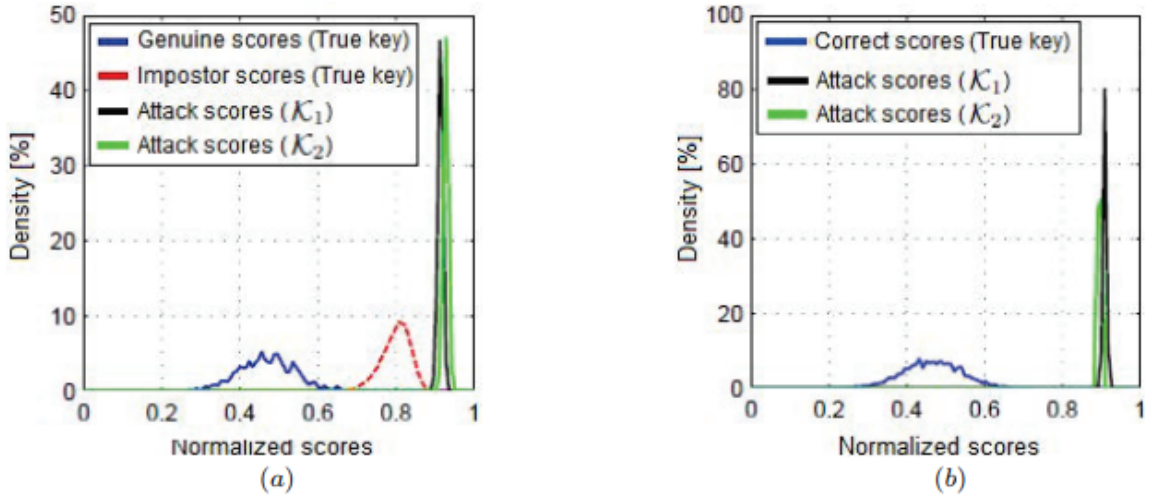



FIGURE 3.5 – Performances du système d'identification basé sur S-DCTNet ouvert / fermé sous des clés secrètes correctes et incorrectes. *(a)* Système d'identification en ensemble ouvert, et *(b)* Système d'identification en ensemble fermé.

Pour les systèmes d'identification ouverts, la Fig. 3.5. *(a)* présente la distribution des scores authentiques et imposteurs obtenus en utilisant la bonne clé ($\mathcal{K}$) ainsi que la distribution des scores authentiques lors du changement de clé en raison d'une attaque (scores obtenus par des clés autres que la bonne clé secrète, donc de mauvaises clés ($\mathcal{K}_1$ et $\mathcal{K}_2$). Dans cette figure, il est clair que tous les scores d'attaque sont complètement déplacés au-dessus du seuil de sécurité ($\gg T_o$), et sont ainsi devenus des scores d'imposteurs pour le système. De plus, un plus grand intervalle de confiance entre les scores réels et d'attaque a été obtenu, ce qui reflète l'efficacité et la robustesse de notre système biométrique révocable proposé contre toute attaque possible.

Semblable au mode d'identification en ensemble ouvert, la figure 3.5. *(b)* montre les distributions de score correctes et incorrectes (dues aux attaques) obtenues en utilisant la bonne clé et les mauvaises clés dans le mode d'identification en ensemble fermé, où nous pouvons clairement voir la grande séparation des différentes distributions et cela indique l'efficacité de cette méthode. Une analyse sérieuse des résultats précédents

montre que globalement, notre méthode peut améliorer considérablement le niveau de sécurité du système grâce à l'utilisation du principe de révocabilité, ce qui permet de les utiliser dans des applications nécessitant une haute sécurité.

## 3.5 Conclusion

Ce chapitre est consacré à la conception des systèmes biométriques avec et sans protection, nous avons implémenté la méthode S-DCTNet pour sécuriser notre système en utilisant 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 dans notre méthode. De plus, notre méthode peut fonctionner efficacement avec de très grands espaces clés, surtout si le nombre de couches convolutionnelles et de filtres utilisés augmente.

# Conclusion Générale

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 simple 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 gabarits ont attiré l'attention des chercheurs en raison de leur haute sécurité par rapport à celles basées 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 (DCTNet) 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 afin 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 très efficaces dans les systèmes de sécurité de l'information. De plus, nous avons utilisé l'une des techniques les plus importantes en cryptographie, qui est *fuzzy vault* en raison de sa simplicité et de son efficacité. Les expériences ont été réalisées sur une base de données moyenne contenant 400 personnes représentées chacune par deux modalités biométriques efficaces, à savoir l'empreinte palmaire et la veine palmaire. 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. De plus, notre méthode peut fonctionner efficacement avec de très grands espaces clés, surtout si le nombre de couches convolutionnelles et de filtres utilisés augmente. Les travaux futurs de cette étude se concentreront sur l'utilisation d'autres techniques d'apprentissage en profondeur comme CNN 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

Il existe dans la littérature de nombreuses métriques pour quantifier la performance du système. On ne s'intéressera dans cette section qu'aux mesures des taux d'erreur et aux courbes de performance.

## A.1 Les mesures des taux d'erreur

La performance d'un système biométrique peut se mesurer principalement à l'aide de trois critères : sa précision, son efficacité (vitesse d'exécution) et le volume de données qui doit être stocké pour chaque personne. il existe plusieurs indicateurs d'erreur qui peuvent être utilisés pour évaluer leur performance [89].

• *Le taux d'échec à la capture (Failure to Acquire Rate, FTA)* qui est la proportion des tentatives de captures pour lesquelles le système ne peut pas détecter un échantillon biométrique.[90]

• *Le taux d'échec à l'enrôlement (Failure To Enroll Rate, FTER)* qui mesure la proportion des individus pour lesquels le système ne peut pas créer de modèle biométrique.[90]

• *La fausse acceptation(False Acceptance,FA)* lorsque le système déclare l'individu comme étant légitime alors que c'est un imposteur.[90]

• *Le faux rejet (False Rejection, FR)* lorsque le système refuse un individu alors qu'il s'agit d'un utilisateur légitime.[90]

• *Le taux des fausses acceptations (False Acceptance Rate, FAR)* qui mesure la proportion des fausses acceptations par rapport au nombre total des transactions imposteurs.[90]

• *Le taux des faux rejets (False Rejection Rate, FRR)* qui mesure la proportion des faux rejets par rapport au nombre total des transactions légitimes.[90]

• *Le taux d'égale erreur (Equal Error Rate, ERR)* qui indique le taux d'erreur lorsque le système est configuré de manière à avoir le FAR égal au FRR.[90]

• *Le Zéro FRR* qui est défini comme le plus faible FAR lorsqu'aucun faux rejet ne

survienne.[90]
• *Le Zéro FAR* qui est défini comme le plus faible FRR lorsqu'aucune fausse acceptation ne survienne.[90]

Pour qualifier la fiabilité d'un système biométrique, l'EER est généralement le plus utilisé. Plus il est faible, plus le système est performant. Néanmoins, il est tout aussi intéressant de considérer le Zéro FAR qui, en général, est plus intéressant pour les cas pratiques.[90]

## A.2 Les courbes de performance

Pour visualiser les performances des systèmes biométriques lorsque le seuil varie, nous utilisons des courbes de performance. Les courbes de performance les plus utilisées sont :
• *Courbe de distributions des scores client et imposteur* : Pour évaluer la précision d'un système biométrique, nous devons calculer des scores à partir des échantillons biométriques appartenant à une même personne, et des scores issus des échantillons biométriques de différentes personnes. La distribution des scores issus des échantillons biométriques appartenant à une même personne est appelée distribution des personnes clients. La distribution de scores issus d'échantillons biométriques de différentes personnes est appelée distribution des imposteurs. La figure (A.1) illustre les distributions des scores client et des scores imposteur. Il est clair d'après cette figure que si le seuil *To* varie, les valeurs respectives de FAR et FRR changent.[17]
• *Courbe de variation des FAR et des FRR en fonction du seuil de décision* : Comme nous l'avons vu auparavant, les performances d'un système biométrique (vérification ou identification ensemble ouvert) sont généralement évaluées suivant les FAR et FRR. Il est à noter que ces deux taux sont très corrélés et si l'un d'eux augmente l'autre diminue.[17]

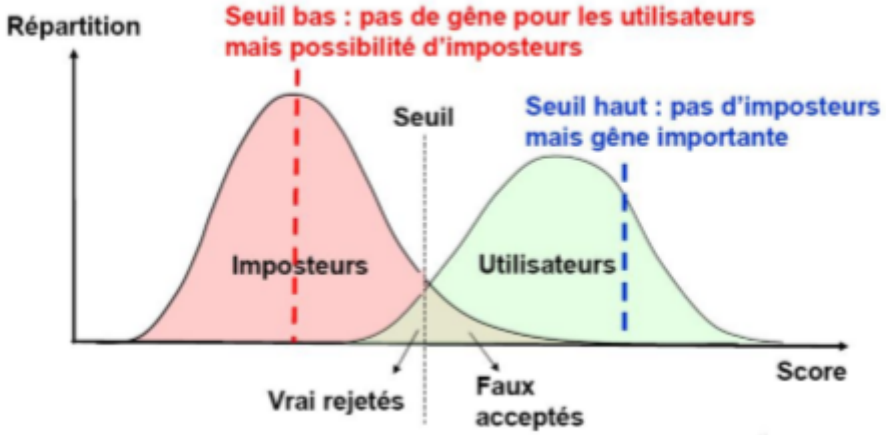



FIGURE A.1 – Distributions des scores client et des scores imposteur.[17]

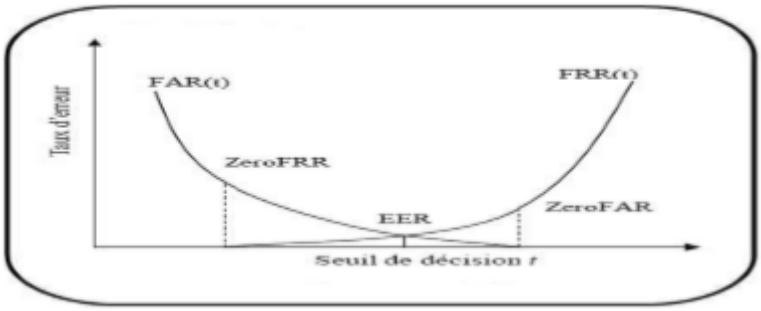



FIGURE A.2 – Variation des FRR et des FAR en fonction du seuil.[17]

La corrélation entre les FAR et de les FRR est illustrée par la figure(A.2). Elle est principalement due à la difficulté d'isoler les deux distributions client et imposteur. Sur cette figure, nous pouvons lire les valeurs des taux d'erreur pour chaque valeur du seuil. En plus, le seuil du point EER, correspond au seuil pour lequel les FAR et les FRR sont égaux, est l'intersection des deux courbes.

• *La courbe réceptrice des caractéristiques (ou la courbe ROC)* : illustrée par la figure (A.3) cette courbe trace le FRR en fonction du FAR. Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé [17].


FIGURE A.3 – Exemple de Courbe ROC.[17]

# Annexe B

# Chaos et cryptographie

La sécurisation de la chaîne de transmission devient de plus en plus nécessaire avec l'évolution des communications en termes de nombre d'utilisateur et nature d'information à transmettre. Durant ces années, des nouvelles méthodes de modulation basées sur le chaos dans les systèmes de transmission sont développées.[91]

Les différentes possibilités d'utiliser les signaux chaotiques en cryptographie s'articulent aujourd'hui autour de deux directions principales de travail : l'utilisation de chaos pour crypter les messages à transmettre et l'utilisation de chaos pour l'échange d'un secret commun servant de clé de communication entre interlocuteurs autorisés. Ces deux directions sont indépendantes et compatibles entre elles : elles peuvent donc être réunies au sein d'un même système final.[92]

## B.1 Principe du cryptosystème basée chaos

Plus tard, le chaos et suite a ses propriétés (que nous détaillons dans le paragraphe suivant) a été introduit dans le chiffrement des données. Les algorithmes de chiffrement chaotique utilisent des nombres pseudo-aléatoires générés par les fonctions (ou générateurs) chaotiques. Une fonction est dite chaotique, si elle est non linéaire et surtout si elle est sensible aux modifications, même extrêmement faibles de la valeur de la clé secrète qui est formée des conditions initiales et des paramètres du système[93]. La séquence de nombre pseudo-aléatoire générée est utilisée par l'algorithme chaotique pour chiffrer le message en clair comme montre la figure B.1.

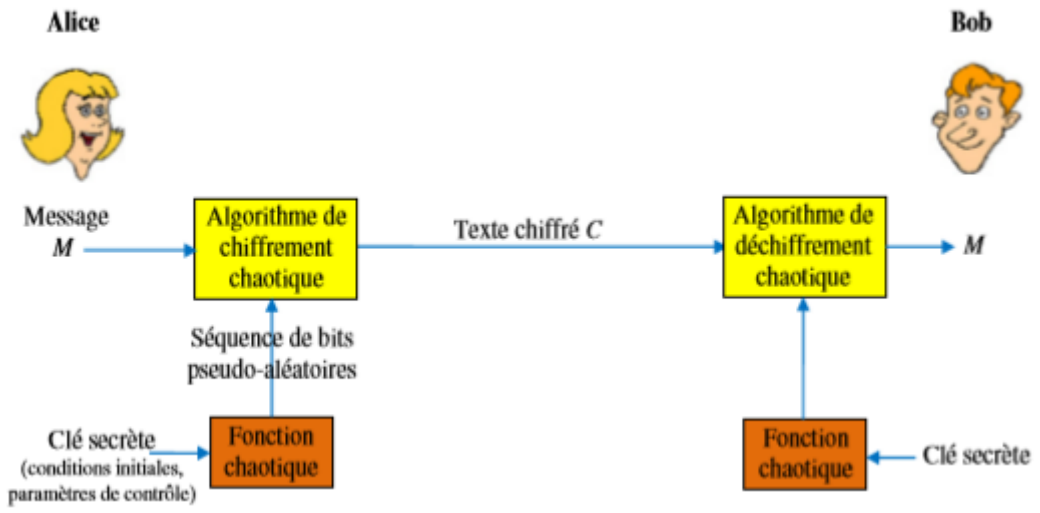



FIGURE B.1 – Schéma de principe d'un cryptosystème basé chaos.[93]

À la réception, la même fonction chaotique est utilisée par Bob avec la même clé secrète pour générer la même séquence de nombres pseudo-aléatoires. Cette séquence sera utilisée par un algorithme de déchiffrement chaotique afin de récupérer le message en clair qui peut être des données numériques, une image, un texte, etc. Parmi les fonctions chaotiques, il y a la carte : *logistique, PWLCM, Frey, et Skew tent map.* Ces fonctions chaotiques sont des systèmes de récurrence. En effet, une simple fonction de récurrence peut produire des dynamiques chaotiques assez complexes et riches.

La plupart des algorithmes de chiffrement/ déchiffrement basé chaos développés dans la littérature, sont des algorithmes à clé symétrique pour le chiffrement par bloc ou par flux.[93]

## B.2 Propriétés cryptographiques et chaotiques

La similarité entre les propriétés des fonctions chaotiques et les propriétés que nous trouvons dans les systèmes cryptographiques ont conduit au développement des cryptosystèmes basé chaos comme celui présenté dans la figure B.1. Nous allons citer les principaux requis cryptographiques ainsi que les propriétés des fonctions chaotiques afin de montrer la correspondance entre les deux.[93]

Les besoins cryptographiques essentiels sont[93] :

1. *Sensibilité aux clés* : un changement d'un bit de la clé génère un texte chiffré totalement différent pour le chiffrement d'un texte en clair identique.
2. *Sensibilité au texte en clair* : un changement d'un bit de texte en clair change totalement le texte chiffré, même si la même clé est utilisée.
3. *Texte chiffré aléatoire* : le texte chiffré doit avoir un fort caractère aléatoire.

Les propriétés des fonctions chaotiques correspondantes aux besoins précédents sont [93] :

1. *Sensibilité aux paramètres* : une petite variation des paramètres de contrôle génère deux trajectoires chaotiques très différentes même si elles partent de la même condition initiale.
2. *Sensibilité aux conditions initiales* : deux systèmes chaotiques qui partent des conditions initiales qui différent de très peu auront des trajectoires très différentes.
3. *Ergodicité* : les trajectoires qui partent des points arbitraires ont une distribution uniforme.
4. *Dynamique et déterministe* : avec un comportement apériodique pour les systèmes dynamiques à temps continu et périodique pour les systèmes à temps discrets.

Comme on voit, la correspondance est claire entre les trois besoins cryptographiques et les trois premières propriétés chaotiques.

## B.3 Les cartes chaotiques

Les cartes chaotiques sont des systèmes dynamiques définis en réel par des relations de récurrence :

$$x_i(n) = f\big(x_1(n-1), x_2(n-1), \ldots, x_m(n-1)\big), \qquad i = 1, 2, \cdots m$$

où $x \in S$, $f : S^m \longrightarrow S^m$ est une fonction de $m$-dimensions, $S^m \subset [0,1]^m$ ou $[-1,1]^m$

Certaines cartes chaotiques mono-dimensionnelles, comme la carte Logistique, la carte PWLCM (Piecewise Linear Chaotic Maps), et la carte Skew tent et des cartes chaotiques bidimensionnelles telles que : les cartes Cat, Standard, Hénon et Lozi sont bien étudiées dans la littérature et largement utilisées pour la conception de générateurs de nombres aléatoires et comme fonctions de substitution, de permutation, voire de diffusion, dans les différentes couches des cryptosystèmes basés chaos.[94]

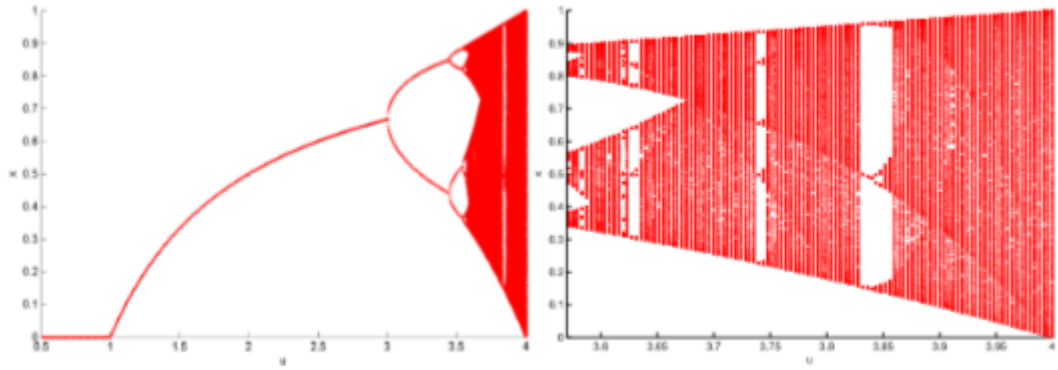
Nous allons voir un exemple de carte chaotique de base dans la partie suivante.

### B.3.1 Carte Logistique

La *suite logistique* (*logistic map* en anglais) est une suite simple qui est définie par récurrence. Cette suite est caractérisée par une récurrence qui n'est pas linéaire. Mathématiquement, la suite logistique est définie comme suit :

$$x_{n+1} = \mu x_n(1 - x_n)$$

Selon la valeur de $\mu$, nous pouvons observer un comportement chaotique dans l'intervalle [3.5699456, 4] (Figure B.2). On appelle cette propriété : *la sensibilité aux conditions initiales* (*SIC* ou *Sensitivity to Initial Conditions* en anglais) comme on a mentionné dans la section précédente. D'une manière simple, SIC veut dire que si nous avons un petit changement / perturbation arbitraire dans les conditions actuelles, alors on va avoir un comportement futur significativement très différent. En exploitant cette propriété de la suite logistique, elle a été utilisée dans plusieurs applications, y compris la sécurité des informations. Par exemple, les séquences aléatoires de la zone chaotique peuvent être utilisées pour sécuriser cryptographiquement les canaux de transmission dans les systèmes biométriques et dans les systèmes de télécommunications également.[94]



(a) Intervalle *[0.5, 4]* (b) Intervalle chaotique *[3.5699456, 4]*

FIGURE B.2 – Implémentation de la suite logistique.[94]

# Bibliographie


[1] V. Phartchayanusit, S. Rongviriyapanish. “Safety Property Analysis of Service-Oriented IoT Based on Interval Timed Coloured Petri Nets”, In : 15th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2018.

[2] Husam Rajab, Tibor Cinkelr. “IoT based Smart Cities”, In : International Symposium on Networks, Computers and Communications (ISNCC) Rome, Italy, 2018.

[3] J. Blasco, T. M. Chen, J. Tapiador, and P. Peris-Lopez. “A survey of wearable biometric recognition systems”, In : ACM Comput. Surv., 2016, vol. 49, no. 3, p. 43.

[4] Unar J, Seng W, Abbasi A. “A review of biometric technology along with trends and prospects”, In : Pattern Recognit, 2014, vol. 47, no 8, pp. 2673–2688.

[5] Salami MJ, Eltahir W, Ali H. “Design and evaluation of a pressure based typing biometric authentication system”, In : Riaz Z (ed.), Biometric Systems, Design and Applications, InTech, 2011, pp. 235-262.

[6] L. Nanni, S. Ghidoni and S. Brahnam. “Handcrafted vs. nonhandcrafted features for computer vision classification”, In : Pattern Recognition, 2017, vol.71, pp. 158-172.

[7] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain. “Biometric cryptosystems : issues and challenges”, In : Proceedings of the IEEE, 2004, vol. 92, no. 6, pp. 948-960.

[8] Onur Can Kurban, Tulay Yildirim, Ahmet Bilgic. “A multi-biometric recognition system based on deep features of face and gesture energy image”, In : INISTA, 2017, pp. 361-364.

[9] A. K. Jain, K. Nandakumar, and A. Nagar. “Biometric template security”, In : EURASIP Journal on advances in signal processing, 2008, 113.

[10] Dang T, Truong Q, Le T, Truong H. “Cancelable fuzzy vault with periodic transformation for biometric template protection”, In : In : IET Biometrics, 2016, 5(3), pp. 229– 235.

[11] Rathgeb, C., Uhl, A. “A survey on biometric cryptosystems and cancelable biometrics”, In : EURASIP Journal on Information Security, 2011.

[12] J. Yu, B. Zhang, Z. Kuang, D. Lin, and J. Fan. “iPrivacy : Image privacy protection by identifying sensitive objects via deep multi-task learning”, In : IEEE Trans. Inf. Forensics Security, 2017, vol. 12, no. 5, pp. 1005-1016.

[13] Gregory, P. & Simon, M. A. Biometrics for dummies, John Wiley & Sons, 2008.(ISBN :0470292881 9780470292884).

[14] Max Chasse. La biometrie au québec : Les enjeux. 2002.

[15] Soltane, M., & Bakhti, M. Multi-modal biometric authentications : concept issues and applications strategies. International Journal of Advanced Science and Technology, 2012, vol. 48.

[16] N. V. Boulgouris, K. N. Plataniotis and E. Micheli-Tzanakou., “Biometrics : Theory, Methods,and Applications”, David B. Fogel, Series Editor, Willy publisher, IEEE Press on Computational Intelligence, 2010.

[17] MERAOUMIA, A. Modelé de Markov caché applique à la multi-biométrie, UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOMEDIENNE, 2014.

[18] BENNACEUR, B. & DJERADI, F. Sécurité des systèmes multi-biométriques, Centre Universitaire Belhadj Bouchaib d’Aïn-Témouchent, 2019.

[19] J. Wayman, A. Jain, D. Maltoni and D. Maio, “Biometric Systems, Technology, Design and Performance Evaluation”, Springer, London, 2005.

[20] Y. H. Pang, A. TeohBeng Jin, D. Ngo, and C. Ling, “Palmprint Authentication System Using Wavelet based Pseudo Zernike Moments Features”, Inter Journal of The Computer, the Internet and Management, Vol. 13, No.2, pp. 13-26, 2005.

[21] Rui Zhao, Kunlun Li, Ming Liu, Xue Sun, “A Novel Approach of Personal Identification Based on Single Knuckle-print Image”, Asia-Pacific Conference on Information Processing-APCIP, 2009.

[22] C. Tisse, L. Martin, L. Torres and M. Robert, “Person identification technique using human iris recognition”, Proc. of Vision Interface, pp. 294-299, 2002.

[23] Cardinaux F, Sanderson C, Bengio S, “Face verification using adapted generative models”, The 6th IEEE International Conference Automatic Face and Gesture Recognition-AFGR, Seoul, pp 825-830, 2004

[24] Lajevardi, S.M. ; Arakala, A. ; Davis, S.A. , Horadam, K.J. , “Retina Verification System Based on Biometric Graph Matching”, IEEE Transactions onImage Processing, Vol. 22, No. 9, pp. 3625- 3635, 2013

[25] A. K. Jain, R. Bolle, S. Pankanti. ”Biometrics, Personal Identification in Networked Society : Personal Identification in Networked Society ”, Kluwer Academic Publishers, Norwell, MA, USA, 1998.

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

[27] J. Campbell. "Speaker recognition : a tutorial ", Proceedings of the IEEE, Vol. 85(9), pp. 1437- 1462, 1997.

[28] F. Monrose, A. Rubin. "Authentication via keystroke dynamics ", In Proceedings of the 4th ACM conference on Computer and communications security, pp. 48-56, 1997.

[29] Jain Eli and Ak Hong L Pankanti S . Promising frontiers for emerging identification market. Biometrics-Computer, 33(2) :91-98, 2000.

[30] L. Nanni and A. Lumini, "Fusion of color spaces for Ear Authentication", Pattern Recognition, Vol.42, No.9, pp.1906-1913Sept. 2009.

[31] S. Purushotham, and M. Anouncia„ "Enhanced Human Identification System Using Dental Biometrics", The 10th WSEAS International Conference on Neural Networks, Prague, Czech Republic, pp. 120 -125, 2009.

[32] Choras, M., "Lips Recognition for Biometrics", Advances in Biometrics, pp. 1260-1269, 2009.

[33] Martin D. Gibbs, "Biometrics : body odor authentication perception and acceptance", ACMSIGCAS Computers and Society, Vol.40, No.4, pp.16-24, Dec 2010.

[34] Chetana Hegde, Rahul Prahu H, Sagar D S, P Deepa Shenoy, Venugopal K R and L M Patnaik, "Heartbeat biometrics for human authentication", Signal, Image and Video Processing, Vol. 5, No. 4, pp 485-493, Nov. 2011.

[35] Zorkadis, V., & Donos, P., "On biometrics-based authentication and identification from a privacyprotection perspective : Deriving privacy-enhancing requirements", Information Management & Computer Security, Vol. 12, No. 1, pp. 125-137, 2004.

[36] AK Jainand A. Kumar, "Biometrics of next generation : An overview", Second GenerationBiometrics, Springer, 2010.

[37] Wu S.Q., Gu Z.H., Chia S.H, "Infrared facial recognition using modified blood perfusion", International conference on information, communication and signal processing, ICICS, Singapore, pp. 1-5, 2007.

[38] GHACHOUA, A., & KAHLAOUI, I. Reconnaissance de personnes en utilisant L'empreintes Palmaires multispectral basés sur L'apprentissage approfondi, UNIVERSITE KASDI MERBAH OUARGLA, 2016.

[39] KIBOU, S., & ZIDANE, A. L'identification multi vue multimodale des individus en utilisant la fusion au niveau de décision et de scores, Mémoire master, Université Hassiba Ben Bouali Chlef, 2018.

[40] YADDADEN, Y. & SERIR, A. Authentification et/ou Identification Biométriques. Université des Sciences et de la Technologie de Houari Boumediene, 2013.

[41] Morizet, N. Reconnaissance biométrique par fusion multimodale du visage et de l'iris, Doctoral dissertation, Télécom ParisTech, 2009.

[42] Perronnin, F. & Dugelay, J. L. Introduction à la biométrie Authentification des individus par traitement audio-vidéo. Traitement du signal, 2002, vol. 19, no 4.

[43] El-Abed, M. Évaluation de système biométrique, Doctoral dissertation, Université de Caen, 2011.

[44] J. Ruiz-del-Solar, C. Devia, P. Loncomilla and F. Concha, "Offine signature very cation using local interest points and descriptors", Progress in Pattern Recognition, Image Analysis and Applications,Lecture Notes in Computer Sciences, Vol. 5197, pp.22-29, 2008.

[45] Allano, L. (2009). La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles, Doctoral dissertation, Evry, Institut national des télécommunications, 2009.

[46] Ku Shahna, Anuj Mohamed. "An Image Encryption Technique Using Logistic Map and Z-Order Curve", In : IEEE International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR), 2018, Ernakulam, India, pp. 16.

[47] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(03) :614–634, 2001.

[48] Maltoni,D., Maio, D. , Jain, A. k. et Prabhakar, S. Handbook of fingerprint recognition. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[49] Belguechi, R., Le-Goff, T., Cherrier, E., & Rosenberger, C. (2011, May). Study of the robustness of a cancelable biometric system. In Network and Information Systems Security (SAR-SSI), 2011 Conference on (pp. 1-7), IEEE.

[50] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. EURASIP Journal on Advances in Signal Processing, page 113, 2008.

[51] Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil K Jain. Biometric cryptosystems : issues and challenges. Proceedings of the IEEE, 92(6) :948-960, 2004.

[52] Jeong, M., Lee, C., Kim, J., Choi, J. Y., Toh, K. A., and Kim, J. Changeable biometrics for appearance based face recognition. In Biometric Consortium Conference, 2006 Biometrics Symposium : Special Session on Research at the (pp.1-5). IEEE (2006, September).

[53] Ari Juels et Martin Wattenberg ; A fuzzy commitment scheme.In Proceedings of the 6th ACM conference on Computer and communications security,CCS '99, pages 28–36, New York, NY, USA. ACM. 1999.

[54] Juels, A. et Sudan, M. A fuzzy vault scheme. In Proceedings of IEEE International Symposium on Information Theory, 2002, pages 408.

[55] Moujahdi, C. Protection des systèmes de sécurité biométriques : Contributions à la protection des modèles biométriques. Thèse de Doctorat, UNIVERSITÉ MOHAMMED V – AGDAL FACULTÉ DES SCIENCES Rabat, 2014.

[56] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and communications security, pages 28-36. ACM, 1999.

[57] IR Buhan, JM Doumen, PH Hartel, and RNJ Veldhuis. Constructing practical fuzzy extractors using qim. 2007.

[58] Qiming Li, Yagiz Sutcu, and Nasir Memon. Secure sketch for biometric templates. In Advances in Cryptology-ASIACRYPT, pages 99-113. Springer, 2006.

[59] Ratha, N., Connell, J., Bolle, R. M., & Chikkerur, S. Cancelable biometrics : A case study in fingerprints. In 18th International Conference on Pattern Recognition (ICPR'06), (2006, August), Vol. 4, pp. 370-373). IEEE

[60] Abhishek Nagar, Karthik Nandakumar, and Anil K Jain. Biometric template transformation : a security analysis. In IS&T/SPIE Electronic Imaging, pages 75410O-75410O. International Society for Optics and Photonics, 2010.

[61] Christian Rathgeb and Andreas Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, (1) :1-25, 2011.

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

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

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

[65] Thian Song Ong, Andrew Teoh Beng Jin, and David Chek Ling Ngo. Application-specific key release scheme from biometrics. IJ Network Security, 6(2) :127-133, 2008.

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

[67] Bhatnagar G. and Wu Q. M. J. "Chaos-Based Security Solution for Fingerprint Data during Communication and Transmission", In : Proceedings of the IEEE Transactions on Instrumentation and Measurement, 2012, vol. 61, no 4.

[68] 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

[69] 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.

[70] Li X., Jiang Y., Chen M., Li F. “Research on iris image encryption based on deep learning”, In : EURASIP Journal on Image and Video Processing, 2018, no 126.

[71] Hsiao H.I. and Lee J. “A novel fingerprint image encryption algorithm based on chaos using APFM nonlinear adaptive filter”, In : Proceedings of the IEEE 17th International Symposium on Consumer Electronics (ISCE ’13), 2013, pp. 95-96, Hsinchu, Taiwan.

[72] Abdellatef E., Ismail N.A., Abd Elrahman S. E., Ismail K.N., Rihan M. and Abd ElSamie F.E. “Cancelable multibiometric recognition system based on deep learning”, In : The Visual Computer International Journal of Computer Graphics, Springer Link, 2019.

[73] Jang Y.K., Cho N.L. “Deep Face Image Retrieval for Cancelable Biometric Authentication”, In : Proceedings of the 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2019.

[74] Liu Y., Ling J., Liu Z., Shen J., Gao C. “Finger vein secure biometric template generation based on deep learning”, In : Soft Computing, 2017, Vol. 22, pp. 2257-2265.

[75] Veeru Talreja, Matthew C. Valenti, Nasser M. Nasrabadi. “Multibiometric secure system based on deep learning”, In : IEEE Global Conference on Signal and Information Processing (Global SIP), 2017.

[76] Rathgeb C., Gomez-Barrero M., Busch C., Galbally J., Fierrez J. “ Towards cancelable multi-biometrics based on bloom filters : a case study on feature level fusion of face and iris”, In : 3rd International Workshop on Biometrics and Forensics (IWBF), 2015.

[77] D.F. Coelho, R.J. Cintra, V.S. Dimitrov. “Efficient computation of the 8-point DCT via summation by parts”, In : J. Signal Process. Syst., 2018, Vol. 90, No. 4, pp. 110.

[78] Nada Hamad, Mizanur Rahman, Saiful Islam.. “Novel remote authentication protocol using heart-signals with chaos cryptography”, In : International Conference on Informatics, Health & Technology (ICIHT), 2017, Riyadh, Saudi Arabia, pp. 1-7.

[79] A. Azzouz, R. Duhr, M. Hasler. “Bifurcation diagram for a piecewise-linear circuit”, In : EEE Transactions on Circuits and Systems , 1984, Vol. 31 , Issue : 6.

[80] 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.

[81] Peizhen Wang, Huixin Gao, Mutian Cheng, Xiaosan Ma. “A new image encryption algorithm based on hyperchaotic mapping”, In : International Conference on Computer Application and System Modeling (ICCASM), 2010, Taiyuan, China.

[82] 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.

[83] C. J. Ng and A. B. J. Teoh, DCTNet. “A simple learningfree approach for face recognition”, In : IEEE Signal and Information Processing Association Annual Summit and Conf. (APSIPA 15), 2015, pp. 761768.

[84] Hakim Bendjenna, Abdallah Meraoumia, Othaila Chergui. “Pattern recognition system : from classical methods to deep learning techniques”, In : J. Electron. Imaging, 2018 27(3), 033008.

[85] Hong Kong Polytechnic University (PolyU). “Multispectral palmprint database”, In : http ://www.comp.polyu.edu.hk/biometrics, 2013.

[86] Gurjit Singh Walia, Shivam Rishi, Rajesh Asthana, Aarohi Kumar, Anjana Gupta. “Secure multimodal biometric system based on diffused graphs and optimal score fusion”, In : IET Biometrics, 2018, Vol. 8, Issue 4, pp. 231242.

[87] A. F. H. Sallehuddin, M. I. Ahmad, R. Ngadiran and M. N. M. Isa. “Score level normalization and fusion of iris recognition”, In : 3rd International Conference on Electronic Design (ICED), 2016, Phuket, Thailand, pp. 464469.

[88] G. Bhatnagar and Q. M. J. Wu. “Enhancing the transmission security of biometric images using chaotic encryption”, In : Multimedia Syst.”, In : 2014, 20(2), pp. 203–214.

[89] BENCHENNANE, I. (2015). Etude et mise au point d’un procédé biométrique multimodale pour la reconnaissance des individus, Doctoral dissertation, University of sciences and technology in Oran, 2015.

[90] Rima Ouidad Belguechi. Sécurité des systèmes biométriques : révocabilité et protection de la vie privée. Traitement des images [eess.IV]. Ecole nationale Supérieure en Informatique Alger, 2015. Français. fftel-01230691v1f

[91] Nada REBHI, Mohamed Amine BEN FARAH, Abdennasser KACHOURI & Mounir SAMET « Analyse De Sécurité d'une Nouvelle Méthode De Cryptage Chaotique » Laboratoire d'Electronique et des Technologies de l'Information (LETI) ,2007

[92] Aïcha Essedikia, Guemidi Zoulikha, Application des systèmes chaotiques à la cryptographie. UNIVERSITE Dr. TAHAR MOULAY SAIDA 2018.

[93] Kassem Ahmad. Protocoles, gestion et transmission sécurisée par chaos des clés secrètes. Applications aux standards : TCP/IP via DVB-S, UMTS, EPS.. Electronique. UNIVERSITE DE NANTES ; UNIVERSITE LIBANAISE, 2013. Français. <NNT : ED503-196>. <tel-01104943>.

[94] Chouaib MOUJAHDI, Protection des systèmes de sécurité biométriques : contributions à la protection des modèles biométriques. UNIVERSITÉ MOHAMMED V – AGDAL FACULTÉ DES SCIENCES Rabat 2014.

[95] N. I. Cho and S.U. Lee, "Fast Algorithm and Implementation of 2-D DCT," IEEE Transactions On Circuits and Systems, vol. 38 p. 297, March 1991. rECE 802 – 602 : Information Theory and Coding Seminar 1 – The Discrete Cosine Transform : Theory and Application 31