N°d'ordre: .....

République Algerienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la Recherche scientifique

Université Djillali Liabès de Sidi Bel Abbès
Faculté des Sciences Exactes
Département d'informatique
Laboratoire EEDIS

Thèse de Doctorat en Sciences

Filière : Informatique
Spécialité : Intélligence Artificille

Par

M^me Fatima Bedad

Protection des données multi-biométriques

Soutenue le .. .. 201. devant le jury :

Pr.	Boukli Hacene sofiane	UDL SBA	Président du jury
Pr.	Amar Bensaber Djamel	ESI SBA	Examinateur
Pr.	Keskes Nabil	ESI SBA	Examinateur
Pr.	Réda Adjoudj	UDL SBA	Directeur de thèse

Année Universitaire : 2021 - 2022

Je dédie ce travail Particulièrement .....à ma très chère maman , ceci est ma profonde gratitude pour ton éternel amour , que cet doctorat soit le meilleur cadeau que je puisse t'offrir . . .

Remerciements

En tout premier lieu, Je remercie Dieu, le tout puissant de nous avoir gardé en bonne santé, de nous avoir donné le courage et la patience pour l'accomplissement de ce travail.

Je tiens tout d'abord à exprimer mes sincères remerciements à mon directeur de recherche Pr. ADJOUJ Réda qui a accepté d'encadrer et diriger le présent travail, qui m'a encouragé et soutenu.

Je tiens aussi à remercier les membres du jury pour leur précieux temps accordé à l'étude de ma thèse.

Je remercie très spécialement Melle BOUSSAHBA Nassima et sa famille pour leur sincère amitié et confiance, leur soutien inconditionnel et leur encouragement.

Que toute personne ayant œuvré de près ou de loin à la réalisation de ce projet par une quelconque forme de contribution, trouve ici le témoignage de ma plus profonde reconnaissance.

Je garde pour la fin les personnes de mon cœur, compagnons de souffrances mais surtout d'échanges chaleureux ; mes parents, mon mari, mon fils et mes sœurs .

À tous ces intervenants, je présente mes remerciements, mon respect et ma gratitude.

Lieu, le 10 avril 2022.

Table des matières

Liste des figures

Liste des tableaux

Introduction 1

Sommaire

1.1 PROBLÉMATIQUE ET LES OBJECTIFS DE RECHERCHE

Au cours de ces dernières années, la reconnaissance des personnes doit être de plus en plus une activité primordiale dans plusieurs secteurs et plusieurs applications quotidiennes, dont cela, la sécurité informatique contre les attaques et les fraudes doit être obligatoire.Pour les systèmes d'information, les techniques génériques ou classiques pour l'identification traditionnelles sont basées sur deux méthodes : La première est basée sur ce que l'on sait (code PIN,mot de passe, etc.). La seconde est basée sur ce que l'on possède (badge, carte à puce, etc.). Bien que les méthodes classiques souffrent de plusieurs problèmes par exemple l'utilisateur peut perdre ou égarer son mot de passe ou celui-ci peut être deviné par quelqu'un d'autre. , le badge (ou la carte d'identité ou la clé) peut être volé ou perdu. Une autre méthode d'identification a été créée afin de surmonter cette limitation ou cette déficience, à savoir ce que l'on est ou ce que l'on sait faire (empreinte digitale, dynamique du clavier, etc.). La biométrie est le terme utilisé pour décrire cette dernière.

La biométrie est devenue l'une des technologies les plus pertinentes utilisées pour la sécurité des systèmes d'informations, . En revanche, les performances, l'universalité d'utilisation et la détection des fraudes sont les limitations majeures des systèmes biométriques uni-modaux qui utilise un seul trait, ce qui a donné naissance aux système multi-biométrie qui consiste à utiliser plusieurs données biométriques au sein de meme système pour améliorer les performances de l'authentification.

En effet même les systèmes multi biométriques souffrent de vulnérabilités .Pour cela les spécialistes de protection des informations doivent garantir que la disposition des systèmes multi biométriques est épuisée de telle manière que l'accès aux informations biométriques est limité aux personnes autorisées, sous certaines conditions, avec un contrôle explicite sur l'utilisation finale. De toute manière, plutôt que de se baser essentiellement sur des normes de grande précision, il serait préférable d'assurer la confidentialité lors de la conception du système multi biométrique, avant même son installation.

De nos jours, une nouvelle ligne d'enquête inexploitée a vu le jour, dont l'objectif est de coordonner l'assurance de sécurité de la vie privée en tant que contrainte du système multi biométrique. Il s'agit d'une adresse de recherche d'arrangements spécialisés (et non pas comme s'il s'agissait uniquement de dispositions juridiques), qui compléteraient l'innovation multi biométrique, afin d'assurer les données de référence. Quoi qu'il en soit, il a été constaté qu'en conservant la protection des données de la vie privée, les taux et les performances de la reconnaissance a eu tendance à détériorer complètement. Les objectifs de sécurité et de protection de la vie privée sont régulièrement en conflit et l'un des défis majeurs est d'assurer l'intégralité positive entre les deux.

Cette thèse vise principalement les objectifs suivants :

1. Examiner le problème de la sécurité des systèmes multi biométriques de façon à identifier et évaluer les menaces et les attaques possibles, en particulier celles liées aux méthodes de protection ;
2. Étudier et analyser l'état actuel de l'art actuel de la protection des modèles multi biométriques ;
3. Faire la comparaison entre les différents modèles de protection des données multi biométriques ;

4. Élaborer une nouvelle approche générique pour la protection des modèles multi biométriques dans le but d'améliorer la robustesse des systèmes multi biométriques contre d'éventuelles attaques, sans changer radicalement la structure du système à protéger ;
5. Évaluer la méthode proposée en se basant sur des protocoles de test efficaces et des bases de données largement disponibles pour la communauté de la recherche biométrique.

1.2 CONTRIBUTION

Cette thèse a pour principales contributions :

1. la réalisation d'une nouvelle approche basée sur la multi biométrie révocable, plus précisément la méthode du Biohashing, pour la protection des modèles multi biométriques (représentés sous forme de vecteurs) de reconnaissance d'empreintes digitales, laquelle répond aux critères de révocabilité, de diversité, de sécurité et de performance.
2. un descripteur biométrique de longueur fixe est exigé dans un grand nombre d'algorithmes de protection . Dans ce contexte, les attributs de texture de l'empreinte digitale sont utilisables. Dans un premier temps, nous analysons les différents descripteurs de texture récents tels que les filtres de Gabor ou l'analyse LBP (Local Binary Pattern) et déterminons le descripteur approprié en tenant compte de différentes contraintes telles que l'efficacité ou la taille du descripteur. Le filtre de Gabor 2-D a été choisies comme meilleur descripteur parmi ceux étudiés.Par la suite, nous soumettons un schéma révocable des empreintes digitales basé sur ce descripteur.
3. Étant donné, l'absence d'une méthode unifiée d'évaluation des algorithmes de protection. Nous observons un cadre d'évaluation commun, composé d'un ensemble de mesures pour évaluer la sécurité et la préservation de la vie privée dans les systémes multi biométriques révocables, Cette structure nous permet de faire l'évaluation de notre travail.

1.3 ORGANISATION DE LA THÈSE

Ce manuscrit de thèse est organisé selon les cinq chapitres suivants :

— Le chapitre 2 étant l'état de l'art sur les systémes biométriques mono modale , multi modaux.L'accent sera mis sur une présentation de la biométrie et la multi modalitée en se basant sur les niveaux de fusion ainsi que l'architecture des systémes biométriques correspondants à chaque niveau, une représentation des différents modalités ,les applications et les bases de données de cette derniére.
— Le chapitre 3 présente une étude de l'état de l'art des travaux sur la protection des systémes de sécurité multi biométriques en mettant l'accent sur la biométrie révocable (le Biohashing). Cet état de l'art présente un survol sur les principales méthodes utilisées pour résoudre le probléme de la vulnérabilité des systémes multi biométriques. Cette étude souligne les limites et les avantages de différentes techniques proposées et cela pour motiver notre choix .

— Le chapitre 4 met en relief la méthode d'évaluation proposée pour les méthodes de protection multi biométriques. Un ensemble de métriques sous forme des attaques est proposé pour analyser les approches par transformation révocable (le Biohashing).
— Le chapitre 5 aborde notre approche révocable des empreintes digitales qui serai utilisée ultérieurement dans notre expérimentation.
— Le chapitre 6 présente les méthodologies d'évaluation spécifiques aux modéles de protection des données multi biométriques dans le but d'évaluer l'approche proposée pour la sécurité des systémes multi biométriques.
— Une conclusion générale résume les principaux résultats obtenus dans cette recherche et une liste des différentes perspectives et les travaux futurs de cette thèse.

Généralités sur La biométrie 2

Sommaire

2.1 Introduction

Pour les systèmes d'information, les techniques conventionnelles ou classiques de maintien de la sécurité ne sont plus suffisantes, car n'importe qui peut les utiliser. Il existe deux approches pour assurer cette sécurité : La première est basée sur ce que vous avez déjà appris sur le sujet (PIN, mot de passe, etc.). La seconde dépend des ressources que vous possédez déjà (badge, carte à puce, etc.). Dans le premier scénario, l'utilisateur peut perdre ou égarer son mot de passe ou celui-ci peut être deviné par quelqu'un d'autre. Dans le second scénario, le badge (ou la carte d'identité ou la clé) peut être volé ou perdu. Une autre méthode de sécurité a été créée afin de surmonter cette limitation ou cette déficience, à savoir ce que l'on est ou ce que l'on sait accomplir (empreinte digitale, dynamique du clavier, etc.). La biométrie est le terme utilisé pour décrire cette dernière. Grâce à la biométrie, nous pouvons confirmer ou établir l'identification d'une personne sur la base de ses caractéristiques biologiques, comportementales ou physiques.[El-Abed 2011].

2.2 Les caractéristiques biométriques

Les caractéristiques biométriques sont des aspects des données biométriques d'une personne qui peuvent être utilisés pour vérifier l'identification de cette personne.

La Figure 2.1 est une illustration d'une modalité de mesure biométrique. Pour classer ces modalités, il faut s'intéresser aux données de l'individu, qui peuvent être réparties en trois catégories : biologiques, comportementales et morphologiques.

Il est possible d'utiliser la biométrie biologique pour identifier un individu spécifique (salive, ADN, etc.). Le comportement d'une personne peut être étudié à l'aide de la biométrie comportementale (style de marche, dynamique de frappe, etc.).

La biométrie morphologique est basée sur les caractéristiques physiques permanentes et distinctes d'une personne (empreinte digitale, visage, etc.). Dès lors qu'il répond aux critères suivants, un trait morphologique ou comportemental peut être utilisé comme caractéristique biométrique :

- Universalité : elle doit être présente chez tous les individus dont l'identité est recherchée ;
- Unicité : des informations différentes selon les personnes sont nécessaires pour garantir l'unicité ;
- Permanence : les informations recueillies doivent être disponibles pour une personne tout au long de sa vie ;
- Collectabilité : Afin de pouvoir effectuer des comparaisons, les données doivent être collectées et quantifiables ;
- Acceptabilité : le systéme doit respecter certains critéres (facilite d'acquisition , rapidité , etc.) afin d'etre employé.

Ces qualités ne sont pas présentes dans toutes les caractéristiques biométriques, ou elles ne le sont qu'à des degrés divers dans certaines d'entre elles. Le tableau 2.1 compare les principales modalités biométriques en fonction de l'universalité, de l'unicité, de la permanence, de la possibilité de collecte, de l'acceptabilité et de la performance, telles qu'elles sont extraites de [Jain *et al.* 1997]. Ce graphique montre qu'aucun attribut n'est parfait et qu'ils peuvent être mieux adaptés à certaines tâches. Lorsqu'il s'agit de confirmer ou d'identifier une personne, l'analyse de l'ADN est l'une des méthodes les plus efficaces.[Kumar *et al.* 2003].

Il ne peut cependant pas être utilisé pour le contrôle d'accès logique ou physique, en raison des contraintes de temps de calcul et aussi parce que personne ne veut soumettre un minuscule échantillon de sang pour vérification. Il est donc nécessaire de choisir entre l'existence et l'absence de certaines caractéristiques lors de la sélection du type de mode, afin de répondre aux exigences spécifiques de chaque application. Il est crucial de se rappeler que la modalité biométrique choisie dépend de la culture locale des personnes qui l'utilisent.

Les méthodes sans contact sont plus fréquemment utilisées et approuvées dans les pays asiatiques que les méthodes nécessitant un contact physique, comme les empreintes digitales, pour des raisons de propreté.

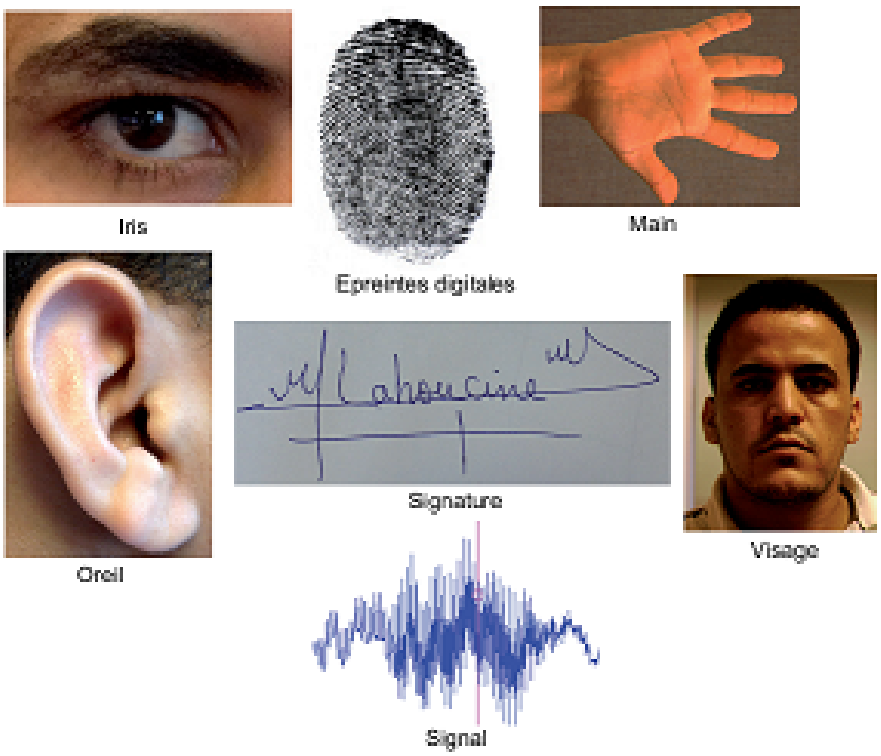


FIGURE 2.1 – *les caractéristiques biométriques*

Information	U	N	P	C	A	E
ADN	Oui	Oui	Oui	Faible	Faible	*****
Sang	Oui	Non	Oui	Faible	Non	*
démarache	Oui	Non	Faible	Oui	Oui	***
Dynamique de frappe	Oui	Oui	Faible	Oui	Oui	****
Voix	Oui	Oui	Faible	Oui	Oui	****
Iris	Oui	Oui	Oui	Oui	Faible	*****
Rétine	Oui	Oui	Oui	Oui	Faible	*****
Visage	Oui	Non	Faible	Oui	Oui	****
Géométrie de la main	Oui	Non	Oui	Oui	Oui	****
Oreille	Oui	Oui	Oui	Oui	Oui	*****
Empreinte digitale	Oui	Oui	Oui	Oui	Moyenne	****

TABLE 2.1 – *Comparaison des modalités biométriques selon les propriétés suivantes : (U) Universalité, (N) Unicité, (P) Permanence, (C) Collectabilité, (A) Acceptabilité et (E) Performance. Pour la performance, le nombre d'étoiles est relié à la valeur du taux d'égale erreur (EER) obtenue dans l'état de l'art .*

2.2.1 Les modèles biométriques

L'ensemble des données utilisées pour décrire une personne est appelé modèle biométrique (parfois appelé gabarit dans ce contexte). Il est important de savoir que les caractéristiques biométriques collectées ne sont enregistrées nulle part et sont utilisées telles quelles. Une phase de traitement est utilisée pour minimiser les données biométriques brutes et produire le modèle biométrique. La Figure 2.1 illustre certains des modèles biométriques dont nous avons parlé jusqu'à présent. En ce qui concerne l'endroit où ces modèles sont stockés, il existe quatre options principales : une clé USB, une base de données centralisée, un ordinateur de bureau et un capteur biométrique. Chacune de ces options présente des avantages et des inconvénients. En ce qui concerne la vitesse de traitement, la confidentialité et le respect de la vie privée, chaque emplacement présente ses propres avantages et inconvénients. Par exemple, la Commission Nationale Informatique et Libertés en France interdit l'utilisation généralisée d'une base de données centralisée (CNIL).

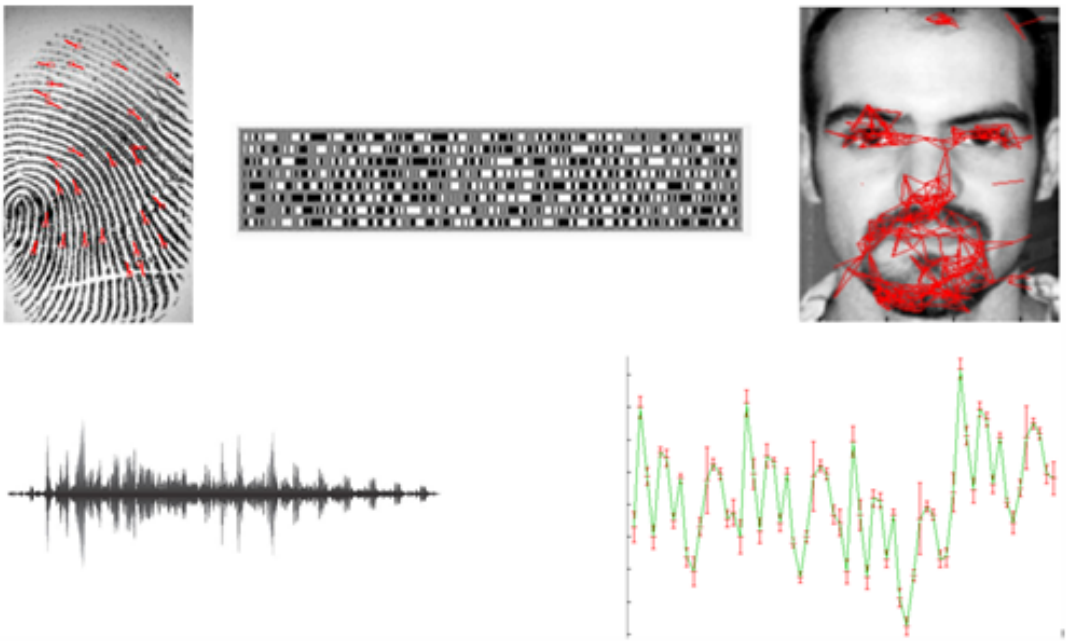


FIGURE 2.2 – *Voici quelques illustrations de modèles biométriques en usage. Les minuties d'une empreinte digitale, le code de l'iris, un graphique facial réalisé à partir de zones d'intérêt, un signal vocal et la dynamique de la frappe au clavier sont présentés de gauche à droite et de haut en bas.*

2.2.2 Utilisation de la biométrie

Le domaine de la biométrie se développe à un rythme jamais vu auparavant. il est clair que cette industrie a connu une croissance rapide au cours des dernières années. Certaines statistiques et certains chiffres sur sa progression dans le temps, à l'échelle mondiale, américaine, européenne ou française peuvent être pris en considération..

Peu de fournisseurs peuvent prétendre offrir une gamme complète de produits dans le secteur de la sécurité informatique, qui est encore fragmenté. Selon les experts du secteur, ce marché est en expansion et se consolide.

Comme le prévoit le Yole Development Research Institute dans son étude intitulée Sensors for Biometry and Recognition 2016, les principales technologies d'empreintes digitales s'orienteront de plus en plus vers des solutions multimodales. En conséquence, l'un des résultats les plus notables est que le secteur des applications pour smartphones représente près de 66 % du marché mondial de la biométrie.

EN 2019, le secteur mondial de la biométrie est généré un chiffre d'affaires de 11 milliards de dollars. Lorsqu'il s'agit de nations émergentes, où les actes d'état civil sont peu nombreux ou inexistants, cette croissance se distingue.

Les parts de marché par technologie :

Les empreintes digitales continuent à être la principale technologie biométrique en terme de part de marché, près de 50% du chiffre d'affaires total (hors applications judiciaires). La reconnaissance du visage, avec 12% du marché (hors applications judiciaires), dépasse la reconnaissance de la main, qui avait avant la deuxième place en termes de source de revenus après les empreintes digitales http://www.biometrie-online.net/biometrie/le-marche.

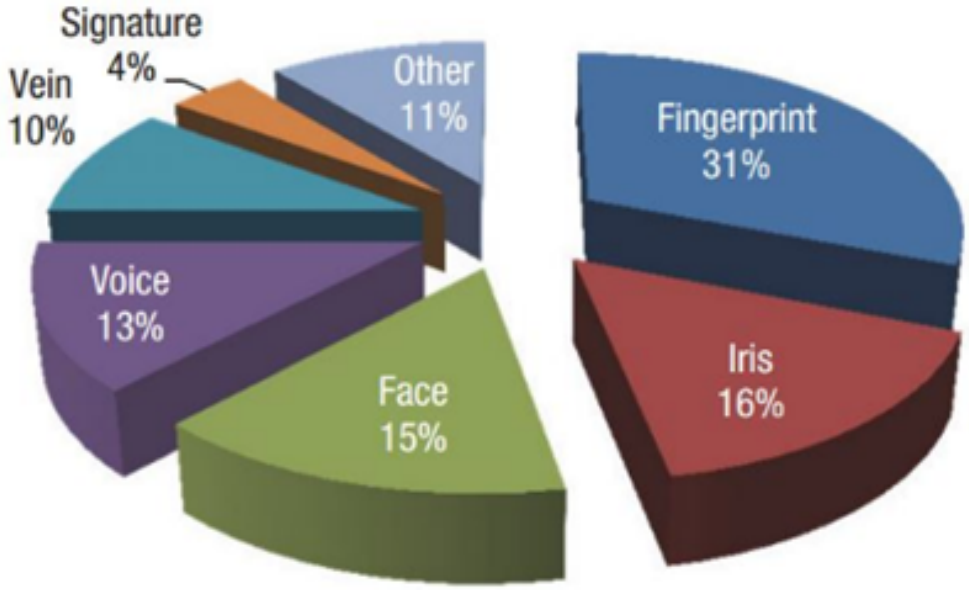


FIGURE 2.3 – *Parts de marché des techniques biométriques en 2019*

2.3 TECHNOLOGIE BIOMÉTRIQUE

Un système biométrique utilise les données biométriques uniques d'une personne pour créer un système de reconnaissance des formes. Un système biométrique peut fonctionner en mode inscription(enrôlement), vérification ou identification selon l'environnement de l'application. [Ababsa 2008].

— **Inscription**
Tout système biométrique commence par l'enrôlement. Pour acquérir des informations biométriques sur les personnes qui seront identifiées, le mode d'enrôlement sert de phase d'apprentissage. Plusieurs campagnes de collecte de données peuvent être réalisées afin de vérifier que le système de reconnaissance résiste aux changements de données dans le temps. Dans le cadre de ce processus, un capteur biométrique capture les caractéristiques biométriques uniques d'un individu, qui sont ensuite converties en signatures numériques par une technique d'extraction et enregistrées dans une base de données ou sur un élément personnel propre à l'individu ;

— **Vérification ou authentification**
Une comparaison "1 pour 1" est utilisée dans le mode de vérification ou d'authentification, dans lequel le système confirme l'identification d'une personne en comparant les données biométriques recueillies avec le modèle biométrique stocké pour cette personne. Le système doit alors répondre à la requête suivante lorsqu'il est dans ce mode : "Est-il vrai que je suis celui que je dis être ?". Un numéro d'identification personnel (PIN), un nom d'utilisateur ou une carte à puce sont désormais utilisés pour la vérification ;

— **Identification**
Une comparaison "1 à N" est utilisée pour l'identification, le système comparant une personne à un modèle dans la base de données pour l'identifier. Il y a une chance que la personne ne soit pas dans le système. Dans cette méthode, une identité est liée à un individu spécifique. En d'autres termes, elle

apporte des solutions à des questions telles que "Que suis-je exactement ? [Ababsa 2008].

2.3.1 Architecture de conception d'un système biométrique

La Figure 2.4 décrit l'architecture d'un système biométrique, qui se compose de cinq éléments :

- le **module de capture** a pour mission de recueillir les données biométriques d'un individu (il peut s'agir d'une caméra, d'un lecteur d'empreintes digitales, d'une caméra de sécurité, etc,),
- le **module d'extraction de caractéristiques** Ce module recueille les informations essentielles des données biométriques capturées avant d'en former une nouvelle représentation, en utilisant cette nouvelle représentation comme entrée. Cette nouvelle représentation devrait, en théorie, être unique pour chaque personne et raisonnablement insensible aux changements au sein d'une même classe,
- le **module de correspondance** Lorsqu'une collection de caractéristiques extraites est comparée à un modèle de système existant, cela indique à quel point elles sont similaires (ou différentes),
- le **module de décision** Décider de vérifier ou non l'identification revendiquée par un utilisateur ou de s'assurer de l'identité d'une personne en comparant les caractéristiques extraites à un ou plusieurs modèles précédemment stockés[Morizet 2009].

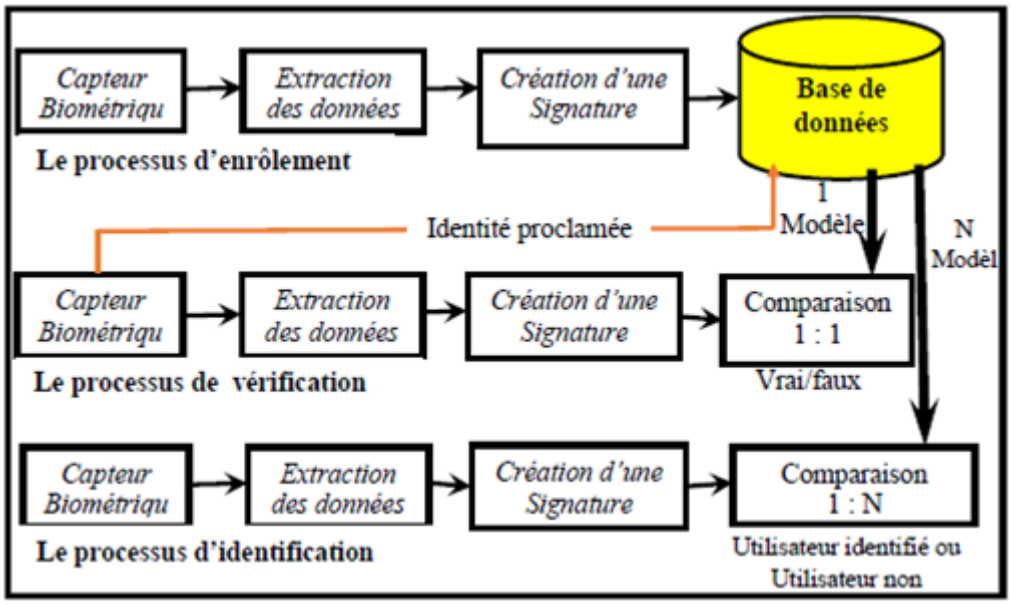


FIGURE 2.4 – *Les différents modes de systèmes biométriques et leurs principaux composants.*

2.4 LES MODALITÉS BIOMÉTRIQUES

Cette section traite de plusieurs modalités biométriques basées sur une analyse biologique, comportementale ou morphologique. Pour de nombreuses raisons, nous limitons le nombre de modalités biométriques que nous considérons. Tout d'abord, les technologies biométriques telles que l'identification par le visage et les

empreintes digitales sont assez couramment utilisées de nos jours. Les modalités biométriques qui, jusqu'à présent, ont le mieux répondu à nos tests d'unicité de permanence et de régularité sont celles qui peuvent être capturées par un équipement de façon ergonomique et rentable .

2.4.1 Biologique

L'odeur corporelle, le rythme cardiaque et l'analyse de l'ADN ne sont que quelques-uns des éléments qui entrent dans ce vaste domaine. Cette forme de biométrie n'est pas traitée en profondeur car elle est peu courante, moins permanente que les autres et plus difficile à afficher et à enregistrer de manière cohérente.

2.4.2 Comportementale

L'examen des actions d'un individu, telles que la dynamique de sa signature, sa démarche, sa frappe au clavier et sa voix, constitue la base de ce type d'analyse. Nous vous montrerons quelques exemples de cette modalité dans les sections qui suivent.

Signature dynamique

Différents facteurs sont inclus dans une analyse comportementale (mesure de la vitesse, ordre d'écriture, pression exercée, accélération...). sont évalués pendant de la signature. Il est réalisable de faire de la falsification par le biais d'une phase expérimentale, dont la signature peut se dégrader sous le stress de l'utilisateur.

FIGURE 2.5 – *Capture d'une signature.*

La voix

Une des caractéristiques biométriques intéressantes est celle de la voix de la personne, car elle dépend de la structure anatomique de chaque personne ainsi que de la langue maternelle. Pour la capture de la voix, il est possible d'utiliser un microphone, mais le bruit ambiant peut altérer la qualité de la voix.

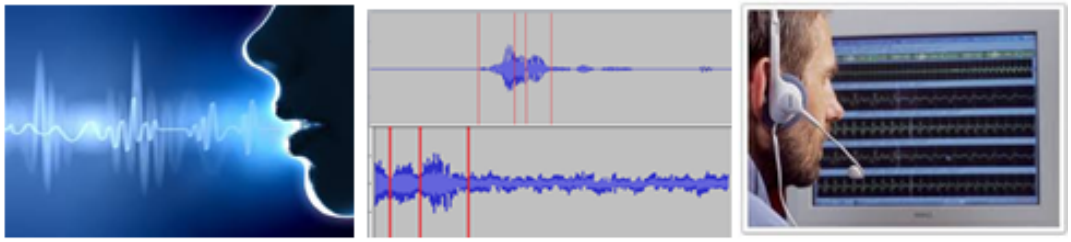


FIGURE 2.6 – *Spectre d'un signal voix*

La dynamique de frappe

Comme chaque ordinateur est équipé d'un clavier, un système basé sur la mécanique du clavier ne nécessite pas l'achat d'un équipement supplémentaire. Lorsqu'un doigt est placé sur une touche, ce programme mesure le temps qu'il reste en l'air (entre deux frappes). Un millier de fois par seconde est à peu près correct. Cette séquence d'entrée de type mot de passe est prédéfinie. Pour commencer, le mot de passe doit être saisi de nombreuses fois jusqu'à ce qu'un modèle se forme dans l'esprit de l'utilisateur. Par conséquent, ce gadget biométrique est utilisé pour l'authentification du commerce électronique et la vérification de l'accès aux bases de données.

2.4.3 Morphologique

Cette catégorie porte sur les traits physiques distinctifs d'une personne, tels que la couleur des yeux ou le type de cheveux, les visages 2D et 3D, les empreintes digitales, la géométrie de la main et les iris. Nous examinerons quelques exemples concrets de modalités morphologiques dans les sections qui suivent.

Forme de la main

Les mains ont une forme unique pour chaque personne. Un scanner spécialisé peut être utilisé pour l'obtenir. La longueur, l'épaisseur et la position relative des doigts de l'image ont toutes été récupérées et comparées à des valeurs stockées dans une base de données pour arriver à cette conclusion. Toutefois, à mesure que les gens vieillissent, leur biométrie peut changer. Les systèmes biométriques en forme de main sont faciles à déployer et bien tolérés par les utilisateurs finaux.

FIGURE 2.7 – *Dispositif de reconnaissance par géométrie de la main*

L'iris

La première exploration du modèle d'iris date d'un manuel d'ophtalmologie rédigé par James Hamilton Doggarts en 1949. Selon les estimations de Daugmann, la possibilité de trouver deux iris suffisamment identiques pour être confondus est de $1/10^{72}$.

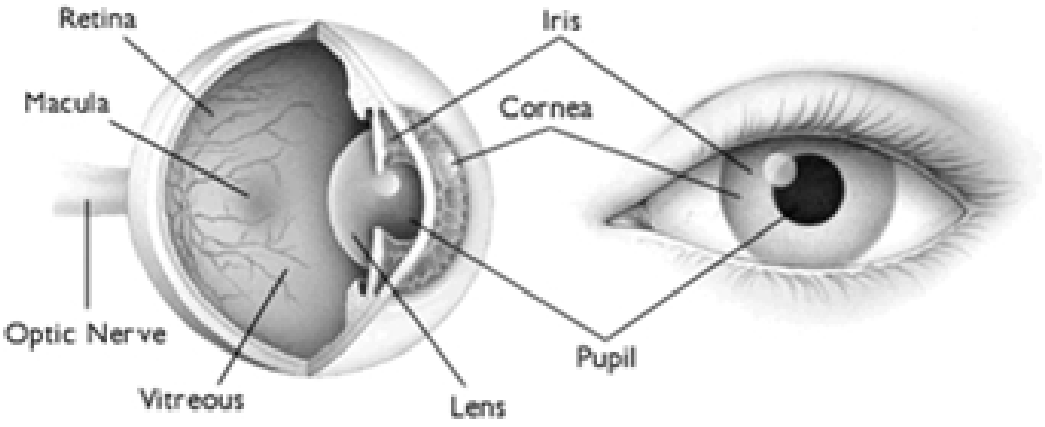


FIGURE 2.8 – *Vue détaillée de l'oeil humain*

Chaque oeil est unique et il est possible de compter plus de 200 paramètres indépendants dans l'iris de l'oeil . Déjà en 1980, les ophtalmologistes ont noté que si la couleur de l'iris peut différer au fil du temps, le motif (voir Figure 2.9) demeure inchangé.

FIGURE 2.9 – *Motif de l'iris*

Dans un premier temps, il faut capturer l'image de l'iris. Il faut savoir que l'œil est un organe très sensible qui peut changer de taille et d'acuité en fonction de la quantité de lumière et de la fatigue qu'il reçoit. Le fait que les cils, les paupières et les lentilles puissent tous refléter la lumière ou bouger de manière incontrôlée pour la cacher complique encore les choses. Une caméra CCD monochrome sert de point de collecte des données du système (640 x 480) avec une longueur d'onde de source lumineuse comprise entre sept cent et neuf cents nanomètres, qui est imperceptible pour l'homme.

Ainsi, pour la capture, il faut prendre la photo, le plus souvent par infrarouge pour prévenir la dilatation de la pupille. Par la suite, l'image est nivelée, et après un traitement mathématique (ondelettes de Gabor), nous obtenons un code qui peut être inséré dans une base de données. Ce processus est représenté à la figure 2.10.

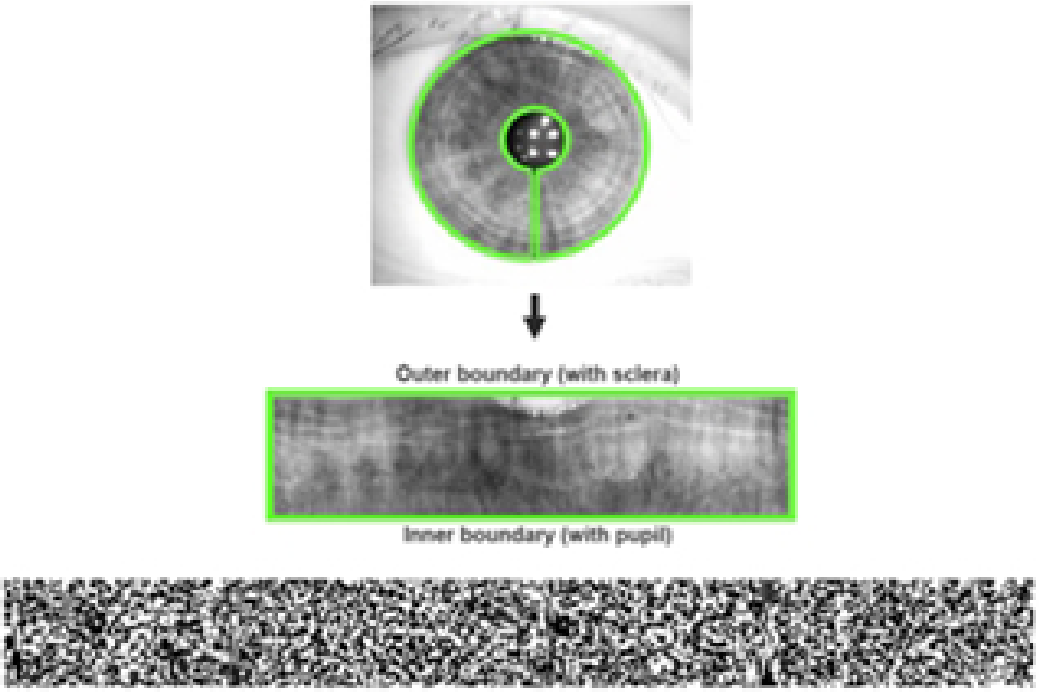


FIGURE 2.10 – *Processus d'enregistrement de l'iris*

Les empreintes digitales

Cette technique d'identification est la plus ancienne, remontant au début du 20ème siècle. Les origines de cette technique remontent au chercheur britannique Sir Francis Galton, qui a découvert la permanence, l'individualité et l'inaltérabilité d'un dessin de la conception à la mort.

En dehors de cela, l'empreinte digitale de chaque personne a son propre motif formé par un ensemble de lignes parallèles locales. Lorsque vous touchez quelque chose, vous sentez les stries (ou crêtes, qui sont les lignes qui entrent en contact avec la surface) (creux entre deux stries). Les stries sont ponctuées d'une série de pores répartis uniformément sur toute leur longueur. Chaque empreinte présente un ensemble de points globaux (centres et deltas) et locaux (points) que l'on peut considérer comme des minuties. Les centres correspondent aux points de convergence des stries, tandis que les deltas appartiennent aux points de divergence. Un capteur d'un type quelconque, tel qu'un capteur optique, thermique, capacitif ou ultrasonique, recueille les données.

FIGURE 2.11 – *Type de minuties*

La technique d'extraction des empreintes porte le nom d'EDR : Empreinte Digitale Réduite. Le processus est illustré par la figure 2.12.

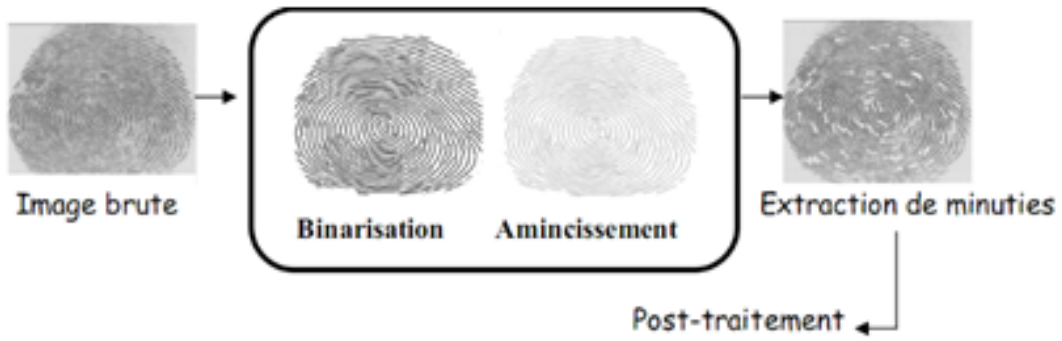


FIGURE 2.12 – *Processus de détection des minuties*

Le visage

La conception de systèmes biométriques basés sur la reconnaissance de la forme du visage représente l'un des plus récents. Dans les années 1982, deux chercheurs, Hay et Young, déclarent que les humains, pour identifier un visage, exploitent ses spécificités globales et locales.

Des travaux de recherche plus approfondis ont été entrepris afin de déterminer la capacité de reproduction électronique de cette fonction de reconnaissance.

Le MIT a développé un système de reconnaissance faciale appelé EIGENFACE sur des études qu'ont été menées en 1989 par le neurobiologiste TeuvoKohonen de l'Université d'Helsinki et par des chercheurs de l'Université Brown de Rhode Island à la fin des années 1980, Kirby et Sirovich (1989).

La photo du visage est prise par une caméra. Ainsi, il est possible que le sujet

puisse librement choisir de se présenter devant l'appareil photo ou que son image puisse être prise à son insu pour révéler certaines caractéristiques.

Selon le gadget, l'utilisateur doit se tenir directement en face de l'appareil ou se trouver à une certaine distance de celui-ci. Les données biométriques obtenues sont ensuite comparées au fichier de référence.

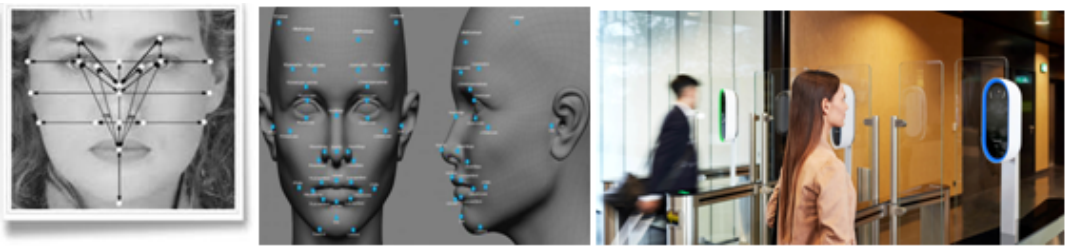


FIGURE 2.13 – *Capture de l'image d'un visage*

Empreintes des articulations des doigts (FKP)

À l'aide d'images à faible résolution, cette technologie biométrique peut extraire des caractéristiques distinctives telles que les lignes et les crêtes primaires et secondaires de la surface arrière du doigt. Chaque doigt de la main possède un ensemble de caractéristiques qui lui est propre. L'enregistrement des informations pour chacun d'entre eux est donc nécessaire pour une reconnaissance précise dans la zone d'identification [Lina 2016] .

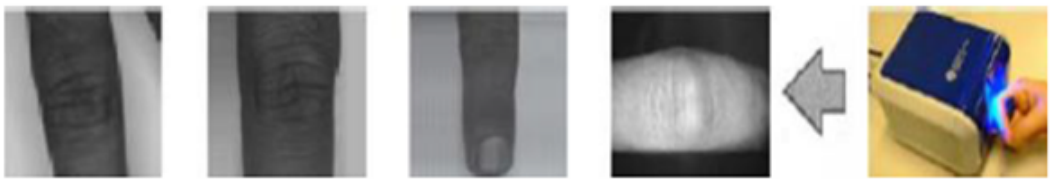


FIGURE 2.14 – *Empreinte des articulations des doigts*

2.5 Les Normes biométriques

Grâce aux normes biométriques, les systèmes et applications biométriques de différents fabricants seront compatibles et les données biométriques pourront être échangées. Les gouvernements et les organismes d'application de la loi ont commencé à élaborer des normes biométriques pour l'échange de données d'empreintes digitales dans les années 1980, mais ce n'est qu'en 2002 que les choses ont vraiment commencé à avancer. Un certain nombre d'organisations, tant nationales qu'internationales, travaillent actuellement à la création de ces directives. Un certain nombre d'organisations de normalisation ont proposé le développement d'une API (interface de programme d'application) pour les systèmes biométriques afin d'améliorer la compatibilité entre un large éventail de technologies biométriques et de faciliter la communication entre les implémentations. Le Consortium BioAPI est l'une de ces organisations. L'Organisation de l'aviation civile internationale (OACI) et l'Organisation internationale du travail (OIT) élaborent des normes dans leurs domaines respectifs qui n'ont peut-être pas été abordées par d'autres organisations, tandis que les principaux groupes industriels élaborent des normes pour soutenir les objectifs de leurs membres. L'OACI, par exemple, est chargée de normaliser les documents de voyage lisibles à la machine comme les passeports électroniques,

tandis que l'Organisation internationale du travail a créé des règles pour les documents d'identification biométriques des marins. Depuis la création du sous-comité 37 sur la biométrie en juin 2002, le comité technique mixte ISO/CEI a créé plus de 30 normes internationales relatives à la biométrie. Outre le sous-comité 27 sur les approches de la sécurité informatique (qui traite de la protection des modèles, de la sécurité algorithmique et de l'évaluation de la sécurité) et le sous-comité 17 sur les cartes d'identité et l'identification, le JTC travaille également sur des normes biométriques dans ces comités. Après que l'UIT-T a commencé à travailler sur les normes biométriques en 2001, la Commission d'étude 17 a été formée pour coordonner tous les efforts des organisations. L'identification des personnes et la protection de la vie privée sont des responsabilités de la Commission d'études 17 de l'UIT-T, un sous-comité de l'UIT-T consacré à la gestion de l'identité. En raison du besoin actuel d'infrastructures, de services et d'applications de réseau plus sécurisés, le rythme de travail augmente. Les terminaux mobiles et les services Internet dans les télécommunications nécessitent des techniques d'authentification à la fois sûres et faciles à utiliser.

2.6 La biométrie a plusieurs usages.

Les services de sécurité, les bureaux gouvernementaux, les parlements, les bases militaires et autres lieux de haute sécurité utilisent l'authentification biométrique pour s'assurer que seules les personnes autorisées y ont accès. En ce qui concerne la reconnaissance, les forces de l'ordre et les fonctionnaires de l'immigration l'utilisent fréquemment dans les aéroports, ainsi que pour la recherche dans les bases de données criminelles. En outre, elle est de plus en plus répandue dans les applications civiles, telles que la vérification des cartes de crédit, des permis de conduire et des passeports.

Des efforts croissants sont déployés par tous les fournisseurs de produits et de services pour se protéger contre toutes les incursions frauduleuses imaginables, à mesure que l'internet et les services basés sur le web gagnent en popularité et qu'une variété de services sont développés en ligne, notamment le commerce électronique (E-commerce).

Il existe trois grandes catégories d'applications biométriques [Ababsa 2008] :

— **Applications commerciales :** Les utilisations commerciales comprennent la mise en place de réseaux informatiques, la sécurisation des données électroniques, la conduite des affaires via Internet, l'utilisation de cartes de crédit, le contrôle de l'accès physique et l'utilisation de téléphones cellulaires.

— **Applications gouvernementales :** Les applications des administrations fédérales, étatiques et locales , par exemple, une carte d'identité nationale ou un permis de conduire.

— **Applications légales :** Utilisations dans le système juridique ,anthropologie médico-légale, enquêtes criminelles, identification des terroristes, etc.

2.7 Les limitations des systèmes biométriques monomodaux

Grâce à la biométrie, il est possible d'établir un lien plus sûr entre un individu et son identité. Cependant, malgré leurs nombreux avantages, les systèmes biométriques ne sont pas actuellement utilisés dans toutes les applications typiques en raison de leurs contraintes inhérentes. L'inconvénient le plus important est la

performance globale du système. Si les badges, les cartes, les clés et les mots de passe peuvent poser des problèmes de sécurité en raison de la possibilité de vol, de perte ou de falsification, ce qui romprait le lien avec une personne physique spécifique, ils sont efficaces à 100 % en matière d'identification. Tant que la clé ou le mot de passe est saisi correctement, le système répond par OUI ; sinon, il répond par NON, indiquant une correspondance à 100 %. Contrairement à la croyance populaire, les systèmes d'identification biométrique ne permettent pas ce niveau de reconnaissance parfaite, car ils utilisent plutôt ce qu'on appelle un "score de similarité", c'est-à-dire une valeur numérique comprise entre 0 et 1 qui représente le degré de similarité entre deux ensembles de données biométriques. Un seuil de décision doit être mis en place avant que le score de similarité puisse être utilisé. C'est pourquoi les systèmes biométriques sont dotés de modules de décision. Pour s'assurer que les échantillons proviennent de personnes différentes, le score doit être supérieur au seuil de décision. Si le score de similarité n'est pas supérieur ou inférieur à un certain niveau, les deux échantillons ne sont pas identiques et la personne est écartée (l'identité revendiquée n'a pas été vérifiée). Plusieurs facteurs contribuent à la grande diversité des données biométriques et à l'impossibilité de trouver une correspondance parfaite :

— Variabilité dans le processus de capture.
— La nature cyclique des données biométriques.
— Le manque de caractère distinctif de la biométrie.
— Les attaques

Variabilité dans le processus de capture : La variabilité du capteur, le bruit d'acquisition (par exemple, une empreinte digitale avec une cicatrice ou une voix altérée par le froid sont des exemples de données bruitées), et la déformation physique pendant la capture sont autant de causes de variabilité pendant la capture. Des erreurs lors de la numérisation peuvent également causer ces problèmes, comme l'utilisation d'un capteur endommagé ou mal entretenu. La biométrie elle-même n'a aucune incidence sur cette diversité ; elle est plutôt due à la numérisation de la biométrie elle-même.

La nature cyclique et la non-unicité : La variabilité interclasse (variabilité entre les modalités pour plusieurs personnes) et la variabilité intraclasse (variabilité à l'intérieur d'une modalité pour un individu) sont d'autres termes pour la variabilité temporelle et la non-unicité.[Allano 2009].

— **Les variations d'intra-classe :** Les données biométriques d'un individu acquises pendant l'authentification peuvent être très différentes des données qui ont étaient employées pour générer le modèle pendant l'inscription, cette variation est typiquement causée par un utilisateur qui agit incorrectement avec le capteur (voir figure 2.15) ou quand les caractéristiques du capteur sont modifiés pendant la phase de vérification.

FIGURE 2.15 – *Variation d'intra-classe associée avec l'image du visage d'un individu dû au changement de poses. Un système de reconnaissance du visage ne sera pas capable de comparer ces trois images avec succès, bien qu'ils appartiennent à la même personne*

— **La non-unicité :** Tandis qu'on s'attend a ce qu'un trait biométrique change de manière significative à travers les individus, il peut y avoir de grandes similitudes d'interclasse dans les ensembles des caractéristiques employés pour représenter ces traits. Cette limitation limite la distinction fournie par le trait biométrique. Ils ont prouvé, que le contenu de l'information (le nombre de modèles distinguables) dans deux représentations les plus généralement utilisées de la géométrie de la main et le visage est seulement de l'ordre 105 et de 103 respectivement [Adjoudj 2006] Ainsi chaque trait biométrique a une certaine limite théorique supérieure en terme de ses possibilités de distinction [Jourani 2012].

La **non-universalité de la biométrie** est une autre restriction à l'utilisation de la biométrie dans les applications d'authentification. Pour cette raison, certains groupes démographiques devront renoncer à utiliser les outils biométriques. Les empreintes digitales de certaines personnes, par exemple, ne contiennent pas suffisamment de données pour être utilisées comme outil d'identification. [1], dans un tableau. Seuls environ 2% des personnes sont incapables d'utiliser leurs empreintes digitales pour prouver leur identité d'après une étude publié par NIST (National Institute of Standards and Technology) footnoteNIST Biometric Accuracy, Tamper Resistance, and Interoperability Standards, 2002 .

Une capture biométrique peut devenir difficile en raison de facteurs environnementaux tout au long du processus. La reconnaissance vocale, par exemple, est inefficace dans un environnement bruyant, tout comme la reconnaissance faciale la nuit (si l'on utilise une caméra à lumière visible).

Les technologies biométriques présentent également l'inconvénient d'être vulnérables à la fraude **(Les attaques)**. Il est peut-être plus difficile de falsifier un iris, mais la reproduction de certaines caractéristiques biométriques est toujours possible, quelle que soit la difficulté de falsifier une carte ou de déchiffrer un mot de passe. S'il est facile d'imiter la voix ou de recréer la signature d'une personne, il est plus difficile de le faire avec son iris ou ses empreintes digitales, même si cela reste faisable. En fait, certaines recherches ont prouvé que le silicone peut dupliquer les empreintes digitales [Matsumoto *et al.* 2002].

Enfin, il existe des restrictions à l'utilisation de la biométrie pour des raisons culturelles ou d'usage. Depuis son utilisation par les autorités, la biométrie, en particulier les empreintes digitales, a une réputation négative. Elles sont souvent liées à la surveillance des personnes et à l'activité criminelle. De plus, les empreintes

1. NIST Biometric Accuracy, Tamper Resistance, and Interoperability Standards, 2002

digitales laissent des traces qui peuvent être récupérées et exploitées, ce qui en fait un choix moins populaire pour la plupart des gens. Un autre point à prendre en compte est que la CNIL(Commission Nationale de l'Informatique et des Libertés), l'autorité française de protection des données, n'autorise les applications qui utilisent des traces biométriques (comme les empreintes digitales) que si la sécurité est une priorité absolue (par exemple, VISA, passeports). Ces méthodes ne nécessitent pas de base de données, et les empreintes digitales ne peuvent donc pas être utilisées pour des applications moins sûres, comme le contrôle d'accès par carte pour les écoles ou les bâtiments. Par conséquent, lorsque les données biométriques sont enregistrées sur un support personnel plutôt que dans une base de données, il y a moins de risques qu'elles soient utilisées à mauvais escient au cas par cas. D'autres biométries sont entravées par leur complexité d'utilisation, comme l'iris, qui est une modalité très fiable mais qui est considérée comme invasive par certains en raison de la proximité de la méthode d'acquisition avec l'œil [Allano 2009].

Le **système biométrique multimodal** est une réponse à tous ces inconvénients : il utilise plusieurs modalités biométriques au sein d'un même système.

2.8 La multi modalité

L'utilisation de plusieurs systèmes biométriques est une approche de type multi-modalité. Le but du regroupement de différents systèmes consiste à réduire les limites mentionnées à la section 2.7, puisque le but premier de l'utilisation de plusieurs systèmes est d'améliorer les performances de reconnaissance. Par une meilleure quantité d'informations discriminantes de chaque personne, nous cherchons à accroître le pouvoir de reconnaissance du système. En outre, l'utilisation de multiples modalités biométriques réduit le risque d'incapacité à s'enregistrer et réduit la robustesse face à la fraude.

2.8.1 Les différents multi-possibles

En intégrant divers systèmes biométriques, les systèmes multimodaux pallient les limites des systèmes monomodaux. Il existe cinq types distincts de systèmes multimodaux en fonction des systèmes qu'ils intègrent (Figure 2.16). Ils portent les noms suivants :

- **Multi-capteurs :** Ce type de système utilise plusieurs capteurs pour acquérir le même caractère biométrique sous différents angles. Par exemple, l'acquisition d'une image 2d d'un visage se fait avec une caméra classique alors que la même acquisition 3D se fait avec une autre caméra plus sophistiquée. En particulier, ce type de système peut être utilisé lors de la fusion au niveau du capteur.
- **Multi-instances :** Ce type de système permet d'acquérir le même caractère biométrique sur plusieurs intervalles de temps. Nous visons ici à considérer la variation interpersonnelle de la modalité biométrique. Un exemple typique de ce type de système est l'acquisition de plusieurs empreintes digitales via le même capteur.
- **Multi-algorithmes :** En fait, c'est le type le plus classique. L'extraction des caractéristiques s'effectue au moyen de différents algorithmes avant l'étape de fusion. Par exemple, deux algorithmes peuvent être combinés pour traiter la même image d'empreinte digitale, l'un qui analyse la texture et l'autre

extrait les minuties. Le recours à un seul capteur est plus que suffisant dans ce cas.

— **Multi-échantillons :** Dans ce type de capture, plusieurs captures de la même modalité sont réalisées en utilisant le même dispositif d'acquisition afin d'enrichir le modèle biométrique d'une personne. Les exemples incluent l'acquisition du profil facial frontal d'une personne ainsi que des profils gauche et droit pour tenir compte des variations de la pose faciale.

— **Systèmes multicaractères ou multimodaux :** Ce type de système est une combinaison de différentes modalités biométriques d'un individu. Il apporte une amélioration significative de la performance du système. Différents capteurs et algorithmes dédiés sont nécessaires pour chaque modalité biométrique. L'une des principales caractéristiques de ce type de système est que les caractères biométriques considérés peuvent être plus dé corrélés que pour les systèmes multi-capteurs.par exemple le système de l'empreite digitale et le système de l'iris .

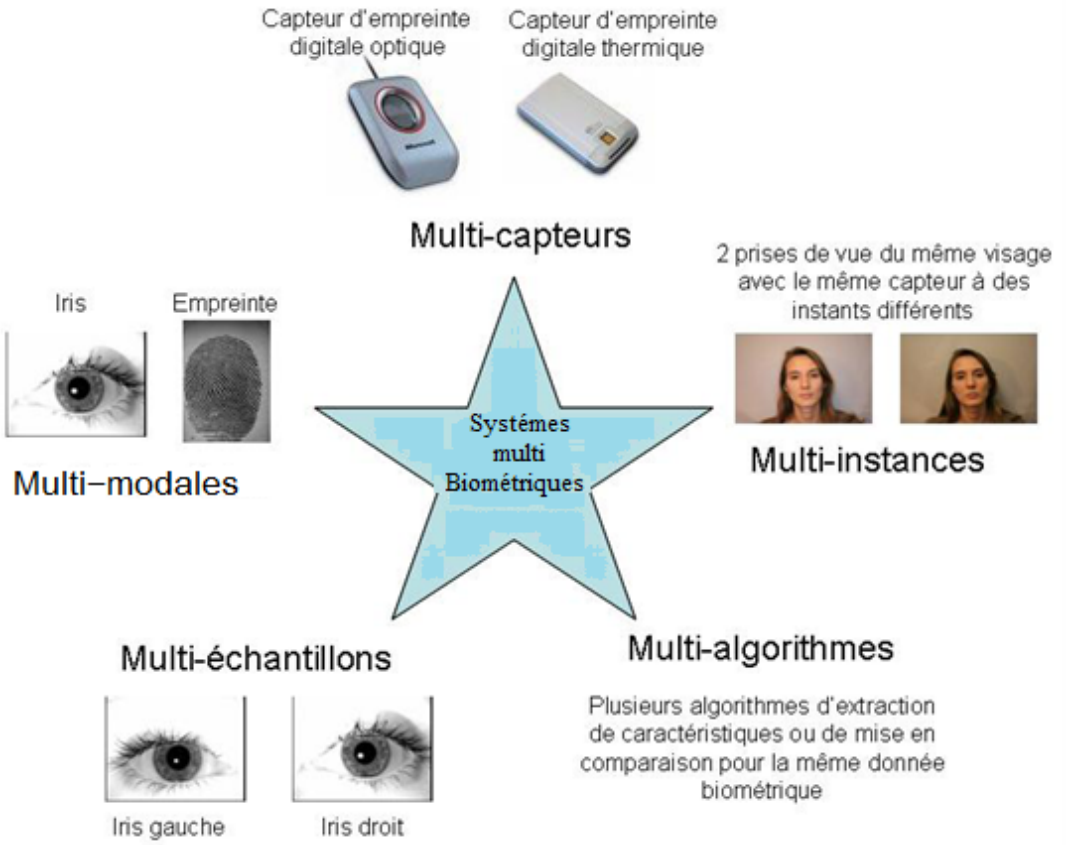


FIGURE 2.16 – *Les différents systèmes multi Biométriques*

2.8.2 Principes et méthodes de conception des architectures

Les systèmes multimodaux nécessitent une collecte et un traitement des données variés puisqu'ils intègrent plusieurs systèmes biométriques. L'architecture sérielle consiste à acquérir et à traiter les données de manière séquentielle, tandis que l'architecture parallèle consiste à le faire simultanément.

le traitement est l'aspect le plus important d'une architecture. En réalité, pour des raisons pratiques, les données biométriques sont souvent acquises de manière séquentielle. Cependant, il est difficile d'obtenir une image d'empreinte digitale et

d'iris dans des circonstances idéales. Certains capteurs, comme les capteurs d'empreintes digitales, permettent l'acquisition simultanée de plusieurs doigts, voire de l'empreinte de la paume, tandis que d'autres ne permettent l'acquisition que d'un seul doigt.

Par conséquent, le traitement et la prise de décision sont étroitement liés en termes d'architecture. Pour obtenir un score de similarité, vous pouvez utiliser soit un système multimodal série, soit un système multimodal parallèle.

Comme le montre la Figure 2.17, l'architecture la plus populaire(en parallèle) tire parti de toutes les informations disponibles pour augmenter les performances du système. Elle demande beaucoup de temps et d'équipement, et le fait de disposer d'un grand volume de données biométriques diminue son utilité. La conception en série (Figure 2.18) peut donc être souhaitable dans certaines applications, par exemple si la multimodalité est utilisée pour donner une option à ceux qui ne peuvent pas utiliser les empreintes digitales . Les empreintes digitales de la plupart des personnes sont collectées et analysées, mais une méthode basée sur l'iris est employée pour authentifier ceux qui ne peuvent pas être identifiés de cette manière.

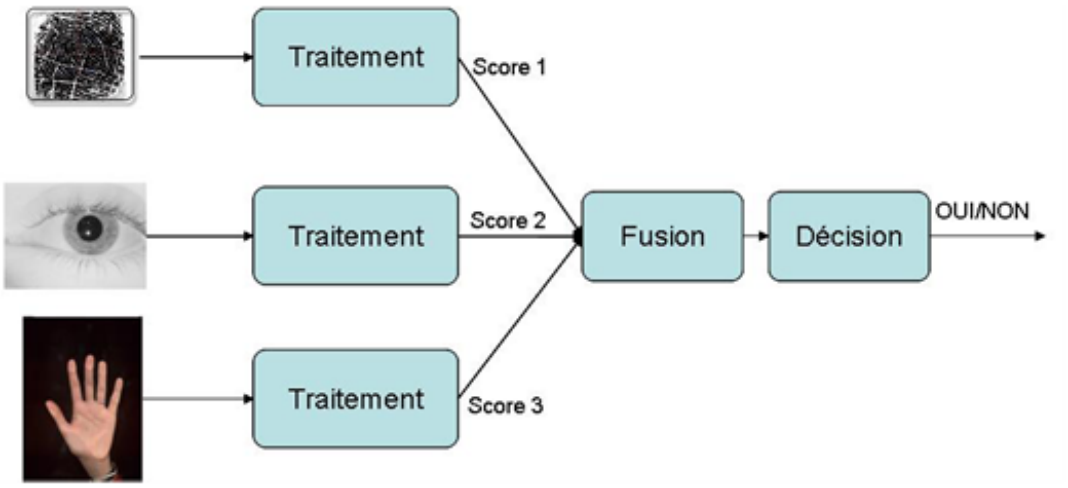


FIGURE 2.17 – *Architecture de fusion en paralléle*

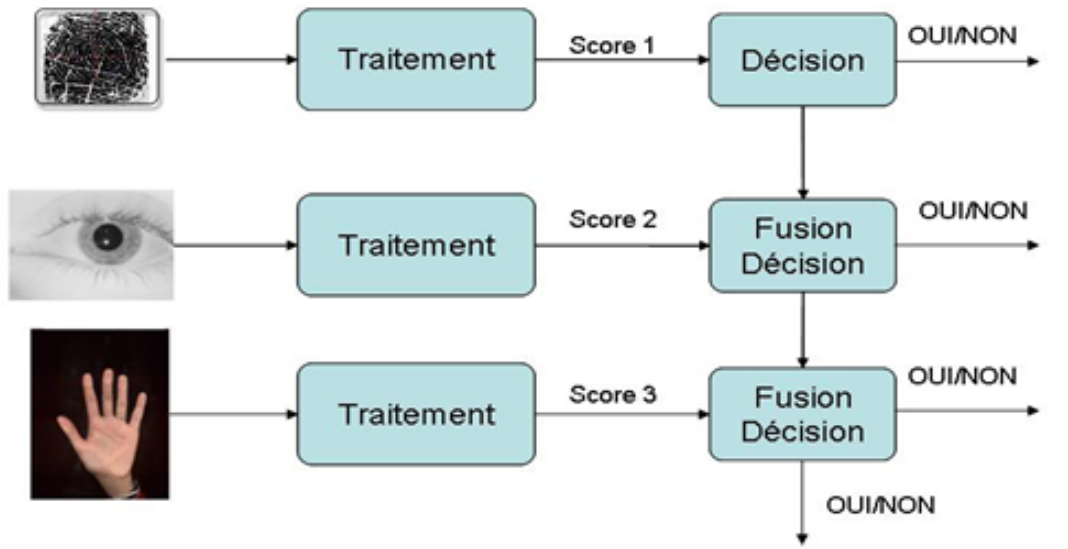


FIGURE 2.18 – *Architecture de fusion en série (incrémentale ou séquentielle)*

2.8.3 Les différents niveaux de fusion

Les données, les caractéristiques extraites, les scores des modules de comparaison ou les choix du module de décision peuvent tous être utilisés pour combiner plusieurs systèmes biométriques. [BENCHENNANE 2015] (voir figure 2.19).

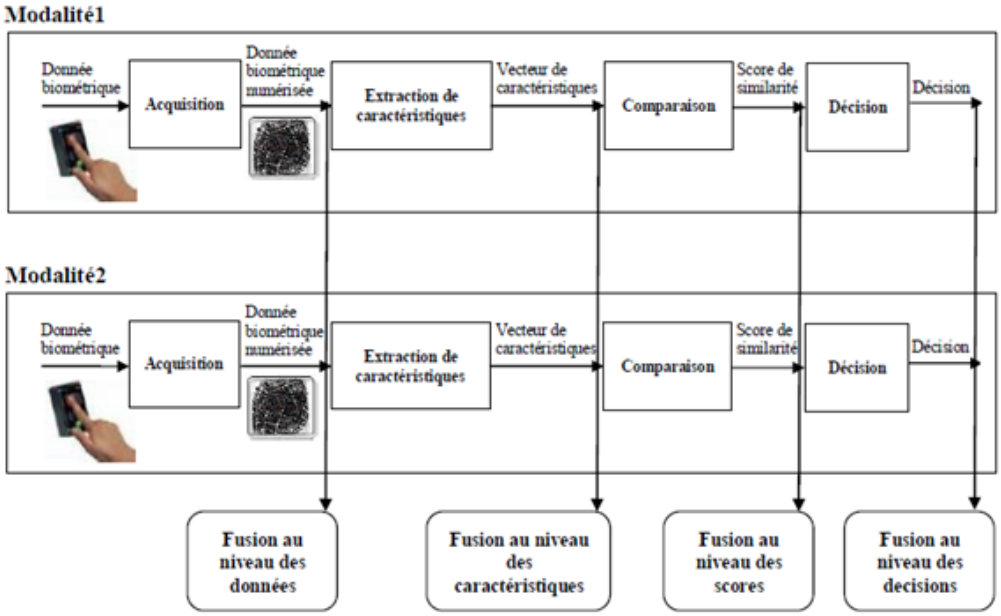


FIGURE 2.19 – *les différents niveaux de fusion*

Ces quatre niveaux de fusion peuvent être classés en deux grandes familles :
— La fusion pré-classification (avant la comparaison),
— La fusion post-classification (aprés la comparaison).

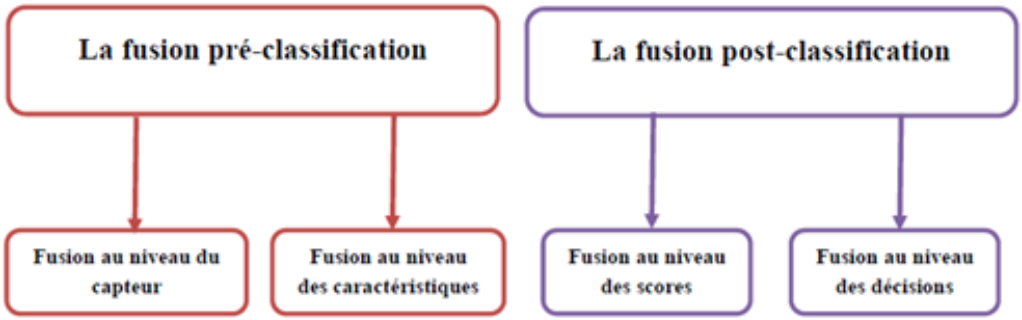


FIGURE 2.20 – *Les familles des niveaux de fusion*

1. **La fusion pré-classification**

   Fait référence à la combinaison de données provenant de plusieurs capteurs (images brutes) ou aux caractéristiques extraites par le module d'extraction de caractéristiques au niveau du capteur. L'homogénéité des données est requise pour ce type de fusion [Hafs 2016].

   Fusion au niveau du capteur (Sensor Level) :

   En combinant les données de fusion au niveau des capteurs, les données brutes des capteurs peuvent être analysées [Iyengar *et al.* 1995]. L'utilisation

de plusieurs capteurs appropriés pour combiner les données biométriques n'est possible que si les données capturées sont une seule instance de la même ligne biométrique, ou plusieurs instances de la même ligne biométrique. Il doit y avoir une compatibilité entre les captures, et les points de données brutes acquis doivent être connus à l'avance. Un modèle 3D du visage d'une personne peut être créé, par exemple, en combinant des photos de visages prises avec différents appareils photo. Si les instances de données ne sont pas compatibles, la fusion au niveau du capteur peut s'avérer impossible (par exemple, il peut être difficile de fusionner des images du visage provenant de caméras ayant des résolutions différentes).

Fusion au niveau des caractéristiques (Feature Level) :

Lorsque vous effectuez une fusion au niveau des caractéristiques, vous concaténerez des vecteurs de caractéristiques provenant de diverses sources, telles que des capteurs de la même ligne biométrique, des instances de la même ligne biométrique ou des unités de la même ligne biométrique.

Il est possible de calculer un vecteur de caractéristiques unique à partir de plusieurs vecteurs de caractéristiques homogènes (par exemple, de nombreuses photos d'empreintes digitales d'un utilisateur). Tant que les vecteurs de caractéristiques sont hétérogènes (par exemple : vecteurs de caractéristiques de l'iris et du visage), on peut les concaténer en un seul. Lorsque les ensembles de caractéristiques sont contradictoires, la concaténation est impossible. Par exemple, les minuties d'empreintes digitales et les coefficients de visage propres de l'ACP en sont des exemples. Certes, il est difficile de réaliser la fusion au niveau des caractéristiques dans la pratique en raison des facteurs suivants :

(a) Un vecteur de caractéristiques à haute dimension peut être créé en concaténant deux vecteurs de caractéristiques.

(b) Si les ensembles de fonctionnalités ne fonctionnent pas ensemble (incompatibles), la concaténation échouera..

Les méthodes de fusion pré-classification sont rarement utilisées en raison des nombreuses restrictions qu'elles imposent et qui ne peuvent être satisfaites que dans un petit nombre d'applications très particulières. Alors que la fusion post-classification est la plus prometteuse pour les chercheurs, [Hafs 2016].

2. **La fusion post-classification**

Il est possible d'effectuer la fusion post-classification en utilisant les scores du module de comparaison ou les scores du niveau de décision. Il s'avère que les "systèmes à classificateurs multiples" sont un problème bien connu de la communauté scientifique. [Hafs 2016].

Fusion au niveau des décisions (Decision Level) :

Avec cette approche, chaque sous-système biométrique effectue de façon autonome les étapes d'extraction des caractéristiques, comparaison et reconnaissance [Kankrale & Sapkal 2012]. Ensuite, Dans le système de décision-fusion, chaque système fournit un choix binaire OUI ou NON, qui peut être représenté par 0 et 1. La décision finale est alors prise en utilisant cette séquence de 0 et 1[Hafs 2016]. Pour arriver à la décision finale, plusieurs méthodes peuvent être utilisées [Lina 2016] :

- *Le vote à la majorité « majority voting » :* les méthodes de vote consistent à interpréter chaque sortie d'un classifieur comme un vote pour l'une des classes possibles. La classe ayant un nombre de votes majoritaire ou supérieur à un seuil préfixe est retenue comme décision finale. Les votes des classifieurs ne sont pas pondérés et chaque classe reçoit autant de votes qu'il ya de classifieurs à combiner [Arif 2005] .
- *Aléatoire :* une décision (sortie d'un classifieur) est choisie aléatoirement. Le but de cette technique est de lutter contre l'usurpation des identités, les imposteurs ne savent pas à priori laquelle des biométries sera sollicitée par le système.
- *Les régles « ET et OU » :* la décision finale renvoie l'identifiant d'une personne si toutes les décisions des sous-systèmes renvoient le même identifiant [Daugman 2000]

La facilité de la fusion au niveau décisionnel la rend populaire.

Fusion au niveau score (Score Level) :

La forme la plus courante de fusion est la fusion de niveau de score, qui peut être utilisée avec n'importe quel système. Ce type de niveau utilise une fusion des résultats de plusieurs systèmes de notation pour arriver à une note finale [Fiérrez-Aguilar *et al.* 2003]. Il existe deux méthodes pour fusionner les scores : OUI ou NON pour la décision finale d'un vecteur de nombres réels, et ce vecteur a une dimension égale au nombre de sous-systèmes qu'il contient. Pour combiner les résultats de différents matchers, il existe deux méthodes. Il y a deux façons de voir les choses : comme un problème de classification ou comme un problème de combinaison. Pour être clair, les auteurs de [Ross & Poh 2009] ont montré que les techniques de combinaison surpassent la grande majorité des algorithmes de classification. Voici une répartition des différentes méthodes de fusion en fonction des scores de reconnaissance de [Hafs 2016].

2.9 Evaluation des performances d'un système biométrique

Ainsi que nous l'avons mentionné dans les sections précédentes, les systèmes biométriques, qu'il s'agisse d'un mode monomadale (une modalité biométrique unique) ou multimodal (la combinaison de plusieurs modalités biométriques), sont conçus pour être utilisés dans un large éventail d'applications. Ces systèmes doivent être évalués afin de pouvoir estimer leur performance en utilisation réelle pour envisager leur déploiement dans la vie de tous les jours. Il y a de nombreux aspects de l'évaluation de la performance qu'il peut être plus ou moins important de tester selon l'application. Il s'agit notamment de la facilité d'utilisation pour les utilisateurs, de la sécurité, du coût, des questions de protection des données, de la fiabilité des systèmes ou des capteurs, des exigences de maintenance, des exigences humaines pour la surveillance opérationnelle et, évidemment, des taux d'erreur de reconnaissance.

La communauté des chercheurs a constitué plusieurs bases de données sur les différentes modalités biométriques dans le but de permettre aux chercheurs de procéder à l'évaluation de leurs systèmes biométriques ainsi qu'à la comparaison entre les différents systèmes. Il est important de noter que certaines de ces bases de données ne contiennent qu'une seule modalité alors que d'autres sont multimodales. Les systèmes biométriques sont évalués à l'aide de bases de données, qui seront

traitées en profondeur dans la section suivante, qui donne un aperçu de ces bases. Cette caractéristique des bases de données est essentielle.

2.9.1 Evaluation des performances des systèmes d'authentification biométriques

Il existe plusieurs mesures disponibles dans la littérature qui peuvent être utilisées pour évaluer l'efficacité du système. Nous nous contenterons dans cette section d'étudier les taux d'erreur et les courbes de performance. Pour plus d'informations, la norme ISO/IEC 19795 [ISO 2006] est consacrée uniquement à la prise en charge de la problématique de l'évaluation des performances.

Les mesures des taux d'erreur

- Le taux d'échec à la capture (Failure to Acquire Rate, FTA) qui est la proportion des tentatives de captures pour lesquelles le système ne peut pas détecter un échantillon biométrique.
- Le taux d'échec à l'enrôlement (Failure To Enroll Rate, FTER) qui mesure la proportion des individus pour lesquels le système ne peut pas créer de modèle biométrique.
- La fausse acceptation (False Acceptance, FA) lorsque le système déclare l'individu comme étant légitime alors que c'est un imposteur.
- Le faux rejet (False Rejection, FR) lorsque le système refuse un individu alors qu'il s'agit d'un utilisateur légitime.
- Le taux des fausses acceptations (False Acceptance Rate, FAR) qui mesure la proportion des fausses acceptations par rapport au nombre total des transactions imposteurs.
  $TFA = \frac{nombre\ des\ imposteurs\ accets\ (FA)}{nombre\ total\ d'acces\ imosteurs}$
- Le taux des faux rejets (False Rejection Rate, FRR) qui mesure la proportion des faux rejets par rapport au nombre total des transactions légitimes.
  $FRR = \frac{nombre\ des\ clients\ rejets\ (FR)}{nombre\ total\ d'acces\ de\ clients}$
- Le taux d'égale erreur (Equal Error Rate, ERR) qui indique le taux d'erreur lorsque le système est configuré de manière à avoir le FAR égal au FRR.
- Le Zéro FRR qui est défini comme le plus faible FAR lorsqu'aucun faux rejet ne survienne.
- Le Zéro FAR qui est défini comme le plus faible FRR lorsqu'aucune fausse acceptation ne survienne.

Pour qualifier la fiabilité d'un système biométrique, l'EER est généralement le plus utilisé. Plus il est faible, plus le système est performant. Néanmoins, il est tout aussi intéressant de considérer le Zéro FAR qui, en général, est plus intéressant pour les cas pratiques [Belguechi 2015].

Les courbes de performance

Les courbes de performances permettent de visualiser les performances pour toutes les valeurs du seuil sans fixer au préalable un seul seuil. Ainsi, nous pouvons représenter l'évolution des deux taux d'erreur (FAR et FRR) dans le cas où le seuil varie pour les distributions des scores du client et de l'importateur indiquées à la figure 2.21.

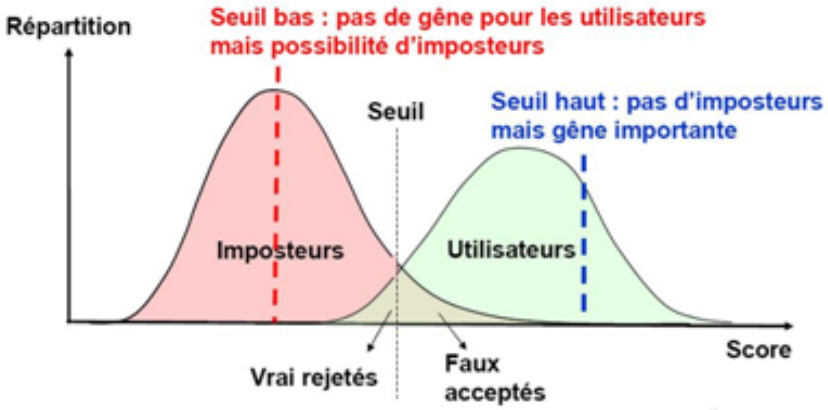


FIGURE 2.21 – *Illustration du FRR et du FAR.*

Sur la Figure 2.22, on peut lire les valeurs des taux d'erreurs pour chaque valeur du seuil.

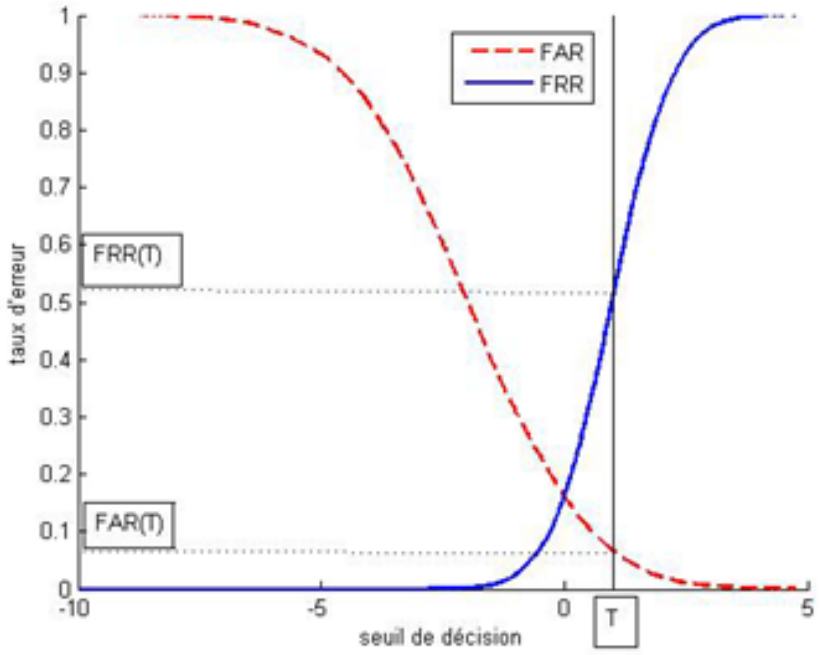


FIGURE 2.22 – *Variation des taux de Faux Rejets (FRR) et taux de Fausses Acceptations (FAR) en fonction du seuil de décision*

Étant donné que les taux d'erreur FAR et FRR dépendent du même seuil de décision, la variation du FRR en fonction du FAR peut également être tracée sur une courbe lorsque le seuil change. La Figure 2.23 illustre ces courbes, appelées courbes ROC (Receiver Operating Charcteristic).

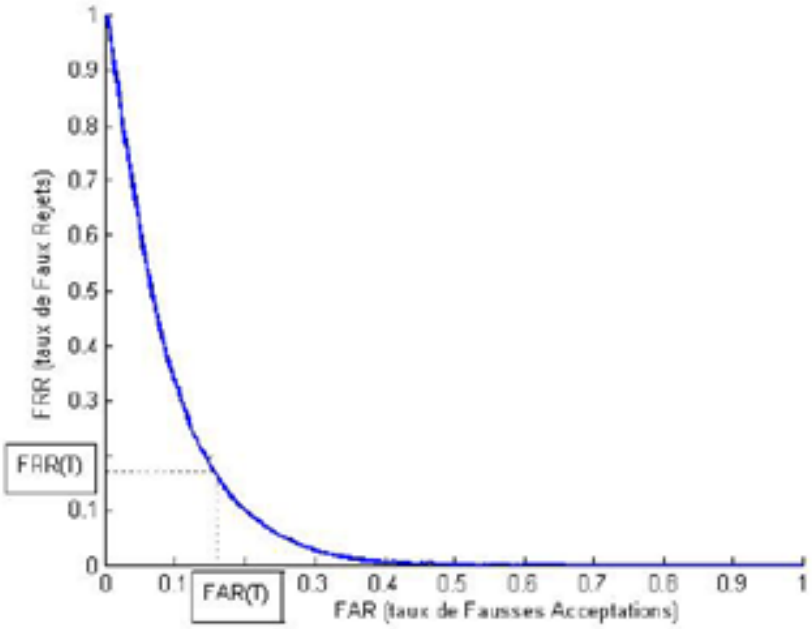


FIGURE 2.23 – *Courbe ROC : Variation du taux de Faux Rejets (FRR) en fonction du taux de Fausses Acceptations (FAR) lorsque le seuil de décision varie*

Lorsque les échelles des deux taux d'erreur sont logarithmiques, on utilise le terme DET (détection d'erreur Tradeoff) au lieu de ROC . Avec ces deux courbes, il est possible de voir comment le système se comporte dans son ensemble.

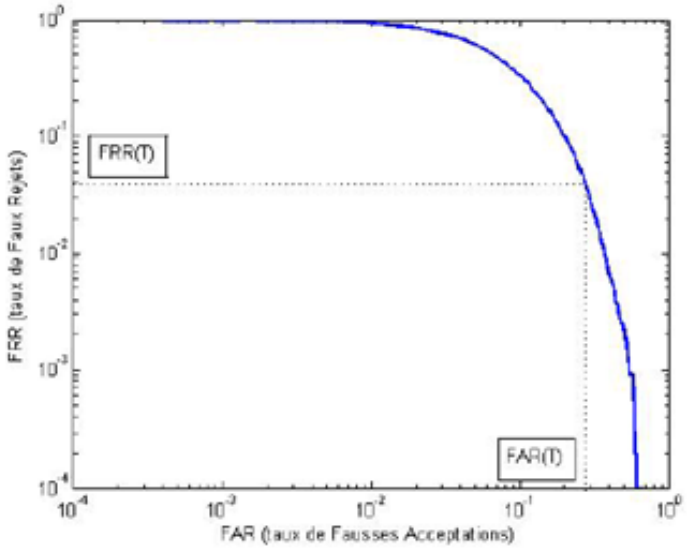


FIGURE 2.24 – *Courbe DET : Variation du taux de Faux Rejets (FRR) en fonction du taux de Fausses Acceptations (FAR) en échelle logarithmique lorsque le seuil de décision varie [Allano 2009]*

2.10 Les Bases de Données

Il est utile d'apprêter d'une base de données dédiée à cette évaluation pour déterminer les performances de vérification de l'identité d'un système biométrique, autrement dit pour mesurer les taux d'erreur de classification. Nous avons besoin,

dans la mesure des taux d'erreur, de modèles sur lesquels nous pouvons exploiter le système et sur lesquels nous pouvons mesurer les statistiques d'erreur de classification de façon à déterminer un seuil de décision. Ces bases de données fournissent donc un processus d'acquisition uniforme pour toutes les plateformes. L'adaptation des paramètres d'un système mono-modal (réglage du seuil de décision) ou multi-modal (réglage du poids de fusion) peut se faire à l'aide de bases de données biométriques qui stockent les empreintes digitales d'une personne. Les bases de données biométriques réelles et les bases de données biométriques synthétiques sont les deux grandes catégories dans lesquelles s'inscrivent les ensembles de données biométriques collectées.

2.10.1 Bases de données réelles

Ces bases contiennent des données biométriques réelles acquises grâce à la participation de volontaires. Dans la littérature, il existe deux ensembles des bases : 1) bases monomodales et 2) multimodales. Un exemple de bases monomodales est FACES94, AR , FERET , FVC2002 DB2 ,CASIA , FRGC (Face Recognition Grand Challenge) , USF Human ID Gait Baseline , ENSIB , GREYC-Keystroke , etc. Un exemple des bases multimodales est XM2VTSDB , BANCA , BIOSECURE , SDUMLAHMT. Dans cette section, nous présentons quelques bases de données monomodales et multimodales.

Bases de données monomodales :

Cette section résume les bases de données monomodales, pour ce système on trouve plusieurs bases de données pour chaque modalité biométrique.

BD1 FACES94 : La base de données FACES94 contient un total de 152 personnes composée de 20 images par personne. Des différentes d'expression faciale capturées pour constituer cette base. Un exemple de visages de cette base est présenté dans la figure 2.25.

Figure 2.25 – *Exemple de visages de la base FACES94*

BD2 AR

La base de données AR a été créée par Aleix Martinez et Robert Benavente au Computer Vision Center (CVC). Elle contient 120 personnes (26 images par personne) avec plusieurs expressions faciales, d'eclairage, et d'occultation (lunettes de soleil et écharpe). la figure 2.26 présente quelques images de cette base .

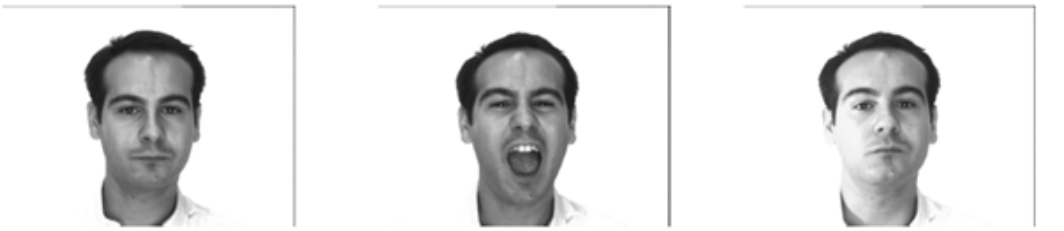


FIGURE 2.26 – *Exemple de visages de la base AR*

BD4 FV C2002 DB2 :
cette base de données contient des empreintes digitales dans le but d'utiliser dans la compétition Fingerprint Verifecation Competition (FVC2002).cette base contient 100 personnes (8 images par personne). Des exemples des images sont présentées dans La figure 2.27 illustre [El-Abed 2011].

FIGURE 2.27 – *Exemple de visages de la base FVC2002 DB2*

BD5 CASIA :
Les Figures. 2.28a et 2.28.b présentent la base de données CASIA-IrisV3 qui a été rassemblée par le "Chinese Academy of Sciences Institute of Automation". Cette base est considéré comme la plus vaste base d'iris, elle contient plusieurs images apportent plusieurs d'occlusions (vision de l'iris par les paupières). CASIA-IrisV3 contient 3 sous-groupes : CASIA-IrisV3-Interval (voir Figure. 2.28.b), CASIA-IrisV3-Lamp et CASIA-IrisV3-Twins. Le nombre total de photos dans cette base est 22051 images d'iris par 700 personnes [El-Abed 2011].

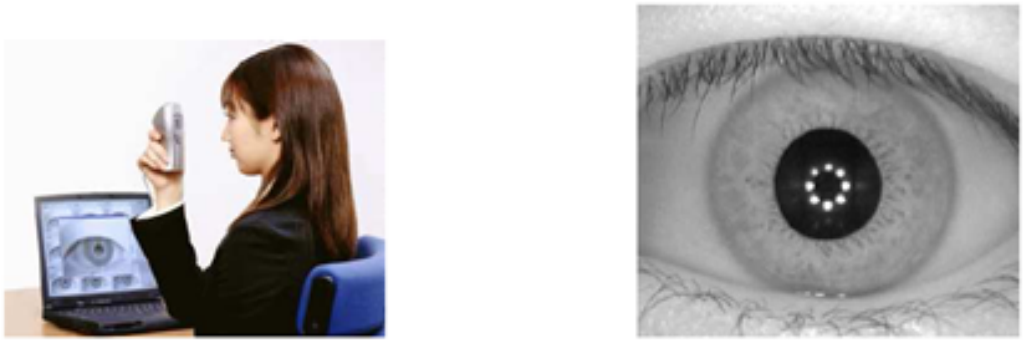


FIGURE 2.28 – *Exemple de visages de la base d'iris de CASIA-IrisV3-Interval (1.28.b).*

Les Bases de données biométriques multimodales peuvent être classés en deux groupes : 1) les bases de données contiennent des échantillons biomé-

triques Multimodale et 2) les bases de données contiennent des multimodales scores[El-Abed 2011].

Bases de données multimodales comprenant des échantillons biométriques :

Nous résumons dans cette section les bases de données multimodales, les signaux biométriques plus largement utilisés, tels que les images d'empreintes digitales ou les signaux vocaux déclarés. Dans le cadre de la biométrie multimodale, le principal problème auquel nous sommes aujourd'hui exposés est l'absence de « réels » bases de données d'utilisateurs. Véritablement, le mot réel, implique que les modalités biométriques proviennent de la même personne. Certaines bases de données multimodales d'utilisateurs réels associent les modalités, dont nous trouvons :

BD1 XM2VTS :

Cette base de données XM2VTS (M2VTS étendu) a été constituée dans le cadre du projet M2VTS (Multimodal Verification for Teleservices and Security Applications) du programme l'UE ACTES, qui se focalise sur le contrôle d'accès par le biais de l'identification multimodale du visage et de la voix. 295 personnes ont fourni des enregistrements de leur voix et des images de leur visage. On a consigné chaque objet en quatre séances sur une durée de quatre mois.

BD2 BANCA :

Cette importante base de données BANCA, qui a été élaborée dans le cadre du projet européen portant le même nom, a été constituée en 2003 et regroupe 208 personnes. Elle est constituée de quatre langues européennes et de deux modalités (visage et voix). Ainsi, le principe de ce système était de pouvoir tester différentes conditions : capteurs de bonne ou mauvaise qualité, acquisitions contrôlées ou non contrôlées. Elle était plus axée sur l'étude de la voix et du visage de façon séparée plutôt que sur l'étude de leur fusion. Toutefois, certains travaux ont analysé la fusion de ces deux modalités sur ces données sans pour autant réellement comparer plusieurs méthodes.

BD4 BIOMET

La base de données BIOMET est constituée de cinq modalités différentes : l'audio, l'image du visage, l'image de la main, les empreintes digitales et la signature. Dans le cas du visage, en plus des images d'un appareil photo numérique conventionnel, une caméra à éclairage infrarouge (conçue pour supprimer l'influence de la lumière ambiante) est également mise en application. Les participants ont tenu trois séances différentes, avec trois à cinq mois d'intervalle. Pour la première session, le nombre de participants atteignait 130 pour la première campagne, 106 pour la deuxième et 91 pour la dernière campagne.

BD5 SMARTKOM :

Il s'agit d'une base de données multimodale pour l'étude de l'interaction homme-machine créée par le consortium SmartKom (Allemagne) , Elle a été enregistrée dans des lieux publics (cinémas et restaurants) dans la configuration technique publique SmartKom. Nous pouvons retrouver les caractéristiques suivantes : la main, la signature, les empreintes digitales et la voix de 96 utilisateurs et 172 acquisitions.

BD6 BIOSECURE

En effet, le réseau d'excellence BioSecure a facilité la constitution d'une grande base de données multimodale (de 500 à 1000 personnes en fonction des sous-bases par modalité) tout au long de la durée du programme. Jusqu'à présent, il exis-

tait peu de bases multimodales, dont la taille était encore limitée. Dans la base de données multimodale BioSecure, nous avons trois bases de données multimodales acquises dans des circonstances variées. En effet, dans la première sous-base DS1 (DataSet 1), il s'agit de données acquises dans des conditions non supervisées et en ligne sur Internet, ainsi que des données audio et vidéo. Quant à la deuxième sous-base DS2 (DataSet 2), celle-ci est une base acquise dans des conditions contrôlées permettant de traiter un grand nombre de modalités biométriques : voix, visage, empreintes digitales, iris, forme de la main et signature. Pour ce qui est de la troisième sous-base DS3 (Dataset 3), elle se compose de données recueillies dans des conditions dégradées et mobiles. De fait, nous pouvons retrouver quatre modalités, voix, visage, empreinte et signature, toutes acquises sur des plates-formes mobiles comme les PDAs...

BD7 SDUMLAHMT :

Dans cette base de données, il y a 106 empreintes digitales et veines de personnes, ce qui en fait la plus complète. Il y a 3816 images de veines dans la base de données. Des fichiers BMP de 320*240 pixels sont utilisés pour stocker toutes les images. La base de données a une taille totale de 0,85 Gbytes. Au format Bmp, chaque image d'empreinte digitale est stockée avec une valeur de 256 niveaux de gris. Cinq types de capteurs différents ont été utilisés pour capturer les six doigts. La Figure 2.29 montre une sélection d'images provenant de plusieurs bases de données [Yin *et al.* 2011].

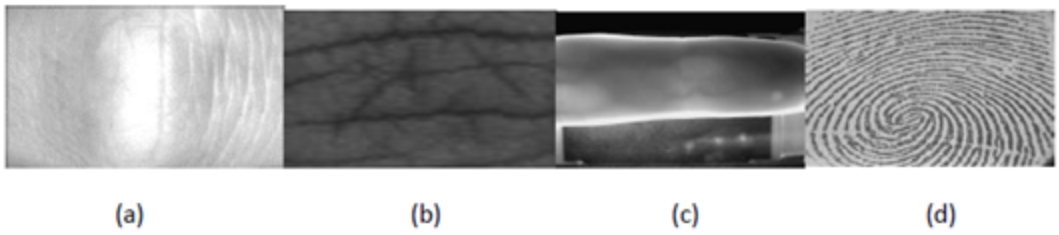


FIGURE 2.29 – *Les images originales, (a) image FKP Polytechnique, (b) image FKP Delhi, (c) image des veines, (d) image d'empreinte digitale*

BD8 poly U :

La base de données poly U est un dépôt massif de matériel universitaire. Le nombre total de photos dans cette base est de 7920, créées par 165 personnes utilisant leurs index droit et gauche, ainsi que leurs majeurs gauche et droit, soit un total de 660 doigts avec 12 captures chacun.Pour la nouvelle caractéristique biométrique, l'empreinte d'articulation , seules quelques bases de données ont été proposées, notamment celles de l'Université polytechnique de Hong Kong et du Delhi Biometrics Center. [Ross *et al.* 2006] .

Bases de données multimodales comprenant des scores biométriques

Dans cette catégorie de bases de données multimodales, les scores de correspondance des caractères individuels étudiés sont uniquement utilisés pour la recherche multimodale basée sur le score de fusion ou la décision de fusion.

BD1 NIST :

L'ensemble de scores NIST Biometric Scores Set (BSSR1)représente un ensemble de scores de similarité publiés par deux systèmes de reconnaissance faciale de 2002 et un système d'empreintes digitales de 2004, qui travaillent sur les faces avant et les index d'empreintes digitales gauche et droite.

BD2 IDIAP La base de données des scores est conçue sur XM2VTS, dans le strict respect des protocoles standard Lausanne I et II (LP1 et LP2) . LP1 dispose de huit systèmes de référence et LP2 de cinq systèmes de base. Cette base de données des scores dispose de deux protocoles de fusion : 1) la fusion de deux experts avec des combinaisons spécifiques de manière à pouvoir expérimenter la fusion multimodale, la fusion intermodale avec des ensembles de caractéristiques différents et la fusion intra-modale avec la même fonction, ainsi que 2) la fusion par le biais de protocoles avec toutes les combinaisons possibles.

2.10.2 Bases de données synthétiques

les bases de données synthétiques simulent des données biométriques réelles. De plus, une base synthétique doit posséder deux propriétés. Tout d'abord, la performance d'une base de données synthétique doit se rapprocher de celle obtenue avec une base de données réelle. Ensuite, les données de la base de données synthétiques ne doivent pas reproduire les données biométriques réelles d'une personne. Cette base de données, SFinGe, générée par le logiciel SFinGe, a été élaborée par le laboratoire italien BioLab [2] , et elle représente un exemple de base de données synthétique. Nous pouvons voir à la figure 2.30 quelques empreintes digitales générées par ce logiciel.

FIGURE 2.30 – *Exemple d'empreintes synthétiques générés par SFinG*

2.11 CONCLUSION

La biométrie est aujourd'hui largement considérée comme la méthode de sécurité la plus sûre qui soit. En raison de ses avantages, elle est de plus en plus utilisée dans la vie réelle. Dans ce chapitre, nous avons présenté l'idée des systèmes biométriques, ainsi que leurs différentes conceptions et utilisations. Par conséquent, nous avons fait la démonstration de quelques techniques biométriques. Nous avons également présenté le marché mondial de la biométrie.

Ensuite, nous avons abordé la biométrie qui fait appel à plusieurs sens. Un système biométrique à modalité unique présente des limites, tandis qu'un système multimodal présente des avantages. Nous avons ensuite discuté des nombreuses combinaisons potentielles de modalité, des architectures et des niveaux de fusion qui peuvent être utilisés dans un système multimodal. Nous avons conclu par quelques recommandations dans le but d'améliorer la performance de l'authentification /identification des personnes et rendre la sécurité plus robuste et plus

2. http ://biolab.csr.unibo.it/

sûre, Des études montrant que non seulement les systèmes biométriques multimodaux ne sont pas plus sûrs, mais ils présentent des vulnérabilités supplémentaires. C'est pour cette raison il est nécessaire de sécuriser les données multi biométriques.

Dans les chapitres qui suivent nous présentons un état de l'art de l'ensemble de solutions proposées pour la protection des données multi biométriques.

Protection du modèle multi biométrique

3

Sommaire

3.1 Introduction

Pour qu'un système biométrique soit fiable et convivial, il doit être sécurisé. Dans ce chapitre, nous examinerons l'état actuel de l'art en matière de sécurité des systèmes multi-biométriques. Ce chapitre examine les nombreuses technologies utilisées par la communauté de recherche sur la sécurité des systèmes multibiométriques, en soulignant les avantages et les inconvénients de chacune. La transformation des caractéristiques, les systèmes biométriques cryptographiques et les modèles hybrides sont trois stratégies de protection des systèmes multibiométriques présentées dans ce chapitre. La transformation réversible, à savoir la technique du Biohashing, revêt une importance particulière dans cette thèse.

3.2 Sécurité multi-biométrique

Ce travail de recherche sur la protection multi-biométrique a pour objectif premier de produire des initiatives industrielles présentées dans un cadre générique. Le système doit être capable de fusionner n modèles sans qu'il soit nécessaire de les représenter à l'aide de niveaux de fusion spécifiés (k la représentation pourrait être impliquée). Le processus de représentation se poursuit, et un mécanisme général de protection des données biométriques a été mis en place (Figure 3.1). Une représentation commune des vecteurs de caractéristiques est établie dans un module de fusion, et les vecteurs de caractéristiques sont fusionnés de manière sensible. Le modèle multi-biométrique est ensuite protégé à l'aide d'une stratégie de protection de modèle appropriée. Plusieurs problèmes se posent lorsqu'on se concentre sur une fusion générique de modèles multi-biométriques dans une stratégie de protection de modèle. La littérature actuelle sur la protection des modèles multi-biométriques est principalement classée en catégories.[Rathgeb & Busch 2012].

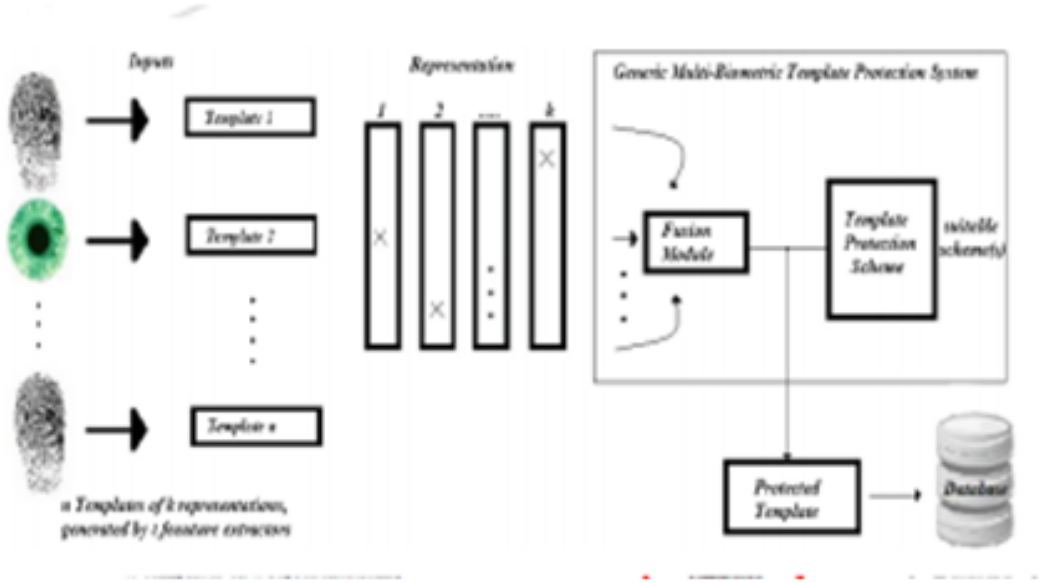


Figure 3.1 – *Le framework d'une protection générique multi-biométrique au niveau des caractéristiques*

La littérature actuelle sur les méthodes de protection de modèles multi biométrique sont largement classifies [Bedad & Adjoudj 2018b].

3.3 SCHÉMAS DE PROTECTION DES MODÈLES MULTI-BIOMÉTRIQUES

Les quatre caractéristiques suivantes doivent être présentes dans une stratégie idéale de protection des modèles biométriques [Maltoni *et al.* 2009] :

- ***Diversité :*** le modèle sécurisé ne doit pas permettre une compatibilité croisée entre les bases de données, garantissant ainsi la confidentialité de l'utilisateur.
- ***Révocabilité :*** il doit être facile de révoquer un modèle compromis et d'en relancer un nouveau basé sur les mêmes données biométriques.
- ***Irréversibilité :*** il doit être difficile d'obtenir des calculs du modèle biométrique original à partir du modèle sécurisé. Cette propriété empêche un adversaire de créer une parodie physique de la caractéristique biométrique à partir d'un modèle volé.
- ***Performance :*** le programme de protection du modèle biométrique ne doit pas dégrader les performances de reconnaissance (FAR et FRR) du système biométrique.

La Figure 3.2 présente une classification des stratégies de protection des modèles multi-biométriques proposées dans la littérature, qui sont divisées en trois catégories, à savoir : (i) les crypto-systèmes biométriques, (ii) les approches de transformation , et (iii) les approches hybrides . Tous ces systèmes ont un point commun : ils n'enregistrent pas les données biométriques brutes directement dans la base de données, mais sur un support externe (carte à puce, token) ou après leur transformation [Belguechi *et al.* 2011].

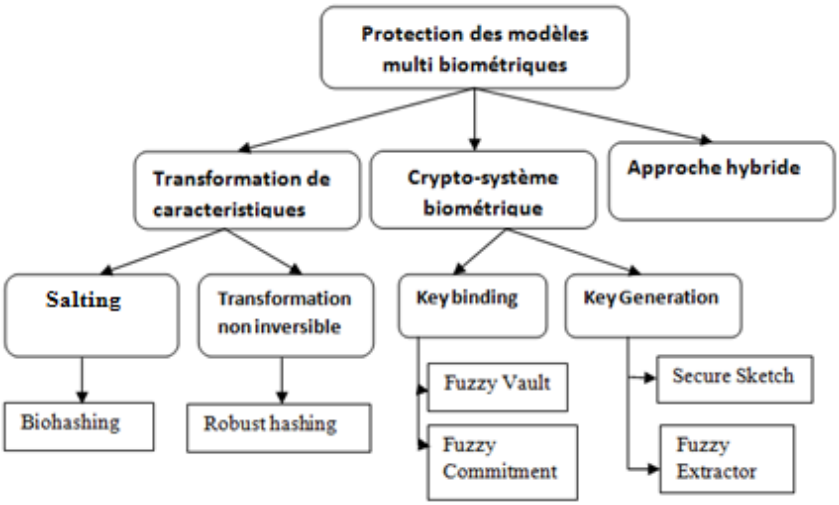


FIGURE 3.2 – *les catégories de protection des modèles multi biométriques*

3.3.1 Les crypto-systèmes multi biométriques

Les crypto-systèmes multi biométriques sont un hybride entre le crypto-système et la multi biométrie, principe sous-jacent des crypto-systèmes traditionnels [Bruce 1996] [Degabriele & Paterson 2010] Ils ont été associés au principe de reconnaissance biométrique afin d'améliorer la sécurité des systèmes d'authentification personnelle basés sur la biométrie. L'objectif principal de ces approches est de réduire la quantité de données biométriques stockées pour les modèles protégés et la base de données globale du système. La majorité des systèmes de cryptage biométrique fonctionnent de la manière suivante : pendant l'enregistrement, un

code de correction d'erreur φ est appliqué au modèle biométrique B et une clé K pour extraire l'ensemble de données H (l'ensemble H est appelé *Helper Data* en anglais). Pendant le processus d'authentification, un code de correction d'erreur φ est appliqué à l'aide des données H et du modèle de test Q pour déterminer la clé K (Figure 3.3). Les crypto-systèmes biométriques peuvent être divisés en deux catégories en fonction de la manière dont ils aident à l'extraction des données. Les crypto-systèmes de type *key-binding* et de type *key-generation* sont examinés dans[Jain *et al.* 2008] [Rathgeb & Uhl 2011] Un crypto-système à liaison par clé (keybinding)est un crypto-système dans lequel les données utiles sont récupérées à l'aide d'une clé indépendante des caractéristiques biométriques. Un crypto-système à génération de clé (key-generation) est un crypto-système dans lequel les données d'aide sont extraites uniquement du modèle biométrique et la clé est créée directement à partir des caractéristiques [Chouaib 2014].

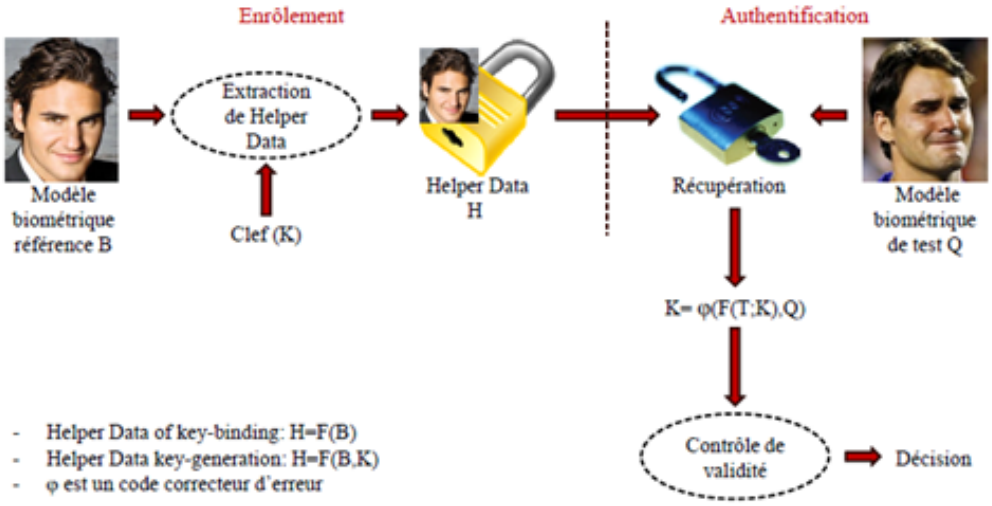


FIGURE 3.3 – *Mécanisme d'authentification général des crypto-systèmes biométriques de key-binding et key génération*

Les crypto-systèmes multi-biométriques de type « key-binding » [Juels & Wattenberg 1999] [Hao *et al.* 2006] , .)]sont résistants aux variations intra-sujet dans les modèles biométriques. On peut interpréter cette résistance par la capacité du code de correction d'erreur employé. En revanche, leur conception ne vise pas à garantir la diversité ou la révocabilité. D'autre part, si des algorithmes de transformation de caractéristiques sont utilisés pour classer les cryptosystèmes biométriques, des codes correcteurs d'erreurs doivent être utilisés pour éviter l'utilisation de classificateurs classiques conçus spécifiquement pour comparer des modèles biométriques. Les « nominations » suivantes sont les approches les plus utilisées dans cette catégorie : *Fuzzy Commitment* [Juels & Wattenberg 1999] et *Fuzzy Vault* [Juels & Sudan 2002] [Chouaib 2014]. Juels et Wattenberg ont été les premiers à proposer une solution appelée FuzzyCommitment en 1999 [Juels & Wattenberg 1999] Une formule dénommée Fuzzy commitment, traduite mot à mot : engagement flou. En principe, leur méthode consiste à se baser sur les données biométriques actuelles pour procéder à un nouveau calcul d'une valeur qui sera ensuite utilisée pour l'authentification des utilisateurs. De façon générale, la méthode dite du fuzzy commitment est répartie en deux étapes : enrôlement (l'inscription) et l'authentification. En biométrie, l'étape d'enrôlement consiste gé-

néralement à prendre plusieurs fois les données biométriques de l'utilisateur (son empreinte digitale par exemple) pour constituer une valeur de référence. La phase d'authentification se résume à la comparaison de la valeur actuelle avec la valeur de référence pour établir si l'utilisateur est bien celui prévu. Le processus dit du fuzzy commitment respecte ces deux étapes, excepté que la valeur de référence stockée n'est pas une donnée biométrique et ne permet pas de localiser les données biométriques utilisées pour la générer. A cette fin, le fuzzy commitment repose sur un ensemble de mots de code dans $\{0,1\}^n$ et une fonction de hachage H.

— **Enrôlement :** Dans le cas de l'utilisateur U, son empreinte biométrique est représentée sous la forme d'une séquence x de n bits. Le système choisit au hasard un mot de code c $\in \{0,1\}^n$ et calcule (c-x,H (c)). Le paramètre utilisateur flou (Fuzzy commmitment)U est le couple (c-x,H(c)). Cette donnée est enregistrée, le reste est supprimé. Au terme de cette étape, le système validera comme U tout utilisateur susceptible de produire une empreinte biométrique afin de récupérer le mot de code c.

— **Authentification :** Si un utilisateur se présente comme U et que son signal biométrique actuel est x'.. Pour la vérification de l'engagement(c-x,H (c)), le système emploie x'. .Dans ce cas, il faut d'abord calculer (c-x)+ x'.. Dans la mesure où l'utilisateur est la personne qu'il revendique, alors son empreinte biométrique actuelle x'. doit être proche de son empreinte biométrique de référence x et donc (c-x)+ x'. doit être proche de c. A cette fin, il suffit de vérifier que H (c') = H (c) où (c') représente le mot de code le plus proche de (c-x)+ x'.

L'approche Fuzzy Vault peut être considérée comme une amélioration du Fuzzy Commitment. Le principe général de fonctionnement du fuzzy vault est le suivant [Juels & Sudan 2002] : Pour générer un polynôme P [1]une clé d'utilisateur K est requise lors de l'enrôlement. La projection polynomiale P(T) du modèle biométrique de référence T est ensuite calculée. Enfin, on ajoute du bruit à P(T) pour construire les données d'aide H du fuzzy vault. Pour reconstruire le polynôme P et acquérir la clé K, un code de correction d'erreur (le plus souvent un code de Reed-Solomonhttp://fr.wikipedia.org/wiki/Code_de_Reed-Solomon est appliqué au modèle de test Q et aux données d'aide H pendant l'authentification/vérification. La faible performance discriminante est un problème pour les systèmes de cryptage multi-biométriques à génération de clés, qui peut être mesuré en termes de stabilité de la clé 2 [2]et d'entropie de la clé 3 [3] [Jain *et al.* 2008] . Il y a une forte stabilité de la clé, mais pas une entropie zéro, lorsqu'un système offre la même clé quel que soit le modèle d'entrée, d'où un taux de fausse acceptation élevé. Lorsqu'un système crée des clés distinctes pour différents modèles d'un même utilisateur, il présente une grande entropie mais une faible stabilité, ce qui entraîne un taux de faux rejets élevé. Par conséquent, l'obtention simultanée d'une stabilité des clés et d'une entropie élevée constitue une difficulté majeure dans la conception de ces systèmes de protection.Les systèmes connus sous le nom de *Secure Sketch* [Bringer *et al.* 2008] et *Fuzzy Extractor* [Dodis *et al.* 2008] sont les approches les plus courantes dans ce domaine. L'objectif des systèmes Secure Sketch est de traiter la variance intra-sujet des modèles biométriques en réduisant

1. le mécanisme de construction de P est comme suit : les coefficients de P sont les chiffres de K et le degré de P est le nombre de ces chiffres moins un. Par exemple, si K=72451 alors P = $7x4 + 2x3 + 4x2 + 5x + 1$
2. Taux de répétibilité d'une clé générée à partir les données biométriques
3. Nombre de clés possibles (différentes) qui peuvent être générées

la quantité de données biométriques dans les *sketchs* (les modèles sont appelés sketchs dans un cryptosystème Secure Sketch). Ces stratégies sont toutefois insuffisantes pour atteindre un équilibre efficace entre stabilité et entropie des clés.Le fuzzy extractor est un ajout à Secure Sketch qui permet de gérer simultanément les variations intra-sujet et la stabilité/entropie des clés.
Ces quatre versions des cryptosystèmes multi-biométriques (*Fuzzy Commitment, Fuzzy Vault, Secure Sketch, Fuzzy Extractor*) ont été testées sur une variété de modalités biométriques. Ils existes de nombreux travaux qui suggèrent le Crypto système multi Biométrique, en 2008 ***Nandakumar et al*** [Nandakumar & Jain 2008] ont décrit une approche pour la sécurité des modèles multi biométriques en utilisant un schéma de fuzzy vault . Ils proposent un schéma pour sécuriser plusieurs modèles d'un utilisateur en tant qu'entité unique. ils dérivent un modèle multi biométrique unique à partir des modèles individuels et on le sécurisons , en utilisant le cadre de fuzzy vault . ils démontrent qu'une vault multi biométrique offre de meilleures performances de reconnaissance et une sécurité supérieure par rapport à une vault uni biométrique. Par exemple, notre vault multi biométrique basée sur l'empreinte digitale et l'iris réalise une GAR de 98,2% (1-FRR est appelé Genuine Accept Rate (GAR)). à un FAR de 0,01%, tandis que les valeurs GAR correspondantes de l'iris individuel et des vault d'empreintes digitales sont respectivement de 88% et 78,8%. En outre, ils montrent également que la sécurité du système n'est que de 41 bits lorsque les vault d'iris et d'empreintes digitales sont stockées séparément. D'autre part, le fuzzy vault multi biométrique basée sur l'empreinte digitale et l'iris fournit 49 bits de sécurité. ***Kelkboom et al.*** [Kelkboom *et al.* 2009]suggérent une application du modèle protégé à partir de deux algorithmes de reconnaissance 3D (fusion multi-algorithmes) au niveau des caractéristiques, des scores et des décisions. Les auteurs montrent que la fusion peut être appliquée aux niveaux de fusion connus avec la technique de protection des modèles connues sous le nom de Helper-Data System (Crypto système biométrique). ***Meenakshi et al*** [Meenakshi & Padmavathi 2010] Cette approche assure la sécurité et la révocabilité des modèles d'iris et de rétine à l'aide d'une combinaison de l'utilisateur et une Biométrie souple basée sur le mot de passe de fuzzy vault biométrique multimodal durci. Le durcissement par mot de passe assure la sécurité et la révocabilité des modèles biométriques. La biométrie des yeux, à savoir l'iris et la rétine, a certains mérites par rapport à l'empreinte digitale. Les caméras de capture d'iris et de rétine peuvent être montées sur un seul appareil pour améliorer la commodité de l'utilisateur. La sécurité de la vaut est mesurée en termes de min-entropie. ***Kanade et al*** [Kanade *et al.* 2010] Ont proposé une approche pour combiner la multi-biométrie avec la cryptographie pour obtenir des clés d'entropie élevées, et proposer une nouvelle méthode de fusion de niveau d'entité par correction d'erreur pondérée (FeaLingECc). Avec cette méthode, des différents poids peuvent être appliqués à différentes données biométriques. Le système de shooing, que ils ont appliqué plus tôt aux données biométriques, est utilisé dans ce système pour randomiser les codes de correction des erreurs qui permettent de rendre le système plus sécurisé. Deux systèmes sont proposés : (1) un système de type multi-unités, et (2) un système de type multimodal. Les informations provenant des iris gauche et droite d'une personne sont combinées dans le système de type multi-unités pour obtenir des clés crypto-bio à entropie longue et haute. Le deuxième schéma est un système basé sur la biométrie multimodale dans lequel l'information provenant de l'iris et du visage est combinée. Pour les tests à deux iris, ils peuvent obtenir des clés de 147 bits ayant une entropie de 147 bits avec 0% de FAR et 0,18% de FRR.

Et avec le système multi-modal (iris + visage), ils peuvent obtenir des clés de 210 bits ayant une entropie de 183 bits à 0,91% de FRR et 0% de FAR. ***Argyropoulos et al.*** [Argyropoulos *et al.* 2010]ont présenté un système pour la sécurité des modèles biométriques dans les systèmes d'authentification biométrique multimodaux basés sur des codes de correction d'erreur. Cette méthode attaché le modèle biométrique dans une clé cryptographique et une méthode SVM où la biométrie du visage et de la démarche est utilisée dans cette méthode. Le point d'opération résultant EER = 3.05% et EER = 2.54% pour la méthode SVM. Les transactions en e-commerce ,et e-bancaire utilisent le crypto système multi biométrique électronique, c'est pourquoi ***Geethanjali et al*** [Geethanjali *et al.* 2012] Ont fourni une sécurité au modèle biométrique en générant un Secure sketch en utilisant le crypto système multi biométrique et qui est stocké dans une base de données. Une fois que le modèle biométrique est volé, cela devient un problème sérieux pour la sécurité du système et aussi pour la confidentialité des utilisateurs. Dans cette approche , la fusion au niveau de caractéristiques est utilisée pour combiner les caractéristiques de manière sécurisée avec des crypto systèmes biométriques bien connus, à savoir le fuzzy vault et le fuzzy commitment. Les inconvénients de cet système incluent la précision de la biométrie doivent être améliorés et les bruits de la biométrie doivent également être réduits . En 2012 , ***Nagar et al*** [Nagar *et al.* 2012] Ont proposé un système de fusion au niveau de caractéristiques simultanément pour protéger plusieurs modèles d'un utilisateur en tant que un unique Secure sketch . Ils sont utilisés des crypto systèmes biométriques, à savoir un fuzzy vault et un fuzzy commitment, et deux bases de données (une base de données multimodale réelle et une base multimodale virtuelle) contenant chacune les trois modalités biométriques les plus populaires, L'empreinte digitale, l'iris et le visage. Les résultats expérimentaux montrent que les crypto systèmes multi biométriques proposés ici ont une sécurité et une performance de correspondance plus élevées par rapport à leurs homologues uni biométriques. ***Yang et al*** [Yang *et al.* 2012] ont présenté une évaluation des résultats de fusion au niveau de la décision des identificateurs pseudonymes basés sur les minuties d'empreintes digitales générés par trois algorithmes biométriques de protection des modèles développés dans le projet de recherche européen TURBINE.Il existe huit scénarios de différents fusion couvrant plusieurs échantillons, algorithmes, capteurs, instances et leurs combinaisons dans ses tests. Sur le niveau de décision binaire et d'évaluer leurs performances biométriques et leur efficacité de fusion sur une base de données d'empreintes digitales multi-capteurs avec 71 994 échantillons. Le point de fonctionnement de fusion résultant (FAR = 0,0012 ; FRR = 0,0703).
Dans la même année ,***Merkle et al*** [Merkle *et al.* 2012] recommandé une approche de multimodal et Multi-Instance Fusion pour les Crypto systèmes biométriques, on analyse des stratégies de fusion multi-biométriques pour les crypto systèmes biométriques en ce qui concerne leur impact sur la sécurité et la précision de la reconnaissance. Et ils ont également introduit le niveau de hachage en tant que nouveau niveau de fusion. En outre, ils ont utilisé le Fuzzy Commitment Schema et le Fuzzy Vault.

En 2014 ***Lu et Peng*** [Lu & Peng 2014]Ont proposé un nouveau crypto système multi-biométrique à doigts utilisant une fusion au niveau des caractéristiques pour protéger simultanément plusieurs modèles d'empreintes digitales, empreinte du vein, empreintes d'articulation des doigts et de Traits de forme du doigt en tant que Secure sketch. Ils analysent théoriquement la fusion de niveau caractéristique pour

le crypto système multi-biométrique du doigt en ce qui concerne leur impact sur la sécurité et la précision de la reconnaissance. Les résultats expérimentaux comparatifs montrent que le crypto système multi-biométrique à doigts surpassé les homologues uni-biométriques en termes de performance ,de vérification et de sécurité de modèle. Tandis que ***Beulah and Rani*** [Beulah & Rani 2014] Son approche intégrée des crypto systèmes (HDS) avec le visage et l'empreinte digitale .La biométrie de sorte que ils réalisent un système dans lequel les modèles sont protégés par la protection de la vie privée, et plusieurs modèles peuvent être dérivés des mêmes images faciales et d'empreintes digitales dans le but de renouveler le modèle. L'extraction de vecteurs caractéristiques binaires constitue une étape essentielle dans ce processus. Les vecteurs de caractéristiques binaires sont intégrés dans le HDS conduisant à un processus d'extraction de fonctionnalité d'empreinte digitale protégé contre la vie privée et un algorithme de reconnaissance faciale avec FAR et GAR satisfaisants, a déclaré que la variation intra-classe est suffisamment petite. ***Amirthalingam*** [Amirthalingam & Radhamani 2014]A proposé une méthode pour sécuriser le modèle biométrique multimodale visage et oreille. L'extraction de caractéristiques de l'ensemble multimodale du visage et de l'oreille est appliqué à la technique de biocrypto système fuzzy vault on utilisant un multi polynomial pour éviter la dégradation possible de la sécurité. La sécurité et l'exactitude des modèles de fuzzy vault du système multi biométrique dépendent de l'infaillibilité du problème de reconstruction polynomiale. Les résultats expérimentaux de la méthode proposée sont évalués ,il utilise le taux de concordance erreur(FMR) et le taux d'acceptation authentique (GAR) avec le degré de polynômes. La performance de la méthode proposée montre la croissance prometteuse de la reconnaissance biométrique multimodale et de la sécurité des modèles. ***Lalithamani et Sabrigiriraj*** [Lalithamani & Sabrigiriraj 2015] suggérent une technique pour générer le visage et la veine de la main basé sur le fuzzy vault pour un crypto système multi-biométrique. Dans cette méthode, les caractéristiques sont extraites des images traitées de la main et des veines palmaires en découvrant des points communs unique . Les points de balle sont ajoutés aux points déjà extraits pour obtenir le vecteur de caractéteristque combiné. Les points clés secrets qui sont générés en fonction de l'entrée de clé utilisateur sont ajoutés au vecteur de fonctionnalité combiné pour avoir le fuzzy vault. Pour le décodage, le modèle biométrique multimodal de l'image de la veine palmaires et de l'image de la veine de la main est construit et combiné avec le fuzzy vault stockée pour générer la clé finale. Les résultats montrent que la technique proposée a obtenu de meilleurs résultats avec GAR de 94% sans bruit et 88% avec du bruit. Une autre approche du schéma de fuzzy vault multimodale à la veine palmaires et à l'empreinte digitale décrite par ***Chidemyan*** [Chidemyan 2015] Les expériences montrent qu'il y a 50 points en moyenne après la description de la fusion au niveau de caractéristiques a été appliquée. Cette quantité de points suffit pour la clé de 192 bits Génération et pour la précision pratique du système (FAR <0.04). ***Sankareswari et Jothi***[Sankareswari & Jothi 2015] Ont proposé une approche hybride pour la sécurisation des modèles biométriques utilisant la cryptographie visuelle ,où la cryptographie visuelle est la technique utilisée pour chiffrer les données sous forme d'informations visuelles telles que les images. Étant donné que les modèles biométriques stockés dans la base de données sont généralement sous forme d'images, la cryptographie visuelle peut être utilisée efficacement pour chiffrer les modèles contre les attaques. ***Thanki et Borisagar*** [Thanki & Borisagar 2015] ont décrit des techniques de tatouage à base de théorie de la compression résistante (CS) sont proposées pour la protection biomé-

trique de l'image dans un système multi biométrique. En proposant des techniques de tatouage, l'image biométrique du filigrane est cryptée dans son domaine dispersé en utilisant la théorie du CS et l'intégration dans des coefficients épars d'une image biométrique hôte. L'image biométrique à filigrane et l'image biométrique de filigrane reconstruit, constituent un système multi biométrique. En 2016,***Scholar*** [Scholar 2016] A proposé une approche pour un réseau à base de Crypto systèmes biométriques basée sur le niveau de sécurité, dans ce travail, un crypto système multi biométrique basé sur l'empreinte digitale (MBC) utilisant la fusion au niveau de la décision. Les fonctions Hash sont utilisées dans la construction MBCD à chaque trait biométrique unique. Le résultat expérimental donne une meilleure précision d'authentification par rapport à un crypto système basé sur une biométrie unique. Dans un travail plutôt récent, un nouveau cadre pour un crypto système biométrique dans lequel une clé cryptographique est cachée avec des modalités biométriques proposées par ***Kumar et al*** [Kumar & Kumar 2016] La modalité biométrique candidate est sécurisée à l'aide de deux fonctions : 1) l'encodage BCH, qui délivre le code de parité stocké pour l'alignement du modèle biométrique de requête et 2) la fonction Hash pour calculer le code hash afin de préserver son intégrité. Le crypto système est formé en créant deux ensembles cellulaires différents. Le code hash est dispersé sur un ensemble de cellule par une position de colonne choisie au hasard, et la clé secrète est distribuée sur le deuxième groupe de cellules sur la même position. Les autres sites de l'ensemble de cellules sont remplis avec la génération aléatoire. En 2017 , ***Gomez-Barrero et al*** [Gomez-Barrero *et al.* 2017] introduit un cadre général pour la protection de modèles multi-biométriques basé sur le chiffrement probabiliste homomorphique, où seules les données chiffrées sont traitées. Trois niveaux de fusion sont analysés en profondeur, ce qui montre que toutes les exigences décrites dans la norme ISO / CEI 24745 sur la protection biométrique des données ne sont pas dégradées. En outre, même si tout le processus est effectué dans le domaine chiffré, aucun chiffrement n'est nécessaire pendant la vérification, permettant ainsi une vérification efficace qui peut être déployée pour des applications en temps réel. Enfin, les expériences sont réalisées sur un cadre de recherche reproductible. Les résultats obtenus affichent des taux de précision élevés, atteignant des EER aussi bas que 0,12%, et nécessitent des modèles protégés comprenant 200 Ko. ***Maiand et al*** [Mai *et al.* 2017] Ont recommandé une approche de fusion de caractéristiques binaires pour les crypto systèmes multi-biométriques. La méthode proposée 1) extrait un ensemble faiblement dépendant de groupe de caractéristiques des multiples de caractéristiques uni modales ; Et 2) Proposé une approche de fusion de caractéristiques binaires pour les crypto systèmes multi-biométriques. La méthode proposée 1) extrait un ensemble faiblement dépendant de groupe de caractéristiques des multiples de caractéristiques unimodales ; Et 2) fusionne chaque groupe à un bit à l'aide d'un mappage qui minimise les variations intra-utilisateur et maximise les variations inter-utilisateur et l'uniformité du bit fusion. Les résultats expérimentaux sur trois bases de données multimodales montrent que la caractéristique binaire fusionnée de la méthode proposée présente une plus grande discriminabilité et une entropie plus élevée par rapport aux caractéristiques unimodales et aux caractéristiques fusionnées générées par l'état de l'art des approches de fusion binaire. ***Dinca et al*** [Dinca & Hancke 2017] Cette approche est une étude sur les implications de la falsification de données biométriques pour la récupération de la clé dérivée. Ils démontrent que la biométrie falsifiée peut générer la même clé, ce qui entraînera un attaquant pour obtenir la clé privée. Une implémentation pratique est proposée en utilisant l'empreinte digitale et l'iris

comme biométrie et le fuzzy extractor pour l'extraction des clés biométriques.
En 2021 , [Sarier 2021],décrivent un nouveau système d'authentification biométrique préservant la confidentialité (PPBA) conçu pour l'informatique mobile (MEC) et la biométrie multimodale. ils concentrent sur les attaques d'escalade qui révèlent des modèles biométriques à des adversaires internes malgré le stockage crypté dans le cloud. Tout d'abord, ils présentent un résultat d'impossibilité sur l'existence de systèmes PPBA bipartites résistants à ces attaques. Pour surmonter ce résultat négatif, ils ajoutent un serveur de périphérie sans collusion pour détecter les attaques d'escalade à la fois dans le modèle semi-honnête et malveillant. Le serveur de périphérie qui stocke les paramètres secrets de chaque utilisateur permet d'externaliser la base de données biométrique vers le cloud et d'effectuer la correspondance dans le domaine crypté. Le système proposé combine les mesures de chevauchement des ensembles et de distance euclidienne en utilisant la fusion des niveaux de score. Ici, les serveurs cloud et Edge ne peuvent pas apprendre le score de correspondance fusionné. De plus, le serveur de périphérie ne peut accéder à aucun score partiel. L'efficacité des crypto-primitives employées pour chaque modalité biométrique entraîne un calcul linéaire et une surcharge de communication. Dans différents scénarios MEC, le nouveau système s'avère être le plus efficace avec une architecture à 2 niveaux, qui atteint une latence inférieure de 75% par rapport au cloud computing mobile. Dans la même année [Choudhary & Naik 2021],recommandé une authentification biométrique multimodale (vérification et identification) avec des modèles sécurisés. Le cadre proposé effectue l'authentification des personnes à l'aide du visage et des empreintes digitales. Les modèles biométriques sont protégés en cachant les empreintes digitales dans le visage à des endroits secrets, grâce à un filigrane aveugle et basé sur des clés (key-based watermarking). Les caractéristiques du visage sont extraites de la sous-bande d'approximation de la transformée en ondelettes discrète, ce qui réduit le plan de travail global. La méthode proposée montre également une grande robustesse des modèles biométriques contre les attaques par canal commun. [Tantubay & Bharti 2021], valident l'efficacité de la technique proposée sur le schéma de voûte floue utilisant des ensembles de données biométriques d'empreintes digitales et d'iris. Leur système proposé est mis en œuvre pour protéger la clé secrète cryptographique de l'utilisateur et supprimer efficacement l'utilisation du système d'infrastructure à clé publique (PKI) en raison de ses coûts de gestion d'émission et de distribution de certification complexes, et de sa structure centralisée qui utilise un système de réseau conventionnel et montre un point de défaillance unique. Le système donne 99,96 % de précision, avec 99,98% de GAR et 0 % de FMR.

Discussion

Pour sécuriser le modèle multi biométrique, nous disposons de systèmes de cryptage multi biométrique. Dans la plupart des cas, ces systèmes sont destinés à rectifier le bruit des données biométriques en convertissant une information publique appelée données auxiliaires W (ou helper data) depuis le modèle biométrique X. Ces données W contribuent aussi bien à cacher une clé utilisateur S dans la biométrie soit à créer une nouvelle clé S. De plus, dans tous les cas, seul W sera stocké dans la base de données et la révélation de S ne peut se faire que par introduction de la biométrie Y correcte. Toutefois, l'application de ces régimes présente de nombreuses difficultés. Dans la majorité des cas, ces schémas exigent la saisie d'un modèle X sous forme vectorielle et discrétisée, dont la modélisation n'est pas aisée pour certaines représentations d'empreintes, au même titre que pour les minuties.

En outre, ils provoquent une perte d'entropie quand il y a une certaine corrélation entre les éléments vectoriels X, par exemple pour les fonctions d'engagement flou(fuzzy commitment) ou de blindage. Afin de garantir l'irréversibilité du système, X devrait être réparti de manière identique et indépendante, chose qui n'est pas évidente à assurer pour les modèles multi biométriques. Par ailleurs, nous avons également noté que, du point de vue de la protection de la vie privée, ces systèmes, qui reposent généralement sur des codes correcteurs d'erreurs, étaient difficiles à réutiliser et ne pouvaient donc pas être supprimés.
La section suivante traite la deuxième catégorie de méthodes de protection, l'approche de la transformation des caractéristiques (ou transformations révocables).

3.3.2 Transformation de caractéristiques

L'idée principale des approches de transformation de caractéristiques est d'utiliser une fonction de transformation pour transformer un modèle biométrique non protégé en un modèle protégé [Ratha *et al.* 2001] [Ratha *et al.* 2006]. Selon le système et la modalité envisagée, il existe une variété d'options.La fonction de transformation peut prendre différentes formes selon le système et la modalité souhaitée, et elle peut également impliquer l'utilisation de certains paramètres de transformation (par exemple, une clé utilisateur). En cas de vol ou de compromission des modèles biométriques transformés, les paramètres de transformation sont modifiés pour mettre à jour le modèle biométrique protégé. Des paramètres de transformation distincts, voire des fonctions de transformation différentes, doivent être appliqués à chaque application afin d'empêcher les imposteurs de suivre les utilisateurs autorisés (utilisateurs légitimes) enregistrés dans de nombreux systèmes et de préserver ainsi la vie privée.
Ces approches sont résumées comme suit (Figure 3.4) : supposons que lorsque X est enregistré, il sera traduit en données codées T à l'aide d'une fonction F. La requête biométrique Y sera traduite en T' à des fins de vérification, toujours à l'aide de la fonction F, et l'authentification sera réussie si T est proche de T' à l'aide d'une certaine mesure de similarité. Pour garantir la révocabilité du système, chaque utilisateur U se voit attribuer une donnée aléatoire S sous la forme d'une clé. La fonction de transformation F utilise alors la clé S comme argument d'entrée. Cette clé d'utilisateur sera directement remplacée si elle est révoquée.

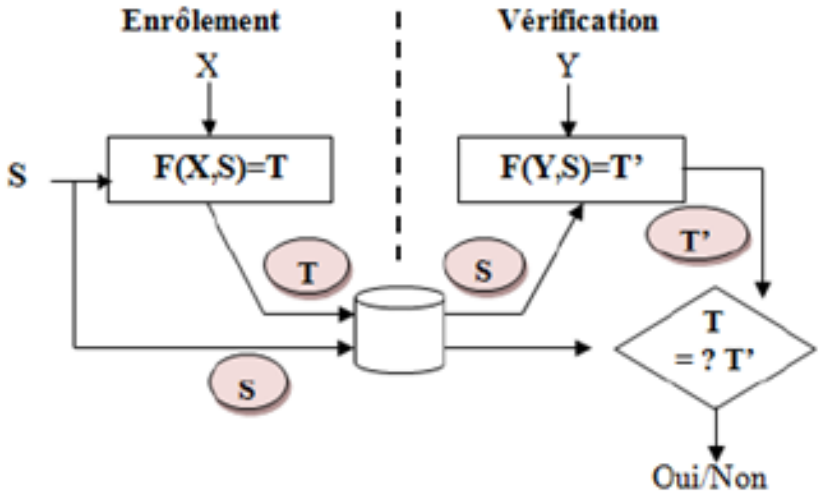


FIGURE 3.4 – *Le fonctionnement générique des transformations révocables*

Il s'agira d'un mécanisme de salage avec une transformation qui mélange X avec des données aléatoires créées à partir de S.
S, quant à lui, est le grain *seed* d'un générateur pseudo-aléatoire. *Salting* (également connue sous le nom de Biohashing) et *la transformation non-inversible* [Jain *et al.* 2008] [Rathgeb & Uhl 2011] sont les deux types de schémas de transformation de caractéristiques. [Pillai *et al.* 2010]décrivent le Biohashing comme une technique à deux facteurs basée sur la projection aléatoire. Il s'agit d'une stratégie de projection de modèles biométriques dans d'autres domaines ou espaces à l'aide de matrices orthogonales aléatoires tout en conservant les distances entre les modèles avant et après la transformation.
Le principe de base du Biohashing est la projection aléatoire, qui a été proposée comme une méthode autonome pour la protection des modèles biométriques visant à résoudre la propriété de révocabilité. Le principe de base du Biohashing est de créer un BioCode binaire (utilisé pour l'inscription et la vérification) en utilisant une représentation des données biométriques (comme les paramètres de texture ou les minuties pour les empreintes digitales) et un nombre aléatoire. Cette procédure est utilisée à la fois pour l'inscription de l'utilisateur (où seul le BioCode produit est conservé) et pour la vérification (où le BioCode est recalculé à chaque vérification et nécessite un stockage sécurisé du caractère aléatoire). Une distance de Hamming de base entre le BioCode de référence et le BioCode généré est utilisée pour calculer le résultat de la vérification. Cette stratégie est intéressante car elle permet de révoquer le BioCode (en utilisant un autre nombre aléatoire) et même de le diversifier. Pour s'authentifier auprès de différents services, il peut être intéressant de produire des BioCodes distincts à partir des mêmes données biométriques (par exemple, l'empreinte digitale). La procédure complète est décrite dans la Figure 3.5 [Belguechi *et al.* 2011].

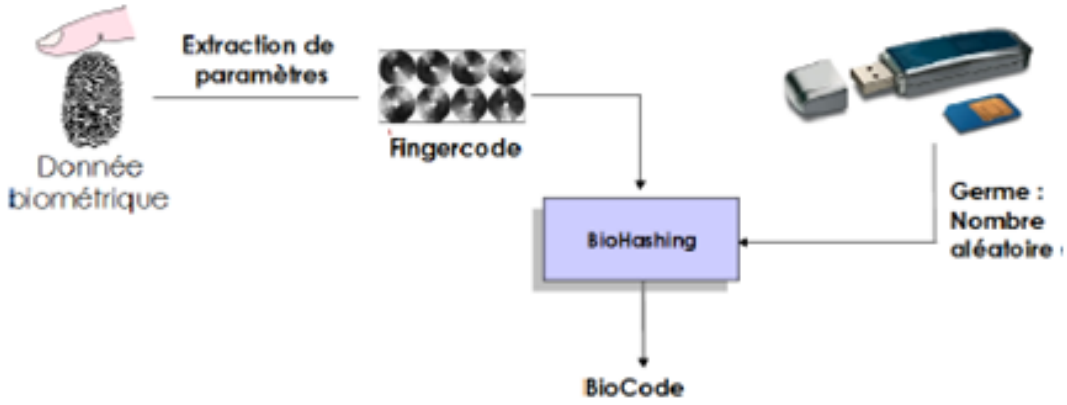


FIGURE 3.5 – *Schéma général de protection d'une donnée biométrique*

La méthode en question consiste à projeter les données biométriques (normalisées) sur une base orthonormée dérivée de l'aléa. La dimension résultante est au plus égale à la dimension de représentation des données biométriques. Dans cette situation, cette phase consiste à dissimuler les données biométriques dans une zone spécifique. Comme établi par le lemme de Johnson-Lindenstrauss, les connexions de similarité entre deux données biométriques projetées peuvent être assurées par l'emploi d'une base orthonormale (voir référence [Dasgupta & Gupta 1999]). La deuxième étape vise à quantifier cette découverte en utilisant un seuil de base comme point de départ. Par conséquent, cette étape assure la non-réversibilité du processus (retrouver les données biométriques initiales à partir du BioCode) ainsi que sa robustesse (permettre des différences mineures dans le vecteur projeté inhérent à la collecte des données biométriques). La Figure 3.6 [Belguechi *et al.* 2011]résume le principe général.

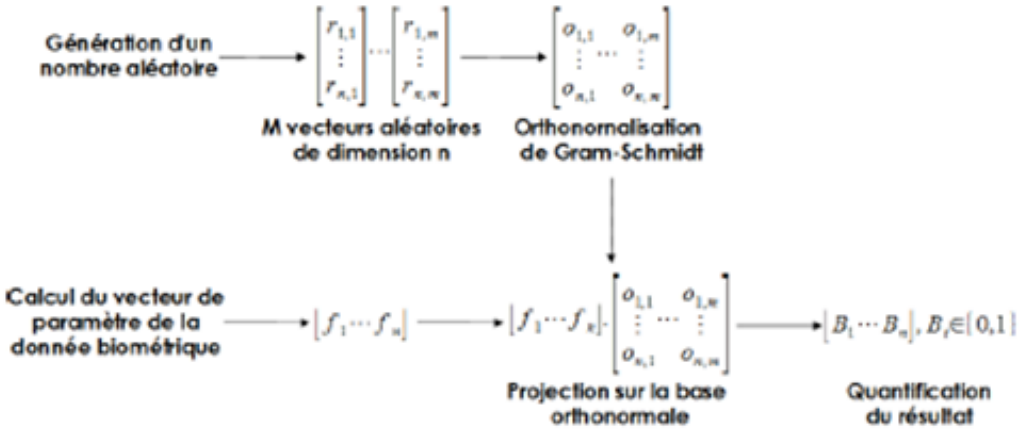


FIGURE 3.6 – *Description du procédé de génération d'un BioCode avec la méthode de Ratha*

Cette technique garantit que le BioCode ne peut pas être utilisé pour récupérer la biométrie originale. Le BioHashing est une approche générique pour révoquer les données biométriques, comme décrit ci-dessus. [Belguechi *et al.* 2011] l'ont appliquée à de nombreuses modalités biométriques.

Dans le cas de transformations non-inversables (la deuxième catégorie d'approches de transformation de caractéristiques). Un modèle original peut être sécurisé dans la plupart des cas en utilisant une caractéristique non-invertible [4], qui est une caractéristique à sens unique dans la plupart des travaux [Rathgeb & Uhl 2011]. Le principe de la transformation non-inversable (également connu sous le nom de biométrie révocable) a été initialement proposé dans la littérature par [Ratha *et al.* 2001]. (Il a été nommé *Cancelable biometrics*dans [Bolle *et al.* 2002]). L'un des aspects les plus essentiels de cette catégorie est qu'il est impossible de restaurer le modèle original même si la clé et/ou le modèle modifié sont connus / pris par un adversaire (en termes de complexité de calcul). Les modèles biométriques sont correctement protégés dans ce scénario.
Dans le contexte de la transformation irréversible, l'un des types les plus importants de la fonction de transformation est l'utilisation de distorsions ou de changements géométriques pour protéger les modèles biométriques [Ratha *et al.* 2006], [Ratha *et al.* 2007]., Selon la modalité biométrique utilisée, ces transformations diffèrent pour chaque système. Une transformation géométrique contrôlée par divers paramètres est appliquée aux photos d'inscription comme principe de base (les images transformées sont ensuite traitées par la méthode standard du système d'extraction de caractéristiques pour construire les modèles de référence). La même modification doit être apportée aux images de test lors de l'authentification/identification, sinon elles ne correspondront pas aux images de référence. En effet, pour répondre aux exigences de révocabilité/diversité, ces transformations doivent satisfaire à la contrainte selon laquelle de nombreux modèles résultant de distorsions distinctes ne doivent pas se superposer les uns aux autres.
Les paragraphes suivants présentent un survol sur les formes les plus significatives dans l'état de l'art de cette catégorie :
En 2006 ***Nanniand et Lumini*** [Nanni & Lumini 2006] Étudient comment combiner le BioHashing dans une approche de fusion multimodale basée sur l'intégration des données de visage et d'empreinte digitale ; Comment combiner le BioHashing et les fonctionnalités d'Iris spécifiques à l'utilisateur. Les résultats de cette approche confirment qu'une biométrie multimodale peut surmonter certaines des limites d'une biométrie unique, ce qui entraîne une amélioration substantielle de la performance. En outre, ils montrent qu'un système multi-matcher basé sur la fusion entre les fonctionnalités "BioHashed" Iris et un "standard" Iris matcher permet d'obtenir une bonne performance lorsqu'un "imposteur" vole les nombres pseudo-aléatoires et un EER près de 0 ,notez quand personne ne vole les nombres pseudo-aléatoires.
Jeong et al [Jeong *et al.* 2006]Combinent deux méthodes d'extraction de caractéristiques différentes pour obtenir une biométrie révocable (cancelable) de visage . Les vecteurs de coefficients PCA et ICA extraits d'une image de visage d'entrée sont normalisés en utilisant leur norme. Les deux vecteurs normalisés sont brouillés au hasard et un nouveau vecteur de coefficient de visage transformé (modèle transformé) est généré par l'addition des deux vecteurs normalisés. Lorsqu'un modèle transformé est compromis, il est remplacé par l'utilisation d'une nouvelle règle de brouillage. Parce que le modèle transformé est généré par l'addition de deux vecteurs, les coefficients PCA et ICA d'origine ne peuvent pas être récupérés à partir des coefficients transformés.
Une autre fois, le Biohashing utilise d'autres modalités biométriques, telles que l'empreinte digitale, la forme de la main et le visage par ***Teoh et al***

4. L'invisibilité peut être exprimée en termes de la complexité de calcul et le nombre d'essais pour récupérer un modèle original à partir un modèle transformé.

[Teoh *et al.* 2008]Dans cette approche, l'ensemble de projection aléatoire quantifié basé sur le lemme Johnson-Lindenstrauss est utilisé pour établir les fondements mathématiques de BioHashing. Sur la base de ce modèle, ils expliquent les caractéristiques de BioHashing dans la reconnaissance des modèles aussi bien que des points de vue de sécurité et proposent de nouvelles méthodes pour remédier au problème de vol qualifié.
Maiorana et al [Maiorana *et al.* 2011] ont proposé une approche pour protéger la signature en ligne a base du système de reconnaissance biométrique , où la biométrie considérée est sécurisée en appliquant un ensemble de transformations non inversibles, générant ainsi des modèles modifiés à partir desquels la récupération de l'information originale est aussi difficile que de la deviner. Les résultats expérimentaux rapportés, évalués sur la base de données de signature MCYT publique, montrent que les taux de reconnaissance réalisables ne sont que légèrement affectés par le plan de protection proposé, qui est capable de garantir la sécurité et la renouvelabilité souhaitées pour la biométrie considérée.
En 2012, ***Paul et Gavrilova*** [Paul & Gavrilova 2012] Les auteurs ont abordé le problème de l'annulation de la biométrie multimodale et présentent une nouvelle solution pour la biométrie révocable dans le système multimodal. ILS développent un nouvel algorithme de génération de modèle révocable biométrique utilisent la projection aléatoire et une transformation basée sur l'extraction et la sélection de caractéristiques . La performance de l'algorithme proposé est validée sur la base de données multimodales visage et oreille.
Dans l'approche ,***Canuto et al*** [Canuto *et al.* 2013] une étude spécifique de performance de différentes approches de fusion dans le contexte de la reconnaissance de la multibiométrie révocable. Dans cette enquête, ils ajustent l'ensemble de structure à utiliser pour un système biométrique et ils utilisent comme exemples deux modalités biométriques différentes (données vocales et iris) dans un contexte multibiométrie, en adaptant trois transformations révocable pour chaque modalité biométrique.
Tandit que ***Rathgeb et Busch*** [Rathgeb & Busch 2014], Dans leurs travail, des transformations adaptables à base de filtre Bloom sont appliquées afin de mélanger les modèles biométriques d'iris binaires au niveau des caractéristiques, où les codes iris sont obtenus à partir des deux yeux d'un seul sujet. La transformation de mélange irréversible, qui génère des modèles sans alignement, les informations cachées présentent dans différents codes iris. De plus, la transformation est paramétrée afin de réaliser la non-mobilité, la mise en ouvre de multi biométrie révocable . Les expériences réalisées sur la base de données IISD Iris version 1.0 confirment la solidité de l'approche proposée, (1) le maintien de la performance biométrique à des taux d'erreur égaux inférieurs à 0,5% pour différentes méthodes d'extraction de caractéristiques et scénarios de fusion et (2) la réalisation d'une compression de modèles mixtes jusqu'à 10% de taille d'origine.
En 2015,***Sushma et Sandeep*** [Sushma & Sandeep 2015] deux méthodes ont été utilisées pour extraire les caractéristiques de l'image, à savoir : 1) filtre Gabor et 2) techniques de projection aléatoire (RP). Dans la méthode d'extraction des caractéristiques de filtre Gabor, les filtres log-Gabor en ondelette sont convolés avec une image biométrique normalisée pour extraire des vecteurs de code de caractéristique. Où, comme dans la méthode RP, les matrices aléatoires sont multipliées par une image biométrique normalisée afin d'extraire des vecteurs de code de caractéristiques. Les multiples caractéristiques sont fusionnées à l'aide d'un non inversible adaptatif de filtre Bloom pour protéger le modèle biométrique.

Rathgeb et al [Rathgeb *et al.* 2015] Ont proposé un cadre générique pour générer une représentation irréversible de multiples modèles biométriques basés sur des filtres Bloom adaptatifs. La technique présentée permet une fusion au niveau des caractéristiques de différentes données biométriques (visage et iris) à un seul modèle protégé, améliorant la protection de la vie privée par rapport aux systèmes correspondants basés sur un seul trait biométrique. Dans le même temps, un gain significatif de la performance biométrique est atteint, confirmant la solidité de la technique proposée.
Damasceno et al [Damasceno *et al.* 2015] ont évalué un système de protection multibiométrique de la vie privée utilisant des ensemble de systèmes. L'ensemble de systèmes, également appelés systèmes multi-classificateurs ou fusion d'experts. Le système multi-confidentialité combine l'utilisation multi-algorithmes et d'échantillons biométriques protégés. Quatre transformations révocables (Interpolation, BioHashing, BioConvolving et Double Sum) ont été utilisées pour protéger une modalité comportementale (TouchAnalytics). Cependant, les auteurs utilisent plusieurs algorithmes de correspondance ou de similarité. L'EER de Biohashing, 28,6% dans le meilleur des cas (BioCBioH). Cette approche a des inconvénients a l'utilisateur parce que l'individu doit présenter plus d'une clé pour coder son échantillon biométrique lors de la vérification. En 2016 ,***Stokkenes et al*** [Stokkenes *et al.* 2016] Dans leurs travail, un système protégé par un modèle multi-biométrique est proposé, basé sur les filtres Bloom et les fonctionnalités d'image statistique binarisées (BSIF). Les caractéristiques sont extraites du visage et des deux régions périoculaires et des modèles protégés à l'aide des filtres Bloom. La fusion au niveau de score est appliquée pour augmenter la précision de la reconnaissance. Le système est testé sur une base de données, composée de 94 sujets d'images collectées avec des smartphones. Une comparaison entre les modèles non protégés et les modèles protégés dans le système montre la faisabilité de la méthode de protection du modèle avec un taux de correspondance authentique (GMR) observé de 95,95% pour les modèles non protégés et 91,61% à un tarif de fausses correspondances (FMR) de 0,01%. L'irréversibilité et la non-compatibilité du système sont analysées en fonction d'un cadre d'évaluation de la sécurité récemment publié. En 2017 , ***Yildiz et al*** [Yildiz *et al.* 2017] Ont présenté un système d'authentification biométrique qui construit un modèle multi-biométrique en superposant plusieurs données biométriques d'un utilisateur, de sorte qu'il est difficile de séparer les couches individuelles. Ainsi, le systéme utilise la biométrie de l'utilisateur pour les dissimuler entre eux. Le modèle biométrique résultant est également révocable (en anglais cancelable) si le système est implémenté avec une biométrie révocable , comme la voix. ils présentent une réalisation de cette idée combinant deux ou trois empreintes différentes de l'utilisateur, ils utilisent quatre méthodes différentes de construction de modèles. Trois des méthodes utilisent de plus en plus d'informations sur la biométrie constitutive, de manière à réduire le risque de fuite et les taux de réticulation. Les résultats sont évalués sur les bases de données d'empreinte degitale Finger Verification Championship (FVC) 2000, 2002 et NIST accessibles au public. Avec les bases de données FVC, ils obtiennent un taux d'erreur EER égal à 2,1%, 3,9% et 3,4%, ils utilisent les trois méthodes proposées, tandis que l'etat de l'art du système commercial atteint 1,9%. En outre, ils affichent des taux de réticulation bas de moins de 63% dans différents scénarios, alors que les taux d'identification authentiques sont de 100%, avec une petite galerie de 55 modèles. ***Bringer et al*** [Bringer *et al.* 2017]Ont développé une analyse de non-lisibilité et d'irréversibilité de soi-disant le filtre Bloom a base de la protection de gabarit biométrique d'iris

introduite dans ***Ratheb et al***[Rathgeb & Busch 2014].Tout d'abord, ils analysent la non-capacité sur les modèles protégés à partir de deux codes d'iris différents provenant du même iris. En outre, ils introduisent une analyse d'irréversibilité qui exploite la non uniformité des données biométriques. Son expériences démontrent de nouvelles vulnérabilités de ce schéma. Ensuite, ils discuteront de la sécurité de d'autres modèles biométriques protégés similaires basés sur des filtres Blooms qui ont été suggérés dans la littérature depuis 2013. En fin, ils proposent un protocole du calcul multipartite sécurisé (SMC), qui bénéficie de la fonctionnalité sans alignement de cette construction de filtre Bloom, Afin de calculer efficacement et en toute sécurité les scores correspondants [Bedad & Adjoudj 2018a].
En 2019 , [Bokade & Kanphade 2019] Ont présenté un système qui propose une méthode de concaténation de vecteurs de caractéristiques de dimension réduite pour trois traits biométriques comme le visage, l'empreinte palmaire et l'oreille. L'utilisation d'un seul algorithme d'analyse en composantes principales pour l'extraction de caractéristiques et de distance euclidienne pour l'appariement final rend le système robuste en réduisant la complexité de calcul. Le modèle biométrique résultant est également protégé en utilisant le mélange de schémas de vecteurs de caractéristiques. Tandis que [Walia *et al.* 2020], proposent un système biométrique revocable multimodal basé sur la Deep Feature Unification (DFU) en temps réel. Pour cela, une extraction de caractéristiques génériques basée sur des images clés est introduite pour obtenir la révocabilité et la réduction de la dimensionnalité. La non-inversibilité est obtenue par projection aléatoire des fonctionnalités Key Deep vers les fonctionnalités Query Deep. Le processus de fusion adaptatif proposé basé sur des graphes extrait non seulement des informations complémentaires sur plusieurs modalités, mais génère également un modèle unifié multimodal. La diffusion croisée de graphes normalisés et optimaux assure la dissociation et la robustesse à l'environnement dynamique. Le système biométrique proposé est évalué sur des ensembles de données de référence et montre des performances prometteuses par rapport aux méthodes de pointe. Dans la même année, [Sharma & Selwal 2020] ont décrit un nouveau schéma de hachage basé sur le code régional (RCHTSS) pour la protection des modèles dans un système biométrique multi-instance est présenté. Le RCHTSS utilise deux instances de la modalité biométrique des empreintes digitales, c'est-à-dire les images de l'index de la main droite et de la main gauche. Dans le cas de l'étape d'inscription, les images d'empreintes digitales acquises à partir des dispositifs de détection sont utilisées pour extraire des caractéristiques locales de minutie à l'aide d'un module d'extraction de caractéristiques biométriques (FE). Le RCHTSS utilise des codes de région locaux pour convertir le vecteur de caractéristiques à valeur réelle (FV) de l'image d'empreinte digitale pour la protection. Le RCHTSS utilise une fusion de niveau de score d'appariement pondéré pendant l'authentification avec des performances de reconnaissance plus élevées à un poids de =0,5. En 2021 , [Gupta *et al.* 2021] proposent un système biométrique multimodal révocable qui combine plusieurs traits au moyen d'une approche basée sur la projection. L'approche proposée génère une caractéristique biométrique annulable qui est utilisée pour obtenir des modèles révocables et non inversibles. Les caractéristiques annulables sont générées en projetant les points caractéristiques sur un plan aléatoire obtenu à l'aide d'une clé spécifique à l'utilisateur. Le point de projection est ensuite transformé en coordonnées cylindriques et une caractéristique combinée annulable est obtenue. Des expériences approfondies sont réalisées sur 3 bases de données multimodales chimériques et les résultats révèlent des performances élevées.En outre, la méthode proposée est analysée avec succès pour les

problèmes de confidentialité, à savoir la révocabilité, la non-inversibilité et la dissociabilité. De plus, le système proposé a fait preuve de tolérance contre diverses attaques de sécurité telles que les attaques par force brute, les attaques via une multiplicité record et les attaques de substitution. **Discussion** Nous avons illustré différentes approches de transformation révocable. Bien que ces méthodes, tout en utilisant des fonctions de transformation dans leurs principes, se rejoignent aux points suivants :

- En premier lieu, leur objectif commun consiste à empêcher le stockage du modèle biométrique original et idéalement, être en mesure de procéder à une reconnaissance fiable dans le domaine de la transformation.
- Elles sont utilisées pour révoquer et générer un nouveau modèle de référence La principale raison en est l'introduction d'une clé utilisateur autorisant cette diversification du modèle à partir de la même modèle biométrique.
- Pour cette raison, la sécurité de Biohashing est fondée exclusivement sur le secret de la clé Ainsi, comme la transformation est réversible, la clé doit être conservée en toute sécurité par le système et aussi par l'utilisateur pour la présenter lors de la vérification. Cette nécessité d'informations supplémentaires sous la forme d'une clé permet d'accroître la diversité des modèles biométriques et de les faire plus difficilement déchiffrer par un adversaire.
- L'algorithme de Biohashing a plusieurs avantages [Jain *et al.* 2008]. Comme la clé est spécifique à chaque utilisateur, nous pouvons générer plusieurs modèles biométriques (à partir du même utilisateur) en utilisant des clés différentes. Ce système permet également la révocabilité, car si un modèle est compromis, il est facile de le révoquer et de le remplacer par un nouveau modèle à l'aide d'une nouvelle clé utilisateur. Il est important de se rappeler que la clé utilisateur n'offre pas seulement la diversité / révocabilité, en plus d'améliorer la performance de la reconnaissance [Maltoni *et al.* 2003, A. K. Jain 2007].
- L'objectif principal du Biohashing est d'augmenter la taille du BioCode (plus il est grand, moins une attaque de force peut se produire) et d'augmenter l'efficacité. Étonnamment, la question de la protection des données biométriques a souvent été abordée par le biais de la performance (minimisation du taux d'erreur et maximisation de la taille du BioCode) [Belguechi *et al.* 2011].
- Ils peuvent transformer de petites différences de position entre deux points caractéristiques (deux minuties) de l'espace d'origine en grandes différences dans l'espace de transformation (augmentation des variations intra-sujet), ce qui peut conduire à un grand nombre de faux rejets. Par conséquent, ces chercheurs ont conseillé d'utiliser des transformations lisses pour prévenir ce problème et préserver les performances.
- En dernier lieu, le point culminant du projet réside dans la capacité d'effectuer une analyse rigoureuse de la sécurité des méthodes proposées. De nos jours, aucune méthode formelle ou normalisée n'existe encore. Cette situation représente un véritable problème.
- En général, ces méthodes sont sensibles aux attaques courantes lesquelles la recherche devra couvri. Parmi ceux-ci, notons le vol de la clé utilisateur.(Le niveau de FAR est dans ce cas suffisamment élevé pour une application sûre de la méthode).Par ailleurs, en fonction des méthodes présentées, la transformation peut être fréquemment inversée (partiellement ou totalement) si tous les paramètres sont connus sous la clé S et le modèle de transformation

3.3.3 Approches hybrides

Une approche hybride de la sécurisation des modèles multibiométriques consiste à protéger le modèle en se basant sur plus d'une des quatre approches principales (biohashing, transformation non inversible, liaison par clé cryptographique et génération de clé cryptographique). L'objectif de cette stratégie hybride est de combiner les avantages de plusieurs mécanismes de protection de base tout en minimisant leurs inconvénients. Karthi et Azhilarasan [Karthi & Azhilarasan 2013]utilisent un système cryptographique pour générer des clés et un mécanisme de transformation des caractéristiques dans le système qu'ils proposent (biométrie révocable). Cette méthode a permis de surmonter la limitation de la transformation des caractéristiques. Ces stratégies se concentrent sur l'utilisation de l'iris et des empreintes digitales comme attributs (c'est-à-dire la biométrie multimodale). Lorsque la biométrie du système cryptographique (CSB) et la biométrie révocable sont utilisées ensemble, les résultats démontrent l'absence de dégradation (RB). Suzwani et al. [Ismail *et al.* 2015]ont présenté une autre technique hybride. Les modèles multi-biométriques basés sur les systèmes révocables et le schéma FuzzyCommitment de l'iris droit et gauche d'un seul individu seront employés comme modèles d'entrée pour la sécurisation. Pour tester la résilience du système proposé, l'expérience sera réalisée en utilisant la base de données CASIA-v3 sur l'iris. Cette étude devrait prouver que l'approche de protection hybride suggérée peut répondre à toutes les exigences de protection des modèles sans diminuer les performances de reconnaissance de l'iris [Bennaceur & Bedad 2019]. Une nouvelle technique de deepl learning a été introduit par [Arora *et al.* 2020] en 2020 ,pour fusionner les caractéristiques extraites du visage et de l'iris de l'individu (gauche et droite) pour obtenir un système de vérification biométrique plus sécurisé. Tout d'abord, ils extraient séparément les caractéristiques du visage et de l'iris à l'aide de divers modèles de réseaux de neurones convolutifs (CNN). De plus, les vecteurs de caractéristiques des couches CNN finales des deux modèles sont fusionnés pour obtenir une classification des individus avec des performances améliorées. Le système proposé est testé sur la base de données CASIA-Face V5 pour les visages et la base de données d'iris IITD pour les iris gauche et droit. Les résultats obtenus prouvent la supériorité du système multimodal proposé. Il est efficace, fiable et robuste. En 2021, [Atanda *et al.* 2021] ont présenté un système de sécurité biométrique multimodal qui utilise un CNN modifié (CNN-GA) pour l'extraction et la classification des caractéristiques a été développé. Le système a été testé sur une base de données composée de 1026 images entraînées et de 684 images de sonde biométriques du visage, de l'oreille et de l'iris. Le résultat montre qu'à des valeurs de seuil variables de 0,20, 0,35, 0,50 et 0,76, le CNN-GA surpasse le CNN standard appliqué au système développé en termes de sensibilité, spécificité, précision, précision de reconnaissance et temps. À la valeur seuil de 0,76, CNN-GA a atteint une sensibilité de 97,66%, une spécificité de 98,25 %, une précision de 99,40%, une précision de reconnaissance de 97,81% et un temps de reconnaissance de 455,54 secondes tandis que le CNN standard a atteint une sensibilité de 95,91%, une spécificité de 92,98%, précision de 97,62%, précision de reconnaissance de 95,18% et temps de reconnaissance de 565,02 secondes.

3.4 CONCLUSION

Nous avons pu constater deux grandes familles de solutions après avoir souligné la nécessité de protéger le modèle multi-biométrique. Les solutions basées sur le système cryptographique multi-biométrique et la transformation réversible sont les plus courantes. L'état de l'art des techniques de protection du système multi-biométrique a été donné dans ce chapitre. Nous avons commencé par décrire cette solution, qui cherche principalement à dissimuler les données biométriques. Nous nous sommes ensuite intéressés aux méthodes révocables, qui tentent de protéger les modèles biométriques en appliquant des fonctions de transformation, avec un accent particulier sur les techniques de biohashing.
De nos jours, la question de la biométrie révocable est un sujet de grande importance. Bien que des recherches aient été menées ces dernières années pour suggérer des systèmes de protection des données multi biométriques, très peu de travaux ont porté sur la sécurité et la robustesse des protocoles. Cependant, cela est essentiel dans un domaine comme la biométrie qui vise la manipulation de données de caractère très confidentiel. C'est le but du chapitre suivant.

4 Étude de la robustesse de La biométrie révocable :BioHashing

Sommaire

4.1 Introduction

Lorsque les informations d'un modèle multi biométrique d'un utilisateur tombent entre les mains d'un adversaire, elles peuvent gravement compromettre la sécurité (menaces d'intrusion) du système multi biométrique et la confidentialité (menaces de liaison) de l'utilisateur. Par conséquent, la protection des modèles multi biométriques est un problème critique qui doit être résolu pour améliorer l'acceptation de la technologie multi biometrique par le public.
Compte tenu de l'augmentation récente du nombre de techniques développées pour protéger les modèles multi biométriques, il est essentiel de développer un ensemble de mesures permettant d'évaluer la force de ces techniques. L'une des approches bien connues pour la protection des données multi biométriques est la technique de transformation de modèle ou de caractéristique. Comparés aux systèmes de cryptographie multi biométriques, les schémas de transformation de gabarit présentent certains avantages, comme la facilité de révocabilité et la flexibilité dans la conception du matcher et l'intraçable.Mais ces avantages sont contrecarrés par l'absence d'une analyse approfondie de la sécurité de ces techniques.
Dans cette partie nous avons contribué par une étude d'un certain nombre de métriques. La métrique est l'élément principal d'un processus d'évaluation. Dans ce cadre, une métrique sert à produire des valeurs qui permettent de comparer les différents schémas par rapport aux critères à évaluer pour tester la robustesse et ainsi analyser la sécurité des méthodes de transformation inversible comme notre cas en prenant comme exemple la méthode de biohashing.
Une étude de la solidité du BioHashing permet de déterminer la capacité du système face à un ensemble d'attaques visant les données biométriques du client et la sensibilité du BioHashing aux divergences intrusives.
La référence de Nagar et al[Nagar *et al.* 2010a]analyse les risques d'inversibilité et de traçabilité dans le BioHashing.
Dans ce chapitre, nous étudions formellement la force de sécurité des techniques de transformation de gabarit et définissons les sept métriques qui facilitent une évaluation de sécurité holistique.

4.2 Exigences de sécurité et de protection de la vie privée

Un système multi biométrique agir, par définition, des données personnelles sensibles des individus. Ces données doivent être protégées pour éviter le vol, leur modification ou la torture [Barbier & Rosenberger 2014] Un processus général d'évaluation des transformations révocables présenté par [Nagar *et al.* 2010a] , ou les critères potentiels à évaluer peuvent être classés comme suit :

— **Critères concernant la sécurité**

1. Les risques díntrusion.
2. La révocabilité et le renouvellement.
3. Le contrôle de confidentialité : ce critère peut être assimilé aux deux critères d'irréversibilité et de divulgation partielle de l'information biométrique.

— **Critères concernant la préservation de la vie privée**

1. Irréversibilité.
2. Divulgation partielle de l'information biométrique (privacy leakage).

3. Intraçabilité.
4. Diversité.

Ces critères sont maintenant définis de manière plus formelle dans le cadre des transformations révocables.

4.3 Définitions et propriétés

Nous supposons avoir une modalité biométrique où le modèle est représenté par un vecteur de valeurs réelles ; ce qui est une hypothèse réaliste, puisqu'il peut être généralisé à toute représentation comme un axe intéressé.
Nous utilisons les notations suivantes comme dans l'article de Nagar et al. [Nagar *et al.* 2010a] :

— Soit b_z et $b_z^{'}$, représentant respectivement, le modèle et les caractéristiques biométriques de l'utilisateur z.
— Soit f la fonction de transformation . Nous notons n la dimension du résultat (biocode) de $f(b_z)$ pour l'utilisateur z.
— Soit K_z, l'ensemble des paramètres de la transformation correspondant à l'utilisateur z.
— Soit D_O désigner une fonction de distance entre les caractéristiques biométriques dans le domaine non traduit (original) et D_T une fonction de distance dans la transformation.

Le système biométrique révocable produit une décision de vérification indiquée R_z si la la distance entre le biocode de référence et le biocode de requête est inférieure à un seuil ϵ Désigné comme suit :

$$R_z = 1_{\{D_T(f(b_z,K_z),f(b_z^{'},K_z))\leq\epsilon\}} \tag{4.1}$$

Très peu d'ouvrages ont été consacrés à l'évaluation de tels systèmes biométriques dans la littérature [Adler 2007] ,[Nagar *et al.* 2010b] , [Zhou *et al.* 2009] . L'ISO / CEI 24745 « Technologies de l'information - Techniques de sécurité - Protection de l'information biométrique » définit les propriétés de sécurité d'un système biométrique, nous utilisons les mêmes termes. Les systèmes annulables doivent remplir plusieurs propriétés, comme mentionné également dans [Maltoni *et al.* 2003] :

1. **Risque d'intrusion (performance) :**
   La protection du modèle ne doit pas détériorer la performance de l'original système biométrique . En effet, la performance est directement liée à la sécurité du processus d'authentification (par exemple, minimiser le nombre de fausses acceptations),un système biométrique révocable doit être aussi efficace que possible.
   Pour évaluer l'efficacité d'un système biométrique (sans transformation), nous considérons généralement deux mesures d'erreur suivantes :

$$FRR_O(\epsilon) = P(D_O(b_z, b_z^{'}) \leq \epsilon); \tag{4.2}$$
$$FAR_O(\epsilon) = P(D_O(b_z, b_z^{'}) > \epsilon). \tag{4.3}$$

   Où FRR_O est le taux faux de rejet et FAR_O est le taux de fausse acceptation du système biométrique d'origine (sans aucune protection de modèle). Pour

le système avec protection, nous considérons les deux paramètres suivants définies selon Nagar et al[Nagar *et al.* 2010a] .

$$FRR_T(\epsilon) = P(D_T(f(b_z, K_z), f(\acute{b_z}, K_z)) \leq \epsilon); \tag{4.4}$$

$$FAR_T(\epsilon) = P(D_T(f(b_z, K_z), f(\acute{b_z}, K_z)) > \epsilon). \tag{4.5}$$

Où FRR_T est le taux faux de rejet et FAR_T est le taux de fausse acceptation du système biométrique révocable (avec la protection du modèle).

2. **Révocabilité/Renouvellement :**
Il devrait être possible de révoquer le modèle transformé et de générer un nouveau modèle à partir des mêmes données d'origine. Compte tenu du modèle biométrique de l'utilisateur z ,grâce à un système biométrique révocable basé sur la transformation,Il est possible de calculer le modèle $f(b_z, {K_z}^1)$ en utilisant les paramètres ${K_z}^1$et de le révoquer en le remplaçant $f(b_z, {K_z}^2)$ par l'introduction d'un autre ensemble de paramètres ${K_z}^2$. Comme le seul biocode de référence est stocké, la révocabilité peut être facilement réalisée.
3. **Irréversibilité et divulgation partielle de l'information biométrique :**
Il ne devrait pas être possible d'obtenir, à partir du modèle transformé, suffisamment d'information sur la biométrie d'origine (modèle ou échantillon biométrique). Cela assure la confidentialité de la donnée biométrique et prévient des attaques consistant à falsifier la biométrie à partir d'un modèle compromis ou volé. Quelque soit le processus d'inversion, l'imposteur aura une information A_z qui peut l'authentifier comme l'utilisateur légitime [Belguechi 2015] . Le succès de l'attaque est donné par :

$$FAR_A(\epsilon) = P(D_T(f(b_z, K_z), A_z) \leq \epsilon). \tag{4.6}$$

4. **Intraçabilité/Diversité :**
Il devrait être possible de générer différents biocodes pour plusieurs applications, et aucune information ne doit être déduite de la comparaison ou de la corrélation entre différentes réalisations. Il s'agit d'une propriété importante pour les problèmes de confidentialité car il évite la possibilité de tracer un individu en fonction des informations d'authentification. Soit $B_z = \{f(b_z, {K_z}^1), .., f(b_z, {K_z}^Q)\}$, l'ensemble des Q modèles générés pour l'utilisateur z et ${K_z}^i$ l'ensemble des paramètres concernant l'utilisateur z par rapport à la ième révocation. B_z doit constituer un sous-ensemble aléatoire dans $\{0,1\}^Q$, Cette propriété empêche également l'attaque de liaison consistant à utiliser différents biocodes d'un utilisateur pour prédire un élément admissible. Ceci est lié à une attaque consistant en un impostor pour écouter différentes réalisations de biocodes pour le même utilisateur.

Ces propriétés sont bien connues et souvent citées dans des documents de l'état de l'art. Nous allons plus loin dans cette thèse : étant donné un système biométrique révocable, comment pouvons-nous vérifier si ces propriétés sont remplies ? Est-il possible de quantifier le risque associé à la faisabilité d'une attaque limitant l'une de ces propriétés ? Nous proposons dans la prochaine section, des mesures et des attaques pour répondre à ces deux questions.

4.4 Sécurité et analyse de confidentialité

Basé sur certains des premiers travaux [Ratha *et al.* 2001] ,[Bolle *et al.* 2002] qui ont identifié des liens faibles dans chaque sous-système d'un système

d'authentification générique, certains documents considérés les attaques possibles dans les systèmes biométriques révocables (tels que ceux présentés dans [Teoh *et al.* 2008] ,[Jain *et al.* 2008] ,[Nagar *et al.* 2010b] ,[Saini & Sinha 2011] . Nous suivons la maxime de Shannon ("L'ennemi connaît le système "), nous supposons donc que l'imposteur dispose de toutes les informations nécessaires sur le processus utilisé pour générer le biocode (méthode de génération de fonctionnalité, taille de biocode ...).
Notez que l'étude suivante exige que le seuil de décision ϵ doit être fixé . Dans cette thèse, nous définissons le seuil de décision ϵ_{EER_T} à la valeur EER du système multi biométrique révocable (sans aucune protection de modèle). Même si ce point de fonctionnement du système multinbiométrique n'a aucun sens opérationnel, il est souvent utilisé et peut toujours être estimé. Vous pouvez utiliser d'autres valeurs différentes ϵ selon les exigences de sécurité de l'application. Afin de quantifier la robustesse du système multi biométrique révocable étudié, on suppose avoir une base biométrique avec plusieurs échantillons biométriques pour chaque utilisateur. Certains échantillons permettent de générer le modèle biométrique de chaque utilisateur tandis que les autres sont utilisés pour les tests. Ainsi, la détermination des critères à évaluer est une étape nécessaire pour aider au choix cohérent des métriques. Ces points peuvent être communs à tous les algorithmes de protection.
L'analyse de la sécurité et de la vie privée peut être effectuée pour les deux étapes classiques de la biométrie. Nous nous concentrons d'abord sur un problème d'authentification (un contre un correspondant) : nous développons différents scénarios d'attaque qu'un intrus réussirait à se faire passer un authentique utilisateur particulier. Dans une deuxième étape, l'identification (une contre plusieurs correspondances) problème est considérée. Dans ce cas, l'imposteur essaie de se faire passer pour l'un des individus dans la base de données.

4.5 Détermination des métriques

Nous proposons un ensemble de métriques $A_i \in [0,1]$, $i = 1, \ldots, 7$

4.5.1 Authentification

— **Critères sur les risques d'intrusion (performance) :**

1. Dégradation des performances(A_1) :
   Pour l'usage/le risque d'intrusion dans le système révocable nous considérons, respectivement, les mesures suivantes :

$$FRR_T(\epsilon) = P(D_T(f(b_z, K_z), f(\acute{b_z}, K_z)) \leq \epsilon); \tag{4.7}$$

$$FAR_T(\epsilon) = P(D_T(f(b_z, K_z), f(\acute{b_z}, K_z)) > \epsilon). \tag{4.8}$$

   Pour l'évaluation, il est commun de mettre le seuil de décision ϵ à la valeur (ϵ p) où FRRT (ϵ p) = FART (ϵ p). Dans ce cas, la métrique A_1, est considérée comme la valeur EER lorsque FRR_T (ϵ p) = FART (ϵ p).
   Pour vérifier si l'efficacité n'est pas diminuée par l'utilisation du système de protection par rapport au système biométrique d'origine, nous proposons de calculer la mesure suivante :

$$A_1 = 1 - \frac{\mathrm{AUC}(\mathrm{FAR_T}, \mathrm{FRR_T})}{\mathrm{AUC}(\mathrm{FAR_O}, \mathrm{FRR_O})} \tag{4.9}$$

Avec AUC (Area Under the Curve), l'aire sous la courbe ROC des deux systèmes avec et sans protection. De nombreux cas sont intéressants à considérer. Tout d'abord, il peut arriver que A_1 soit égale à o reflétant un système révocable parfait (sans erreur i.e. $EER = 0\%$). D'autre part, si la valeur A_1 est négative, cela signifie que l'efficacité du système biométrique est détériorée par le système de protection. Sinon, au contraire, la protection améliore les performances.

2. Irréversibilité et divulgation partielle de l'information biométrique (A_2 à A_5) :

   Cette propriété essentielle peut être évaluée à travers différentes attaques. Pour toutes ces attaques, nous utilisons un ou plusieurs échantillons biométriques pour générer une requête $\acute{b_z}$ admissible de l'utilisateur z.

   Sur la base du principe de chaque attaque, nous générons beaucoup de fausses tentatives A_z de l'utilisateur authentique (comme décrit dans l'équation 4.6) :

   — *Attaque à zéro effort* (A_2) :
   Dans ce scénario, l'imposteur tente d'usurper la véritable identité de l'utilisateur z en représentant ses propres données biométriques $\acute{b_y}$ avec des paramètres inconnus K_y. On aura alors : $A_z = f(\acute{b_y}, K_y)$.

   — *Attaque par force brute* (A_3) :
   Dans ce scénario, l'imposteur décide de suborner le module de protection en envoyant un modèle prêt à être comparé par le module de comparaison. Il estime aléatoirement différentes valeurs A de telle sorte que A : $A_z = A$.

   — *Attaque par vol de clé* (A_4) :
   L'imposteur a obtenu les paramètres K_z de l'utilisateur z et essaie différentes valeurs b pour générer : $A_z = f(b, K_z)$

   — *Attaque par vol de biométrie* (A_5) :
   L'imposteur obtient $\acute{b_z}$ (directement ou après avoir fait le calcul à partir d'un échantillon biométrique compromis comme la trace d'une empreinte par exemple). Il essaie différentes valeurs de K pour générer : $A_z = f(\acute{b_z}, K)$.

   Pour évaluer l'efficacité de ces quatre attaques, nous proposons de calculer pour chacune d'elles les critères suivants :

   $$A_i = FAR_A(\epsilon_{EER_T}),\ i = 2, \ldots, 5 \tag{4.10}$$

   En effet, du point de vue de l'imposteur, le FAR est la valeur pertinente : l'intrus doit générer $f(\acute{b_z}, K_z)$ en utilisant différentes données disponibles (K_z, $\acute{b_z}\ldots$).. Rappelons que le seuil a été fixé à la valeur ϵ_{EER_T} (obtenue par le calcul de EER du système biométrique révocable).
   Du point de vue de l'imposteur, les valeurs A_i, $i = 2, \ldots, 5$ doivent être aussi élevées que possible. La valeur obtenue pour chaque attaque A_i, $i = 2, \ldots, 5$ nous permet un classement des différentes attaques et donne directement le risque au système qu'un imposteur puisse être authentifié comme un véritable utilisateur.

3. Critère d'intraçabilité/diversité (A_6 à A_7) :
   Les attaques précédentes sont des attaques que l'on peut trouver dans la littérature. Nous allons présenter maintenant un type de métrique qui, à la

connaissance des utilisateurs. Il s'agit des métriques adaptées à la nature révocable du BioHashing :
Une caractéristique importante d'un système biométrique révocable est sa capacité à produire différentes références pour la même personne et pour différentes applications.
Dans ce contexte, la préservation de la vie privée repose sur le fait que ces références soient suffisamment aléatoires pour prévenir d'un possible lien entre elles. Nous commençons par proposer des métriques qui mesurent la complexité des attaques possibles.

— *Attaque par écoute (A_6, A_7) : :*
Un imposteur ne doit pas être en mesure d'extraire des informations de différents biocodes émis par le même utilisateur. Nous supposons qu'un intrus a intercepté N BioCodes distincts du même utilisateur b_1, ..,b_N. On génère alors, sur la base de ces Q écoutes, un BioCode dont les bits sont fixés à la valeur (0 ou 1) .
Ces attaques sont testées par le processus suivant :
— Génération de Q biocodes pour l'utilisateur z :
$B_z = \{f(b_z, {K_z}^1), .., f(b_z, {K_z}^Q)\}$
— Prédiction d'une valeur de biocode possible en fixant la valeur la plus probable de chaque bit donné B_z,
— Calcul de l'équation (4.10).
$\Rightarrow$ valeur A_6 pour $Q = 3$ et A_7 pour $Q = 11$

Ces critères permettent de quantifier la robustesse des systèmes de vérification multi biométrique révocable.

4.5.2 Identification

Pour l'identification, les propriétés sont les mêmes mais les critères de calcul sont légèrement différents. Premièrement, les valeurs A_i, $i = 1,6$ sont les mêmes pour les contextes d'authentification et d'identification. En ce qui concerne les propriétés de non-inversion et d'irréversibilité, l'équation (4.6) doit être modifiée pour :

$$FAR_A(\epsilon) = \max_z P(D_T(f(b_z, K_z), A_z) \leq \epsilon). \tag{4.11}$$

En effet, dans le cas d'identification, l'imposteur tente se faire passer l'identité de tous les individus dans la base de données. Les attaques sont similaires mais quantifiées d'une manière différente. Le calcul de A_i, $i = 2 : 5, 6 : 7$ est réalisé en considérant l'équation 4.11.
En conclusion de la méthodologie suivie, la sécurité et la robustesse d'un système multi biométrique révocable est caractérisées par un vecteur à 7 dimensions (A_i, $i = 1, \ldots, 7$). Le principal avantage de cette présentation quantitative est de permettre facilement la comparaison de systèmes multi biométriques révocable.

4.6 CONCLUSION

La principale contribution de ce chapitre est de définir une démarche expérimentale d'analyse de la robustesse des méthodes de protection des données multi biométriques en utilisons la biométrie révocable dans différents scénarios.
Nous avons présenté sept mesures différentes pour évaluer la sécurité des schémas de transformation révocable de gabarit.

Sur la base de ces métriques A_1,.., A_7 qu'on va les utiliser pour tester et comparer notre deux approches proposées.
Dans le chapitre suivant, nous présentons notre nouvelle schéma révocable des empreintes digitales.

Conception et réalisation 5

Sommaire

5.1 Introduction

Le développement d'un système de protection des données multi biométriques peut être envisagé à deux niveaux différents : la conception de système multi biométrique et la conception des algorithmes de protection mis en ouvre sur le système. En effet, la majorité des contraintes relevées au cours de la phase de développement de système sont en rapport avec le choix des modalités biométriques les mieux adaptées à l'environnement concerné, l'architecture générale de système, le champ des informations biométriques (base de données ou carte à puce ?) et le degré d'intégration des algorithmes de protection. Les autres choix sont notamment l'ergonomie de système ou les coûts d'administration et de maintenance. Les principales tâches lors de la conception d'algorithmes sont les spécifications de système et les spécifications expérimentales : (i) extraction des caractéristiques (ii) la fusion et (iii) la décision. Dans le cadre de ce travail, il faut également tenir compte d'autres facteurs, notamment la maîtrise de l'information et l'évaluation de performance. Dans les chapitres précédents, nous avons fait une étude théorique générale de l'état de l'art et des approches utilisées dans la protection des données multi biométriques et aussi une étude de performance de la biométrie révocable précisément le Biohashing dans le cadre de la conception d'un système de protection des données multi biométriques. Dans ce qui suit, nous allons voir les méthodes sur lesquelles on s'est basé pour exploiter ces différents concepts mathématiques afin de réaliser notre projet ainsi qu'une présentation détaillée des différents modules de système qui le composent et la manière dont nous avons implémenté les algorithmes afin de mettre en place notre système.

5.2 Problématique

Considérant le problème des applications de la protection des données multi biométriques ou les transactions entre l'architecture de système multi biométrique et les algorithmes de protection s'effectuent à travers les niveaux de fusion.

C'est a dire que Notre projet est basé sur le couplage de deux palier : la multi modalité et le biohashing . Lorsqu'on parle du multi modalité nous orientons directement vers la fusion mais la question qui se pose, à quel niveau de fusion nous allons appliquer l'algorithme de biohashing ?

5.3 Solution Proposée

Pour répondre à cette problématique, en biométrie multi modale on peut fusionner les données à plusieurs niveaux : capteur, paramètres ou bien caractéristiques, scores, décision etc. la troixième méthode est la plus employées pour notre travail. Pourquoi ? ?

Parce que la fusion au niveau de scores est la plus utilisé, car elle peut être appliquée à tous les types de systèmes et la deuxieme raison car elle donne le meilleur compromis entre la richesse d'information et la facilité d'implémentation.

Notre contribution sera exclusivement consacrée pour pallier ce problème. Pour ce faire, nous proposons une approche basée sur l'application de Biohashing sur les différents modalités puis on applique la fusion au niveaux de scores . A la fin nous allons tester l'approche en termes de performance et de fiabilité .

Le reste de ce chapitre est organisé comme suit. Dans la section suivante, nous

allons présenter l'approche proposée, une propre section est consacrée à cette nouvelle méthode. La section 3 sera consacré au Motivation des choix et des paramètres utilisés, mais avant de présenter l'architecture de l'approche proposée, nous fixons au préalable le mode de reconnaissance biométrique utilisé dans notre système proposé .comme nous a dit au premier chapitre, il existe deux modes de reconnaissance biométrique : l'identification et l'authentification.
Dans ce travail nous allons être principalement intéressés par le problème de vérification en utilisant les empreintes digitales comme modalité. En général, la vérification multi biométrique consiste en deux étapes :(i) inscription et (ii) authentification : durant l'inscription, la biométrie de l'utilisateur est capturée et les caractéristiques extraites (Templates) sont sauvegardées sur une base de données. Durant l'authentification, la biométrie de l''utilisateur est de nouveau capturée et les caractères extraits sont comparés avec ceux qui existent déjà dans la base de données pour déterminer la correspondance (le matching).
Chaque enregistrement spécifique retenu pour la comparaison est défini sur la base de l'identité proposée par l'utilisateur. Cette base de données est centralisée ou distribuée directement afin que chaque utilisateur dispose de son identité biométrique via un port externe.La figure suivante présente l'architecture d'un système de vérification biométrique :

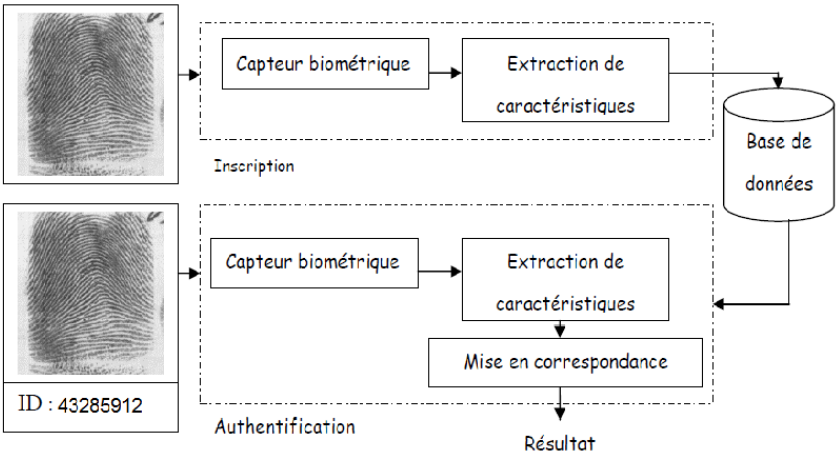


FIGURE 5.1 – *Architecture générale d'un système de vérification biométrique.*

Nous vérifierons le travail à travers l'architecture suivante, autant avoir posé les définitions de base suivantes concernant un système de vérification de l'identité :

5.3.1 Définition du problème de vérification

Dans ce cas, nous examinerons la question de la procédure de vérification biométrique de façon plus systématique. Lors d'un problème de contrôle, le signal biométrique provenant de l'utilisateur est mis en comparaison avec un seul gabarit enregistré. Le choix de ce modèle se fait en se basant sur l'identité de chaque personne. Tous les utilisateurs i sont représentés par leur Biométrie B_i. Les caractéristiques extraites seront représentées par une machine à T_i de la biométrie capturée. Pendant la procédure de vérification, l'utilisateur indique son identité j et transmet un signal biométrique T_j. La reconnaissance se fait en calculant le score de similarité $S(T_i,T_j)$. Cette identité annoncée est considérée comme réelle si $S(T_i,T_j)> th$ avec th un seuil de comparaison sélectionné ; son choix détermine un compromis entre la commodité de l'utilisateur et la sécurité de système.

Dans la partie suivante, nous exposons la solution d'un système multimodale avec la biométrie révocable (Biohashing).

5.4 Description de l'approche proposée

Dans cette section, nous présentons une nouvelle approche pour la protection des modèles multi biométriques. Notre objectif est de construire une technique d'hybridation entre la biométrie multi modale et la transformation Biohashing basée sur le Biohashing pour l'authentification qui répond aux exigences de la révocabilité, la diversité, la sécurité et la performance.

Le principe général de la méthode proposée est donné par la figure 5.2

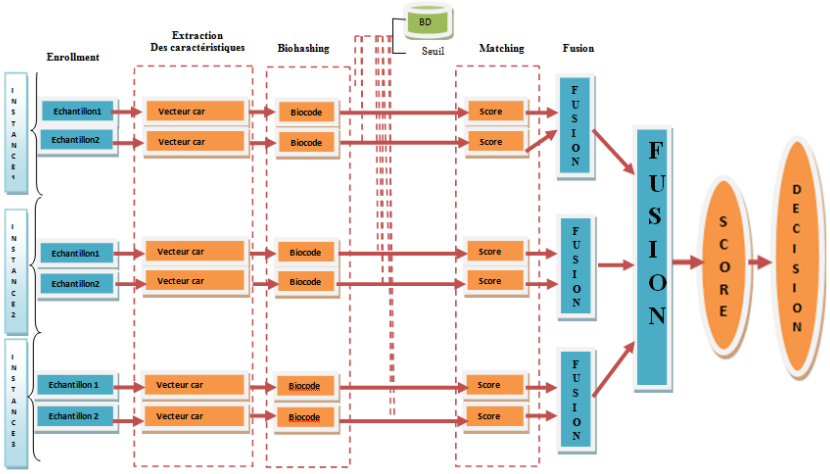


Figure 5.2 – *Description de l'approche .*

Nous commençons la présentation de l'approche :

Pendant la phase d'enrôlement, L'utilisateur doit fournir ses empreintes digitales au capteur pour générer ses templates de référence. Puis une méthode d'extraction des caractéristiques est appliqué sur chaque Template séparément pour générer un vecteur de caractéristique . A partir de deux vecteurs caractéristiques obtenus, on doit par la suite appliquer l'algorithme de Bio-Hashing pour protéger les modèles biométriques, six Bio Codes sont calculés chaqu'un représente une empreinte digitale . Un Bio Code est calculé et comparé au Bio Code de référence par un matching (distance euclidienne), Une valeur de décision est fournie est comparé par un seuil pour décider si l'utilisateur doit être authentifié ou non, constituant ainsi la fusion de score multi-échantillons (qui prend en compte l'exposition variable et la qualité de l'image acquise) .Ce principe constitué la première partie de notre contribution. La deuxième partie de notre contribution consiste à appliquer une fusion de score multi-instances de trois doigts de la main est ajoutée pour une meilleure protection et un taux d'erreur réduit, ce qui donne un score global. On utilise une approche spécifique en ajoutant les trois scores instances. Cette approche est la somme pondérée, qui représente un poids équilibré égal à un. A partir de ce score le système génère une décision selon l'utilisateur s'il possède un score maximal.

5.5 Sécurité des approches proposées

Nous avons présenté un schéma d'authentification multi biométrique dans lequel les données biométriques ne sont pas stockées et comparée directement dans la base de donnée mais on utilisons des bio codes . La méthode BioHashing utilisée précédemment est une méthode générique permettant de révoquer une donnée biométrique.
Dans ce qui suit, nous allons présenter nos contributions et nos brèves descriptions des méthodes en commun entre les deux approches proposées sont les suivantes.

1. **Entrée :** Les entrées de système multi biométrique sont des données brutes provenant de capteurs. Il peut s'agir de toutes les données biométriques, y compris le visage, l'oreille, l'empreinte digitale, la signature palmaire, etc. Dans notre système biométrique multimodale proposé, nous avons effectué des expériences en utilisant les empreintes digitales .Dans les figures 5.2 les entrées sont marquée comme instance 1 , instance 2 et instance 3.

2. **Extraction des caractéristiques :**

   Cette étape représente le coeur de système de reconnaissance multi biométrique, on extrait de l'image les informations qui seront sauvegardées en base de données pour être utilisées plus tard dans la phase de décision (matching). La problématique qui se pose est qu'elle nécessite de trouver des algorithmes dans lequel les résultats des vecteurs caractéristiques est stable en taille car l'Algorithme Biohashing est appliqué aux données biométriques représentées par un vecteur à valeur réelle de longueur fixe.
   Il existe deux approches pour l'extraction : les approches locales et les approches globales. La représentation des attributs de l'empreinte constitue la phase la plus importante lors de la conception d'un système de vérification.
   La première est basée sur l'emplacement des minuties. La représentation n'est pas forcément de dimension fixe puisqu'une minutie peut se manifester ou disparaître selon la qualité de l'acquisition. Pour la même cause, la représentation n'est pas ordonnée.
   Nous avons opté à orienter notre travail vers les approches globales . Le but général de ses approches est de procéder à un certain traitement pour saisir la texture et la quantifier à l'aide, généralement, de mesures statistiques telles que le calcul d'histogramme. Voir La référence [Tuceryan & Jain 1993] présente un résumé sur les méthodes d'analyse de texture. Plusieurs techniques récentes largement utilisées dans les problèmes de vision par ordinateur. Principalement, les filtres 2D de Gabor et l'opérateur LBP (Local Binary Pattern) avec un ensemble de ses variantes.
   Nous détaillons dans cette section le filtre utilisé.

   — **Description des filtres de Gabor**
   Les fonctions de Gabor sont un outil d'analyse de texture très prise. Il existe plusieurs travaux publiés sur leurs applications depuis que Gabor proposa en (1946) [1] La fonction 1-D de Gabor. Daugman a lancé la gamme de filtres Gabor 2-D en 1980 comme pré-projet pour étudier l'orientation sélective et les propriétés de fréquence de ces filtres. Daugman a ensuite les approfondies en 1985 sur le plan mathématique.
   Les caractéristiques de Gabor constituent un outil d'analyse de texture

1. D.Gabor. "Theory of Communication". IEE 93

très prisé. Elles possèdent des propriétés sélectives en orientation et en fréquence. Elles présentent donc une résolution spatiale/fréquence commune optimale (c'est-à-dire qu'elles sont très efficaces pour sélectionner à la fois la fréquence et l'orientation). Sur un plan mathématique, un filtre de Gabor est le résultat de produit d'une sinusoïde complexe et d'une enveloppe gaussienne. Dans le domaine spatial $(x; y)$ de l'image, un filtre 2D complexe est défini par l'équation 5.2.

$$G(x,y) = \exp\left(-\frac{1}{2}\left[\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right]\right) \times \exp(i(2\pi F x_\theta + \phi)) \tag{5.1}$$

avec :

$$-\begin{pmatrix} x_\theta \\ y_\theta \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{5.2}$$

— F la fréquence spatiale de la sinusoïde et ϕ la phase de la sinusoïde ;
— σ_x et σ_y qui représentent, respectivement, l'écart-type de l'enveloppe gaussienne le long des axes (x, x') et (y, y').

La composante réelle du filtre, souvent utilisée en pratique, est donnée par 5.3 et sa réponse impulsionnelle est illustrée sur la figure (référence de l'image voulue).

$$G(x,y) = \exp\left(-\frac{1}{2}\left[\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right]\right) \times \cos(i(2\pi F x_\theta + \phi)) \tag{5.3}$$

L'application de ce filtre sur une image I se fait par produit de convolution (voir équation 5.4) entre chaque pixel $I(i, j)$ de l'image et le masque M du filtre de *Gabor*.

$$I(i,j) = \sum_{n=\frac{-(d-1)}{2}}^{\frac{d-1}{2}} \sum_{m=\frac{-(d-1)}{2}}^{\frac{d-1}{2}} I(i+n, j+m) M(n,m) \tag{5.4}$$

Le premier algorithme représente le calcul des descripteurs de Gabor. Dans le domaine fréquentiel, le produit de convolution est exécuté (il est réduit à une simple multiplication). Le comportement de filtrage est exprimé par sa moyenne et sa variance. Dans le cadre d'un descripteur, nous avons toutes les moyennes et les variances de toutes les réponses de la banque de filtres. Dans notre système, nous avons appliqué ce filtre

sur les empreintes avec des paramètres qui nous ont donné un meilleur résultat, ses paramètres sont fréquence = 4, orientation = 6.

Algorithme 1 : Génération du descripteur de l'empreinte par un banc de filtres de Gabor

Data : I l'image en entrée
$Freq$: le nombre de fréquences du banc
$orientations$: le nombre d'orientations du banc
$A \leftarrow fft2(I)\%$ avec $fft2(I)$ la transformée de Fourrier rapide de l'image I
for $s \leftarrow 1$ **to** $Freq$ **do**
  for $n \leftarrow 1$ **to** $orientations$ **do**
    $M \leftarrow$ Masque de Gabor calculé en utilisant l'équation
    $D \leftarrow abs(ifft2(A \times GW))$
    $Feature(1, (s-1) \times orientations + n) \leftarrow mean(D)$
    $Feature(2, (s-1) \times orientations + n) \leftarrow variance(D)$
  end
end

3. **BioHashing :**
La méthode de Biohashing est un algorithme utilisé pour les données biométriques qui sont exprimées par un vecteur de valeur réelle de longueur fixe et génère un modèle binaire nommé BioCode de longueur inférieure ou équivalente à la taille originale.

Pour le BioHashing, le but est de générer un code unique, appelé biocode, à travers deux données : le modèle biométrique et un nombre aléatoire qui, pour une meilleure protection, doit se trouver sous la forme d'un jeton ou d'une clé USB. Nous appliquons le même schéma de transformation en même temps :

— Lors de l'enrôlement, où le biocode est stocké à la place du modèle biométrique.
— Lors de l'étape de vérification, où un nouveau biocode est généré à partir du nombre aléatoire assigné à l'utilisateur lors de l'enrôlement.

La procédure de vérification est ensuite fondée sur le calcul de la distance de euclidienne entre le biocode de référence et le biocode récemment émis. En utilisant différents nombres aléatoires pour différentes applications, ce principe assure la révocabilité et la diversité du biocode. La figure 6 représente le processus de BioHashing.
Nous pouvons constater que le modèle est un système à deux facteurs d'authentification, ce qui signifie que la fonction de transformation réunit un nombre aléatoire, en forme de grain, stocké dans un jeton, dont le modèle biométrique est représenté par un vecteur de longueur fixe $X = (x_1, \ldots, x_n), X \in R^n$.

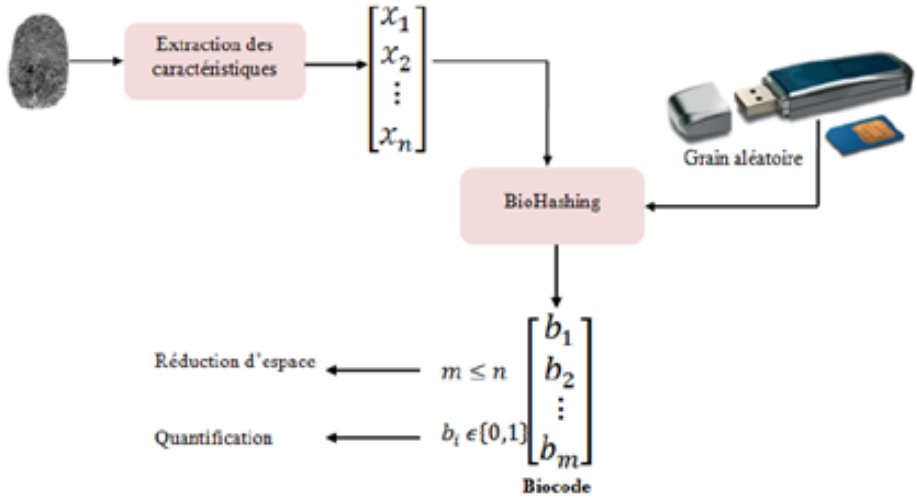


FIGURE 5.3 – *Transformation par BioHashing[Belguechi 2015]*

Le principe du BioHashing, détaillé dans [Jin *et al.* 2004] , Il s'agit d'une projection aléatoire suivie d'une étape de quantification. Nous allons désormais fournir plus de détails sur ces étapes.

— **Projection aléatoire**

- Pour obtenir une projection aléatoire, on multiplie un vecteur de données $X \in R^n$ par une matrice aléatoire R pour générer un vecteur $W \in R^m$ de taille réduite $m < n$, à partir du produit : $W = RX$. Dans le secteur de la biométrie, le caractère utile d'une telle projection varie selon la préservation ou non des distances entre les différents vecteurs caractéristiques d'un même utilisateur. Il convient de noter $R = (R_{ij})_{ij} \in 1, n] \times [1, m]$, la matrice de projection.*S*.Kaski a présenté que [Kaski 1998] si la matrice R est orthonormée, la similarité entre les vecteurs est maintenue (R devient une base).

Le résultat de la projection est noté $W = (w_1, \ldots, w_m)$. Dans un sens, cette projection se résume à masquer les données biométriques recueillies dans un certain espace.

En pratique,

La matrice R est générée à partir du nombre aléatoire stocké sur le jeton, appelé clé, et considéré alors comme le grain d'un générateur pseudo-aléatoire.

Une orthonormalisation est nécessaire pour transformer la matrice aléatoire R en une base de projection. Pour ce faire, nous utilisons le processus de Gram-Schmidt [Hoffmann 1989].Par ailleurs, il est indispensable de vérifier que les vecteurs de colonne R présentent une indépendance linéaire avant d'appliquer le procédé Gram-Schmidt.

— **Quantification**

La présente étape est dédiée à la conversion vers un vecteur à valeurs binaires, du vecteur à valeurs réelles W, résultant de l'étape de projection. De plus, cette binarisation de un à plusieurs est ajoutée pour renforcer l'irréversibilité de la transformation (qui repose déjà sur le processus de projection). La définition d'un seuil t_b est nécessaire pour calculer le biocode final $B =$

$(b_1, \ldots, b_m)$, sur la base de la formule ci-dessous :

$$b_i = \begin{cases} 1 & si \quad x \leqslant t_b \\ 0 & si \quad x > t_b \end{cases}$$

Concrètement, le seuil t_b est choisi égal à o car les résultats de la projection ont la même probabilité d'être négatifs ou positifs. Par conséquent, chaque bit b_i du biocode B aura la même probabilité d'occurrence, qui a pour effet de multiplier le contenu de l'information réellement présente dans B et donc sa robustesse.

— **Application du BioHashing**

Désormais, nous présentons dans l'algorithme qui suit le processus de protection du vecteur moyen $C = (c_1, \ldots, c_n)$ par BioHashing.

Algorithme 2 : processus de protection par BioHashing

Data : I C :le vecteur moyenne de l'utilisateur U de taille n
S : la clé sous forme d'un nombre aléatoire attribuée à l'utilisateur U
Result : :B :le biocode de taille m avec $m < n$

1. Générer à partir de S une matrice aléatoire uniforme $R_n \times m$(n lignes et m colonnes)
2. Contrôler que les vecteurs de R sont linéairement indépendants sinon aller à 1 .
3. Appliquer le processus de Gram-Schimdt Pour transformer R en une matrice orthonormée.
4. Projeter le vecteur C sur la nouvelle matrice R :
$$\begin{bmatrix} c_1, & c_2, & \ldots, & c_n \end{bmatrix} \begin{bmatrix} r_{11} & \cdots & r_{1m} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nm} \end{bmatrix} = \begin{bmatrix} w_1, & w_2, & \ldots, & w_n \end{bmatrix}$$
5. Binarisation de W , à partir du seuil $t_b = 0$, pour obtenir le biocode B $=b_1, b_2, \ldots, b_m$ tel que :
$$b_i = \begin{cases} 1 & si \quad x \leqslant t_b \\ 0 & si \quad x > t_b \end{cases}$$
6. Effacer le vecteur C et sauvegarder le vecteur B comme référence de l'utilisateur U

4. Matching :

La classification est la partie la plus importante d'un système multi biométrique car les décisions de vérification et d'identification sont prises par ce module. L'architecture de système proposée est la vérification biométrique multimodale révocable. L'objectif principal de cette thèse est de générer les modèles robustes, sécurisés, révocables et discriminants. Par conséquent, le module de comparaison peut se réduire à un simple calcul de distance entre vecteurs. Dans le cas où le vecteur a pu être binarisé, il s'agira d'une simple distance euclidienne. le resultat de cette phase est un score pour chaque échantillion .

5. Fusion :

La fusion de score est appliquée dans cette étape, on fusionne le score résultant des multi échantillons pour prendre en considération les différentes poses des images acquises, le résultat de cette fusion est un score global pour chaque instance . Une autre fois on applique la fusion de score multi ins-

tances de trois doigts de la main gauche pour augmenter la performance.Le résultat de cette fusion est un score global de trois instances .

6. Décision :

C'est l'étape finale de l'approche proposé afin de faire la décision finale d'accepter le client ou non . Durant cette étape le système doit accepter le client qui possède le score maximal après une comparaison avec d'autres scores .

5.6 Motivation des choix et des paramètres utilisés

Plusieurs types de paramètres ont été utilisés pour la vérification dans l'approche proposée. Dans la suite, nous introduisons brièvement les motivations de chaque choix. ***Pourquoi les empreintes digitale ?***

- La reconnaissance d'empreinte digitale est la technique biométrique la plus ancienne et c'est l'une des plus matures.
- C'est l'une des modalités qui a connu un grand succès. Son utilité a été prouvée pour le service de la médecine légale, ainsi que la criminologie.
- De nos jours, des techniques biométriques fiables telle que la reconnaissance des empreintes digitales s'imposent un peu partout pour l'authentification des personnes et peuvent donc être réservées aux applications de très haute sécurité.
- Grâce à sa simplicité d'acquisition et son acceptation par le public.
- L'existante d'une base données réelles pour les empreintes digitales.

Pourquoi l'authentification ?

Le domaine de la reconnaissance individuelle est un domaine de recherche en perpétuelle progression. De nos jours, les exigences de sécurité sont les facteurs qui encouragent le recours à la reconnaissance pour la sécurisation des documents électroniques, des locaux privés ou gouvernementaux, le contrôle des employés, le commerce électronique, etc. Ce système de sécurité est considéré comme étant fiable pour établir l'identité des personnes en vue de sécuriser l'accès et le fonctionnement de ce type d'applications. Au-delà de l'authentification, ce système assure un autre service de sécurité très important et nécessaire, appelé non répudiation.

Pourquoi l'utilisation du filtre de Gabor ?

Dans notre étude, nous avons décidé de travailler sur des paramètres relatifs à la fréquence . Le choix de ce type de paramètres est motivé par le fait qu'il permet une représentation de l'empreinte par un vecteur de taille fixe. Cette caractéristique devrait être définie dans le but de comparer deux Bio codes et d'attester de leur similarité ou de leur différence. Ces comparaisons impliquant une fiabilité variable se traduisant dans la pratique par de possibles rejets et acceptations. En utilisant la méthode de distance de euclidienne comme méthode de comparaison.

5.7 CONCLUSION

Dans le présent chapitre, nous avons présenté le coeur de notre travail qui consistait en la proposition d'un système de protection des données multi modales

(les empreintes digitales) A cet effet nous avons proposé une approche de fusion de score selon le mode de fonctionnement, l'authentification.

Les différentes étapes : enrôlement, extraction de paramètres , Biohaching et la comparaison sont détaillées.

Nous avons présenté dans ce chapitre un schéma d'authentification et de protection multi biométrique . Notre construction permet de limiter le risque de vol des données biométriques et améliore donc la sécurité de l'authentification multi biométriques.

Dans le chapitre suivant, nous allons étudier une étude de performance de notre approche proposée selon les méthodes d'évaluation des systèmes biométriques et des systèmes révocables dans le but de pallier au problème de protection des données multi biométriques.

Tests et évaluation des résultats 6

Sommaire

6.1 Introduction

Dans ce chapitre, nous allons exposer les résultats des différents tests effectués sur l'approche (fusion au niveau de score), et dans le mode de reconnaissance (Vérification), pour le but d'évaluer l'algorithme Biohashing, selon une étude de performance pour cet algorithme .
Dans un premier temps, Nous exposerons d'abord la base de données sur laquelle nous avons travaillé ainsi que les tests effectués selon le mode vérification . Ensuite, nous ferons une autre étude de l'approche selon les performances du Biohashing cités au chapitre précédent. Nous terminerons par une conclusion des tests réalisés et une comparaison de notre proposition avec les autres travaux existants .

6.2 Base de données et protocole de test

L'étude expérimentale de cette recherche est basée sur la protection de reconnaissance de personnes par leurs empreintes digitales en utilisant les approches décrites dans le chapitre précédent. Les images des empreintes digitales que nous avons utilisées dans nos expérimentations sont issues de la base de données SDUMLA-HMT [Yin *et al.* 2011] À l'heure actuelle, la reconnaissance des empreintes digitales est la méthode biométrique la plus largement utilisée. La base de données la plus complète des empreintes digitales a été utilisée, la base de données SDUMLA-HMT. Cette base de données comprend 106 individus. Chaque image d'empreinte digitale est sauvegardée sous un format «.Bmp» de 256 niveaux de gris. La capture a été faite pour les six doigts avec 5 types de capteurs différents. La base de données d'empreintes digitales multi-capteurs contient $6 \times 5 \times 8 \times 106 = 25440$ images d'empreintes digitales au total.

Ou :
nombre =106 Personnes .
capteur : 5 capteurs.
instance : 6 instances .
échantillon : 8 échantillons .

La figure suivante montre quelques images pour différents capteurs.

FIGURE 6.1 – *Quelques images pour différents capteurs.*

Le choix de la base de données SDUMLA-HMT est justifié par le fait que c'est une base de données réelle des images des empreintes digitales qu'elle contient sont relativement de bonne qualité.
Le protocole de test adopté est le suivant : Afin de former nos bases de données multi-biométriques, nous avons pris en compte le capteur FT-2BU et le capteur AES2501. Afin d'évaluer la performance de la méthode proposée, nous utilisons la méthodologie suivante. , nous sélectionnons les 3 doigts de la main gauche et nous utilisons le premier et le troisième échantillon de chaque utilisateur de notre base de données comme référence de modèle. Le reste des images de l'utilisateur et celles des autres utilisateurs sont utilisés pour tester les schémas proposées. Au total, nous avons la base de donnée de test $3 \times 6 \times 106 = 1908$ images d'empreintes digitales et la base de données d'apprentissage $3 \times 2 \times 106 = 636$ images d'empreintes digitales.
Les performances de système sont évaluées en termes de taux d'égale erreur (Equal Error Rate ou EER) qui indique le point où les taux des fausses acceptations et des faux rejets sont égaux.
Nous suivons le même protocole de test des performances de vérification biométrique que la FVC (Fingerprint Verification Competition), à savoir :

— Pour calculer le FRR, chaque échantillon est comparé avec les échantillons restants du même utilisateur.

— Pour calculer le FAR, chaque premier échantillon est comparé avec les premiers échantillons des autres utilisateurs.

6.3 Implémentation

Le filtre Log-Gabor 2D est utilisé dans ce travail pour choisir les meilleurs paramètres possibles. Un vecteur de caractéristiques dont la taille est de 552 caractéristiques pour chaque image est le résultat de ce processus d'extraction.
Pour le chemin secret, nous utilisons ces dernièrs vecteurs pour calculer le BioCode de référence alors nous avons obtenu la même taille 552 biocodes (le résultat du biohashing).
A l'authentification, en appliquant l'algorithme du *distance euclidienne* entre les empreintes en cours et les empreintes enregistrées dans la base de données .Une opération de *matching* des empreintes sera réalisée le bio code des empreintes en cours et les biocodes enregistrées dans la base de données. Ceci est dans l'objectif de filtrer les tentatives légitimes et de freiner les intrus qui arrivent à décoder un nombre important de l'ensemble de caractéristiques. A l'issue de cette étape, et suivant un seuil de *matching* prédéfini, on récupère un score .
La première fusion (multi échantillon) au niveau de score est appliquée par fusion de deux scores des échantillons de la même instance puis une application de la deuxième fusion (multi instance)au niveau de score par combiner les trois scores de trois instances, pour former le score global , par l'utilisation d'une simple méthode : la somme pondérée avec un poids équilibré égal a 1.

Notons que notre implémentation à été effectuée sur une machine serveur de l'université de djillali liabes sidi bel abbes , département mathématique et informatique .
L'implémentation des différents algorithmes de notre système ainsi que le déroulement de tous les tests sont faits sous Matlab 2013*b*. Matlab est un environnement de calcul scientifique et de visualisation de données très puissant et largement utilisé dans la valorisation des travaux de recherche. Sa facilité d'apprentissage et d'utilisation en ont fait un standard adapté pour les divers problèmes de l'ingénierie. Ceci est grâce à ses nombreux avantages, comme ses nombreuses fonctions prédéfinies prêtes à l'emploi, sa programmation simplifiée, sa rapidité de calcul, sa fiabilité, sa robustesse, etc.
Avant l'analyse de la performance de système biométrique multimodale révocable, il est important d'établir la performance pour le système multimodale sans protection . Pour valider les méthodes proposées.

6.4 Résultat de système multimodale sans Biohashing

L'objectif principal de ce test est de vérifier la performance de système biométrique multimodale dont le but d'amélioration les performances et protéger les données multi biométrique.
Nous avons utilisé l'algorithme de filtre Log-Gabor 2D pour extraire les caractéristiques des empreintes digitales. Ces algorithmes sont classés parmi les meilleurs descripteurs de textures actuels. Le résultat de cette expérimentation illustré dans la figure suivante :

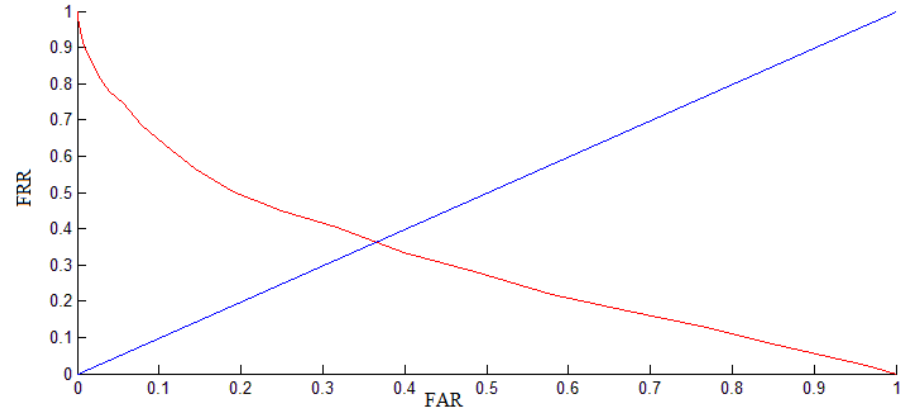


FIGURE 6.2 – *Performance de système biométrique multimodale*

La figure 6.2 illustre l'évolution de l'EER en fonction des différents seuils de décision, Nous remarquons d'après cette figure que l'EER égale à 36% avec un seuil égal à 0,9690.

6.5 RÉSULTAT DE SYSTÈME MULTIMODALE AVEC BIOHASHING

Le but de l'algorithme de Biohashing est d'amélioré le niveau de sécurité de système tel que le taux d'identification des modalités biométriques fusionnées soit supérieur au maximum des taux d'identification des modalités prises séparément. La figure 6.3 Récapitule les Performances de notre approche.

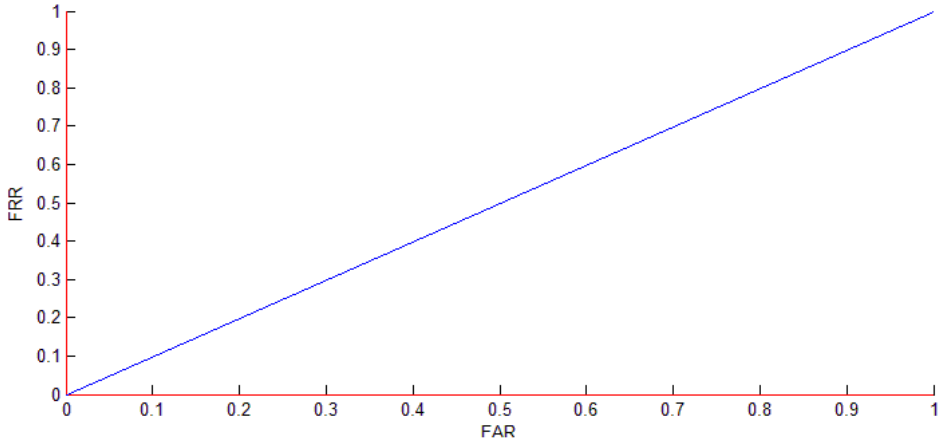


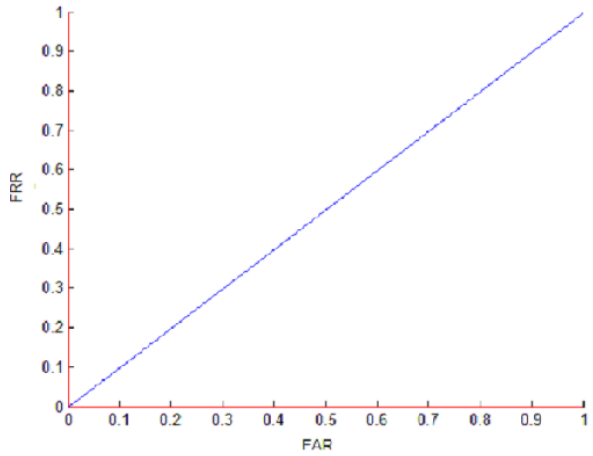
FIGURE 6.3 – *Performance de système biométrique multi multimodal proposé*

A partir de la courbe représentative du taux de FAR et FRR (figure 6.3), nous constatons que l'approche proposée a la capacité de préserver et d'accroître la performance des systèmes protégés, le taux EER égalent à 0%. Ceci s'explique par le fait que l'algorithme de Biohashing a démunie le taux d'EER et protégé les données multi biométrique.
Cela nous a motivé à étudier la performance de biométrie révocable (vue au chapitre 3) pour démontrer la sécurité de l'approche proposée contre les attaques possibles.

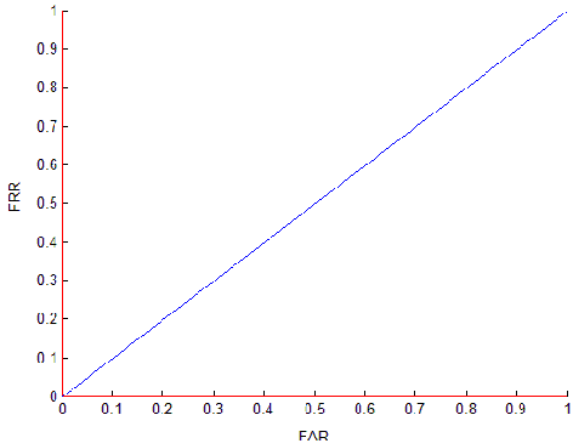
6.6 Évaluation de système multi biométrique révocable

Dans cette partie on va voir les différents résultats qui correspondent aux différentes métriques. Ces résultats ont été présentés par la courbe de ROC (Receiver Operating Characteristics). Ainsi ils seront représentés par l'approche proposée.

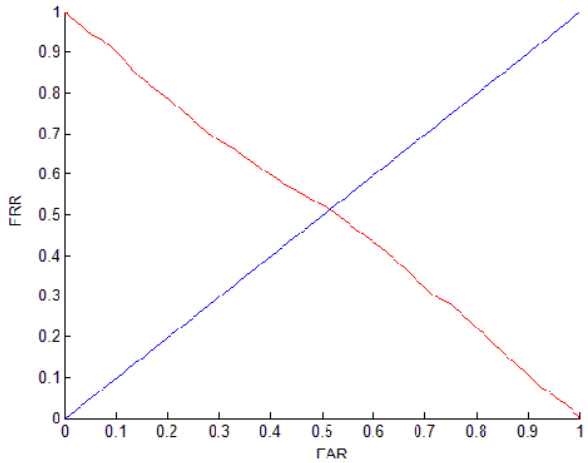
La Figure 6.4 présente les courbes ROC de système propsé pour les métriques : $A1$(performance) ,$A2$ (attaque à zéro effort), $A3$ (attaque par force brute), $A4$ (attaque par vol de clé), $A5$ (attaque par vol de biométrie), $A6$(attaque par écoute de 3 biocodes différents d'un même utilisateur), $A7$ (attaque par écoute de 11 biocodes différents d'un même utilisateur).



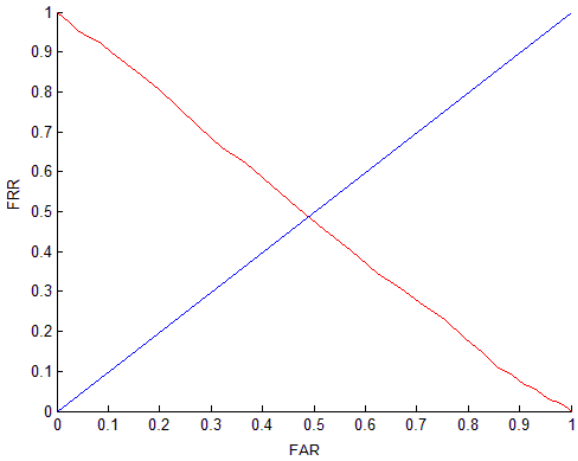
(a) *A1 performance*



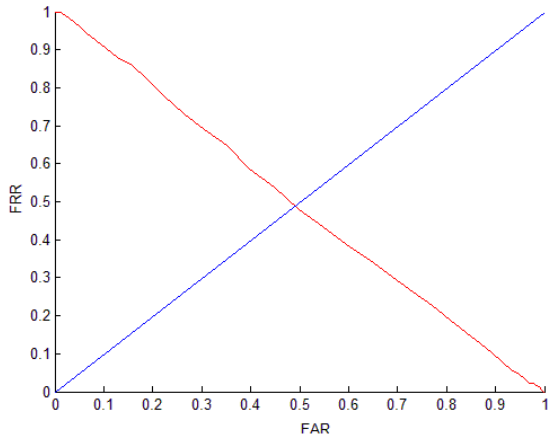
(b) *A2 attaque à zéro effort*



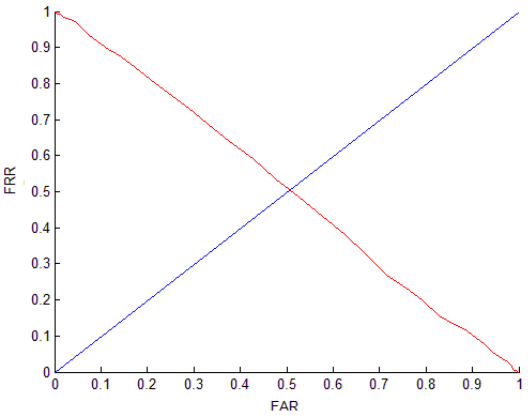
(c) *A3 attaque par force brute*



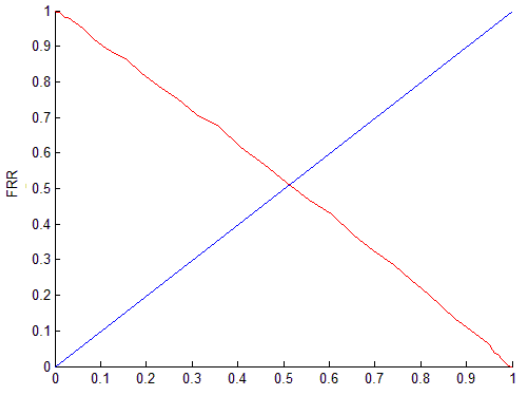
(d) *A4 attaque par vol de clé*



(e) *A5 attaque par vol de biométrie*



(f) *A6 attaque par écoute de 3 biocodes différents*



Nous commençons par paramétrer la valeur du EER de système révocable (fusion de score) selon les différents attaques .Le tableau 1 résume les valeurs des différentes EER selon les métriques $A1, \ldots, A7$.

Les métriques	$A1$	$A2$	$A3$	$A4$	$A5$	$A6$	$A7$
EER	0%	0%	50%	47%	47%	51%	51%

TABLE 6.1 – *Évaluation de système révocable par les différentes métriques*

La figure 6.5 illustre l'évolution du FAR en fonction des différents seuils de décision pour les métriques $A1, \ldots, A7$:

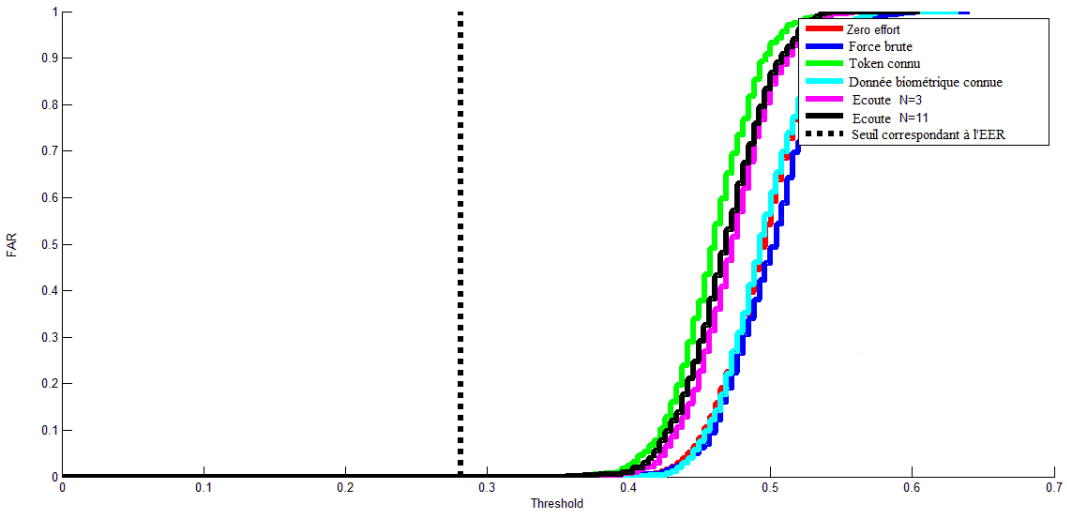


FIGURE 6.5 – *Évolution du FAR pour différents scénarios d'attaque.*

La Figure 6.6 présente l'histogramme de la distribution des scores légitime / imposteur de lapproche. On peut observer que les deux pseudo-légitimes distributions sont bien séparées de la distribution des légitimes dans l'approche. Rappelons qu'un histogramme est un outil de représentation statistique d'une série de N données xi . En abscisse on représente les classes, c'est-à-dire les intervalles $[a_j; a_j + 1]$ au sein desquels on va décompter les données.

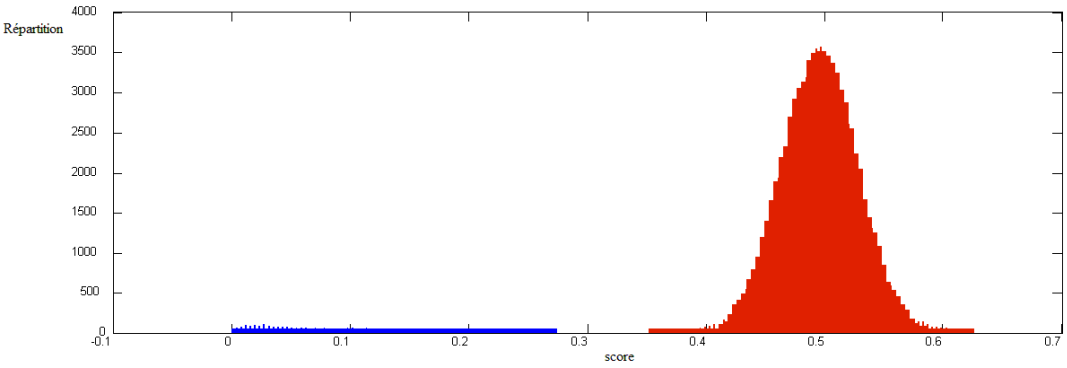


FIGURE 6.6 – *histogramme de la distribution des scores légitime (bleu) / imposteur de l'approche*

Cette distribution présente un facteur d'évaluation des modèles enregistrés dans un système multi biométrique .les classes considérées sont les individus enre-

gistrés .Chaque classe regroupe plusieurs modèles des informations de l'individu concerné :

- La classe intra-classe (légitime) : elle représente un taux de changement ou de dissimilitude entre les modèles du même individu (représentatifs de la même classe).
- La classe inter-classe(imposteur) : elle représente un taux de changement ou de dissimilitude entre les modèles de différents individus(différentes classes de la base de données).

Le système multi biométrique doit être basé sur des méthodes prenant en compte ces deux classes , pour assurer une meilleure discrimination .Plus la classe intra-classe est importante plus il y a risque d'avoir une augmentation du FRR .D'autre part , plus la classe inter-classe diminue , plus il y a risque d'avoir une augmentation du FAR.

6.7 Commentaires sur les résultats

- La comparaison entre les valeurs d'évolution du FAR pour différents scénarios d'attaque présente, la probabilité de réussite d'une attaque sur ce schéma révocable, sous plusieurs hypothèses. Nous remarquons que pour l'approche que toutes les attaques peuvent être efficaces. Nous pouvons également remarquer une dégradation des performances de l'approche en introduisant des attaques spécifiques. Cependant, pour notre approche , la valeur EER de système révocable est marqué au seuil égale à **0.28** .On notera également l'attaque token connu(Stolen token), qu'un seuil fixé à **0.38** suffit pour cette attaque vaincre l'approche. Pour l'attaque force Brute à le même seuil pour l' approche .Les attaques précédentes peuvent être détaillées dans la littérature. Nous allons maintenant discuter d'un type d'attaques adaptées à la nature révocable de BioHashing : attaque personnelle par écoute de N BioCodes $N = 3$ et $N = 11$. Pour ce test, on suppose que l'intrus dispose de 3 ou 11 BioCodes (interceptés après révocation), La figure 6.5 montre que le système est résistant à l'attaque personnelle. On peut remarquer qu'entre $N = 3$ et $N = 11$, l'attaque ne progresse pas beaucoup.la même figure montre que si le seuil est fixé suffisamment bas (**0,40** dans le cas $N = 3$ et dans le cas $N = 11$), nous pouvons débarrasser de cette attaque dans le but de toutes les valeurs du FAR s'annulent et sécuriser totalement le système multi biométrique **FAR=0%**. Ces valeurs sont expliquées par la taille du bio code utilisé ,Ces attaques nous informe aussi que durantl' implémentation, il est conseillé de considérer la taille du biocode m à la plus grande valeur qui converge vers un système révocable parfait .
- En outre, Nous avons montré à la figure 6.7 la distribution hypothétique des taux de performance qui seraient obtenus par les utilisateurs légitimes et les imposteurs pour l'approche proposée , quand la partie bleue représente les utilisateurs légitimes, tandis que la partie rouge représente les attaquants . une séparation entre les deux taux ce qui signifie que le la révocabilité et la diversité sont atteintes par notre approche proposée ceci est expliquer par le taux de la classe intra-classe(légitime)diminue se que signifie une diminution du FRR .D'autre part , plus la classe inter-classe (imposteur) augmente , plus il y a une diminution de FAR.
  En général, nous pouvons conclure que l'efficacité des régimes de protection est bien influencée par la taille du biocode utilisé .Au moment de l'authenti-

fication, l'utilisateur est tenu de présenter ses clés pour générer des biocodes dans les systèmes protégés par Biohashing . Dans le cas des systèmes multi biométriques non protégé, l'authentification se faite par le besoin seulement d'une clé utilisateur.

Pour conclure sur les évaluations réalisées, le tableau suivant donne une idée de l'importance du travail fourni. Il présente une comparaison entre différentes approches pour sécuriser des données multimodales en utilisant des méthodes de transformation Révocable

TABLE 6.2 – *comparaison entre différentes approches pour sécuriser les données multimodales.*

Auteur	Année	Principe	Les modalités	Méthode	performance
Nanni et al [Nanni & Lumini 2006]	2006	combiner le BioHashing dans une approche de fusion multimodale (fusion au niveau de décision)	visage + empreinte digitale	BioHashing	$EER \approx 0\%$
Jeong et al [Jeong *et al.* 2006]	2006	Combiner deux méthodes d'extraction de caractéristiques différentes pour obtenir une biométrie révocable (PCA et ICA).	empreinte digitale + empreinte palmaire + visage	BioHashing	EER =21.53%
Maiorana et al [Maiorana *et al.* 2011]	2011	la biométrie est sécurisée en appliquant un ensemble de transformations non inversibles, générant ainsi des modèles modifiés à partir desquels la récupération de l'information originale est aussi difficile que de la deviner.	la signature en ligne (BDD MCYT)	transformations non inversibles	EER =34.22%
Paul et al [Paul & Gavrilova 2012]	2012	développer un nouvel algorithme de génération de modèle révocable biométrique utilisent la projection aléatoire et une transformation basée sur l'extraction et la sélection de caractéristiques .	visage et oreille.	Biométrie révocable	EER =14.03%
Canuto et al [Canuto *et al.* 2013]	2013	étudier spécifiquement la performance de différentes approches de fusion dans le contexte de la reconnaissance de la multi biométrie révocable.	données vocales et iris	Biométrie révocable	EER =4%
Rathgeb et al [Rathgeb & Busch 2014]	2014	Application des transformations adaptables à base de filtre Bloom sont appliquées afin de mélanger les modèles biométriques binaires au niveau des caractéristiques	iris (BDD IISD)	Transformation irréversible (basée sur le filtre Bloom)	EER <0.5%
Sushma et al [Sushma & Sandeep 2015]	2015	deux méthodes sont été utilisées pour extraire les caractéristiques de l'image, à savoir : 1)filtre Gabor et 2) techniques de projection aléatoire (RP).	Deux iris	Transformation irréversible (basée sur le filtre Bloom)	EER non définie
Damasceno et al [Damasceno *et al.* 2015]	2015	utilisant des ensembles de systèmes. L'ensemble de systèmes,(multi-classificateurs)	deux iris	Biohashing	EER =28,6%
Rathgeb et al [Rathgeb *et al.* 2015]	2015	La fusion au niveau de score est appliquée pour augmenter la précision de la reconnaissance.	Visage+iris	Transformation irréversible (basée sur le filtre Bloom)	EER non definie

Stokkenes et al [Stokkenes *et al.* 2016]	2016	La fusion au niveau de score est appliquée pour augmenter la précision de la reconnaissance.	Visage + iris	filtre Bloom + caractéristiques d'images statistiques binarisées (BSIF)	FAR = 0,01%
Yildiz et al [Yildiz *et al.* 2017]	2017	construit un modèle multi-biométrique en superposant plusieurs données biométriques d'un utilisateur, de sorte qu'il est difficile de séparer les couches individuelles.(fusion au niveau de capteur)	Voix + empreinte digitale	Biométrie révocable	EER = 2,1%
Bringer et al [Bringer *et al.* 2017]	2017	Une approche a développé l'approche de [Rathgeb & Busch 2014]. ils analysent la non-capacité sur les modèles protégés à partir de deux codes d'iris différents provenant du même iris.	Deux iris	Transformation irréversible (Bloom filter)	EER non définie
Bokade et al [Bokade & Kanphade 2019]	2019	Un système a proposé une méthode de concaténation de vecteurs de caractéristiques de dimension réduite et utilise d'un seul algorithme d'analyse en composantes principales pour l'extraction de caractéristiques et de distance euclidienne.	le visage, l'empreinte palmaire et l'oreille	Transformation de caractéristiques	EER non définie
Walia et al [Walia *et al.* 2020]	2020	un système biométrique revocable multimodal basé sur la Deep Feature Unification (DFU) en temps réel. La non-inversibilité est obtenue par projection aléatoire des fonctionnalités Key Deep vers les fonctionnalités Query Deep. Le processus de fusion adaptatif proposé basé sur des graphes extrait non seulement des informations complémentaires sur plusieurs modalités, mais génère également un modèle unifié multimodal	les empreintes digitales	Transformation de caractéristiques	EER = 0,12
Sharma et al [Sharma & Selwal 2020]	2020	un nouveau schéma de hachage basé sur le code régional (RCHTSS) pour la protection des modèles dans un système biométrique multi-instance est présenté	les empreintes digitales	Transformation de caractéristiques(schéma de hachage)	FAR = 0,2 %, FRR= 0,05 %.

Gupta et al [Gupta *et al.* 2021]	2021	un système biométrique multimodal révocable qui combine plusieurs traits au moyen d'une approche basée sur la projection, Les caractéristiques annulables sont générées en projetant les points caractéristiques sur un plan aléatoire obtenu à l'aide d'une clé spécifique à l'utilisateur	Transformation de caractéristiques non inversibles	FAR = 0,004%.
bedad et al [Bedad *et al.* 2021]	2021	un système de protection des modèles multi biométriques révocable basé sur la fusion de scores à deux niveaux : multi échantillons et multi instances au moyen d'une approche basée sur la transformation Biohashing. Pour réaliser cette approche nous avons combiné les fonctions multicapteurs d'empreintes digitales de trois doigts humains (base de données SDUMLA-HMT).	Transformation de caractéristiques par le Biohashing	EER= 0%.

De nombreux travaux pour sécuriser les données multi biométriques utilisant la transformation révocable ont été réalisés. L'une des premières analyses de sécurité a été présentée par Nanni et al [Nanni & Lumini 2006] où ils ont utilisés le Biohashing avec un système multi modales au niveau de décision, l'approche concernent précisément le visage et l'empreinte digitale ou le $EER \approx 0\%$. Apres d'autres travaux ont été clairement effectuées sur certaines modalités , utilisant la biométrie révocable , le filtre de Bloom, d'autres stratégies de fusion comme la fusion au niveau de caractéristiques , et même d'autres systèmes multi biométriques tel que multi-algorithmes , on remarque que le taux de performance de l'approche de Nanni et al [Nanni & Lumini 2006] reste le meilleur par rapport aux autres travaux . contrairement au notre travail[Bedad *et al.* 2021] qui presente une meilleure performance un EER =0 %.

Après cette comparaison, nous pouvons dire que notre approche fusion de scores vise à assurer un équilibre entre la sécurité et la performance, mais aussi l'acceptation de l'utilisateur qui est une exigence des systèmes multi biométriques.

6.8 CONCLUSION

Ce chapitre présente une analyse comparative des résultats de tests que nous avons effectués sur la base SDUMLA-HMT des empreintes digitales pour l'approche proposée .
Nous avons commencé par une étude de performance entre le système multi biométrique non protégé par le Biohashing et le même système mais protégé avec le Biohashing .
Après nous avons testé l'approche par un ensemble de métriques $A1, \ldots, A7$ dans le but de l'évaluation des schémas de multi biométrie révocable.
Étudier la robustesse du BioHashing revient à tester la performance de système par rapport aux variations des attaques adressé aux données biométriques d'un individu et la sensibilité du BioHashing par apport aux l'approche.
L'exécution de ces propositions dans notre plateforme de test nous a fait obtenir des résultats plus encourageons.
A travers ces tests on constate que note approche a prouvé son efficacité pour les systèmes d'authentifications multi biométriques.

Mes contributions scienfifiques

  - Bedad F, Adjoudj R. (2018). Secured Multimodal Biometric System. Journal of Multimedia Processing and Technologies Volume 9 Number 3 page 77.
  - Bedad F, Adjoudj R. (2018, November). Multi-biometric Template Protection : An Overview. In International Conference in Artificial Intelligence in Renewable Energetic Systems (pp. 70-79). Springer, Cham.
  - Bedad F., Adjoudj R. (2019) Multi-biometric Template Protection : An Overview. In : Hatti M. (eds) Renewable Energy for Smart and Sustainable Cities. ICAIRES 2018. Lecture Notes in Networks and Systems, vol 62. Springer, Cham. https ://doi.org/10.1007/978-3-030-04789-47.
- Bedad, Fatima, Réda Adjoudj, and Nassima Bousahba. "Study of the robustness of a transformation-based multi-biometric template schemes protection." International Journal of Computing and Digital System (2022) Volume 11 Number 3 (pp. 336-344).

Conclusion générale

«Il est facile de manquer le but et difficile de l'atteindre »
Aristote

Cette thèse a étudié le problème de la protection des systèmes multi biométriques. Alors que les systèmes multi biométriques présentent des avantages par rapport aux systèmes traditionnels d'authentification personnelle, la question de la sécurisation et de la confidentialité des données multi-biométriques demeure essentielle. Le recours plus fréquent aux techniques biométriques en matière de sécurité a éveillé un nouveau regain d'intérêt pour la recherche et l'exploration de nouvelles techniques pour la prévention des attaques contre les systèmes multi biométriques.

L'étude de la sécurité via des systèmes multi biométriques est confrontée à un principal problème contre lequel le défi reste toujours posé. Ce problème consiste dans la complexité des algorithmes d'extraction et de matching des modèles biométriques ainsi que dans la protection de ces derniers.

L'application de la biométrie révocable permet la diversification et la sécurisation des données biométriques et multi biométriques, de manière qu'elles n'utilisent pas directement les données d'origine et assurent ainsi la protection de la vie privée des utilisateurs. Toutefois, ces systèmes reposent sur la modalité biométrique utilisée et doivent nécessairement tenir compte des contraintes de sécurité et de variabilité des données. La mise en place de tels systèmes représente un défi majeur pour la protection de la vie privée et la normalisation de l'évaluation de la robustesse de ces techniques se poursuit.

Le travail présenté dans cette thèse s'inscrit dans ce contexte. Notre travail contribue à la vérification multi-biométriques de personnes par reconnaissance de leurs empreintes digitales en utilisant la biométrie révocable :le Biohashing .

Nous voulons bien confirmer à la fin de cette thèse, que la sécurité totale n'existe pas. Il est vraiment très important de comprendre, tout simplement, que les systèmes de reconnaissance personnelle (traditionnels et biométriques) parfaits n'existent pas ; et peut-être ils n'existeront jamais. Cependant, Nous pouvons dire que les systèmes d'authentification basés sur la biométrie peuvent toujours fournir l'assurance de l'identité , qui est fondamentale pour la sécurité des systèmes, si on l'utilise avec prudence et en collaboration avec d'autres techniques de protection (biométrie révocable , cryptographie, etc.). Notre méthode présente en outre l'avantage de pouvoir révoquer la donnée secrète . Notre construction peut s'utiliser en remplacement des applications habituelles de l'authentification multi biométrique.

Perspectives

Nous avons proposé une méthode de vérification multi biométrique réellement utilisable en pratique, nos résultats expérimentaux ont donné des résultats encourageants. Ce travail peut être considéré comme une base pour les travaux futurs dans cette direction de recherche. Les travaux futurs sont suggérés vers :

— Amélioration de la caractérisation de l'empreinte digitale. Nous pensons qu'une méthode hybride utilisant à la fois l'analyse de texture et les minuties et une méthode générale d'extraction de caractéristiques serait intéressante à étudier.
— Tester la méthode sur des grandes bases de données et sur d'autres modalités.
— Proposition d'une étude de la gestion décentralisée des modèles multi biométriques (base de donnée), pour éviter les attaques, actuelles et possibles, il est important de gérer en toute sécurité les clés des utilisateurs et les modèles transformés (bio codes).
— Le problème du vol de clés est l'un des points faibles des transformations révocables.
— Pour résoudre ce problème, nous allons utilisé des architectures sécurisées. Dans le futur, nous souhaitons aborder ce problème au niveau algorithmique. Nous étudions des solutions qui combineraient une transformation révocable avec un crypto système multi biométrique. Cette thématique a été peu étudiée par les recherches alors qu'il pourrait être utile d'utiliser des approches de type secure sketch sur la biométrie révocable dans le but de combiner les avantages des deux approches (c'est-à-dire que les transformations révocables offrent une bonne diversité et que les secure sketch éliminent le risque de vol de clés qui est dissimulé dans les données auxiliaires).
— Nous souhaitons en outre nous intéresser à tout ce qui concerne la sécurité et la confidentialité des modèles multi biométriques en temps réel , utilisant le deep learning et l'exécution sur une machine HPC.

Bibliographie

[A. K. Jain 2007] P. Flynn et A. A. Ross. A. K. Jain. *Handbook of biometrics.* Springer-Verlag New York, Inc., Secaucus, NJ, USA,, pages 21, 33 et 47, 2007.

[Ababsa 2008] Souhila Guerfi Ababsa. *Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D*. Evry-Val d'Essonne, 2008.

[Adjoudj 2006] Réda Adjoudj. *Authentification automatique par identification et reconnaissance dans un système de haute sécurité*. PhD thesis, Université El Djillali Liabès de Sidi Bel Abbès, 2006.

[Adler 2007] Andy Adler. *Biometric system security*. Handbook of Biometrics. Springer, 2007.

[Allano 2009] Lorène Allano. *La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles*. PhD thesis, Evry, Institut national des télécommunications, 2009.

[Amirthalingam & Radhamani 2014] Gandhimathi Amirthalingam et G Radhamani. *Multimodal Biometric Cryptosystem for Face and Ear Recognition Based on Fuzzy Vault*. Research Journal of Applied Sciences, Engineering and Technology, vol. 7, no. 20, pages 4211–4219, 2014.

[Argyropoulos *et al.* 2010] Savvas Argyropoulos, Dimitrios Tzovaras, Dimosthenis Ioannidis, Yannis Damousis, Michael G Strintzis, Martin Braun et Serge Boverie. *Biometric template protection in multimodal authentication systems based on error correcting codes*. Journal of Computer Security, vol. 18, no. 1, pages 161–185, 2010.

[Arif 2005] Muhammad Arif. *Fusion de données ; ultime étape de reconnaissance de formes : application à l'identification et à l'authentification*. PhD thesis, Tours, 2005.

[Arora *et al.* 2020] Shefali Arora, MPS Bhatia et Harshita Kukreja. *A Multimodal Biometric System for Secure User Identification Based on Deep Learning*. In International Congress on Information and Communication Technology, pages 95–103. Springer, 2020.

[Atanda *et al.* 2021] OG Atanda, AS Falohun et AO Afolabi. *Development of a Multimodal Biometric Security System using Modified Convolutional Neural Network*. LAUTECH JOURNAL OF COMPUTING AND INFORMATICS, vol. 2, no. 1, pages 133–144, 2021.

[Barbier & Rosenberger 2014] Morgan Barbier et Christophe Rosenberger. *Tatouage d'images avec des données biométriques révocables pour la preuve de propriété*. In

Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SAR SSI), 2014.

[Bedad & Adjoudj 2018a] Fatima Bedad et Réda Adjoudj. *Multi-biometric Template Protection : An Overview*. In International Conference in Artificial Intelligence in Renewable Energetic Systems, pages 70–79. Springer, 2018.

[Bedad & Adjoudj 2018b] Fatima Bedad et Réda Adjoudj. *Secured Multimodal Biometric System.* JMPT, vol. 9, no. 3, pages 77–87, 2018.

[Bedad *et al.* 2021] Fatima Bedad, Réda Adjoudj et Nassima Bousahba. *Study of the robustness of a transformation-based multi-biometric template schemes protection*. International Journal of Computing and Digital System, 2021.

[Belguechi *et al.* 2011] Rima Belguechi, T Le-Goff, Estelle Cherrier et Christophe Rosenberger. *Study of the robustness of a cancelable biometric system*. In Network and Information Systems Security (SAR-SSI), 2011 Conference on, pages 1–7. IEEE, 2011.

[Belguechi 2015] Rima Ouidad Belguechi. *Sécurité des systèmes biométriques : révocabilité et protection de la vie privée*. PhD thesis, Ecole nationale Supérieure en Informatique Alger, 2015.

[BENCHENNANE 2015] Ibtissam BENCHENNANE. *Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus*. PhD thesis, University of sciences and technology in Oran, 2015.

[Bennaceur & Bedad 2019] Djeradi Bennaceur et Bedad. Sécurité des systémes multi biométriques. Master's thesis, CUAT, 2019.

[Beulah & Rani 2014] IM Beulah et Leela Rani. *Ensuring Privacy and Renewability Using Helper Data Systems on Multibiometric Cryptosystems*. International Journal of Advanced Research in Computer Science & Technology, 2014.

[Bokade & Kanphade 2019] Gayatri U Bokade et Rajendra D Kanphade. *Secure multimodal biometric authentication using face, palmprint and ear : a feature level fusion approach*. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pages 1–5. IEEE, 2019.

[Bolle *et al.* 2002] Ruud M Bolle, Jonathan H Connell et Nalini K Ratha. *Biometric perils and patches*. Pattern Recognition, vol. 35, no. 12, pages 2727–2738, 2002.

[Bringer *et al.* 2008] Julien Bringer, Hervé Chabanne, Gerard Cohen, Bruno Kindarji et Gilles Zemor. *Theoretical and practical boundaries of binary secure sketches*. IEEE Transactions on Information Forensics and Security, vol. 3, no. 4, pages 673–683, 2008.

[Bringer *et al.* 2017] Julien Bringer, Constance Morel et Christian Rathgeb. *Security analysis and improvement of some biometric protected templates based on Bloom filters*. Image and Vision Computing, vol. 58, pages 239–253, 2017.

[Bruce 1996] Schneier Bruce. *Applied cryptography : protocols, algorithms, and source code in C*. New York : Wiley, 1996.

[Canuto *et al.* 2013] Anne MP Canuto, Fernando Pintro et João C Xavier-Junior. *Investigating fusion approaches in multi-biometric cancellable recognition*. Expert Systems with Applications, vol. 40, no. 6, pages 1971–1980, 2013.

[Chidemyan 2015] Sergey Sergueïevitch Chidemyan. *veine Palm et système de voûte floue multimodale à base d'empreintes digitales*. notes scientifiques de l'Université d'Etat d'Erevan, série Sciences physiques et mathématiques, pages 41–46, 2015.

[Chouaib 2014] Moujahdi Chouaib. *Protection des systèmes de sécurité biométriques : Contributions à la protection des modèles biométriques*. PhD thesis, Université Mohammed V-Agdal, Faculté des Sciences, Rabat, 2014.

[Choudhary & Naik 2021] Swati K Choudhary et Ameya K Naik. *Multimodal Biometric-Based Authentication with Secured Templates*. International Journal of Image and Graphics, vol. 21, no. 02, page 2150018, 2021.

[Damasceno *et al.* 2015] Marcelo Damasceno, Anne MP Canuto et Norman Poh. *Multi-privacy biometric protection scheme using ensemble systems*. In Neural Networks (IJCNN), 2015 International Joint Conference on, pages 1–8. IEEE, 2015.

[Dasgupta & Gupta 1999] Sanjoy Dasgupta et Anupam Gupta. *An elementary proof of the Johnson-Lindenstrauss lemma*. International Computer Science Institute, Technical Report, pages 99–006, 1999.

[Daugman 2000] John Daugman. *Biometric decision landscapes*. Rapport technique, University of Cambridge, Computer Laboratory, 2000.

[Degabriele & Paterson 2010] Jean Paul Degabriele et Kenneth G Paterson. *On the (in) security of IPsec in MAC-then-encrypt configurations*. In Proceedings of the 17th ACM conference on Computer and communications security, pages 493–504. ACM, 2010.

[Dinca & Hancke 2017] Lavinia Mihaela Dinca et Gerhard Hancke. *User-Centric Key Entropy : Study of Biometric Key Derivation Subject to Spoofing Attacks*. Entropy, vol. 19, no. 2, page 70, 2017.

[Dodis *et al.* 2008] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin et Adam Smith. *Fuzzy extractors : How to generate strong keys from biometrics and other noisy data*. SIAM journal on computing, vol. 38, no. 1, pages 97–139, 2008.

[El-Abed 2011] Mohamad El-Abed. *Évaluation de système biométrique*. PhD thesis, Université de Caen, 2011.

[Fiérrez-Aguilar *et al.* 2003] Julian Fiérrez-Aguilar, Javier Ortega-Garcia et Joaquin Gonzalez-Rodriguez. *Fusion strategies in multimodal biometric verification*. In Multimedia and Expo, 2003. ICME'03. Proceedings. 2003 International Conference on, volume 3, pages III–5. IEEE, 2003.

[Geethanjali *et al.* 2012] N Geethanjali, K Thamaraiselvi et R Priyadharshini. *Feature Level Fusion of Multibiometric Cryptosystem in Distributed System*. International Journal of Modern Engineering Research (IJMER), vol. 2, no. 6, pages 4643–4647, 2012.

[Gomez-Barrero *et al.* 2017] Marta Gomez-Barrero, Emanuele Maiorana, Javier Galbally, Patrizio Campisi et Julian Fierrez. *Multi-biometric template protection based on Homomorphic Encryption*. Pattern Recognition, vol. 67, pages 149–163, 2017.

[Gupta *et al.* 2021] Keshav Gupta, Gurjit Singh Walia et Kapil Sharma. *Novel approach for multimodal feature fusion to generate cancelable biometric*. The Visual Computer, vol. 37, no. 6, pages 1401–1413, 2021.

[Hafs 2016] Toufik Hafs. *Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne*. PhD thesis, UNIVERSITE BADJI MOKHTAR-ANNABA, 2016.

[Hao *et al.* 2006] Feng Hao, Ross Anderson et John Daugman. *Combining crypto with biometrics effectively*. IEEE transactions on computers, vol. 55, no. 9, pages 1081–1088, 2006.

[Hoffmann 1989] Walter Hoffmann. *Iterative algorithms for Gram-Schmidt orthogonalization*. Computing, vol. 41, no. 4, pages 335–348, 1989.

[Ismail *et al.* 2015] Suzwani Ismail, Fakariah Hani Hj Mohd Ali et Syed Ahmad Aljunid. *A New Hybrid Approach for Securing Multibiometric Templates Based on Cancelable and Fuzzy Commitment Scheme*. semantic scholar, 2015.

[ISO 2006] ISO ISO. *IEC 19795-1 : Information technology-Biometric performance testing and reporting-Part 1 : Principles and framework*. ISO/IEC, Editor, 2006.

[Iyengar *et al.* 1995] SS Iyengar, L Prasad et Hla Min. *Advances in distributed sensor technology*, 1995.

[Jain *et al.* 1997] Anil K Jain, Lin Hong, Sharath Pankanti et Ruud Bolle. *An identity-authentication system using fingerprints*. Proceedings of the IEEE, vol. 85, no. 9, pages 1365–1388, 1997.

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

[Jeong *et al.* 2006] MinYi Jeong, Chulhan Lee, Jongsun Kim, Jeung-Yoon Choi, Kar-Ann Toh et Jaihie Kim. *Changeable biometrics for appearance based face recognition*. In Biometric Consortium Conference, 2006 Biometrics Symposium : Special Session on Research at the, pages 1–5. IEEE, 2006.

[Jin *et al.* 2004] Andrew Teoh Beng Jin, David Ngo Chek Ling et Alwyn Goh. *Biohashing : two factor authentication featuring fingerprint data and tokenised random number*. Pattern recognition, vol. 37, no. 11, pages 2245–2255, 2004.

[Jourani 2012] Reda Jourani. *Reconnaissance automatique du locuteur par des GMM à grande marge*. PhD thesis, Université de Toulouse, Université Toulouse III-Paul Sabatier ; Université Mohammad V-Agdal de Rabat, 2012.

[Juels & Sudan 2002] A Juels et M Sudan. *A Fuzzy Vault Scheme Proc*. In Intl Symp. Inf. Theory, A Lapidoth, E. Teletar, Eds, page 408, 2002.

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

[Kanade *et al.* 2010] Sanjay Kanade, Dijana Petrovska-Delacrétaz et Bernadette Dorizzi. *Obtaining cryptographic keys using feature level fusion of iris and face biometrics for secure user authentication*. In Computer Vision and Pattern Recognition Workshops (CVPRW), 2010 IEEE Computer Society Conference on, pages 138–145. IEEE, 2010.

[Kankrale & Sapkal 2012] RN Kankrale et SD Sapkal. *Template level concatenation of iris and fingerprint in multimodal biometric identification systems*. International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE), vol. 2, page 29, 2012.

[Karthi & Azhilarasan 2013] Govindharaju Karthi et M Azhilarasan. *Hybrid multimodal template protection technique using fuzzy extractor and random projection*. IJRCCT, vol. 2, no. 7, pages 381–386, 2013.

[Kaski 1998] Samuel Kaski. *Dimensionality reduction by random mapping : Fast similarity computation for clustering*. In Neural networks proceedings, 1998. ieee world congress on computational intelligence. the 1998 ieee international joint conference on, volume 1, pages 413–418. IEEE, 1998.

[Kelkboom *et al.* 2009] EJC Kelkboom, Xuebing Zhou, J Breebaart, Raymond NJ Veldhuis et C Busch. *Multi-algorithm fusion with template protection*. In Biometrics : Theory, Applications, and Systems, 2009. BTAS'09. IEEE 3rd International Conference on, pages 1–8. IEEE, 2009.

[Kumar & Kumar 2016] Amioy Kumar et Ajay Kumar. *A Cell-Array-Based Multibiometric Cryptosystem*. IEEE access, vol. 4, pages 15–25, 2016.

[Kumar *et al.* 2003] Ajay Kumar, David Wong, Helen Shen et Anil Jain. *Personal verification using palmprint and hand geometry biometric*. In Audio-and Video-Based Biometric Person Authentication, pages 1060–1060. Springer, 2003.

[Lalithamani & Sabrigiriraj 2015] N Lalithamani et M Sabrigiriraj. *Palm and hand vein-based fuzzy vault generation scheme for multibiometric cryptosystem*. The Imaging Science Journal, vol. 63, no. 2, pages 111–118, 2015.

[Lina 2016] BENAGGA Abderahmane TELIB Lina. Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt. Master's thesis, UNIVERSITE KASDI MERBAH OUARGLA, 2016.

[Lu & Peng 2014] Li Lu et Jialiang Peng. *Finger multi-biometric cryptosystem using feature-level fusion*. International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, no. 3, pages 223–236, 2014.

[Mai *et al.* 2017] Guangcan Mai, Meng-Hui Lim et Pong C Yuen. *Binary feature fusion for discriminative and secure multi-biometric cryptosystems*. Image and Vision Computing, vol. 58, pages 254–265, 2017.

[Maiorana *et al.* 2011] Emanuele Maiorana, Patrizio Campisi et Alessandro Neri. *Cancellable biometrics for on-line signature recognition*. In New Technologies

for Digital Crime and Forensics : Devices, Applications, and Software, pages 290–315. IGI Global, 2011.

[Maltoni *et al.* 2003] D Maltoni, D Maio et A Jain. *S. Prabhakar,"4.3 : Minutiae-based Methods'(extract) from Handbook of Fingerprint Recognition"*, 2003.

[Maltoni *et al.* 2009] Davide Maltoni, Dario Maio, Anil Jain et Salil Prabhakar. Handbook of fingerprint recognition. Springer Science & Business Media, 2009.

[Matsumoto *et al.* 2002] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada et Satoshi Hoshino. *Impact of artificial gummy fingers on fingerprint systems*. In Proceedings of SPIE, pages 275–289, 2002.

[Meenakshi & Padmavathi 2010] VS Meenakshi et Dr G Padmavathi. *Securing Revocable Iris and Retinal Templates using Combined User and Soft Biometric based Password Hardened Multimodal Fuzzy Vault*. IJCSI International Journal of Computer Science Issues, vol. 7, no. 5, pages 1694–0814, 2010.

[Merkle *et al.* 2012] Johannes Merkle, Tom Kevenaar et Ulrike Korte. *Multi-modal and multi-instance fusion for biometric cryptosystems*. In Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the, pages 1–6. IEEE, 2012.

[Morizet 2009] Nicolas Morizet. *Reconnaissance biométrique par fusion multimodale du visage et de l'iris*. PhD thesis, Télécom ParisTech, 2009.

[Nagar *et al.* 2010a] Abhishek Nagar, Karthik Nandakumar et Anil K Jain. *Biometric template transformation : a security analysis*. In Media Forensics and Security II, volume 7541, page 75410O. International Society for Optics and Photonics, 2010.

[Nagar *et al.* 2010b] Abhishek Nagar, Karthik Nandakumar et Anil K Jain. *A hybrid biometric cryptosystem for securing fingerprint minutiae templates*. Pattern Recognition Letters, vol. 31, no. 8, pages 733–741, 2010.

[Nagar *et al.* 2012] Abhishek Nagar, Karthik Nandakumar et Anil K Jain. *Multibiometric cryptosystems based on feature-level fusion*. IEEE transactions on information forensics and security, vol. 7, no. 1, pages 255–268, 2012.

[Nandakumar & Jain 2008] Karthik Nandakumar et Anil K Jain. *Multibiometric template security using fuzzy vault*. In Biometrics : Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on, pages 1–6. IEEE, 2008.

[Nanni & Lumini 2006] Loris Nanni et Alessandra Lumini. *Empirical tests on biohashing*. Neurocomputing, vol. 69, no. 16, pages 2390–2395, 2006.

[Paul & Gavrilova 2012] Padma Polash Paul et Marina Gavrilova. *Multimodal cancelable biometrics*. In Cognitive Informatics & Cognitive Computing (ICCI* CC), 2012 IEEE 11th International Conference on, pages 43–49. IEEE, 2012.

[Pillai *et al.* 2010] Jaishanker K Pillai, Vishal M Patel, Rama Chellappa et Nalini K Ratha. *Sectored random projections for cancelable iris biometrics*. In Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, pages 1838–1841. IEEE, 2010.

[Ratha *et al.* 2001] Nalini K. Ratha, Jonathan H. Connell et Ruud M. Bolle. *Enhancing security and privacy in biometrics-based authentication systems*. IBM systems Journal, vol. 40, no. 3, pages 614–634, 2001.

[Ratha *et al.* 2006] Nalini Ratha, Jonathan Connell, Ruud M Bolle et Sharat Chikkerur. *Cancelable biometrics : A case study in fingerprints*. In Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, volume 4, pages 370–373. IEEE, 2006.

[Ratha *et al.* 2007] Nalini K Ratha, Sharat Chikkerur, Jonathan H Connell et Ruud M Bolle. *Generating cancelable fingerprint templates*. IEEE Transactions on pattern analysis and machine intelligence, vol. 29, no. 4, pages 561–572, 2007.

[Rathgeb & Busch 2012] Christian Rathgeb et Christoph Busch. *Multi-biometric template protection : Issues and challenges*. In New trends and developments in biometrics. InTech, 2012.

[Rathgeb & Busch 2014] Christian Rathgeb et Christoph Busch. *Cancelable multi-biometrics : Mixing iris-codes based on adaptive bloom filters*. Computers & Security, vol. 42, pages 1–12, 2014.

[Rathgeb & Uhl 2011] Christian Rathgeb et Andreas Uhl. *A survey on biometric cryptosystems and cancelable biometrics*. EURASIP Journal on Information Security, vol. 2011, no. 1, page 3, 2011.

[Rathgeb *et al.* 2015] Christian Rathgeb, Marta Gomez-Barrero, Christoph Busch, Javier Galbally et Julian Fierrez. *Towards cancelable multi-biometrics based on bloom filters : a case study on feature level fusion of face and iris*. In Biometrics and Forensics (IWBF), 2015 International Workshop on, pages 1–6. IEEE, 2015.

[Ross & Poh 2009] Arun Ross et Norman Poh. *Multibiometric systems : Overview, case studies, and open issues*. Handbook of Remote Biometrics, pages 273–292, 2009.

[Ross *et al.* 2006] AA Ross, K Nandakumar et AK Jain. *Handbook of multibiometrics (international series on biometrics). Secaucus*, 2006.

[Saini & Sinha 2011] Nirmala Saini et Aloka Sinha. *Soft biometrics in conjunction with optics based biohashing*. Optics communications, vol. 284, no. 3, pages 756–763, 2011.

[Sankareswari & Jothi 2015] K. Sankareswari et S. A. Jothi. *Hybrid Approach for Securing Biometric Templates such as fingerprint images and iris codes.Using Visual Cryptography.* International Journal of Advance Research, vol. 9, no. 3, 2015.

[Sarier 2021] Neyire Deniz Sarier. *Multimodal biometric authentication for mobile edge computing*. Information Sciences, vol. 573, pages 82–99, 2021.

[Scholar 2016] PG Scholar. *A Biometric Cryptosystem based Secured Future Level Network*. International Journal of Engineering Science, vol. 5388, 2016.

[Sharma & Selwal 2020] Deepika Sharma et Arvind Selwal. *A Novel Transformation Based Security Scheme for Multi-instance Fingerprint Biometric System*. In International Conference on Information, Communication and Computing Technology, pages 147–159. Springer, 2020.

[Stokkenes *et al.* 2016] Martin Stokkenes, Raghavendra Ramachandra, Morten K Sigaard, Kiran Raja, Marta Gomez-Barrero et Christoph Busch. *Multi-biometric template protection—A security analysis of binarized statistical features for bloom filters on smartphones*. In Image Processing Theory Tools and Applications (IPTA), 2016 6th International Conference on, pages 1–6. IEEE, 2016.

[Sushma & Sandeep 2015] HR Sushma et R Sandeep. *Multi Biometric Template Protection using Random Projection and Adaptive Bloom Filter*. International Journal of Research in Electronics and Computer Engineering (IJRECE), vol. 3, no. 2, 2015.

[Tantubay & Bharti 2021] Neeraj Tantubay et Jyoti Bharti. *Multimodal key-binding biocryptosystem using leastsquare polynomial curvefitting based new feature level fusion method*, 2021.

[Teoh *et al.* 2008] Andrew BJ Teoh, Yip Wai Kuan et Sangyoun Lee. *Cancellable biometrics and annotations on biohash*. Pattern recognition, vol. 41, no. 6, pages 2034–2044, 2008.

[Thanki & Borisagar 2015] Rohit M Thanki et Komal R Borisagar. *Experimental study of sparse watermarking techniques for multibiometric system*. Indian Journal of Science and Technology, vol. 8, no. 1, page 42, 2015.

[Tuceryan & Jain 1993] Mihran Tuceryan et Anil K Jain. *Texture analysis*. In Handbook of pattern recognition and computer vision, pages 235–276. World Scientific, 1993.

[Walia *et al.* 2020] Gurjit Singh Walia, Kartik Aggarwal, Kuldeep Singh et Kunwar Singh. *Design and analysis of adaptive graph based cancelable multi-biometrics approach*. IEEE Transactions on Dependable and Secure Computing, 2020.

[Yang *et al.* 2012] Bian Yang, Christoph Busch, Koen De Groot, Haiyun Xu et Raymond NJ Veldhuis. *Performance evaluation of fusing protected fingerprint minutiae templates on the decision level*. Sensors, vol. 12, no. 5, pages 5246–5272, 2012.

[Yildiz *et al.* 2017] Muhammet Yildiz, Berrin Yanikoğlu, Alisher Kholmatov, Alper Kanak, Umut Uludağ et Hakan Erdoğan. *Biometric layering with fingerprints : template security and privacy through multi-biometric template fusion*. The Computer Journal, vol. 60, no. 4, pages 573–587, 2017.

[Yin *et al.* 2011] Yilong Yin, Lili Liu et Xiwei Sun. *SDUMLA-HMT : a multimodal biometric database*. Biometric Recognition, pages 260–268, 2011.

[Zhou *et al.* 2009] Xuebing Zhou, Stephen D Wolthusen, Christoph Busch et Arjan Kuijper. *Feature correlation attack on biometric privacy protection schemes*. In Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on, pages 1061–1065. IEEE, 2009.

حماية البيانات البيومترية المتعددة

من بين نماذج أمن الحاسوب تلك القياسات الحيوية، التي تتعلق باستخدام البيانات الفسيولوجية و السلوكية لتحقق من هوية الأفراد. وعلى الرغم من المزايا التي تتمتع بها هذه الأنظمة البيومترية على أنظمة المصادقة التقليدية ، إلا أنها لا تزال عرضة لقيود معينة ، مما أدى إلى ظهور أنظمة مقاييس حيوية متعددة تتضمن استخدام بيانات بيومترية متعددة لتحسين أداء المصادقة. لسوء الحظ ، حتى الأنظمة متعددة القياسات الحيوية الراسخة تعاني من نقاط الضعف.

في هذه الأطروحة اقترحنا نظاما متعدد المقاييس الحيوية قابلا للإلغاء لتأمين بيانات بيومترية متعددة، ركزنا اهتمامنا على طريقة *BioHashing* وهي تقنية حديثة يمكنها حل مشكلة السرية والأمان. وكان هدفنا هو حماية نظام متعدد الوساط، كان علينا أن نحقق نهج يتكون من الاندماج بين نهجين من الاختلاط على مستوى العينات و على مستوى الحالات ، على أساس التهجين بين القياس الحيوي متعدد الوسائط والتحول القابل للانعكاس. ولتحقيق هذا النهج، قمنا بتجميع وظائف بصمات الأصابع متعددة المستشعرين من ثلاث أصابع بشرية قاعدة بيانات ($SDUMLA-HMT$) . نقترح نموذج تقييم يقوم على أساس مجموعة من المعايير والهجمات المحددة لتقييم معايير الأمن والخصوصية.

الكلمات المفتاحية : أنظمة القياسات الحيوية متعددة الوسائط ، حماية النماذج متعددة القياسات الحيوية ، الهجوم ، الأمن ، التحول ، الأداء.

Résumé

Parmi les paradigmes de la sécurité informatique, la biométrie qui concerne à l'utilisation des données physiologiques et / ou comportementales pour vérifier l'identité des individus. Malgré les avantages de ces systèmes biométriques par rapport aux systèmes d'authentification traditionnels, ils sont encore vulnerables aux limitations spécifiques, ce qui a donné naissance aux systèmes multi biométrie qui consiste à utiliser plusieurs données biométriques pour améliorer les performances de l'authentification. Malheureusement, même les systèmes multi biométriques bien établis souffrent de vulnérabilités. Dans cette thèse, nous avons proposé un schéma multi-biométrique révocable pour sécuriser les données multi-biométriques, nous avons focalisé notre attention sur la méthode BioHashing qui est une technique récente capable de répondre à l'inversion du problème de confidentialité et de sécurité. Notre objectif étant de protéger un système multimodale, nous étions mené à réaliser une approche de fusion de scores à deux niveaux : multi échantillons et multi instances, basée sur l'hybridation entre la biométrie multi modale et la transformation révocable. Pour réaliser cette approche nous avons combiné les fonctions multi-capteurs d'empreintes digitales de trois doigts humains (base de données SDUMLA-HMT).Nous proposons un modèle d'évaluation basé sur un ensemble de métriques et des attaques spécifiques, pour évaluer les critères de sécurité et de protection de vie privée.

Mots clés : Systèmes biométriques multimodaux, protection des modèles multi-biométriques, attaque, sécurité, transformation, performance.

Abstract

One of the paradigms of computer security is biometrics, which concerns the use of physiological and/or behavioural data to verify the identity of individuals.Despite the advantages of these biometric systems over traditional authentication systems, Despite the advantages of these biometric systems over traditional authentication systems, they are still vulnerable to specific limitations, which has given rise to multi-biometric systems. which consists of using several biometric data to improve authentication performance. Unfortunately, even well-established multi-biometric systems suffer from vulnerabilities.In this thesis , we proposed a revocable multi-biometric scheme to secure multi-biometric data, we focused our attention on the BioHashing method which is a recent technique that can solve the inversion of the confidentiality and security problem.Our objective being to protect a multimodal system, we had to realize an approache a two-level scoring merging approach: : multi samples and multi instances, based on hybridation between multi modal biometry and revocable transformation. To achievethis approache we have combined the multi-sensor functions of fingerprints from a three human fingers (SDUMLA-HMT database).We propose an evaluation model based on a set of metrics and specific attacks, to evaluate security and privacy criteria.

Keywords : Multi-modal biometric systems, multi-biometric templates protection, attack, security, transformation, Performance.