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

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

MEMOIRE
DE FIN D'ETUDES POUR L'OBTENTION DU DIPLOMEDE MASTER INFORMATIQUE
SPECIALITE : RESAUX ET SECURITE INFORMATIQUE

THEME

Crypto-système biométrique pour la protection du Template d'empreinte palmaire

Présenté par : Kecheroud Ramzi

Devant le jury :

Mohammed Cherif Nait Hamoud	**MCB**	**Président**
Menassel Rafik	**MCA**	**Examinateur**
Laimeche Lakhdar	**MCA**	**Encadreur**
Abdallah Meraoumia	**professeur**	**Co-Encadreur**

Année universitaire 2021/2022 .

Remerciement :

Je tiens avant tout à remercier mes encadreurs, Ms. Laimeche Lakhdar et Ms. Meraoumia Abdallah qui m'ont aidé beaucoup. Je les remercie également pour leurs temps et son investissement dans tous les aspects de mon travail .

Je tiens également à remercier les membres du Jury :

Dr. Mohammed Cherif Nait Hamoud et Dr. Rafik Menassel .

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

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

Ces remerciements ne seraient pas complets sans remercier tous mes enseignants de l'année scolaire 2021/2022 .

Merci à toute ma famille .

Kecheroud Ramzi

Résumé : *Ce projet présente un crypto-système biométrique basé sur le descripteur de texture HOG. Dans cette méthode, nous avons utilisé un système chaotique basé sur les cartes logistiques pour produire des caractéristiques biométriques protéger. L'importance de ces systèmes chaotiques réside dans l'extrême sensibilité a tout changement des conditions initiales qui sont les états initiaux et les paramètres de contrôle. Nous avons testé le crypto-système biométrique proposé sur une base de données multispectrale d'empreintes palmaires de 30 personnes. La méthode proposée a également montré un niveau de sécurité élevé (protection des templates).*

Mots clés : *Sécurité, Biométries, Empreinte palmaire multi-spectrales, HOG, cartes chaotiques.*

Abstract:

This project present a biometric cryptosystem based on a novel palmprint on HOG texture descriptor. In this method, we have based on chaotic system based on the logistic map to produce a protected biometric template. The importance of these systems is due to its extreme sensitivity to initial conditions. We have tested the proposed system on a multispectral palmprint database of 30 people. The proposed method shown a high level of security (template protection).

Index term*: Security, Biometrics, Multispectral palmprint, HOG, Chaotic Map*

ملخص يقدم هذا المشروع نظام تشفير بيو متري يعتمد على طريقة HOG. في هذه الطريقة اعتمدنا على نظام فوضوي من اجل توفير ميزات بيو مترية عميقة وقابلة للإلغاء. اختبرنا نظام التشفير البيو متري المقترح على قاعدة بيانات تضم 30 شخص، ووجدنا تحسنًا كبيرًا في معدل تحديد الهوية من خلال طريقة استخراج الميزات (HOG). كما أظهرت الطريقة المقترحة أيضًا مستوى عالٍ من الأمان (حماية الميزات) .

الكلمات المفتاحية: *الحماية، البيو متري، بصمة كف اليد متعددة الأطياف، HOG، الخرائط الفوضوية.*

Table des Matières

Liste des Figures

Figures

Page

Liste des tableaux :

Glossaire

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

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

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

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

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

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

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

Introduction Générale

De nos jours, la reconnaissance biométrique des individus est devenu une approche primordiale dans le domaine de la sécurité et de contrôle d'accès au sein des infrastructures et des systèmes informatiques telles que la protection de l'accès à un ordinateur, un téléphone portable, un établissement, des cartes bancaires... etc. De nombreux systèmes biométriques ont été développés basés sur les modalités biométriques physiologique ou comportementale (iris, voix, empreintes digitales, empreinte faciale, signature....)

La construction d'un système biométrique repose quatre modules: acquisition, extraction de caractéristiques, comparaison et décision. Le module d'extraction de caractéristiques et le module responsable de la construction d'un modèle biométrique. Ce dernier est une représentation numérique de la modalité biométrique correspondante. Quelle que soit la technique d'extraction de caractéristiques utilisée, la conception de modèles biométriques est généralement motivé par les exigences suivantes pour augmenter la sécurité du système biométrique: non-réversibilité (c'est-à-dire que la récupération de modèle original à partir d'un modèle donné doit être calculée généralement très coûteux), performances de haut niveau (c'est-à-dire que les mécanismes de protection utilisés ne doivent pas affecter la précision du système), diversité (c'est-à-dire correspondance entre les bases de données ne devrait pas être faisable), et la révocabilité (c'est-à-dire, créer un nouveau modèle devrait être facilement faisable).

Cependant, répondre à ces exigences reste une tâche difficile. En général, il existe trois manières différentes afin de générer un modèle biométrique protégé : chiffrement à l'aide d'algorithmes classiques symétriques ou à clé publique, transformation de caractéristiques et Crypto-systèmes biométriques.

Dans ce projet de fin d'étude, nous avons proposé un crypto-système biométrique pour protéger les templates biométriques basé sur les systèmes chaotiques en raison de son extrême sensibilité aux conditions initiales. Dans cette approche, nous avons utilisés les cartes logistiques pour la transformation de gabarit biométrique construit par la méthode HOG afin d'améliorer sa protection.

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

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

Dans le deuxième chapitre, nous allons présenter les différentes menaces et vulnérabilités des systèmes biométriques. Puis, les approches de protections des systèmes biométriques à savoir les crypto-systèmes et qui sont basées sur les méthodes de transformations sont détaillées. Un état de l'art sur les différentes techniques de protection des systèmes biométriques est ensuite présenté.

Dans le dernier chapitre, nous présentons la méthode proposée ainsi que les résultats expérimentaux. Dans une première étape, des prérequis théoriques à savoir les systèmes chaotiques et la méthode HOG, sur lesquelles repose notre système proposé, sont détaillés. Ensuite, un nouveau système biométrique révocable est proposé. L'originalité de notre système réside dans la transformation de gabarit biométrique obtenu par la méthode d'extraction de caractéristique HOG et les cartes logistiques. Dans une deuxième étape, les résultats expérimentaux sont détaillés et discutés. Finalement, Nous clôturons ce mémoire par une conclusion générale, ainsi que les perspectives visées.

Chapitre 01

Sécurité d'information et biométrie

Résumé :

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

Introduction

La biométrie est le moyen le plus approprié pour identifier et authentifier les individus de manière fiable et rapide grâce à des caractéristiques biologiques uniques , la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent . dans ce qui suit nous présentons les notion fondamentales des systèmes biométriques et leur fonctionnement ainsi que ces inconvénients et limitations .

I.1 Nécessitée de la biométrie

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

I.2 Définition de la biométrie

La biométrie recense nos caractères physiques et comportementaux (voir figure I.1) les plus uniques, qui peuvent être captés par des instruments et interprétés par des ordinateurs de façon à être utilisés comme des représentants de nos

personnes physiques dans le monde numérique. Ainsi, nous pouvons associer à notre identité des données numériques permanentes, régulières et dénuées de toute ambiguïté, et récupérer ces données rapidement et automatiquement à l'aide d'un ordinateur." [1].

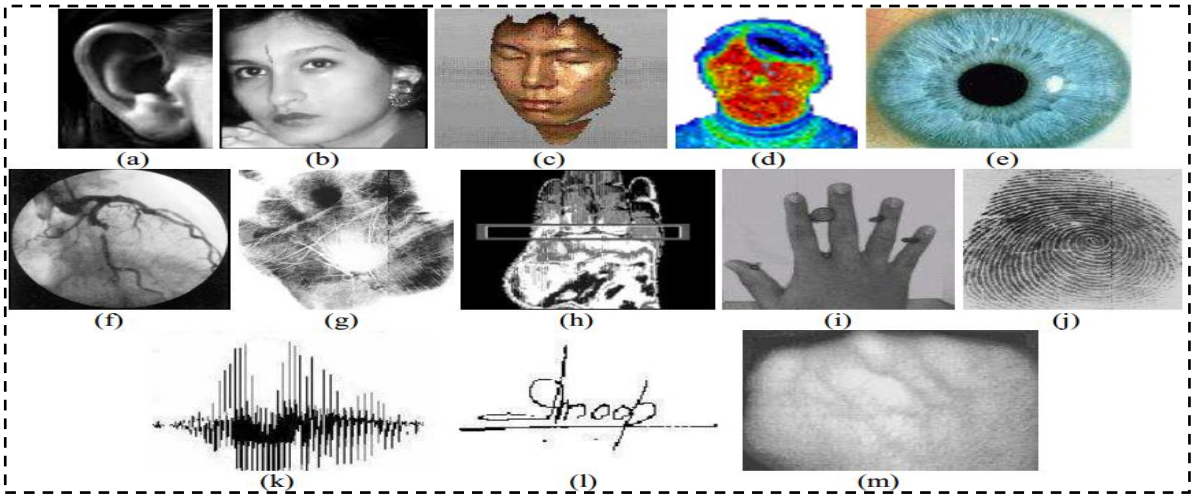


Figure. I.1 : Exemple des traits biométriques utilisé pour l'identification [2].

I.3 Types des modalités biométriques

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

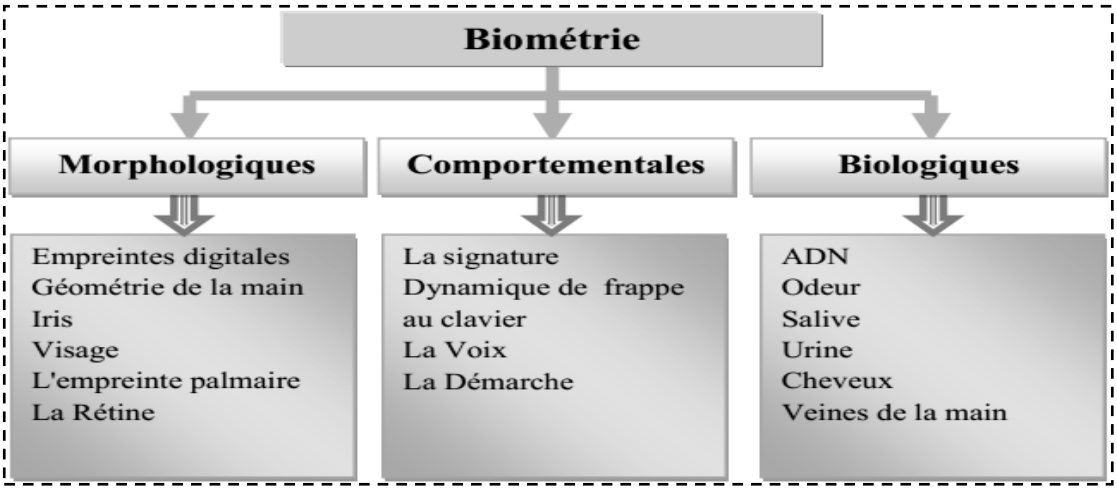


Figure .I.2. : Classification d'un certain nombre de modalités biométriques [3]

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

I.3.2 Modalités comportementale:

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

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

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

I.4 Comparaison entre les différentes modalités biométriques

La comparaison entre les différentes modalités biométriques permet de choisir une modalité en fonction des contraintes liées à l'application. En effet, chaque caractéristique (ou modalité) biométrique a ses forces et ses faiblesses, et faire correspondre un système biométrique spécifique à une application dépend du mode opérationnel de l'application et des caractéristiques biométriques choisies.

En France le Club de la Sécurité des Systèmes d'Information Français [4] a proposé une comparaison (avantages / inconvénients) des principales modalités biométriques en se basant sur la facilité ou l'ergonomie d'utilisation, la vulnérabilité aux attaques, aux contournements, la fiabilité relative à la précision et à l'efficacité de la reconnaissance (voir tableau I.1).

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

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

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

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

Modalités biométriques	Universalité	Distinctif	Permanence	Mesurabilité	Acceptabilité

Empreinte digitale	Moyenne	Haute	Haute	Moyenne	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Haute
Iris	Haute	Haute	Haute	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Faible
ADN	Haute	Haute	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Haute
Démarche	Moyenne	Faible	Faible	Haute	Haute
Frappe clavier	Faible	Faible	Faible	Moyenne	Moyenne
Géométrie de la main	Moyenne	Moyenne	Moyenne	Haute	Haute
Veines main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne

I.5 Fonctionnement d'un système biométrique

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

- L'objectif de l'enregistrement consiste à collecter des échantillons biométriques, et à générer des modèles numériques pour des comparaisons ultérieures. Nous pouvons distinguer la "capture directe" de l'enregistrement en la définissant comme le processus visant à collecter des échantillons biométriques en direct lors d'une tentative d'accès ou d'identification, puis à les comparer à une "galerie" de modèles précédemment enregistrés.
- L'extraction de modèle nécessite un traitement du signal des échantillons biométriques bruts (ex : images ou échantillons audio) afin d'obtenir un modèle numérique. Les modèles sont habituellement générés et stockés lors de l'enregistrement pour gagner du temps lors du traitement des comparaisons ultérieures. La comparaison de deux échantillons biométriques applique des calculs algorithmiques destinés à évaluer leur similarité.

- Lors de la comparaison, un score de correspondance est attribué. S'il est supérieur à un seuil donné, les modèles sont considérés comme identiques. En règle générale, les algorithmes d'extraction de modèle biométrique et de comparaison sont propriétaires (différents et secrets), aussi ne peuvent-ils pas être utilisés au sein d'un même système avec ceux d'autres fournisseurs (ex : pour comparer des modèles générés par différents produits, ou pour utiliser un algorithme de recherche de correspondance d'une société afin de comparer des modèles générés par les algorithmes d'une autre société).

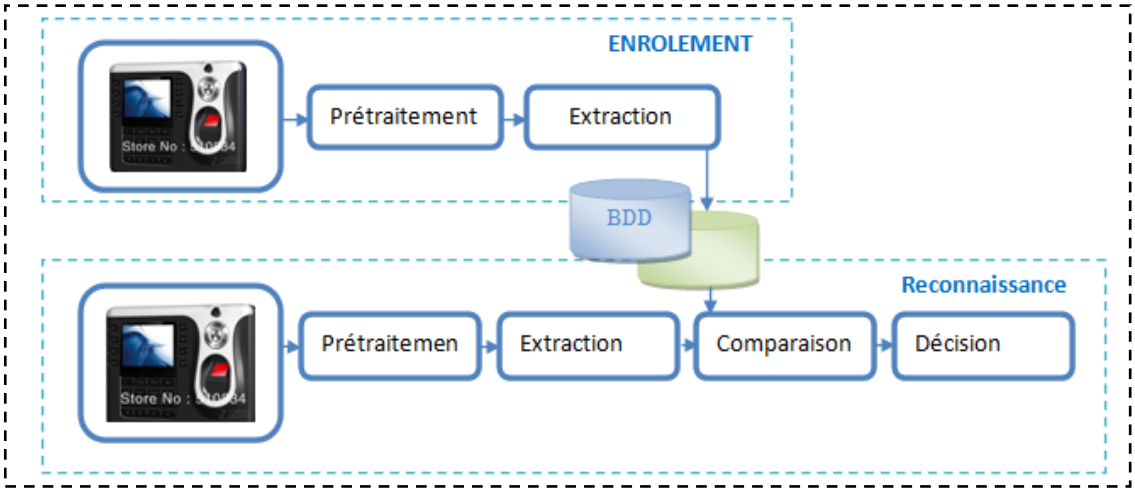


Figure. I.3 : Système de reconnaissance biométrique

1) - Modes de fonctionnement d'un système biométrique

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

Phase de reconnaissance: C'est la phase de vérification ou d'identification d'identité de la personne qui veut accéder au système, elle est primordiale dans

le fonctionnement de la biométrie, Au cours de cette phase le système effectue une saisie de la donnée biométrique puis un ensemble de paramètres sera extrait comme dans la phase de l'enrôlement. Le capteur utilisé dans la phase de reconnaissance doit être aussi proche de celui utilisé dans la phase d'enrôlement.

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

Mode de vérification : c'est la comparaison 1-à-1, entre les données biométriques capturées (modèle de test) et les données stockées dans sa propre base (modèle d'apprentissage). Dans un tel système, un individu qui désire être identifié réclame une identité, habituellement par l'intermédiaire d'un PIN (numéro d'identification personnelle), d'un nom d'utilisateur, d'une carte d'identité, etc. Le système doit alors répondre à la question suivante "*Suis-je réellement la personne que suis-je entrain de proclamer ?*" [6].

Mode d'identification : nommée aussi mode d'authentification, le système identifie un individu en cherchant les signatures (Template) de tous les utilisateurs dans la base de données. Par conséquent, le système conduit plusieurs comparaisons 1-à-N pour établir l'identité d'un individu [7]. En résumé, un système biométrique opérant en mode identification répond à la question "*Suis-je bien connu du système ?*".

2) - Système en ligne et système hors ligne

Les systèmes de reconnaissances biométriques sont classifiés en deux catégories :

- **Système hors ligne** : un système biométrique hors ligne traite les images capturées précédemment. Par exemple, des images obtenues a partir des doigts des mains encrées digitalisées par un scanner numérique. Ces approches peuvent fournir des images à haute résolution et conviennent aux méthodes qui exigent des images de résolution fine pour extraire des lignes,

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

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

I.6 Biométrie multimodale

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

1) - Scénarios de combinaisons

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

- **multi-capteurs :** lorsqu'ils associent plusieurs capteurs pour acquérir la même modalité, par exemple un capteur optique et un capteur capacitif pour l'acquisition de l'empreinte digitale.
- **multi-instances :** lorsqu'ils associent plusieurs instances de la même biométrie, par exemple l'acquisition de plusieurs images de visage avec des changements de pose, d'expression ou d'illumination.
- **multi-algorithmes :** lorsque plusieurs algorithmes traitent la même image acquise, cette multiplicité des algorithmes peut intervenir dans le module d'extraction en considérant plusieurs ensembles de caractéristiques et/ou dans le module de comparaison en utilisant plusieurs algorithmes de comparaison.
- **multi-échantillons :** lorsqu'ils associent plusieurs échantillons différents de la même modalité, par exemple deux empreintes digitales de doigts différents ou les deux iris. Dans ce cas les données sont traitées par le même algorithme mais nécessitent des références différentes à l'enregistrement contrairement aux systèmes multi-instances qui ne nécessitent qu'une seule référence.
- **multi-biométries :** lorsque l'on considère plusieurs biométries différentes, par exemple visage et empreinte digitale. Un système multimodal peut bien sûr combiner ces différents types d'associations, par exemple l'utilisation du visage et de l'empreinte mais en utilisant plusieurs doigts.

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

raison que les systèmes multi-biométries ont reçu beaucoup d'attention de la part des chercheurs.

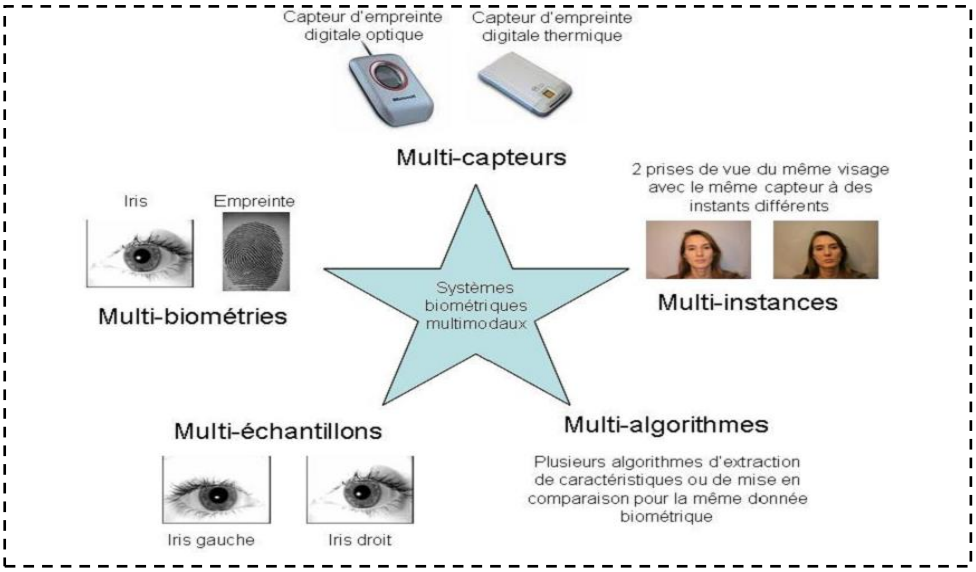


Figure. I.4 : Différents systèmes multimodaux

2) - Technologies de fusion

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

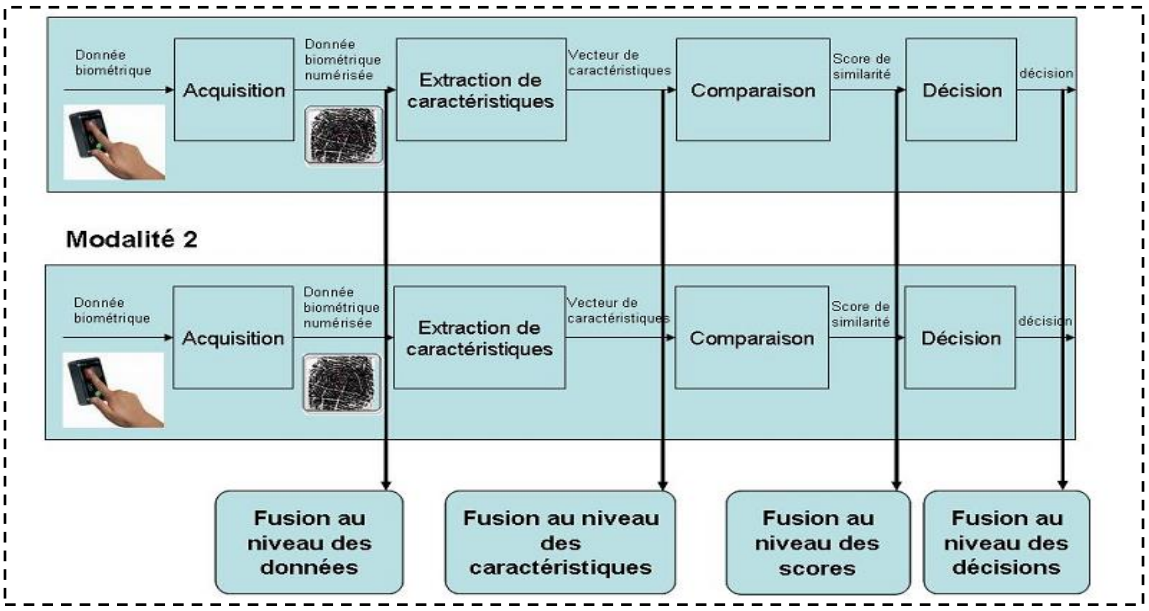


Figure. I.5. Différents niveaux de fusion.

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

caractéristiques individuels. Le vecteur résultant. Néanmoins, quand les vecteurs de caractéristiques sont hétérogènes (de différentes tailles), le vecteur résultant se constitue de la concaténation des vecteurs de caractéristiques individuels.

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

1.7. Domaine d'applications

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

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

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

- **Identification judiciaire :** Dès le début du 20ème siècle, la biométrie est acceptée comme moyen d'identification formelle d'une personne. L'utilisation de la biométrie s'est rapidement répandue. Elle est utilisée pour la première fois dans le domaine judiciaire. Les modalités

biométriques utilisées sont l'empreinte digitale et l'empreinte génétique. Les empreintes digitales sont utilisées depuis longtemps pour prouver certains faits relatifs à des infractions criminelles, dont la présence de l'accusé en un lieu, le fait qu'il ait touché un objet ou une personne,...etc. L'ADN est extrait des cellules de criminel qui sont trouvées sur le lieu du crime. Ces cellules peuvent être des taches de sang, des cellules buccales déposées par de la salive, des cheveux ou encore des cellules coincé sous les ongles de la victime. Il est possible de disculper ou de confondre un suspect avec une très grande sûreté, en identifiant certaines séquences d'ADN propres à un individu et en les comparants à celles présentes dans l'ADN trouvées dans le lieu d'un crime par son auteur. Encore que la recherche criminelle, la vérification des signatures est utilisée dans les contrats afin d'éliminer de les falsifier .

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

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

I.8 Limitations des systèmes biométriques

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

Bruit introduit par le capteur : du bruit peut être présent dans les données biométriques acquises, ceci étant principalement dû à un capteur défaillant ou mal entretenu.

Non-universalité : Cependant, toutes les modalités biométriques ne sont pas vraiment universelles. Le *National Institute of Standards and Technologies* (NIST) a rapporté qu'il n'était pas possible d'obtenir une bonne qualité d'empreinte digitale pour environ 2% de la population (personnes avec des handicaps liés à la main, individus effectuant de nombreux travaux manuels répétés, etc.). La non-universalité entraîne des erreurs d'enrôlement dans un système biométrique,

Manque d'individualité : Par exemple, une certaine partie de la population peut avoir une apparence faciale pratiquement identique due à des facteurs génétiques (père et fils, vrais jumeaux, etc.). Ce manque d'unicité augmente le taux de fausse acceptation,

Sensibilité aux attaques : bien qu'il semble très difficile de voler les modalités biométriques d'une personne, il est toujours possible de contourner un système biométrique en utilisant des modalités biométriques usurpées. Les études dans [18, 19] ont montrés qu'il était possible de fabriquer de fausses empreintes digitales en gomme et de les utiliser pour contrer un système biométrique.

1.9 Conclusion

De nos jours la protection des droits d'auteur est réaliser à l'aide des données biométriques car elle est le moyen de sécurité le plus utilisé grâce à la variabilité des données biométriques est ses avantages. Dans ce chapitre, nous avons, dans une première étape, présenté les différentes modalités biométriques, leurs caractéristiques et une comparaison entre elles. Ensuite, nous avons présenté les

systèmes biométriques unimodaux et multimodaux avec les divers types de combinaisons des modalités possibles, les architectures et les niveaux de fusion qui peuvent être utilisés. Finalement, nous avons terminé ce chapitre par la présentation de quelques techniques de tatouage numérique basées sur les données biométrique pour la protection des droits d'auteur .

Chapitre 02 :

Systèmes biométrique menaces et sécurité

Résumé

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

Introduction

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

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

II.1 Vulnérabilités et menaces d'un système biométrique

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

C'est la raison pour laquelle tout système biométrique doit être analysé, et des contre-mesures doivent être prises lors de la conception du système biométrique. Les différentes attaques dans les systèmes biométriques sont les suivantes [9]:

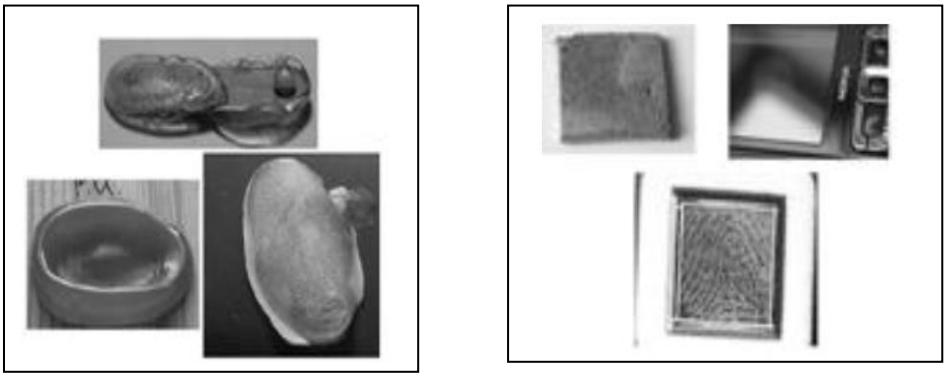
1. Faux biométrie :

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

silicone, la lentille sur un iris, etc. sont quelques-unes de ces attaques malveillantes contre le capteur [10].

2. Attaque par rejoue :

Un attaquant peut présenter une photographie ou lire une vidéo du visage, par exemple, d'un vrai client au capteur, ou à la caméra électronique, du système d'authentification. Ce point est le plus vulnérable dans le système d'authentification car dans un système entièrement automatisé, la possibilité de présenter une photographie est toujours accessible à un attaquant sauf si l'espace physique devant la caméra est supervisé par un observateur humain ou par une seconde modalité biométrique en plus de la caméra d'image faciale. Si un attaquant peut accéder à l'intérieur de la caméra ou à la connexion entre la caméra et l'arrière du système, l'attaquant n'a pas besoin de montrer une photographie ou une vidéo physique à l'appareil photo, mais peut injecter directement dans le système un signal électronique approprié qui correspond à l'image du visage du client [11] .



(a) (b)

Figure. II.1. Attaque par rejoue :

(a) Empreintes digitales en plastique (gélatine, silicone, moule en plastique),

(b) Fausse empreinte digitale, une empreinte latente sur téléphone portable.

3. Transmission de données biométriques interceptées

Ici, l'attaquant rejoue une ancienne donnée biométrique stockée dans le système sans passer par le capteur biométrique. C'est le cas de la présentation d'une ancienne copie de l'image de l'empreinte digitale. Étant donné que l'attaquant contourne le capteur biométrique en fournissant au système une ancienne donnée enregistrée, les métadonnées n'auront aucun effet contre cette forme d'attaque [11].

4. Attaque sur le module d'extraction de caractéristiques

Ce module pourrait être remplacé par le virus cheval de Troie afin de produire des informations choisies par l'attaquant. L'utilisateur légitime ne se rend pas compte que ce module a été corrompu et a fourni des informations conformément aux instructions du pirate. Le module d'extraction de caractéristiques étant compromis par l'hacker, les métadonnées ne seront pas efficaces contre ce genre d'attaque [12].

5. Altération des caractéristiques extraites

Une fois les données obtenues par le module d'extraction de caractéristiques, elles sont altérées voire remplacées par d'autres données définies par l'attaquant. Pour les attaques d'infrastructure non sécurisées, nous sommes dans des situations où le système biométrique est corrompu et ne fournira des réponses qu'en fonction de l'intention du pirate. Les métadonnées ne seront pas efficaces dans ces contextes [12].

6. Remplacement du module du correspondant par un module malveillant

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

7. Corruption de la base de données

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

II.2 Protection des systèmes biométriques

Tel que précisé par **Jainet Aldan sil** dans [13], existe principalement deux classes pour les méthodes de protection du modèle biométrique que sont : les crypto-systèmes biométriques et les approches par transformation .

Crypto systèmes biométriques

Pour résoudre les problèmes mentionnés ci-dessus, nous présentons dans cette section les crypto-systèmes biométrique. Fondamentalement, la combinaison de la cryptographie et d'un système biométrique est connue sous le nom de crypto-système biométrique.

En utilisant cette technique, la cryptographie fournira un niveau de sécurité élevé et la biométrie aidera à éviter de se souvenir des mots de passe. De plus, les clés cryptographiques sont générées à partir des modèles biométriques de l'utilisateur.

À moins que la même personne ne participe à nouveau, le système ne révélera pas les clés précédemment stockées pour la vérification, Il existe deux types de crypto-systèmes biométriques, selon la façon dont les données auxiliaires sont dérivées :

- système de liaison des clés et système de génération des clés.
- Schémas de génération de clés

Crypto système de liaison des clés

Dans ce schéma, des données auxiliaires sont obtenues en liant une clé cryptographique choisie à un modèle biométrique. À la suite du processus de

liaison, une fusion de la clé secrète et du modèle biométrique est stockée en tant que données auxiliaires. En appliquant un algorithme de récupération de clé approprié, les clés sont obtenues à partir des données auxiliaires lors de l'authentification. Étant donné que les clés cryptographiques sont indépendantes des références biométriques, elles sont révocables, tandis qu'une mise à jour de la clé nécessite généralement un réenregistrement afin de générer de nouvelles données auxiliaires [13]. Le mode de fonctionnement général d'un schéma de liaison de clé est illustré sur la figure II.2.

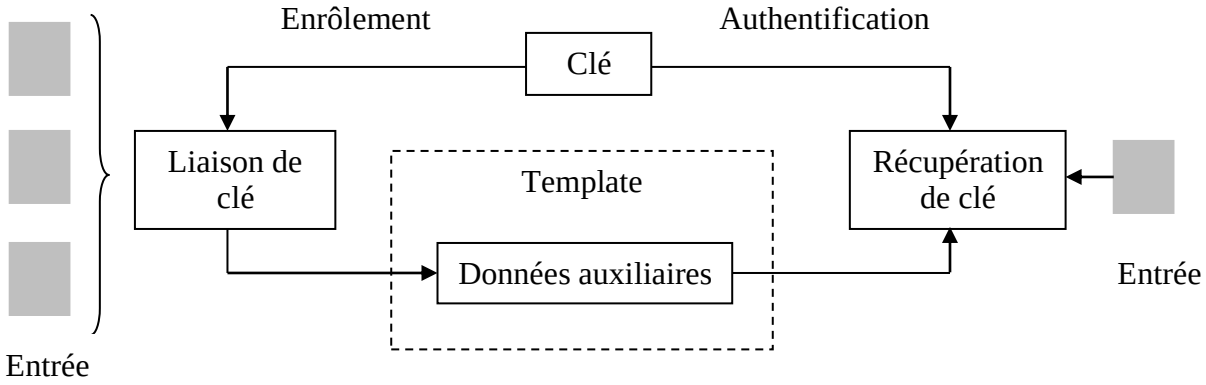


Fig II.2. Mode de fonctionnement général d'un schéma de liaison de clé

Crypto système de génération de clés

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

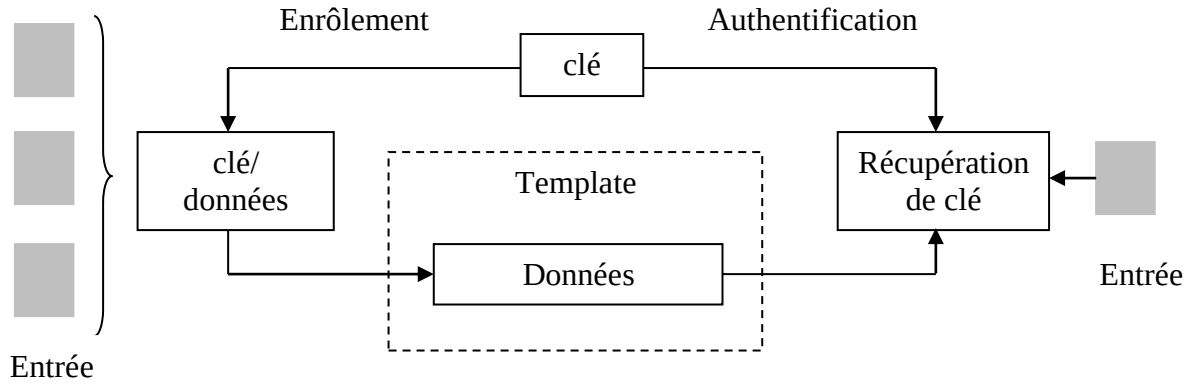


Fig. II.3. Mode de fonctionnement général d'un schéma de génération de clé .

Un problème spécifique lié à la robustesse de ces systèmes biométriques contre les attaques réside dans leur garantie d'assurer la sécurité des modèles biométriques des gabarits sauvegardés dans une base de données, Quelle sera alors la capacité de ces systèmes pour freiner un intrus à modifier ou supprimer les gabarits biométriques existants ou encore d'en introduire de nouveaux modèles dans la base de données ?

A priori la solution naïve qui peut provenir à nos esprits pour renforcer la sécurité de ces systèmes est l'incorporation des données biométrique dans un système classique de cryptage – décryptage, cependant le problème reste non résolu devant une entrée caractérisée principalement par son non uniformité et variation au fil du temps. Le couplage des crypto-systèmes aux systèmes biométriques se fait intelligemment et s'annonce prometteur dans une association qui profite des avantages de l'un pour combler les lacunes de l'autre, produisant ainsi un bloc unique ayant le potentiel de fusionner la sécurité

prouvée des crypto-systèmes à l'utilisation faciles et pratiques des systèmes biométriques .

Crypto système base sur la transformation révocable

Les approches de cette famille n'utilisent pas de données auxiliaires pour compenser la variabilité du signal biométrique, ce qui signifie que la comparaison est effectuée dans le domaine de la transformation directement entre les modèles transformés. Supposons que **X** sera transformé en données codées **T** lors de l'enrôlement par l'utilisation d'une fonction **F**. Pour la vérification, la requête biométrique **Y** sera transformée en **T'** toujours en utilisant la fonction **F** et l'authentification réussira si **T** est proche de **T'**en utilisant une certaine mesure de similarité. Pour assurer la révocabilité du système, une donnée aléatoire **S** sous forme d'une clé est attribuée à chaque utilisateur **U**. La clé **S** est alors considérée comme un paramètre d'entrée de la fonction de transformation **F**. La révocation consiste au remplacement direct de cette clé utilisateur. La figure II.4 résume le fonctionnement des transformations révocables .

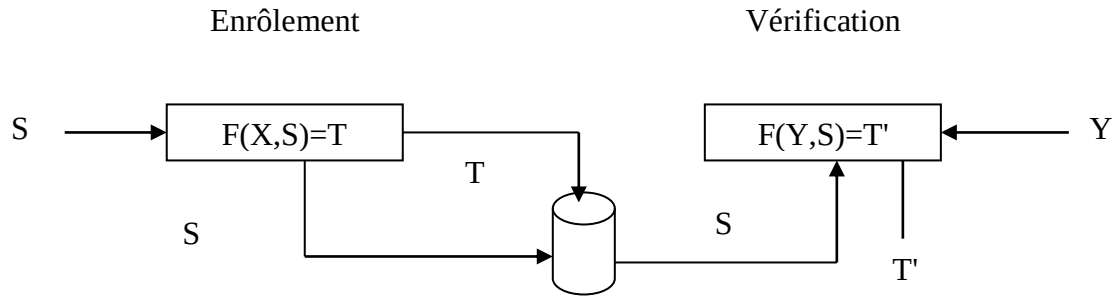


Fig. II.4. Fonctionnement générique des transformations révocable .

II.3 Techniques hybrides

Dans les systèmes hybrides, les deux méthodes de protection; transformation des caractéristiques et les crypto-systèmes biométriques sont combinées pour construire un système robuste. Le but principal de faire cette combinaison de différentes approches est d'exploiter les avantages des deux techniques tout en évitant leurs des avantages. Feng et al [13] ont proposé une approche hybride basée sur la reconnaissance faciale en utilisant premièrement une projection aléatoire puis la méthode des crypto-systèmes biométriques Fuzzy Commitment. Autres techniques d'hybridation sont basées sur l'utilisation de mots de passe pour renforcer la sécurité des crypto-systèmes. Dans leur travail, Nanda Kumar et al [13] ont utilisé un mot de passe pour transformer les caractéristiques des empreintes digitales en se basant sur la méthode des crypto-systèmes Fuzzy Vault, Ari et al [13] ont proposé une méthode hybride basée sur la génération de la clé secrète durant l'enrôlement à partir des données biométriques en appliquant le hachage discret.

II.4 Travaux connexes

Il y a eu un certain nombre d'efforts de recherche visant à résoudre les problèmes liés aux crypto-systèmes biométriques. L'un des premiers crypto-systèmes biométriques implémentant la liaison de clé a été proposé par Soutar et al [13]. Dans cette méthode, un algorithme de liaison de clé dans un système de correspondance d'empreintes digitales basé sur la corrélation optique est proposé. Cet algorithme lie une clé cryptographique aux images d'empreintes digitales de l'utilisateur au moment de l'inscription. La clé n'est ensuite récupérée qu'après une authentification réussie. L'algorithme crée d'abord une fonction de filtre de corrélation qui à la fois les composantes d'amplitude et de phase. Les critères de conception pour cette fonction incluent à la fois la tolérance à la distorsion et la discriminabilité.

L'algorithme calcule également une sortie qui est obtenue par convolution/corrélation des images d'empreintes digitales d'apprentissage avec la fonction de filtre de corrélation, Ensuite le conjugué complexe de la composante de phase de la fonction de filtre de corrélation est multiplié par un réseau de phase uniquement généré aléatoirement de la même taille. Alam et al [13] à proposé un crypto-système biométrique, qui intègre la transformée de Fourier discrète (DFT) et une technique révocable basée sur la projection aléatoire pour renforcer la sécurité. Dans le système proposé, les caractéristiques d'empreintes digitales basées sur une grille polaire sont transformées en utilisant la DFT et la projection aléatoire, créant un modèle non inversible. En outre une stratégie de basculement de bits est utilisée pour injecter du bruit dans le modèle généré a fin de renforcer davantage la sécurité du modèle.

Sarkar et Singh [13] ont proposé la génération de clés cryptographiques à partir de modèles d'empreintes digitales Différentes clés d'une longueur de 128 bits peuvent être générées en annulant et en rééditant différents modèles d'empreintes digitales. Cela réduit le risque potentiel que la même clé secrète qui existait avec le récepteur et l'expéditeur puisse être divulguée après négociation Dans [13], Liu et Zhao ont utilisé la minimisation l1 pour protéger les modèles d'empreintes digitales et les stocker sous forme de texte chiffré. La correspondance d'empreintes digitales est effectuée dans le domaine crypté et l'authentification n'est réussie que lorsque l'empreinte digitale de la requête est suffisamment proche de l'empreinte digitale modèle. Comme le modèle est généré à partir du Minutai Cylinder Code (MCC) avec la conception appropriée de l'algorithme sécurisé, le système proposé atteint une sécurité et une précision de reconnaissance élevées. Xi et al [13] ont proposés un extracteur flou utilisant une structure locale bicouche. Dans ce système, les extracteurs flous sont basés sur des codes correcteurs d'erreurs Une clé cryptographique est codée avec un code de contrôle d'erreur, puis la séquence codée de bits s'intègre aux

caractéristiques biométriques qui sont calculées à l'aide des données de l'échantillon d'apprentissage. Ce processus génère une chaîne ouverte. Alors que la personne authentifiée présente les données biométriques, les données sont calculées avec la chaîne ouverte en utilisant XOR. Le processus aboutit à une libération de clé avec des bits erronés corrigés. Li et al ont proposé un schéma de voûte floue, qui combine deux structures locales, le descripteur de minutie et la structure locale de minutie. En utilisant trois approches de fusion, les deux structures locales invariantes par transformation sont intégrées dans le schéma proposé. Li fang Wu et al ont développé un crypto-système biométrique basé sur la biométrie faciale. Pendant le cryptage, le vecteur de caractéristiques de l'analyse en composantes principales (ACP) à 128 dimensions est initialement obtenu à partir de l'image du visage. Par la suite, un vecteur binaire de 128 bits est obtenu par seuillage. Ensuite, l'auteur a sélectionné des bits distinguables pour générer une bio-clé. De plus, un code de correction d'erreur est produit à l'aide de l'algorithme de Reed-Solomon. Afin de fournir un décodage de correction d'erreur plus précis dans un schéma d'engagement flou basé sur l'iris, qui se rapproche d'une borne théorique obtenue par Bringer et al, les auteurs appliquent un décodage mini-sum itératif bidimensionnel. Dans leur approche, une matrice est créée où les lignes ainsi que les colonnes sont formées par deux codes binaires différents de Reed-Muller.

Des approches hybrides [14,18] qui utilisent à la fois des schémas de génération de clés et des concepts de liaison de clés ont également été proposées. Dans les auteurs proposent une approche hybride qui tire parti à la fois de l'approche du crypto-système biométrique et de l'approche basée sur la transformation. Un algorithme hybride en trois étapes est conçu et développé sur la base d'une projection aléatoire, d'une transformation préservant la discriminabilité (DP) et d'un schéma d'engagement flou. La projection aléatoire est utilisée pour fournir l'annulation. La transformation DP est développée pour convertir des modèles

annulables à valeur réelle en modèles binaires tandis que la discriminabilité est préservée, de sorte qu'elle puisse être facilement chiffrée dans le schéma d'engagement flou.

II.5 Avantages des crypto-systèmes biométriques

Les crypto-systèmes biométriques offrent plusieurs avantages par rapport aux systèmes biométriques conventionnels. Les principaux avantages peuvent être résumés comme suit:

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

II.6 Conclusion

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

Chapitre 03
Résultats et Expérimentaux

Résumé

L'étape d'extraction de caractéristiques dans un système de reconnaissance de formes est l'une des étapes les plus importantes du système . D'un point de vue sécuritaire, cette étape doit fournir une nouvelle représentation à la fois unique pour distinguer différentes personnes et révocable en cas de piratage.

Ce chapitre se concentre sur l'évaluation de la méthode d'extraction de caractéristiques proposée (CL-HOG) des deux aspects, la précision du système d'identification et la robustesse contre les tentatives de piratage. Tous les tests ont été réalisés à l'aide d'un système d'identification biométrique, en utilisant une base de données biométrique multi spectrale.

Introduction

Les systèmes de reconnaissance biométrique sont susceptibles de fournir un degré plus élevé de sécurité et de fiabilité, mais des préoccupations subsistent quant au risque que des templates biométriques soient volés et réutilisés illégalement. Dans ce chapitre, nous allons proposer un Crypto-Système Biométrique capable de générer des templates biométriques avec les empreintes palmaire en cas de falsification. La méthode proposée est basée la transformation des ces derniers en utilisant les Cartes Logistiques (CSB-CL) .

III.1 Prérequis théoriques

La protection des gabarits biométriques est l'une des opérations le plus utilisée dans la conception finale d'un système biométrique afin de minimiser les risques des attaques malveillantes. Dans cette section, nous essayons de donner les pré-requis théoriques concernant la méthode d'extraction de caractéristique HOG et les cartes logistiques sur les quels est basé le crypto-système biométrique proposé .

1. Extraction de caractéristiques : Histogramme des gradients orientés

Le HOG est une nouvelle méthode utilisée en vision par ordinateur pour la détection d'objet et la détection des régions d'intérêts. Le principe de base de cette méthode est de calculer les histogrammes locaux de l'orientation du gradient sur une grille dense, c'est-à-dire sur des zones régulièrement réparties sur l'image .

L'objectif de la méthode HOG est que l'apparence et la forme locale d'un objet dans une image peuvent être décrites par la distribution de l'intensité du gradient ou la direction des contours. La figure III.1, illustre les différentes étapes de la méthode HOG. Le principe de cette méthode consiste à diviser une image à des

régions adjacentes de petite taille, appelées cellules, et en calculant pour chaque cellule l'histogramme des directions du gradient ou des orientations des contours pour les pixels à l'intérieur de cette cellule. La combinaison des histogrammes forme alors le descripteur HOG. Pour de meilleurs résultats, les histogrammes locaux sont normalisés en contraste, en calculant une mesure de l'intensité sur des zones plus larges que les cellules, appelées des blocs, et en utilisant cette valeur pour normaliser toutes les cellules du bloc. Cette normalisation permet une meilleure résistance aux changements d'illuminations et aux ombres .

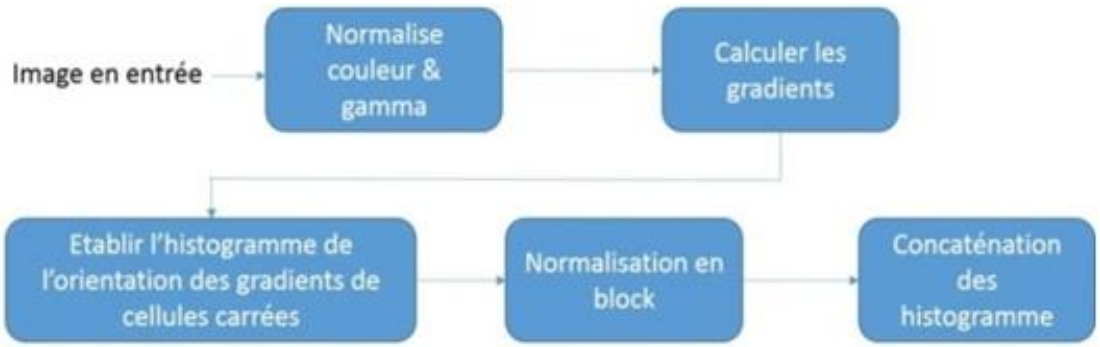


Fig. III.1 : Schéma des blocs de méthode HOG

2. Les cartes Logistiques

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

$$x_{n+1} = \Gamma_L(x_n, \mu) \quad (1)$$

$$= \mu x_n(1 - x_n),\ \mu \in [0,4],\ x_n \in [0,1] \quad (2)$$

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

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

III.2 Schéma fonctionnel de la méthode proposée

La Figure .III.1 montre le schéma fonctionnel de la méthode proposée pour la protection du gabarit de l'empreinte palmaire. En général, la méthode proposée est être divisée en deux étapes principales : *projection*, et *déguisement* .

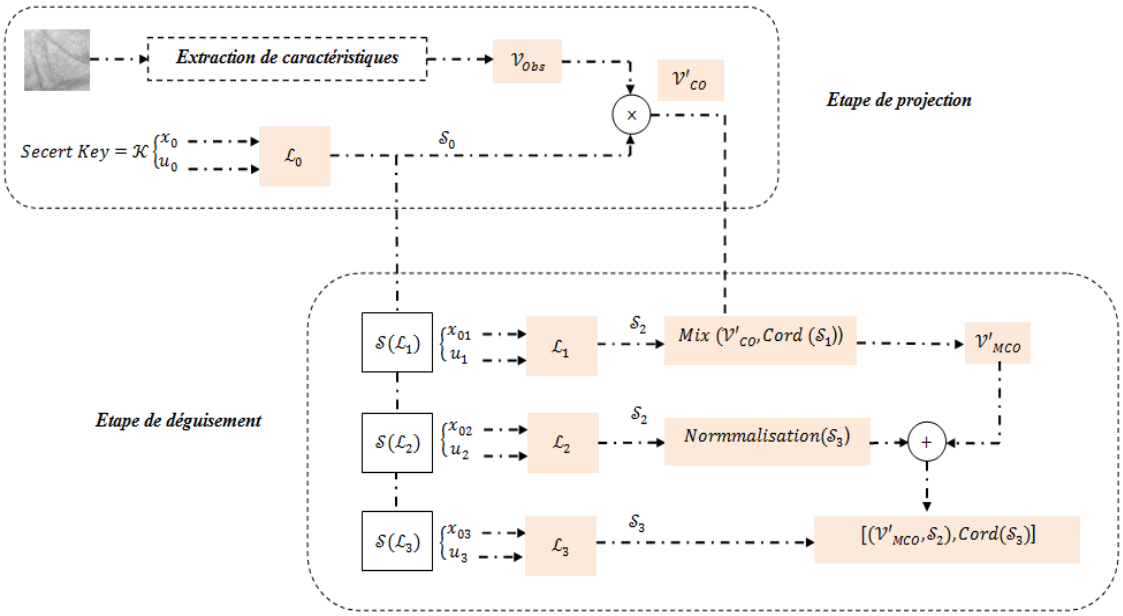


Fig. III.3. Schéma fonctionnel de la méthode de protection du template biométriques basée sur les cartes chaotiques .

La figure III.3, montre que notre système utilise plusieurs systèmes chaotiques, dont l'un est dite maitre (clé secrète) et les autres sont dites esclaves (servent au déguisement du gabarit transformé). Il est important de souligner que la clé secrète ($\mathcal{K}$) de notre système peut être représentée par une valeur réelle ou entière codée en hexadécimal .

1. **Etape de projection**

Dans cette étape, après l'extraction des vecteurs de caractéristiques par la méthode HOG, notre système utilise le premier système chaotique $\mathcal{L}_0$ avec une clé secrète $\mathcal{K}$ pour générer une séquence $\mathcal{S}_0$ qui est utilisée à la fois pour contrôler les systèmes chaotiques utilisés dans l'étape de déguisement et pour la transformation de vecteur de caractéristiques dans l'étape de projection. Nous notons que la taille de cette séquence est égale à la taille du gabarit biométrique . Le processus de transformation de vecteur de caractéristiques repose sur la projection de ce dernier dans un espace chaotique ($\mathcal{S}_0$) généré par la clé secrète $\mathcal{K}$.

Soit :

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

$$\mathcal{V}_{obs} = [x_1, x_2, x_3, \cdots, x_n] \quad (3)$$

Le vecteur de caractéristiques $\mathcal{V}_{obs}$ d'un utilisateur sera transformé en vecteur $\mathcal{V}_{CO}$:

$$\mathcal{V}_{CO} = \mathcal{V}_{obs} * \mathcal{S}_0 \quad (4)$$

2. Etape de déguisement

Dans cette étape, afin de mieux protéger le gabarit biométrique, nous le déguisons en utilisant un concept quelque peu similaire au Fuzzy Vault. L'étape de déguisement, présenté dans la figure III.3, génère également trois séquences $\mathcal{S}_1(L_1)$, $\mathcal{S}_2(L_2)$, et $\mathcal{S}_3(L_3)$ qui permettent : *i)* de créer des shaff-points, *ii)* de réorganiser les éléments de $\mathcal{V}_{CO}$ et *iii)* de construire le gabarit déguisé.

i. Les composants de la première séquence $\mathcal{S}_1(L_1)$ sont utilisées comme un ensemble de chaff points, la taille de cette séquence est égale à la taille du gabarit biométrique. Les composants de cette séquence sont normalisés en se basant sur la pondération de la séquence $\mathcal{S}_1(L_1)$ avec la valeur maximale du gabarit biométrique $\mathcal{V}_{CO}$:

$$\mathcal{S}_1(L_1) = \mathcal{S}_1(L_1) \times Max(\mathcal{V}_{CO}) \quad (5)$$

ii. La deuxième séquence $\mathcal{S}_2(L_2)$ est utilisée pour réorganiser les éléments de gabarit biométrique:

Premièrement, la séquence $\mathcal{S}_2(L_2)$ est triée en ordre croissant ou décroissant

$$\mathcal{S}_2^S(L_2) = Sort(\ \mathcal{S}_2(L_2)) \quad (6)$$

Ensuite, une séquence de composantes entières représentant les coordonnées de la séquence $\mathcal{S}_2^S(L_2)$ dans $\mathcal{S}_2(L_2)$

$$Cord_{L_2}^{\mathcal{S}_2} = index\left(\mathcal{S}_2^S(L_2)_i,\ \mathcal{S}_2(L_2)\right),\ i = 1 \dots len(\mathcal{V}_T) \quad (7)$$

Finalement, une simple permutation entre les composants de $\mathcal{V}_{CO}$ basée sur $Cord_{L_2}^{\mathcal{S}_2}$ est appliquée donnant $\mathcal{V}_{MCO}$.

iii. La troisième séquence $\mathcal{S}_3(L_3)$ est utilisée pour réorganiser les coordonnées de vecteur déguisé $\widetilde{\mathcal{V}_T}$ regroupant les composants de $\mathcal{V}_{MCO}$ et les chaff points $\mathcal{S}_1(L_1)$. La taille de cette séquence est égale à deux fois de la taille du gabarit biométrique.

Premièrement, la séquence $\mathcal{S}_3(L_3)$ est triée en ordre croissant ou décroissant

$$\mathcal{S}_3^S(L_3) = Sort(\mathcal{S}_3(L_3)) \quad (8)$$

Ensuite, une séquence de composantes entières représentant les coordonnées de la séquence $\mathcal{S}_3^S(L_3)$ dans $\mathcal{S}_3(L_3)$

$$Cord_{L_3}^{\mathcal{S}_3} = index\left(\mathcal{S}_3^S(L_3)_i,\ \mathcal{S}_3(L_3)\right),\ i = 1 \dots len\ (2 \times\ \mathcal{V}_{MCO}) \quad (9)$$

Finalement, Le gabarit biométrique déguisée final ($\widetilde{\mathcal{V}_T}$) est déni comme suit:

$$\widetilde{\mathcal{V}_T} = [\mathcal{S}_1(L_1),\ \mathcal{V'}_T\ ]_i,\ i\ \epsilon\ Cord_{L_3}^{\mathcal{S}_3} \quad (10)$$

III.3 Résultats expérimentaux

Le but de cette section est d'évaluer les performances de la méthode proposée, nous avons donc implémenté notre méthode pour un système d'identication biométrique à base de l'empreinte palmaire.

1. Base d'images: Pour l'évaluation de notre méthode proposée, nous avons utilisé une base de données d'empreintes palmaires créée par l'Université polytechnique de Hong Kong (PolyU). Cette base de données a été obtenue en collectant des images d'empreintes palmaires multispectrales de 500 individus à l'aide d'un dispositif de capture d'empreintes palmaires multispectrales. Les personnes inscrites dans cette base de données sont les étudiants et les travailleurs de PolyU et qui sont invitées en deux sessions pour fournir environ 12 images (six images dans chaque session). L'intervalle moyen entre la première et la deuxième session est de 9 jours. Toutes les images ont été fournies sous différentes conditions d'éclairage. Cette base de données (PolyU) contient 60000 images de quatre bandes spectrales différentes : Rouge, Vert, Bleu et proche infrarouge. Toutes les images originales ont une taille de 352x288 pixels et une résolution de <100 dpi.

Dans nos tests, nous n'avons utilisé les trois bandes Rouge, Vert, Bleu afin de construire des biométries palmaire en niveau de gris.

2. Protocole de tests : Dans le cadre de notre travail, nous avons utilisé une base de données contenant 400 personnes (12 images pour chaque personne, donc 4800 images). Cette base est similaire au nombre d'employés des petites et moyennes entreprises. Dans la phase d'enrôlement, nous avons utilisés au hasard quatre échantillons de la modalité biométrique pour chaque personne, soit 400 × 4 =1600 échantillons, tandis que les huit autres échantillons ont été utilisés pour l'évaluation des performances du système, soit 400 × 8 =3200 échantillons.

En utilisant toutes les images de test, 641600 scores correspondants ont été obtenus, dont 3200 scores pour des expériences authentiques et 638400 scores pour des expériences d'imposteurs.

3. Evaluation de performance: Les résultats expérimentaux que nous allons présenter dans ce travail sont divisés en deux parties. Nous donnerons dans un

premier temps les résultats obtenus concernant la sélection des meilleurs paramètres de la méthode d'extraction de caractéristiques HOG. La deuxième partie des résultats se concentre en particulier sur le système protégé en exploitant notre méthode proposée.

A. Sélection des paramètres de HOG

Avant d'évaluer les performances de crypto système biométrique proposé, une phase de sélection de paramètre concernant l'algorithme HOG est réalisé. Trois paramètres importants dans le méthode HOG et qui sont la taille de bloc, la taille de fenêtre et le pourcentage de chevauchement entre les blocs adjacents. Ce que nous intéressent c'est bien la taille de bloc et la taille de fenêtre (plusieurs travaux montrent que un pourcentage de chevauchement égale à 50% est suffisant pour que l'algorithme fonctionne efficacement). Pour avoir des meilleurs paramètres (paramètres optimaux), nous avons testé l'algorithme HOG avec des blocs de tailles 40×40, 60×60, et 80×80, des fenêtre de tailles 16×16 et 32×32 et avec le même pourcentage de chevauchement avec le classifieurs 1-PPV.

Pour examiner l'effet de ces paramètres sur la précision du système d'identification biométrique (en mode ensemble ouvert), nous illustrons avec le classifieur KPPV (*k* Plus Proches Voisins) les performances du système sous forme seuil et de taux d'erreur égales.

Tableau III.1: performances de système biométrique basées sur les paramètres de HOG

Taille de Fenêtre	16x16		32x32	
Taille de Bloc	To	EER	To	EER
40x40	0.4105	0.212	**0.4005**	**0.132**
60x60	0.3984	0.208	0.4014	0.188
80x80	0.4020	0.282	0.4120	0.201

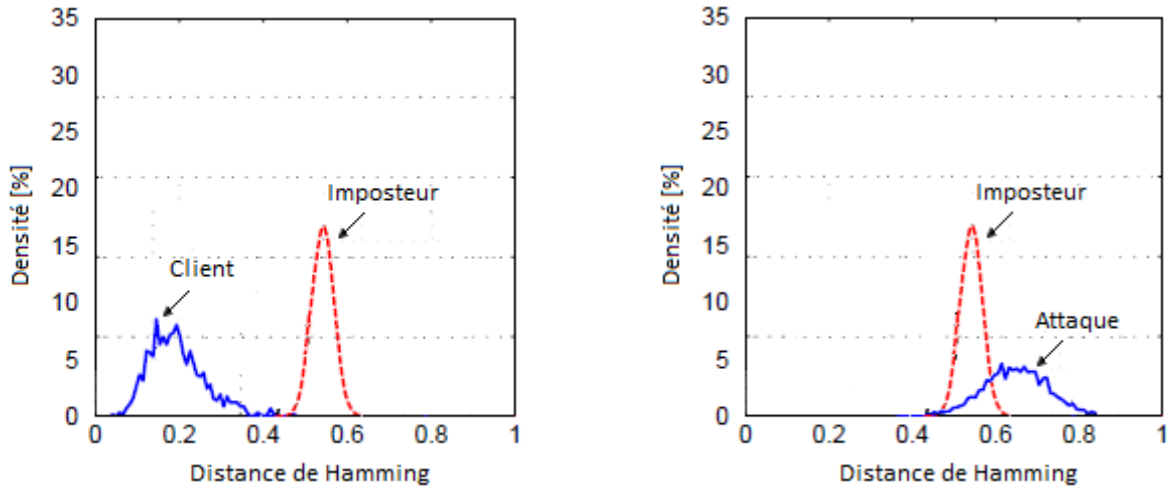
Le tableau III.1 montre les performance de système biométrique en terme de ERR et le seuil T_0.

Nous observons, en général, que ces paramètres offrent des résultats très acceptables en terme de ERR. Une meilleur performance peut être obtenue avec un bloc de taille 40x40 et une fenêtre de taille 32x32 (ERR=**0.132**, T_0=**0.4005**).

B. Performance de système biométrique

Dans cette sous-section, nous évaluerons les performances du système sécurisé (template protégé : CL-HOG) en se basant sur les meilleurs paramètres de HOG (un bloc de taille 40x40 et une fenêtre de taille 32x32) obtenus dans la section précédente.

Pour se faire, nous avons tracé les performances de crypto-système biométrique proposé avec une clé correcte et avec une clé incorrecte afin de voir le changement qui peut se produire dans le comportement de système proposé (voir Fig. III.4).



(a) *(b)*

Fig. III.4. Comparaison des performances de système protégé avec une clé correcte et système protégé avec une clé incorrecte

La figure III.4 (a), montre que le système avec une template protéger fonctionne efficacement avec un taux d'erreur nul (EER = 0,000% avec un seuil T_o = 0,046) avec un intervalle de confiance assez large (IC = 0,0420).
D'autre part, nous observons, dans la figure III.4 (b), un changement des scores des clients à la même position que les scores des imposteurs lors de l'utilisation d'une fausse clé de sécurité (tentative d'attaque). Le meilleur cas est lorsque tous les scores d'attaque sont supérieur au seuil de sécurité (T_o).

III.4. Conclusion

Dans ce chapitre, nous avons proposés un crypto système biométrique basé sur la méthode d'extraction de caractéristiques HOG et les cartes logistiques. L'objectif de ce crypto système est la protection du gabarit de template palmaire contre les attaques. les résultats expérimentaux montrent que les performances du système biométrique sont généralement dégradées lors d'une attaque, ce qui est très normal car le template biométrique a été soumis à un processus de transformation.

Conclusion Générale

Afin d'assurer les quatre fonctions de la sécurité de l'informations (confidentialité, intégrité, non-répudiation, et traçabilité), trois techniques peuvent être utilisées: la dissimulation de l'information, la cryptographie et la biométrie.

De nos jours, la biométrie a connu un grand succès afin d'assurer le contrôle d'accès des individus. En fait, plusieurs systèmes biométrique ont été développés et jugés efficaces vue de leurs haute performances dans l'authentification des individus. Malheureusement, ces systèmes peuvent être utilisés dans des applications à distance, ce qui conduit au vol de gabarit de la modalité biométrique. Plusieurs solutions ont été proposés et consiste à l'utilisation de la cryptographie afin d'assurer le transfert du gabarit biométrique. Alors, d'un autre coté, la récupération illégale de la clé cryptographique peut conduire à la perte du gabarit biométrique une fois pour toutes, et donc compromettre la vie privée de la personne.

Dans ce travail, nous avons proposé une méthode pour la protection du gabarit biométrique des empreintes palmaire. Notre méthode repose sur des systèmes chaotiques pour produire une transformation du gabarit obtenu par la méthode d'extraction de caractéristique HOG en raison de son extrême sensibilité aux conditions initiales. Ces systèmes sont récemment révélés tries efficaces dans les systèmes de sécurité de l'information.

Les expériences ont été réalisées sur une base de données moyenne contenant 40 personnes représentées par des images d'empreintes palmaires Les résultats expérimentaux ont montré un taux d'identification élevé, qui peut également être amélioré en changeant la méthode d'extraction de caractéristique. Les travaux futurs de cette étude se concentreront sur l'utilisation d'autres techniques d'apprentissage en profondeur comme DCTNET et ICANET .

Annexe A

Evaluation des performances

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

A.1 Mesures des taux d'erreur

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

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

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

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

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

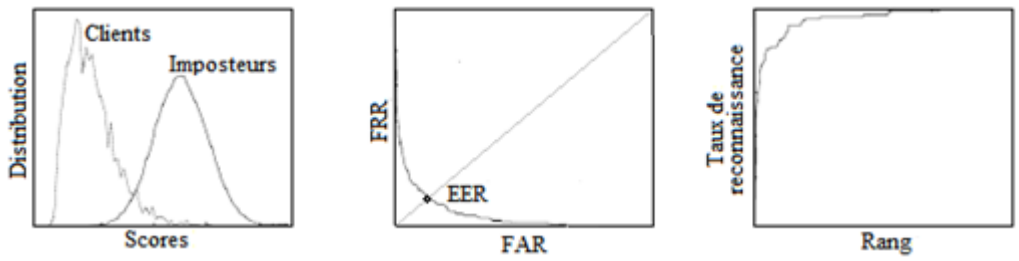
Taux des clients acceptés (*GAR* : Genuine Acceptance Rate**) :** C'est le taux des personnes clients autorisées qui sont acceptées par le système biométrique, ce

taux est important car elle représente le sucées de système. Il est exprimé par la relation suivant :

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

A.2 Courbes de performance

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



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

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

A.3 Point de fonctionnement

Le point de fonctionnement qui définit le choix du seuil dans le module de décision dépend de l'application visée [38]. En général lorsqu'il n'y a pas

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

Annexe B

Prétraitement

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

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

Figure B.1 : Image originale filtrée

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

Figure B.2 : Image binaire

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

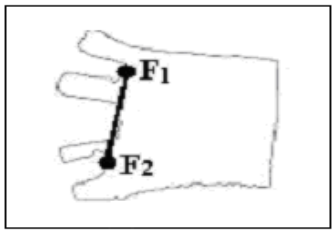


Figure B.3 : Contour extérieur

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

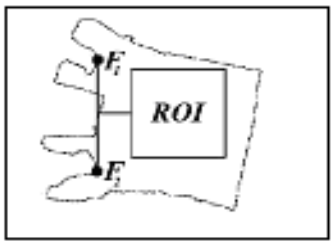


Figure B.4 : Image tourné

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

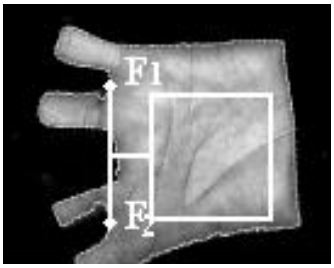


Figure B.5 : Sélection de la région d'intérêt

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

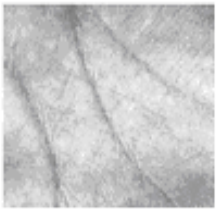


Figure B.6 : Région d'intérêt ROI

Bibliographies

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

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

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

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

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

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

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

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

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

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

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

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

[13] Lafkih M., Lacharme P., Rosenberger C., Mikram M., Ghouzali S., and Haziti M., “Vulnerabilities of Fuzzy Vault Schemes Using Biometric Data with Traces,” in

Proceedings of IEEE International Wireless Communications and Mobile Computing Conference, Dubrovnik, pp. 822-827, **2015**.

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

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

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

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

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