الجمهورية الجزائرية الديمقراطية الشعبية

Republique Algerienne Democratique Et Populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة العربي التبسي - تبسة

Université Larbi Tébessi – Tébessa –

Faculté des Sciences et de la Technologie

Département de Génie Electrique

MEMOIRE

Présenté pour l'obtention du **diplôme** de **Master Académique**

En : Télécommunications

Spécialité : Réseaux et Télécommunications

Par : Hamzaoui Saoussene et Guerrad Chadia

Sujet

Protection des gabarits biométriques à l'aide de systèmes chaotiques

Présenté et évalué, le 11/06/ 2022 par le jury composé de :

M. Lotfi HOUAM	MCB	Président
M. Abdallah MERAOUMIA	Prof.	Rapporteur
Mme. Amel BOUCHEMHA	MCA	Examinatrice

Promotion : 2021/2022


بسم الله الرحمن الرحيم


وقل رب زدني علما

Dédicace

Je dédie ce travail à ma mère qui n'a jamais dit non à mes exigences, pour m'avoir toujours et jusqu'à ce jour soutenu et encouragé, Aussi pour sa douceur, sa patience et sa volonté le long de tout mon parcours. Que dieu la protège.

A mon père pour tous les sacrifices, guidé et soutenu au long de mon étude. Que dieu le protège.

A mon grand frère - Mahdi - et ma grande sœur –Nesrine - pour leur encouragement et leur aide.

A mes autres frères et sœurs pour leurs soutiens, que je souhaite tous le bonheur et la réussite.

A mes amis qui m'ont soutenue et qui ont toujours cru en moi.

A mon binôme et proche amie – chadia - pour son soutien moral et sa compréhension tout au long de ce travail.

A tous les personnes que j'ai connues, qui me sont chères et qui m'apportent aujourd'hui la joie de vivre.

Saoussene Hamzaoui

Dédicace

Je dédie ce modeste travail tout d'abord à mes parents pour leur soutien, confiance et courageux, que dieu les protège.

Aucune dédicace ne saurait être assez éloquente pour exprimer ce que vous méritez pour tous les sacrifices que vous n'avez cessés de me donner et qui m'ont permis d'être là où je suis aujourd'hui.

A me frère – Samí – pour son encouragement et son aide.

A toutes mes sœurs pour leurs soutiens et compréhensions.

A la famille Brakní - Je vous dédie ce travail en témoignage de mon grand respect et mon estime envers vous.

A mon courageux binôme et proche amie – Saoussene – pour la douce amitié et sa présence.

En souvenir des moments heureux passés ensemble, je dédie ce travail a me chère amie Drid Meriem avec mes vœux sincères de réussite, bonheur, santé.

A tous ceux que j'aime et qui m'aiment, où qu'ils soient,

A tous ce qui m'ont aidé et encouragé.

Chadia Guerrad

Remerciement

Avant tous nous remercions notre DIEU – Allah - pour tout ce qu'il nous a donné.

Puis, On tient à exprimer notre profonde gratitude et nos sincères remerciements à Monsieur Abdallah. MERAOUMIA directeur et encadrant de mémoire pour les efforts qu'il a déployés et les conseils qu'il nous a prodigués, sa patience, son soutien et sa confiance et surtout sa compréhension qui nous ont permis d'avancer et de bien mener ce travail le long de ces mois.

Nous adressons nos remerciements les plus chaleureuses à l'ensemble des membres du jury :

Mr. Houam.L , d'avoir accepté de présider ce jury.

Mme. Bouchemha.A , d'avoir accepté d'examiner ce travail.

Nous tiens aussi à remercier Monsieur Abdelhakim. FARES notre enseignant pour son suivi permanent, sa disponibilité et ses conseils pratiques qui nous ont aidés à mieux aborder et concevoir le sujet de la thèse.

Nos remerciements vont à tous ceux qui ont contribué d'une quelconque manière à l'aboutissement de ce travail.

S. Hamzaoui et C. Guerrad

Table des Matières

Liste des Figures

Liste des tableaux

Introduction Générale

Introduction

Récemment, nous assistons à une véritable révolution de l'accès à l'information dans tous les domaines de l'activité humaine, et par conséquent la sécurité des systèmes d'information est devenue une branche importante de la recherche pour assurer un accès sécurisé aux systèmes et aux organisations. Concevoir un système d'identification fiable et efficace est une étape nécessaire pour la sécurité des données, d'une part, et la confidentialité et la vie privée des utilisateurs, d'autre part. Malheureusement, certaines recherches [1] ont montré que les taux de vol de données, en particulier en ligne, ont fortement augmenté ces dernières années et que les systèmes de sécurité échouent souvent à assurer la protection nécessaire des données. En fait, diverses informations sont ciblées par des attaques telles que le vol, le plagiat et la falsification.

Il est entendu que toute donnée, qu'elle soit stockée ou via Internet, est propre à une ou plusieurs personnes morales ou physiques. De plus, toute demande d'accès à ces informations est faite par une personne bien déterminée. Par conséquent, connaître l'identité d'une personne est un facteur essentiel dans le processus de demande d'accès. Traditionnellement, il existe deux façons d'identifier l'identité d'une personne, par ce qu'elle sait (basé sur une connaissance), comme un mot de passe et un code PIN, ou par ce qu'elle possède (basé sur une possession), comme un badge ou une carte d'identité. Ces moyens présentent plusieurs faiblesses qui permettent à des personnes non autorisées de voler les données et donc de les utiliser illégalement. En effet, ces problèmes peuvent être considérablement réduits par une nouvelle technique émergente et plus fiable appelée biométrie.

En s'appuyant sur les caractéristiques humaines pour identifier/authentifier les personnes, la biométrie est devenue l'une des techniques les plus importantes utilisées pour la sécurité des systèmes d'information [2]. En effet, ses caractéristiques, qu'elles soient physiques sous forme d'empreintes digitales ou acquises sous forme comportementale, sont associées à chaque personne et ne souffrent donc pas des faiblesses des méthodes basées sur la connaissance ou la possession. La biométrie est la mesure et l'analyse statistique des caractéristiques physiques et/ou comportementales des personnes, dans le but de les distinguer.

Les systèmes biométriques ont montré certaines limites, vis-à-vis du problème de sécurité, pour cela l'adoption d'une procédure de sécurité au sein de ces systèmes peut présenter une solution partielle, puisque les systèmes souffrent encore de faiblesses. Fondamentalement, les données biométriques brutes sont stockées directement dans la base de données, c'est pourquoi lorsque les données biométriques d'un utilisateur sont compromises, l'identité personnelle et la confidentialité sont également compromises, car le gabarit biométrique ne peut pas être annulé ou réédité. L'une des procédures de sécurité utilisées est de protéger le gabarit biométrique soit dans la base de données, soit lors de la transmission. En effet, afin de sécuriser les gabarits biométriques, de nombreuses approches sont proposées dans la littérature, ces techniques de protection se divisent en deux grandes catégories : celles basées sur la cryptographie et celles basées sur la révocabilité [3]. Ainsi, la sécurité dans la première approche reste faible car si la clé de cryptage est récupérée illégalement, le gabarit biométrique peut être décodé puis volé [1]. Heureusement, dans la deuxième approche, il est impossible de reconstituer le gabarit biométrique d'origine car ce gabarit a été converti avec une fonction irréversible, il est possible de changer la fonction de conversion pour éliminer complètement l'ancien gabarit afin qu'il ne soit pas utile. Dans ce mémoire, nous avons proposé une méthode pour sécuriser les gabarits biométriques basée sur une approche hybride combinant à la fois la transformation et/ou le cryptage des gabarits. Dans cette approche, nous avons reconstruit la méthode d'extraction de caractéristiques ICANet/PCANet pour pouvoir extraire un modèle précis et révocable. Nous avons ajouté deux couches à cette méthode, une pour la transformation du gabarit et l'autre pour le cryptage du gabarit afin d'améliorer sa protection. Notre méthode repose également sur des systèmes chaotiques pour produire les matrices de transformation en raison de son extrême sensibilité aux conditions initiales. Ces systèmes se sont récemment révélés très efficaces dans les systèmes de sécurité de l'information.

Pour atteinte notre objectif, ce manuscrit est organisé en trois chapitres:

Le **premier chapitre** contient un aperçu des méthodes les plus importantes utilisées pour la sécurité de l'information. Dans ce chapitre, tout ce qui concerne l'utilisation des technologies biométriques dans le processus d'identification/vérification de l'identité des personnes est également couvert.

Dans le **deuxième chapitre**, nous aborderons d'abord les méthodes de protection des gabarits biométriques (en particulier la biométrie révocable). Ensuite, nous présenterons la carte logistique et son rôle dans la protection des gabarits biométriques.

Le **troisième chapitre** donne les résultats expérimentaux du système proposé avec toutes les analyses et discussions nécessaires, en utilisant une base de données de 300 personnes.

Enfin, une **conclusion générale** avec des futures perspectives que nous envisagerons est donnée à la fin de cette thèse.

Chapitre 1

Sécurité Biométrique

Principes et Applications

Résumé

Depuis plusieurs années, la sécurité est devenue une préoccupation majeure à l'échelle internationale, ce qui a conduit plusieurs pays à adopter des méthodes efficaces et fiables d'identification des utilisateurs. C'est pourquoi la biométrie est aujourd'hui intégrée dans de nombreux usages liés à la sécurité. Dans ce chapitre, nous allons d'abord introduire les concepts de sécurité de l'information. Puis, dans un second temps, nous donnons un aperçu des systèmes d'identification utilisant les techniques biométriques.

Sécurité Biométrique

Principes et Applications

La sécurité des systèmes d'information est devenue une priorité pour toutes les institutions et les personnes, ce qui signifie la nécessité d'assurer l'exactitude de l'identification/vérification de l'identité des utilisateurs. Par conséquent, les chercheurs tentent de trouver des moyens efficaces d'assurer le plus haut degré de sécurité dans diverses opérations. De manière générale, le problème de la sécurité réside dans le contrôle d'accès au système [4]. Certaines des méthodes utilisées, qualifiées de traditionnelles, ne sont pas complètement sécurisées en raison de la possibilité d'usurpation d'identité, donc pour résoudre ce type de problème de sécurité, ces méthodes ont été remplacées par d'autres liées aux propriétés intrinsèques de l'utilisateur ou à ses caractéristiques biométriques.

I.1 Sécurité d'information

Aujourd'hui, l'émergence des nouvelles technologies de l'information et de la communication a favorisé l'explosion mondiale des échanges d'informations, ce qui a poussé la communauté scientifique mondiale des chercheurs à lancer plusieurs applications en ligne dans plusieurs domaines. En effet, pour assurer une très bonne acceptation du public, des systèmes d'information fiables doivent toujours assurer la sécurité des données partagées. De même, l'identité des utilisateurs qui accèdent à ces informations doit être précisément authentifiée.

I.1.1 Cryptographie

C'est la science qui utilise les mathématiques pour chiffrer et déchiffrer les données. La cryptographie permet de stocker ou de transmettre des informations sensibles sur des réseaux non sécurisés (tels qu'Internet) de manière à ce qu'elles ne puissent être lues par personne d'autre que le destinataire prévu. Dans les processus de chiffrement/déchiffrement, une clé cryptographique, sous la forme d'une série de symboles, est utilisée pour contrôler les processus. En d'autres termes, la clé est une valeur mathématique introduite dans l'algorithme

cryptographique choisi [5].Un crypto-système est un processus cryptographique qui chiffre des données claires à l'aide d'une clé de chiffrement et déchiffre le cryptogramme résultant à l'aide d'une clé de déchiffrement [6]. Un système très complexe est appelé un crypto-système fort. Selon la figure I.1, les crypto-systèmes peuvent être classés principalement en trois catégories: le crypto-système symétrique (à clé secrète ou privée), le crypto-système asymétrique (à clé publique) et le crypto-système de hachage (avec ou sans clé).

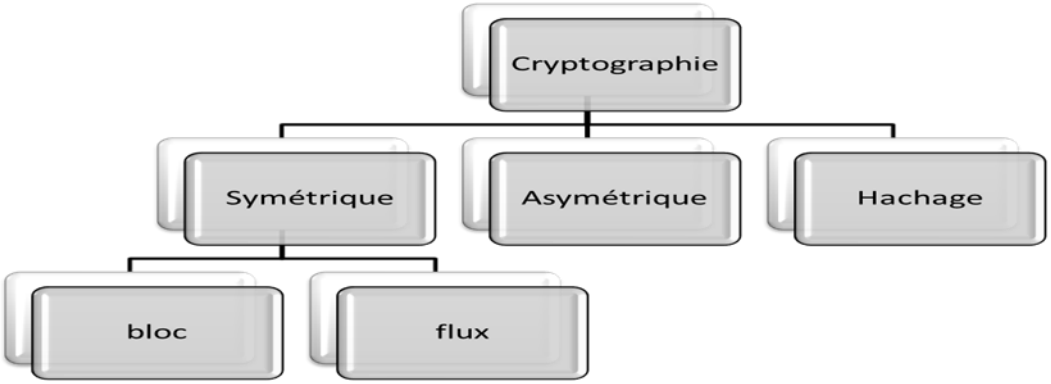


Fig. I.1: Différents cas de cryptographie [7]

✍ **Crypto-système symétrique:** Le cryptage symétrique, ou chiffrement à clé secrète, utilise une clé unique pour chiffrer et déchiffrer les données. Pour cela, la clé utilisée doit être partagée avec le destinataire. La figure I.2 montre la cryptographie à clé secrète ou conventionnelle.

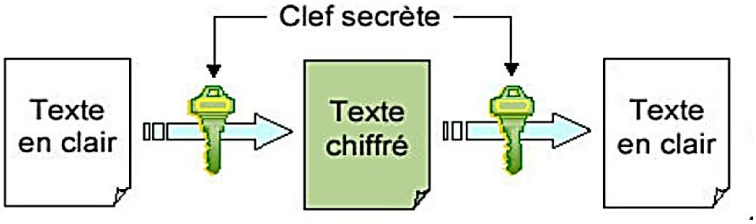


Fig. I.2: Cryptographie à clé secrète ou conventionnelle [7]

Il existe de nombreux algorithmes de chiffrement symétriques, par exemple : DES (Data Encryption standard) et AES (Advanced Encryption standard).

☑ **Avantages :**

- Clés relativement courtes (128 ou 256 bits)
- Système rapide de chiffrement et déchiffrement
- Bonne performances
- Sécurité bien étudié

☑ **Inconvenients :**

- Echange de la clé secrète point faible
- Difficulté de distribuer la clé secrète
- Ne permet pas de signature électronique

La cryptographie symétrique classée en chiffrements de flux et chiffrements par blocs. Les chiffrements de flux (*Stream ciphers*) chiffrent le texte en clair en effectuant un XOR (OU exclusif) entre le texte en clair et le flux de clé de continu. Il s'agit d'un processus de pad unique, ce qui signifie que le flux de clés produit par une certaine clé secrète ne peut être utilisé qu'une seule fois pour l'algorithme de cryptage. Les chiffrements par blocs (*Block ciphers*) chiffrent le texte en clair bloc par bloc. Ils obéissent à la théorie de Shannon de la sécurité de l'information qui nécessite un haut niveau de confusion et des propriétés de diffusion pour un crypto-système sécurisé.

✍ **Crypto-système asymétrique:** Le chiffrement asymétrique nécessite deux clés pour fonctionner. Premièrement, une clé publique doit être rendue publique afin de chiffrer les données. Deuxièmement, une clé privée utilisée pour déchiffrer les données. La figure I.3 montre la cryptographie à clé publique.

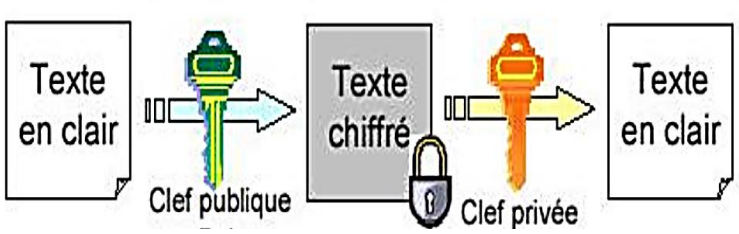


Fig. I.3: Cryptographie à clé publique [7].

Il existe de nombreux algorithmes de chiffrement symétriques, par exemple : RSA (Rivest Shamir Adleman).

☑ **Avantages :**

- Utilise deux clés différentes
- Très utile pour échanger les clés
- Pas de secret à transmettre
- Nombre des clés à distribuer est réduit par rapport aux clés symétriques

☑ **Inconvénients :**

- Clés plus longues
- Lenteur de calcul
- Pas d'authentification de la source
- Gestion de certificats des clés publiques

Le chiffrement hybride (qui combine le chiffrement symétrique et asymétrique) du message se fait en deux étapes : dans un premier temps, l'émetteur choisit une clé symétrique aléatoire, puis utilise cette clé pour chiffrer le message (de façon symétrique). Puis chiffre asymétriquement la clé avec la clé publique du destinataire, il envoie à son destinataire le message chiffré et la clé chiffrée. Le destinataire décrypte d'abord la clé, puis l'utilise pour trouver le message.

✍ **Fonction de hachages:** La fonction de hachage est utilisée pour générer la valeur de hachage d'un texte donné pour des raisons cryptographiques telles que l'intégrité et l'authentification du texte et d'autres raisons de sécurité. Cette fonction est à sens unique. Les fonctions de hachage peuvent être classées en deux catégories principales en fonction de l'utilisation des clés. La fonction qui utilise une clé secrète appelée fonction de hachage principale et celle qui n'utilise pas de clé secrète appelée fonction de hachage sans clé.
Les fonctions de hachage transforment une série de n'importe quelle taille en une série de taille fixe et sont souvent plus petites. La chaîne résultante est appelée empreinte digitale. Cette fonction accepte des tailles variables de message d'entrée et génère une sortie de taille statique. C'est ce qu'on appelle le code de hachage (voir figure I.4).

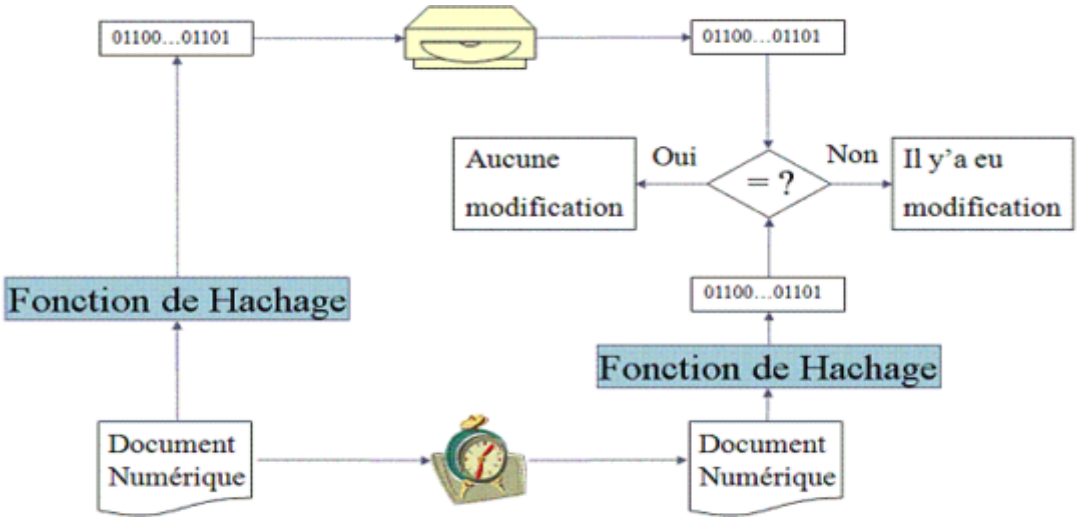


Fig. I.4: Fonction de Hachage [8]

Il est très difficile de générer deux chaînes avec la même empreinte. Ce type de fonction est général mais très sûr car s'il change légèrement, toute l'empreinte peut changer.

I.1.2 Tatouage numérique (watermarking)

L'une des applications les plus prometteuses de la stéganographie est le filigrane de documents électroniques (tatouage numérique ou *watermarking* en anglais). Il ne s'agit plus de cacher une image dans un document, mais de la marquer de manière indélébile. Les objectifs recherchés sont multiples : le premier d'entre eux est la protection du droit d'auteur. Des informations relatives à son auteur sont inscrites sur le document, afin que personne ne puisse se l'approprier. Le tatouage numérique (voir figure I.5) est une technique de masquage des métadonnées appelée marque (filigrane) dans les données numériques sans affecter la qualité des données d'origine. Une marque peut être visible ou invisible. C'est un secret pour les utilisateurs non autorisés et est robuste contre les attaques.

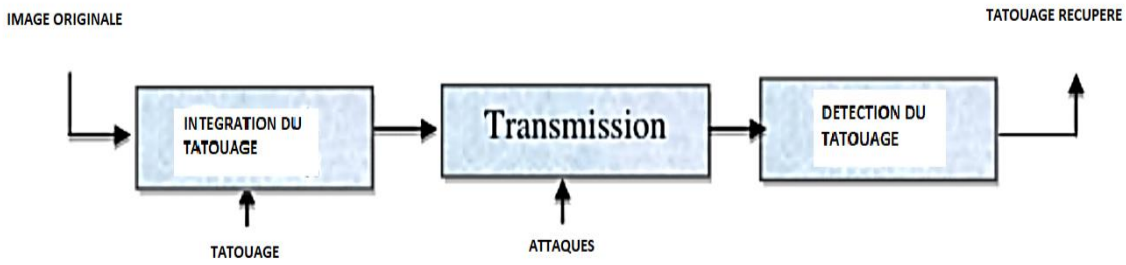


Fig. I.5: Schéma général d'un système de tatouage numérique des images [9]

Certains algorithmes de tatouage sont basés sur un domaine spatial, tandis que d'autres sont basés sur un domaine fréquentiel dans lequel les données originales sont transformées en un domaine fréquentiel, et la marque est insérée à ces coefficients de fréquence. Le domaine fréquentiel a été préféré au spatial car il offre un haut degré de robustesse contre les attaques.

I.1.3 Stéganographie

La stéganographie est utilisée pour cacher des messages secrets dans d'autres messages afin que l'existence même du secret soit dissimulée. Habituellement, l'expéditeur écrit un message inoffensif et cache un message secret dans le même papier, ce message secret n'est lu que par les détenteurs de la technique de détection. Le principal inconvénient de la stéganographie est que dans les mains d'une personne de mauvaise intentionnée, cette technique rend difficile la détection d'opérations frauduleuses, ce qui est le cas pour les hackers qui peuvent également utiliser cette technique pour camoufler leurs attaques (voir figure I.6)

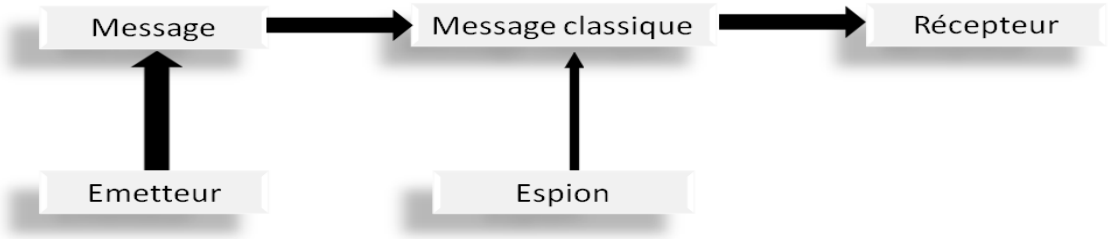


Fig I.6 : Principe de stéganographie [10]

Le hacker peut très bien dissimuler des codes fragmentés à travers les stego-médias (comme la photo et la vidéo) et reconditionner le code fragmentés à malveillant directement sur l'ordinateur de la victime (ex : par une pièce jointe exécutable) [11]

I.2 Biométrie et sécurité d'information

Généralement, la vulnérabilité de la sécurité est un problème majeur dans un certain nombre d'applications sensibles liées aux infrastructures économiques, sociales et institutionnelles. La nécessité de protéger la vie privée d'une part et de lutter contre la fraude et la criminalité d'autre part, nous oblige à placer des dispositifs de sécurité dans de nombreux domaines tels que les transports, le contrôle d'accès, la surveillance des frontières, le secteur bancaire et les services publics [12].

I.2.1 Intérêt de la biométrie

Actuellement, la reconnaissance biométrique est un enjeu important pour la sécurisation des systèmes. En effet, l'intérêt croissant accordée à la biométrie est dû à plusieurs facteurs, notamment [12] :

- **Haute sécurité :** Combiné à d'autres technologies comme le cryptage ou la carte à puce, certains systèmes rendent la fraude très compliquée.
- **Confort :** En remplaçant uniquement les méthodes traditionnelles, comme le mot de passe, la biométrie permet de respecter des règles de sécurité de base. Lorsque ces règles sont respectées, la biométrie évite aux administrateurs d'avoir à répondre à de nombreuses demandes de changement de mot de passe.
- **Sécurité/psychologie :** Dans certains cas, notamment pour l'e-commerce et l'e-banking, le client ne fait pas confiance. Il est indispensable pour ces organisations de convaincre le client d'effectuer des transactions. L'authentification biométrique peut changer le comportement des clients.

I.2.2 Domaines d'application

Généralement, la biométrie répond aux exigences de sécurité dans presque tous les domaines. Les applications de la sécurité biométrique peuvent être classées en quatre sections principales [13].

✍ **Service public :** La biométrie est utilisée dans le service public pour contrôler et sécuriser les bâtiments gouvernementaux et frontaliers, pour contrôler les immigrés entrant et sortant d'un territoire, pour identifier les personnes dans les aéroports (Iris, visage et empreinte numérique) et aussi dans la santé publique et enfin pour aider à passer de la carte d'assurance sociale (pour supprimer ces cartes ou au moins vérifier l'identité de leur propriétaire).

✍ **Pouvoir judiciaire :** La biométrie est utilisée dans le pouvoir judiciaire pour prouver certains faits concernant des infractions pénales, pour identifier l'identité d'un tel criminel à l'aide de traits biométriques extraits de la scène du crime, dans le vote électoral par Internet et dans l'identification d'enfants disparus (dont la véritable identité a été masqué) et enfin dans la protection électronique des documents.

✍ **Secteur des banques :** Avec la chute des prix de la technologie biométrique et la puissance croissante des ordinateurs personnels (PC) pour effectuer le traitement biométrique, les entreprises se tournent vers la biométrie pour prévenir la fraude bancaire et par carte de crédit [14]. Ainsi, la biométrie est utilisée dans le secteur bancaire pour effectuer des transactions bancaires (retraits en espèces, cartes bancaires, paiement par téléphone et internet) et pour réduire la proportion de fraude grâce à l'intégration de cartes à puce avec reconnaissance d'empreintes digitales.

✍ **Accès physique et logique :** La biométrie est effectivement utilisée pour contrôler les accès physiques et logiques. Il sert soit à contrôler un accès physique comme la sécurisation d'un lieu (bâtiment ou pièce) soit à contrôler un accès logique comme la sécurisation d'une session informatique (ordinateur, téléphone portable ou base de données privée) [15].

I. 3 Biométrie

La biométrie est la science qu'on utilise pour différencier des personnes les unes des autres grâce à leur biologie (physiologique ou comportementale) automatiquement reconnaissable et vérifiable. Ainsi, nous pouvons associer à notre identité des données numériques permanentes, régulières et dénuées de toute ambiguïté, et récupérer ces données rapidement et automatiquement à l'aide d'un ordinateur.

1.3.1 Technologie de la biométrie

La technologie biométrique se développe rapidement et tend à être associée, à court terme, aux technologies actuelles telles que les cartes à puce, les badges, les clés, etc. Il existe deux catégories de technologies biométriques (vor figure I.7):

Fig. I.7: Exemple des technologies biométriques [7].

☑ **Analyse de la morphologie (physiologique):** Ils utilisent une partie du corps humain (empreintes digitales, forme de la main, traits du visage, structure de l'iris ou de la rétine, empreinte palmaire). Ces éléments ont l'avantage de ne pas changer dans la vie d'un individu et ne subissent pas autant les effets du stress.

☑ **Analyse du comportement :** Ils utilisent ce que fait la personne, comme la dynamique de la signature (vitesse de déplacement du stylet, accélération, pression exercée, inclinaison), la façon dont un clavier d'ordinateur est utilisé (pression exercée, vitesse de frappe), la manière de marcher et la voix.

I.3.2 Industrie et biométrie

Actuellement, les différentes méthodes de réalisation de systèmes biométriques sont nombreuses. Elles sont toutefois la propriété des fabricants et des centres de recherche qui travaillent souvent de façon autonome et sans aucune corrélation. Le prix très élevé de technologies biométriques a été, pendant longtemps, un frein à leur développement. Aujourd'hui par contre, le profit qu'elles peuvent engendrer à long terme les rend plus attractives et relance l'économie.

1.4 Modalités biométriques

Les systèmes biométriques permettent de différencier les personnes en utilisant plusieurs technologies biométriques physiques, biologiques ou comportementales.

I.4.1 Propriétés d'une modalité biométrique

Pour être efficaces dans l'exploitation de la biométrie, les modalités biométriques utilisées doivent bien entendu posséder certaines propriétés pour permettre le développement de systèmes biométriques fiables et robustes. Les propriétés essentielles pour chaque modalité biométrique sont les suivantes :

a) **Universalité :** Toute la population doit posséder cette modalité [12] ;
b) **Unicité :** Deux personnes différentes doivent avoir des représentations différentes de leur biométrie [12];
c) **Stabilité :** Une biométrie, pour servir de moyen d'authentification, doit être relativement stable dans le temps et surtout doit être stable pour une personne quelles que soient les circonstances de l'acquisition (conditions extérieures, conditions émotionnelles de la personne...) ;
d) **Acceptabilité et facilité d'utilisation :** Désigne les contraintes liées à l'acquisition et à l'utilisation d'une modalité biométrique, elle doit être acceptée par le public ;
e) **Non-reproductibilité :** concerne la facilité ou non de falsifier une modalité biométrique pour éviter une utilisation frauduleuse du système ;
f) **Permanence :** l'information doit être constante au cours du temps [12];
g) **Performance :** reconnaitre efficacement un individu, critère prédéterminé établi pour évaluer la performance d'un système biométrique ;
h) **Mesurabilité :** elle peut être mesurée avec différentes capteurs.

Le tableau I.1 montre une comparaison entre certains traits biométriques couramment utilisés en utilisant certaines propriétés.

Traits	*(a)*	*(b)*	*(d)*	*(f)*	*(h)*	*(g)*
Emp. digitale	Moyenne	Haute	Moyenne	Haute	Moyenne	Haute
Visage	Haute	Faible	Haute	Moyenne	Haute	Faible
Rétine	Haute	Haute	Faible	Moyenne	Faible	Haute
Iris	Haute	Haute	Faible	Haute	Moyenne	Haute
Emp. palmaire	Moyenne	Haute	Moyenne	Haute	Moyenne	Haute
Voix	Moyenne	Faible	Haute	Faible	Moyenne	Faible
Signature	Faible	Faible	Haute	Faible	Haute	Faible
Frappe clavier	Faible	Faible	Moyenne	Faible	Moyenne	Faible
Démarche	Moyenne	Faible	Haute	Faible	Haute	Faible
Veines de la main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne
ADN	Haute	Haute	Faible	Haute	Faible	Haute

Tableau I.1: Comparaison entre les traits biométrique à l'aide de quelques propriétés [16].

1.4.2 Types de modalités biométriques

Les différentes modalités biométriques ont en commun de viser à établir l'identité d'une personne en analysant ses caractéristiques physiques (morphologiques), comportementales ou biologiques. Parmi les différentes modalités biométriques existantes, on distingue trois grandes catégories :

- **Modalités biométriques physiques (morphologies) :** dans le domaine de la biométrie, la morphologie est la mesure d'une forme d'une partie d'une personne pour créer un gabarit biométrique.
- **Modalités biométriques biologiques :** également appelées biométrie cachée. Il rassemble les caractéristiques qui sont à l'intérieur du corps humain.
- **Modalités biométriques comportementales :** cette catégorie nécessite l'analyse de certains comportements d'une personne.

La figure I.8 montre quelques exemples de ces trois catégories.

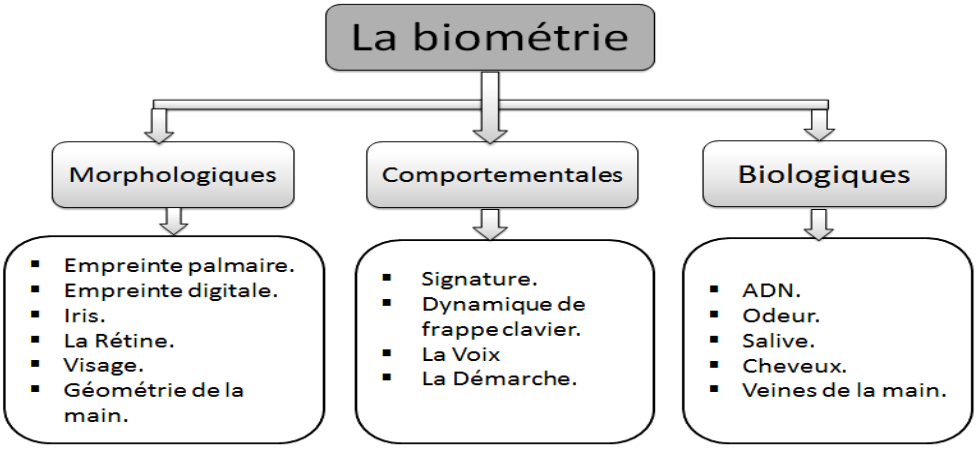


Fig. I.8: Classification d'un certain nombre de modalités biométriques [6].

La comparaison entre les différentes modalités biométriques permet de choisir une modalité en fonction des contraintes liées à l'application. En effet, chaque modalité biométrique a ses forces et ses faiblesses, et l'adéquation d'un système biométrique spécifique à une application dépend de son mode de fonctionnement et des modalités biométriques choisies. Généralement, la comparaison des principales modalités biométriques est basée sur la facilité ou l'ergonomie d'utilisation, la vulnérabilité aux attaques, les contournements, la fiabilité relative à la précision et l'efficacité de la reconnaissance [17].

I.5 Principales techniques biométriques

1.5.1 Biométrie morphologique (physiologique)

Cette catégorie est basée sur l'identification et/ou la vérification de traits physiques particuliers, elle comprend notamment, mais pas exclusivement, l'empreinte digitale, le visage, la rétine, l'iris, l'empreinte palmaire.

✍ **Empreinte digitale:** La reconnaissance d'empreintes digitales (voir Fig. I.9) est la technique biométrique la plus utilisée. Chacun de nos doigts a un motif de lignes ou de crêtes qui est unique à chaque personne [18] et il n'y a jamais deux personnes avec les mêmes empreintes digitales.

Les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes digitales. Ces éléments sont appelés minuties. Ce type de technique biométrique est utilisé par les institutions financières, les hôpitaux, les aéroports, etc. [14].

Fig. I.9: Empreintes digitales [16,19].

Avantages

- Plus efficace, moins cher et plus rapide dans le traitement.
- Plus éprouvée techniquement et mieux connue du grand public.
- Petite taille du lecteur qui facilite son intégration dans la plupart des applications (téléphones portables, PC).

Inconvénients

- Nécessite la coopération de l'utilisateur (pose correcte du doigt sur le lecteur).
- Acceptation d'un doigt moulé ou d'un doigt coupé par les systèmes (la détection du doigt vivant empêche ce type d'usurpation).

✍ **Visage:** Nos visages (joues, yeux, nez, bouche…etc.) sont des objets complexes dont les traits (distance entre différents points, positions, formes…etc.) peuvent varier dans le temps (voir Fig. I.10). Cependant, les humains ont une capacité naturelle à reconnaître les visages et à identifier les personnes en un coup d'œil.

Fig. I.10 : Visages [12]

Dans les machines, cette reconnaissance est très difficile mais pas impossible. Les systèmes de reconnaissance faciale ont potentiellement une application très large. Ils peuvent identifier les photos numériques de personnes stockées sur un ordinateur, comme lorsque des photos sont prises pour les permis de conduire dans certains États, et ils peuvent être utilisés partout où une caméra vidéo est disponible. La reconnaissance faciale est utilisée comme système de surveillance ou d'identification par les autorités ou les corps policiers principalement dans les lieux publics [20].

Avantages

- Acceptable par le public et peu coûteux.
- Ne nécessite aucune action de l'utilisateur (peu intrusif), aucun contact physique.

Inconvénients

- Sensible à l'environnement (éclairage, position, expression faciale…) et aussi aux changements (barbe, moustache, lunettes, piercing, chirurgie…).
- Les vrais jumeaux ne sont pas différenciés.

✍ **Rétine:** La rétine est la paroi interne et opposée de l'œil sur laquelle sont projetées les images que nous voyons (voir Fig. I.11). En effet, les vaisseaux sanguins d'une rétine sont uniques pour chaque individu.

Fig. I.11 : Rétine [12].

Les systèmes rétiniens sont principalement utilisés dans les établissements de très haute sécurité, comme les centrales nucléaires, les distributeurs automatiques de billets bancaires également pour le contrôle d'accès aux locaux sensibles [21].

Avantages

- La rétine différente entre jumeaux,
- Très difficile et assez stable au cours de la vie de la personne.
- Les taux de faux rejet (FRR) et faux acceptable (FAR) sont faibles.
- L'empreinte rétinienne est peu exposée aux blessures (coupures, brûlures).

Inconvénients

- Elle est contraignante et moins acceptée par les utilisateurs car l'œil est un organe sensible.
- Système intrusif, la mesure doit en effet être réalisée à très faible distance du capteur (quelques centimètres) pour que le balayage soit réussi [21].
- Coût plus important que les autres techniques et non adapté à un flux de passage important.

✍ **Iris:** L'iris est la région, en forme d'anneau, située entre la pupille et le blanc de l'œil (voir Fig. I.12), elle est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques à chaque individu.

Fig. I.12: Iris [12].

Le système d'iris nécessite uniquement qu'une personne regarde une caméra infrarouge (IR), de sorte que la personne doit être placée à une courte distance de l'appareil [22]. Les lunettes, les lentilles de contact et la couleur des yeux n'ont aucun effet sur la biométrie, pas plus que la couleur des yeux. De même, changer la taille de l'iris ne change pas la biométrie [18]. Il est utilisé dans les distributeurs de billets, en contrôle d'accès physique (locaux, machines, équipements spécifiques) et aussi le contrôle logique (systèmes d'information).

Avantages

- L'iris contient une grande quantité d'information.
- Vrais jumeaux non identifié.

Inconvénients

- Aspect psychologiquement invasif de la méthode.
- L'iris est généralement visible et peut photographier, les problèmes de sécurité sont liés aux vérifications effectués lors de la prise de vue.

✍ **Empreinte palmaire:** Cette technique utilise la surface interne de la paume pour l'identification et/ou la vérification des personnes (voir Fig. I.13). Elle est bien adaptée pour les systèmes de moyenne sécurité telle que le contrôle d'accès physique ou logique [23].

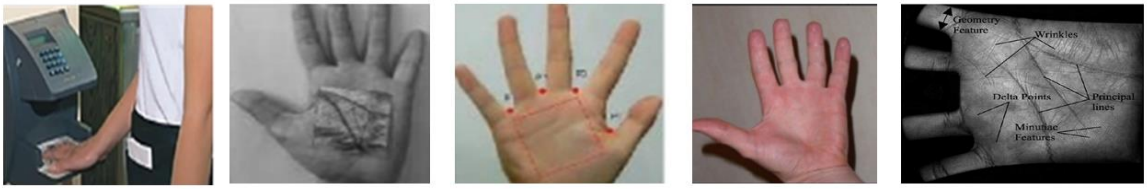


Fig. I.13: Empreinte palmaire [12].

Avantages

- Très bien accepté en raison de sa facilité d'utilisation.
- Une méthode propre qui ne laisse aucune trace sur la main.

Inconvénients

- Pourrait être identique chez les jumeaux ou encore certains nombres de famille.
- Instable au fur et à mesure des changements (blessure, vieillissement, etc.).

1.5.2 Biométrie comportementale

La biométrie comportementale repose sur l'analyse de certains comportements d'une personne, comme la voix, la signature manuscrite, la façon de marcher, la façon de taper sur un clavier.

✍ **Voix:** La voix humaine (voir Fig. I.14) varie d'une personne à l'autre et peut comprendre des composantes physiologiques et comportementales. Les gens peuvent être identifiés à un degré limité par leur voix ou leur modèle de parole. Pour utiliser un système de reconnaissance vocale, une personne doit pré-enregistrer des mots spécifiques sur le système. Plus tard, lorsque l'authentification est requise, le système invite la personne à prononcer l'un de ces mots. Un ordinateur analyse le modèle de parole et tente de déterminer si la voix correspond à la version préenregistrée.

Fig. I.14 : Système biométrique basé sur La Voix [12].

Avantages

- Cette technique est plus facile que les autres.
- Plus utilisable et pas intrusif

Inconvénients

- Sensible aux bruits / l'état physique.
- Taux de faux rejeté (FRR) et fausse acceptation (FAR) sont élevés
- Il peut falsifier facilement à partir de l'enregistrement est donc l'utilisation frauduleuse du système est possible.

- La voix d'une personne peut changer à cause d'une maladie ou d'un stress, et les femmes sont plus difficiles à identifier que les hommes.

✍ **Signature manuscrite:** Chaque personne possède une signature unique qui peut donc être utilisée pour les identifier. Il existe deux modes de reconnaissance : le mode statique et le mode dynamique (voir Fig. I.15).

Fig. I.15: Système biométrique basé sur La Signature manuscrite [24]

La vérification de la signature statique fait ressortir les formes géométriques de la signature, dans ce mode en général la signature est normalisée à une taille connue puis décomposée en un simple élément. Le mode dynamique utilise les caractéristiques dynamiques telles que l'accélération, la vitesse et les profils de trajectoire de la signature [25].

Avantages

- La signature écrite sur un document peut être conservé des certains documents.
- Action qui implique la responsabilité de demandeur.
- Utilisation très facile et très acceptable par les usagers.
- Très facile à utiliser et très acceptable pour les utilisateurs.

Inconvénients

- Besoin d'une tablette graphique.
- Sensible aux émotions de l'individu.
- La signature étant changeante à partir d'une combinaison de données (vitesse d'exécution ou autre tout cela est nécessaire
- Non utilisable pour le contrôle d'accès extérieur par exemple

✍ **Dynamique de frappe au clavier:** C'est un système de reconnaissance basé sur la manière de ses écritures sur un clavier (voir Fig. I.16). Le système utilise un dispositif logiciel pour calculer la vitesse de frappe, la séquence de lettres, le temps de frappe et la pause entre chaque mot [25].

Fig. I.16: Système biométrique basé sur Frappe dynamique sur le clavier [12]

Avantages

- Geste non intrusif et naturel pour un individu.
- Aucun matériel supplémentaire, un simple logiciel suffit.
- Permet d'identifier une personne à distance depuis son ordinateur.

Inconvénients

- Sensibilité à la différence entre les claviers.
- La façon d'appuyer sur la touche diffère en raison de l'état de santé et de la fatigue.

✍ **Démarche :** Chaque personne a une façon particulière de marcher, on peut l'identifier par la nature du mouvement des jambes, des bras et des articulations ou le mouvement spécial obtenu par une caméra vidéo (voir Fig. I.17) puis l'envoyer à un ordinateur pour l'analyse afin de déterminer la vitesse et l'accélération de chaque individu.

Fig. I.17: Système biométrique basé sur Le Démarche [12].

Avantages

- Acceptable par les individus.
- Très facile à utiliser.

Inconvénients

- N’est pas constante (âge, fatigue, maladie).

I.5.3 Biométrie biologique

La biométrie biologique repose sur l'analyse des traces biologiques d'une personne, telles que l'analyse de l'ADN, les veines de la main, la thermographie faciale.

✍ **Veines de la main :** Une main a des caractéristiques tridimensionnelles distinctes, notamment la longueur, la largeur et l'épaisseur des doigts, le contour des doigts, les veines et d'autres caractéristiques, qui sont utilisées dans les systèmes biométriques. Il s'agit d'analyser le motif formé par le réseau de veines sur une partie du corps d'un individu (la main), voir Fig. I.18, pour en extraire quelques points caractéristiques.

Fig. I.18 : Système biométrique basé sur La Veines de la main [12].

L'utilisateur place sa main dans une chambre ou un gabarit de lecture. Les caractéristiques des veines sont lues par une caméra infrarouge qui en tire une image en deux dimensions. Cette image est ensuite numérisée et enregistrée pour comparaison future. Le système peut également être sensible aux problèmes environnementaux, tels que la température ou la lumière qui brille sur la caméra.

Avantages

- Gabarit de petite taille.
- Très facile à utiliser, bonne acceptation des utilisateurs.
- Insensibilité à la poussière, aux coupures de doigts, l'humidité et de l'état des doigts.

Inconvénients

- Risque de fausse acceptation pour les jumeaux ou les membres d'une même famille.
- La forme des mains ou des doigts change avec l'âge, ce qui affecte la mesure à long terme.
- Très couteuse.

✍ **Analyse de l'ADN :** L'ADN ou acide désoxyribonucléique est le moyen le plus précis de déterminer l'identité d'une personne. Il est impossible de trouver deux personnes ayant le même ADN, voir Fig. I.19. Cette biométrie a l'avantage d'être unique et permanente tout au long de la vie [26].

Fig. I.19 : Système biométrique basé sur L'ADN [12].

Avantages

- Très haute précision.
- Impossible que le système fasse des erreurs.

Inconvénients

- Très cher, prend beaucoup de temps pour obtenir le résultat (lent).

✍ **Thermographie faciale :** La quantité de chaleur émise par les différentes parties du visage caractérise chaque personne. Cela dépend de l'emplacement des veines mais aussi de l'épaisseur du squelette, de la quantité de tissu, de muscle, de graisse, etc. Une caméra thermique permet de prendre une image infrarouge du visage. Cela permet de mettre en évidence une répartition de la chaleur propre à chaque individu (voir Fig. I.20).

Fig. I.20: Système biométrique basé sur La Thermographie faciale [12].

Avantages

- Non intrusive.
- Reconnaitre les individus même avec les artifices (fausses moustaches, barbe, lunette…).

Inconvénients

- Les taux de reconnaissances très élevés si on a l'éclairage.
- Le visage est trop changent pour être au repère biométrique suffisamment fiable.

1.6 Système biométrique

Les systèmes biométriques sont de plus en plus utilisés, il s'agit essentiellement d'un système de reconnaissance de formes qui connaît une personne sur la base d'un vecteur de caractéristiques dérivé d'un trait physiologique ou comportemental spécifique que la personne possède. En général, un système biométrique comporte deux phases.

I.6.1 Fonctionnement d'un système biométrique

Les systèmes biométriques ont trois principaux modes de fonctionnement qui sont le mode d'enregistrement (ou enrôlement), le mode de vérification (ou authentification) et le mode d'identification (ou reconnaissance) subdivisé en deux phases [27], voir Fig. I.21:

1) Phase d'enrôlement (création de la base de données) : C'est la première phase de tout système biométrique, c'est l'étape au cours de laquelle un utilisateur est enregistré dans le système pour la première fois et où un certain nombre de modalités biométriques sont capturées et enregistrées dans une base de données biométriques (liant un vecteur de caractéristiques à une identité). Cet enregistrement peut s'accompagner de l'ajout d'informations biographiques dans la base de données [28].

2) Phase de Reconnaissance (Test) : La tâche de la phase de reconnaissance est de vérifier ou d'identifier l'identité de la personne qui a l'intention d'accéder au système. Lors de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres (gabarit biométrique ou vecteur de caractéristiques) est extrait comme lors de l'enrôlement. Le capteur utilisé doit avoir des propriétés aussi proches que possible du capteur utilisé lors de la phase d'enrôlement. Le reste de la reconnaissance sera différent selon le mode de fonctionnement du système de vérification ou d'identification [28].

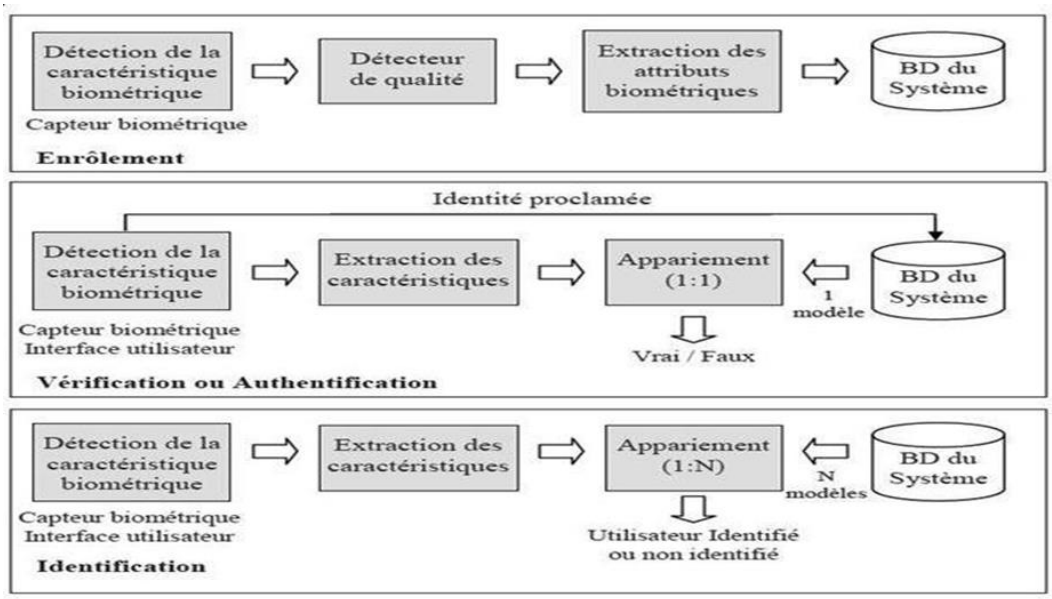


Fig. I.21 : Enrôlement, vérification et l'identification dans un système biométrique [29]

☑ **Mode de vérification:** Dans le mode de vérification, aussi appelé authentification, la personne qui veut accéder au système proclame son identité, puis l'algorithme établit une opération de comparaison entre un gabarit biométrique associé à l'identité de la personne en question et un gabarit biométrique préenregistrés dans la base de données. Lors de la vérification, le système répond à la question "Suis-je la personne que je prétends être ?" avec oui ou non c'est une décision binaire. Il suffit donc de le comparer avec un seul des gabarits présents dans la base de données (1:1).

☑ **Mode d'identification:** La personne qui souhaite accéder au système ne proclame pas son identité. Le système répond donc à une question du type « Qui suis-je ? » en acceptant si l'utilisateur a un gabarit dans la base ou en rejetant si l'utilisateur n'a pas de gabarit dans la base. Dans ce mode, l'utilisateur fournit un gabarit biométrique qui sera comparé à tous les gabarits biométriques contenus dans la base de données lors de la phase d'enrôlement (1 : N).

Le mode d'identification peut être décomposé en deux modes de fonctionnement :

Mode ensemble fermé : la sortie du système biométrique consiste en l'identité de la personne dont le gabarit (référence) présente le plus haut degré de similarité avec l'échantillon biométrique présenté en entrée.

Mode à ensemble ouvert: si la similarité la plus élevée entre l'échantillon biométrique testé et tous les gabarits pré-enregistrés est inférieure (ou supérieure) au seuil de sécurité, la personne est rejetée, ce qui implique que l'utilisateur n'est pas enrôlé sinon la personne est acceptée.

1.6.2 Modules de systèmes biométriques

Un système biométrique typique peut être représenté par quatre modules principaux :

1) Module de capture: Responsable de l'acquisition des données biométriques d'un individu (il peut s'agir d'une caméra, d'un lecteur d'empreintes digitales, d'une caméra de sécurité, etc.)

2) 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. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe.

3) Module de correspondance: Compare l'ensemble des caractéristiques extraites avec les gabarits enregistrés dans la base de données du système et détermine le degré de similitude (ou de divergence).

4) Module de décision: Vérifie l'identité affirmée d'un utilisateur ou détermine l'identité d'une personne sur la base du degré de similitude entre les gabarits extraits et le(s) gabarit(s) stocké(s).

I.7 Conclusion

De nos jours, la biométrie est considérée comme le moyen de sécurité le plus sûr. Il est de plus en plus appliqué dans la réalité grâce à ses avantages. Dans ce chapitre, nous avons présenté un état de l'art sur les technologies biométriques et souligné le grand nombre de ces technologies. Nous avons également indiqué quelques points forts et points faibles de chaque technologie ce qui met en évidence le fait qu'elles ne sont pas toutes aussi efficaces. Nous avons présentés aussi le concept de vérification de l'identité de la personne et de la structure globale et des domaines d'utilisation du système biométrique.

Chapitre 2

Protection des gabarits biométriques

Nécessités et Avantage

Résumé

Ces dernières années, l'utilisation de diverses technologies biométriques pour l'identification automatique des personnes s'est considérablement développée. Malgré leurs avantages, ils sont menacés par des attaques qui conduisent au vol de la vie privée d'un individu. Pour prévenir le vol de gabarits biométriques, il est souhaitable de proposer des solutions permettant d'améliorer la sécurité, ce qui conduira nécessairement à la confiance des utilisateurs. Il existe des solutions telles que les systèmes crypto biométriques ou la biométrie révocable. Dans ce chapitre, nous présentons les vulnérabilités et les menaces ainsi qu'un aperçu des méthodes de protection des gabarits biométriques (crypto-système biométrique et biométrie révocable).

Protection des gabarits biométriques

Nécessités et Avantage

La biométrie concerne l'utilisation des caractéristiques intrinsèques des personnes pour identifier ou vérifier l'identité d'un utilisateur. Récemment, des discussions sur la sécurité des systèmes biométriques ont été émergées. La sécurité d'un système biométrique est l'une des tâches les plus cruciales de sa conception. Les gabarits biométriques sont des données personnelles et sensibles aux menaces externes. Pour assurer leur sécurité, de nombreux systèmes ont été mis en place pour les protéger et, par conséquent, protéger la vie privée et l'identité des individus. Dans ce chapitre, nous présentons les vulnérabilités et les menaces d'un système biométrique. Ensuite, nous discutons des approches existantes pour protéger le gabarit biométrique. Enfin, la méthode proposée pour générer des gabarits biométriques profonds, révocables et cryptés sera présentée.

II.1 Vulnérabilités et menaces d'un système biométrique

Le système biométrique est sujet à de nombreuses attaques malveillantes qui peuvent être menées par diverses formes de menaces. Les attaques malveillantes contre le système biométrique sont un problème de sécurité qui peut sérieusement dégrader les performances du système. Le système biométrique a différentes limites telles que les attaques par usurpation d'identité, les données bruyantes, les variations interclasses et les similitudes interclasses, etc. De plus, les données biométriques sont généralement considérées comme sensibles aux menaces à la vie privée.

✍ **Menace:** Une menace pour le système biométrique est la possibilité qu'un événement ou une action entraîne une perte de sécurité, une dégradation de la fiabilité ou des performances de la technologie, ou une atteinte à la vie privée d'une personne.

✍ **Vulnérabilité :** Une vulnérabilité est une faiblesse d'un bien, qui peut être exploitée par une ou plusieurs menaces. La vulnérabilité d'un système biométrique est définie comme la possibilité d'une attaque contre un système biométrique, par un attaquant actif.

✍ **Risque :** Un risque spécifique pour la technologie biométrique est la probabilité qu'une menace spécifique à cette technologie soit également exploitée contre une vulnérabilité spécifique, avec des conséquences et des effets potentiellement néfastes [30].

C'est pourquoi tout système biométrique doit être analysé, et des contre-mesures de prévention doivent être prises dans la conception du système biométrique. Les différentes attaques dans les systèmes biométriques sont (voir Fig. II.1) :

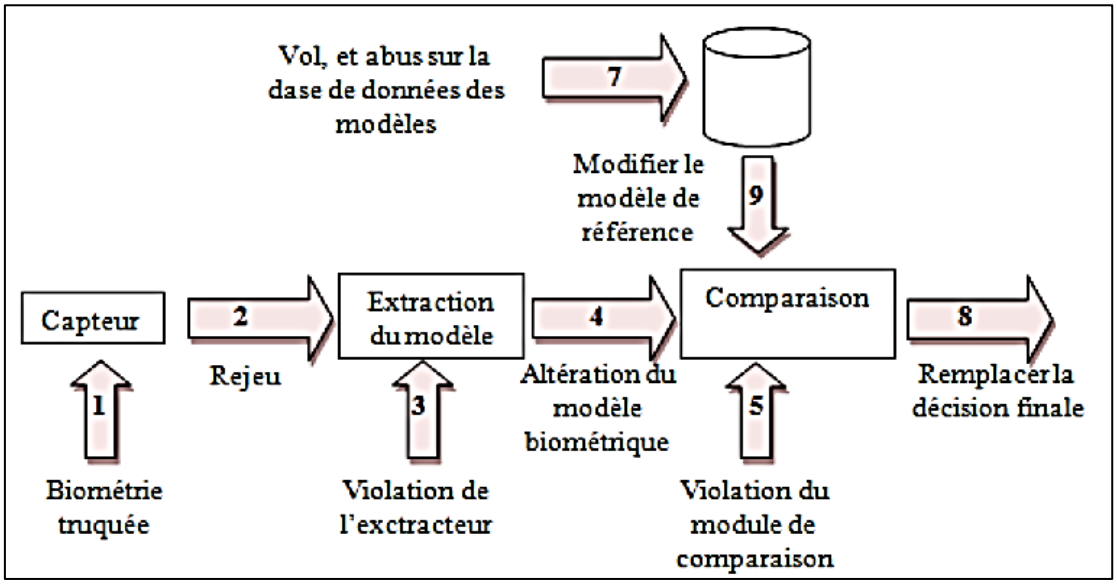


Fig.II.1 : Points de vulnérabilités d'un système biométrique [31]

Pour leur généralité, nous détaillons les points d'attaques de Ratha et al. [31] illustrées sur la figure II.1 :

– Point 1 : Attaque sur le capteur en présentant une modalité biométrique truquée.
L'attaque est effectuée en présentant au capteur un doigt truqué généré à partir d'une image d'empreinte, qui elle, a été reconstruite à partir du modèle des minuties, volé de la base de données.
Cette menace met en avant l'importance de protéger les données biométriques à l'intérieur des bases de données.

– Points 2, 4, 6, 8 : Attaque sur les canaux de communication. Si aucune mesure de sécurité n'est prise en charge, l'attaquant peut intercepter (Eavesdropping), modifier et insérer les données biométriques (Man-in-the-Middle) ou rejouer les mêmes données biométriques (Replay). Il peut aussi manipuler la décision issue du module de comparaison en la compromettant.

– Points 3,5 : Attaque sur les modules de traitement. Un des plus grands risques de sécurité informatique concerne l'injection de programmes malicieux qui peuvent ensuite contrôler le comportement du module initial (comme fournir le modèle ou le score souhaités).

– Point 7 : Attaque sur les modèles. L'attaquant peut capturer le modèle de référence, le substituer, le modifier et ainsi il peut compromettre la base de données [31].

II.1.1 Faux biométrie

Il s'agit de la faiblesse la plus importante lorsque l'on parle de systèmes biométriques, c'est de violer ou de fournir de fausses données biométriques physiques conçues pour contourner le système biométrique. Cette attaque peut être effectuée relativement facilement en raison d'un manque de connaissances techniques du système ou d'un manque de besoins. Les matériaux nécessaires pour créer de fausses données biométriques sont généralement présents et faciles à obtenir. Un autre facteur est que ces attaques sont menées au point d'entrée du système, de sorte que de nombreux mécanismes de protection numérique, tels que le cryptage et l'utilisation de signatures numériques, ne sont pas efficaces.

De nombreuses données biométriques (y compris les empreintes digitales, les mains et l'iris) sont exposées à cette forme d'attaque. Les données biométriques originales peuvent être obtenues relativement facilement à partir de plusieurs sources, avec ou sans l'autorisation et la coopération du propriétaire de ces données biométriques. En effet, nous laissons de nombreux effets biométriques, comme les empreintes digitales et les empreintes de mains, sur les bureaux, les portes, les ustensiles et de nombreuses autres surfaces. En outre, faux masques faciaux, fausses empreintes digitales en silicone, lentille sur l'iris, etc., font partie de ces attaques malveillantes sur le capteur [6].

II.1.2 Attaque par rejoue

L'attaquant peut fournir une photographie ou une vidéo du visage, par exemple, d'un vrai client à un capteur électronique ou à une caméra électronique pour le système biométrique. Ce point est le plus risqué dans le système biométrique car dans un système entièrement automatisé, la possibilité de présenter une photographie est toujours accessible à l'attaquant sauf si l'espace physique devant la caméra est supervisé par un observateur humain ou par une deuxième modalité biométrique. Si l'attaquant peut accéder à l'intérieur de la caméra, il n'a pas besoin de montrer une photo ou une vidéo à la caméra, mais peut injecter un signal électronique approprié directement dans le système qui correspond à l'image du visage du client [6].

II.1.3 Transmission de données biométriques interceptées

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

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

Ce module pourrait être remplacé par le virus cheval de Troie afin de produire des informations choisies par l'attaquant. L'utilisateur légitime ne se rend pas compte que ce module a été corrompu et a fourni des informations selon les instructions du pirate. Le module

d'extraction des caractéristiques est pénétré par le hacker, et les métadonnées ne seront pas efficaces contre ce type d'attaque.

II.1.5 Altération des caractéristiques extraites

Une fois les données obtenues par le module d'extraction de caractéristiques, elles sont modifiées ou remplacées par d'autres données spécifiées par l'attaquant. En ce qui concerne les attaques contre des infrastructures non sécurisées, nous sommes dans des situations où le système biométrique est corrompu et nous ne fournirons des réponses qu'en fonction de l'intention de l'attaquant. Les métadonnées ne seront pas efficaces dans ces contextes.

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

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

II.1.7 Corruption de la base de données

La base de données de gabarits biométriques est disponible localement, à distance ou distribuée sur plusieurs serveurs. Dans ce type d'attaque, l'attaquant modifie un ou plusieurs gabarits pour permettre au fraudeur voire empêcher l'utilisateur légitime d'y accéder [6].

II.2 Améliorer la sécurité des systèmes biométriques

Avec le développement rapide de la technologie numérique et la transformation rapide de divers domaines vers la numérisation, en particulier dans des domaines sensibles tels que les institutions financières, la sécurité de l'information est devenue une nécessité pour gagner la confiance des clients, et pour atteindre une expansion rapide et augmentation des bénéfices [32]. Ainsi, les chercheurs tentent de trouver des moyens efficaces pour assurer le plus haut degré de sécurité dans diverses opérations. De cette façon, nous évitons le vol de gabarits biométriques stockés par des fraudeurs. Pour cela, il existe trois technologies de protection des gabarits biométriques (voir Fig. II.2) :

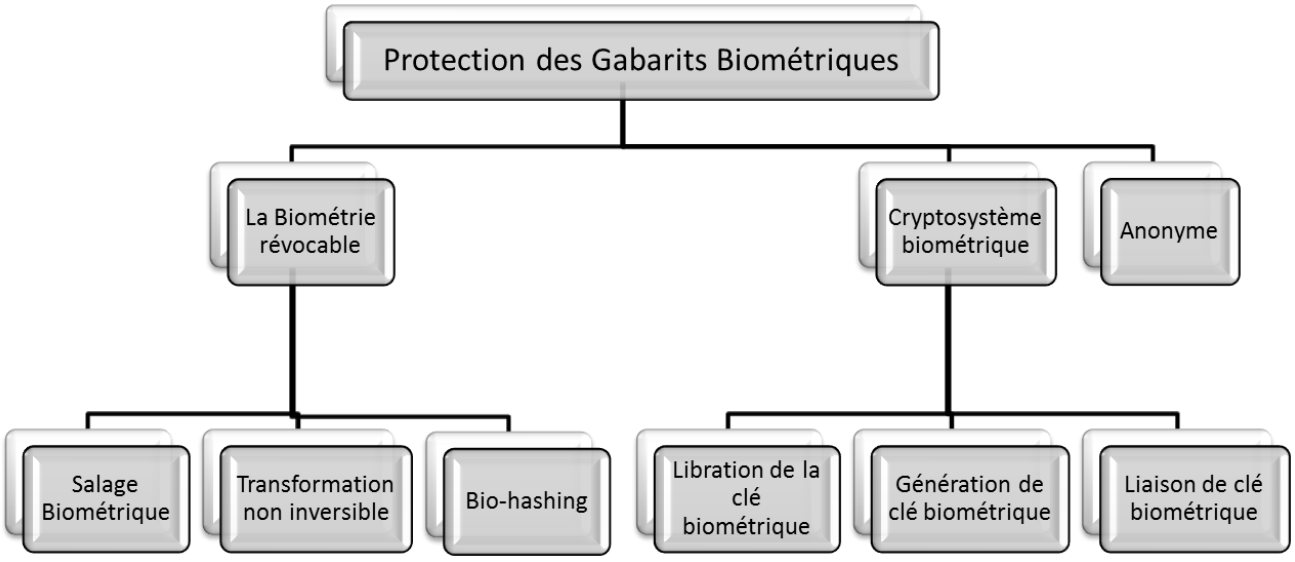


Fig. II.2: Technologies de protection des gabarits biométriques [33].

Juels et Wattenberg [34] ont initialisé une nouvelle méthode appelée "Fuzzy Commitment Scheme". Au début des années 2000, *Ratha et al.* [31] ont présenté les algorithmes de transformation non inversibles où les données initiales ne peuvent plus être récupérées. En 2002, le "Fuzzy Vault Scheme" a été présenté par *Juels et Sudan* [35]. En 2003, *Goh et al.* [36], ont présenté le Biohashing comme une nouvelle technique de transformation des gabarits biométriques. Cet algorithme a été initialement proposé pour le visage et les empreintes digitales par *Scheirer et al.* [37] ont développé des méthodes hybrides présentant des Biotokens révocables associant des crypto-systèmes à des algorithmes de transformation de gabarits. Ainsi, l'évolution des différents schémas de protection biométrique donnée par la Figure II.3 :

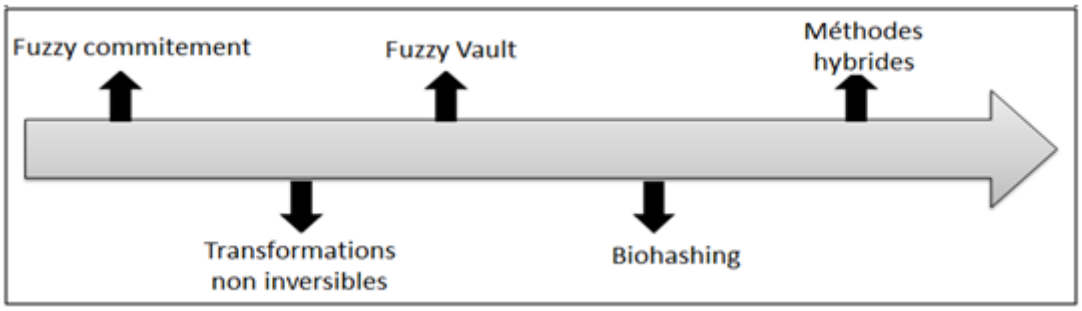


Fig. II.3 : Évolution des algorithmes de protection de gabarits biométriques [33].

II.2.1 Crypto-système biométrique

De nombreux travaux, sur différentes modalités biométriques, ont été menés afin de concevoir des crypto-systèmes biométriques appelés aussi systèmes bio-crypto. Dans le cas des crypto-systèmes biométriques, la biométrie peut être utilisée pour protéger une clé cryptographique, tandis que la clé est utilisée pour protéger le gabarit biométrique (voir Fig. II.4).

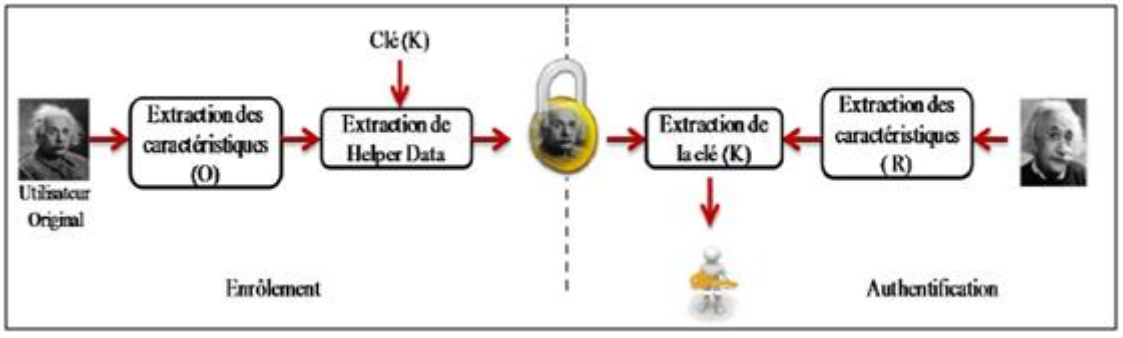


Fig. II.4 : Principe de fonctionnement de crypto-systèmes [38].

Ces crypto-systèmes biométriques peuvent être classés en trois catégories. Systèmes dédiés à l'authentification (*key release* et *key binding*), systèmes dédiés à la protection des gabarits biométriques et systèmes assurant les deux aspects. Pour lier la biométrie à la cryptographie il y a trois manières différentes et cela se fait selon trois modes :

- **Libération de la clé biométrique (*Biometrics key release*):** Il s'agit de protéger une clé qui ne sera libérée qu'en cas d'authentification par biométrie (voir Fig. II.5) [39].

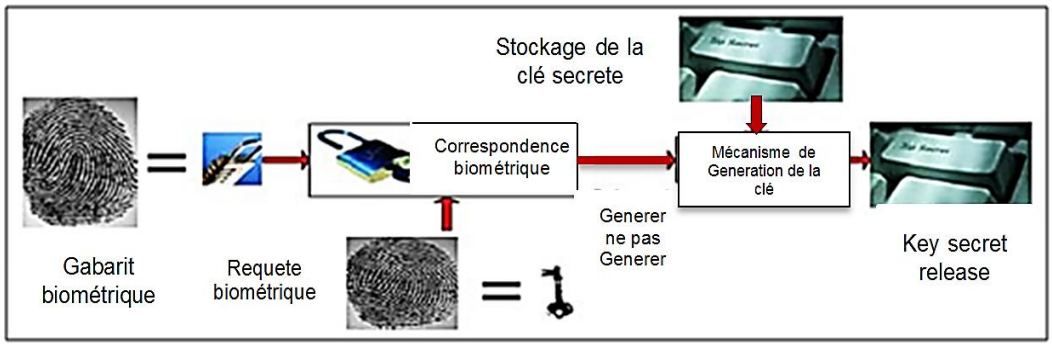


Fig.II.5: Mode d'opération d'un système crypto-biométrique (Key release) [39].

- **Génération de clé biométrique (*Biométrics key generation*) :** Dans un tel système, la clé cryptographique est dérivée des données biométriques. Ces données biométriques permettent donc de calculer une clé cryptographique, qui serait unique ; obtenu à partir du calcul sur les données biométriques (voir Fig. II.6)[39].

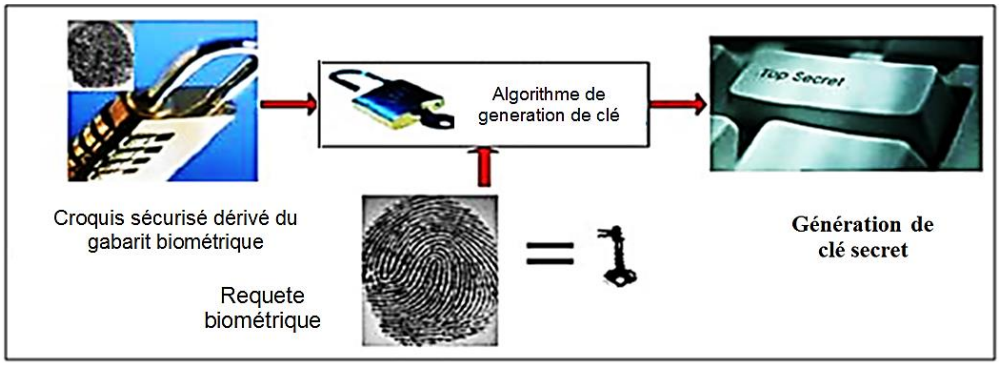


Fig. II.6: Mode d'opération d'un système crypto-biométrique (Key generation) [39]

- **Liaison de clé biométrique (*Biometrics key binding*):** Le système associe une clé cryptographique aux données biométriques de l'utilisateur au moment de l'enrôlement. La clé ne sera retrouvée qu'en cas d'authentification réussie (voir Fig. II.7) [39].

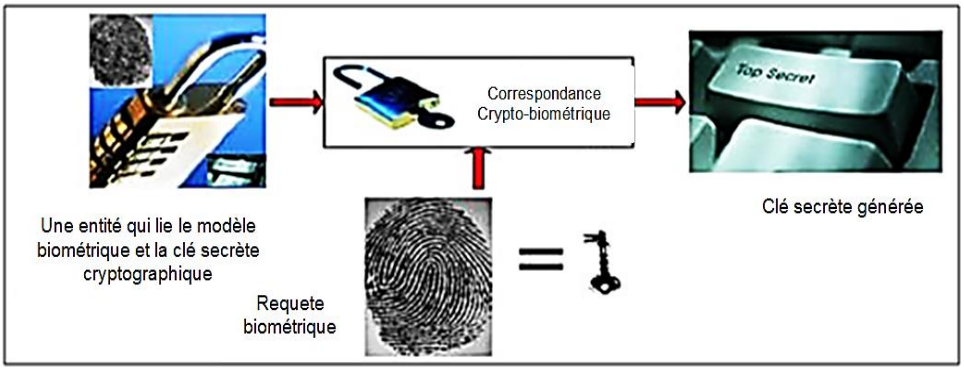


Fig.II.7: Mode d'opération d'un système crypto-biométrique (Key binding) [39].

Pour les systèmes basés sur la protection des données biométriques on peut citer *Tuyls et al.* [40] qui propose d'utiliser une version modifiée des données biométriques. *Dodis et al.* [41] s'inspirent de ces travaux pour développer la notion de *Fuzzy extractors* qui permettent l'extraction de clés fortes à partir de données bruitées variables et non uniformes.

Davida et al. [41] sont les premier à travailler sur des systèmes dédiés à l'authentification (*key binding* et *key genération*). Ils proposent de travailler sur l'iris en utilisant sa texture. *Juels et Wattenberg* propose le protocole « *fuzzy commitment scheme* » [34] ou engagement flou. Cette méthode fait partie des systèmes dédiés à l'authentification en mode *key binding* avec protection de données biométriques. Ainsi, sécurise les gabarits biométriques sous forme de vecteurs binaires (ce schéma combine la cryptographie avec des codes correcteurs d'erreurs pour assurer une meilleure protection des gabarits biométriques)

De plus, *Juels et Sudan* [35] proposent un nouveau protocole appelé *fuzzy vault* (ou encore coffre-fort secret). Ce protocole permet d'avoir un code basé sur des données biométriques, mais dans le cas de *fuzzy vault* il s'agit plutôt d'utiliser un polynôme $p(x)$ au lieu d'un mot de passe. On calcule ici les valeurs de $p(x_i)$, les x_i étant des valeurs extraites de données biométriques. On forme ainsi un ensemble de points $(x_i, p(x_i))$. Ainsi, ce protocole sécurise la clé comme un ensemble non ordonné de points.

II.2.2 Biométrie anonyme

La biométrie anonyme « ou non identifiée » est un dispositif dans lequel les données biométriques ne sont liées à aucune donnée personnelle permettant d'identifier la personne, et qui ne permet aucune interconnexion avec un autre système où elle pourrait être identifiée. Il ne peut être utilisé que pour des dispositifs d'authentification, par exemple en faisant appel à un tiers de confiance qui authentifierait les données biométriques à la demande de la personne ou du fournisseur de service. La seule donnée communiquée serait un numéro de transaction. Cela nécessiterait que le tiers de confiance mette en place des procédures sécurisées et adéquates d'enrôlement, de stockage et de comparaison [42].

Selon *Max Snijder*, la mise en œuvre d'un système d'authentification biométrique anonyme a quatre conditions :

- Les données biométriques utilisées doivent rester secrètes.
- Les données biométriques et le gabarit ne doivent pas être stockés sur le système.
- Les données de référence qui seront conservées ne doivent pas permettre de retrouver les données biométriques sources.
- Les données de référence stockées et créées à partir de données biométriques ne doivent pas pouvoir être reliées à des données d'identification personnelles.

Ces technologies présentent donc de nombreux avantages pour les usages d'authentification, notamment sur Internet, afin d'éviter le piratage et l'entourement des données.

II.2.3 Biométrie révocable

La biométrie révocable fait également partie des technologies biométriques non traçables. Dans ce cas, il s'agit de créer, à partir des données biométriques, un gabarit «transformé» et non biométrique qui seul sera conservé. En effet, les données biométriques ne sont pas stockées, comme pour le cryptage biométrique. La comparaison est faite entre les deux gabarits «transformés». Il est également possible ici d'annuler et de renouveler un gabarit (la figure II.8 montre un exemple de la biométrie révocable).

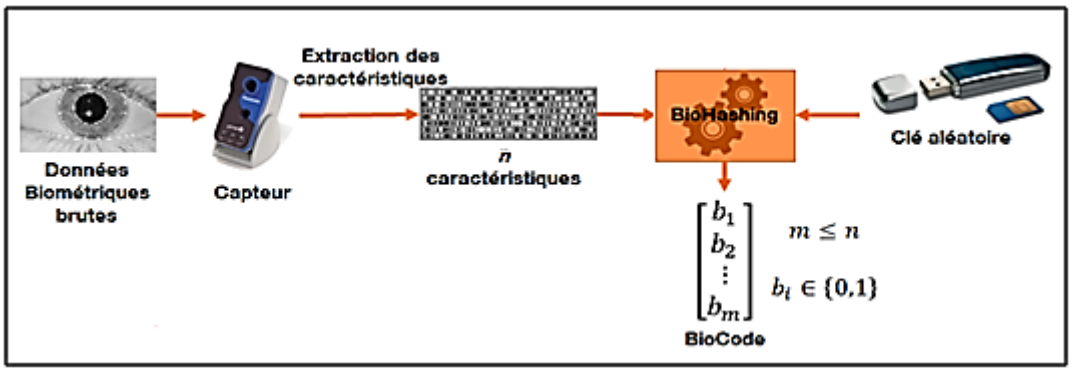


Fig. II.8 : Schéma de biométrie révocable [33]

Les travaux dans [43, 44] définissent pour la première fois le terme de biométrie révocable. Ce concept repose sur la transformation de données biométriques brutes, de manière à ce que les données transformées soient sécurisées et respectueuses de la vie privée. La biométrie révocable doit respecter les caractéristiques détaillées par *Maltoni et al.* [45] :

- **Non-inversibilité:** Il ne doit pas être possible de retrouver des informations sur la donnée biométrique originale à partir de sa transformée.
- **Performance:** l'efficacité du système biométrique ne doit pas être détériorée par la transformation.
- **Diversité:** il doit être possible de générer plusieurs données protégées à partir d'une seule donnée brute. Le chevauchement de différentes données protégées ne devrait pas affecter la protection de la vie privée.
- **Révocabilité:** il doit être possible de révoquer facilement les données en cas de compromission.

Enfin, il est important de noter que ces méthodes peuvent être combinées avec une approche hybride qui améliore la sécurité du système. Par exemple, les méthodes de protection basée sur la révocabilité peuvent être combinées avec celles des crypto-systèmes biométriques pour créer un système robuste qui peut tirer parti des avantages des deux méthodes.

Par exemple, Feng et al. [46] proposent une approche hybride basée sur la reconnaissance faciale, utilisant d'abord la projection aléatoire du gabarit biométrique, puis chiffrant les résultats à l'aide d'un crypto-système biométrique basé sur l'engagement flou (*fuzzy commitment*). De plus, Song et al. [47] ont proposé une méthode hybride basée sur la

génération de clés secrètes lors de l'enregistrement à partir de données biométriques en appliquant le Hachage discret et le code de correction d'erreur de *Reed Solomon* [48].

II.3 Méthodes de la biométrie révocable

Il existe trois méthodes de la biométrie révocable qui sont :

II.3.1 Salage biométrique

Le salage biométrique est similaire au salage de mot de passe en cryptographie, qui consiste en des bits aléatoires *r* utilisés comme facteur d'entrée à concaténer avec une clé secrète, *k*. La sortie est souvent stockée sous forme de hachage *H(r+k)* dans la base de données. En effet, le salage biométrique (voir Fig. II.9) suit un principe selon lequel le facteur d'entrée indépendant de l'utilisateur (données auxiliaires comme le mot de passe ou les numéros aléatoires de l'utilisateur) est mélangé aux données biométriques pour dériver une version déformée du gabarit biométrique [38].

Étant donné que les données auxiliaires sont extraites de l'extérieur et interagissent directement avec les données biométriques, elles peuvent être facilement modifiées et révoquées, mais doivent rester secrètes pour une protection maximale. Cependant, étant donné que les clés externes secrètes ou les mots de passe peuvent facilement être perdus, volés ou compromis, l'exactitude et les vulnérabilités des systèmes existants doivent être justifiées.

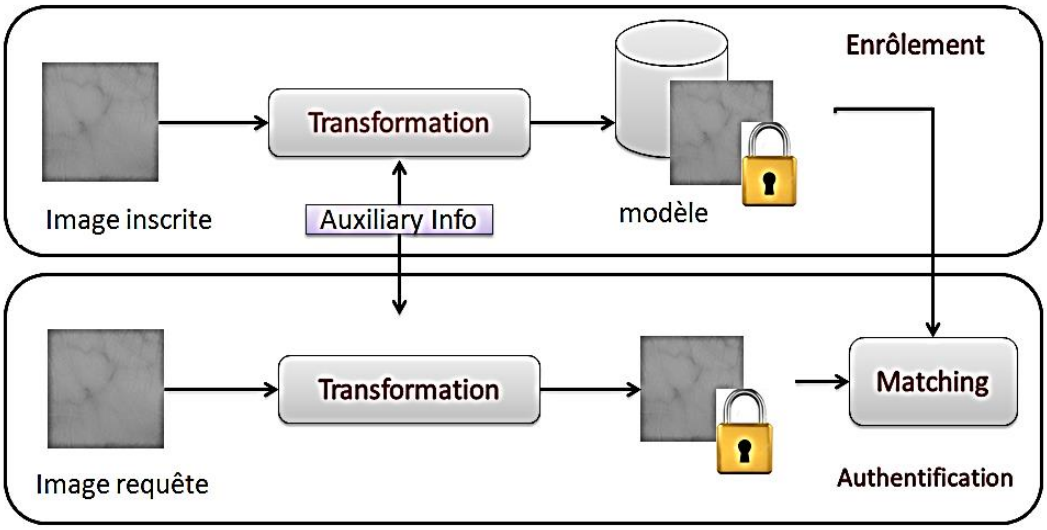


Fig.II.9: Schéma fonctionnel du salage biométrique [38].

Dans ce contenu, un certain nombre d'efforts de recherche ont été déployés pour résoudre les problèmes liés à la sécurité des systèmes biométriques. *Savvides et al.* [49] proposent une méthode de salage biométrique qui encode des images d'apprentissage en synthétisant le filtre de convolution pour la reconnaissance faciale. Ils ont montré que différents gabarits des mêmes données biométriques peuvent être obtenus en modifiant les noyaux de contournement aléatoires et en autorisant ainsi des gabarits révocables. Notez que les noyaux aléatoires ont été créés à partir de différentes matrices aléatoires créées à l'aide du code PIN de l'utilisateur.

Herata et al. [50] ont proposé une nouvelle méthode utilisant la mise en correspondance basé sur la corrélation. Dans leur travail, l'image biométrique a été convertie en transformant le nombre théorique, et le résultat a ensuite été masqué par un filtre aléatoire. Il est possible de calculer la corrélation entre l'image enrôlées et l'image d'entrée dans le champ masqué (crypté) sans connaître les images originales. Les auteurs ont appliqué la méthode proposée pour vérifier les réseaux veineux des doigts et ont obtenu des performances de vérification très élevées.

Jeong et al. [51] ont proposé un schéma de salage biométrique pour le gabarit facial basé sur l'apparence. Deux vecteurs de caractéristiques ont été extraits à l'aide de PCA (analyse en composantes principales) et ICA (analyse en composantes indépendantes) à partir d'une image de visage, puis ces vecteurs ont été normalisés. Les vecteurs résultants ont ensuite été commutés à l'aide d'une matrice de permutation dérivée du code et combinées au niveau des caractéristiques via la règle SUM. Si ces vecteurs sont compromis, un nouveau vecteur de caractéristiques peut être créé en changeant la matrice de permutation.

Lee et al. [52] ont introduit des valeurs fixes de translation et de rotation, qui ont été extraites à l'aide des informations d'orientation à chaque minute. Ces valeurs ont ensuite été utilisées comme entrées pour deux des fonctions de conversion spécifiques à l'utilisateur chargées de générer les paramètres de translation et de rotation. Des gabarits biométriques ont ensuite été construits. Lorsque le gabarit révocable est compromis, un nouveau gabarit peut être régénéré en remplaçant les fonctions de transformation.

Farouk et al. [53] ont présenté une méthode en convertissant les minuties des empreintes digitales en une série binaire annulable. L'idée est basée sur le fait que les empreintes digitales peuvent être représentées par un groupe de triangles dérivés de groupes de trois minuties qui peuvent être utilisés directement dans la correspondance basée sur un modèle. La méthode proposée s'est avérée irréversible en termes de calcul et a satisfait aux critères de réutilisation et de diversité. Notez que la réutilisation est obtenue en définissant une clé unique pour chaque base de données d'utilisateurs pour le modèle d'utilisateur aléatoire, et en cas de compromis, le gabarit biométrique peut être annulé une fois qu'une clé différente est définie.

II.3.2 Transformations non inversibles

La transformation non irréversible est une fonction conçue pour changer intentionnellement l'image biométrique brute en une nouvelle forme dans le contexte de la fonction ou de l'espace de signal. Cette fonction sert d'agent comme facteur de sécurité pour les gabarits qui permettent la non-inversibilité, la réutilisabilité et la diversité des gabarits. Comme cette fonction n'interagit pas directement avec la biométrie brute, l'avantage majeur de cette méthode est qu'elle n'a pas besoin d'être gardée secrète [31, 43].

La réalisation d'une transformation non inversible a été rapportée par *Ratha et al.* dans [31] dans lequel les données d'empreintes digitales sont transformées par une séquence de trois fonctions de transformation non inversibles, (voir figure. II.10).

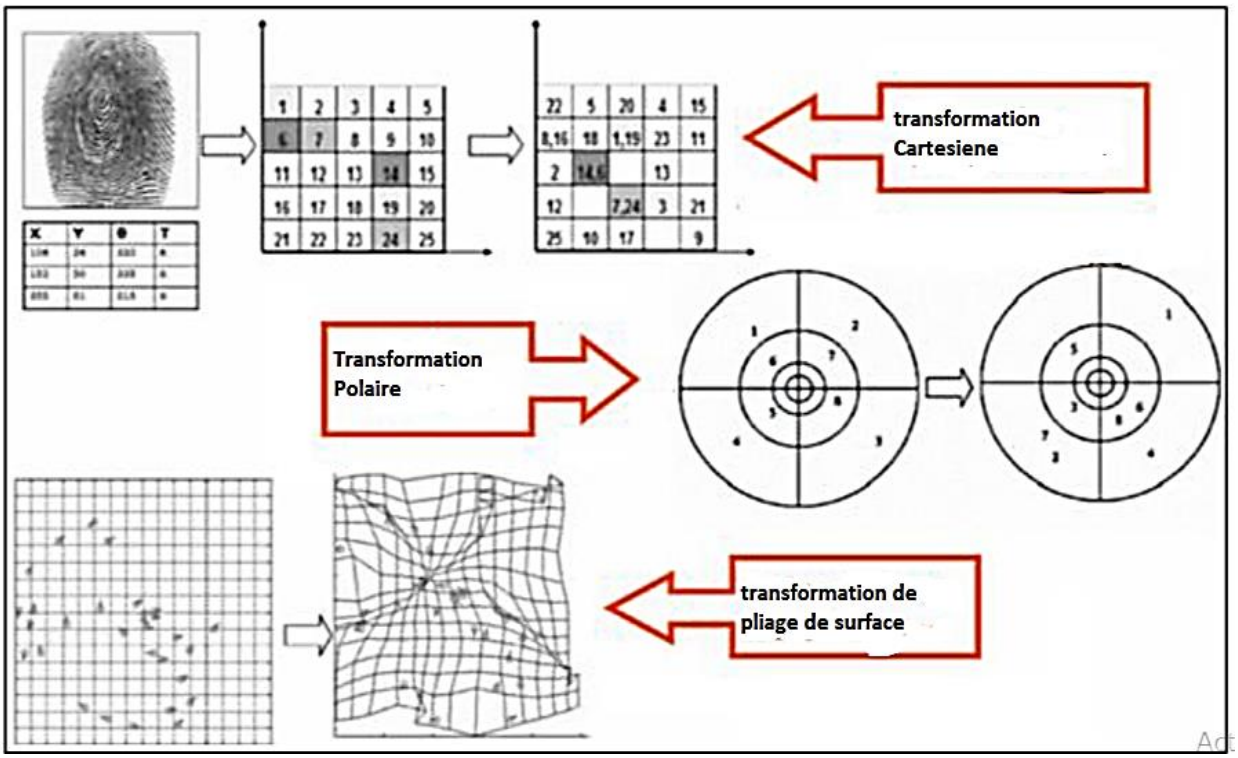


Fig II.10 : Gabarits révocable de différentes transformations [38]

Comme le montre cette figure, les trois fonctions de conversion sont basées sur la transformation cartizienne, polaire et de pliage en surface des sites des minuties.

✍ **Transformation polaire:** Dans la méthode de transformation polaire, les emplacements des minuties sont mesurés par les coordonnées polaires par rapport à la position centrale. Les angles sont mesurés par rapport à la direction du noyau. Ainsi, l'espace de coordonnées est divisé en régions polaires. La transformation inversible consiste à changer l'emplacement des coins polaires. Les angles de minutie changent également avec les différences d'emplacement des coins avant et après la transformation [53, 43].

✍ **Transformation cartizienne:** Dans cette transformation, les positions des minuties sont mesurées en coordonnées rectangulaires par rapport à la position du point unique en alignant l'axe X avec sa direction, le système de coordonnées est divisé en cellules de taille fixe. Il est à noter que cette transformation n'est pas qu'un simple changement car chaque cellule, qui peut contenir quelques minutes, est transférée à une nouvelle position par une transformation inversible [53, 43].

✍ **Transformation de pliage de surface :** Dans la méthode de transformation de pliage de surface, un mélange gaussien 2D est utilisé pour traduire les points de minutie. Étant donné

que les transformations utilisées dans le mélange sont localement lisses, cela n'aura qu'un effet minimal sur les taux d'erreur et ne réduira pas considérablement la distinction des minuties par rapport aux deux transformations précédentes. Cependant, étant donné qu'un petit changement dans la position des minuties de l'empreinte originale peut entraîner une grande transformation, surtout si le point traverse la frontière, un pré-alignement approprié en référence est nécessaire en ce qui concerne la position du point central pour s'assurer que la caractéristique biométrique est convertie de manière cohérente à travers plusieurs instances de minuties.

II.3.3 Bio-hachage

Pour sécuriser le vecteur de caractéristiques (gabarit) extrait par la phase d'extraction des caractéristiques, une méthode très populaire, basée sur la transformation non inversible de caractéristiques "*Biohashing*", est généralement appliquée. La BioHachage a été proposé en 2003 pour la reconnaissance faciale [36], puis en 2004 pour les empreintes digitales [54]. Lors de la phase d'enrôlement, l'utilisateur présente son empreinte digitale et son visage et la clé secrète stockée sur une clé USB, une carte à puce ou plus généralement un token. Les paramètres sont extraits de l'empreinte digitale et du visage (par exemple à l'aide d'un filtre Log-Gabor) sous forme de deux vecteurs, après avoir fusionné ces vecteurs pour donner un seul vecteur caractéristique, la fonction de transformation prend en entrée ce vecteur et la clé pour générer un *BioCode* binaire. Ce *BioCode* est ensuite stocké dans la base de données.

La transformation comprend deux étapes : la projection des données biométriques originales dans une matrice orthonormée pseudo-aléatoire (générée à partir de l'aléa stocké sur le token), suivie d'une quantification selon un seuil prédéfini [55], voir figure II.11.

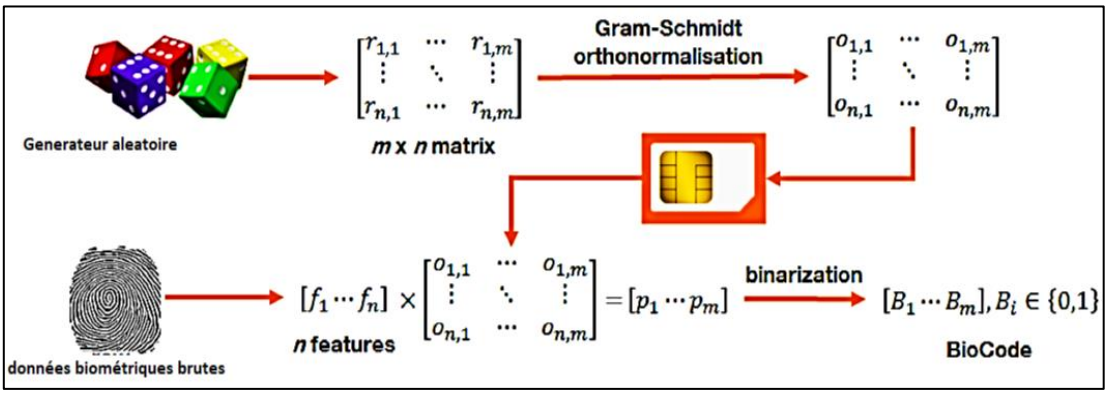


Fig. II.11. Schéma de BioHachage [33]

II.4 Méthode proposée

Dans l'étape d'extraction de caractéristiques, l'image prétraitée est soumise à des opérations mathématiques afin d'extraire les caractéristiques discriminantes, qui doivent remplir deux conditions fondamentales : augmenter la corrélation entre les échantillons de la même classe et la diminuer entre les échantillons de classes différentes. Les méthodes d'extraction de caractéristiques doivent être soigneusement conçues par des spécialistes (ingénierie des

caractéristiques) utilisant leurs connaissances et leur expertise [11]. Généralement, ces techniques sont appliquées à l'image sans connaissance préalable de son contexte. Heureusement, avec l'avènement de l'apprentissage profond, les classifiers eux-mêmes font automatiquement le travail de l'expert dans les couches de convolution.

II.4.1 Gabarit biométrique non sécurisé

La méthode proposée pour l'extraction de gabarits biométriques non sécurisés est basée sur une architecture simple et légère de Deep Learning. Cette technique est largement utilisée dans de nombreuses applications pour fournir un système efficace de reconnaissance de formes. En fait, la méthode d'extraction de caractéristiques utilisée est basée sur PCANet et ICANet. La principale différence entre ces deux méthodes réside uniquement dans la méthode utilisée pour former les filtres de convolution. En effet, PCANet/ICANet utilise respectivement l'analyse en composantes principales (ACP) et l'analyse en composantes indépendantes (ICA) [8] pour constituer des banques de filtres. Contrairement à l'architecture CNN [56], qui donne des valeurs aléatoires pour les poids des filtres, puis les ajuste pour obtenir un taux de reconnaissance élevé, les poids des filtres dans PCANet/ICANet sont initialisés en appliquant l'algorithme PCA/ICA à la base de données d'apprentissage.

Compte tenu de l'importance de la méthode d'extraction de caractéristiques utilisée, dans cette partie, nous expliquerons en détail la méthode d'apprentissage profond PCANet/ICANet. En tant qu'analyse profonde, l'architecture ICANet se compose de trois étapes successives. La première étape consiste à filtrer l'image sur plusieurs stages (couches de convolution), tandis que la deuxième étape réduit la quantité de données (couche de regroupement) et la dernière étape aplatit (couche d'aplatissement) les données sous un vecteur de caractéristiques unidimensionnel. Dans cette section, la méthodologie d'extraction de caractéristiques basée sur PCANet/ICANet en deux étapes (voir Fig. III.12) sera expliquée.

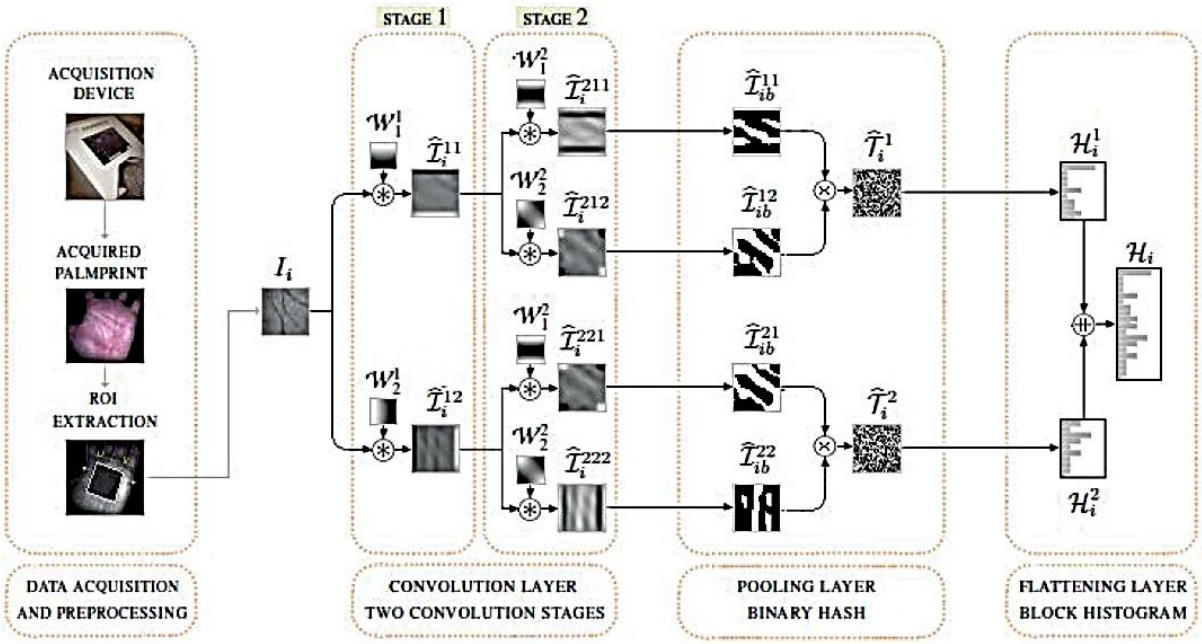


Fig. II.12: Extraction de caractéristiques basée sur PCANet/ICANet en deux-stages

1) Etape de convolution: Soit I_i l'image à traiter et L_1 le nombre de filtres du premier stage (ℓ = 1). A ce stage, l'image est filtrée avec tous les L_1 filtres ($W_j^{\ell}\big|_{j=1..L_1}^{\ell=1}$) comme suit :

$$\hat{\mathrm{I}}_{\mathrm{i}}^{1\mathrm{j}} = \mathrm{I_i} * \mathrm{W_j^1}, \quad \text{où} \quad j = 1, 2, ..., L_1 \tag{1}$$

où $\hat{I}_i^{1j}$, $j = 1, 2, ..., L_1$ désigne l'image filtrée avec le $W_j^{\ell}\big|_{j=1..L_1}^{\ell=1}$ filtre L_1 et * représente l'opération de convolution bidimensionnelle. Dans le deuxième stage, toutes les sorties du premier stage ($\hat{I}_i^{1j}$) sont filtrées par les L_2 filtres du deuxième stage ($W_j^{\ell}\big|_{j=1..L_2}^{\ell=2}$) selon la formule suivante:

$$\hat{I}_i^{2jk} = \hat{I}_i^{1j} * W_{\mathrm{k}}^2, \quad \text{où} \quad j = 1, 2, ..., L_1 \ , k = 1, 2, ..., L_2 \tag{2}$$

où $\hat{I}_i^{2jk}$, k = *1, 2, ..., L_2* désigne l'image filtrée avec le filtre $W_j^{\ell}\big|_{j=1..L_2}^{\ell=2}$.

2) Etape de regroupement : Le but de cette étape est de réduire la quantité de données. Pour ce faire, les sorties du deuxième stage sont soumises à deux procédures principales, la première consiste à quantifier les données, tandis que la seconde consiste à convertir les données quantifiées en valeurs décimales. Pour la première procédure, la fonction Heaviside a été utilisée, qui renvoie 1 si la valeur est positive et 0 sinon.

$$\hat{I}_{ib}^{jk} = \begin{cases} 1 & \text{if} \quad \hat{I}_i^{2jk} > 0 \\ 0 & \text{ailleurs} \end{cases} \qquad j = 1, 2, ..., L_1 \ , k = 1, 2, ..., L_2 \tag{3}$$

Pour le processus de décimation, toutes les sorties binarisées du deuxième stage pour chaque image filtrée ($\hat{I}_{ib}^{jk}$) sont converties avec la formule suivante :

$$\hat{T}_i^{j}(x, y) = \sum_{k=1}^{L_2} 2^{k-1}\, \hat{I}_{ib}^{jk}(x, y), \qquad j = 1, 2, ..., L_1 \tag{4}$$

La sortie de cette procédure sont des images avec des pixels entiers appartenant à l'inervalle $[0, 2^{L_2-1}]$.

3) Etape d'aplatissement : La dernière étape consiste à aplatir le vecteur de caractéristiques de l'image d'entrée. Dans cette étape, chaque image ($\widehat{\mathrm{T}}_{\mathrm{i}}^{\mathrm{j}}$) est divisée en plusieurs blocs superposés/non-superposés, puis l'histogramme (*Histogram of Oriented Gradients-HOG*) de chaque bloc est calculé et concaténé en un histogramme ($\mathcal{H}_i^{j}\big|_{j=1}^{L_1}$) pour représenter chaque sous-image. Ensuite, tous les vecteurs résultants de I_i sont concaténés en un vecteur de caractéristiques ($\mathcal{H}_i$) pour représenter l'image d'entrée :

$$\mathcal{H}_i = [\mathcal{H}_i^1, \mathcal{H}_i^2, \ldots., \mathcal{H}_i^{L_1}] \tag{5}$$

Il est à noter que la méthode d'extraction de caractéristiques basée sur PCANet/ICANet est caractérisée par plusieurs paramètres qui peuvent être modifiés pour obtenir un excellent taux de classification, notamment le nombre de stages de convolution (L), le nombre de filtres dans chaque stage ($L_\ell|_{\ell=1}^{L}$) et la taille des filtres ($k_{1\ell} \times k_{2\ell}$).

II.4.2 Gabarit biométrique sécurisé

Dans le système non sécurisé, deux étapes supplémentaires sont ajoutées. La première étape consiste à transformer les images filtrées en les projetant dans des matrices de projection, tandis que la deuxième étape consiste à déguiser le vecteur de caractéristiques (gabarit). Les deux étapes utilisent des systèmes de chaos.

Etape 1 : Projection : En tant que solution de sécurité, cette étape masque les gabarits biométriques afin qu'ils puissent être annulés et remplacés par un autre à tout moment. Ainsi, les gabarits résultants changent avec le changement de clé secrète tout en préservant, dans la mesure du possible, les performances du système biométrique. Dans notre système, nous avons adopté le principe de la projection de gabarits dans un espace orthogonal. Cette étape contient deux processus, à savoir la génération de l'espace de projection (matrice) et la projection dans l'espace généré. Dans notre proposition, nous avons utilisé la carte logistique unidimensionnelle définie par :

$$\mathcal{L}_i^c(x_0, \mu_i): \qquad x_{n+1} = \mu_i \times x_n(1 - x_n) \tag{6}$$

Où $x_n \in [0,\ 1]$ dénote l'état du système, $x_0 \in [0,\ 1]$ dénote l'état initial du système et $\mu_i \in [3.57,\ 4]$ est le paramètre de contrôle. Dans de tels systèmes, x_0 et μ_i peuvent être utilisés comme clé secrète. Le schéma proposé est présenté dans la figure II.13.

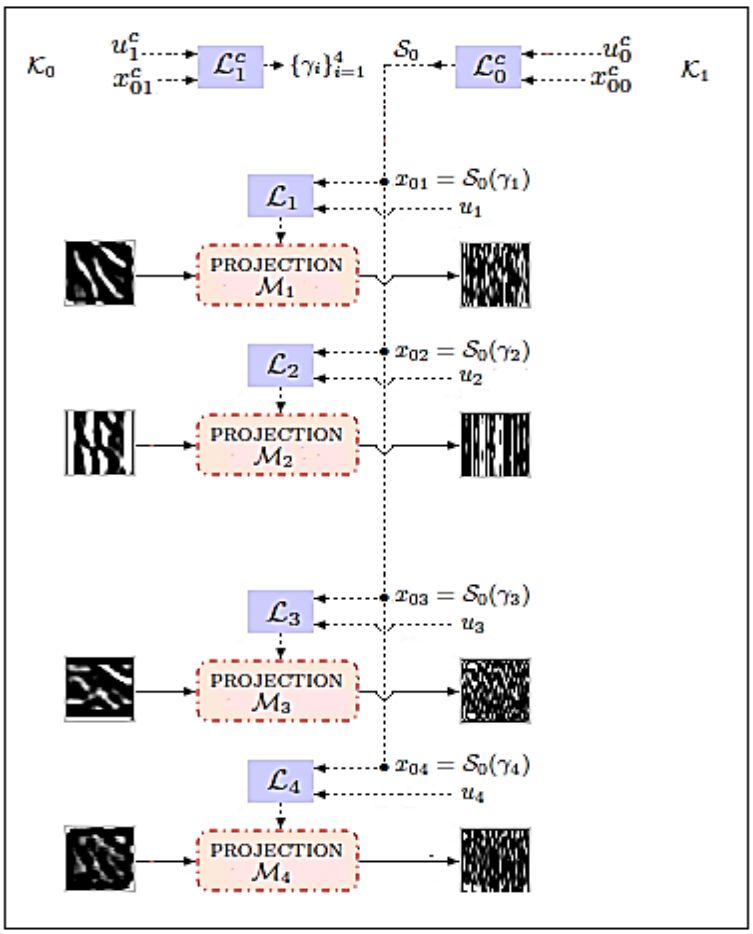


Fig. II.13: Schéma proposé pour la révocabilité

La méthode de révocabilité utilisée dans notre travail est basée sur le principe de transformation. En fait, l'algorithme suivant est exécute :

- La clé $k_1 = (x_{01}^c, \mu_1^c)$ est utilisée par le système chaotique $\mathcal{L}_i^c$ pour générer une séquence S_1. Après normalisation ([0..500]), les N premières valeurs sont utilisées comme coordonnées dans S_0 pour déterminer les états initiaux des N systèmes chaotiques ($\mathcal{L}_i, i = 1..N$), dans notre exemple $N = 4$;
- La clé $k_0 = (x_{00}^c, \mu_0^c)$ est utilisée par le système chaotique $\mathcal{L}_0^c$ pour générer une séquence S_0. Les N valeurs situées à $\gamma_i$dans S_0 $(S_0(\gamma_i))$ sont utilisées comme états initiaux des N systèmes chaotiques ($\mathcal{L}_i, i = 1..N$).
- La sortie de chaque système ($\mathcal{L}_i, i = 1..N$) est réorganisé en matrice M de même taille que l'image filtrée ;
- Décomposition de chaque matrice M_i par la décomposition orthogonale, comme suit:

$$M_i = Q \cdot R \qquad \text{avec} \qquad Q^{-1} = Q^T \tag{7}$$

- Projeter les N image filtrées dans Q

$$\hat{I}_i = I_i \cdot Q \tag{8}$$

Etape 1 : Déguisement: Presque la même idée est utilisée pour déguiser le gabarit biométrique. Cependant, une autre clé est utilisée pour cette étape comme le montre la figure II. 14. En fait, l'algorithme suivant est exécuté :

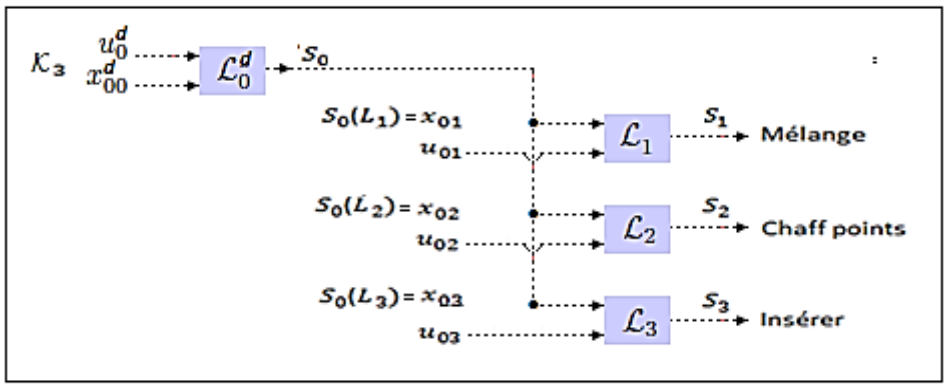


Fig. II.14: schéma proposé pour le déguisement

- La clé $k_3 = (x_{00}^d, \mu_0^d)$ est utilisée par le système chaotique $\mathcal{L}_0^d$ pour générer une séquence S_0. Les 3 valeurs situées à $L_i$dans S_0 $(S_0(L_i))$ sont utilisées comme états initiaux des 3 systèmes chaotiques ($\mathcal{L}_i, i = 1..3$).
- La première séquence S_1 , de même taille que la taille du gabarit, est utilisée pour mélanger le gabarit biométrique;
- La seconde séquence S_2, de taille H, permet de créer H chaff points (dans notre test H est égal à la même taille que la taille du gabarit). Il est à noter que les valeurs des chaff points doivent être dans la même dynamique que les valeurs de gabarit:

$$c_i = \rho \cdot S_2 \quad (9)$$

Où ρ dénote la valeur moyenne de gabarit biométrique.

- La troisième séquence S_3, de taille $2H$, permet de déterminer les positions d'insertion à la fois des composants du gabarit et des chaff points dans un vecteur de taille $2H$;
- Insertion des composants du gabarit et des chaff points dans les positions déterminées précédemment afin de créer un vecteur déguisé de taille $2H$.

II.5 Conclusion

Ces dernières années, l'utilisation des technologies biométriques a conduit à une croissance de la reconnaissance automatique de l'identité humaine. Mais ces systèmes biométriques sont plus adaptés à un niveau de sécurité moyen. En effet, plus le niveau de sécurité est élevé, plus l'utilisation de mécanismes de protection est importante, plus performants et plus surs. Les données biométriques d'un individu sont hautement sensibles en raison de leur association permanente avec l'utilisateur, ce qui justifie des préoccupations croissantes concernant la vie privée et l'anonymat des individus face à toute tentative de piratage. Par conséquent, de nombreuses études se sont concentrées sur la recherche de moyens d'extraire des caractéristiques biométriques qui peuvent être annulées et remplacées à tout moment lorsqu'elles sont compromises [57]. Dans ce chapitre, après avoir présenté les vulnérabilités et les menaces des systèmes biométriques, nous avons évoqué quelques solutions issues de la littérature pour protéger le gabarit biométrique et terminons par une proposition de méthode d'extraction de gabarits biométriques profonds, révocables et cryptés.

Chapitre 3

Résultats Expérimentaux

Evaluations et discussions

Résumé

L'extraction de caractéristiques est une tâche importante dans les applications de reconnaissance de formes basées sur l'image en raison d'une grande quantité de caractéristiques existant dans l'image et de ses multiples domaines d'application. En raison de cette nécessité, un effort très considérable a été fait par les chercheurs dans ce sens, conduisant dans de nombreux cas à d'excellents résultats de classification. Dans ce chapitre, l'impact des techniques d'apprentissage profond sur les performances de ces systèmes sera évalué. Pour une évaluation fiable, un système biométrique basé sur l'empreinte des réseaux veineux a été développé. Dans cette étude, des architectures d'apprentissage profond simples et légères (PCANet et ICANet) ont été utilisées pour le processus d'extraction de caractéristiques. De plus, les gabarits extraits sont mieux protégés par deux méthodes de sécurités, à savoir la révocabilité et le cryptage.

Résultats Expérimentaux

Evaluations et discussions

Les systèmes biométriques sécurisés sont de plus en plus utilisés en raison de leur impact sur le degré de fiabilité de la sécurité de l'information. Un système biométrique sécurisé doit respecter deux contraintes essentielles : la précision exigée par le système biométrique et la sécurité de l'information. Dans ce chapitre, nous nous intéressons à la présentation d'un système biométrique sécurisé basé sur l'empreinte des veines de la paume de la main. Les expériences réalisées dans ce chapitre, qui s'appuient sur une base de données biométriques récente, montrent que notre méthode est plus efficace que plusieurs méthodes existantes.

III.1 Base de données expérimentale

Dans nos expérimentations, nous avons utilisé la base des données d'empreinte palmaire créé par l'Université de Polytechnique de Hong Kong (PolyU) [58], cette base des données a été obtenu par la collection d'images d'empreinte palmaire multi-spectrale de 300 individus à l'aide d'un dispositif de capture d'empreinte palmaire multi-spectrale, ces individus sont des étudient et des travailleurs dans PolyU. Dans ce jeu de données, 195 personnes sont des mâles et les restes sont des femelles, et la distribution de l'âge entre 20 et 60 ans. Les gens ont été invité pour fournir d'environ de 12 images. Les images ont été recueillies dans deux occasions, où les six premières images ont été capturées lors de la première occasion et les six autres ont été capturées dans la deuxième occasion. Cette base de données contient 3600 images en quatre bandes (rouge, bleue, verte et proche infrarouge). Il est important de noter que dans nos tests, nous n'avons utilisé que la bande spectrale proche infrarouge.

III.2 Environnement du développement

Pour tester notre proposition nous avons choisi d'utiliser le logiciel MATLAB qui est un logiciel interactif basé sur le calcul matriciel. Il est utilisé dans les calculs scientifiques et les problèmes d'ingénierie car il résout des problèmes numériques complexes, grâce à une multitude de fonctions intégrées et plusieurs programmes outils testés et regroupés dans des dossiers appelés boîtes à outils ou *Toolbox*. De plus, MATLAB intègre des fonctions prédéfinies dédiées au traitement d'image. Nous avons utilisé MATLAB R2009a, une version 64 bits (win64) sous un ordinateur portable *hp* intégré par un processeur Intel(R) Core(TM) i5-8250U avec une vitesse de 1.60GHz et 6GHo de DRAM. Notre PC utilise Windows 10 comme système d'exploitation.

III.3 Mesure de performance

L'évaluation des performances d'un système biométrique est une étape importante dans le processus de sa conception et de sa mise en œuvre dans la mesure où elle permet de savoir si le système est suffisamment performant pour l'application visée. Elle permet aussi de comparer les systèmes entre eux. Cette performance peut être mesurée principalement à l'aide de plusieurs métriques et visualisée à l'aide de plusieurs courbes de performance.

III .3.1 Taux d'erreur

Afin de comprendre comment déterminer les performances d'un système biométrique, nous devons définir clairement trois critères principaux.

- **Taux de faux rejet :** Ce taux (False Reject Rate-FRR) représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système, il s'exprime par la relation suivante :

$$\text{FRR}\,[\%] = \; 100 \times \frac{Nbr\ des\ clients\ rejetés\ (FR)}{Nbr\ total\ d'accès\ de\ clients} \qquad (1)$$

- **Taux de fausse acceptation :** Ce taux (False Accepte Rate-FAR) représente le pourcentage de personnes qui ne sont pas censées être reconnues mais qui sont tout de même acceptées par le système, il s'exprime par la relation suivante :

$$\text{FAR}\,[\%] \; = 100 \times \frac{Nbr\ des\ imposteurs\ acceptés\ (FA)}{Nbr\ total\ d'accès\ imposteurs} \qquad (2)$$

- **Taux des clients acceptant :** ce taux (Genuine Accepte Rate-GAR) représente le pourcentage de personnes autorisées (clients) qui sont acceptées par le système biométrique, il s'exprime par la relation suivante:

$$\text{GAR}\,[\%] = (1\text{-FRR}) \times 100 \qquad (3)$$

- **Taux d'égale erreur :** Ce taux (Equal Error Rate-EER) est calculé à partir des deux premiers taux et constitue un point commun de mesure de la performance. Ce point correspond à FRR = FAR, c'est à dire le meilleur compromis entre faux rejets et fausses acceptations, il s'exprime par la relation suivante :

$$\text{EER}\,[\%] = 100 \times \frac{Nbr\ de\ FR + Nbr\ de\ FA}{Nbr\ total\ d'accès} \quad (4)$$

III.3.2 Courbes de performance

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

(a) *(b)*

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

III.4 Evaluation de performance

Comme mentionné précédemment, les résultats expérimentaux de notre travail sont divisés en deux parties principales. Dans une première partie, nous présenterons les résultats de l'évaluation des performances du système biométrique non sécurisé. Dans cette partie, nous choisirons les meilleurs paramètres système, qui sont la méthode d'extraction de caractéristiques (ICANet ou PCANet) et le classifier utilisé (KNN ou SVM). Puis, dans une deuxième partie, nous présentons les résultats des tests du système biométrique sécurisé. En fait, nous allons ajouter les couches de sécurité au meilleur système (en utilisant les meilleurs paramètres choisis précédemment) et réévaluer les performances du système ainsi que le niveau de sécurité.

III.4.1 Protocole de tests

Pour tester les performances de notre système biométrique proposé, nous avons divisé la base de données en deux galeries. La première, qui représente 25% soit 1200 images également réparties entre toutes les personnes (3 images pour chaque personne), est destinée à la phase d'enrôlement, tandis que la galerie restante, 75% soit 3600 images (9 images pour chaque personne), a été utilisée pour le processus de test. Cette division nous a permis d'obtenir un nombre total de scores égal à 721800. Parmi ces scores, 3900 scores sont authentiques et 718200 scores sont des scores imposteurs. De plus, nous avons divisé nos expériences en deux sections principales. Dans la première section, nous avons mené plusieurs expériences

afin de choisir les paramètres optimaux des méthodes d'extraction de caractéristiques utilisées, tandis que dans la deuxième section, nous avons examiné les performances du système en utilisant les deux configurations : sécurisée et non sécurisée, en utilisant les meilleurs paramètres sélectionnés.

III.4.2 Extraction de la région d'intérêt (Prétraitement)

Dans les deux systèmes (basés sur le PCANet et basés sur l'ICANet), une tâche de prétraitement pour préparer l'image originale pour la phase d'extraction des caractéristiques est nécessaire. La méthode d'extraction de la région d'intérêt (ROI) appliquée dans notre système est basée sur l'algorithme décrit dans [59].

☑ **Etape 1 :** dans cette étape, nous appliquons un filtre passe-bas (Gaussien) à l'image originale pour lisser l'image, le but du filtrage est de réduire le bruit (voir Fig. III.2).

Fig. III.2 : Image originale filtrée

☑ **Etape 2 :** Un seuil T_P est appliqué, pour convertir l'image original à une image binaire, cette image et nécessaire pour l'application de l'algorithme (bug flowing) (voir Fig. III.3).

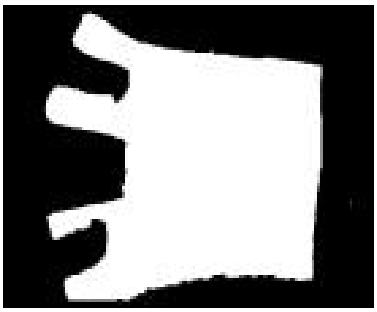


Fig. III.3 : Image binaire

☑ **Etape 3 :** Obtenir le contour extérieur de l'image binaire et les deux points des références F_1 et F_2. l'algorithme utilisé pour l'extraction de contour extérieur est l'algorithme de *bug flowing*. Les deux points F_1 et F_2 sont nécessaires pour localiser la région d'intérêt ROI (voir Fig. III.4).

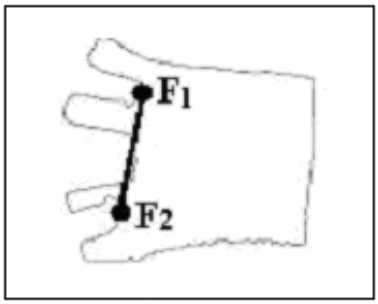


Fig. III.4 : Contour extérieur

☑ **Etape 4 :** Calculer l'angle entre le segment F_1F_2 et l'axe vertical, ensuite tourner l'image par l'angle correspondant pour que le segment F_1F_2 soit perpendiculaire (Voir la Fig. III.5).

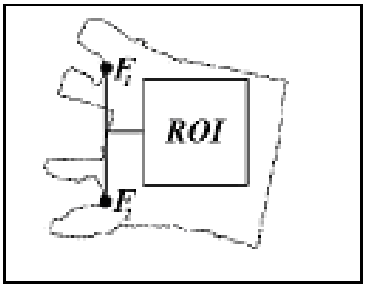


Fig. III.5 : Image tournée

☑ **Etape 5 :** Tourner l'image (originale) avec l'angle calculé précédemment puis localiser la région d'intérêt (voir Fig. III.6).

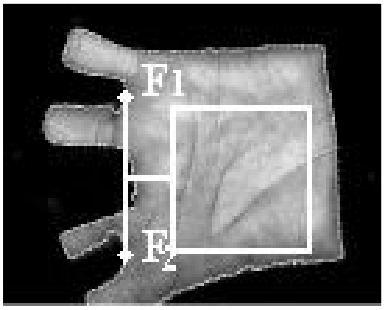


Fig. III.6 : Sélection de la région d'intérêt

☑ **Etape 6 :** Extraction de la région d'intérêt. La région d'intérêt (ROI) à une dimension fixe (128x128 pixels), de sorte que toutes les régions seront conformes à une même dimension (voir Fig. III.7).

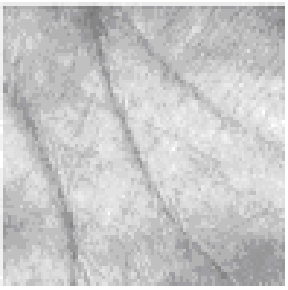


Fig. III.7 : Région d'intérêt ROI

III.4.3 Système biométrique non-sécurisé

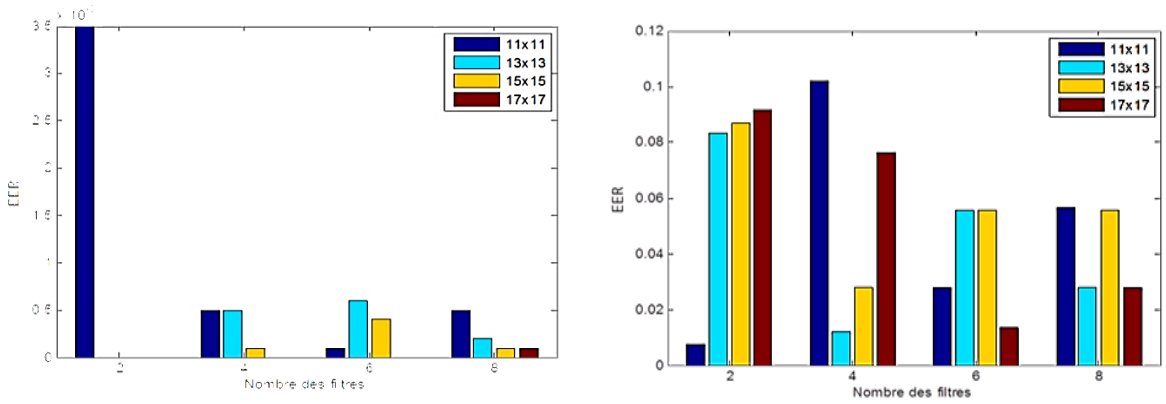
Les méthodes d'extraction de caractéristiques utilisées (PCANet et ICANet) sont caractérisées par plusieurs paramètres, notamment le nombre des stages dans la couche de convolution (L), le nombre de filtres dans chaque stage (L_ℓ) et la taille des filtres dans chaque étage ($k_{1\ell} \times k_{2\ell}$). Pour cela, nous choisissons d'abord les meilleurs paramètres pour les deux méthodes, puis nous examinons les performances du système en fonction de la meilleure configuration.

Les deux méthodes sont structurées pour fonctionner sur une seule étape ($L = 1$) et on va essayer de choisir le nombre de filtres (L_1) parmi quatre nombres prédéfinis [2, 4, 6, 8], en plus, la taille des filtres de convolution ($k_{11} \times k_{21}$) sera choisi parmi quatre tailles prédéfinies [11×11, 13×13, 15×15, 17×17]. En effet, nous examinerons l'effet de ces paramètres sur la précision du système d'identification, nous varions donc le nombre de filtres pour chaque taille de filtre prédéfinie et mesurons la précision du système (performance du système) en utilisant les deux classifiers (SVM et KNN). Il est à noter que nos méthodes d'extraction de caractéristiques (PCANet et ICANet) utilisent une technique d'extraction de gabarit basée sur l'analyse d'images par blocs à l'aide de HOG, pour cela nous avons limité les tests à la configuration suivante : taille de bloc d'analyse 40×40, taux de chevauchement de blocs 50%, HOG taille de fenêtre 7x7 et enfin le BIN est égal à 9.

Les résultats obtenus sont présentés dans le tableau III.1, qui contient les résultats expérimentaux des deux méthodes d'extraction de caractéristiques utilisées avec les deux classifiers utilisés. De plus, les figures III.8 et III.9 montrent une comparaison entre les différentes configurations pour les deux classifiers.

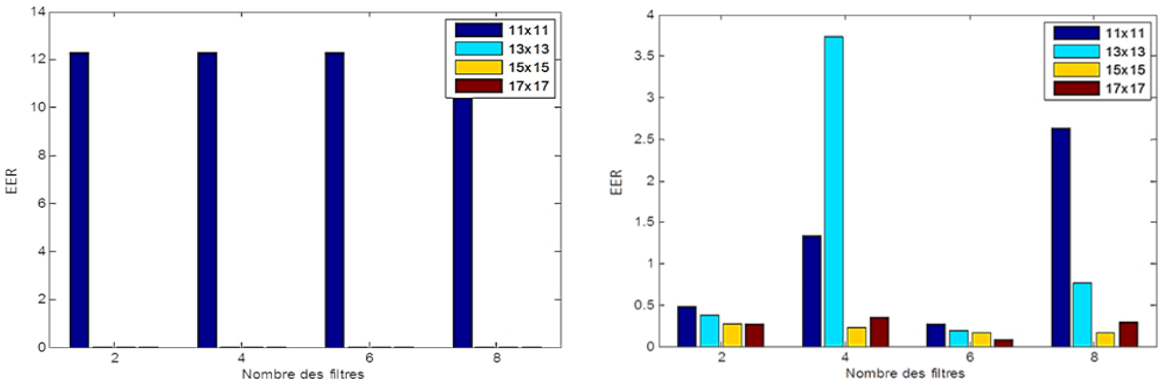
L_1	$k_{11} \times k_{21}$	SVM				KNN			
		PCANet		ICANet		PCANet		ICANet	
		T_0	EER	T_0	EER	T_0	EER	T_0	EER
2	11×11	0.3304	0.0035	0.4088	0.0077	0.2413	0.0315	0.3702	0.4885
	13×13	0.3560	0.0000	0.4065	0.0833	0.5894	0.0144	0.3937	0.3826
	15×15	0.3650	0.0000	0.4085	0.0876	0.5886	0.0222	0.3965	0.2735
	17×17	0.3800	0.0000	0.4029	0.0918	0.5810	0.0278	0.3916	0.2763
4	11×11	0.3241	0.0005	0.3830	0.1020	0.2413	0.0325	0.3260	0.3438
	13×13	0.3241	0.0005	0.4057	0.0121	0.5894	0.0144	0.2747	0.7321
	15×15	0.3360	0.0001	0.3767	0.0278	0.5886	0.0222	0.4041	0.2306
	17×17	0.3500	0.0000	0.3832	0.0762	0.5810	0.0278	0.3965	0.3561
6	11×11	0.3240	0.0001	0.3729	0.0278	0.2413	0.0305	0.3887	0.2733
	13×13	0.3031	0.0006	0.3648	0.0556	0.5894	0.0144	0.4124	0.1944
	15×15	0.3150	0.0004	0.3593	0.0556	0.5886	0.0222	0.4143	0.1667
	17×17	0.3240	0.0000	0.3854	0.0134	0.5810	0.0278	0.4154	0.0833
8	11×11	0.3211	0.0005	0.3931	0.0568	0.2413	0.0365	0.2812	0.6353
	13×13	0.3030	0.0002	0.3524	0.0278	0.5894	0.0144	0.3554	0.7648
	15×15	0.3120	0.0001	0.3589	0.0556	0.5886	0.0222	0.4110	0.1667
	17×17	0.3090	0.0001	0.3995	0.0278	0.5810	0.0278	0.3665	0.2961

Tableau III.1 : Test de performance du système biométrique basé sur PCANet et ICANet.



(a) *(b)*

Fig. III.8: Test de performance du système biométrique basé sur le SVM : (a) PCANet et (b) ICANet.



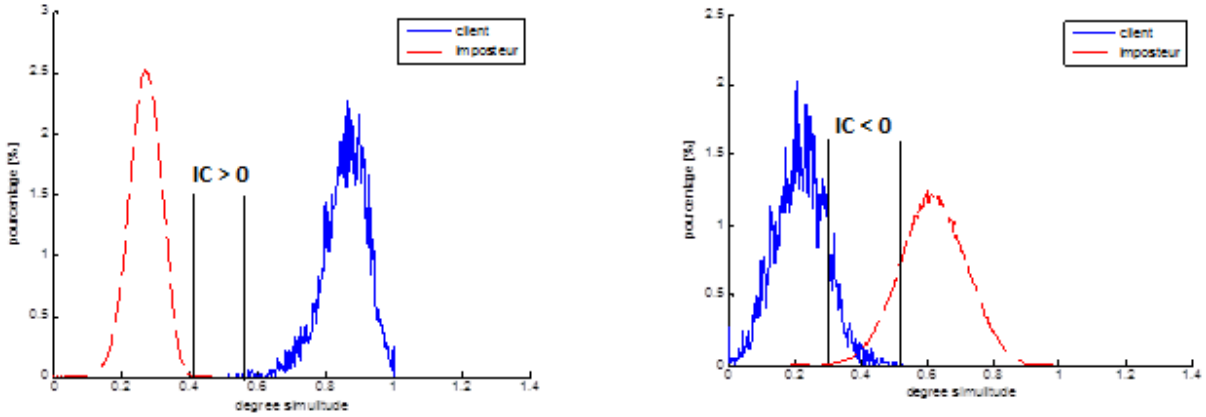
(a) *(b)*

Fig. III.9: Test de performance du système biométrique basé sur le KNN : (a) PCANet et (b) ICANet.

Ainsi, par une analyse judicieuse de ces résultats expérimentaux, nous pouvons tirer les observations suivantes :

- L'observation préliminaire de ces résultats prouve l'excellente efficacité des méthodes d'analyse profond pour produire des vecteurs de caractéristiques (gabarits) capables de présenter efficacement le contenu de l'image. La plus grande valeur d'erreur obtenue est EER = 0,7648% (avec un seuil *To* égal à 0,3554) dans le cas d'ICANet avec 8 filtres de taille 13x13 chacun et le classifier KNN. De plus, le système d'identification biométrique peut parfaitement fonctionner (EER = 0,00%) dans de nombreux cas.
- Plus la taille du filtre utilisé est importante, plus le système d'identification biométrique fonctionne avec une excellente précision (EER → 0,000%).
- Comparé à ICANet, le système d'identification biométrique basé sur PCANet a montré une supériorité remarquable dans tous les cas.
- De même, par rapport au SVM, le système d'identification biométrique basé sur KNN a montré une supériorité remarquable dans tous les cas.

Le système d'identification biométrique proposé fonctionne parfaitement dans la plupart des configurations, d'autres critères doivent donc être pris en compte pour juger des méthodes d'extraction de caractéristiques utilisées. Par conséquent, nous avons utilisé l'intervalle de confiance (IC), qui mesure le taux de séparation des deux distributions (authentique et imposteur). En effet, plus l'IC obtenu est grand, plus le système d'identification biométrique est précis, la figure III.10 illustre de cet intervalle.



(a) *(b)*

Fig.III.10: Illustration de l'intervalle de confiance. *(a)* Intervalle de confiance positif et *(b)* Intervalle de confiance négatif.

Dans nos résultats expérimentaux, le meilleur IC obtenu est égal à 0.4055 - 0.3700 = 0.0355 pour le cas d'un classifier SVM avec 2 filtres de taille 17×17. Enfin, il convient de noter que nous n'avons testé le système qu'en un seul stage, car il a atteint des performances parfaites et qu'il n'est donc pas nécessaire de le tester dans d'autres stages. Sur la base des résultats décrits ci-dessus, nous pouvons affirmer l'efficacité de l'apprentissage profond dans la reconnaissance d'images, en particulier la méthode d'extraction de caractéristiques basée sur PCANet.

III.4.4 Système biométrique sécurisé

Dans cette partie, nous examinons en détail les performances du système biométrique sécurisé. Avant de commencer, il convient de mentionner que notre système utilise une méthode hybride pour sécuriser le gabarit biométrique, à savoir la révocabilité et le cryptage.

✍ **Performance de système biométrique:** Il est à noter que l'implication de la partie révocabilité peut souvent dégrader les performances du système, alors que l'implication de la partie cryptage ne modifie pas ces performances. Par conséquent, nous réévaluerons le système après avoir ajouté la partie révocabilité. En effet, afin d'évaluer sérieusement le système biométrique révocable proposé, trois points principaux liés à son comportement doivent être examinés. Ces points sont :

✍ Les scores trouvés par le système biométrique sécurisé doivent présenter des distributions (authentiques et imposteurs) presque similaires à celles présentées par le système biométrique non sécurisé.

- Les distributions trouvées par le système biométrique sécurisé ne doivent pas changer de manière significative lors de l'utilisation de différentes clés secrètes.
- Un changement soudain des scores authentiques en dessous du seuil de sécurité (To) lors de l'utilisation d'une fausse clé de sécurité (tentative d'attaque). Le meilleur cas est lorsque tous les scores d'attaque sont inférieurs au point FAR = 0.

Pour le premier point, nous avons comparé les performances du système sécurisé et non sécurisé afin de voir le changement qui peut se produire sur le comportement du système sécurisé lors de l'intégration de la couche de sécurité. Pour ce faire, nous choisissons aléatoirement deux clés de sécurité, et nous mesurons les performances du système biométrique sécurisé (à l'aide de 2 filtres de taille 17x17 et d'un classifier SVM) et les résultats sont présentés dans le tableau III.2.

Clés	système non-sécurisé		système sécurisé	
$k_1 = (x_{01}^c, \mu_1^c)$	To	EER	To	EER
(0.12, 3.58)			0.3800	
(0.37, 3.74)	0.3800	0.000	0.3791	0.000
(0.92, 3.98)			0.3821	

Tableau III.2 : Test de performance du système biométrique sécurisé sous plusieurs clés.

D'après les résultats obtenus, on peut conclure que le comportement général du système sécurisé n'a pas changé et reste similaire au système non sécurisé.

Pour le deuxième point, il suffit de prouver que le système sécurisé peut fonctionner avec un seul seuil, quel que soit le changement de la clé secrète, et ceci ne peut être atteint que si les différents scores changent dans le même intervalle. Nous pouvons voir dans le tableau III.2 que les différents seuils de sécurité ont varié dans le même intervalle pour les deux systèmes, nous pouvons donc effectivement utiliser le même seuil (*To*) du système biométrique non sécurisé (*To* = 0,3800).

Dans le troisième point, nous examinerons le comportement du système sécurisé lors d'une attaque. Ainsi, dans nos tests, tous les utilisateurs sont enregistrés dans la base de données par ($k_0 = (0.75, 0.88)$ et $k_1 = (0.70, 0.61)$) et dans le test d'identification nous utilisons d'autres clés (nous changeons au moins une clé). Ainsi, pour voir les performances des systèmes d'identification vis-à-vis des attaques, sur la Fig. III.11, nous illustrons les résultats des tests avec deux fausses clés. Dans ces figures, il est clair que tous les scores d'attaque sont complètement décalés en dessous du seuil de sécurité (en dessous de 0,3800). Il est très remarquable que le point, où le taux d'attaque est nul (0,2610), soit beaucoup plus petit que le point 0,3800, ce qui reflète l'efficacité et la robustesse de notre système contre toute attaque possible. À partir de ces résultats, nous pouvons clairement voir l'efficacité de notre système proposé, qui peut fonctionner en toute sécurité avec un EER minimum de 0,0000 % avec un seuil de 0,3800 pour la modalité basée sur le réseau veineux de la paume.

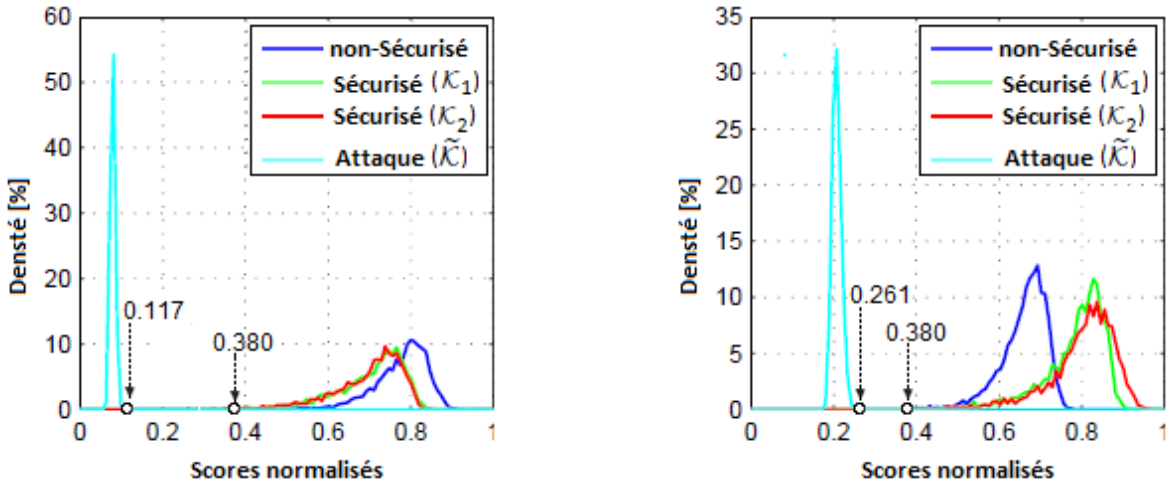


Fig.III.11: Test de performance du système biométrique utilisant deux fausses clés. *(a)* $k_0 = (0.11,0.59)$ et *(b)* $k_1 = (0.31, 0.81)$

✍ **Analyse de sécurité:** Cette partie vise à évaluer le niveau de sécurité lorsque notre système est exposé à diverses attaques sur des gabarits biométriques, nous allons donc mener une analyse de sécurité pour vérifier la robustesse de la méthode proposée face à d'éventuelles attaques. En effet, lors de la conception d'un système biométrique sécurisé, les contraintes suivantes doivent être prises en compte :

- Même si la structure du système est connue, le gabarit biométrique est pratiquement introuvable ;
- L'impossibilité de trouver des gabarits biométriques à travers une recherche exhaustive, donc l'espace de clés doit être très grande.
- Un petit changement dans la clé sécrète produit des gabarits biométriques complètement différents.

Il convient de noter que notre système biométrique sécurisé (Hybride : révocabilité + cryptage) fonctionne avec trois systèmes chaotiques principaux ($\mathcal{L}_0^c$, $\mathcal{L}_1^c et\ \mathcal{L}_1^d$) et $3 + \xi$ avec $\xi = \Pi_{i=1}^{\ell} L_1$ systèmes chaotiques auxiliaires ($\mathcal{L}_i|_{i=1}^{\xi}$). Les principaux systèmes chaotiques ont pour rôle de faire varier l'état initial des systèmes chaotiques auxiliaires. En général, les paramètres qui contrôlent la sécurité de notre système sont les états initiaux de $\mathcal{L}_0^c$ et $\mathcal{L}_1^c$ ($x_{0i}|_{i=1}^{2}$) ainsi que les paramètres de contrôle de $\mathcal{L}_0^c$, $\mathcal{L}_1^c$, $\mathcal{L}_1^d$ et $\mathcal{L}^i|_{i=1}^{3+\xi}$ (u_0^c, u_1^c, $u_i|_{i=1}^{3+\xi}$).

Analyse de l'espace clé : Dans cette partie, nous allons calculer l'espace de tentatives (utilisant tous les systèmes chaotiques) qui permet à l'attaquant de récupérer le gabarit biométrique. En effet, soit $S^x, \tilde{S}^x, S^u, \tilde{S}^u$ quatre séquences générées par le même système chaotique dans les conditions suivantes :

$$\begin{cases} S^x = \mathcal{L}_0^c(x_{01}^c, \mu_1^c) \\ \tilde{S}^x = \mathcal{L}_0^c(x_{01}^c + d, \mu_1^c) \end{cases} \qquad \begin{cases} S^\mu = \mathcal{L}_0^c(x_{01}^c, \mu_1^c) \\ \tilde{S}^\mu = \mathcal{L}_0^c(x_{01}^c, \mu_1^c + \mathrm{d}) \end{cases} \tag{5}$$

Où d est une très petite valeur. L'erreur absolue moyenne $\varepsilon_\ell|_{\{x,u\}}$ pour le système chaotique est définie comme suit :

$$\varepsilon_\ell(\mathcal{S}^\ell, \tilde{\mathcal{S}}^\ell) = \frac{1}{L^\ell}\sum_{j=1}^{L^\ell}\left|\mathcal{S}^\ell(j) - \tilde{\mathcal{S}}^\ell(j)\right| \quad (6)$$

Ainsi, l'espace des clés pour x_0, appelé s_x qui vaut $1/d_x$, où d_x est la valeur de d pour laquelle $\varepsilon_\ell = 0$. La même chose pour l'espace des clés de μ qui appelé s_μ, il est égal à $1/d_\mu$, où d_u est la valeur de d pour laquelle $\varepsilon_\ell = 0$. Comme on a déjà mentionné, notre système utilise trois systèmes chaotiques principaux $\mathcal{L}_0^c$, $\mathcal{L}_1^c$, $\mathcal{L}_1^d$ et $\mathcal{L}^{\mathrm{i}}|_{\mathrm{i}=1}^{3+\xi}$ (u_0^c, μ_1^c, $\mu_i|_{\mathrm{i}=1}^{3+\xi}$) systèmes chaotiques auxiliaires, ainsi, l'espace des clés total de chaque groupe devient :

$$\mathcal{S}_{principal} = s_x^{c0} \cdot s_u^{c0} \cdot s_x^{c1} \cdot s_u^{c1} \cdot s_x^{d0} \cdot s_u^{d0} \quad (7)$$

$$\mathcal{S}_{\text{auxiliaire}} = \prod_{i=1}^{3+\xi} s_u^{\mathrm{i}} \quad (8)$$

Donc, l'espace des clés totale est :

$$S_g = \mathcal{S}_{principal} \cdot \mathcal{S}_{\text{auxiliaire}} = s_x^{c0} \cdot s_u^{c0} \cdot s_x^{c1} \cdot s_u^{c1} \cdot s_x^{d0} \cdot s_u^{d0} \cdot \prod_{i=1}^{3+\xi} s_u^{i} \quad (9)$$

Pour tout système logistique, la valeur de s_x est égale à $1.011 \cdot 10^{16}$ et la valeur de s_μ est égale à $0.241 \cdot 10^{16}$. Par conséquent, l'espace des clés total de notre schéma devient :

$$\mathcal{S}_{principal} = (1.011)^3 \cdot 10^{48} \cdot (0.241)^3 \cdot 10^{48} = 1{,}01446 \cdot 10^{96} \quad (10)$$

$$\mathcal{S}_{\text{auxiliaire}} = (0.241)^{3+\xi} \cdot 10^{48+16\xi} \quad (11)$$

Notre système utilise 2 filtres dans la couche de convolution, donc $\xi = 2$:

$$\mathcal{S}_{\text{auxiliaire}} = (0.241)^5 \cdot 10^{48+80} = (0.241)^5 \cdot 10^{128} = 0.70968 \cdot 10^{128} \quad (12)$$

Donc l'espace de clé est :

$$\mathcal{S}_g = 0.70968 \cdot 10^{128} \cdot 1{,}01446 \cdot 10^{96} = 0.7199 \cdot 10^{244} \quad (13)$$

Il est clair que notre système est très efficace car il donne un espace de clé plus important que de nombreuses méthodes de la littérature.

III.5 Conclusion

Aujourd'hui, les techniques d'apprentissage profond sont largement utilisées dans de nombreuses applications pour fournir un système de reconnaissance de formes efficace. L'objectif principal de cette étude est de montrer la performance de ces techniques dans le développement d'un système biométrique. Malheureusement, ces systèmes sont vulnérables à une variété d'attaques, dont peut-être la plus grave est l'attaque du gabarit, ce qui rend la sécurité de ce gabarit plus importante dans la conception des systèmes biométriques. Ce travail suggère donc une méthode d'extraction de caractéristiques efficace qui peut fournir un gabarit biométrique profond, révocable et crypté. Les résultats obtenus sont très excellents.

Conclusion Générale

Conclusion et Perspectives

Avec le développement rapide de la technologie numérique et la transformation rapide de divers domaines vers la numérisation, en particulier dans des domaines sensibles tels que les institutions financières, la sécurité de l'information est devenue une nécessité pour gagner la confiance des clients, et pour atteindre une expansion rapide et des bénéfices accrus. En effet, les technologies biométriques, notamment avec les progrès des techniques d'intelligence artificielle, ont prouvé leur efficacité mais elles restent insuffisantes, surtout dans les applications de haut niveau de sécurité.

Dans cette mémoire, un système biométrique basé sur une nouvelle méthode d'extraction de caractéristiques est proposé. Cette méthode extrait des gabarits biométriques profonds, révocables et cryptés pour garantir à la fois des performances élevées et une sécurité renforcée (basée sur des systèmes chaotiques). Dans notre étude, nous utilisons les modalités biométriques des réseaux veineux de la paume puisqu'il existe une base de données biométriques connue et disponible. Les expérimentations menées dans cette thèse ont été réalisées sur une base de données moyenne contenant 300 personnes. De plus, pour la classification, nous avons utilisé deux classifiers célèbres, à savoir KNN et SVM. Les résultats expérimentaux ont montré un taux d'identification élevé ainsi qu'un grand espace clé. Nous nous envisageons dans les travaux futurs d'utiliser d'autres méthodes d'extraction de caractéristiques ainsi que d'autres systèmes hyper-chaotiques tels que les attracteurs de Rössler, Lorenz et Hénon.

Bibliographies

[1] Z. Jin, A. Teoh, B. Goi and Y. Tay, "Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation", *Pattern Recogn*, 1(56), pp. 5062, 2016.

[2] C. Jonietz, E. Monari, H. Widak and C. Qu, "Towards mobile and touchless fingerprint verification", In: *Int Conf. on Ad- vanced Video and Signal Based Surveillance (AVSS)*, pp.1 6, Aug 2015.

[3]T. Dang, Q. Truong ,T. Le and H.Truong, "Cancelable fuzzy vault with periodic transformation for biometric template protection", In:*IET* Biometrics, 5(3), pp. 229235, **2016.**

[4] J. Laufenberg, T. Kropf, and O. Bringmann,"Stastic Analysis of Controller Area Network Communication for Attack Detection", Eur J Secur Res, **2022.**

[5] J. Ashbourn, " Guide To Biometrics For Large-Scale Systems " , Springer **2011.**

[6] R. Bendjenna, "Protéger l'échange d'information via un système crypto-biométrique ", thèse de master en informatique, université larbi tebessi –tebessa, **2021.**

[7] Mr. A.SABRI "la sécurité de la transmission des données biométriques dans un réseau " Thèse du Doctorat en sciences, université Oran des sciences et Technologies, **2019.**

[8] " introduction à la sécurité informatique" **https://images.app.goo.gl/DcrnY9BWb1rWSWNX9**

[9] I. SSINI, A.BADRI, K.SAFI, H.LEBBAR and A. BALLOUK " Technique avancée pour le tatouage des images Médicales " Laboratoire d'électronique, Electrotechnique, Automatique,université Hassan IL Casablanca, Maroc.

[10] "la cryptographie et la stéganographie" **https://images.app.goo.gl/D1kyeYyCDUFiTYHL6**

[11]St.Paul(Minnesota), "Biométrie dans l'application de la loi et la pravention du crime" Université d'État métropolitaine, **Avril1999.**

[12] Youcef. HAMLA and Loukman. ATMANIA "reconnaissance biométrique basée sur l'empreinte palmaire multi spêctrale " master en télécommunication, université larbi tebessi-tebessa, **2018.**

[13] S. BOUDJELIAL, "Détection et identification d'individu par méthode biométrique", Thèse de Magister en Electronique, Université Mouloud Mammeri de Tizi-Ouzou, **2014.**

[14]Z. Guo, D. Zhang, L. Zhang, and L. Wenhuang, "feature band selection for online multispectral palmprint recognition ", IEEE transactions on Information Forensics and security, Vol. 7, No. 3, pp.1094-1099,**June 2012.**

[15] Linda. GASMI, "Deep Learning for face Recognition Deep Learning for face Recognition'' MEMOIRE de fin d'etude Présenté pour l'obtention du diplôme de MASTER, Université Mohamed Boudiaf- M'SILA, **2020.**

[16] Frédéric. MASSICOTE," la biométrie, sa fiabilité et ses impacts sur la pratique de la démocratie libérale ", Université de Québéc à Montréal, mémoire présenté comme exigence partielle de la maitrise en science politique, **2007.**

[17] Gilles. ZEMOR, "cours de cryptographie ", Cassini, **2000.**

[18] Chafia. FERHAOUI, "Un Cryptosystème à Base de la Biométrie Pour l'Authentification", Magister en Informatique Ecole nationale Supérieure d'Informatique (E.S.I) (ex. I.N.I) **, 2010.**

[19] Ibtissem. BECHENNANE, "Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus " ,diplôme de doctorat en sciences, Université des Sciences et de la Technologie d'Oran Mohamed Boudhiaf , **2016.**

[20] L .Zhu, and S. Zhang, "multimodal biometric identification system based on finger Geometry, knuckle print and palmprint", pattern recognition letters, Vol. 31,pp.1641-**2010.**

[21] G. Boreki, and A. Zimmer, "Hand geometry: a new approach for feature extraction", Fourth IEEE Workshop on Autimatic Identification Advanced Technologies, pp. 149-154, **2005.**

[22] F. Perronnin, and J. DUGELAY, "An Introduction to biometrics audio and Video-Based Person Authentication ". Volume, No. 4, **2002.**

[23] N. Joshitha J, R. S. Mdona, "Image Fusion using PCA in multifeature Based Palmp-rint Recognition" , international Journal of Soft Computing and Engineering-IJSCE, Vol. 2, No. 2, pp. 226-230, **2012.**

[24] Jain, A. K., Griess, F. D. and Connell, S. D, "On-line signature verification", Pattern Recognition, Vol. 35, No. 12, pp. 2963- 2972, 2002.

[25] L. Alano, "la biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquée aux bases de personnes virtuelles", thèse de doctorat, Institut national des télécommunications, Université d'Evry d'Essonne, **2009.**

[26] Matthieu. WIROTIUS, "Authentification Par Signature Manuscrite Sur Support Nomade", Thèse Pour Obtenir Le Grade De Docteur De L'université de Tours, **2005.**

[27] A. Bouchemha. "Etude et Application des transformées géométriques à la Compression des images hautes résolutions et à la Biométrie (Authentification/Vérification de l'empreinte palmaire) ". Doctoral dissertation, Université de Annaba, **2016.**

[28] Nicolas. MORIZET, "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris", Thèse Pour Obtenir Le Grade De Docteur de l'Ecole Nationale Supérieure des Télécommunications, **2009.**

[29] Anis. CHAARI, " Nouvelle approche d'identification dans les bases de données biométrique basée sur une classification non supervisée", thèse de doctorat pour Ingénieur et Informatique, Université d'Evry Val d'Essonne, **2009.**

[30] E. Cherrier, "Authentification biométrique : comment (ré) concilier sécurité, utilisabilité et respect de la vie privée ? ", le diplôme de Habilitation à Diriger des Recherches, Normandie Université.

[31] N. Ratha, J. Connell, and R. M. Bolle. "Enhancing security and privacy in biometrics based authentication systems". IBM Systems, 40(3) :614–634, **2001.**

[32] V. JShalamanov, S. Matern, and G. Penchev "Digitalization and Cyber Resilience Model for the Bulgarian Academy of Sciences", Tagarev T., Atanassov K.T., Kharchenko V., Kacprzyk J. (eds) Digital Transformation, Cyber Security and Resilience of Modern Societies. Studies in Big Data, vol 84. Springer, Cham, **2021.**

[33] TAKOUA. GUIGA " Anthentification transparente dans un environnement numérique ubiquitaire ", diplôme de doctorat, au sein de l'Université de Caen Normandie.

[34] A. Juels and M.Wattenbeg. "A fuzzy commitment scheme. In 6th ACM Conference on Computer and Communication Security", pages 28-36,**1999.**

[35] A. Juels and M. Sudan. "A fuzzy vault scheme. In Proceedings of IEEE International Symposium on Information Theory", **2002.**

[36] A. Goh and C. Ngo. " Computation of Cryptographic Keys from Face Biometrics", volume 2828 of LNCS. Springer, Berlin, **2003.**

[37] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in 2007 Biometrics Symposium. IEEE, pp. 1–6, **2007.**

[38] S. H. Strogatz. " Nonlinear dynamics and chaos", Addison-Wesley, **1994.**

[39] K. Anil Jain " Fingerprint-based Fuzzy Vault: Implementation and Performance Karthik Nandakumar", Student Member, IEEE, Fellow, IEEE and Sharath Pankanti, Senior Member, IEEE.

[40] J.-P .Linnartz and P. Tuyls. "New shielding functions enhance privacy and prevent misuse of biometric templatesc. In Proc. 4th International Conference on Audio- and Video-based Biometric Person Authentification, **2003.**

[41] G. I. Davida, Y .Frankel, and B. J. Matt, "On enabling secure applications through on-line biometric Identification", In Proc. 1998 IEEE Symposium on Privacy and Security, pages 148-157,**1998.**

[42] "La biométrie, une technologie protectrice de la vie privée?", https://www.biometrie-online.net/biometrie/biometrie-et-vie-privee

[43] R.M. Bolle, J.H. Connel, and N.K. Ratha. "Biometric perils and patches. Pattern Recognition", 35(12) :2727–2738, **2002.**

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

[45] Y. Cheng Feng, C. Pong Yuen, and K . Anil Jain. A "hybrid approach for generating secure and discriminating face template". IEEE Transactions on Information Forensics and Security,5(1) :103_11, **2010.**

[46] T. Song Ong, A. Teoh Beng Jin, and D. Chek Ling Ngo, "Application specific key release scheme from biometrics". IJ Network Security, 6(2) :127_133, **2008.**

[47] F. Jessie , W. Mac, and N.J.A. Sloane. "The theory of error correcting codes", vol 16. Elsevier. **1977,**

[48] M. Savvides, K. Vijaya, B.V.K. and P.K. Khosla, "Cancelable Biometrics Filters for Face Recognition". Int. Conf. of Pattern Recognition, vol.3: 922-925, **2004.**

[49] **S.** Hirata, and K. Takahashi, "Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching". Lecture Notes in Computer Science 5558: 868-878, **2009.**

[50] M.Y. Jeong, et al. "Changeable Biometrics for Appearance Based Face Recognition". Biometric Consortium Conference, Biometrics Symposium : 1-5, **2006.**

[51] C. H. Lee, C.Y. Choi, and K.A. Toh, " Alignment-Free Cancelable Fingerprint Templates Based on Local Minutia Information". *IEEE Transactions on Systems, Man and Cybernetics, Part B,* vol. 37, no. 4: 980-992, **(2007b).**

[52] S. Tulyakov, F. Farooq, P. Mansukhani and V. Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems'', Pattern Recognition Letters 28, 427–2436, **2007.**

[53] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," IEEE Trans. Pattern Anal. Mach. Intell, vol. 29, no. 4, pp. 561–572, **Apr. 2007.**

[54] A.B.J. Teoh, D. Ngo, and A. Goh. " Biohashing : two factor authentication featuring fingerprint data and tokenised random number". Pattern recognition, 40, **2004.**

[55] E. Cherrier, P. Lacharme, and C. Rosenberger, " La biométrie révocable : principes et limites. In Atelier de Protection de la Vie Privée" (pp. 6-p), (APVP **2012**).

[56] **"**Qu'est-ce que le tatouage numérique?**"**. Sécurité – 2022 https://fr.theastrologypage.com/digital-watermarking

[57] S. Djeddi , F. and Z. Mahdjoub , "Renforcement de la sécurité des systèmes biométriques à l'aide des caractéristiques profondes de la biométrie de la main ", université larbi tebessi tebessa, **2020.**

[58] The Hong Kong Polytechnic University; PolyU MSP multispectral palm print Database, http://www.comp.poly.uedu.hk/sbiometrics/MultispectralPalmprint/MSP.htm.

[59] V. Roux, S. Aoyama, K. Ito, and T. Aoki, "Performance improvementof phase-based correspondence matching for palmprint recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. , pp. 70–77, **2014.**

[60] Soltani, F, Drzewiecki, G. Nonlinear dynamics equations and chaos. IEEE Conference. Vol 29, Issue, 22-23 March ,**2003.**

[61] Heinz-Otto Peitgen, Hartmut Jürgens, Dietmar Saupe. Fractals for the classroom: Part 1: Introduction to fractals and chaos. Springer-Verlag New York Inc. **1992.**

[62] T. Yoshida, 1 H. Mori, 1 and H. Shigematsu 1 "Analytic Study of Chaos of the Tent Map: Band Structures, Power Spectra, and Critical Behaviors", Journal of Statistical Physics, VoL 31, No. 2, 1983.

[63] X. Zhang1 and Y. Cao2,3 Research Article "A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme", Hindawi Publishing Corporatione Scientific World Journal https://www.hindawi.com/journals/tswj/713541/2014.

[64] The 10th International conference on Engirneering Mathematics and physics, " Logistic Map: Stability and Entrance to Chaos", Journal of Physics conference series 2021**.**

[65] " carte logistique" https://stringfixer.com/fr/Logistic_map.

[66] X. Zhang1 and Y. Cao2,3 Research Article "A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme", Hindawi Publishing Corporatione Scientific World Journal https://www.hindawi.com/journals/tswj/713541/**2014.**

Glossaire

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

ADN : Acide DésoxyriboNucléique.

AES : Advanced Encryption standard

CNN : Convolutional Neural Network.

DES : Data Encryption standard

DRA : Directive régionale d'aménagement

EER : Equal Error Rate.

FAR : False Acceptance Rate.

FRR : False Rejection Rate.

GAR : Genuine Acceptance Rate.

PolyU : Histogramme of Oreinted Gradient.

ICANet : Indépendant Component Analysis Network.

KNN : K- Nearest Neighbors.

PCANet : Principal Component Analysis Network.

ROI : Region Of Interest.

ROC : Receiver Operating Curve.

RSA : Rivest Shamir Adleman.

SVM : Support Vector Machine.

USB : Universal Serial Bus.

Annexe A

Systèmes

Chaotiques

A.1 Carte logistique

Soltani et al, en 2003 [60] montré que le chaos, également appelé comportement étrange, est actuellement l'un des sujets les plus passionnants de la recherche sur les systèmes non linéaires.

Le chaos est un comportement apériodique dans un système déterministe qui montre une dépendance sensible aux conditions initiales. Fondamentalement, c'est un phénomène qui se produit largement dans les systèmes dynamiques non linéaires. Le système chaotique présente un comportement apparemment aléatoire et imprévisible. Dans un système déterministe partant d'une condition initiale exactement connue, nous pouvons répéter la séquence de résultats autant de fois que nous le souhaitons. Alors que, dans un système purement aléatoire (probabiliste), la séquence des résultats ne peut pas être répétée, discuté par Hei nz-Otto Peitgen et al, en 1992 [61].

La dynamique chaotique est omniprésente dans la nature et le comportement chaotique peut être trouvé dans de nombreux systèmes physiques et cartes mathématiques. Il existe les cartes en temps continu bien connues : carte de Lorenz, système de Chen, Van de Système Pol, système Rossler, système Duffing, etc. Cependant, comparés aux cartes discrètes, ils ne conviennent pas pour être appliqués en cryptographie. Pour les cartes chaotiques discrètes, leur dynamique riche et l'avantage de la facilité de mise en œuvre les rendent adaptés à la mise en œuvre du cryptosystème.

La carte logistique qui est d'abord étudié par P.J. Myrberg [62], est l'une des cartes chaotiques les plus étudiées parmi les cartes non linéaires les plus simples. et il apparaît fréquemment dans les conceptions de systèmes cryptographiques basés sur le chaos. Elle est aussi la solution en temps discret du modèle de Verhulst [63]. Le terme « logistique » provient de l'ouvrage de Pierre François Verhulst qui appelle courbe logistique la solution en temps continu de son modèle. Il écrit en 1845 dans son ouvrage consacré à ce phénomène : « Nous donnerons le terme de logistique à cette courbe ». Aussi est un exemple simple de suite dont la récurrence n'est pas linéaire. Souvent citée comme exemple de la complexité pouvant surgir de simple relation non linéaire. A cause de la simplicité de son équation de récurrence, en 1947 Ulam et Von Neumann l'ont utilisé en tant que générateur de nombre pseudo-aléatoire. Cette récurrence

fut popularisée par le biologiste Robert May en 1976. [63], l'histogramme des séquences générées n'est pas uniforme. [64] Sa relation de récurrence est :

$$X_{n+1} = \mu X_n(1 - X_n) \quad (1)$$

Elle conduit, suivant les valeurs de μ, à une suite convergente, une suite soumise à oscillations ou une suite chaotique.

Comportement selon μ :

Dans le modèle logistique, la variable notée ici x_n désigne l'effectif de la population d'une espèce. En faisant varier le paramètre μ, plusieurs comportements différents sont observés, comme indique dans la figure suivante :

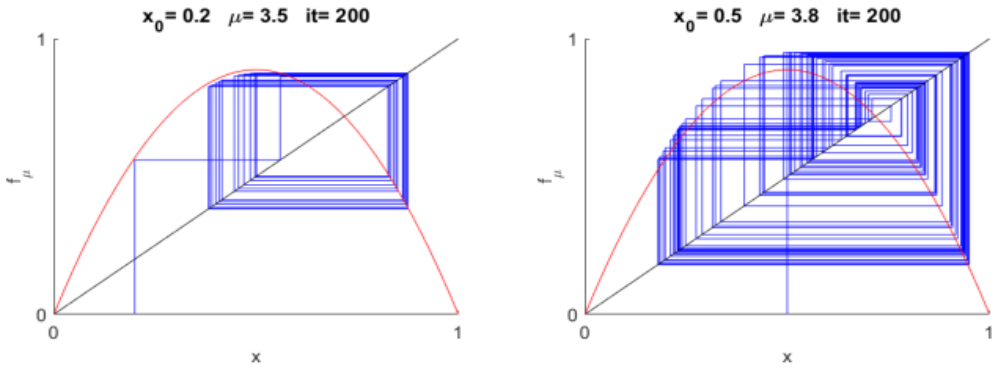


Fig A.1 : Le comportement est chaotique à partir de μ égal à 3.6 [65].

- Si $0 \leq \mu \leq 1$, l'espèce finira par mourir, quelle que soit la population de départ.
- Si $1 \leq \mu \leq 3$, la population se stabilisera sur la valeur $(\mu-1)/\mu$ quelle que soit la population initiale.
- Si $3 < \mu \leq 1+\sqrt{6}$ (approximativement 3,45), la population oscillera entre deux valeurs. Ces deux valeurs sont indépendantes de la population initiale.
- Si $3{,}45 < \mu < 3{,}54$ (approximativement), la population oscillera entre quatre valeurs, là encore sont indépendantes de la population initiale.
- Si μ est légèrement plus grand que 3,54, la population oscillera entre huit valeurs, puis 16, 32, etc.
- Vers $\mu = 3{,}57$, le chaos s'installe. Aucune oscillation n'est encore visible et de légères variations de la population initiale conduisent à des résultats radicalement différents.
- La plupart des valeurs au-delà de 3,57 présentent un caractère chaotique, mais il existe quelques valeurs isolées de μ avec un comportement qui ne l'est pas. Celles-ci s'appellent parfois les iles de la stabilité. Par exemple autour de la valeur 3,82, un petit intervalle de valeurs de μ présente une oscillation entre trois valeurs et pour μ légèrement plus grand,

entre six valeurs, puis douze, etc. ces comportements sont encore indépendants de la valeur initiale.

- Au-delà de μ = 4, la population quitte l'intervalle [0 ; 1] et diverge presque pour toutes les valeurs initiales. [66], Lorsque μ = 4, la carte logistique a le plus grand exposant de Lyapunov qui est approximativement égal à 0,6928, ce qui implique qu'il atteint la dynamique chaotique la plus élevée.

Le diagramme de bifurcation montre le comportement d'un système dynamique par rapport aux paramètres. Le diagramme de bifurcation de la carte logistique est illustré à la figure A.2 permet de résumer tout cela :

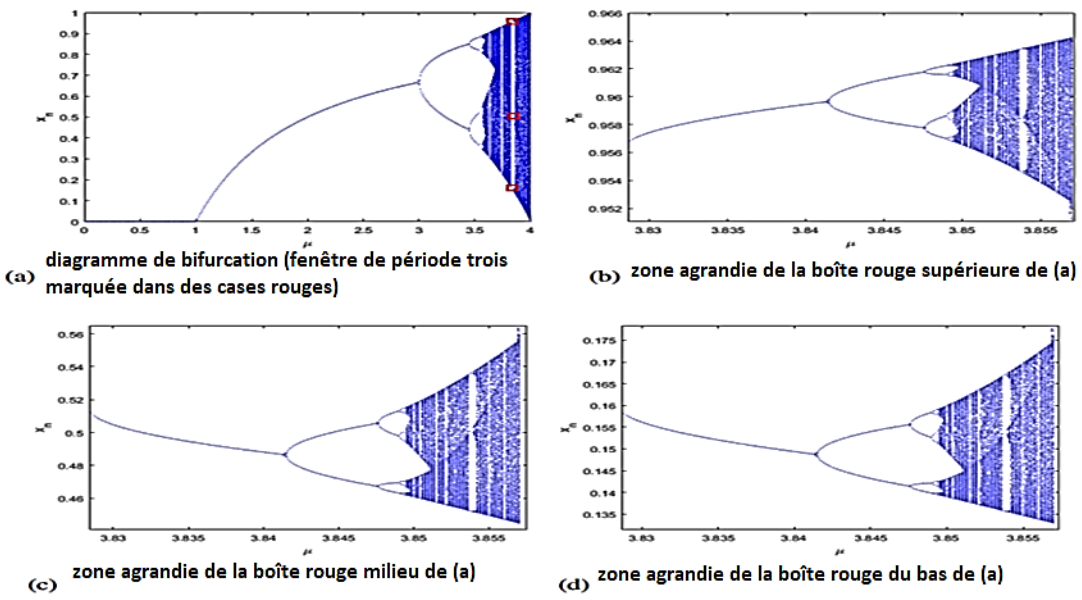


Fig A.2 : La fractale existe dans le diagramme de bifurcation de la carte logistique (autosimilarité) [64].

L'intérêt est dû à ses caractéristiques importantes, dont elle est déterministe, sensible aux conditions initiales, son mouvement est ergodique et elle est intégrée avec un nombre infini d'orbites périodiques instable. La figure A.3, présente l'attracteur de l'équation logistique, qui justifie le choix du paramètre μ entre 0 et 3.999.

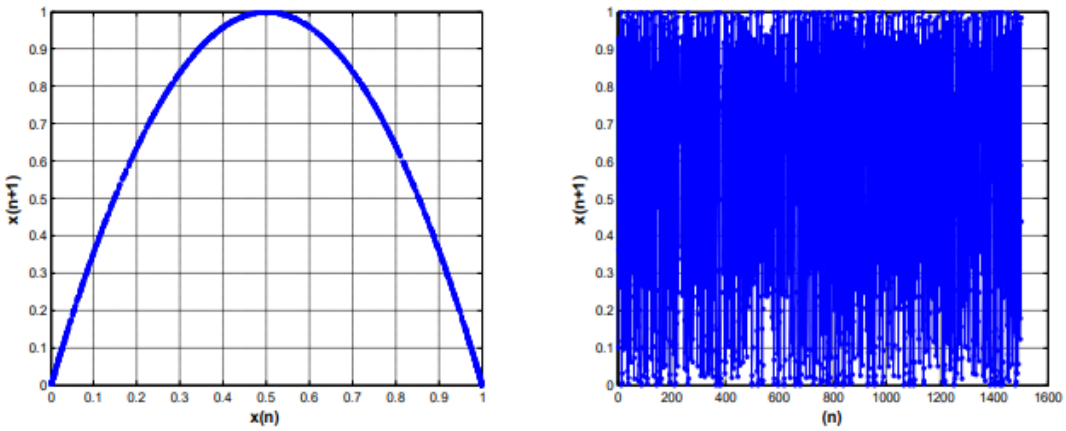


Fig A.3: Diagramme Cobweb (à gauche) et Forme d'onde du domaine temporel (droite) pour la carte logistique (N = 1500, μ = 4, X_0= 0.1) [65].

Généralement, le chaos a les caractéristiques suivantes :

1. Un spectre de puissance avec une partie continue.
2. Un nombre infini de solutions périodiques à l'équation différentielle associée, chaque solution étant instable.
3. Extrême sensibilité des trajectoires par rapport aux conditions initiales
4. Sensibilités extrêmes des trajectoires vis-à-vis des paramètres.

Par conséquent, Steven H.Strogatz en 1994 [38] que le chaos peut être décrit comme une oscillation bornée, apériodique et bruyante : un système déterministe semble se comporter de manière aléatoire même s'il n'y a pas d'entrée aléatoire. Dans les systèmes non linéaires instables, une variété d'effets étranges sont observés, y compris les sous-harmoniques, l'oscillation quasi-périodique, l'intermittence et le comportement chaotique ; mouvement erratique apparemment aléatoire.

Résumé

Au cours des dernières années, la disponibilité de dispositifs d'acquisition de données biométriques à faible coût et le développement remarquable de la technologie numérique ont fortement accru l'utilisation des technologies biométriques pour l'identification automatique des personnes. Les données biométriques sont très sensibles du fait de leur lien permanent avec l'utilisateur, ce qui justifie le souci croissant de la vie privée et de l'anonymat des individus face à toute tentative de piratage. Dans ce travail, nous avons proposé une nouvelle méthode d'extraction de caractéristiques profondes, révocables et cryptées. Dans ce processus, le principe d'apprentissage profond est utilisé pour extraire des caractéristiques efficaces et des systèmes chaotiques pour sécuriser les gabarits extraits. Pour atteindre un haut niveau de sécurité, les approches de révocabilité et de cryptage ont été hybridées. Les performances du système proposé, basé sur la modalité de l'empreinte des réseaux veineux de la paume, ont été évaluées à l'aide d'une base de données publique. Les résultats obtenus mettent en évidence l'efficacité du système proposé concernant la précision et la difficulté de piratage du fait de l'espace très important des clés de sécurité.

Mots clés : Sécurité, biométrique, Biométrie révocable, Caractéristique profonde, PCANet, ICANet, système chaotiques, empreinte des réseaux veineux de la paume.

Abstract

In recent years, the availability of low-cost biometric data acquisition devices and the remarkable development of digital technology have greatly increased the use of biometric technologies for automatic identification of persons. Biometric data is very sensitive because of its permanent link with the user, which justifies the growing concern for the privacy and anonymity of individuals in the face of any hacking attempt. In this work, we have proposed a new deep, revocable and encrypted feature extraction method. In this process, the principle of deep learning is used to extract efficient features and chaotic systems to secure the extracted templates. To achieve a high level of security, revocability and encryption approaches have been hybridized. The performances of the proposed system, based on the palm-vein modality, were evaluated using a public database. The results obtained highlight the effectiveness of the proposed system concerning the precision and the difficulty of hacking due to the very large space of the security keys.

Keywords*:* Security, Biometrics, Revocable Biometrics, Deep Feature, PCANet, ICANet, Chaotic Systems, Palm-Vein.

ملخص

في السنوات الأخيرة ، أدى توافر أجهزة الحصول على البيانات الحيوية منخفضة التكلفة والتطور الملحوظ للتكنولوجيا الرقمية إلى زيادة كبيرة في استخدام تقنيات القياسات الحيوية لتحديد هوية الأشخاص تلقائيًا. تعتبر البيانات البيومترية حساسة للغاية بسبب ارتباطها الدائم بالمستخدم ، مما يبرر الاهتمام المتزايد بخصوصية الأفراد وإخفاء هويتهم في مواجهة أي محاولة قرصنة. في هذا العمل ، اقترحنا طريقة جديدة لاستخراج ميزة عميقة وقابلة للإلغاء ومشفرة. في هذه العملية، يتم استخدام مبدأ التعلم العميق لاستخراج ميزات فعالة وأنظمة فوضوية لتأمين القوالب المستخرجة. لتحقيق مستوى عالٍ من الأمان، تم تهجين أساليب الإلغاء والتشفير. تم تقييم أداء النظام المقترح ، المبني على بصمة اوردة كف اليد، باستخدام قاعدة بيانات عامة. النتائج التي تم الحصول عليها تسلط الضوء على فعالية النظام المقترح فيما يتعلق بالدقة وصعوبة القرصنة بسبب المساحة الكبيرة جدًا لمفاتيح الأمان.

الكلمات المفتاحية : الأمان ، القياسات الحيوية ، القياسات الحيوية القابلة للإلغاء ، الميزة العميقة ، PCANet، ICANet، الأنظمة الفوضوية ، بصمة اوردة كف اليد.