REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

UNIVERSITE SHEIKH AL-ARABI TEBESSI

FACULTE DES SCIENCES EXACTES, DES SCIENCES NATURELLES ET DE LA VIE

DEPARTEMENT DE MATHEMATIQUES ET D'INFORMATIQUE

MEMOIRE

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

SPECIALITE : RESEAUX ET SECURITE INFORMATIQUE

THEME

Un système crypto-biométrique pour sécuriser les paiements en ligne

Présenté par : MANSOUR Abdelaali

Devant le jury :

Mohamed Yassine Haouam	**MCA**	**Président**
Mohamed Salah Souahi	**MCB**	**Examinateur**
Abdallah Meraoumia	**Professeur**	**Encadreur**
Hakim Bendjenna	**Professeur**	**Co- Encadreur**

Année Universitaire 2021/ 2022


بسم الله الرحمن الرحيم

Dédicace

Je dédie ce modeste travail à : A mes parents. Aucun hommage ne pourrait être à la hauteur de l'amour Dont ils ne cessent de me combler. Que dieu leur procure bonne santé et longue vie.

Aux personnes qui m'ont soutenu tout au long de ce projet : mes frères et sœurs, ma famille, et mes amis.

Et bien sur mes encadrant Pr. Abdallah meraoumia et Pr Hakim bendjenna.

Et à tous ceux qui ont contribué de près ou de loin pour que ce projet soit possible, je vous dis merci.

Remerciement

Je voudrais tout d'abord adresser toute ma reconnaissance à directeurs de ce mémoire, Pr. Abdallah Meraoumia, et Pr. Hakim Bendjenna pour leurs patiences, leurs disponibilités et surtout leurs judicieux conseils. Et surtout leurs compréhensions qui nous a permis d'avancer et de si bien faire ce travail durant ces mois.

Je tiens également à remercier les membres du jury :

Dr: M. Mohamed Yassine Haouam.

Dr : Mohamed Salah Souahi

Je tiens également à remercier tous les étudiants avec lesquels j'ai été heureux d'étudier pendant ces années d'université.

Je remercie tous les enseignants que j'ai pu rencontrer et bénéficier.

Finalement, je tiens à remercier tous ceux qui m'ont aidé de près ou de loin dans la réalisation et l'accomplissement de ce travail.

Résumé : *En raison du développement énorme et distinctif de la technologie numérique, la plupart des secteurs ont numérisé leurs activités pour tirer parti des avantages de la numérisation. En conséquence, de nombreuses villes et collectivités de toutes tailles ont adopté l'Internet des objets (IoT) pour améliorer l'efficacité de leurs services publics et offrir plus de confort à leurs concitoyens. Cette tendance est un investissement modéré pour un bénéfice immédiat et peut affecter de nombreux secteurs, tels que la gestion intelligente de l'énergie. L'une des utilisations les plus courantes de l'IoT est de contrôler la consommation d'énergie des communautés et même des entreprises, y compris la tâche de payer les factures d'électricité. Dans cette mémoire de fin d'étude, une architecture basée sur l'IoT pour le paiement des factures d'électricité est proposée. Dans cette architecture, un crypto système biométrique est intégré pour identifier le consommateur de manière sécurisée. Afin de développer un crypto système robuste, nous avons utilisé le principe d'engagement flou et la théorie du chaos en cryptographie et le filtre de Gabor pour l'extraction de caractéristiques dans le système d'identification biométrique. Les résultats expérimentaux obtenus montrent que le crypto système biométrique proposé donne les meilleures performances pour identifier le consommateur, et qu'il peut fournir un excellent taux d'identification et apporter plus de sécurité.*

Mots clés : *Securité d'information, Biométries, Empreinte palmaire, Filtre de Gabor, Système chaotique.*

Abstract: *Due to the enormous and distinctive development of digital technology, most sectors have digitized their activities to take advantage of the benefits of digitization. As a result, many cities and communities of all sizes have adopted the Internet of Things (IoT) to improve the efficiency of their public services and provide more comfort to their fellow citizens. This trend is a moderate investment for the immediate benefit and can affect many sectors, such as smart energy management. One of the most common uses of IoT is to control the energy consumption of communities and even businesses, including the task of paying electricity bills. In this end of study thesis, an architecture based on IoT for the payment of electricity bills is proposed. In this architecture, a biometric cryptosystem is integrated to identify the consumer in a secure way. In order to develop a robust cryptosystem, we used fuzzy commitment principle and chaos theory in cryptography and Gabor filter for feature extraction in biometric identification system. The experimental results obtained show that the proposed biometric cryptosystem gives the best performance to identify the consumer, and that it can provide an excellent identification rate and bring more security.*

***Index term**: Information Security, Biometrics, Palmprint, Gabor Filter, Chaotic System*

ملخص: نظرًا للتطور الهائل والمميز للتكنولوجيا الرقمية، قامت معظم القطاعات برقمنة أنشطتها للاستفادة من مزايا الرقمنة. نتيجة لذلك، اعتمدت العديد من المدن والمجتمعات من جميع الأحجام إنترنت الأشياء (IoT) لتحسين كفاءة خدماتها العامة وتوفير المزيد من الراحة لمواطنيها. يعتبر هذا الاتجاه استثمارًا معتدلًا لتحقيق فائدة فورية ويمكن أن يؤثر على العديد من القطاعات، مثل إدارة الطاقة الذكية. أحد الاستخدامات الأكثر شيوعًا لإنترنت الأشياء هو التحكم في استهلاك الطاقة للمجتمعات وحتى الشركات، بما في ذلك مهمة دفع فواتير الكهرباء. في مذكرة نهاية الدراسة، تم اقتراح بنية تعتمد على إنترنت الأشياء لدفع فواتير الكهرباء. في هذه البنية، يتم دمج نظام تشفير المقاييس الحيوية لتحديد هوية المستهلك بطريقة آمنة. من أجل تطوير نظام تشفير قوي، استخدمنا مبدأ الالتزام الغامض ونظرية الفوضى في التشفير ومرشح غابور لاستخراج الميزات في نظام تحديد المقاييس الحيوية. تظهر النتائج التجريبية التي تم الحصول عليها أن نظام التشفير البيومتري المقترح يوفر أفضل أداء لتحديد هوية المستهلك، ويمكنه توفير معدل تعريف ممتاز وتحقيق المزيد من الأمان.

الكلمات المفتاحية: أمن المعلومات، القياسات الحيوية، بصمة كف اليد، مرشح غابور، النظام الفوضوي

Table des matières

LISTE DES FIGURES

Listes des tableaux

Glossaire

A

ADN	L'acide désoxyribonucléique
AES	Advanced Encryption Standard

B

BCH	Bose, Ray-Chaudhuri and Hocquenghem codes

C

CRC	Cyclic redundancy check

D

DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DET	Detection error tradeoff

E

EER	Equal Error Rate.

F

FAR	False Acceptance Rate.
FRR	False reject Rate

I

IC	Interval de confionce.
IDEA	International Data Encryption Algorithm
IDO	Internet des objets
IoT	Internet of things

K

KNN	k-nearest neighbors

P

PolyU	l'Université polytechnique de Hong Kong

R

ROC	Receiver Operating Curve
ROI	Region Of Interest
ROR	Rank-One Recognition
RPR	Rank of Perfect Recognition
RSA	Rivest–Shamir–Adleman

T

TIC	Les technologies de l'information et de la communication

Introduction Générale

Introduction Générale

Une ville intelligente est un développement urbain économiquement durable qui offre un niveau de vie élevé à ses citoyens. En effet, la technologie joue un rôle important dans la création de ces villes, donc une ville qui aspire à être intelligente doit inclure une variété de facteurs, dont les plus importants sont les technologies de l'information et de la communication (TIC) et l'Internet des objets (IoT) [1]. L'idée derrière l'IoT est de connecter des objets (qui sont généralement représentés par des appareils électroniques) à Internet pour une surveillance et une gestion efficaces des activités quotidiennes. Dans l'ensemble, de nombreux acteurs et composants technologiques se réunissent pour obtenir un système IoT. Il s'agit notamment des réseaux de communication sans fil, des plateformes de collecte et de traitement des données, des applications et des services aux utilisateurs, ainsi que de la supervision et de la sécurité de l'ensemble de la chaîne. Fondamentalement, l'objet connecté peut effectuer les tâches suivantes : *i)* collecter et traiter les données obtenues à partir de capteurs, *ii)* communiquer avec des passerelles, et *iii)* recevoir des requête (instructions) du serveur central (*serveur cloud*) pour agir [2]. En effet, il convient de décharger au maximum l'objet d'un traitement informatique complexe et encombrant.

Comme déjà mentionné ci-dessus, les TIC et l'IoT sont cruciaux et essentiels dans la création d'une infrastructure intelligente pour gérer et soutenir la population urbaine pour la ville intelligente. Bien sûr, pour une efficacité optimale d'un IoT, le réseau de capteurs doit être généralisé à l'ensemble de la ville intelligente. En conséquence, la plupart des services

fournis aux citoyens peuvent devenir efficaces, rapides et pratiques. L'un des nombreux domaines qui pourraient être gérés intelligemment est celui des ressources énergétiques, ce qui implique inévitablement un contrôle en temps réel de ces ressources afin d'éviter les lacunes et donc d'être exploitées rationnellement. En effet, l'IoT offre de nombreux avantages pour le secteur de l'énergie tels que le contrôle en temps réel de la consommation d'énergie, la maintenance à distance, la planification des interventions et le paiement des factures [3].

Le paiement traditionnel des factures des consommateurs est un processus papier où le consommateur reçoit une facture papier avec la quantité d'énergie consommée, qu'il paie en espèces ou par chèque. Ce processus comporte plusieurs étapes dont les plus importantes sont : le relevé des compteurs, qui nécessite le déplacement de l'employé sur le site du consommateur, et la création et l'impression des factures et leur remise à chaque consommateur. Malheureusement, le coût du traitement, de l'impression et de l'envoi des factures, ainsi que l'utilisation de plus d'un employé pour relever tous les compteurs, peuvent augmenter les dépenses d'entreprise et les erreurs de facturation qui peuvent nuire à la crédibilité de l'entreprise. En général, le processus de paiement de factures traditionnel présente des problèmes importants qui peuvent affecter en particulier l'horaire et la fiabilité. En effet, le processus de facturation traditionnel ne permet pas aux consommateurs de recevoir leurs factures n'importe quand et n'importe où. De plus, la livraison de la facturation peut prendre beaucoup plus de temps s'il y a des erreurs dans les adresses des clients. En matière de fiabilité, les systèmes de facturation traditionnels ne fournissent pas de mécanisme de livraison garanti, et les factures perdues peuvent entraîner des problèmes de service client et des frais de retard pour les consommateurs. Pour pallier les faiblesses évoquées ci-dessus, nous essayons dans cette thèse de proposer un système efficace pour gérer intelligemment le paiement des factures d'électricité des consommateurs. Par conséquent, notre système utilise la cryptographie et la biométrie pour *i)* crypter le message (prix de la facture) et la modalité biométrique et *ii)* identifier à distance le consommateur. Notre proposition repose sur la généralisation du télé-relevé (relevé à distance) des compteurs électriques sur l'ensemble de la ville. Pour cela, tout compteur électrique doit comporter un module de mémorisation des quantités d'énergie consommées à transmettre via le réseau IoT lors de la demande de facturation de l'entreprise (*smart meters*). Ensuite, l'entreprise émet et envoie la facture au consommateur qui, à son tour, utilise son smart-phone pour transférer le montant de la facture de son compte bancaire vers celui de l'entreprise.

Dans ce système, on va essentiellement sécuriser le transfert des messages, gabarit biométrique et clé cryptographique en utilisant le principe de l'engagement flou [4]. Par conséquent, nous avons utilisé une méthode d'extraction de caractéristiques biométriques avec une sortie binaire (filtre de Gabor [5] avec seuillage) puis avons combiné ce gabarit ($\mathcal{T}$) avec une clé aléatoire ($\mathcal{K}$) pour obtenir un offset (ξ). Le système envoie alors l'offset, le message crypté (prix de la facture) et une signature sur la clé ($h(\mathcal{K})$) au serveur. Au niveau du serveur, à l'aide du gabarit pré-enregistré ($\tilde{\mathcal{T}}$), le système récupère la clé ($\mathcal{K}$), récupère le gabarit ($\mathcal{T}$) puis identifie l'identité du consommateur. Si l'authentification est réussie, le système déchiffre le message et exécute la transaction, puis envoie un accusé de réception à l'entreprise, qui à son tour envoie un accusé de réception au consommateur l'informant du succès de l'opération (paiement de la facture).

Le manuscrit est organisé en trois chapitres :

Le **premier chapitre** de ce mémoire présente d'abord un aperçu des principales techniques de sécurité de l'information, puis un état de l'art sur la biométrie ainsi que les technologies biométriques existantes dans le domaine de la reconnaissance seront discutés. Ces technologies faisant l'objet de nombreux travaux, nous présentons les principaux avantages et inconvénients pour chacune des technologies.

Dans **le deuxième chapitre**, nous aborderons d'abord la sécurité du système biométrique. Ensuite, nous présenterons les différentes techniques utilisées dans les crypto-systèmes biométriques.

Le **troisième chapitre** présente notre contribution ainsi que 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 et Biométrie

Principes et Applications

Résumé

La combinaison de la biométrie et de la cryptographie a beaucoup de potentiel. Étant donné que la biométrie est directement liée au propriétaire, elle est très efficace pour améliorer le processus de cryptage. Le crypto-système biométrique représente le schéma le plus adapté pour sécuriser l'échange de clés cryptographiques dans des canaux non sécurisés et pour identifier à distance les utilisateurs autorisés. Dans ce chapitre, nous expliquerons en détail les différents aspects de la sécurité de l'information, puis fournirons des informations générales sur la biométrie, ses propriétés et modalités biométriques, ainsi que la structure générale des systèmes biométriques.

Sécurité et Biométrie
Principes et Applications

Introduction

Aujourd'hui la sécurité des systèmes d'information est devenue une priorité au sein de plusieurs institutions. Sur le marché de la reconnaissance, la biométrie représente une part de plus en plus importante. C'est l'un des systèmes avec un très haut niveau de sécurité, et est considéré comme plus sûr que le login et le mot de passe traditionnels. Ce chapitre introduit quelques rappels sur la sécurité de l'information. Ensuite, nous présentons les techniques biométriques et leurs applications. Il présente également les généralités d'un système biométrique pour une application d'identification ou de vérification.

I.1 Sécurité des informations

Depuis plusieurs années, des efforts importants ont été faits dans le domaine de la recherche en sécurité de l'information. Ce constat s'explique par la présence d'un contexte mondial dans lequel les besoins de sécurité deviennent de plus en plus importants et où les enjeux socio-économiques sont colossaux.

I.1.1 Cryptographie

La cryptographie est la science qui consiste à transformer un ensemble de données claires pour le rendre incompréhensible ou vice versa. Le cryptage garantit que les informations hautement confidentielles sont transmises via des canaux de communication non sécurisés afin qu'elles ne puissent être récupérées que par le destinataire autorisé. [40]. C'est une branche des mathématiques qui crypte et décrypte les données. Dans les processus de cryptage/décryptage, une clé cryptographique, sous la forme d'une suite de symboles, est indispensable pour contrôler les processus.

Selon la Fig. I.1, un algorithme cryptographique peut être classé principalement en deux catégories : cryptographie symétrique (clé privée), cryptographie asymétrique (clé publique).

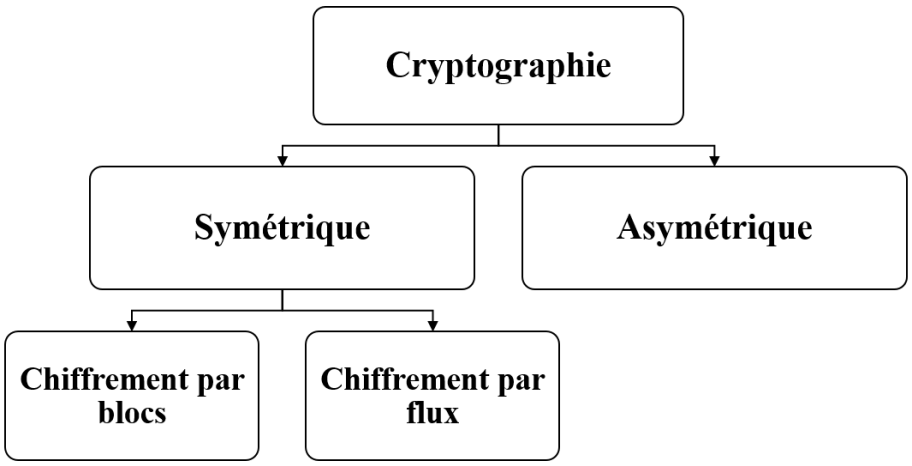


Fig. I.1 Classification de la cryptographie [40]

☑ **Cryptographie symétrique :** Pour chiffrer et décoder les messages, la cryptographie à clé symétrique utilise des clés partagées. Avant d'envoyer des messages cryptées, l'expéditeur et le destinataire doivent s'entendre sur une clé à utiliser. La procédure de cryptage pour ce type de système (voir Fig. 2.I), dans le cas où A veut envoyer un message crypté à B, est mise en œuvre comme suit [41] :

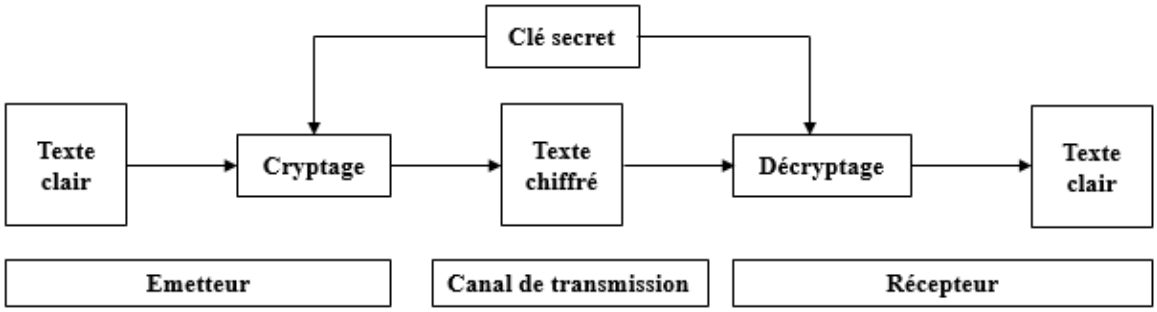


Fig. I.2 Schéma d'une cryptographie symétrique [40]

✍ $\mathcal{A}$ envoie la clé secrète à $\mathcal{B}$ et l'informe que le système de cryptage $\mathcal{A}$ utilise cette clé secrète.

✍ $\mathcal{A}$ crypte alors son message et l'envoie à $\mathcal{B}$ en utilisant cette clé et un algorithme de cryptage.

✍ $\mathcal{B}$ reçoit le message crypté, le décrypte à l'aide de la clé convenue et de l'algorithme de décryptage correspondant, pour obtenir le message original de $\mathcal{A}$.

Le cryptage et le décryptage de ce type sont très rapides, et les méthodes de cryptage symétriques sont souvent moins complexes que les techniques de cryptage asymétrique, ce qui les qualifie pour utiliser relativement peu de ressources système.

La cryptographie symétrique classée en deux catégories [40] :

- ***Chiffrements par blocs (Block ciphers) :*** fonctionne en divisant le message brut en blocs de taille fixe et en les chiffrant un par un pour produire des blocs de chiffrement de même taille. [41]
- ***Chiffrements de flux (Stream ciphers) :*** peuvent être considérés comme une méthode de chiffrement par bloc où le bloc a une dimension unitaire. Pour effectuer des modifications de base, cette approche utilise un flux de clés, qui est une séquence de bits générée aléatoirement. [41]

Le Tableau I.1 illustre les algorithmes de chiffrement symétrique les plus importants.

Tableau I.1 Classification des méthodes de chiffrement symétrique [41]

Chiffrement par bloc	**Chiffrements de flux**
DES	RC4
AES	
BLOWFISH	
IDEA	

☑ **Cryptographie asymétrique :** Dans la cryptographie asymétrique (voir Fig. I.3), la clé de chiffrement et la clé de déchiffrement sont censées être distinctes dans ces techniques. La clé de chiffrement peut être utilisée par n'importe qui, mais seule la clé de déchiffrement peut être utilisée pour déchiffrer la communication chiffrée [40].

RSA (*Rivest–Shamir–Adleman*) est l'algorithme de chiffrement asymétrique le plus populaire. Enfin, il convient de noter qu'en raison de l'efficacité du chiffrement symétrique en termes de rapidité et de l'efficacité du chiffrement asymétrique en termes de non partage des clés de chiffrement, ces deux méthodes sont combinées en une seule méthode hybride. Dans cette méthode, le message est chiffré avec un chiffrement symétrique à l'aide d'une clé aléatoire, qui est ensuite chiffré avec un chiffrement asymétrique. [41]

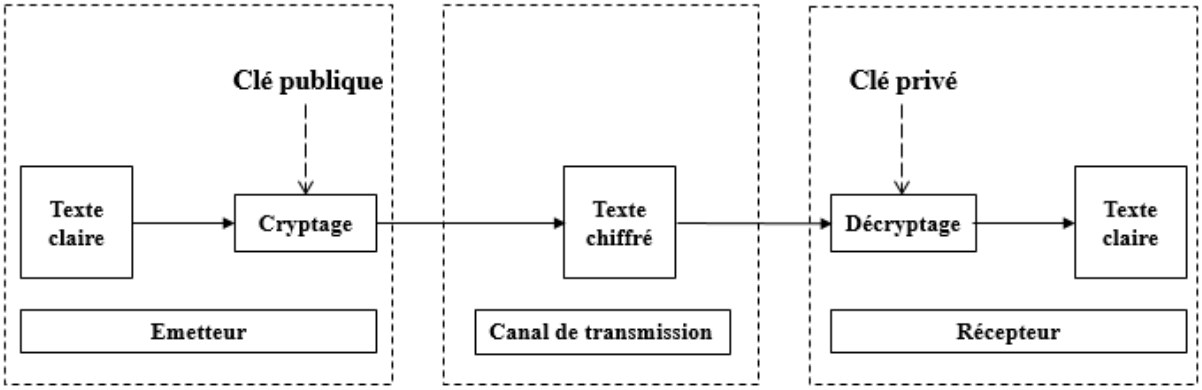


Fig. I.3 Schéma d'une cryptographie asymétrique [40]

I.1.2 Tatouage numérique

Le tatouage numérique est une technique qui utilise un algorithme pour insérer un filigrane contenant des droits de propriété intellectuelle sur des photos, des vidéos, des fichiers audio et d'autres données multimédias. Ce type de filigrane comprend des informations sur le créateur et l'utilisateur, telles que le logo du propriétaire, le numéro de série ou des informations de contrôle. En fait, il tire parti de la redondance et de l'imprévisibilité omniprésentes des données en ajoutant des informations difficiles à découvrir mais discernables pour protéger les droits d'auteur des produits et la pureté des données [7].

✍ **Système de tatouage numérique :** Le tatouage numérique est une technique qui utilise un algorithme pour insérer un filigrane contenant des droits de propriété intellectuelle sur des photos, des vidéos, des fichiers audio et d'autres données multimédias, voir Fig. I.5.

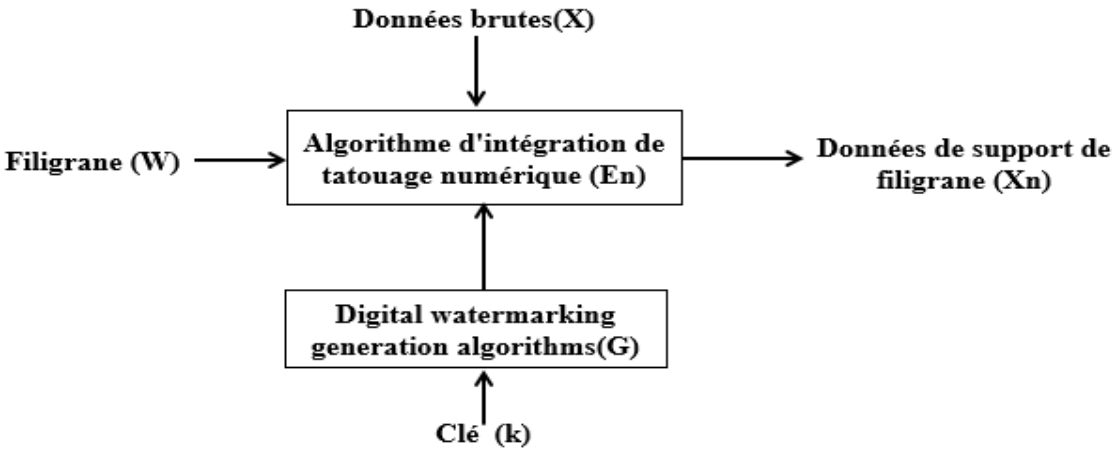


Fig. I.5 Processus d'insertion dans le tatouage numérique [7]

Le type de filigrane comprend des informations sur le créateur et l'utilisateur, telles que le logo du propriétaire, le numéro de série ou les informations de contrôle. En fait, il tire parti de

la redondance et de l'imprévisibilité omniprésentes des données en ajoutant des informations difficiles à découvrir mais discernables pour protéger les droits d'auteur des produits et la pureté des données [7].

✍ **Caractéristique de tatouage numérique :** Une distinction est généralement faite entre les tatouages visibles et invisibles. Dans les tatouages visuels, une image est généralement ajoutée pour en distinguer une autre. Par exemple, il est courant pour les agences photo d'ajouter un filigrane visible pour protéger les droits d'auteur. Les tatouages invisibles modifient le message d'une manière imperceptible. Les deux types ont les caractéristiques suivantes [7].

- ***Robustesse* :** la quantification, l'amélioration de l'image, la compression avec perte et d'autres méthodes de traitement du signal numérique n'affectent pas les filigranes.
- ***Imperceptibilité* :** n filigrane invisible à l'œil nu et inaudible à l'oreille humaine ne peut être détecté qu'avec un traitement spécial. Cela implique que la valeur d'appréciation, la valeur d'usage et la valeur économique de l'information sur le support ne seront pas affectées par le filigrane.
- ***Sûr et fiable* :** la protection du droit d'auteur est obtenue grâce à l'utilisation de filigranes, qui utilisent des signaux distinctifs appropriés pour identifier tout le monde.
- ***Faible complexité* :** l'intégration, la détection et l'extraction de filigranes seront réussies et rapides grâce à des algorithmes de faible complexité.

✍ **Applications de tatouage numérique :** Compte tenu de l'efficacité de tatouage numérique (visibles et invisibles) dans plusieurs domaines, ils ont été inclus dans de nombreuses applications, par exemple [8] :

- ***Protection des droits d'auteur :*** La protection du droit d'auteur des médias numériques a été le premier domaine d'application où le filigrane a été utilisé. En incorporant des filigranes qui identifient le support d'origine et les utilisations approuvées du matériel, le filigrane numérique ajoute une autre couche de sécurité à la chaîne de protection du contenu, empêchant l'utilisation/la duplication illégale du contenu.
- ***Identification et gestion du contenu :*** Le tatouage numérique permet une identification efficace du contenu en attribuant une identité numérique unique à tous les types de multimédia qui reste avec lui partout. Des filigranes numériques peuvent être simplement insérés dans le contenu sans interférer avec le plaisir de l'utilisateur. Les humains en sont

inconscients, mais les ordinateurs, les réseaux et une large gamme d'équipements numériques ordinaires peuvent le détecter et le comprendre. Le tatouage numérique peut inclure des informations telles que l'identité du propriétaire, la manière dont il peut être utilisé et toute autre information que le propriétaire souhaite communiquer.

- ***Filtrage de contenu :*** Les données du filigrane numériques peuvent être rapidement corrélées avec d'autres matériaux ou activités. D'une part, lorsque le filigrane est détecté, une action spécifique ou même un contenu peut être déclenché, permettant une interaction avec le consommateur. Par exemple, lors de la visualisation d'un film, un appel à l'action spécifique peut être généré, tel qu'appuie sur le bouton rouge de votre télécommande pour en savoir plus.
- ***Sécurité des documents et images :*** Au fur et à mesure que des documents privés sont générés et transmis, un filigrane numérique unique peut être facilement intégré à chaque copie. Les données contenues dans le filigrane peuvent inclure les destinataires de chaque copie, permettant de remonter à la source toute information de divulgation involontaire ou délibérée.

I.1.3 Stéganographie

La stéganographie est une technique permettant de dissimuler des communications secrètes dans d'autres messages sans révéler leur présence. Dans la plupart des cas, l'expéditeur compose un message inoffensif tout en dissimulant un message secret sur la même feuille de papier, qui n'est lisible que par ceux qui possèdent la technique de détection [6].

✍ **Différentes techniques de stéganographie :** Les applications biométriques peuvent être divisées en quatre groupes : la stéganographie de texte, la stéganographie audio, la stéganographie d'image et la stéganographie de vidéo [9] :

- ***Stéganographie de texte :*** des données secrètes peuvent être cachées derrière n'importe quel fichier texte pouvant être transféré sur un canal non sécurisé en utilisant cette approche.
- ***Stéganographie audio :*** dans la stéganographie audio tout signal audio peut être utilisé pour dissimuler des informations secrètes. Cette approche utilise souvent deux formes d'audio. Un fichier audio sert de média de couverture, tandis que l'autre contient le message caché.

- **Stéganographie d'image :** des informations confidentielles peuvent être cachées derrière n'importe quelle image (couverture) en utilisant cette technique. Les données cachées peuvent être trouvées sous forme de texte ou d'images. L'image stego générée peut ensuite être intégrée et transmise sur un canal non sécurisé.

✍ **Stéganographie vidéo :** des données secrètes peuvent être cachées derrière un fichier vidéo. Dans cette technique, une grande quantité de données peut être cachée.

✍ Inconvénients de la stéganographie : L'inconvénient fondamental de la stéganographie est qu'elle rend la conduite frauduleuse difficile à détecter entre les mains d'un individu hostile, comme les pirates. Stego-médias peut être utilisé par un pirate pour dissimuler des programmes fragmentés puis réassembler le code malveillant sur le PC de la victime [6].

✍ **Application de la stéganographie :** La stéganographie a de nombreuses applications [9] :

- Dissimuler la transmission de données sur un lien non sécurisé.
- Pour protéger les données contre la falsification.
- Il peut être utilisé en télédiffusion, ainsi qu'en synchronisation audio et visuelle.
- Pour examiner le trafic réseau de n'importe quel utilisateur.
- Il permet aux utilisateurs d'accéder à des informations numériques.

I.2 Biométrie et moyen de sécurité

La biométrie est la science qui détermine l'identité d'un individu en fonction de ses caractéristiques physiques ou comportementales. Un système biométrique typique collecte les caractéristiques biométriques d'une personne via un module d'acquisition correctement conçu et les compare à des échantillons biométriques (ou gabarits) stockés dans une base de données pour déterminer l'identité de la personne (vérification) [10].

I.2.1 Nécessité de la biométrie

La croissance rapide de nombreuses applications, telles que la banque en ligne, le commerce électronique, a suscité des inquiétudes concernant la sécurité des transactions. Parce que la cybercriminalité est en augmentation, la cybersécurité est une préoccupation essentielle. Les responsables de la sécurité de l'information veulent des solutions de sécurité complètes et fiables en raison des dommages et des souffrances causées par les cybers attaques. Alors que les transactions bancaires et de commerce électronique en ligne deviennent plus fréquents, la technique biométrique est utilisée pour les protéger. La biométrie est un bon moyen de se défendre contre les cybers attaques. Elle est l'un des moyens les plus efficaces et les plus

fiables d'identification humaine dans le domaine de la sécurité physique et cybernétique. Elle a également un effet dissuasif sur les cybercriminels. Les clients sont encouragés à utiliser les empreintes digitales pour authentifier les transactions par les banques [11].

I.2.2 Avantages de la biométrie

Plusieurs raisons peuvent motiver l'utilisation de la biométrie [12] :

- ***Haute sécurité :*** la sécurité des systèmes traditionnels est entravée par le fait que les mots de passe peuvent être facilement devinés, copiés ou oubliés, et que les carte à puce peuvent être piratées ou volées. La biométrie ne ressemble à aucune autre technologie en ce sens qu'elle ne peut être devinée, reproduite, oubliée ou volée. Ils ne peuvent être séparés de la personne, celle-ci doit donc être présente pour l'authentification, ce que personne ne peut accomplir à sa place.

- ***Commodité :*** les utilisateurs doivent mémoriser ou écrire leurs mots de passe dans les systèmes conventionnels. Si les utilisateurs oublient ou perdent leurs identifiants, l'accès aux services demandés sera refusé. La biométrie, contrairement aux méthodes traditionnelles, n'a pas besoin de mémoriser ou de transporter quoi que ce soit. En tout temps, tous les services sont disponibles.

- ***Service de non-répudiation :*** la capacité du système à lier une activité à un utilisateur qui l'a exécutée de telle manière que cette personne ne peut pas rejeter la responsabilité de cette action est connue sous le nom de service de non-répudiation. Toute activité impliquant la biométrie a presque certainement été menée par le véritable propriétaire de la biométrie en cause, car les traits biométriques sont difficiles à tromper.

I.2.3 Propriété des modalités biométriques

Tous les systèmes biométriques n'utilisent pas les caractéristiques qui peuvent les mesurer de la personne pour différencier les individus. Il y a en effet autant de caractéristiques (modalités) pour comparer deux individus. Pour pouvoir être utilisée, une caractéristique biométrique doit normalement satisfaire aux conditions suivantes [13] :

- ***Universalité :*** Chaque utilisateur de l'application biométrique doit utiliser une modalité distincte. Cet attribut devrait être présent chez une majorité significative de personnes, garantissant que tout le monde, ou au moins la majorité des personnes, a au moins une empreinte digitale, un œil ou une oreille avec laquelle ils peuvent être identifiés.

- ***Unicité :*** la modalité biométrique fournie doit être suffisamment différente parmi les utilisateurs qui composent la population. Même les empreintes digitales et les motifs de l'iris des jumeaux identiques diffèrent.

- **Permanence :** la modalité biométrique d'une personne doit être suffisamment invariante dans le temps.

- **Collectabilité :** les modalités biométriques doivent pouvoir être capturées et numérisées avec un équipement adéquat comprenant des capteurs intégrés et ne soumettant pas l'utilisateur à un stress excessif.

- **Performance :** cette mesure est utilisée pour déterminer la précision avec laquelle le système accorde l'accès aux utilisateurs autorisés tout en rejetant les imposteurs. Il prend également en compte les contraintes de l'application, telles que les ressources utilisées et l'environnement, qui peuvent affecter la précision de la reconnaissance.

- **Acceptabilité :** En termes de vitesse d'acquisition, de propreté et d'autres caractéristiques, les utilisateurs doivent l'accepter comme modalité biométrique.

I.2.4 Modalités biométriques

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

✍ **Modalités biométriques morphologiques**

- **Empreintes digitales :** C'est l'une des modalités d'identification les plus largement utilisées et les plus connues. Bien que de nombreuses données soient accessibles, seules quelques caractéristiques différenciatrices sont nécessaires pour reconnaître correctement une empreinte digitale. Les empreintes digitales (voir Fig. I.6) sont permanentes, ce qui améliore la précision des mesures et réduit le risque de faux négatifs entre les collectes [14].

Fig. I.6 Empreinte digitale

Avantages : Technologie la plus éprouvée techniquement et la plus connue du grand public, petite taille du lecteur facilitant l'intégration dans la majorité des applications, facile à mettre en œuvre, très discriminant, technique peu coûteuse, faible vulnérabilité, haute précision, et peut être installé dans une variété d'environnements [15].

Inconvénients : L'enregistrement se fait au toucher, ce qui peut entraîner des réticences psychologiques ou hygiéniques, ainsi que la nécessité de la participation de l'utilisateur (positionnement correct du doigt sur le lecteur) et d'un environnement propre [15].

- **Géométrie de la main :** C'est un moyen d'identifier les caractéristiques de la main (voir Fig. I.7) d'une personne, telles que sa forme, sa longueur, sa largeur et la forme de ses articulations [15].

Avantages : grande acceptabilité par les utilisateurs ; extrêmement simple à utiliser ; résultats indépendants de l'humidité et de la propreté des doigts ; petite taille de fichier (nécessite peu d'espace de stockage) ; cette technique peut fournir une fiabilité élevée et un temps de traitement rapide [15].

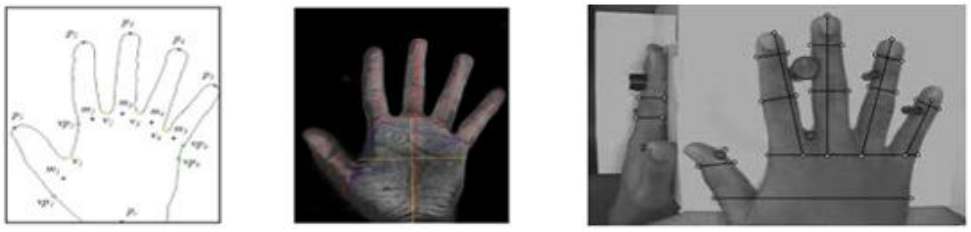


Fig. I.7 Géométrie de la main

Inconvénients : trop encombrants pour une utilisation au bureau ou en voiture, risque d'erreur pour les jumeaux ou les membres d'une même famille, technique non discriminante et sensible aux changements ou altérations naturelles de la main (accident, vieillissement, arthrose), précision limitée, difficile à utilisation pour les patients souffrant d'arthrite [15].

- **Empreinte de palme :** Par rapport à d'autres systèmes biométriques tels que l'identification du visage, des empreintes digitales et de l'iris, il s'agit d'une biométrie relativement nouvelle. La reconnaissance des empreintes palmaires (voir Fig. I.8) est une méthode d'identification biométrique qui repose sur les gabarits uniques de nombreux traits trouvés dans les paumes des gens. La face interne d'une main fait l'objet d'une empreinte palmaire. La peau d'une paume est semblable à celle des doigts, mais elle est plus grosse qu'un bout de doigt.

Fig. I.8 Empreinte de palme

Dans cette modalité, nous pouvons utiliser : des caractéristiques géométriques (telles que la largeur, la longueur et la surface); Caractéristiques de la ligne principale (emplacement et forment des lignes principales); Caractéristiques des rides (lignes plus fines et plus irrégulières) ; Caractéristiques du point delta (le centre d'une région de type delta dans l'empreinte palmaire, généralement située dans la région de la racine du doigt) ; et Caractéristiques des minuties (les lignes les plus fines et les plus irrégulières) [16].

Avantages : Les capteurs d'empreintes palmaires sont moins chers que les capteurs d'iris, et elles incluent plus d'informations qui peuvent être récupérées à partir d'image de faible résolution, ce qui les rend plus discriminantes. Il est possible de créer un système biométrique fiable en intégrant toutes les propriétés d'une empreinte palmaire, telles que les petites lignes ou les plis, et les lignes principales.

Inconvénients : en raison des informations supplémentaires incluses dans une empreinte palmaire, son exécution prend plus de temps qu'une empreinte digitale.

- **Empreinte d'articulation de doigt :** La surface externe du doigt présente des caractéristiques distinctives (voir Fig. I.9), en particulier autour des articulations, telles que des lignes principales, des lignes mineures et des crêtes [15].

Fig. I.9 Empreinte d'articulation de doigt

Avantages : L'acceptation est élevée et c'est simple à utiliser. Il est possible de créer un système biométrique fiable et précis en intégrant tous les doigts de la main.

Inconvénients : pour les jumeaux, il existe un risque de fausse acceptation. Il nécessite la coopération de l'utilisateur (placement correct du doigt sur le lecteur).

- **Iris :** L'un des technologies de reconnaissance biométrique les plus fiables produites récemment est la technique de balayage de l'iris. La reconnaissance de l'iris est une approche biométrique qui utilise l'iris d'un individu pour l'identifier. L'iris (voir Fig. I.10) est dans l'humeur aqueuse, entouré par le blanc de l'œil, avec la pupille au milieu, la cornée devant, et le cristallin derrière lui. La partie colorée de l'œil s'appelle l'iris, et c'est cette région qui est employée en biométrie. La texture de l'iris (c'est-à-dire le motif de l'iris) a une variété de caractéristiques [16].

Fig. I.10 Empreinte de l'iris

Avantage : les structures de l'iris restent stables tout au long de la vie, la texture de l'iris est totalement stable dans le temps, l'iris contient une grande quantité d'informations et les vrais jumeaux ne sont pas confondus.

Inconvénients : la collecte des images provoque un certain inconfort pour l'utilisateur, ce qui peut dissuader certaines personnes de s'inscrire. L'acquisition d'images nécessite des compétences et une formation considérable. En raison des exigences d'éclairage, le matériel est plus coûteux. La distance entre l'œil et la caméra réduit d'autant la fiabilité. Certains clients sont rebutés par l'enregistrement puisqu'il exige qu'ils restent immobiles quelques secondes devant la caméra. Enfin, les gens ont du mal à accepter la biométrie.

- **Visage :** le contour du visage (voir Fig. I.11) d'un individu peut être obtenu à l'aide d'une caméra, puis des caractéristiques spécifiques telles que la distance entre les yeux, la forme des lèvres, la circonférence du visage, l'emplacement des oreilles, etc. peuvent être extraites [15].

Fig. I.11 Visage

Avantages : Parce qu'il ne nécessite aucune intervention de la part de l'utilisateur, il est simple et peut fonctionner sans l'aide de l'utilisateur. Technique peu coûteuse et pouvant être utilisée

avec les équipements de capture d'image existants. Cette approche est bien acceptée par la population générale.

Inconvénients : les altérations physiques peuvent tromper le système. Les jumeaux identiques ne peuvent pas être distingués. Cette approche est trop sensible aux changements d'éclairage et de position de la caméra, et elle pose de sérieux problèmes de confidentialité.

- **Rétine :** La membrane sensible qui tapisse la surface interne de l'arrière du globe oculaire est connue sous le nom de rétine (voir Fig. I.12). Il est composé de plusieurs couches, dont l'une comprend des photorécepteurs, qui sont des cellules spécialisées. Les veines qui traversent les deux rétines sont ce qui les distingue. La disposition de ces veines est cohérente et distincte d'une personne à l'autre (d'un œil à l'autre). Les modèles qui suivent héritent de la stabilité de cette disposition.

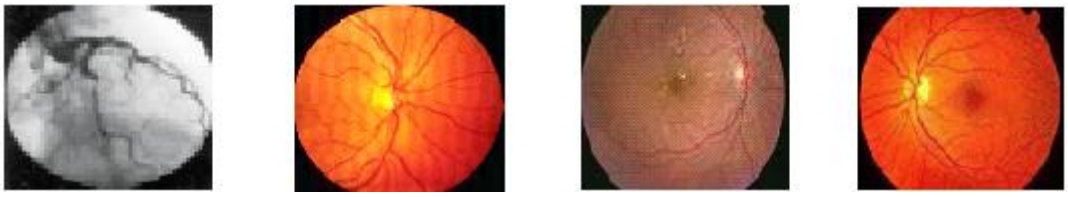


Fig. I.12 Rétine

Les défis liés à la production d'une image d'une rétine sont psychologiques, physiologiques et technologiques. Un faisceau lumineux doit être utilisé pour éclairer l'arrière du globe oculaire afin d'acquérir une image de la rétine. Ce faisceau est assez faible en intensité, il ne dérangera donc pas l'utilisateur ; il est également plus sûr et moins intense que l'équipement ophtalmique. L'image de la rétine est ensuite récupérée à l'aide d'un système de caméras très précis. Il existe des lecteurs rétiniens qui offrent un haut niveau de sécurité. Le logiciel de l'appareil de lecture coupe un anneau autour de la fovéa après avoir obtenu une image de la rétine. Il localise les veines et leur direction dans cet anneau. Il développe alors une "signature oculaire" qui peut être utilisée pour reconnaître la rétine. La procédure est simple à décrire, mais les algorithmes sont compliqués. La rétine permet un haut niveau de reconnaissance. Cette technologie est idéale pour les applications nécessitant un haut niveau de sécurité (sites militaires, coffre-fort, etc.). Les veines de la rétine sont disposées de telle manière qu'elles offrent une excellente fiabilité et une barrière élevée contre la fraude [16].

✍ Modalités biométriques comportementales

- **Analyse de la marche :** L'analyse de la marche (voir Fig. I.13) est l'étude de la façon dont une personne marche. Nous pouvons étendre cette description en discutant de la dynamique

du mouvement associée à la marche. La démarche d'une personne est étudiée depuis la fin des années 1960, avec des recherches portant sur le caractère unique de sa cyclicité et de sa cadence. Pour la première fois en 1973 ; la démarche d'un individu a été modélisée en voyant les mouvements à l'aide de marqueurs lumineux placés directement sur lui [6].

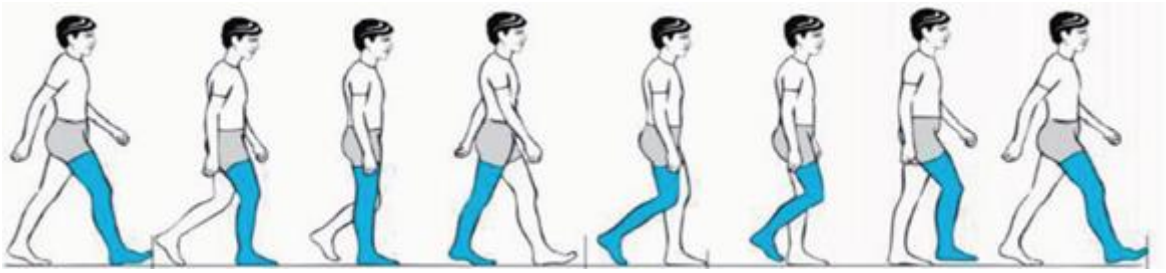


Fig. I.13 Analyse de la marche

Avantages : Une caméra basse résolution peut détecter la démarche à longue distance, ce qui permet de la voir sous n'importe quel angle. [17]

Inconvénients : Il est très sensible aux changements de poids corporel, de vêtements, de chaussures et de la surface sur laquelle une personne marchera. [17]

- **Voix :** Malgré de nombreuses variations dans la voix (voir Fig. I.14) du locuteur pendant la maladie, plusieurs systèmes ont utilisé avec succès des caractéristiques vocales globales telles que la hauteur, la dynamique et la forme d'onde de l'utilisateur analysées à l'aide d'algorithmes de reconnaissance vocale [17].

Fig. I.14 Voix

Avantages : L'infrastructure téléphonique peut être exploitée. Il est simple à mettre en œuvre.

Inconvénients : Il est sensible à l'état physique et mental de l'individu, ainsi qu'aux circonstances d'enregistrement du signal vocal, telles que le bruit et la congestion. Par conséquent, il ne peut pas être installé dans un environnement bruyant.

- **Signature manuscrite :** Le premier outil reconnu d'identification biométrique civile et médico-légale de notre société est la signature manuscrite (Fig. I.15). La vérification humaine est généralement très précise pour détecter les signatures authentiques, malgré certains désaccords sur la paternité des signatures manuscrites. Des informations sur la dynamique des

signatures ont été introduites dans le domaine biométrique de la vérification des signatures manuscrites afin de limiter davantage le potentiel de fraude [17].

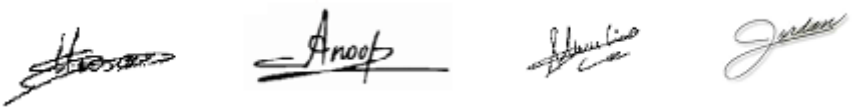


Fig. I.15 Signature manuscrite

Avantages : Comme la signature est un geste normal pour tout le monde, elle est très bien acceptée par les utilisateurs. Pour certains papiers, une signature manuscrite peut être exigée.

Inconvénients : la signature sur une tablette graphique est une nouvelle expérience pour la plupart des utilisateurs (mode dynamique). La stabilité de la technologie est considérée comme moyenne à faible, notre signature évoluant avec le temps. Il est sensible aux sentiments.

- **Dynamique de frappe : La** dynamique de frappe (voir Fig. I.16) de chaque personne est différente des autres. Cette technique est basée sur les caractéristiques uniques des coups de clavier de chaque individu, en particulier la force et le rythme avec lesquels ils frappent [6]. Elle est une solution biométrique "*Software Only*". Elle est utilisée dans le mot de passe, ce qui le rend beaucoup plus difficile à "imiter". L'utilisateur est invité à saisir son mot de passe une dizaine de fois de suite lors du déploiement de cette stratégie. Les 10 entrées sont "moyennes" à l'aide d'un algorithme qui profite du temps d'appui sur chaque touche et du temps entre chaque touche pour créer un "profil de frappe" de l'utilisateur qui servira de référence. La saisie du mot de passe sera liée à un profil de saisie qui sera comparé au profil de référence lors des accès ultérieurs. Le privilège d'accès est ensuite accordé en fonction de la ressemblance de ce profil avec la référence.

Fig. I.16 Dynamique de frappe

C'est une solution fiable, facile à installer et très compétitive car elle ne nécessite pas de matériel, qu'il s'agisse d'une sécurité supplémentaire à une application, d'un single *Sign On*, Intranet ou Internet, ou d'une sécurité à une carte à puce personnelle. Ses principaux avantages sont liés à la facilité avec laquelle il peut être mis en œuvre par un grand nombre de

personnes. Il minimise également considérablement le besoin de changements de mot de passe et les demandes de service informatique. Comme principal inconvénient, vous devez être en bonne forme physique avant d'utiliser le système, sinon votre propre mot de passe ne sera pas autorisé [16].

Avantages : L'acceptabilité des utilisateurs est élevée. Les valeurs par défaut d'authentification par mot de passe sont soigneusement conservées. Cela améliore la sécurité mais pas la commodité.

Inconvénients : cette modalité dépend de l'état physique de la personne.

✍ **Modalités biométriques biologique**

- **ADN :** L'acide désoxyribonucléique (voir Fig. I.17) est une méthode d'identification très précise issue directement de la biologie moléculaire. Étant donné qu'aucun membre du monde ne possède la même combinaison de gènes codés dans l'ADN, sa précision est très élevée. C'est une partie fondamentale des chromosomes dans le noyau cellulaire, stockant les informations génétiques d'un individu. L'ADN, qui est maintenant largement utilisé pour l'identification médico-légale, a été utilisé pour la première fois dans des affaires pénales par le chercheur anglais *Alec Jeffreys* en 1986 [18].

Fig. I.17 ADN

Avantage : Il facilite considérablement l'identification du criminel en distinguant les personnes avec un degré élevé de fiabilité et de caractère distinctif.

Inconvénients : L'analyse prend trop de temps pour produire des résultats. Il a un prix élevé.

- **Odeur corporelle :** Chacun a sa propre odeur distinctive. Les systèmes biométriques qui utilisent cette technique examinent les constituants chimiques de l'odeur et les convertissent en données comparables [18].

Avantages : la capture peut être effectuée dans n'importe quelle situation d'éclairage, même dans l'obscurité totale, ce qui lui donne un avantage sur la reconnaissance faciale traditionnelle. Il peut faire la différence entre des jumeaux identiques.

Inconvénients : des facteurs tels que la température corporelle et l'état mental ont un impact.

I.3 Systèmes biométriques

Un système biométrique est un système de reconnaissance de formes qui obtient les données biométriques d'un individu, extrait les principales caractéristiques des données biométriques, compare ces caractéristiques à des gabarits stockés dans une base de données et prend des décisions en fonction du résultat de la comparaison [19].

I.3.1 Structure d'un système biométrique

Un système biométrique générique peut être considéré comme un processus en quatre modules : capture, prétraitement et extraction de caractéristiques, mise en correspondance et prise de décision [19]. Le fonctionnement de chaque module est détaillé ci-dessous :

✍ **Module de capture :** Pour collecter les données biométriques d'une personne, vous aurez besoin d'un lecteur ou d'un scanner biométrique approprié. Un capteur optique d'empreintes digitales, par exemple, est utilisé pour numériser les structures de frottement des bords du doigt afin d'acquérir des images d'empreintes digitales. Le module de capture, qui définit l'interface d'interaction homme-machine, est essentiel à la fonctionnalité du système biométrique. En effet, une mauvaise connexion homme-ordinateur peut entraîner une augmentation significative du pourcentage de fausses acceptations et, par conséquent, une faible acceptabilité par les utilisateurs.

✍ **Module de prétraitement & d'extraction des caractéristiques :** Pour évaluer si les données biométriques reçues par le capteur biométrique conviennent à un traitement ultérieur, la qualité des données est d'abord analysée. Les données obtenues sont généralement soumises à une procédure de restauration pour améliorer leur qualité. Enfin, une collection de caractéristiques saillantes et discriminantes sera récupérée pour représenter les caractéristiques enregistrées dans la base de données, communément appelée modèle biométrique ou gabarit biométrique.

✍ **Module de correspondance :** Pour créer des scores de correspondance, le vecteur de caractéristiques extrait est comparé aux modèles contenus dans la base de données.

✍ **Module de prise de décision :** Dans ce module, les scores de correspondance sont utilisés pour authentifier une identification revendiquée ou pour proposer une évaluation des identités enregistrées dans la base de données pour identifier cette personne.

I.3.2 Fonctionnement du système biométrique

L'étude du fonctionnement d'un système biométrique permet de mettre en évidence quelques points essentiels de la mise en place d'un système biométrique. Quel que soit le système

biométrique mis en place, celui-ci comporte toujours deux phases principales [20] : la phase d'enregistrement ou d'enrôlement et la phase de reconnaissance.

✍ **Phase d'enrôlement :** La phase d'enrôlement qui peut aussi être appelée phase d'enrôlement consiste en l'enregistrement des caractéristiques biométriques d'un utilisateur sur un support de stockage. L'utilisateur fournit, au cours de cette phase, un ou plusieurs échantillons de la donnée biométrique utilisée (empreintes digitales, images de son iris ou de sa rétine, quelques prototypes de sa signature...etc.). L'acquisition de multiples exemplaires d'une même donnée biométrique se justifie par la variabilité inévitable due aux nombreux facteurs pouvant influencer l'acquisition. L'ensemble des informations obtenu est stocké, dans ce qui est appelé le gabarit d'identité biométrique. [20]

✍ **Phase de reconnaissance :** Cette phase du système biométrique permet d'effectuer la reconnaissance des individus. C'est au cours de cette phase qu'une décision sera prise concernant l'identité de l'utilisateur. Cette phase diffère en fonction de l'objectif recherché : Veut-on vérifier ou identifier un utilisateur ?

- **Vérification ou authentification :** C'est une comparaison "1 à 1" dans laquelle le système vérifie l'identification d'une personne en comparant les données biométriques saisies avec un gabarit biométrique stocké dans la base de données du système [20].

- **Identification :** L'identification est une comparaison "1à N" dans laquelle le système reconnaît une personne en la faisant correspondre à l'un des gabarits de la base de données. Il est possible que l'individu ne soit pas dans la base de données. Associer une identité à une personne fait partie de cette méthode [20].

I.4 Applications de la biométrie

Certains des principaux domaines d'application de la biométrie comprennent [12] :

- **Applications gouvernementales :** Carte nationale d'identité biométrique, passeport biométrique, contrôle aux frontières, sécurité sociale, vote électronique, etc.
- **Contrôle d'accès :** Il peut être physique comme les systèmes de pointage et la sécurité des portes, ou logique comme l'accès à distance aux ressources informatiques et aux systèmes d'information.
- **Applications mobiles :** Les smartphones récents intègrent la technique biométrique qui permet d'identifier le propriétaire, de déverrouiller l'appareil, de conclure des transactions commerciales, etc.

- **Applications commerciales :** La biométrie est utilisée dans la plupart des produits pour améliorer l'expérience client. Accès aux ordinateurs, applications internet, e-commerce, transactions bancaires, etc.
- **Applications militaires :** Il s'agit de systèmes d'identification à utiliser sur le terrain, d'applications de contrôle d'accès et de surveillance dans des zones sensibles, ainsi que de déploiements de bases de données volumineuses.
- **Applications médico-légales La** biométrie est couramment utilisée dans les laboratoires médico-légaux pour identifier les corps décédés et mener des enquêtes criminelles. Selon de nouvelles recherches, l'origine de l'ancêtre d'une personne peut être déterminée par son empreinte digitale.

I.5 Conclusion

Ces jours-ci, le contexte international a fortement mis en lumière les enjeux sécuritaires. A ces questions, les technologies biométriques se targuent d'apporter toute une série de réponses techniques. Dans ce chapitre, nous avons présenté les grands axes de la sécurité de l'information. Une deuxième partie de ce chapitre a été consacrée aux techniques biométriques les plus courantes dans ce domaine de recherche et enfin, la dernière partie traite des différentes phases de conception d'un système de reconnaissance biométrique.

Chapitre 2

Crypto-système Biométrique

Nécessités et Avantage

Résumé

Récemment, notamment dans le domaine des applications en ligne, les crypto-systèmes biométriques sont de plus en plus utilisés en raison de leur impact sur le degré de fiabilité de la sécurité de l'information. Dans ce chapitre, nous présentons en détail les vulnérabilités et les menaces des systèmes biométriques ainsi que les différents schémas de protection des clés de chiffrement (crypto-système biométrique). Enfin, nous donnons un aperçu détaillé des travaux connexes dans le domaine des crypto-systèmes biométriques.

Crypto-système Biométrique

Nécessités et Avantage

Introduction

L'hybridation des systèmes biométriques et cryptographiques permet d'augmenter la sécurité et de contrôler efficacement les accès physiques et logiques. En effet, les systèmes cryptographiques protègent les gabarits biométriques, tandis que les gabarits biométriques permettent un échange sécurisé des clés de chiffrement ainsi que l'identification du client. Dans ce chapitre, nous présentons en détail les vulnérabilités et les menaces des systèmes biométriques ainsi que les différents schémas de protection des clés de chiffrement (crypto-système biométrique). Enfin, nous donnons un aperçu détaillé des travaux connexes dans le domaine des crypto-systèmes biométriques.

II.1 Vulnérabilités et menaces d'un système biométrique

Parce qu'un système biométrique peut être vulnérable aux attaques, il est impératif que des contre-mesures soient prises en compte dans sa conception. Les différentes attaques dans les systèmes biométriques sont (voir Fig. II.1) :

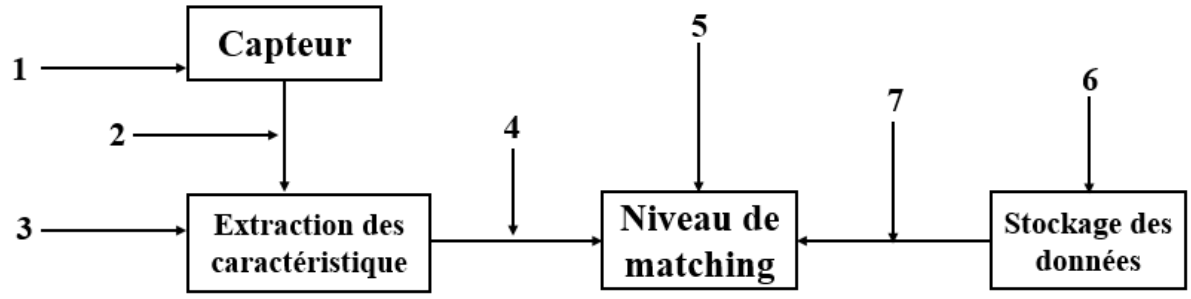


Fig. II.1 Localisation d'éventuelles attaques dans un système biométrique [6]

II.1.1 Attaque au niveau de capteur

Le capteur biométrique sera fourni avec une réplique des données biométriques qui ont été utilisées. L'attaquant peut afficher un faux doigt devant un capteur a contact ou simplement avoir l'image d'un doigt devant un capteur sans contact dans le cas de l'authentification par empreinte digitale. Il faut souligner que ce type d'attaque est plus fréquent avec les empreintes digitales, qui sont des modalités fréquemment utilisées avec un fort pouvoir de discrimination. D'autre part, d'autres modalités, notamment le visage, la rétine et la signature, rendent les données falsifiées plus difficiles à présenter [21].

II.1.2 Attaque lors la transmission entre le capteur et l'extracteur de caractéristiques

L'attaque à ce stade consiste à soumettre à nouveau des données biométriques enregistrées numériquement. Cette capacité est évidemment essentielle dans les applications en ligne où les données biométriques sont fournies par un ordinateur client et l'authentification biométrique est effectuée par un système hôte distant. La collecte de données biométriques frauduleuses par des tiers est également possible dans ce type d'application. Ces attaques sont particulièrement dangereuses pour les applications basées sur Internet. Dans tous les cas, la situation est la même pour le commerce électronique avec la transmission des informations de carte de crédit. Évidemment, il y a un problème supplémentaire avec les données biométriques : bien qu'un numéro de carte puisse être remplacé, les données biométriques ne peuvent pas être remplacées [22].

II..3 Attaque au niveau d'extraction des caractéristiques

Les attaques du module d'extraction de caractéristiques peuvent être utilisées pour échapper à la détection ou générer des imposteurs. La connaissance des processus d'extraction de caractéristiques peut être utilisée pour transformer des caractéristiques particulières en données biométriques fournies, ce qui entraîne le calcul de caractéristiques inexactes [23].

II.1.4 Niveau de stockage de données

Les gabarits biométriques ont été sauvegardés pour une vérification ou une sélection future. La modification du stockage (ajout, modification ou suppression de gabarits), la copie des données du gabarit à des fins secondaires (usurpation d'identité ou saisie directe des informations du gabarit dans une autre étape du système pour effectuer l'authentification) et la modification de l'identité à laquelle la biométrie est attribuée sont tous des exemples de vulnérabilités de stockage [23].

II.1.5 Niveau de transmission des modèles

Les modèles sont volés ou manipulés sur le lien entre la base de données de gabarits et le module de mise en correspondance concerné dans ce type d'attaque [21].

II.1.6 Niveau de correspondance

Le module de mise en correspondance produit un score de similarité basé sur la probabilité que deux échantillons biométriques appartiennent à la même personne. Les attaques de ce module sont un peu incompréhensibles, bien qu'elles puissent être concevables dans certains cas. Les scores extrêmes dans une modalité biométrique peuvent annuler les entrées d'autres modalités dans les systèmes de fusion biométrique [23].

II.1.7 Modification des décisions

Ce type d'attaque modifie la décision binaire du module de décision (oui ou non). Cette attaque présente un risque important car, même si le système est fiable en termes de performances, il peut être rendu inutilisable par ce type d'attaque. [21]

II.2 Crypto-système biométrique

La grande partie des systèmes crypto-biométriques implique le stockage de données auxiliaires, qui sont des informations biométriques publiques utilisées pour obtenir ou produire des clés. La plupart des caractéristiques biométriques sont incapables d'extraire les clés directement en raison de la variation biométrique. Les données auxiliaires, qui ne doivent rien révéler des gabarits biométriques originaux, aident à la reconstitution des clés. La vérification de la validité des clés, où le résultat d'une procédure d'authentification est soit une clé, soit un message d'échec, est une manière indirecte d'effectuer des comparaisons biométriques. Les crypto-systèmes biométriques sont utilisés pour protéger les gabarits biométriques ainsi que pour fournir une clé dépendante de la biométrie puisque la vérification de clé reflète une comparaison biométrique dans un domaine crypté [24].

Il existe différents types de systèmes crypto-biométriques (voir Fig. II.2) *: i)* Crypto-systèmes de libération de clés. *ii)* Crypto-systèmes de génération de clés et *iii)* Crypto-systèmes de liaison de clé.

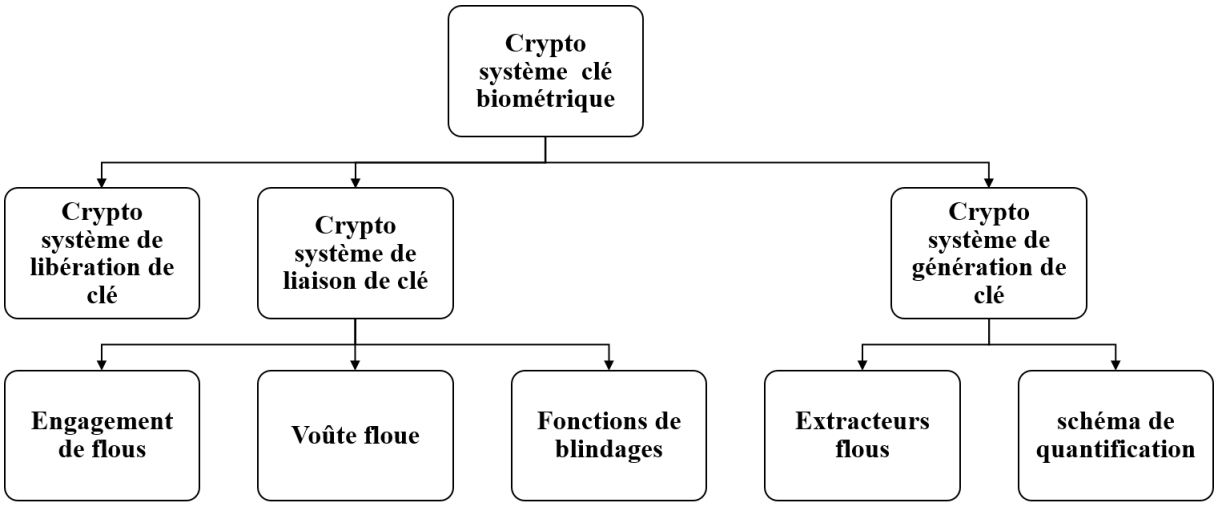


Fig. II.2 Système cryptographique à clé biométrique [25]

II.2.1 Libération de clé cryptographique

Le moyen le plus simple d'intégrer les technologies biométriques dans un cadre cryptographique consiste à stocker les clés cryptographiques en toute sécurité et à ne les publier qu'après une vérification biométrique réussie (voir Fig. II.3). Ainsi, dans ce système, on utilise la vérification biométrique traditionnelle de l'utilisateur, qui délivre le résultat de la vérification et sur laquelle la clé (ou certains paramètres nécessaires à la production de la clé) est libérée. Il convient de noter que ces systèmes doivent contenir des gabarits biométriques traditionnels pour fonctionner correctement [26].

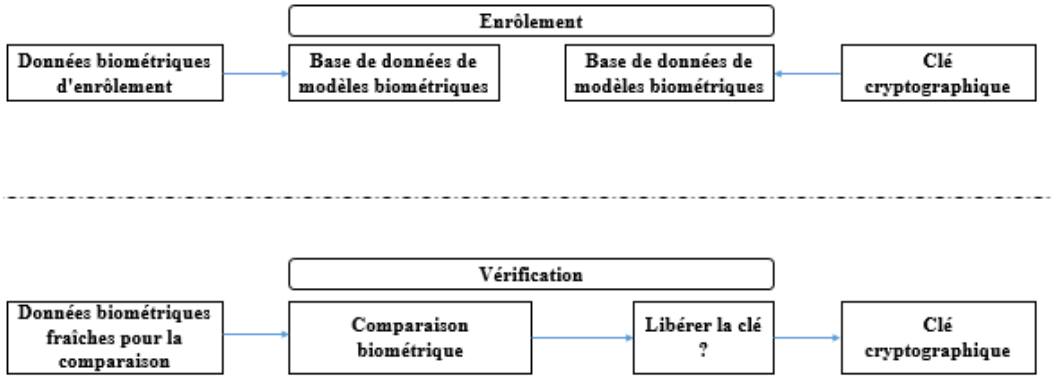


Fig. II.3 Libération de clé cryptographique basée sur la biométrie [26]

II.2.2 Génération de clés

Le gabarit biométrique est la seule source de données d'assistance. Des données auxiliaires et un échantillon biométrique spécifique sont utilisés pour générer directement des clés. Bien

que le stockage des données d'assistance ne soit pas nécessaire, la grande majorité des techniques de génération de clés suggérées le font (si les schémas de génération de clés extraient les clés sans utiliser les données d'assistance, celles-ci ne peuvent pas être mises à jour en cas de compromis).

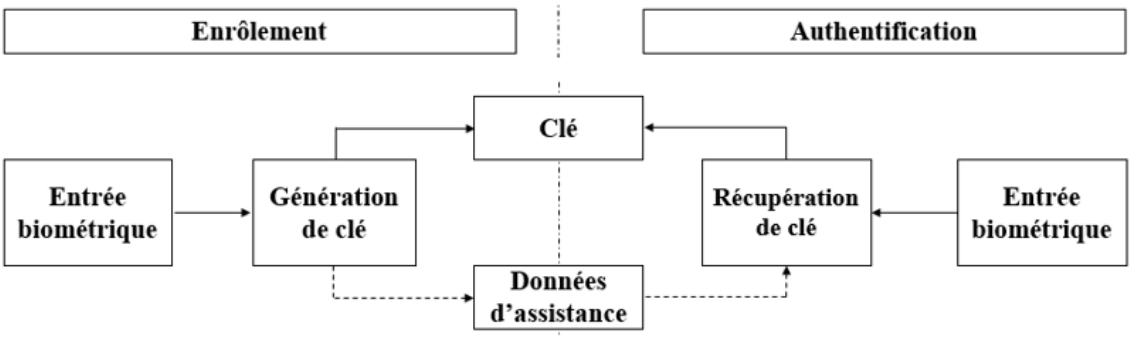


Fig. II.4 Schéma génération de clés [24]

Les systèmes de génération de clés basés sur des données auxiliaires sont également appelés "*Fuzzy extractors*" ou "*secure sketches*". Alors que les données d'assistance stockées facilitent la reconstruction, un extracteur flou extrait de manière cohérente une chaîne uniformément aléatoire à partir d'une entrée biométrique. Dans une *secure sketches*, en revanche, des données auxiliaires sont utilisées pour restaurer le gabarit biométrique d'origine [24].

✍ **Extracteur flou :** C'est la technique la plus populaire sous-jacente aux crypto-systèmes biométriques avec génération de clé. L'utilisation d'extracteurs flous fonctionne de la même manière que l'utilisation d'un coffre-fort flou (voir Fig. II.5). Cette approche récupère la clé privée uniquement à partir de données biométriques erronées (bruyantes).

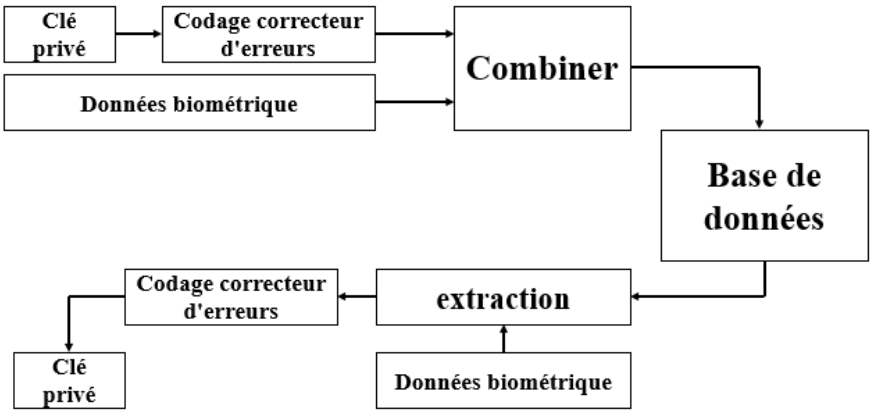


Fig. II.5 Schéma d'extracteur flou [25]

Les extracteurs flous utilisent un processus consistant à créer une séquence dispersée de manière aléatoire à partir des données d'origine, puis à la corriger avec des données extrêmement similaires à l'original. Un code de correction d'erreur est utilisé pour coder une séquence de bits qui est créée en premier. La séquence de bits créée peut être utilisée pour identifier, authentifier ou générer des clés de chiffrement cryptographique [25].

✍ **Schéma de quantification :** Les clés biométriques sont générées à l'aide de données auxiliaires et de traits biométriques binarisés (ou quantifiés) dans des techniques de quantification. Les systèmes de quantification ont la capacité unique d'extraire les mêmes clés d'un large éventail d'images biométriques, même si elles ont été capturées avec différents capteurs. Pour déterminer les intervalles pertinents pour chaque élément, l'approche de quantification nécessite les vecteurs de caractéristiques de nombreux échantillons biométriques.

En tant que données auxiliaires, ces intervalles sont enregistrés. La plupart des techniques utilisent un codage d'intervalle paramétré afin de donner des clés annulables [25].

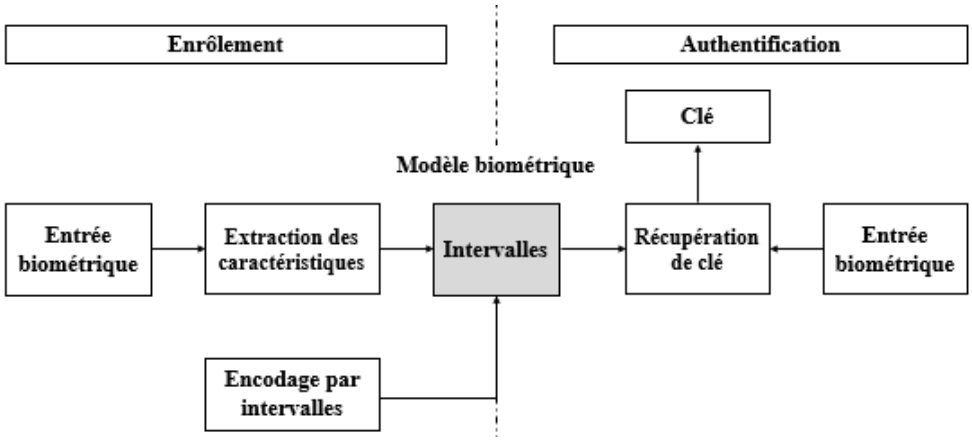


Fig. II.6 Schémas de quantification [24]

II.2.3 Schémas de liaison de clé

Lier une clé choisie à un gabarit biométrique produit des données d'assistance (voir Fig. II.7). Une fusion de la clé secrète et du gabarit biométrique est enregistrée en tant que données auxiliaires après la procédure de liaison. Lors de l'authentification, les clés sont acquises à partir de données supplémentaires à l'aide d'une technique de récupération de clé appropriée. Les clés cryptographiques sont révocables car elles sont indépendantes des gabarits

biométriques, alors qu'une mise à jour de clé nécessite normalement une ré-enrôlement afin de créer de nouvelles données d'assistance [24].

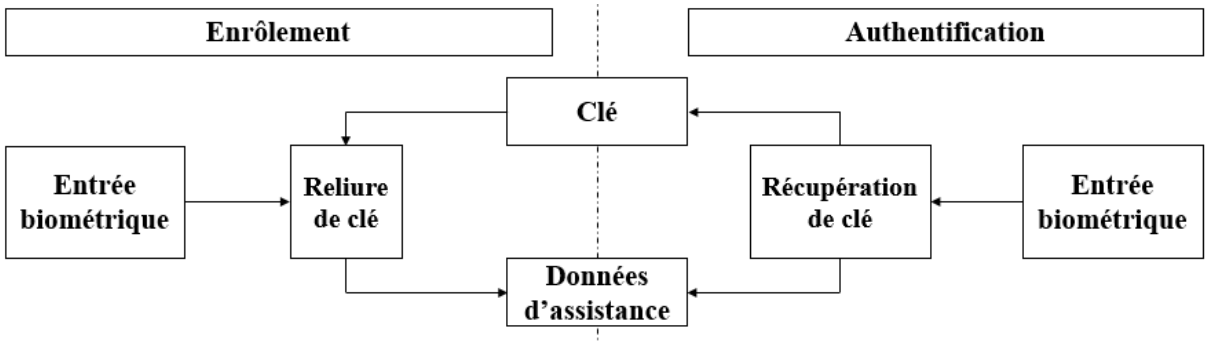


Fig. II.7 Schémas de liaison de clé [24]

✍ **Fuzzy Commitment :** En 1999, Juels et Wattenberg [23] ont fusionné des concepts des domaines des codes correcteurs d'erreurs et de la cryptographie pour créer le schéma d'engagement flou, une forme de primitive cryptographique [4]. Le schéma d'engagement flou (voir Fig. II.8) est un schéma cryptographique qui utilise des méthodes de cryptographie et de codage de correction d'erreurs pour stocker des données biométriques. L'algorithme relie des informations secrètes à des données afin de dissimuler des données et d'empêcher son propriétaire de les révéler de plusieurs manières.

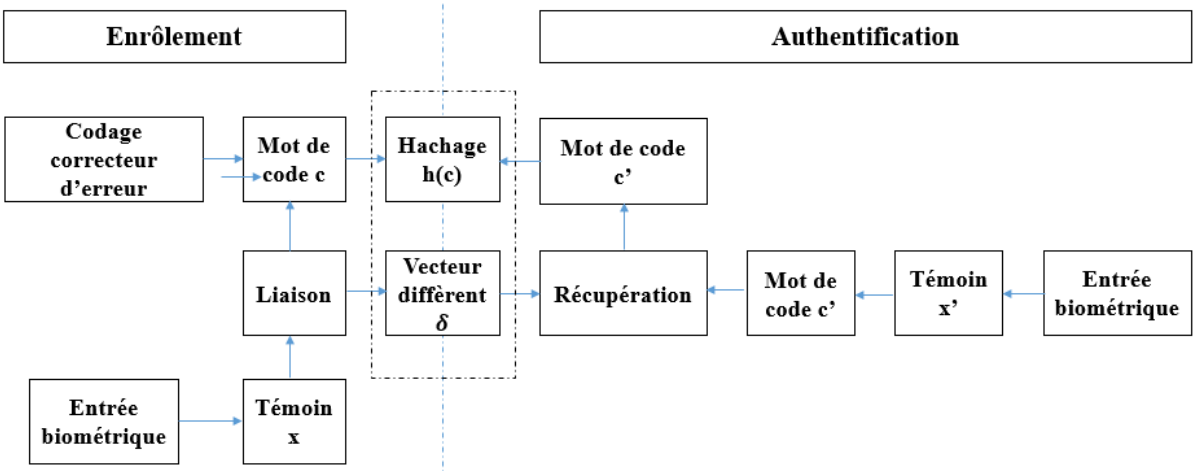


Fig. II.8 Schéma d'engagement flou [24]

Cette technique, qui s'applique aux gabarits biométriques, interprète le gabarit comme une séquence malformée qui doit être décodée sans aucune modification. Un témoin (ou clé de cryptage) est utilisé pour créer le modèle et récupérer les données dans ces systèmes [28].

Un témoin de n bits (x) ne peut être écrit qu'en termes du mot de code (valeur engagée) c et d'un décalage $\delta \in \{0,1\}^n$ tel que $x = c \oplus \delta$. Le but derrière la fonction d'engagement floue F est de cacher c en utilisant une fonction de hachage traditionnelle (h) tout en laissant δ libre. L'information δ fournit la résilience de la clé nécessaire pour ouvrir F. Plus précisément, offre des informations limitées sur x. L'information restante nécessaire pour spécifier x, à savoir le mot de code c, est, par contre, fournie sous une forme cachée comme $h(c)$ [4]. Un gabarit biométrique, tel qu'une empreinte digitale, est souvent représenté par x dans des contextes biométriques. Le mot de code c représentera une clé secrète qui sera sauvegardée par ce gabarit. Par exemple, c peut être une clé de déchiffrement protégée sous l'empreinte x de l'utilisateur en tant qu'engagement $F(c,x)$. Pour déverrouiller et afficher cette clé, l'utilisateur n'a qu'à montrer une image d'empreintes digitales x' suffisamment proche de x.

✍ **Fuzzy Vault:**

Jule et Sudan [29] proposent un schéma auquel nous attribuons la terminologie de fuzzy vault, qui est une amélioration du travail de Juels et Wattenberg [4]. La Fig. II.9 montre le schéma fonctionnel de ce travail. En effet, cette technique comporte deux phases qui sont l'encodage et le décodage :

Supposons que Alice est une cinéphile qui veut trouver quelqu'un avec des goûts similaires sans révéler ses choix aux autres. Pour ce faire, il crée un ensemble A de ses favoris et les met à disposition sous forme cryptée. À ce moment, un autre individu Bob peut décrypter le message et acquérir les informations personnelles de Alice en utilisant son propre ensemble de favoris B, qui est similaire à A.

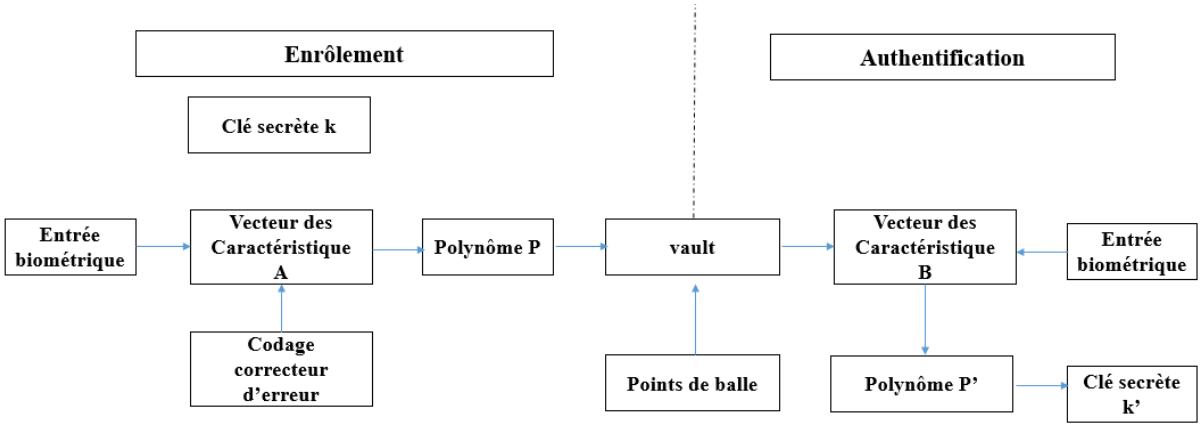


Fig. II.9 Schéma de fuzzy vault [24]

D'autre part, Bob ne pourra pas obtenir cette information s'il tente de décoder avec un ensemble différent de celui de Alice. La précision et le manque de tolérance aux erreurs de

cette stratégie sont ses inconvénients. Bob ne pourra pas récupérer le texte brut si ses signets sont assez similaires à ceux de Alice. La notion de fuzzy vault est présentée pour résoudre ce problème. Il s'agit d'une architecture cryptographique dans laquelle Alice peut crypter ses données personnelles avec son ensemble A, résultant en une VA désignée sûre.
Si Bob essaie de déverrouiller le vault, il réussira tant que ses éléments sont assez similaires à ceux de A. En utilisant un ensemble comme clé de chiffrement, le fuzzy vault est censé être tolérant aux erreurs dans les méthodes de chiffrement et de déchiffrement.

Supposons que Alice soit en possession d'un vault contenant un secret *K* et que le vault soit scellé par ses traits biométriques. Il choisit alors un polynôme P de variable x tel que le polynôme code le secret *K* via les coefficients du secret *K*. Les abscisses sont acquises à partir du gabarit biométrique choisi, et les coordonnées sont calculées à partir des évaluations du polynôme *P* en utilisant l'abscisse x, et les éléments de *A* sont les différentes valeurs des abscisses. Alice génère ensuite une série de points aléatoires asymétriques (points qui ne sont pas calculés à partir de *P* et qui sont du bruit aléatoire). L'ensemble *R*, qui est le vault du secret *K*, est constitué de l'ensemble des points.

Les points biaisés sont inclus pour déguiser le polynôme *P* d'un imposteur et ainsi assurer la sécurité de la construction. Supposons que Bob souhaite obtenir K à partir d'un ensemble B. Si les composants de *B* sont principalement superposés à ceux de *A*, Bob pourra calculer plusieurs points dans R à partir de *P*, lui permettant d'assembler une collection de points principalement précis, bien qu'il peut contenir une petite quantité de bruit.
On peut reconstruire *P* et donc *K* en utilisant le code correcteur d'erreurs. En raison de la présence de plusieurs points asymétriques, Bob serait incapable de connaître *K* si les composants de *B* ne se superposent pas de manière significative à ceux de *A*. Le problème de reconstruction polynomiale, qui est un sous-ensemble des problèmes de décodage de Reed-Solomon, détermine la cohérence du schéma [6].

II.3 Travaux connexe

Soutar et al. [27] ont publié l'un des premiers articles sur les schémas de liaison de clés (1999). Ils ont utilisé une « *phase-only random function* » pour lier les données d'empreintes digitales à l'aide d'une méthode de traitement du signal. La fonction de phase aléatoire unique est multipliée par la composante de phase de la transformée de Fourier des données d'empreintes digitales pour sécuriser en utilisant cryptographie les données combinées. Une table de correspondance est ensuite utilisée pour lier les données combinées avec une clé

cryptographique aléatoire. Cette clé est récupérée lors du processus de vérification. Les auteurs ne fournissent pas d'évaluation expérimentale ou d'analyse de sécurité de l'approche suggérée.

Les esquisses sûres (Safe sketches) et les extracteurs flous ont été introduits par *Dodis et al.* [30] en 2004. Ils présentent une étude théorique de la sécurité des crypto systèmes biométriques permettant de mettre en œuvre des stratégies d'engagement flou et de tronc flou. *Boyen* [31] a fourni une revue théorique des extracteurs flous ainsi qu'une liste de leurs défauts.

Hao et al. [32, 33] en 2006, ont proposé un système de régénération de clé pour la biométrie de l'iris basé sur l'approche d'engagement flou. Le code d'iris est un ensemble ordonné de valeurs binaires tirées d'une image d'iris qui correspond aux critères du schéma d'engagement flou. Ils ont conçu un système de correction d'erreurs à deux niveaux pour traiter les nombreuses erreurs qui peuvent se produire dans les données de l'iris. Les codes *Hadamard* sont utilisés pour réparer les erreurs aléatoires au premier niveau. Au deuxième niveau, les codes Reed-Solomon sont utilisés pour réparer les rafales d'erreurs dans les codes de l'iris causées par les occlusions des paupières, des cils, de l'éblouissement et d'autres facteurs.

Maiorana et al. [34] ont conçu leur technique de régénération de clé basée sur la signature en utilisant l'approche d'engagement flou. Ils ont utilisé la sélection adaptative de codes de correction d'erreurs dans leur méthode suggérée. Ils ont utilisé des codes BCH en particulier, et ils ont déterminé de manière adaptative les paramètres des codes BCH en fonction des fluctuations intra-utilisateur. Le concept suggéré de code de correction d'erreur adaptatif à l'utilisateur est intrigant, d'autant plus que la variabilité intra-utilisateur peut changer de manière significative entre les utilisateurs. Les résultats sont un peu meilleurs que le système biométrique de base.

Un système de protection de gabarit basé sur le visage, qui représente un autre exemple de système hybride crypto-biométrique, est proposé par *Feng et al.* [35]. Dans ce système, les données biométriques sont soumises à une transformation annulable avant d'être soumises à une transformation préservant la discriminabilité. L'approche d'engagement flou protège la chaîne binaire créée à la suite de ces étapes. L'entropie de clé estimée varie de 203 à 347 bits.

Nagar et al. [37, 36] ont également présenté un crypto-système biométrique hybride basé sur les empreintes digitales. Pour rendre le système plus sûr et améliorer les performances de vérification, ils ont utilisé des approches de coffre-fort flou et d'engagement flou (*fuzzy vault*

et *fuzzy commitment*). La technique d'engagement flou est utilisée pour inclure des descripteurs de minutie dans la construction de la vault, qui collectent des informations sur l'orientation et la fréquence des crêtes à proximité d'une minutie [38].

II.4 Conclusion

Le crypto système biométrique représente le schéma le plus adapté pour sécuriser l'échange de clés cryptographiques dans des canaux non sécurisés et pour identifier à distance un utilisateur autorisé. Dans ce chapitre, nous avons présenté un ensemble de risques et de vulnérabilités dans les systèmes biométriques tout en décrivant les étapes pour chacun. Ensuite, nous avons discuté en détail du crypto système biométrique et de ses types, et enfin nous avons conclu ce chapitre par un aperçu des travaux liés au crypto système biométrique.

Chapitre 3

Résultats Expérimentaux

Evaluations et discussions

Résumé

Les crypto-systèmes biométriques sont susceptibles d'offrir un degré de sécurité et de fiabilité plus élevé, leur permettant d'être utilisés dans de nombreux domaines, en particulier ceux utilisés sur Internet tels que le commerce électronique (*e-commerce*), la banque électronique (*e-banking*) et le vote électronique (*e-voting*). Dans ce chapitre, nous présentons notre crypto-système biométrique pour le paiement des factures d'électricité. Ensuite, nous montrerons les résultats de nos expérimentations sur une base de données type, qui indiquent que la contribution que nous avons proposée est robuste et donne de bons résultats comparables à plusieurs travaux de l'état de l'art.

Résultats Expérimentaux

Evaluations et discussions

Introduction

Dans ce chapitre, nous proposerons un crypto-système biométrique basé sur l'empreinte palmaire pour sécuriser la transmission des données et garantir l'accès aux utilisateurs autorisés. La méthode proposée est basée sur une approche d'engagement flou qui vise à renforcer la sécurité. Les performances du système biométrique proposé seront évaluées sous deux aspects : précision et sécurité, à l'aide d'une base de données connue et disponible.

III.1 Cadre de travail

Notre système peut fournir un exemple concret de la réalité IoT et de ses usages pour construire des villes intelligentes capables de fournir des services de haute qualité avec un niveau de sécurité fiable.

III.1.1 Description de l'architecture

L'architecture proposée permet à la compagnie d'électricité d'effectuer plusieurs opérations, notamment la surveillance à distance de la ville, l'analyse de la consommation, la détermination des pannes en temps réel et le paiement des factures sans erreur et sans retard. Par conséquent, cette structure peut être divisée en cinq sous-parties (voir Fig. III.1) :

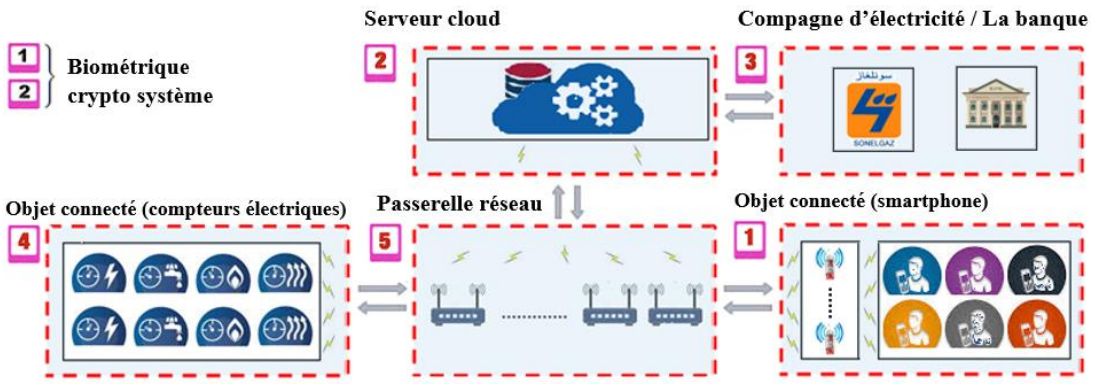


Fig. III.1 Architecture proposée pour les paiements de factures basés sur l'IdO

1) Consommateur : cette sous-partie permet au consommateur de payer la facture via son compte bancaire après l'avoir reçue de l'entreprise. L'identité et le montant du consommateur sont sécurisés et vérifiés grâce à un crypto-système biométrique.

2) Serveur cloud : tous les calculs complexes sont effectués dans le cloud, notamment ceux liés au système biométrique. Habituellement, dans le cloud, il n'y a pas de problèmes de vitesse ou de stockage.

3) Compagnie d'électricité et la banque : Leur base de données est dans le cloud et ont entièrement assurées. Les transferts entre le compte du client et l'entreprise se font dans le cloud. Ainsi, l'entreprise, la banque et le consommateur ont le droit de consulter leurs comptes.

4) Compteurs électriques des consommateurs : compteurs intelligents installés dans tous les locaux de la ville intelligente.

5) Passerelles réseau : passerelles régulièrement distribuées pour couvrir tous les quartiers (est donc tous les locaux) de la ville.

Dans cette architecture, deux situations critiques peuvent apparaître :

i) L'accès au compte du consommateur, qui est sécurisé par la biométrie ; et

ii) La transmission de la modalité biométrique vers le cloud, qui est sécurisée par la cryptographie. Ci-après, nous décrivons en détail le comportement du système de facturation intelligent proposé qui est basé sur la biométrie.

III.1.2 Comportement du système

Dans cette sous-section, nous n'abordons que la procédure de paiement des factures d'électricité. Ainsi, le diagramme de séquence de cette procédure est illustré à la Fig. III.2, qui montre les interactions de toutes les sous-parties disposées en séquence temporelle.

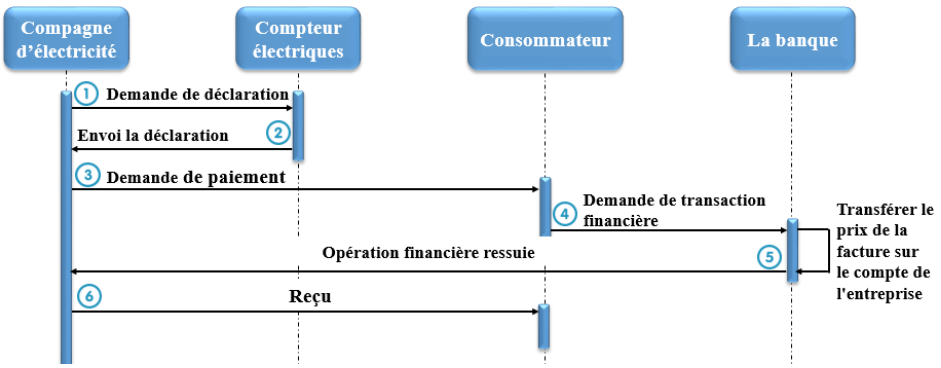


Fig. III.2 Paiements de factures basés sur l'Internet des objets (IoT).

❶ A la date de paiement de la facture, le serveur de l'entreprise envoie une requête au compteur pour remonter l'index. Il est à noter que chaque compteur est identifié par son numéro d'identification.

❷ A réception de la requête de relevé d'index, le compteur électrique transmet son index au serveur de l'entreprise.

❸ Le serveur de l'entreprise envoie la facture, après l'avoir établie, au consommateur via son smartphone. La facture peut être reçue à tout moment et n'importe où.

❹ Le consommateur effectue la transaction bancaire de son compte vers le compte de l'entreprise en envoyant à la fois la modalité biométrique et le prix de la facture d'électricité au serveur cloud. Ces données sont inévitablement cryptées.

❺ Une fois la transaction effectuée, le serveur bancaire envoie l'accusé de réception à l'entreprise.

❻ Enfin, l'entreprise adresse à son tour l'accusé de réception du paiement au consommateur.

Il est à noter que le processus d'identification multi-facteur (clé cryptographique et modalité biométrique) est utilisé pour déterminer l'identité du consommateur, ce qui augmente le niveau de sécurité et augmente ainsi la confiance du consommateur.

III.2 Exigences de sécurité

En général, la confiance des clients est liée au niveau des concessions qui leur sont offertes. L'une des principales préoccupations des clients est la sécurité de leurs informations personnelles, en particulier si elles sont liées à leurs comptes financiers. Par conséquent, le système doit fonctionner avec un taux d'erreur nul pour empêcher l'infiltration d'imposteurs, que ce soit pour de fausses transactions ou pour consulter d'autres comptes.

L'utilisation de la cryptographie avec la technologie biométrique augmente le niveau de sécurité, mais deux points essentiels doivent être remplis. La première est que la méthode de cryptage doit être robuste à la cryptanalyse pour assurer la transmission sécurisée de la modalité biométrique via Internet, et la seconde est que le compte financier du consommateur doit être protégé à l'aide d'un système d'identification biométrique hautement sécurisé.

En général, deux techniques sont utilisées pour combiner la cryptographie et le système biométrique, communément appelés crypto-systèmes biométriques. Ces techniques sont la génération de clé et l'intégration de clé, qui est la technique la plus utilisée. En effet, l'engagement flou et le coffre-fort flou sont les deux méthodes les plus courantes dans les

crypto-systèmes biométriques basés sur l'intégration de clés. Ces systèmes sont très efficaces pour partager des clés cryptographiques, il est donc largement utilisé dans la cryptographie symétrique, qui représente le schéma le plus utilisé par rapport au cryptographie asymétrique en raison de sa rapidité.

III.3 Crypto-système biométrique proposé

Un crypto-système biométrique représente le schéma le plus approprié pour sécuriser l'échange de clés cryptographiques dans des canaux non sécurisés et pour identifier à distance un utilisateur autorisé. Par conséquent, il fournit deux facteurs de sécurité fondamentaux, à savoir la sécurité de l'information à l'aide du cryptage et le contrôle d'accès sécurisé à l'aide de technologies biométriques.

Étant donné que notre système est conçu pour fonctionner sur des comptes financiers, il doit être suffisamment sécurisé pour gagner la confiance des clients. Par conséquent, après avoir combiné la clé de chiffrement avec le gabarit biométrique en utilisant le principe de l'engagement flou, nous déguisons également l'offset obtenu en utilisant des systèmes chaotiques en raison de ses propriétés utiles. De plus, l'extraction de caractéristiques basée sur les filtres de Gabor a été utilisée en raison des excellents résultats qu'elle offrait dans le domaine de la reconnaissance de formes.

III.3.1 Système biométrique

Le système que nous proposons de concevoir est un système d'analyse biométrique de la main (voir Fig. III.3). Il doit pouvoir identifier un individu préalablement inscrit par ses caractéristiques de l'empreinte palmaire.

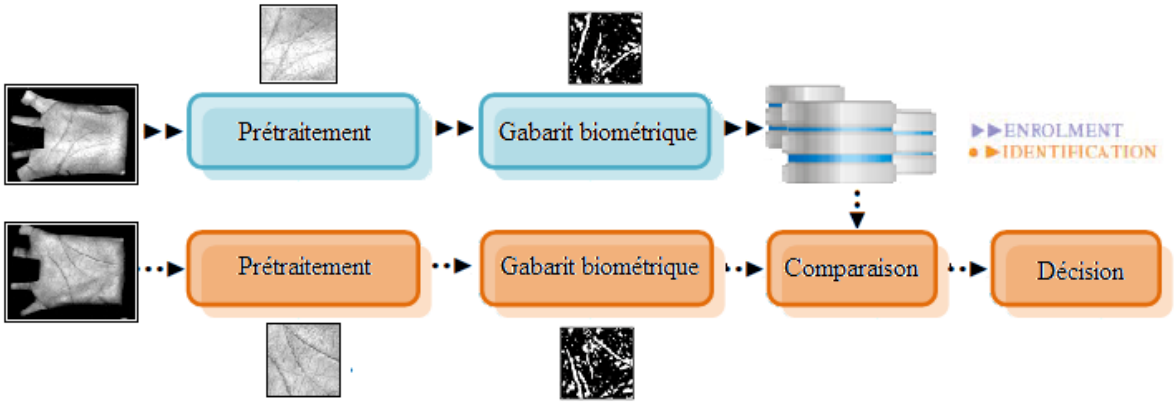


Fig. III.3 Système biométrique proposé basé sur l'empreinte palmaire.

Les images capturées sont soumises à différents traitements pour extraire les caractéristiques discriminantes. Enfin, le système doit pouvoir décider quelle est l'identité exacte de

l'utilisateur à identifier. Le module d'extraction de caractéristiques est basé sur le filtrage de Gabor avec seuillage.

✍ **Extraction de gabarit biométriques :** La plupart des systèmes biométriques ne comparent pas directement les empreintes brutes. Au lieu de cela, différentes méthodes mathématiques sont utilisées pour extraire une plus petite quantité de données, mais contenant la plupart des informations permettant de différencier deux empreintes. Dans notre travail, nous avons utilisé le filtre de Gabor avec seuillage pour extraire les caractéristiques binaires.

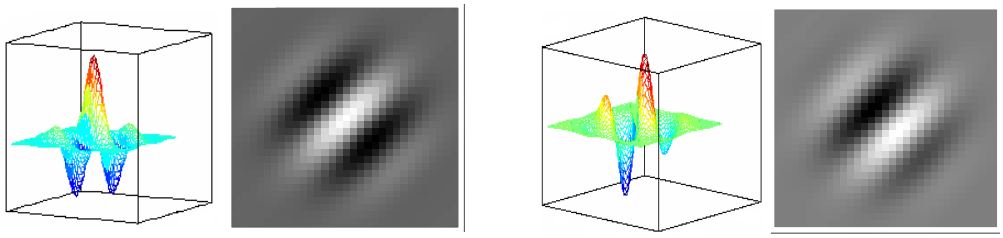
En dimension 2, dans le domaine spatial, la réponse impulsionnelle de ces filtres est définie comme une sinusoïde modulée par une fonction gaussienne (voir Fig. II.2).

$$Gauss\{(x,y,\sigma)\} = (\frac{1}{2\sigma^2})e^{-(\frac{x^2+y^2}{2\sigma^2})} \quad (1)$$

$$Re\{G(x,y,\theta,f_0,\sigma)\} = cos\{2\pi f_0(xcos\theta + ysin\theta)\}Gauss\{(x,y,\sigma)\} \quad (2)$$

$$Im\{G(x,y,\theta,f_0,\sigma)\} = sin\{2\pi f_0(xcos\theta + ysin\theta)\}Gauss\{(x,y,\sigma)\} \quad (3)$$

x et y sont les coordonnées du filtre, fo est la fréquence de l'onde sinusoïdale, σ est l'enveloppe gaussienne, θ est l'orientation de la fonction sinusoïde. La Fig. III.4 montre un filtre de Gabor.



Partie réelle Partie imaginaire

Fig III.4 Filtre de Gabor avec θ = 45°, fo = 0.0091, σ = 5.6179 et N = 17.

Pour extraire les gabarits biométriques, le filtre de Gabor est convolué avec la région d'intérêt de l'image de l'empreinte palmaire. Les deux parties réelle et imaginaire sont ensuite utilisées pour déterminer la phase résultante.

$$Re\{Disp\} = Re\{G(x,y,\theta,\upsilon,\sigma)\} * ROI \quad (4)$$

$$Im\{Disp\} = Im\{G(x,y,\theta,\upsilon,\sigma)\} * ROI \quad (5)$$

$$\varphi = \arctan(\frac{Im\{Disp\}}{Re\{Disp\}}) \quad (6)$$

Pour obtenir le gabarit biométrique, l'image filtrée (phase) est convertie en une image binaire. La technique utilisée est le seuillage avec un seuil utilisé égal à 0 :

$$V_0 = \begin{cases} 1 \; si \; \varphi \; > 0 \\ 0 \; si \; \varphi \; \leq 1 \end{cases}$$

Le résultat (image binaire) représente le gabarit biométrique, avec les pixels noirs correspondant au fond de l'image et les pixels blancs correspondant aux caractéristiques (traits, lignes fines, etc.).

✍ **Mesures des similarités :** Une méthode classique de comparaison de vecteurs binaires est ainsi appliquée : la distance de *Hamming* normalisée. Elle est définie pour deux gabarits V_0^1 et V_0^2 des deux personnes par:

$$d_0 = \frac{\sum_{i=1}^{H} \sum_{j=1}^{W} V_0^1 \oplus V_0^2}{H \times W} \quad (7)$$

Cette distance est sous forme d'une comparaison pixel par pixel et elle donne une réponse normalisée entre 0 et 1 (0 étant la correspondance parfaite).

III.3.2 Combinaison des gabarits et clés

Dans notre proposition, le système biométrique est combiné avec l'approche l'engagement flou (*fuzzy commitment*) pour renforcer la sécurité de système. L'engagement flou utilise le gabarit biométrique et la clé cryptographie pour recalculer une nouvelle donnée qui servira ensuite pour l'authentification et la libération de clé simultanément à une seule étape.

✍ **Insertion de la clé :** Cette tâche est exécutée uniquement lors de transmission (émetteur). Le système extraire le gabarit biométrique pour chaque utilisateur avec la méthode d'extraction des caractéristiques (Gabor) qui donne un gabarit binaire de taille $h \times w$ ($h = w = 128$) bits, vor Fig. III.5.

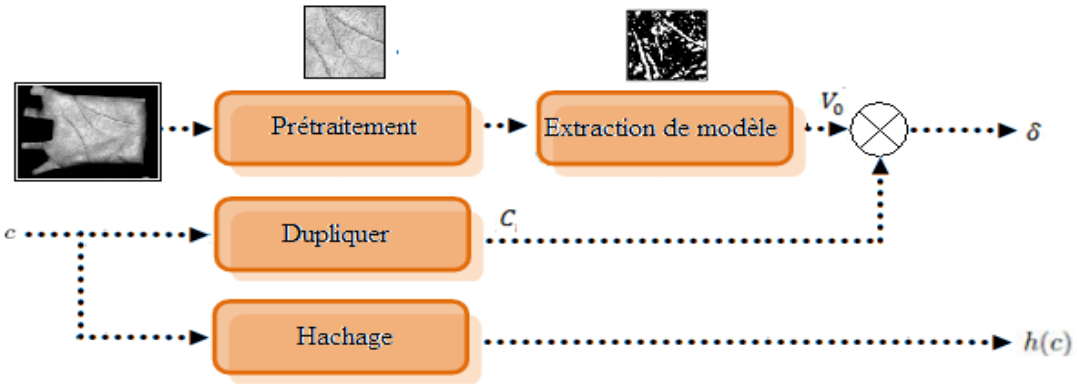


Fig III.5 : Insertion de la clé

Puis un vecteur binaire c est généré aléatoirement dont les paramètres constituent la clé de chiffrement. Ensuite, nous créons une clé C de la même taille que le gabarit biométrique en utilisant la concaténation de plusieurs clés c.

$$\mathrm{C} = [\mathrm{c}, \quad \mathrm{c}, \quad \mathrm{c}, \quad \cdots \quad \mathrm{c}] \tag{8}$$

Maintenant, calculer le l'offset δ par un ou-exclusif (XOR function) entre chaque coefficients de clé C (sous forme d'un bit) et chaque coefficients de gabarit biométrique. Notons que ce dernier présente l'avantage d'être stable en taille et ordonnée.

$$\delta = \mathrm{V_o} \oplus \mathrm{C} \tag{9}$$

Le commitment *P* de l'utilisateur se définit ensuite comme l'ensemble de $P = (\delta, h(c))$, avec h est une fonction de hachage.

✍ **Extraction de la clé :** Cette tâche est exécutée uniquement lors de réception (récepteur). Le processus d'extraction de la clé cryptographie (opération de récupération des clés) dans le récepteur est illustré à la Fig. III.6.

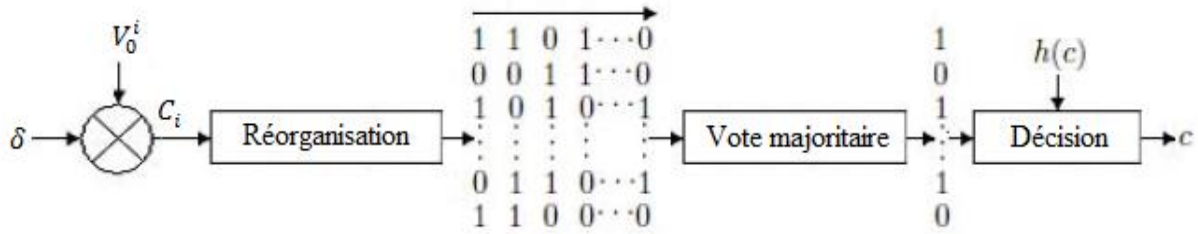


Fig III.6 : Récupération de la clé

Le système examine tous les gabarits biométriques qui sont déjà enregistrés dans la base de données lors d'enrôlement dans le système (banque par exemple). Pour chaque gabarit de la base de données, calculer le vecteur C_i par un ou-exclusif (XOR function) entre l'offset δ et le gabarit biométrique de test.

$$C_i = \delta \oplus V_0^i \tag{10}$$

Maintenant, la clé peut être récupérée. Pour y parvenir, les bits du vecteur binaire C_i sont mappés dans une matrice M_x (avec une taille de $n_1 \times n_2$, où n_1 représente la longueur de la clé et n_2 est le nombre de clé dans C_i) et la récupération de la clé est effectuée en prenant le vote majoritaire parmi M_x. Après cela, pour vérifier si la clé récupérée (c) est identique à la clé insérée ($\tilde{c}$) dans l'émetteur, le système vérifie si $h(c) = h(\tilde{c})$. Si cette clé est correcte, le système doit extraire aussi le gabarit biométrique à partir de la chaîne binaire δ par :

$$\tilde{V}_o^i = \delta \oplus C_i^1 \qquad \text{avec} \qquad C_i^1 = [\mathrm{c}, \quad \mathrm{c}, \quad \mathrm{c}, \quad \cdots \quad \mathrm{c}] \tag{11}$$

Finalement, les gabarits biométriques $\tilde{V}_o^i$ et V_0^i doivent être comparés, si sont de la même personne, la clé peut être utilisée afin de décrypter le message. Il est important de noter que le

succès du processus d'extraction des clés dépend de la variation intra/interclasse des utilisateurs clients.

III.3.3 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 Fig. III. 7. En fait, l'algorithme suivant est exécuté :

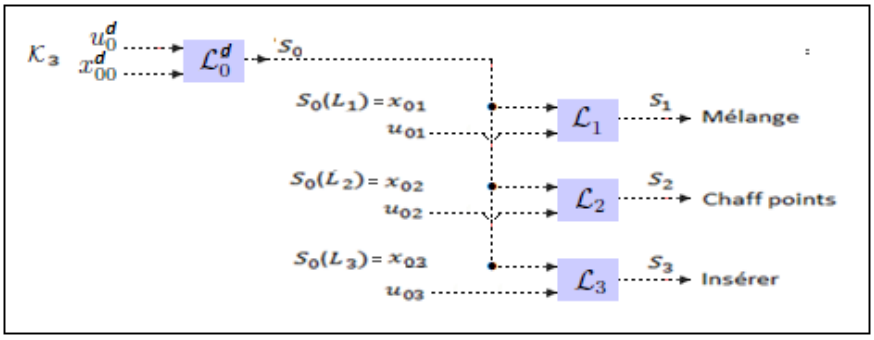


Fig. III.7: Déguisement d'offset

- La clé $k_3 = (x_{00}^d, \mu_0^{\mathrm{d}})$ 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 $(\mathcal{L}_{\mathrm{i}}, i = 1..3)$.
- 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 L, permet de créer L chaff points (dans notre test L 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 :

$$c_i = \rho \cdot S_2 \tag{12}$$

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

III.4 Résultats expérimentaux

III.4.1 Base d'images

Dans nos expériences, nous avons utilisé un ensemble de données d'empreintes palmaires multi spectrales accessibles et publiques de l'Université polytechnique de Hong Kong (PolyU) [39] pour tester et valider la robustesse et l'efficacité du schéma proposé. Ce jeu de données contient 300 personnes qui possèdent chacune 12 images obtenues à partir d'empreintes palmaires (nous avons utilisé une image en niveaux de gris extraite de trois bandes spectrales rouge, verte et bleue). Pour obtenir les performances de notre système biométrique proposé, nous sélectionnons aléatoirement cinq images pour l'enrôlement, et les autres (sept images) sont utilisés pour le test d'identification. Dans nos tests expérimentaux, nous obtenons les scores de correspondance totaux de 316050. Parmi ces scores, 2100 scores de correspondance sont considérés comme authentiques et 313950 scores de correspondance sont des imposteurs.

Ainsi, dans notre étude, les résultats expérimentaux sont divisés en deux parties. Dans la première partie, les performances du système d'identification biométrique (modes d'identification ensemble ouvert et ensemble fermé) sont testées et évaluées. Dans la deuxième partie, nous nous concentrons sur l'analyse de la sécurité de la cryptographie. La raison d'examiner les deux modes d'identification est que le système doit d'abord vérifier si le consommateur appartient ou non à la base de données et si oui, le système l'identifiera précisément. Par conséquent, le mode ensemble ouvert doit être exécuté en premier, suivi d'un ensemble fermé.

III.4.2 Performance de système biométrique

Dans cette partie, nous évaluerons les performances du système biométrique en choisissant les paramètres de la méthode d'extraction de caractéristiques. Il convient de noter que notre système utilise un classifier KNN et un filtre de Gabor pour extraire les gabarits biométriques, qui contient quatre paramètres. Pour réduire le nombre de tests, nous avons fixé la variance de l'enveloppe gaussienne (σ) et la fréquence de l'onde sinusoïdale (*fo)* à 0,0091 et 5,6179, respectivement. Aussi, nous essaierons de choisir l'orientation de la fonction sinusoïdale et la taille du filtre parmi deux ensembles prédéfinis. La taille du filtre de Gabor sera choisie parmi les tailles suivantes {11, 15, 17, 21} tandis que l'orientation de l'onde sinusoïdale sera choisie parmi {0^o, 30^o, 60^o, 90^o, 120^o, 150^o}.

Comme mentionné précédemment, nous avons testé le système dans les deux modes d'identification, le mode ensemble ouvert et le mode ensemble fermé. Le Tableau III.1 et le Tableau III.2 montrent les performances du système en mode ensemble ouvert.

θ	**0**		**30**		**60**	
Taille	T_0	EER	T_0	EER	T_0	EER
11x11	0.297	0.520	0.3254	0.183	0.3319	0.059
15x15	0.264	0.630	0.2986	0.260	0.3051	0.052
17x17	0.258	0.610	0.2946	0.250	0.2997	0.048
21x21	0.268	0.910	0.3090	0.429	0.3120	0.128

Tableau III.1: Performances des systèmes biométriques en mode ensemble ouvert (θ = [(0, 30, 60])

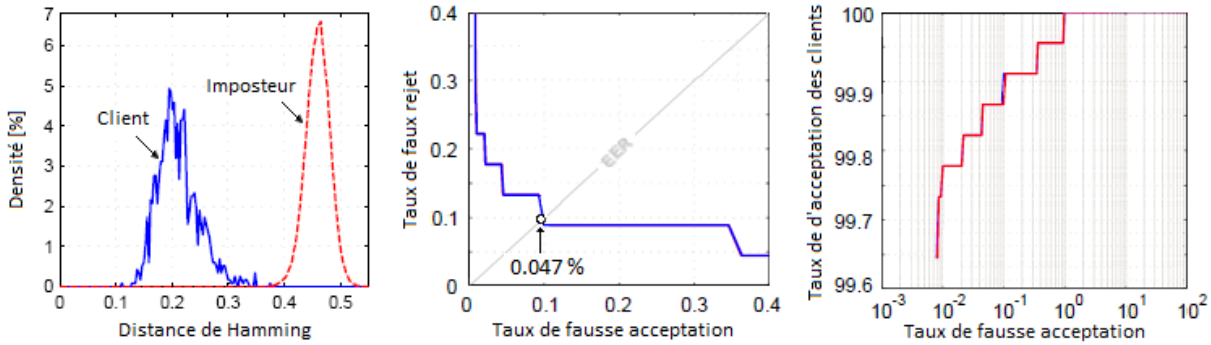
θ	90		**120**		150	
Taille	T_0	EER	T_0	EER	T_0	EER
11x11	**0.3242**	**0.047**	0.345	0.094	0.3355	0.212
15x15	0.2856	0.047	0.319	0.098	0.3060	0.238
17x17	0.2818	0.047	0.314	0.099	0.3035	0.268
21x21	0.2858	0.047	0.316	0.182	0.3123	0.310

Tableau III.2: Performances des systèmes biométriques en mode ensemble ouvert (θ=[(90, 120, 150])

A partir de ces tableaux, nous pouvons voir :

- En général, les performances du système sont efficaces dans tous les cas, le taux d'erreur égal (Equal Error Rate - EER) est toujours inférieur à 1%.
- Les orientations entre 60 et 120 donnent de meilleurs résultats, et c'est logique car les lignes de la paume sont dans ces directions
- Les filtres 11x11, 15x15 et 17x17 (o=90) donnent le minumum EER, mais pour réduire le temps de traitement, le meilleur des cas est la plus petite taille de filtre, donc 11x11.

Le meilleur des cas est d'utiliser un filtre de taille 11x11 et d'orientation 90, et dans ce cas le système peut fonctionner avec un EER égal à 0,047 au seuil (To) de 0,3242. Enfin, dans les sous-figures de la Fig. III.8, nous montrons la distribution des scores, la courbe DET (*detection error tradeoff*) et la courbe ROC (*Receiver Operating Characteristic*) du meilleur système d'identification ensemble ouvert. Ces résultats sont très satisfaisants car ils sont également combinés avec la clé cryptographique et donc d'augmenter le niveau de sécurité du système biométrique afin d'atteindre le parfait.



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

Fig. III.8: Performances des systèmes biométriques en mode ensemble ouvert for θ = 90 and N = 11. *(a)* Distributions de clients et imposteurs, *(b)* Courbe DET, et *(c)* Courbe ROC.

Pour le mode d'identification ensemble fermé (voir tableau III.3 et tableau III.4 pour, Performances des systèmes biométriques en mode ensemble fermé) le système fonctionne de parfaitement avec une cote de premier ordre (ROR) égale à 100,00% et un *Rank-One* Recognition (ROR) égal à 100,00 % et un *Rank of Perfect Recognition* (RPR) de 1.

θ	**0**		**30**		**60**	
Taille	**ROR**	**RPR**	**ROR**	**RPR**	**ROR**	**RPR**
11x11	99.33	100	99.86	20	99.95	4
15x15	99.38	86	99.86	66	100.00	1
17x17	99.33	72	99.76	53	99.95	2
21x21	99.05	91	99.62	46	99.95	2

Tableau III.3: Performances des systèmes biométriques en mode ensemble fermé (θ = [(0, 30, 60])

θ	**90**		**120**		**150**	
Taille	**ROR**	**RPR**	**ROR**	**RPR**	**ROR**	**RPR**
11x11	**100**	**1**	99.95	2	99.81	176
15x15	100	1	100	1	99.76	79
17x17	100	1	100	1	99.71	186
21x21	99.95	13	99.90	3	99.67	189

Tableau III.4: Performances des systèmes biométriques en mode ensemble fermé (θ =[(90, 120, 150])

Généralement, la base de données de la banque est utilisée pour authentifier l'identité des consommateurs lorsqu'ils souhaitent accéder aux services financiers. Raisonnablement, le nombre de clients dans presque toutes les banques est beaucoup plus élevé, ce qui augmente systématiquement la taille de la base de données. Ainsi, la taille plus importante de cette base

de données peut poser plusieurs problèmes tels que l'augmentation du temps de réponse et la dégradation de la précision du système biométrique. Afin de diminuer le temps de réponse et d'augmenter la précision du système biométrique, la base de données est segmentée en quelques petites bases de données appelées sous-bases de données.

III.4.3 Analyse de sécurité

✍ **Récupération de la clé incorporée :** L'objectif de cette partie est de tester les performances des systèmes de récupération des clés déjà incorporés au niveau du récepteur. Par conséquent, nous avons modifié plusieurs fois la longueur de la clé, puis les avons insérées dans le gabarit biométrique (en utilisant les meilleurs paramètres trouvés précédemment). Ensuite, pour chaque clé l'opération de récupération a été appliquée et le taux de récupération de clé a ensuite été calculé et les résultats obtenus sont présentés dans le tableau III.5 et tableau III.6:

Longueur de clé	32	64	128	**144**	160	172	192
Récupération	84%	99.1%	97%	**99.52%**	95%	97%	95%

Tableau III.5: Taux de récupération (clés de petite longueur)

Longueur de clé	224	240	256	320	384	448	512
Récupération	92.14	82.14	84.33	42.1%	18%	18.28%	27.14%

Tableau III.6: Taux de récupération (clés de grande longueur)

D'après ces deux tables, il est clair que le système est capable de récupérer des clés de longueur moyenne. En fait, le système fonctionne très bien pour la longueur de clé de 144 bits, avec un taux de récupération de 99,52 %, ce qui est un taux très acceptable, d'autant qu'il peut être amélioré par : *1)* Intégrer deux copies de la même clé et *2)* Utilisez un code correcteur d'erreur comme le CRC.

✍ **Comportement face à l'attaque :** Dans cette sous-partie, nous examinerons le comportement du système (sécurisé : gabarit déguiser) lors d'une attaque. Ainsi, dans nos tests, tous les utilisateurs sont enregistrés dans la base de données par une clé k= (0.75,0.88) et dans le test d'identification nous utilisons une autre clé. Ainsi, pour voir les performances des systèmes d'identification vis-à-vis des attaques, sur la Fig. III.9, nous illustrons les résultats des tests. Dans cette figure, il est clair que tous les scores d'attaque sont complètement décalés en dessous du seuil de sécurité (en dessus de 0,3242). Ce résultat reflète l'efficacité et la robustesse de notre système contre toute attaque possible.

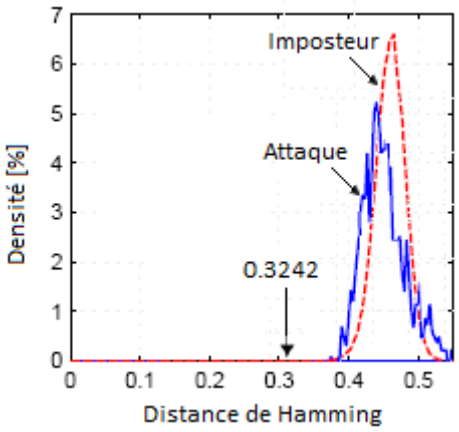


Fig. III.9: Performances des systèmes biométriques en mode ensemble ouvert lors d'une attaque.

✍ **Espace de clé de déguisement :** 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 :

$$\begin{cases} S^x = \mathcal{L}_0^c(x_{01}^c, \mu_1^c) \\ \check{S}^x = \mathcal{L}_0^c(x_{01}^c + d, \mu_1^c) \end{cases} \qquad \begin{cases} S^\mu = \mathcal{L}_0^c(x_{01}^c, \mu_1^c) \\ \check{S}^\mu = \mathcal{L}_0^c(x_{01}^c, \mu_1^c + \mathrm{d}) \end{cases} \tag{13}$$

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

$$\varepsilon_\ell\left(S^\ell, \tilde{S}^\ell\right) = \frac{1}{L^\ell}\sum_{j=1}^{L^\ell}\left|S^\ell(j) - \tilde{S}^\ell(j)\right| \tag{14}$$

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 $\mathcal{E}_\ell = 0$. 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 $\mathcal{E}_\ell = 0$. 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 $\mathcal{L}^{\mathrm{i}}|_{\mathrm{i}=1}^{3+\xi}$ $(u_0^c,\ \mu_1^c,\ \mu_i|_{\mathrm{i}=1}^{3+\xi})$ systèmes chaotiques auxiliaires, ainsi, l'espace des clés total de chaque groupe devient :

$$\mathcal{S}_{principal} = s_x^{c0} \cdot s_u^{c0} \cdot s_x^{c1} \cdot s_u^{c1} \cdot s_x^{d0} \cdot s_u^{d0} \tag{15}$$

$$\mathcal{S}_{\text{auxiliaire}} = \prod_{i=1}^{3+\xi} s_u^{\mathrm{i}} \tag{16}$$

Donc, l'espace des clés totale est :

$$S_g = \mathcal{S}_{principal} \cdot \mathcal{S}_{\text{auxiliaire}} = s_x^{c0} \cdot s_u^{c0} \cdot s_x^{c1} \cdot s_u^{c1} \cdot s_x^{d0} \cdot s_u^{d0} \cdot \prod_{i=1}^{3+\xi} s_u^i \tag{17}$$

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 :

$$\mathcal{S}_{principal} = (1.011)^3 \cdot 10^{48} \cdot (0.241)^3 \cdot 10^{48} = 1{,}01446 \cdot 10^{96} \quad (18)$$

$$\mathcal{S}_{\text{auxiliaire}} = (0.241)^{3+\xi} \cdot 10^{48+16\xi} \quad (19)$$

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

$$\mathcal{S}_{\text{auxiliaire}} = (0.241)^5 \cdot 10^{48+80} = (0.241)^5 \cdot 10^{128} = 0.70968 \cdot 10^{128} \quad (20)$$

Donc l'espace de clé est :

$$\mathcal{S}_g = 0.70968 \cdot 10^{128} \cdot 1{,}01446 \cdot 10^{96} = 0.7199 \cdot 10^{244} \quad (21)$$

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, l'Internet des objets (IoT) est largement utilisé dans de nombreuses applications pour fournir suffisamment d'objets intelligents pour partager le travail avec eux dans la vie quotidienne. L'objectif de cette étude est d'améliorer la sécurité et la confidentialité des informations des consommateurs dans une application de paiement de facture d'électricité en développant une architecture IoT embarquant un crypto-système biométrique. Le crypto-système biométrique proposé utilise les concepts de systèmes chaotiques combinés à la biométrie. Les résultats expérimentaux obtenus montrent l'intérêt de la méthode proposée pour améliorer la vie des citoyens afin d'arriver à une ville intelligente.

Conclusion Générale

Conclusion et Perspectives

La biométrie et la cryptographie sont des solutions très prometteuses en termes de sécurité des données. Malheureusement, les deux solutions ont des inconvénients. La biométrie souffre d'irréversibilité, d'un manque de diversité des gabarits et d'un risque d'atteinte à la vie privée, tandis que la cryptographie nécessite des clés qui ne sont pas étroitement liées à l'identité de l'utilisateur. Un bon moyen de contourner ces limitations consiste à utiliser une combinaison de biométrie et de cryptage. Ces systèmes, qui intègrent la biométrie au cryptage, sont appelés crypto-systèmes biométrique.

Les travaux présentés dans cette thèse s'inscrivent dans le cadre de la sécurisation des échanges de clés cryptographiques dans les canaux non sécurisés et de l'identification des utilisateurs autorisés. Des résultats expérimentaux utilisant une base de données typique de 300 personnes montrent la robustesse de notre méthode vis-à-vis aux attaques. De plus, un petit taux d'erreur a été obtenu, qui peut également être amélioré en utilisant une autre méthode performante d'extraction de caractéristiques. En effet, notre système peut fonctionner efficacement avec de très grands espaces des clés. De manière générale, à partir des résultats obtenus, il est clair que notre système peut être utilisé dans des applications qui nécessitent un très haut niveau de sécurité. Les travaux futurs de cette étude se concentreront sur l'utilisation d'autres techniques d'extraction de caractéristiques basées sur l’apprentissage profond telles que la CNN, DSTNet et ICANet.

Bibliographies

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

[2] A. Šarić; B. Mihaljević; K. Marasović, "Making a smart city even more intelligent using emergent property methodology", 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2017.

[3] Husam Rajab, Tibor Cinkelr, "IoT based Smart Cities", International Symposium on Networks, Computers and Communications (ISNCC), Rome, Italy, 2018.

[4] Juels A, Wattenberg M: A fuzzy commitment scheme. 6th ACM Conf on Computer and Communications Security 1999, 28-36.

[5] Palm, C., Keysers, D., Lehmann, T., & Spitzer, K. (2000, February). Gabor filtering of complex hue/saturation images for color texture classification. In Proc. JCIS (Vol. 2000, pp. 45-49).

[6] FERHAOUI Chafia, Un Crypto système à Base de la Biométrie Pour l'Authentification, Mémoire de Magister, Ecole nationale Supérieure d'Informatique (E.S.I), 2010

[7] Y. Zhang, "Digital Watermarking Technology: A Review," 2009 ETP International Conference on Future Computer and Communication, 2009, pp. 250-252, doi: 10.1109/FCC.2009.76.

[8] Jordi Nin and Sergio Ricciardi, Digital Watermarking Techniques and Security Issues, Department of Computer Architecture, Technical University of Catalonia - BarcelonaTECH (UPC)

[9] R. Mishra and P. Bhanodiya, "A review on steganography and cryptography," 2015 International Conference on Advances in Computer Engineering and Applications, 2015, pp. 119-122, doi: 10.1109/ICACEA.2015.7164679.

[10] Ross, Arun. (2007). Human recognition using biometrics: An overview. annals of telecommunications - annales des télécommunications. 62. 10.1007/BF03253248.

[11] Jaspreet KourM. HanmandluA.Q. Ansari31 October 2016 Defence Science Journal, Vol. 66, No. 6, November 2016, pp. 600-604, DOI: 10.14429/dsj.66.10800

[12] Foudil Belhadj. Biometric system for identification and authentication. Computer Vision and Pattern Recognition [cs.CV]. Ecole nationale Supérieure en Informatique Alger, 2017. English

[13] Christina-Angeliki TOLI, ‘’Secure and Privacy-Preserving Biometric Systems’’, Dissertation presented in partial fulfillment of the requirements for the degree of Doctor of Engineering Science (PhD): Electrical Engineering, ARENBERG DOCTORAL SCHOOL Faculty of Engineering Science,2018

[14] Pierre Bonazza ‘’ Système de sécurité biométrique multimodal par imagerie, dédié au contrôle d’accès’’ THÈSE DE DOCTORAT, L’UNIVERSITÉ DE BOURGOGNE, 2019.

[15] A. Meraoumia, "Modèle de Markov caché applique à la multi biométrie ", mémoire de doctorat, USTHB, 2014.

[16] Abdou-Aziz Sobabe, Tahirou Djara, Antoine Vianou, Biometric System Vulnerabilities: A Typology of Metadata, Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 1, 191-200 (2020)

[17] Gamboa, Hugo & Fred, Ana. (2004). A behavioral biometric system based on human-computer interaction. Proc SPIE. 5404. 381-392. 10.1117/12.542625.

[18] GOUMEZIANE Hayet, LARIBI Djamila,’’ Développement d'un système biométrique pour la reconnaissance de visage, basé sur L'opérateur binaire Local(LBP) et ses variantes.’’,2017,2018

[19] Amir BENZAOUI,’’ Identification Biométrique par Descripteurs de Texture Locaux : Application au Visage & Oreille’’, 2015

[20] Souhail Guennouni, Anass Mansouri and Ali Ahaitou, Biometric Systems and Their Applications, Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

[21] Abdou-Aziz Sobabe*, Tahirou Djara, Antoine Vianou, ‘’ Biometric System Vulnerabilities: A Typology of Metadat’’, Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 1, 191-200 (2020)

[22] M. Faundez-Zanuy, "On the vulnerability of biometric security systems," in IEEE Aerospace and Electronic Systems Magazine, vol. 19, no. 6, pp. 3-8, June 2004, doi: 10.1109/MAES.2004.1308819

[23] Adler A., Schuckers S. (2009) Biometric Vulnerabilities, Overview. In: Li S.Z., Jain A. (eds) Encyclopaedia of Biometrics. Springer, Boston, MA.

[24] Rathgeb, C., Uhl, A. A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. on Info. Security 2011, 3 (2011).

[25] Ilchenko, Mykhailo; Uryvsky, Leonid; Globa, Larysa (2021). [Lecture Notes in Networks and Systems] Advances in Information and Communication Technology and Systems Volume 152, 10.1007/978-3-030-58359-0(), –. doi:10.1007/978-3-030-58359-0

[26] Sanjay Ganesh Kanade. Enhancing information security and privacy by combining biometrics with cryptography. Other. Institut National des Telecommunication's, 2010.

[27] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B.V.K. Vijaya Kumar. Biometric encryption. In ICSA guide to Cryptography. McGraw-Hill, 1999.

[28] Lutsenko, M., Kuznetsov, A., Kiian, A., Smirnov, O., Kuznetsova, T. (2021). Biometric Cryptosystems: Overview, State-of-the-Art and Perspective Directions. In: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Advances in Information and Communication Technology and Systems. MCT 2019. Lecture Notes in Networks and Systems, vol 152. Springer, Cham.

[29] Juels, A., Sudan, M.: A fuzzy vault scheme. Des. Codes Cryptogr. 38(2), 237–257 (2006)

[30] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Proceedings of the Eurocrypt 2004, pages 523{540, 2004}

[31] Xavier Boyen. Reusable cryptographic fuzzy extractors. In 11th ACM Conference on Computer and Communications Security (CCS), 2004.

[32] Feng Hao, Ross Anderson, and John Daugman. Combining crypto with biometrics effectively. IEEE Transactions on Computers, 55(9):1081{1088, 2006}

[33] Feng Hao. On using fuzzy data in security mechanisms. Phd thesis, Queens College, Cambridge, April 2007

[34] Emanuele Maiorana, Patrizio Campisi, and Alessandro Neri. User adaptive fuzzy commitment for signature template protection and renewability. Jounal of Electronic Imaging, 17(1), 2008.

[35] Emanuele Maiorana, Patrizio Campisi, and Alessandro Neri. User adaptive fuzzy commitment for signature template protection and renewability. Jounal of Electronic Imaging, 17(1), 2008

[36] Abhishek Nagar, Karthik Nandakumar, and Anil K. Jain. A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates. Pattern Recognition Letters, 31(8):733{741, 2009.

[37] Abhishek Nagar, Karthik Nandakumar, and Anil K. Jain. Securing fingerprint template: Fuzzy vault with minutiae descriptors. In International Conference on Pattern Recognition (ICPR), pages 1 {4,2008}

[38] Sanjay Ganesh Kanade. Enhancing information security and privacy by combining biometrics with cryptography. Other. Institut National des Telecommunication's, 2010.

[39] The Hong Kong Polytechnic University, PolyU MSP Database, http://www.comp.polyu.edu.hk/sbiometrics/MultispectralPalmprint/MSP.htm.

[40] Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

[41] Delfs, H., Knebl, H., & Knebl, H. (2002). Introduction to cryptography (Vol. 2). Heidelberg: Springer.