République Algérienne Démocratique et Populaire

Ministère de l'enseignement Supérieure et de la Recherche Scientifique

Centre Universitaire Belhadj Bouchaib d'Aïn-Témouchent

Institut des Sciences

Département de Mathématiques et de l'Informatique

Mémoire

Pour l'obtention du Diplôme de Master en Informatique

Option : Réseaux et Ingénierie des Données (RID)

Présenté par :

Melle. BENNACEUR Bouchra

Melle. DJERADI Fayrouz

Sécurité des systèmes multi biométriques

Encadrant :

Mme. BEDAD Fatima

Maitre Assistant "A" à C.U.B.B.A.T.

Soutenu en 2019

Devant le jury composé de :

Président :	Mme. BENOSMAN Amina (M.C.B)	C.U.B.B.A.T.
Examinateurs :	Mr. BOUAFIA ZOUHEYR (M.A.A)	C.U.B.B.A.T.
Encadrant :	Mme. BEDAD Fatima (M.A.A)	C.U.B.B.A.T.

Dédicace

Je dédie ce mémoire

À mes chers parents pour leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières durant toute ma vie, et sans eux je ne serai jamais devenu ce que je suis

À ma sœur et mon frère pour leur appui, leur encouragement, et leur soutien moral

À ma chère grand-mère

À tous mes professeurs et enseignants qui m'ont suivi durant tout mon cursus scolaire et qui m'ont permis de réussir Dans mes études

À toute ma famille et mes amis pour leurs soutiens et leurs encouragements

À Ma chère binôme « Fayrouz» et tous mes collègues avec lesquels j'ai passé 5 années inoubliables

Et à toute personne ayant contribué à ce travail de près ou de loin

Merci d'être toujours là pour moi

BENNACEUR B.

Dédicace

Je dédie ce mémoire à...

À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leurs prières tout au long de mes études

À mes chères sœurs pour leurs encouragements permanents, et leur soutien moral

À toute ma famille et mes amis pour leur soutien tout au long de mon parcours universitaire, et je cite en particulier ma chère copine Bouchra qui m'a beaucoup aider Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible

Merci d'être toujours là pour moi

DJERADI F.

Remerciements

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

Nos remerciements et nos profondes gratitudes vont à notre encadrant Madame, (BEDAD Fatima), pour sa disponibilité et surtout ses judicieux conseils, son écoute et son soutien tout au long de la réalisation de notre travail.

Plus vifs remerciements s'adressent également aux membres de jury Mme BENOSMAN Amina et Mr BOUAFIA Zouheyr qui nous font l'honneur d'accepter de juger notre travail et pour leur précieux temps accordé à l'étude de notre mémoire.

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

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

Résumé

La multi-biométrique est une technologie émergente fait référence à l'utilisation d'une combinaison de deux ou plusieurs modalités biométriques afin d'améliorer les performances de l'authentification / l'identification des individus. En revanche les systèmes multi biométriques souffrent de vulnérabilités à cause de l'impossibilité de révoquer le modèle biométrique. En cas de vol est une préoccupation majeure pour des raisons de confidentialité et de sécurité. Afin de pallier ce problème, nous avons implémenté un schéma de protection des systèmes multi-biométriques basé sur la méthode de transformation des caractéristiques inversible « Biohashing » qui permet de protéger le modèle multi-biométrique révocable. Nous avons proposé deux systèmes multimodaux (avec protection et sans protection) qu'intègrent deux traits à savoir le visage et l'empreinte digitale avec une fusion au niveau des caractéristiques, qu'est précédée une extraction basé sur le filtre de Log-Gabor. Les résultats obtenus montrent une bonne robustesse de ce schéma de protection « Biohashing ». En effet on est arrivé à un taux d'erreur de 0% par rapport à 18.679 % par l'autre système biométrique multimodal sans protection.

Mots clés : Biométrie, multimodale, Sécurité, Fusion des caractéristiques, Log-Gabor, BioHashing, Révocabilité.

Abstract

Multi-biometric is an emerging technology refers to the use of a combination of two or more biometric modalities to improve the performance of authentication/ identification of individuals. On the other hand, the multi-biometric systems suffer from vulnerabilities due to the impossibility of revoking the biometric model. In the event of theft is a major concern for reasons of confidentiality and security. In order to overcome this problem, we have implemented a protection scheme for multi-biometric systems based on transforming invertible characteristics method "Biohashing", which makes it possible to protect the revocable multi-biometric model. We proposed two multimodal systems (with and without protection) that integrate two modalities, namely the face and the fingerprint with a feature level fusion , which is preceded by an extraction based on the Log-Gabor filter. The results obtained show a good robustness of this protection scheme, "Biohashing". Indeed we arrived at an error rate of 0% compared to 18.679% by the other unprotected multimodal biometric system.

Keywords: Biometrics, multimodal, security, feature fusion, Log-Gabor, Bio-Hashing, revocability

Abréviation

ADN : Acide Désoxyribo Nucléique
BKS : Behavior Knowledge Space
CMC : Cumulative Match Caractéristique
EER : Equal Error Rate
FA : Fausses Acceptations.
FAR : False Acceptance Rate
FR : Faux Rejet
FRR : False Rejection Rate
GAR : Gunnies Accept Rate
IBG : International Biometric Group
KNN : K- Nearest Neighbor
LG : Logistique
MAD : Median absolute deviation
ORL : Olivetti Research Laboratory
QLQ : Quadratique-Linéaire-Quadratique
ROC : Receveur Operating Caractéristique
TEE : Taux d'Egale Erreur
TFA : Taux de Fausse Acceptations
TFR : Taux de Faux Rejets

Table des matières

Table des figures

Liste des tableaux

Introduction Générale

Au cours de ces dernières années, l'authentification et l'identification des individus doit être de plus en plus importante dans diverses pratiques quotidiennes, dont cela, la sécurité des systèmes d'information contre les fraudes et les crimes doit être obligatoire. Cependant, les méthodes classiques sont basées sur ce que connait la personne comme un mot de passe, un code, ou sur ce que possède une personne comme un badge ou une carte d'identité, posent des grands problèmes de sécurité car peut être facilitant l'usurpation de l'identité d'une autre personne. Ces problèmes peuvent être éliminés par le développement d'une nouvelle technologie émergente plus fiable appelé la biométrie.

La biométrie est devenue l'une des technologies les plus pertinentes utilisées pour la sécurité des systèmes, il repose sur les caractéristiques de l'être humain pour identifier / authentifier les personnes. 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 systèmes multimodaux qui consiste à concaténer plusieurs données biométriques pour améliorer les performances de l'authentification.

En effet, même les systèmes multi biométriques souffrent de vulnérabilités. Les données biométriques brutes sont directement stockées dans la base. Si la biométrie d'un utilisateur est compromise alors l'identité et la vie privée d'un individu sont également compromises, puisqu'il est impossible de révoquer ou de réémettre le modèle biométrique. Il devient indispensable d'assurer la sécurité, l'intégrité des systèmes multi biométriques et la confidentialité des utilisateurs avec des schémas de protection des modèles multi biométriques sécurisés et révocables.

Notre étude a pour but d'implémenter une approche de protection du système biométrique multimodal, dans lequel nous assurons la sécurité du modèles multi biométriques grâce à l'utilisation d'un schéma de protection révocable « BioHashing », pour améliorer les performances de notre système. En utilisant le filtre de Log-Gabor pour l'extraction des caractéristiques du visage et l'empreinte digitale, une fusion au niveau des caractéristiques, avec une classification par la méthode de plus proche voisin.

Dans ce mémoire, nous allons essayer d'atteindre notre objectif à travers quatre chapitres :
Dans le premier chapitre, nous allons présenter des concepts généraux sur la biométrie et les différentes modalités, ainsi que l'architecture des systèmes biométriques uni-modaux, et nous conclurons par les limitations des systèmes biométriques.
Le deuxième chapitre est consacré à présenter la multi modalité et leurs différentes architectures, ainsi les niveaux de fusions, et les mesures de performance adaptée pour la biométrie.
Dans le troisième chapitre, nous allons présenter un état de l'art sur les différentes techniques proposées pour la protection des systèmes multi biométriques.
Et dans le dernier chapitre, nous présentons la conception des systèmes biométriques multimodaux avec et sans protection. Par la suite nous exposons les résultats de performance obtenue lors de la phase du test d'évaluation de nos systèmes.
Nous clôturons ce mémoire par une conclusion générale, ainsi que les perspectives visées.

Chapitre 1

Des concepts généraux sur la biométrie

Sommaire

1.1 Introduction

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

À ce jour, les méthodes d'identification d'un individu dans un système sont basées sur ce que connait la personne comme un mot de passe, un code, ou sur ce que possède une personne comme un badge ou une carte d'identité, ces derniers posent un grand problème de sécurité car peut être facilement rompue. Donc pour toutes ses raisons, il est obligatoire de créer une nouvelle technologie d'authentification, il s'agit des systèmes biométriques qui sont considérées les plus puissantes en termes de sécurité.

Dans ce chapitre, nous allons présenter des concepts généraux sur la biométrie. On commençant par une définition de terme biométrie. Ensuite, nous décrivons l'architecture des systèmes biométriques, puis nous citons quelques types de modalités utilisées dans les systèmes biométriques, par la suite nous visons une comparaison entre les différentes modalités. Enfin, nous citons les domaines d'application et les limites des systèmes biométriques.

1.2 Définition de la biométrie

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

Le terme biométrie vient du grec ancien "bios" = "vie" et "métron" = "mesure". Bien que la technologie biométrique ait plusieurs utilisations, son objectif principal est de fournir une alternative plus sécurisée aux systèmes de contrôle d'accès traditionnels utilisés pour protéger les actifs personnels ou professionnels[Gregory 2008].

1.3 Les propriétés d'une modalité biométrique

Une caractéristique biométrique idéale devrait respecter les propriétés suivantes [Soltane 2012] :

- **Universalité :** chaque personne devrait posséder les caractéristiques.

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

1.4 Système biométrique

Un système biométrique c'est un système basé sur la reconnaissance de forme d'un individu, sur la base de caractères physiologiques ou de traits comportementaux automatiquement reconnaissable et vérifiable [KIBOU 2018].

1.4.1 Les phases des systèmes biométriques

Un système biométrique fonctionne selon au moins deux phases : La phase d'apprentissage (Learning phase) qui sert à constituer une base de données. La seconde phase est celle de la reconnaissance (Recognition phase) au test qui sert comme son nom l'indique à identifier et/ou authentifier la personne [YADDADEN 2013].

1.4.1.1 Phase d'apprentissage (enrôlement)

Est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données [Morizet 2009]. (voir la figure 1.1).

1.4.1.2 Phase de reconnaissance (test)

Dans cette phase, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir

des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de pré-traitements supplémentaires pour limiter la dégradation des performances [Perronnin 2002]. La suite de la reconnaissance sera différente suivant le mode opératoire du système :

1. **Identification**

   le système doit deviner l'identité d'un individu inconnu. Il répond donc à une question de type : «Qui suis je ?». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données (on parle de test 1 :N) [Perronnin 2002].

2. **Vérification**

   La vérification d'identité consiste à contrôler si l'individu utilisant le système est bien la personne qu'il prétend être. Dans ce cas le système doit répondre à une question de type : «Suis-je bien la personne que je prétends être ?» et renvoie uniquement une décision binaire (oui ou non) [Perronnin 2002]. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données (on parle de test 1 :1).

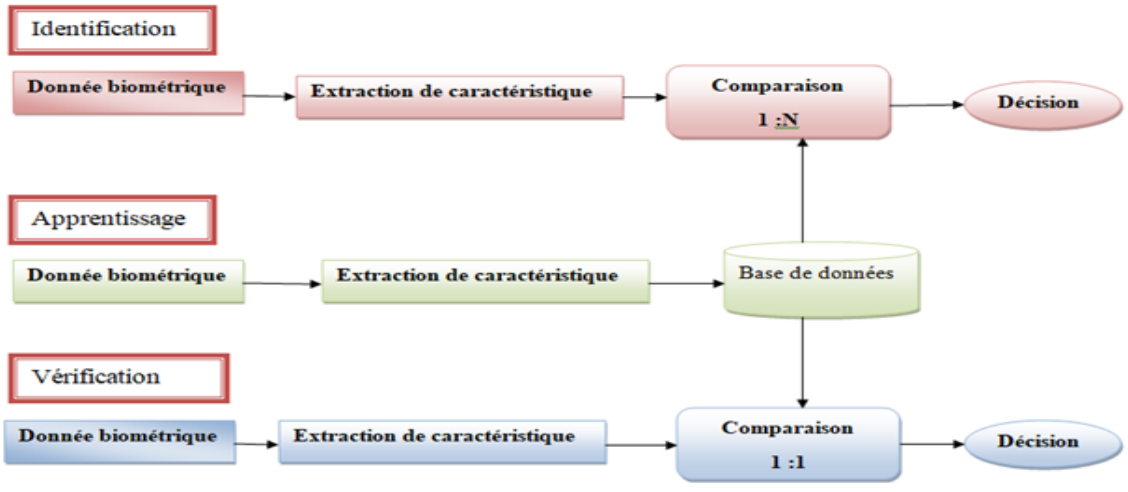


Figure 1.1 – Architecture de système biométrique

1.4.2 Les modules de systèmes biométriques

Un système biométrique est constitué de plusieurs modules [El-Abed 2011] :

- **Le module de capture :** qui consiste à acquérir les données biométriques d'un

individu afin d'extraire une représentation numérique (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, ...etc.).

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

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

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

1.5 Les types de modalités

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

1.5.1 Modalités morphologiques (physiologiques)

Se basée sur l'identification des traits physiques pour chaque individu, qui sont unique et permanents, il existe plusieurs modalité on cite :

L'empreinte digitale

Une empreinte digitale est le motif caractéristique d'un doigt, chaque personne à ses propres empreintes digitales avec l'unicité permanente. Ils sont donc utilisés depuis longtemps pour l'identification et les enquêtes judiciaires [Kaur 2008].

Figure 1.2 – empreinte digitale [Kaur 2008]

Une empreinte digitale est composée de nombreuses crêtes et sillons. Ces crêtes et ces sillons présentent de bonnes similitudes dans chaque petite fenêtre locale, comme le parallélisme et la largeur moyenne. Les deux caractéristiques de crêtes locales les plus importantes, appelées minuties.

Les minuties sont des changements de continuité de l'empreinte digitale. Il existe plusieurs types de minuties : lac, bifurcation, delta ou impasse...etc. Généralement une quarantaine est extraite de la zone scannée. Statistiquement il est impossible de trouver douze points identiques chez deux individus [Kaur 2008].

Figure 1.3 – caractéristiques d'empreinte digitale [Kaur 2008]

Le tableau 1.1 présente une comparaison entre les avantages et les inconvénients de l'utilisation d'empreinte digitale [GHACHOUA 2016] :

Avantages	**Inconvénients**
• Méthode la plus reconnue par le public. • Petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones portables, PC). • Faible coût. • Traitement rapide • Bon compromis entre FAR et FRR.	• Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur). • Certains systèmes peuvent accepter un moulage de doigt ou un doigt coupé (la détection du doigt vivant permet d'éviter ce type d'usurpation).

Table 1.1 – Avantages et Inconvénients de l'utilisation d'empreinte digitale

Le visage

Le visage est certainement la caractéristique biométrique qui les humains utilisent le plus naturellement pour s'identifier entre eux, ce qui peut expliquer pourquoi

elle est en général très bien acceptée par les utilisateurs. Le système d'acquisition est soit un appareil photo, soit une caméra numérique pour développer une image faciale de l'utilisateur pour l'authentification. La difficulté de la reconnaissance du visage varie énormément suivant que l'acquisition se fait dans un environnement contrôlé ou non. Dans un environnement contrôlé, des paramètres tels que l'arrière plan, la direction et l'intensité des sources lumineuses, l'angle de la prise de vue, la distance de la caméra au sujet sont des paramètres maîtrisés par le système. Dans un environnement non-contrôlé, une série de pré-traitements sont souvent nécessaires avant de faire la reconnaissance à proprement parler. Il faut tout d'abord détecter la présence ou l'absence du visage dans l'image (face detection). Le visage doit ensuite être segmenté (face segmentation) [ZITOUNI 2016].

Figure 1.4 – La reconnaissance de visage [ZITOUNI 2016]

Le tableau 1.2 présente une comparaison entre les avantages et les inconvénients de l'utilisation du visage [GHACHOUA 2016] :

Avantages	**Inconvénients**
• accepté par le public • Ne demande aucune action de l'usager, pas de contact physique • Technique peu coûteuse	• Technologie sensible à l'environnement (éclairage, position...) • Les vrais jumeaux ne sont pas différenciés • Sensible aux changements (barbe, moustache, lunette...)

Table 1.2 – Avantages et Inconvénients de l'utilisation du visage

L'iris

L'iris est la membrane colorée, sous forme d'anneau, qui située entre la pupille et le blanc de l'œil. Chaque œil est unique, distinctive et stable durant la vie d'une personne, c'est pour cela la reconnaissance de l'iris est très utilisée dans les applications d'identification et de vérification. L'acquisition de l'iris est effectuée au moyen d'un

capteur qui contient une caméra infrarouge pour pallier aux mouvements inévitables de la pupille.
Le point faible de ce type de système est très sensible (précision, reflet...) et relativement désagréable pour l'utilisation car l'œil doit rester grand ouvert et il est éclaire par une source lumineuse pour assurer un contraste correct [ZITOUNI 2016].

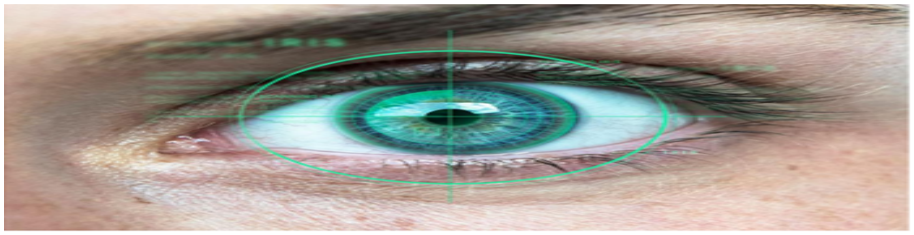


Figure 1.5 – La reconnaissance d'iris [ZITOUNI 2016]

Le tableau 1.3 présente une comparaison entre les avantages et les inconvénients de l'utilisation d'iris [GHACHOUA 2016] :

Avantages	**Inconvénients**
• Grande quantité d'information contenue dans l'iris	• Très sensible à l'environnement, et nécessite une collaboration des utilisateurs
• Vrais jumeaux non confondus	• Les capteurs sont très couteux • Méthode intrusive

Table 1.3 – Avantages et Inconvénients de l'utilisation d'iris

La rétine

Une biométrie basée sur la rétine implique l'analyse de la couche de vaisseaux sanguins située à l'arrière de l'œil. Une technologie bien établie consiste à utiliser une source de lumière de faible intensité au moyen d'un coupleur optique pour numériser les motifs uniques de la rétine. Le balayage précis, mais oblige l'utilisateur à regarder dans un réceptacle et à se concentrer sur un point donné. Ceci n'est pas particulièrement pratique si vous portez des lunettes ou si vous êtes préoccupé par le contact étroit avec l'appareil de lecture [Liu 2001].

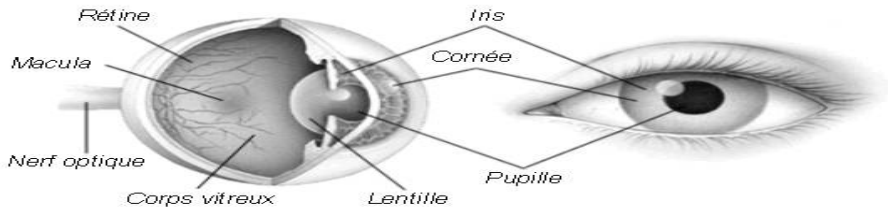


Figure 1.6 – La reconnaissance de la rétine [Liu 2001]

Le tableau 1.4 présente une comparaison entre les avantages et les inconvénients de l'utilisation de la rétine [GHACHOUA 2016] :

Avantages	**Inconvénients**
• L'empreinte rétinienne est peu exposée aux blessures (coupure, brûlure) • Les taux de faux rejet et de fausse acceptation sont faibles • Très difficile, voie impossible, à imiter • La rétine est différente chez les vrais jumeaux • La rétine est stable durant la vie d'un individu	• Système intrusif, il faut placer l'œil près du capteur • Mauvaise acceptation du public (l'œil est un organe sensible) • Coût plus important que d'autres technologies • Pas adapté pour un flux de passage important

Table 1.4 – Avantages et Inconvénients de l'utilisation de la rétine

Géométrie de la main

La géométrie de la main consiste à analyser et mesurer plusieurs caractéristiques de la main : sa longueur, sa largeur, son hauteur, la courbure des doigts...etc. Cette méthode biométrique offre un bon équilibre entre les caractéristiques de performance et relativement facile à utiliser. Cela peut convenir lorsqu'il y a plus d'utilisateurs ou lorsque les utilisateurs ont rarement accès au système et sont peut-être moins disciplinés dans leur approche du système.

La précision peut être très élevée si vous le souhaitez, et le réglage et la configuration des performances souples peuvent s'adapter à un large éventail d'applications. Les organisations utilisent des lecteurs de géométrie à main dans divers scénarios, notamment l'enregistrement de la durée et de la fréquentation, où ils se sont révélés extrêmement populaires. La facilité d'intégration dans d'autres systèmes et processus, associée à la facilité d'utilisation, fait de la géométrie manuelle une première

étape évidente pour de nombreux projets biométriques [Liu 2001].

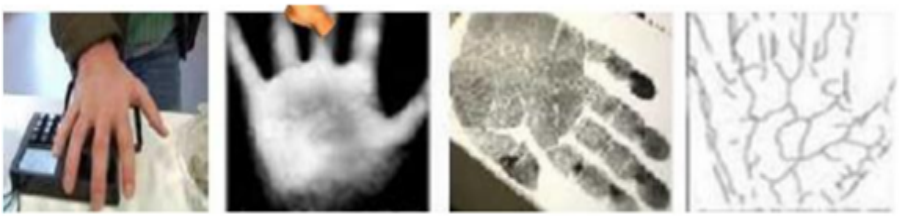


Figure 1.7 – capture de géométrie des main [Liu 2001]

Le tableau 1.5 présente une comparaison entre les avantages et les inconvénients de l'utilisation de la géométrie de la main [GHACHOUA 2016] :

Avantages	**Inconvénients**
• Bonne acceptation des usagés • Très simple à utiliser • Le résultat est indépendant de l'humidité et de l'état de propreté des doigts • Fichier "gabarit" de petite taille	• Trop encombrant pour un usage sur le bureau, dans une voiture ou un téléphone • Risque de fausse acceptation pour des jumeaux ou des membres d'une même famille

Table 1.5 – Avantages et Inconvénients de l'utilisation de la géométrie de la main

1.5.2 Modalités comportementale

Elle est basée sur l'analyse de certains comportements d'une personne.

La signature

La signature a été utilisée depuis longtemps pour identifier des individus. Elle permet de caractériser par sa forme ou bien sa dynamique.

On peut distinguer deux types de signatures hors-ligne et en ligne, la première considère la signature sur les papiers mais le problème c'est que elle est facile à frauder, donc ils ont créé la deuxième qui a été produit sur une tablette digitale ce dernier permet de capturer des caractéristiques dynamiques comme la vitesse, la

pression exercé sur cette tablette pour améliorer l'efficacité de sécurité. Les applications de cette modalité comprennent le contrôle d'accès et l'authentification dans les transactions de commerce électronique [BOUTELLAA,].

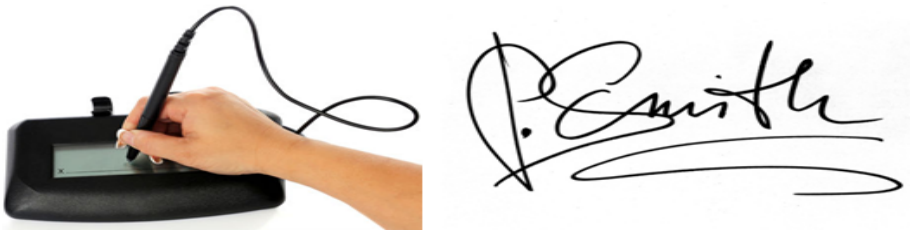


Figure 1.8 – Signature dynamique [BOUTELLAA,]

Le tableau 1.6 présente une comparaison entre les avantages et les inconvénients de l'utilisation de la signature [GHACHOUA 2016] :

Avantages	**Inconvénients**
• La signature écrite sur un document peut être conservée des certains documents • Action qui implique (responsabilité)	• Pas utilisable pour du contrôle d'accès en extérieur par exemple • Sensible aux émotions de l'individu • Besoin d'une tablette graphique

Table 1.6 – Avantages et Inconvénients de l'utilisation de la signature

La voix

A partir de l'oreille et de cerveau, on peut distinguer les personnes par leurs voix. Donc, "Texas Instruments" a développé un modèle biométrie basé sur la voix [ARTABAZ 2011].

Cette modalité basée sur l'analyse des caractéristiques comme les fréquences, les harmoniques et la puissance a fin de prononcer quelques mots.
L'analyse par la voix a été appliqué pour la vérification qui consiste en l'authentification, le contrôle d'accès par téléphone, La détection de l'appartenance de l'interlocuteur à une liste bloquée [BARKA 2016].

Figure 1.9 – image de la voix [BARKA 2016]

Le tableau 1.7 présente une comparaison entre les avantages et les inconvénients de l'utilisation de la voix [GHACHOUA 2016] :

Avantages	**Inconvénients**
• Il est plus facile de protéger le lecteur que dans les autres technologies • Seule information utilisable via le téléphone • Impossible d'imiter la voix • Pas intrusif	• Sensible à l'état physique et émotionnel de l'individu • Taux de faux rejet et fausse acceptation élevés • Sensible aux bruits ambiants • Fraude possible par enregistrement

Table 1.7 – Avantages et Inconvénients de l'utilisation de la voix

Frappe au clavier

La dynamique de frape au clavier appelé aussi la biométrie douce, une modalité biométrique qui permet d'authentifier des individus selon leur façon de taper au clavier. Cette technique a besoin d'un logiciel qui calcule : la vitesse de la frappe, le temps de la frappe, les pauses à partir d'un mot de passe fixe saisi [Giot 2012].

Figure 1.10 – frappe au clavier [Giot 2012]

Le tableau 1.8 présente une comparaison entre les avantages et les inconvénients de l'utilisation de la frappe au clavier [GHACHOUA 2016] :

Avantages	Inconvénients
• Non intrusif, geste naturel pour un individu	• Dépend de l'état (physique, émotion, fatigue...)

Table 1.8 – Avantages et Inconvénients de l'utilisation de la frappe au clavier

1.5.3 Modalités biologiques

Ce type de modalité basé sur l'identification de traits biologique particuliers des personnes telles que l'odeur, le sang, la salive, le cheveu, l'ADN. Cette analyse utilisée généralement dans le domaine médicale.

L'ADN

L'ADN (Acide Désoxyribo Nucléique) est une analyse biologique utilisé pour identifier les humains. Elle considère comme une modalité biométrie la plus sure et efficace car impossible de trouver deux personnes ont le même ADN [BARKA 2016].

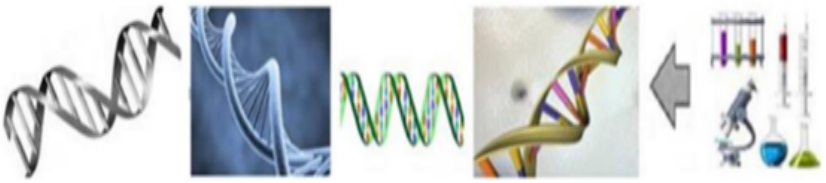


Figure 1.11 – Exemple de l'ADN [BARKA 2016]

Le tableau 1.9 présente une comparaison entre les avantages et les inconvénients de l'utilisation de l'ADN [GHACHOUA 2016]

Avantages	Inconvénients
• Distinguer les individus avec une grande précision	• Lente pour obtenir les résultats
• Il facilite la détection des délinquants	• Avoir un coût élevé

Table 1.9 – Avantages et Inconvénients de l'utilisation de l'ADN

1.6 Comparaison entre les technologies biométriques

N'existe pas un système biométrique parfait. D'une part le Groupe International de la Biométrie IBG (International Biometric Group) a procédé une comparaison des

différentes technologies sur base de 4 facteurs appelée Analyse Zéphyr [Fedias 2013] :

- **Effort** (Effort) : effort fourni par l'utilisateur lors de l'authentification.
- **Intrusion** (Intrusivenes) : information sur l'acceptation du système par les utilisateurs.
- **Coût** (Cost) : coût de la technologie (lecteurs, capteurs, ...etc.).
- **Précision** (Accuracy) : efficacité de la méthode (liée au taux d'erreur ou bien capacité à identifier quelqu'un).

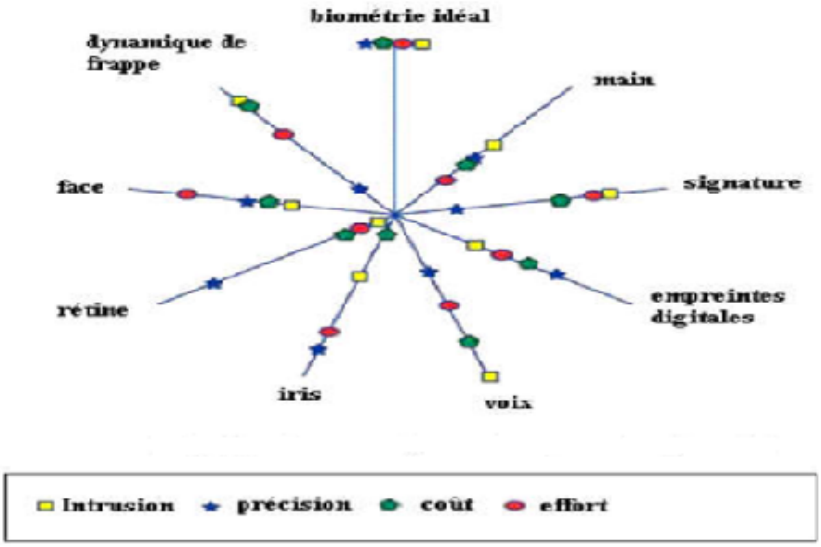


Figure 1.12 – Comparaison de différentes modalité biométrique [Fedias 2013]

Cette comparaison permet de choisir le système idéal en fonction de l'adaptation de l'application à sécuriser.
Pour réussir, un système biométrique doit présenter une logique de marché, c'est-à-dire qu'il doit exploiter le même sens que le périphérique auquel il est joint. Par exemple, la reconnaissance vocale est plus justifiée dans le cadre de l'utilisation du téléphone cellulaire. De même, l'authentification d'une personne à l'aide de sa rétine ou de son iris est plus naturelle lorsque celle-ci désire accéder à son compte bancaire via un guichet automatique, la plupart étant déjà muni d'une caméra. Finalement, un système biométrique qui analyse l'empreinte digitale est plus normalement incorporé à un clavier ou une souris reliant l'ordinateur [Fedias 2013].

1.7 Domaine d'application

Aujourd'hui les principales applications de la biométrie sont la protection d'identité des personnes, le contrôle d'accès à des sites sécurisés, le contrôle des frontières, l'accès aux réseaux, systèmes d'information et stations de travail, le paiement électronique, la signature numérique et même le chiffrement de données... etc. alors on peut trouver la biométrie partout on cite quelques domaines [GHACHOUA 2016] :

Service public

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

Pouvoir judiciaire

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

Secteurs des banques

- Les transactions bancaires (retraits en espèces, les cartes bancaires, paiement par le téléphone et Internet).
- La réduction de la proportion de la fraude grâce à l'intégration des cartes à puce avec la reconnaissance des empreintes digitales.

Accès physique et logique

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

1.8 Les limitations des systèmes biométriques uni-modaux

Les systèmes biométriques uni-modaux sont meilleurs par rapport aux systèmes traditionnels (badge, mots de passe,...). Mais, ils doivent face à de nombreux pro-

blèmes [Allano 2009], parmi eux :

La non-universalité : Malgré l'efficacité des modalités biométriques, on ne peut pas dire qu'un système biométrique uni-modaux est universelle parce qu'il est possible pour un sous-ensemble des utilisateurs de ne pas posséder un biométrique particulier (exemple : des personnes handicapés pour certain modalité).

La non-unicité : Dans certain type du système biométrique uni-modal on peut tomber sur des résultats similaires, par exemple l'apparence faciale des quelques individus (vrai jumeaux, père fils,...).

La variabilité lors de la capture : Est un résultat de plusieurs facteurs : le bruit, la déformation physique de la capture, les erreurs de numérotation... ces variations causent des problèmes lors de la reconnaissance car ils donnent des fausses résultats (même utilisateur mais le système ne l'accepte pas).

La possibilité de fraude : Parmi les limitations des systèmes uni-modaux, la sécurité contre les attaques, exemple les signatures, la voix. Ces modalités sont facile a reproduire aussi il est possible de fraudé l'empreinte digitale.

1.9 Conclusion

De nos jours, la biométrie est considérée comme une technologie permet de renforcer la sécurité des systèmes. Cependant, il existe plusieurs modalités ont été utilisées pour la reconnaissance des personnes.

Dans ce chapitre, nous avons présenté une étude théorique sur les technologies biométriques dans le quel nous avons définir leur architecture, leur fonctionnement, leur domaine d'utilisation et les limitations des systèmes biométriques uni-modaux.

Pour éviter les inconvénients du système biométrique uni-modal, une meilleur solution c'est l'utilisation de plusieurs modalités biométriques au sein d'un même système, on parle alors du système biométrique multimodal qui nous allons présenter dans le chapitre suivant.

Chapitre 2

la biométrie multimodale

Sommaire

2.1 Introduction

Actuellement, il y a une nouvelle tendance qui arrive, c'est la biométrie multimodale, dans lequel on combine plusieurs technologies biométriques, ou plusieurs algorithmes de reconnaissance, ou on utilise divers systèmes pondères dans l'optique d'améliorer les performances de reconnaissance, et l'handicape des systèmes uni-modaux.

Alors dans ce chapitre, nous allons étudier la biométrie multimodale dans le quel on va commencer par une petite définition, par la suite on va citer les différents formes des systèmes multimodaux, ainsi les différents niveaux de fusion et on a terminé par une petite conclusion.

2.2 Définition

La multi-modalité est l'utilisation de plusieurs modalités biométriques. En effet, la biométrie multimodale à pour but de diminuer les limitations des systèmes uni-modaux en combinant plusieurs modalités dans un même système, il permet de réduire le risque d'impossibilité d'enregistrement ainsi que la robustesse aux fraudes. De plus, les systèmes multimodaux permettent d'obtenir de meilleures performances de reconnaissance et d'augmenter l'universalité [Toufik 2016].

2.3 Différentes formes de multi-modalité

Il existe 5 types de systèmes biométriques multimodaux selon les systèmes qu'ils combinent :

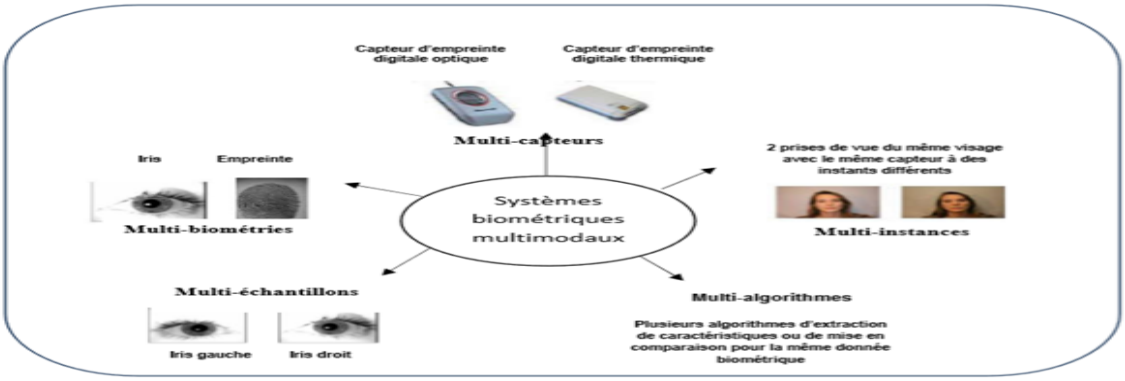


Figure 2.1 – les différents systèmes multimodaux [BENCHENNANE 2015]

2.3.1 Systèmes multi-biométries

Plusieurs modalités biométriques d'une même personne sont acquises et combinées afin d'établir l'identité d'un individu, par exemple combiner le visage et l'empreinte digitale [Jain 2004].

2.3.2 Systèmes multi-capteurs

Pour compléter et améliorer le processus de reconnaissance, plusieurs capteurs sont utilisé pour l'acquisition d'une seule modalité [Dessimoz 2007].
Pour la reconnaissance du visage, par exemple il est possible d'utiliser plusieurs caméras 2D, des capteurs 3D ainsi que des capteurs infra-rouges [DEHACHE 2014].

2.3.3 Systèmes multi-échantillons

Lorsque utilisé un capteur pour extrait plusieurs échantillons ou variantes d'une seule trait pour améliorer le processus de reconnaissance [Dessimoz 2007], par exemple les empreintes digitales de plusieurs doigts, les images de l'iris gauche et droite [POP 2008].

2.3.4 Systèmes multi-instances

Acquisition de plusieurs instances ou unités de la même modalité biométrique [DEHACHE 2014], par exemple plusieurs échantillons de voix, l'acquisition de plusieurs images de visage avec des changements de pose [Allano 2009].

2.3.5 Systèmes multi-algorithmes

La même modalité est traitée à travers plusieurs méthodes ou algorithmes différents [GHACHOUA 2016] par exemple il est possible d'utiliser deux algorithmes pour la reconnaissance des empreintes digitales, l'un opérant sur les caractéristiques texturales, l'autre sur les minuties ou les filtrages extraites à partir d'un même doigt [DEHACHE 2014].

2.4 Architecture des systèmes multimodaux

Les systèmes biométriques multimodaux sont une fusion de plusieurs systèmes biométriques et nécessitent donc l'acquisition et le traitement de plusieurs données qui peuvent se faire successivement (en série) ou simultanément (en parallèle).

2.4.1 L'architecture en parallèle

Dans ce type il permet d'utiliser tous les informations disponibles dans le système simultanément, dont le but d'améliorer les performances de la reconnaissance, c'est pour cela il est plus utilisé. En revanche, l'acquisition et le traitement d'un grand nombre de données biométriques est coûteux en temps et en matériel, et réduit le confort d'utilisation [Nandakumar 2005]. (Voir la figure 2.2).

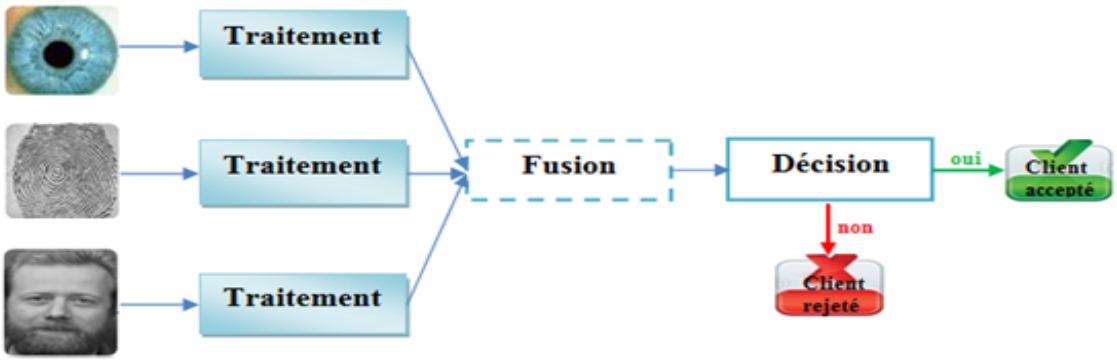


Figure 2.2 – Architecture en parallèle [Nandakumar 2005]

2.4.2 L'architecture en série

Généralement, l'acquisition des données biométriques s'effectue séquentiellement pour des raisons purement pratiques. Par exemple, lorsqu'un système biométrique multimodal en série a une confiance suffisante en l'identité de l'utilisateur après le traitement de la première modalité, l'utilisateur peut ne pas être tenu de fournir les autres modalités [Nandakumar 2005]. (Voir la figure 2.3)

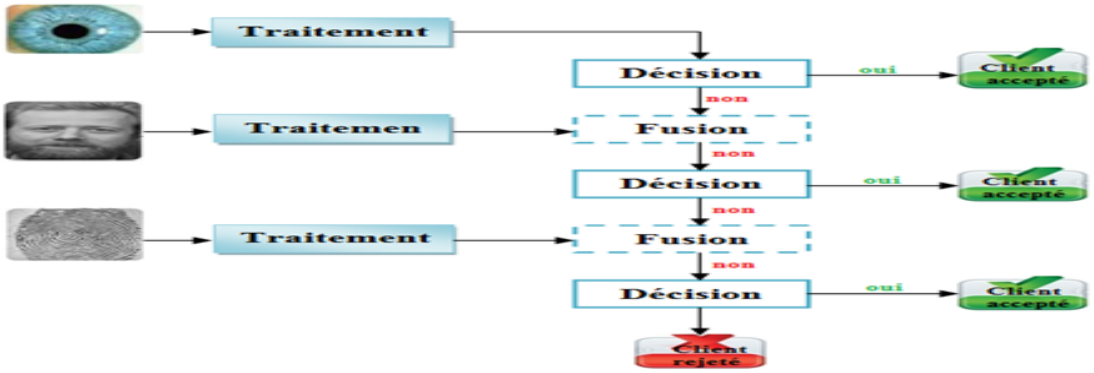


Figure 2.3 – Architecture en série [Nandakumar 2005]

2.5 Niveaux de fusion de la biométrie multimodale

En biométrie multimodale, nous utilisons plus d'une modalité biométrique, nous avons plus d'un canal de décision, alors nous devons concevoir un mécanisme capable de combiner les résultats de la classification de chaque canal biométrique, c'est ce qu'on appelle la fusion biométrique.

La fusion biométrique multimodale c'est la combinaison de plusieurs systèmes biométriques pour renforcer les forces et atténuer les faiblesses des mesures individuelles [Toufik 2016], et peut se faire à quatre niveaux différents (la figure 2.4 résume les 4 niveaux).

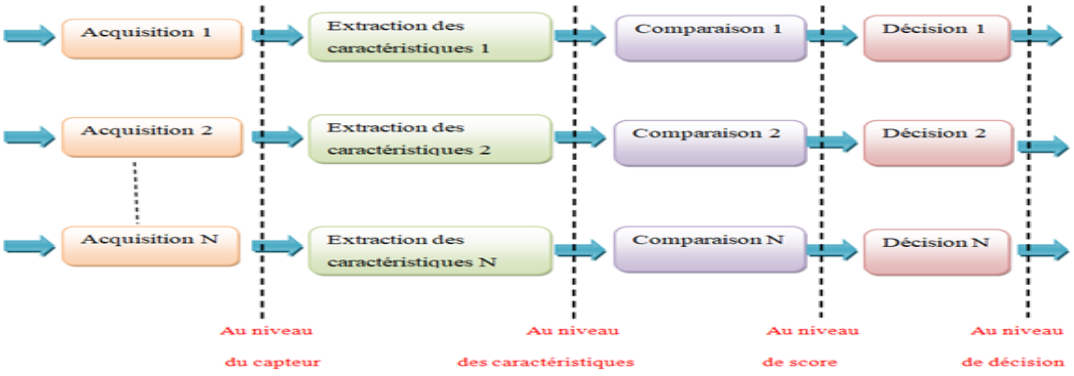


Figure 2.4 – Les niveaux de fusion

Ces quartes niveaux de fusion peuvent être classés en deux sous-ensembles : La fusion pré-classification et la fusion post-classification.

2.5.1 La fusion pré-classification (avant la comparaison)

La fusion pré-classification correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur (images brutes) ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques [Allano 2009].
La fusion à ces deux niveaux est limitée car elle nécessite une homogénéité entre les données. Par exemple, la combinaison de plusieurs images de visages en visible et en infrarouge s'ils correspondent à la même scène (pour le premier niveau), un autre exemple qui ne nécessitent pas vraiment d'homogénéité est la concaténation

de plusieurs vecteurs de caractéristiques avant le traitement par l'algorithme de comparaison (pour le deuxième niveau) [BENCHENNANE 2015].

2.5.1.1 Fusion au niveau du capteur (Sensor Level)

Ce mode de fusion s'agit de combiner plusieurs traits biométriques au niveau du capteur (images brutes), pour le but de former une donnée et un processus biométrique composite et qui contient plus d'informations [DJILI 2016]. Par exemple, détecter un signal de parole simultanément avec deux différents microphones. Un autre exemple, les images du visage obtenues par différentes caméras sont combinées pour former un modèle 3D du visage. La fusion au niveau du capteur n'est généralement pas possible si les instances des données sont incompatibles [DEHACHE 2014] (par exemple, il est difficile de fusionner des images de visages provenant de caméras ayant des résolutions différentes). La figure 2.5 illustre la fusion au niveau du capteur.

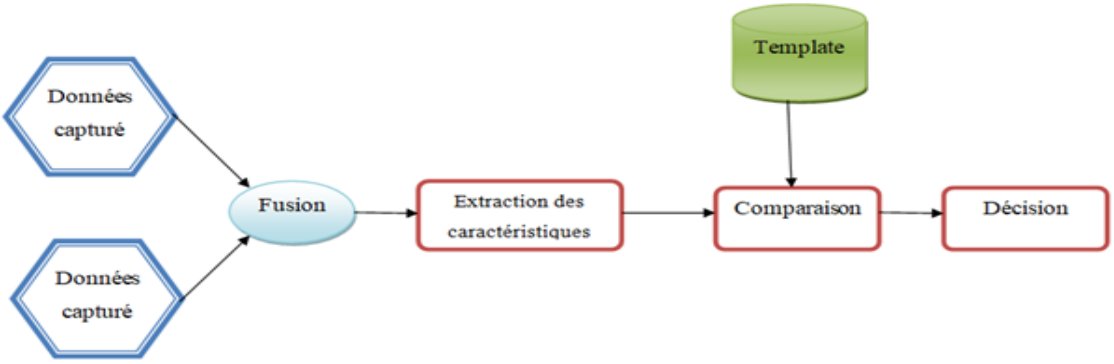


Figure 2.5 – Fusion au niveau de capteur

2.5.1.2 Fusion au niveau des caractéristiques (Feature Level)

Ce mode de fusion consiste à combiner plusieurs vecteurs de caractéristiques qui sont provenus à partir l'une des sources suivantes : plusieurs capteurs du même trait biométrique, plusieurs algorithmes du même trait biométrique, ou encore plusieurs traits biométriques[DEHACHE 2014]. Quand les vecteurs de caractéristiques sont homogènes (comme par exemple plusieurs impressions d'empreinte digitale d'un doigt ou visage), une somme pondérée peut être appliquée pour obtenir un seul vecteur de caractéristiques [Hili 2016]. Dans le cas ou les vecteurs de caractéristiques sont hétérogènes (comme par exemple des vecteurs de caractéristiques de différentes modalités biométriques telles que : le visage et la géométrie des mains), une concaténation de ces derniers est possible par l'algorithme de comparaison afin de former

un seul vecteur de caractéristiques. La concaténation n'est pas possible dans le cas où les caractéristiques ne sont pas compatibles [Nandakumar 2005] (c'est le cas pour les minuties des empreintes et les coefficients d'Eigen-face, par exemple).

La fusion au niveau des caractéristiques offre certes une information plus riche mais, néanmoins, elle est difficile à réaliser dans la pratique pour les raisons suivantes [Nandakumar 2005] :

- La dépendance entre les espaces caractéristiques à fusionner qui est généralement inconnue et qui nécessite d'éliminer les caractéristiques fortement corrélés.
- La concaténation des vecteurs caractéristiques risque de conduire à un espace caractéristique excessivement grand.
- Les vecteurs caractéristiques générés par les systèmes biométriques commerciaux sont la propriété des vendeurs qui, la plupart du temps n'y donnent pas accès.

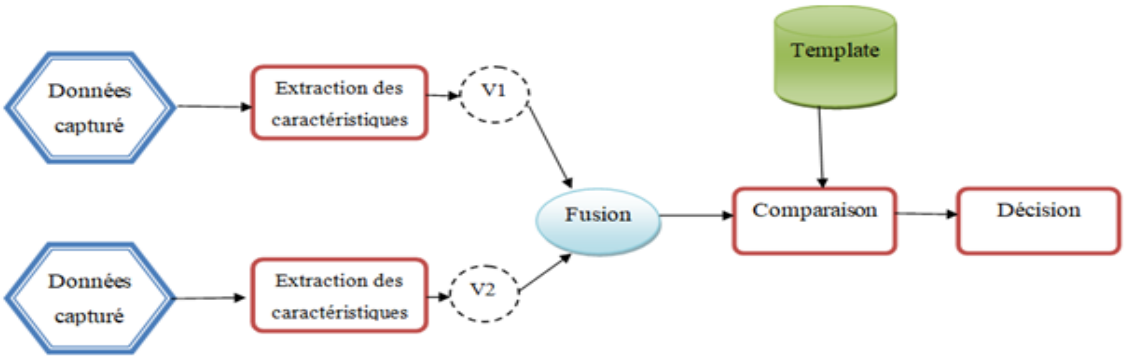


Figure 2.6 – Fusion au niveau des caractéristiques

2.5.2 la fusion post-classification (après la comparaison)

Les schémas d'intégration de l'information après la classification peuvent être divisés en deux catégories : fusion au niveau des scores issus des modules de comparaison et fusion au niveau des décisions [Morizet 2009].

2.5.2.1 Fusion au niveau du score (matching score level)

C'est la méthode la plus utilisé et elle est appliqué dans tous les types de systèmes. Il est facile de combiner les scores générés par les différents matchers. En effet, dans l'approche de classification, un vecteur de caractéristiques est construit en utilisant les scores d'appariement générés par les correspondants individuels, ce vecteur de

caractéristiques est ensuite classé dans l'une des deux classes suivantes : «Accepter» (utilisateur authentique) ou «Rejeter» (imposteur). En conséquence, ce dernier est capable d'apprendre la limite de décision, quelle que soit la manière dont le vecteur de caractéristiques est générée [Morizet 2009].

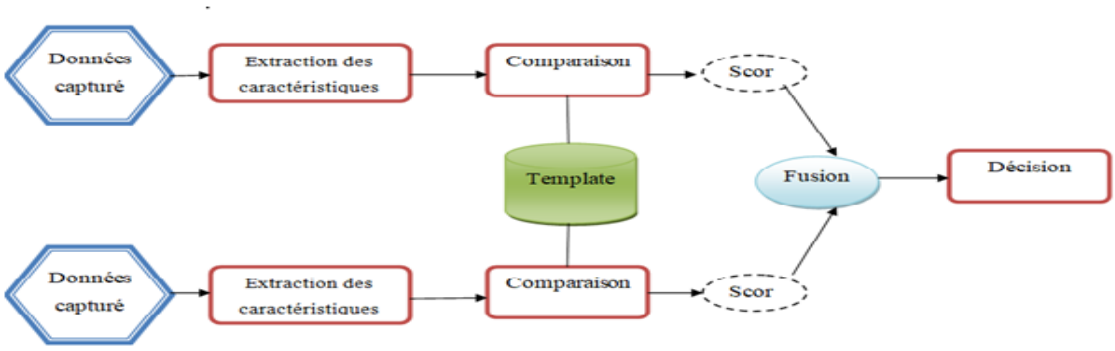


Figure 2.7 – Fusion au niveau de score

Pour appliquer cette méthode on utilise des techniques de normalisation des scores et des méthodes de combinaisons des scores.

1. **Les techniques de normalisation**

Une étape de normalisation est généralement nécessaire avant que les scores bruts provenant de différents classificateurs peuvent être combinés dans l'étape de fusion. Avant de combiner les scores de matchers on a trois problèmes doivent être considérés, premièrement les scores correspondants à la sortie des matchers individuels peuvent ne pas être homogènes. Par exemple, un matcher peut générer une mesure de distance (disimilarité), tandis qu'un autre peut générer une mesure de proximité (similarité). De plus, les résultats des matchers individuels ne doivent pas nécessairement se trouver sur le même intervalle. Enfin, les scores en sortie des matchers peuvent suivre différentes distributions statistiques [Jain 2005]. Les différentes techniques de normalisation de scores sont :

- Normalisation par la méthode Min-Max.
- Normalisation par une fonction quadratique-linéaire-quadratique (QLQ).
- Normalisation par la méthode Z-Score.
- Normalisation par la médiane et l'écart absolu médian (MAD).
- Normalisation par la méthode tangente hyperbolique "Tanh ".

- Normalisation par une fonction double sigmoïde
- Normalisation par logistique (LG)

Nous présentons dans la suite, les trois méthodes de normalisation les plus connues en occurrence la méthode Min-Max, la méthode Z-score et la méthode TanH [Soltane 2012].

- **Normalisation par la méthode Min-Max**

  Cette méthode normalise les scores bruts à l'intervalle [0, 1]. La normalisation min-max est définie pour un score donné S_k selon l'équation suivante, où min et max désignent les scores minimal et maximal du matcher k [Jain 2005].
  Étant donné un ensemble de scores correspondants $S_k, k = 1, 2, ..., n$, les scores normalisés sont donnés par :

$$S'_k = \frac{S_k - min}{max - min} \tag{2.1}$$

- **Normalisation par la méthode Z-score**

  Cette méthode de normalisation est la plus couramment utilisée, elle calculé à l'aide de la moyenne arithmétique et de l'écart type des données. Les scores normalisés sont donnés par [Jain 2005] :

$$S'_k = \frac{S_k - \mu}{\sigma} \tag{2.2}$$

  Où μ est la moyenne arithmétique et σ l'écart type des données.

- **Normalisation par la méthode tangente hyperbolique Tanh**

  Cette méthode introduits par Hampel et al. Sont robustes et très efficaces. Elle est parmi les techniques statistiques les plus solides. La normalisation est donnée par [Jain 2005] :

$$S'_k = \frac{1}{2}\left\{tanh\left(0.01\left(\frac{S_k - \mu_{Gh}}{\sigma_{Gh}}\right)\right) + 1\right\} \tag{2.3}$$

  où μ_{GH} et σ_{GH} sont respectivement les estimations de déviation moyenne et de l'écart type distribution du score authentique.

le Tableau 2.1 résume les caractéristiques de chacune des techniques de normalisation sus-présentées, en termes de robustesse et d'efficacité [Jain 2005].

Technique de normalisation	**Robustesse**	**Efficacité**
Min-Max	Non	N/A
Decimal scaling	Non	N/A
Z-score	Non	Élevée (optimale pour des distribution gaussiennes)
Mediane et MAD	Oui	Modérée
Double sigmoïde	Oui	Élevée
Estimateurs Tanh	Oui	Élevée

Table 2.1 – Récapitulatif des techniques de normalisation de score [Jain 2005]

2. **Les méthodes de combinaisons de scores**

Les méthodes de combinaisons de scores sont des méthodes très simples dont l'objectif est d'obtenir un score final S à partir des N scores disponibles si pour i = 1 à N issus de N systèmes.

Les méthodes les plus utilisées sont le minimum, maximum, la somme, la somme pondéré et le produit [Jain 2005].

- Combiner les scores par la somme consiste à calculer [DJILI 2016] :

$$S = \sum_{i=1}^{N} W_i * S_i \tag{2.4}$$

La somme pondérée permet de donner des poids différents W_i à chacun des sous-systèmes en fonction de leur performance individuelle ou de leur intérêt dans le système multimodal [Toufik 2016].

- Combiner les scores en multipliant tous les scores [DJILI 2016] :

$$S = S_1 * S_2 .....S_n \tag{2.5}$$

- Combiner les scores par le minimum consiste à calculer [DJILI 2016] :

$$S = min\,(S_1 S_2 .....S_n) \tag{2.6}$$

- Combiner les scores par le maximum consiste à calculer [DJILI 2016] :

$$S = max\,(S_1 S_2 .....S_n) \tag{2.7}$$

- Combiner les scores par la somme pondéré consiste à calculer [DJILI 2016] :

$$S = \sum_{i=1}^{N} S_i \tag{2.8}$$

la fusion au niveaux de score offre de meilleures performances que les autres niveaux de fusion car les rangs correspondants sont facilement disponibles et contiennent suffisamment d'informations pour la distinguer. Comme il donne de meilleures performances de manière pratique et réalisable. La portée est suffisante pour concevoir une fusion au niveau score [Geetha 2013].

2.5.2.2 Fusion au niveau de décision (decision level)

L'intégration de l'information au niveau de décision, on dit aussi haut niveau de fusion, peut avoir lieu lorsque chaque modalité est d'abord identifiée de façon indépendante, et fournit une décision binaire sous la forme OUI ou NON qui l'on peut représenter par 0 et 1 (comme par exemple accepté : 1 et rejeté : 0, ou dans le cas de la vérification, l'identité d'un utilisateurs dans le cas d'identification). Pour arriver à la décision finale il existe plusieurs méthodes comme celle le vote à la majorité « Majority voting » (exemple si la majorité des systèmes ont décidé 1 alors OUI) [DEHACHE 2014], le BKS « behavior knowledge space » [Lam 1995], le « weighted voting » basé sur la théorie Dempster-Shafer [Xu 1992] et les règles AND (si tous les systèmes ont décidé 1 alors OUI) et OR (si un système a décidé 1 alors OUI) la figure 2.8 illustre la fusion au niveau de décision.

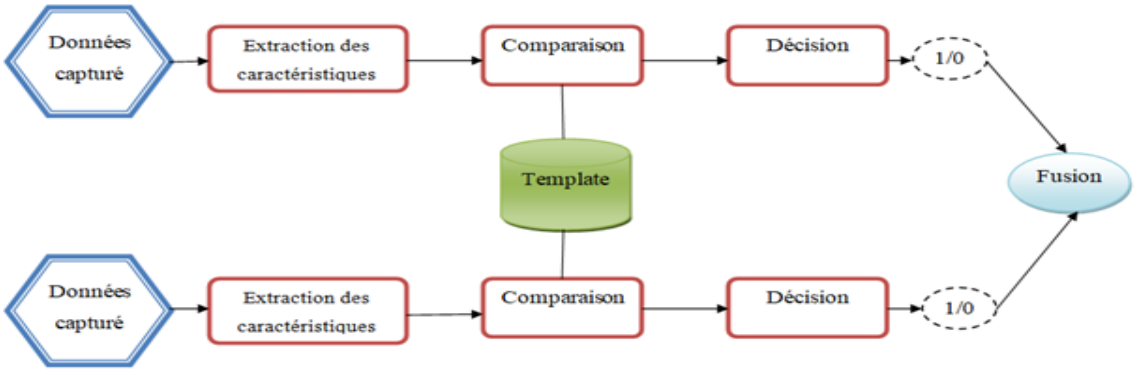


FIGURE 2.8 – Fusion au niveau de décision

2.6 Performances des systèmes biométriques

La performance d'un système de reconnaissance biométrique peut se mesurer principalement à l'aide de trois critères : sa précision, son efficacité (vitesse d'exécution) et le volume de données qui doit être stocké pour chaque personne. il existe deux indicateurs d'erreur qui peuvent être utilisés pour évaluer leur performance [BENCHENNANE 2015].

- **Le taux de faux rejets "TFR"** (False Rejection Rate "FRR") : Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.[BENCHENNANE 2015].

$$FRR = FR/NL \tag{2.9}$$

FR : nombre faux rejets.
NL : nombre total légitimes.

- **Le taux de fausse acceptations "TFA"**(False Acceptance Rate "FAR") : Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système [BENCHENNANE 2015].

$$FRR = FA/NI \tag{2.10}$$

FA : nombre fausses acceptations.
NI : nombre total imposteurs.
il existe aussi

- **Le Taux d'égale erreur "T.E.E"** (Equal Error Rate "EER"), donne un point sur lequel le **FRR** est égal au **FAR**.

$$ERR \rightarrow FAR = FRR \tag{2.11}$$

La figure 2.9 illustre la variation de FAR et FRR en fonction de seuil de décision, et la figure 2.10 illustre le FAR et FRR a partir de distributions des scores imposteurs et authentique.

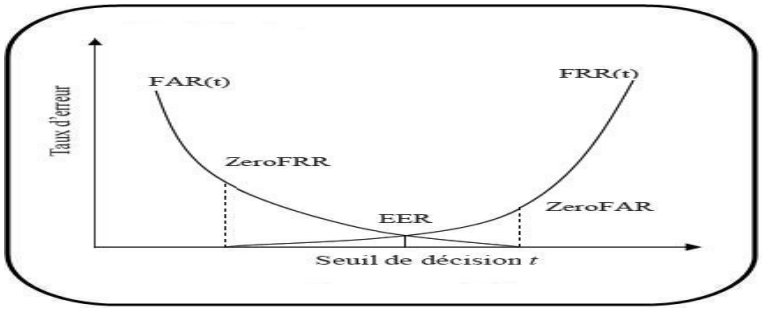


Figure 2.9 – Variation des FRR et FAR en fonction du seuil de décision varie [Ross 2006]

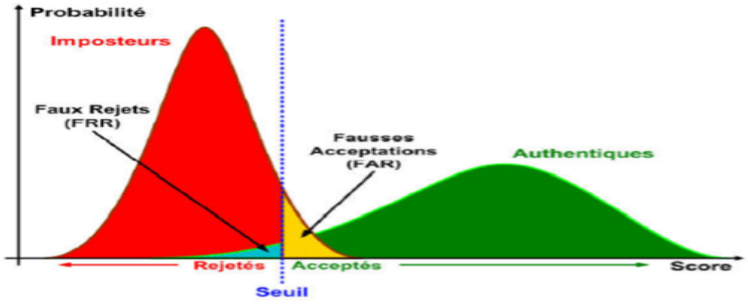


Figure 2.10 – Distributions de scores authentiques et imposteurs [BENCHENNANE 2015]

Comme nous avons vu précédemment, l'identification et la vérification sont des modes opératoires différents, alors selon la nature du système biométrique, il existe deux façons d'en mesurer la performance.

- Lorsqu'un système opère en mode **authentification (vérification)**, les performances de système est présenté à l'aide de la courbe **ROC** ("Receveur Operating Caractéristique" en anglais) illustrée par à la figure 2.11, cette courbe trace le FRR en fonction du FAR. Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé [Ross 2006].
- En revanche, dans le cas d'un système utilisé en mode **identification**, on utilise ce qui l'on appelle une courbe **CMC** ("Cumulative Match Caractéristique" en anglais). La courbe CMC donne le pourcentage de personnes reconnues en fonction d'une variable qui l'on appelle le rang. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On peut donc dire que plus le rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité

Figure 2.11 – Exemple de Courbe ROC [Ross 2006]

faible [Morizet 2009]. La figure2.12 montre un exemple de courbe CMC :

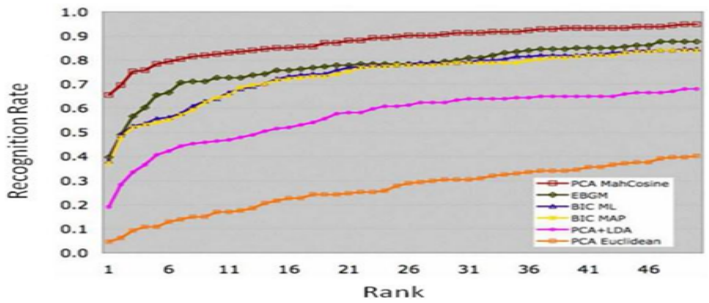


Figure 2.12 – Exemple de courbe CMC [Morizet 2009]

2.7 Conclusion

Dans ce chapitre, nous avons présenté la biométrie multimodale dans le quel nous avons commencé par une définition de multi modalité, ensuite nous avons cité son intérêt et son architecture, ainsi les différentes formes des systèmes biométriques multimodaux, et on a terminé par les niveaux de fusion qui peuvent être utilisés dans un système multimodal dans le but d'améliorer la performance de l'authentification /identification des personnes et rendre la sécurité plus robuste et plus 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, et la performance des systèmes biométriques.

Dans le chapitre suivant, nous présentons un état de l'art de l'ensemble de solutions proposées pour la protection des données multi biométriques.

Chapitre 3

État de l'art : Protection du modèle multi biométrique

Sommaire

3.1 Introduction

La sécurité est une nécessité pour avoir des systèmes biométrique robustes et conviviaux.

Dans ce chapitre, nous allons présenter une étude de l'état de l'art des travaux liés à la protection des systèmes de sécurité multi biométriques. Ce chapitre passe en revue les différentes techniques proposées au sein de la communauté de recherche en sécurité des systèmes multi biométriques, en soulignant les limites et les avantages de chacune d'elle.
Deux catégories de solutions pour protéger les modèles biométriques ont été citées dans ce chapitre : les modèles basés sur la transformation des caractéristiques et les crypto systèmes biométriques.

Dans cet mémoire, nous sommes principalement concernés par les approches de transformation inversible plus précisément, nous sommes plus intéressés à l'approche de Biohashing.

3.2 Sécurité multi biométrique

L'objectif principal de la recherche dans le domaine de la protection multi biométrique est de généré des projets industriels qui sont présentés sur un Framework générique. Le système devrait être capable d'intégrer des n modèles, sans la nécessité de suivre des niveaux de fusion spécifique pour leur représentions, (k la représentation pourrait être impliquée). Le processus se poursuit avec la représentation et le système générique a été appliqué pour la protection des données biométriques (voir la figure 3.1). Dans un module de fusion, une représentation commune de vecteurs de caractéristiques est établie et les vecteurs de caractéristiques sont combinés de manière sensible. Par la suite, un schéma de protection de modèle adéquat est appliqué pour protéger le modèle multi-biométrique. Se concentrer sur une fusion générique de modèles multi-biométrique dans un système de protection de modèle, plusieurs problèmes évoluent [Rathgeb 2012].

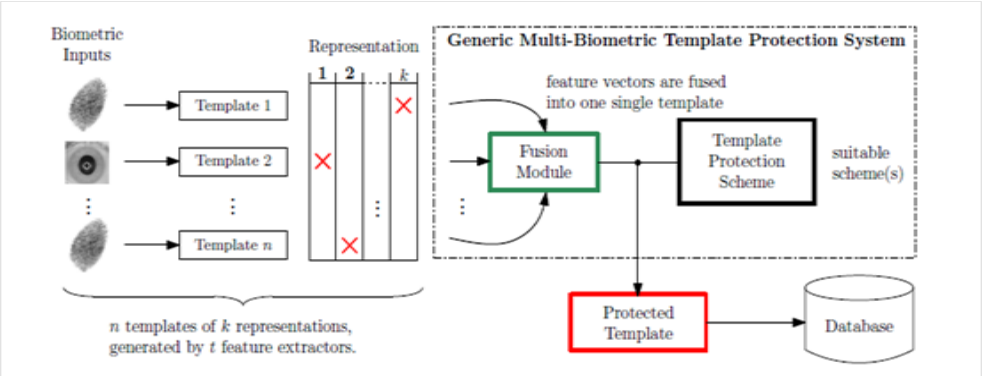


Figure 3.1 – Le framework d'une protection générique multi-biométrique au niveau des caractéristiques [Rathgeb 2012]

La littérature actuelle sur les méthodes de protection de modèles multi-biométrique sont largement classifies.

3.3 Les schémas de protection du modèle multi biométrique

Un schéma de protection de modèle biométrique idéal devrait posséder les quatre propriétés suivantes [Maltoni 2003].

- **Diversité :** le modèle sécurisé ne doit pas permettre la compatibilité croisée sur des bases de données, assurant ainsi la confidentialité de l'utilisateur.
- **Révocabilité :** il devrait être simple de révoquer un modèle compromise et relancez un nouvel basée sur les mêmes données biométriques.
- **Irréversibilité :** Il doit être difficile d'obtenir des calculs du gabarit biométrique d'origine à partir du modèle sécurisé. Cette propriété empêche un adversaire de créer une parodie physique de la caractéristique biométrique à partir d'un modèle de vol.
- **Performance :** le programme de protection de modèle biométrique ne devrait pas dégrader les performances de reconnaissance (FAR et FRR) du système biométrique.

Les schémas de protection des modèles biométriques proposés dans la littérature peuvent être classés en deux catégories (voir la figure 3.2), à savoir (i) les cryptosystèmes Biométriques et (ii) les approches par transformation.

Le point commun à toutes ces méthodes réside dans le fait de ne pas stocker directement dans la base les données biométriques brutes : elles sont soit stockées sur un support externe (carte à puce, token), soit stockées après une transformation [Belguechi 2011].

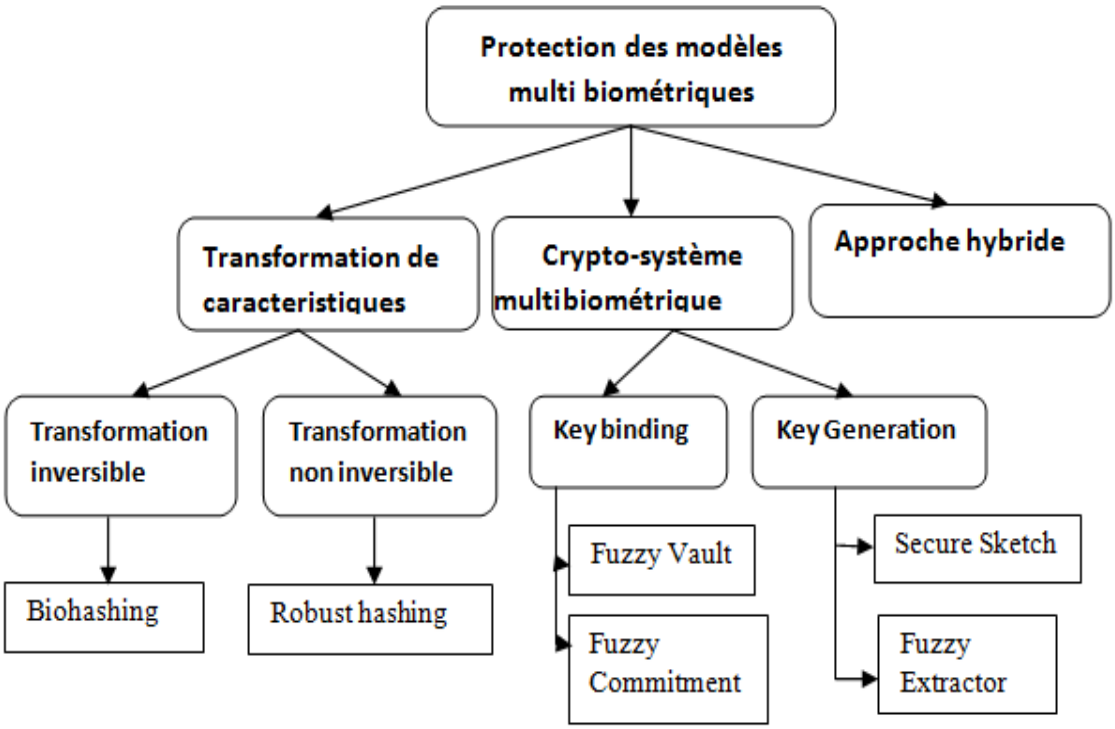


Figure 3.2 – les catégories de protection des modèles multi biométriques [Maltoni 2003]

3.3.1 Les crypto-systèmes multi biométriques

Les crypto-systèmes multibiométriques sont la combinaison entre le crypto-système et la multibiométrie, le principe des crypto systèmes classiques [Schneier 1995] [Ferguson 2010] ont été combiné avec le principe de la reconnaissance biométrique pour améliorer la sécurité des systèmes d'authentification personnelle basés sur la biométrie.

L'objectif principal de ces approches est de minimiser le taux des données biométriques stockées dans les modèles protégés et la base de données du système en général. Le fonctionnement de la plupart des crypto-systèmes biométriques est comme suit : durant l'inscription, on applique un code correcteur d'erreur φ sur le modèle biométrique **B** et une clé **K** pour extraire l'ensemble de données **H** (l'ensemble H

est appelé Helper Data en anglais). Au moment de l'authentification, on applique un code correcteur d'erreur φ sur les helper data **H** et le modèle de test **Q** pour récupérer la clé **K** (Figure 3.3). Selon la façon dont les helper data sont extraites, les crypto-systèmes biométriques peuvent être divisés en deux catégories [Jain 2008] [Christian 2001] : Les crypto systèmes de type key-binding et les crypto-systèmes de type key-generation.

Lorsque les helper data sont obtenues en utilisant une clé qui est indépendante des caractéristiques biométriques, il s'agit d'un crypto-système de type key-binding. Si les helper data sont dérivées seulement à partir du modèle biométrique et la clé est générée directement à partir des caractéristiques biométriques, il s'agit d'un crypto-systèmes de type key-generation [Jeong 2006].

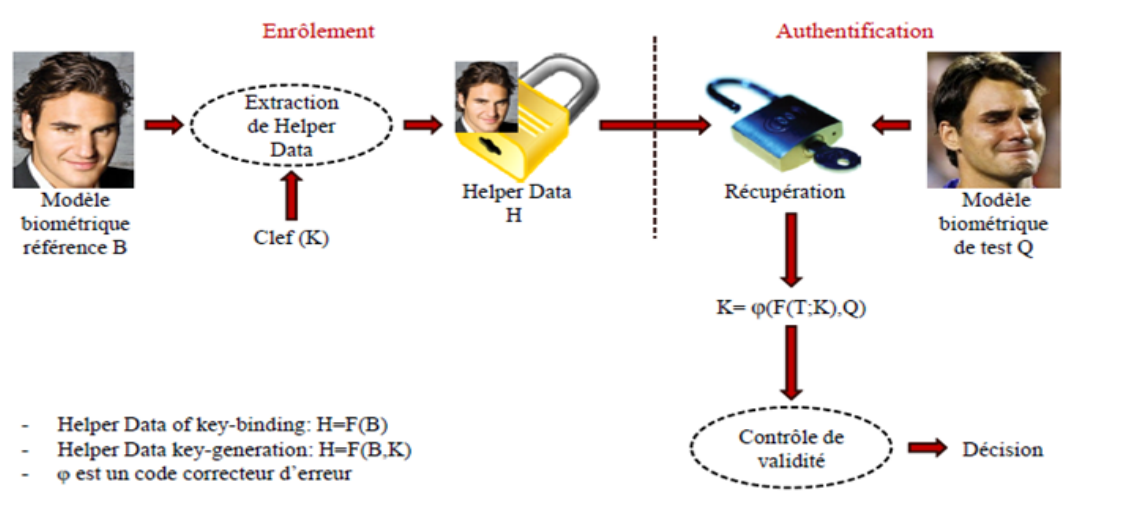


Figure 3.3 – Mécanisme général d'authentification des crypto-systèmes biométriques de type key-binding et key generation [Jain 2008]

Pour les crypto-systèmes biométriques de type key-binding [Ari 1999] [Feng 2006], ils sont tolérants aux variations intra-sujet des modèles biométriques. Cette tolérance peut être interprétée par la capacité du code correcteur d'erreur utilisé. Cependant, ils ne sont pas conçus pour fournir la diversité et la révocabilité. En outre, contrairement aux approches de transformation de caractéristiques, la classification des crypto systèmes biométriques doit être réalisée en utilisant des codes correcteurs d'erreur, ce qui empêche l'utilisation des classifieurs classiques développés spécifiquement pour comparer les modèles biométriques. Les approches les plus populaires

dans cette catégorie sont les systèmes connus sous les nominations : Fuzzy Commitment [Ari 1999] et Fuzzy Vault [Juels 2002][Moujahdi 2014].

En 1999, ***Juels et Wattenberg*** sont les premiers à proposer dans [Ari 1999] une solution appelée Fuzzy commitment, littéralement engagement flou.

Le principe de leur méthode est d'utiliser la donnée biométrique courante pour recalculer une valeur qui servira ensuite pour l'authentification de l'utilisateur. Plus formellement, la méthode dite du fuzzy commitment se décompose en deux étapes : enrôlement puis authentification.

Traditionnellement en biométrie, l'étape d'enrôlement consiste à relever plusieurs fois la donnée biométrique de l'utilisateur (son empreinte par exemple) afin de constituer une valeur de référence. L'étape d'authentification consiste ensuite à comparer la valeur courante à la valeur de référence pour déterminer si l'utilisateur est bien celui attendu. La méthode dite du fuzzy commitment suit ces deux étapes sauf que la valeur de référence stockée n'est pas une donnée biométrique et ne permet pas de retrouver la donnée biométrique utilisée pour la générer. Pour cela, le fuzzy commitment utilise un ensemble de mots de code dans $\{0,1\}^n$et une fonction de hachage H.

Nous pouvons considérer l'approche fuzzy vault comme une amélioration de fuzzy commitment. Le principe du fonctionnement général de fuzzy vault est comme suit [Juels 2002] :

Durant l'enrôlement, une clé utilisateur **K** est utilisée pour construire un polynôme **P** [1]. Ensuite, on calcule la projection polynômiale **P(T)** du modèle biométrique de référence **T**. Enfin, on ajoute un peu de bruit à **P(T)** pour générer le helper data H de fuzzy vault. Au moment de l'authentification/vérification, on applique un code correcteur d'erreur (souvent un code de Reed-Solomon [2]) sur le modèle de test **Q** et le helper data H pour reconstruire le polynôme **P** et récupérer ainsi la clé **K** [Moujahdi 2014].

Pour les crypto-systèmes multi biométriques de type key-generation, ils souffrent généralement d'une discriminative faible, qui peut être évaluée en termes de stabilité

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. http://fr.wikipedia.org/wiki/Code_de_Reed-Solomon

de clé [3] et d'entropie de clé [4] [Jain 2008]. Si un régime génère la même clé quel que soit le modèle d'entrée, alors il y a une grande stabilité de clé mais une entropie nulle, ainsi il aura un taux élevé de fausses acceptations. Si le système génère des clés différentes pour différents modèles d'un même utilisateur, alors le système a une entropie élevée mais une stabilité nulle, et cela conduit à un taux élevé de faux rejets. Alors le grand défi dans la conception de ces schémas de protection est d'atteindre simultanément une stabilité de clé et une grande entropie. Les approches les plus populaires dans cette catégorie sont les systèmes connus sous les nominations : Secure Sketch [Bringer 2008] et Fuzzy Extractor [Yevgeniy 2008].

Le but de régimes Secure Sketch est de gérer les variations intra-sujet des modèles biométriques par la minimisation des informations biométriques dans les sketchs (les modèles protégés sont appelés sketchs dans un crypto-système Secure Sketch). Cependant, ces approches n'arrivent pas à équilibrer efficacement la stabilité/entropie de la clé. Le fuzzy extractor peut être considéré comme une amélioration de Secure Sketch qui adresse la gestion des variations intra-sujet et la stabilité/entropie de la clé simultanément [Moujahdi 2014].
Ces quatre versions des crypto-systèmes multi biométriques(Fuzzy Commitment, Fuzzy Vault, Secure Sketch, Fuzzy Extractor) ont été testées sur plusieurs modalités biométriques.

Le tableau 3.1 résume les travaux qui suggèrent le crypto-system multi-biométrique.

3. Taux de répétibilité d'une clé générée à partir les données biométriques
4. Nombre de clés possibles (différentes) qui peuvent être générées

Auteur	Technique	Modalités	Performance(%)			
			FRR	GAR	FAR	EER
Nandakumar et al, 2008	utilisation d'un schéma de fuzzy vault pour la sécurité des modèles multi-biométriques	Empreinte digitale Iris	-	=98,2%	=0,01%	-
Kelkboom et al, 2009	Fusion multi-algorithmes et protection du modèle multi-biométrique avec l'utilisation de la technique Helper-Data System	Visage	-	-	-	-
Meenakshi et al, 2010	Combinaison de l'utilisateur et une Biométrie souple basé sur Un mot de passe de fuzzy vault biométrique multimodale durci	Iris Rétine	-	-	-	-
Kanade et al, 2010	Combinaison de la multi-biométrique et la cryptographie avec une nouvelle méthode de fusion de niveau d'entité par correction d'erreur pondérée(FeaLingECc)	Iris Visage	=0,91%	-	=0%	-
Argyropoulos et al, 2010	Authentification biométrique multimodaux basés sur des codes de correction d'erreur	Visage Démarche	-	-	-	=3.05%
Geethanjali et al, 2012	Générer un secure sketch en utilisant le cryptosystème multi-biométrique avec un fusion au niveau des caractéristiques	Empreinte digitale Iris	-	-	-	-
Nagar et al, 2012	fuzzy vault avec un fusion au niveau de caractéristiques simultanément	Empreinte digitale Iris Visage	-	-	-	-
Yang et al, 2012	Évaluation des modèles de fusion au niveau de la décision de l'empreinte digitale protégée	Empreintes digitales	=0,0703%	-	=0,0012%	-
Shanthini et Swamynathan, 2012	Système d'authentification sécurisée utilisant la stéganographie la clé cryptographique annulable(cancellable)	Empreinte digitale Visage	=1.21%	=97.2%	-	-
Lu et Peng, 2014	cryptosystème multi-biométrique à doigts basé sur une fusion au niveau des caractéristiques	Empreinte digitale Empreinte du veine Empreintes d'articulation des doigts	-	-	-	-
Beulah et Rani, 2014	Utilisation de helper data sur des cryptosystèmes multi-biométriques	Empreinte digitale Visage	-	-	-	-
Amirthalingam, 2014	La biocryptosystème fuzzy vault en utilisant un multi-polynomial	Visage Oreille.	-	-	-	-
Lalithamani et Sabrigiriraj, 2015	fuzzy vault pour un cryptosystème multi-biométrique	Visage Veine de la main	-	=94%	-	-
Chidemyan, 2015	Fuzzy vault multimodal avec l'utilisation fusion au niveau de caractéristiques	Veine de paume Empreinte digitale	-	-	<0.04%	-
Sankareswari et Jothi, 2015	Approche hybride utilisant la cryptographie visuelle	Empreinte digitale Iris	-	-	-	-
Thanki et Borisagar, 2015	tatouage à base de théorie de la compression résistante (CS)	Empreinte digitale Visage	-	-	-	-
Scholar, 2016	Cryptosystèmes biométriques basée sur le niveau de sécurité	Empreinte digitale	-	-	-	-
Kumar et al, 2016	Encodage BCH et la fonction Hash	Empreinte palmaire Iris	=0.2703%	-	=0.0469%	-
Gomez-Barrero et al, 2017	chiffrement probabiliste homomorphique avec trois niveau de fusion	Empreinte digitale Signature	-	-	-	=0,12%
Maiand et al, 2017	Fusion de caractéristiques binaires pour des cryptosystèmes multi-biométriques discriminants et sécurisés.	Empreinte digitale Visage	-	=20%	-	-
Dinca et al, 2017	fuzzy extractor pour l'extraction des clés biométriques	Empreinte digitale Iris	-	-	-	-
You et al, 2019	fuzzy vault basé sur la fusion d'empreintes digitales et de veines de doigts	Empreinte digitale Empreinte de veine	-	=95%	=0.4%	-
Sujitha et al, 2019	protection des systeme multi-biométrique basé sur Fuzzy Vault	Empreinte digitale Empreinte palmaire	-	=95%	=0,05%	-

Table 3.1 – comparaison entre les approches de crypto-système multi-biométriques

Discussion

Nous venons de voir les crypto-systèmes biométriques comme moyen de sécurisation du modèle multi biométrique. De manière générale, ces systèmes tendent à corriger le bruit de la donnée biométrique en calculant une information publique appelée donnée auxiliaire W (ou helper data) à partir du modèle biométrique X. La donnée W peut aider soit à cacher une clé utilisateur S à l'intérieur de la biométrie, soit à générer une nouvelle clé S . Dans tous les cas, uniquement W sera stockée sur la base de données et la révélation de S ne peut se faire qu'en introduisant la bonne biométrie Y. Néanmoins, il existe de nombreuses difficultés dans l'application de ces schémas. Généralement, ces schémas imposent en entrée un modèle X sous forme vectorielle et discrétisée ce qui n'est pas évident à modéliser pour certaines représentations d'empreintes comme c'est le cas pour les minuties. De plus, ils engendrent une perte d'entropie lorsqu'il y a une certaine corrélation entre les éléments du vecteur X comme c'est le cas pour le fuzzy commitment ou les fonctions de blindage (shielding functions). Pour assurer l'irréversibilité du système, il faudrait que X soit identiquement et indépendamment distribué ce qui n'est pas évident à garantir pour les modèles biométriques. Nous avons aussi vu que du coté préservation de la vie privée, ces schémas, reposant généralement sur les codes correcteurs d'erreur étaient difficilement réutilisables et donc non résiliables [Belguechi 2015].

Dans la suite, nous abordons la seconde classe des méthodes de protection qu'est l'approche par Transformation de caractéristiques (ou les transformations révocables).

3.3.2 Transformation de caractéristiques

L'idée de base des approches de transformation de caractéristiques est de convertir un modèle biométrique non protégé en un modèle protégé en utilisant une fonction de transformation [Ratha 2001] [Ratha 2006]. La fonction de transformation peut prendre plusieurs formes, selon le système et la modalité visée, et elle peut nécessiter aussi l'utilisation de certains paramètres de transformation (par exemple une clef utilisateur). Dans le cas où les modèles biométriques transformés sont volés ou compromis, les paramètres de transformation sont modifiés pour mettre à jour le modèle biométrique protégé. Pour empêcher les imposteurs de suivre les utilisateurs légitimes inscrits dans plusieurs systèmes, et protéger la vie privée par conséquent, il faut appliquer des paramètres de transformation différents ou même des fonctions de transformation différentes pour chaque application [Moujahdi 2014].

Généralement, ces approches fonctionnent comme suit (figure 3.4). Supposons que X sera transformé en données codées T lors de l'enrôlement par l'utilisation d'une fonction F. Pour la vérification, la requête biométrique Y sera transformée en T' toujours en utilisant la fonction F et l'authentification réussira si T est proche de T' en utilisant une certaine mesure de similarité. Pour assurer la révocabilité du système, une donnée aléatoire S sous forme d'une clé est attribuée à chaque utilisateur U. La clé S est alors considérée comme un paramètre d'entrée de la fonction de transformation F. La révocation consiste au remplacement direct de cette clé utilisateur.

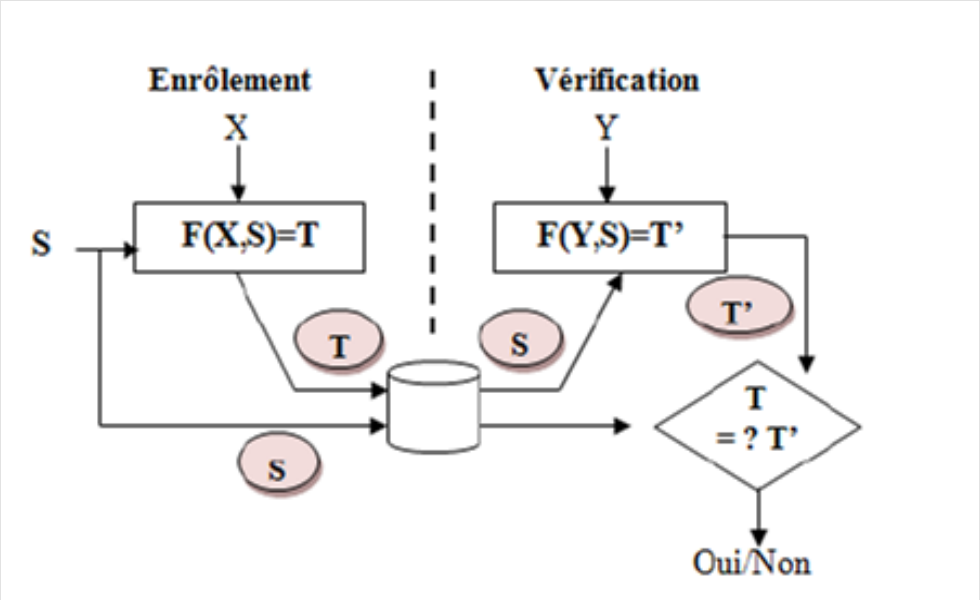


Figure 3.4 – Fonctionnement générique des transformations révocables [Belguechi 2015]

La fonction F s'agira d'un mécanisme de salage où la transformation est une opération qui combine X avec une donnée aléatoire générée à partir de S. Dans tous les cas, S est considéré comme le grain (seed) d'un générateur pseudo-aléatoire[Belguechi 2015]. Les schémas de transformation des caractéristiques peuvent être classés par deux catégories , la transformation inversible (connue sous la dénomination anglaise Salting ou aussi Biohashing) et la transformation non inversible [Jain 2008] [Rathgeb 2011].

Pour la Biohashing, c'est une technique à deux facteurs qui est basée sur l'utilisation de la projection aléatoire (Random projection en anglais)[Navin 2005] [Pillai 2010].

La projection aléatoire est une technique qui utilise des matrices orthogonales aléatoires pour projeter les modèles biométriques dans d'autres domaines ou espaces où les distances entre les modèles avant et après la transformation sont conservées. La projection aléatoire a été proposée comme une solution autonome pour la protection des modèles biométriques qui essaie de répondre à la propriété de la révocabilité, et elle est le principe de base de Biohashing [Moujahdi 2014]. Généralement, pour la Biohashing, son principe général est de générer un BioCode binaire (utilisé pour l'enrôlement et la vérification) à partir de la représentation de la donnée biométrique (comme des paramètres de texture ou les minuties pour les empreintes digitales) et un nombre aléatoire. Ce procédé est employé pour l'enrôlement de l'utilisateur (où seul le BioCode généré est stocké) et pour la vérification (où le BioCode est recalculé à chaque vérification et nécessite le stockage sécurisé de l'aléa). Le résultat de vérification se fait par le calcul d'une simple distance de Hamming entre le BioCode de référence et le BioCode calculé. L'intérêt de cette approche réside dans la possibilité de révoquer le BioCode (en utilisant un autre nombre aléatoire) et même de le diversifier. Il peut être intéressant à partir de la même donnée biométrique (son empreinte digitale par exemple) de générer différents BioCodes pour s'authentifier à différents services. La figure 3.5 illustre le procédé global.

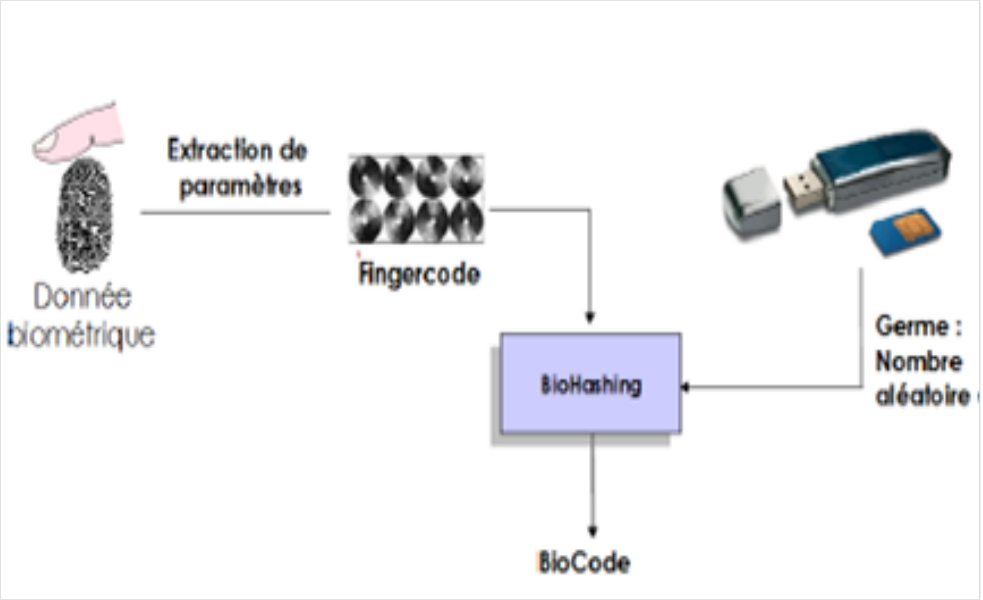


Figure 3.5 – Schéma général de protection d'une donnée biométrique [Belguechi 2011]

Plus précisément, la méthode utilisée consiste à projeter la donnée biométrique (normalisée) sur une base orthonormée générée à partir de l'aléa. La dimension résultante est au plus égale à la dimension de représentation de la donnée biométrique. Cette phase consiste donc à cacher en quelque sorte la donnée biométrique dans une partie de l'espace. L'utilisation d'une base orthonormée permet de garantir la conservation des relations de similarité entre deux données biométriques projetées, comme cela a été démontré par le lemme de Johnson-Lindenstrauss (voir [Dasgupta 1999])

La second étape consiste à quantifier ce résultat à l'aide d'un simple seuillage. Cette étape permet de garantir la non inversibilité du procédé (retrouver la donnée biométrique initiale à partir du BioCode) et de rendre robuste le procédé (en autorisant des différences mineures dans le vecteur projeté inhérent à l'acquisition de la donnée biométrique). Le principe général est résumé dans la figure 3.6 .

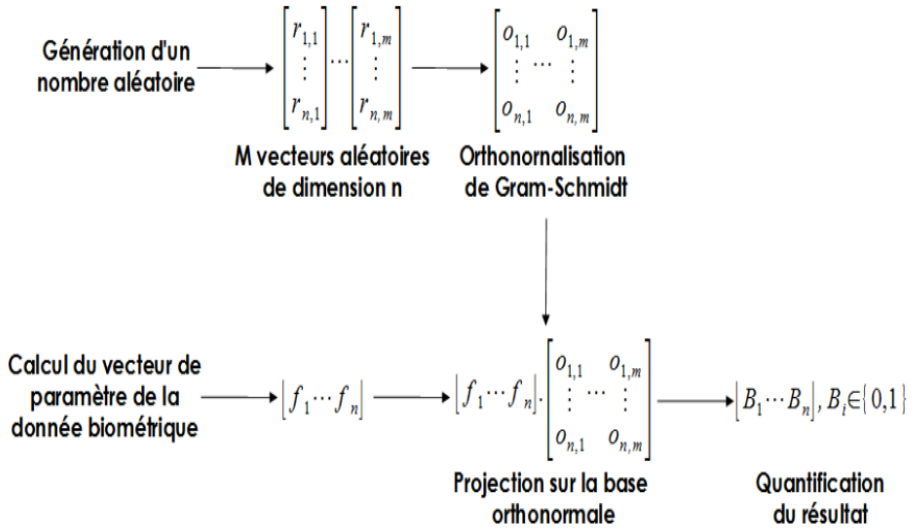


Figure 3.6 – Description du procédé de génération d'un BioCode avec la méthode de Ratha [Belguechi 2011]

Ce procédé permet de garantir qu'il n'est pas possible de retrouver la donnée biométrique initiale à partir du BioCode. La méthode BioHashing détaillée précédemment est une méthode générique permettant de révoquer une donnée biométrique. Elle a été utilisée sur plusieurs modalités biométriques [Belguechi 2011].
Pour la transformation non inversible (la deuxième catégorie des approches de transformation de caractéristiques). Généralement, un modèle original peut être protégé

en utilisant une fonction non inversible [5] qui est dans la plupart des travaux une fonction à sens unique [Christian 2001].En littérature, le principe de la transformation non inversible (bien que le principe de la biométrie révocable) a été proposée pour la première fois par **N. K. Ratha, J. H. Connell et R. M. Bolle**[Ratha 2001], (il a été nommé Cancelable biometrics dans [Ruud 2002]) La propriété la plus importante de cette catégorie est que, même si la clé et/ou le modèle transformé sont connus / volés par un adversaire, il est difficile de récupérer le modèle original (en terme de complexité de calcul). Alors les modèles biométriques sont bien protégés.

L'une des formes de la fonction de transformation les plus significatives dans le contexte des approches de transformation non inversible, est l'utilisation des distorsions ou des transformations géométriques pour protéger les modèles biométriques [Ratha 2006] [Ratha 2007]. Ces transformations varient pour chaque système selon la modalité biométrique utilisée. Le principe de base est d'appliquer une transformation géométrique contrôlée par certains paramètres) sur les images d'enrôlement (les images transformées sont traitées ensuite par les méthodes standards du système de l'extraction de caractéristiques pour construire les modèles de référence). Au moment de l'authentification / identification, la même transformation doit être appliquée sur les images de test, sinon elles ne correspondront pas aux celles de référence. Ces transformations devraient satisfaire la contrainte que, plusieurs modèles, provenant de différentes distorsions, ne devraient pas se correspondre pour assurer les exigences de la révocabilité / diversité [Moujahdi 2014].

Le tableau 3.2 présentent un survol sur les formes les plus significatives dans l'état de l'art de cette catégorie.

5. L'inversibilité 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.

Auteur	Technique	Modalités	Performance(%)			
			FRR	GAR	FAR	EER
Nanniand et Lumini, 2006	Biohashing	Visage Empreinte digitale Iris	-	-	-	≈0%
Jeong et al, 2006	Combinaison de deux méthodes d'extraction des caracteristiques PCA et ICA ,et transformation de vecteur par la biohashing	Visage	-	-	-	-
Maiorana et al,2011	Transformations non inversibles	Signature	-	-	-	
Paul et Gavrilova, 2012	la projection aléatoire et transformation basée sur l'extraction et la sélection de caractéristiques	Visage Oreille	-	-	-	-
Canuto et al,2013	fusion dans le contexte de la reconnaissance de la multi biométrie révocable	Données vocales Iris	-	-	-	-
Rathgeb et Busch,2014	multi biométrie révocable basés sur des filtres de bloom	Iris	-	-	-	<0,5
Sushma et Sandeep, 2015	projection aléatoire et filtre de Bloom	Iris	-	-	-	-
Rathgeb et al,2015	Multi-biométrique révocable basée sur des filtres de Bloom et fusion au niveau des caractéristiques.	Visage Iris	-	-	-	=0.4%
Damasceno et al,2015	Quatre transformations révocables (Interpolation, BioHashing, BioConvolvinget DoubleSum)	Touch Analytics	-	-	-	=28,6%
Stokkenes et al,2016	Protection d'un système multi-biométrique basé sur le filtre de Bloom	Visage deux régions	-	-	-	-
Yildiz et al,2017	Sécurité et confidentialité d'un modèle multi-biométrique en superposant plusieurs données biométriques et fusion de modèles multi-biométriques	Empreinte digitale	-	-	-	=1.9%
Bringer et al,2017	Sécurité de modèles biométriques protégés basés sur des filtres Bloom	Iris	-	-	-	-
Jegede et al, 2018	Matrix Transformation pour la protection de modèle multi biométrique révocable	Visage Iris	=7.889%	-	=2.74%	-
Dwivedi et al,2019	fusion hybride de niveaux de score et de décision pour la vérification biométrique multimodale cancelable	Iris Empreinte digitale	-	-	-	=0.13%

Table 3.2 – comparaison entre les approches de transformation de caractéristiques

3.3.3 Approches hybrides

Quand une méthode de protection des modèles biométriques se base sur plus d'un des quatre approches de base (biohashing, transformation non-inversible, crypto-système keybinding et crypto-système key-generation) présentées dans les sous-sections 2.1 et 2.2 , on l'appelle une approche hybride de protection des modèles biométriques. Ces approches hybrides essaient de combiner les avantages de plusieurs régimes de protection de base sans souffrir de leurs inconvénients respectifs [Moujahdi 2014].

Par exemple dans ***Karthi et Azhilarasan*** [Karthi 2013] Le système proposé utilise le cryptosystème générant des clés et la méthode de transformation des caractéristiques(la biométrie révocable). La limitation de la transformation des caractéristiques a été surmontée par cette approche. Ils concentrent sur ces techniques ,ils utilisent Iris, et l'empreinte digitale (c'est-à-dire la biométrie multimodale) comme traits. Les résultats expérimentaux ne montrent aucune dégradation des résultats en combinant à la fois le système biométrique CryptoSystem (BCS) et la biométrie révocable (CB).

Une autre approche hybride présentée par ***Suzwani et al*** [Ismail 2015] Pour la sécurisation des modèles multi-biométriques basés sur un système révocable et Fuzzy Commitment schema d'iris droit et gauche d'un seul individu seront utilisés comme modèles d'entrée. L'expérience sera réalisée à l'aide de la base de données CASIA-v3 iris pour vérifier la solidité du système proposé. Cette recherche devrait montrer que le modèle hybride de la protection proposé peut satisfaire toutes les exigences de la protection des modèles sans dégrader les performances de la reconnaissance de l'iris.

Discussion

Nous venons de présenter différentes approches de transformation révocable, Ces méthodes, même si elles s'utilisent des fonctions de transformation dans leurs principes, se rejoignent sur les différents points suivants :

- D'abord, leur objectif commun est d'éviter de stocker le modèle biométrique d'origine et dans l'idéal, pouvoir effectuer une reconnaissance fiable dans le domaine de la transformée.
- Elles permettent de révoquer et de générer un nouveau modèle de référence. C'est principalement l'introduction d'une clé utilisateur qui permet cette diversification du modèle à partir du même trait biométrique.

- Par conséquent, la sécurité du régime de Biohashing est basée seulement sur le secret de la clé ou du mot de passe. Alors puisque la transformation est inversible, la clé doit être conservée en toute sécurité par le système et aussi par l'utilisateur pour la présenter lors de l'authentification. Ce besoin d'information supplémentaire sous la forme d'une clé augmente la diversité des modèles biométriques, et les rend plus difficiles à deviner par un adversaire [Belguechi 2015].
- Le régime de Biohashing a plusieurs avantages [Jain 2008]. Il permet la diversité, car puisque la clé est spécifique à chaque utilisateur, nous pouvons générer plusieurs modèles biométriques (du même utilisateur) en utilisant différentes clés. Ce régime permet aussi la révocabilité, parce que dans le cas où un modèle est compromis, il est facile de le révoquer et le remplacer par un nouveau modèle en utilisant une nouvelle clé utilisateur.Il faut noter que la clé utilisateur ne fournit pas seulement la diversité / révocabilité, mais elle améliore également la performance de reconnaissance [Maltoni 2003] [Jain 2007], ce qui n'est pas surprenant étant donné la nature à deux facteurs de ce regime de protection [Moujahdi 2014].
- L'objet de Biohashing est essentiellement d'augmenter la taille du BioCode (plus il est grand, moins une attaque par force brute sera possible) et d'améliorer les performances. La problématique de protection de données biométriques a été souvent abordée de façon étonnante par le biais de la performance (minimisation du taux d'erreur et maximisation de la taille du BioCode) [Belguechi 2011].
- L'une des limites de des transformations non inversible proposées, est qu'elles peuvent convertir des petites différences de position entre deux minuties dans l'espace original en de grandes différences dans l'espace de transformation (augmentation des variations intra-sujet), ce qui peut conduire à un grand nombre de faux rejets. Ces chercheurs ont recommandé ainsi d'utiliser des transformations lisses pour éviter ce problème et conserver la performance [Moujahdi 2014].
- Enfin, le point culminant reste de pouvoir faire une analyse de sécurité rigoureuse de la méthode proposée. Aujourd'hui, il n'existe pas encore de méthode formelle ou bien standardisée pour le faire. Cela constitue une véritable problématique.
- Majoritairement, ces méthodes sont sensibles à des attaques communes auxquelles il faudrait que la recherche pallie. Il s'agit entre autres du vol de la clé utilisateur (Le FAR est dans ce cas assez élevé pour une application sécurisée

de la méthode). De plus, d'après les méthodes présentées, la transformation est souvent inversible (partiellement ou totalement) lorsque tous les paramètres sont connus comme la clé S et le modèle issu de la transformation.

3.4 Conclusion

Après avoir souligné l'importance de protéger le modèle multi biométrique, nous avons pu voir deux grandes familles de solutions. Principalement, des solutions basées sur le crypto système multi biométrique et des solutions orientées sur la transformation révocable.

Dans ce chapitre, nous avons présenté l'état de l'art des approches de protection des systèmes multi biométriques. Nous avons commencé par la description de cette solution qui visent la plupart du temps de cacher les données biométriques . Ensuite, nous avons mis l'accent sur les solutions révocable, qui visent généralement la protection des modèles biométriques on utilisant des fonctions de transformation, en accordant une attention particulière aux approches de transformation inversible (biohashing).

La biométrie révocable est enjeu majeur à l'heure actuelle. Dans le chapitre suivant, nous proposons d'aborder la protection des données multi-biométriques. Nous avons concentré notre attention sur la méthode BioHashing, une technique récente capable de répondre à l'inversion du problème de la confidentialité et de la sécurité.

Chapitre 4

Conception et réalisation du système Biométrique multimodal

Sommaire

4.1 Introduction

Après avoir abordé les différentes méthodes et approches utilisés pour la protection des systèmes biométriques multimodaux dans le chapitre précédent, nous passons à la conception et l'implémentation de notre application pour la sécurité des systèmes multi biométriques.
Nous avons proposé deux systèmes biométriques multimodaux(avec et sans protection), afin d'effectuer une comparaison entre ces deux systèmes. Nous analyserons plus en détail les étapes de conception de nos systèmes pour cela, on applique la méthode de Log Gabor qui permet d'extrait les vecteurs des caractéristiques pour chaque modalité, par la suite nous avons fusionné ces vecteurs. Ensuite pour sécurisé notre système, nous ajoutons une phase de protection dans le quel nous utiliserons la méthode de transformation des caractéristiques « Biohashing ».
Finalement, nous conclurons le chapitre par une analyse et discussion des résultats expérimentaux.

4.2 Architecture des systèmes proposés

Dans notre travail nous avons proposé deux systèmes biométriques multimodaux avec protection et sans protection, pour effectuer une étude comparative entre ces deux systèmes.

4.2.1 Architecture du système biométrique multimodal sans protection

L'architecture de notre système de reconnaissance biométrique multimodal sans protection est illustrée dans la figure 4.1

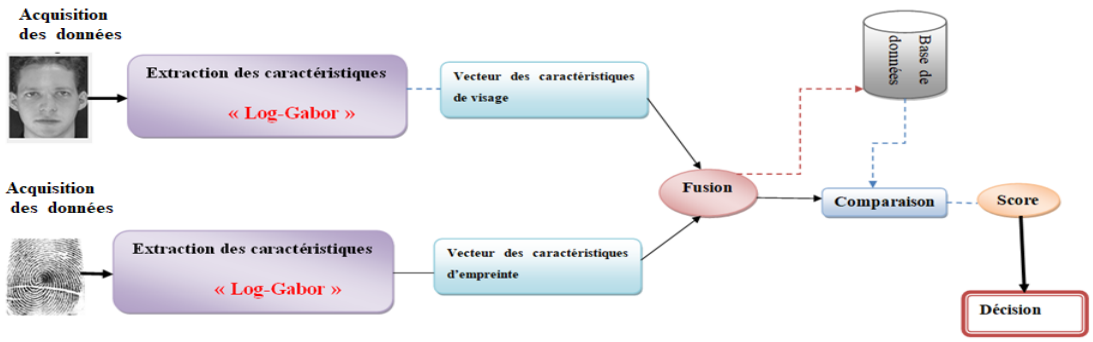


Figure 4.1 – Architecture du système biométrique multimodal sans protection

4.2.1.1 Module d'acquisition des données

Cette étape consiste à capturer l'image de l'utilisateur à l'aide des capteurs biométriques. Nous avons choisi pour notre travail les modalités visage et empreinte digitale.
Pour le visage, l'image de l'utilisateur a été acquise du monde extérieur dans un état statique par un appareil photo ou dynamique par une caméra, et pour l'empreinte digitale, l'image doit être acquise par des procédés directs (un capteur) ou indirect (l'encre).
Dans ce module nous avons utilisé des bases de données (empreinte et visage)

4.2.1.2 Module d'extraction des caractéristiques

Puisque l'extraction des caractéristiques d'une image est une étape très importante dans les phases de reconnaissance, pour cela nous avons choisi dans notre travail une méthode basée sur le filtre de log Gabor qui nous a donné des bonnes résultats dans un temps raisonnable.

1. **Filtre log Gabor**

   Le filtre log Gabor est une modification de la fonction de base de Gabor, il a été proposé par **Dennis Gabor** en 1946 [Gabor 1946]. La fonction log-Gabor présente l'avantage de la symétrie sur l'axe des fréquences logarithme, ce qui donne une représentation plus efficace des images et réduit la redondance dans les basses fréquences. Au contraire, les filtres de Gabor ordinaires surreprésentent les basses fréquences.

2. **La fonction de log Gabor**

   La fonction de filtre log Gabor est définit comme suit [Ammour 2018] :

$$G(f,\theta) = \exp\left(\frac{-(\log(f/f_0))^2}{2(\log(\sigma_f/f_0))^2}\right)\exp\left(\frac{-(\theta-\theta_0)^2}{2\sigma_\theta^2}\right) \tag{4.1}$$

   Où
   f_0 : représente la fréquence centrale du filtre.
   σ_f : donne la bande passante du filtre.
   θ_0 : l'angle d'orientation du filtre.
   σ_θ : facteur d'échelle

3. **Filtres log-Gabor auto-inversibles**

Les filtres Log-Gabor consistent essentiellement en une transformation logarithmique du domaine de Gabor, qui élimine le composant ennuyeux alloué dans les filtres passe-haut et moyen. Ce type de filtre est proposé pour résoudre certains des inconvénients traditionnels qui ont compliqué la fonctionnalité des filtres de Gabor [Fischer 2009]. La figure 4.2 montre un Profils de la réponse en fréquence des filtres de Gabor (à gauche) et des filtres de log-Gabor (à droite).

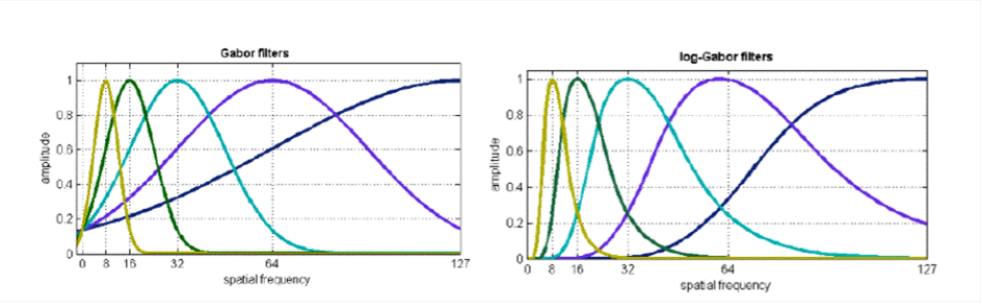


FIGURE 4.2 – Profils de la réponse en fréquence des filtres de Gabor (à gauche) et des filtres de log-Gabor (à droite) [Fischer 2009]

4. **Filtrage d'image**

L'image traitée est filtrée dans une banque de filtres de log Gabor. Les paramètres de filtres sont choisis pour obtenir une couverture uniforme du spectre. La figure 4.3 illustre les filtres de log Gabor pour la même scale et différentes orientations [Zewail 2003].

FIGURE 4.3 – filtre log-gabor pour même scale et différentes orientations [Zewail 2003]

- Dans notre système, nous avons appliqué le filtre log Gabor sur les modalités (visage et empreinte digitale) avec des paramètres qui nous a donné un meilleur résultat, ses paramètres son scale=4, orientation=6, et pour le ratio σ_f / f_0 nous avons choisi 0.75 pour le visage et 0.65 pour l'empreinte et le facteur d'échelle σ_θ nous avons prendre 1.5 pour le visage et 1.3 pour l'empreinte.

4.2.1.3 Le vecteur de caractéristiques

La méthode de Log Gabor permet d'extraire un vecteur de caractéristiques a partir de calcul du moyen de chaque orientation et le stocké dans un vecteur.

Le vecteur de caractéristique qui nous avons extrait est de taille 552 pour les deux modalités (visage et empreinte digitale).

4.2.1.4 La fusion

Le système biométrique multimodal proposé dans notre travail utilise deux types de modalités hétérogènes (visage et empreinte digitale) donc, nous avons utilisé la fusion au niveau des caractéristiques qui permet de concaténé les deux vecteurs des caractéristiques (le vecteur du visage avec le vecteur d'empreinte digital). Alors le vecteur concaténé est de taille 1104.

4.2.1.5 Module de comparaison (matching)

Dans cette phase on cherche a trouvé des correspondances entre le vecteur de la personne en entrée (construit dans l'étape précédente) avec ceux de la base de données. Pour effectue cette comparaison on utilise la méthode du K plus proches voisins K-NN(en anglais : K- Nearest Neighbor) qui permet de calculer la divergence (différence) entre ces deux vecteurs on utilise la métrique de la distance. Dans notre projet nous avons utilisé la distance euclidienne qu'est calculé comme suit :

$$G_{x,y} = \sqrt{\sum_{i=1}^{K} (x_i - y_i)^2} \tag{4.2}$$

1. **Méthode des k plus proches voisins**

   L'algorithme des k-plus proches voisins (En anglais K-Nearest Neighbor ,k-NN ou KNN), est une méthode de classification supervisé la plus simples. Se base sur une comparaison directe entre le vecteur caractéristique représentant l'entité à classer et les vecteurs caractéristiques représentant des entités de référence.

   Dans un contexte de classification d'une nouvelle observation x, l'idée fondatrice simple est de faire voter les plus proches voisins de cette observation. La classe de x est déterminée en fonction de la classe majoritaire parmi les k

plus proches voisins de l'observation x. La méthode KNN est donc une méthode à base de voisinage [Barigou 2013]. L'algorithme 1 résume le principe de cette méthode.

Algorithme 1 : Plus proche voisin K-NN [Lahbib 2012]

```
Soit D= (x',c), c ∈ C L'ensemble d'apprentissage;
Soit x l'ensemble dont on souhaite déterminer la classe ;
début
    pour chaque ((x',c)∈ D) faire
        Calculer la distance dist(x,x');
    fin
    pour chaque x' ∈ kppv(x) faire
        Compter le nombre d'occurrence de chaque classe;
    fin
    Attribuer à x la classe la plus fréquente;
fin
```

2. **Les avantages de l'algorithme K-NN**

   Parmi les avantages de cet algorithme :

   - Ne pas refaire l'apprentissage lors de l'introduction de nouveaux attributs.
   - Traiter tout type de données avec un nombre d'attributs élevé.
   - Fournir des résultats clairs.

4.2.1.6 Module de décision

Dans cette étape, on doit aboutir à une décision sur l'identité de la personne à reconnaître. Pour le faire nous avons calculé une mesure de décision, en utilise le score de distance (d) produit par l'étape de comparaison, la métrique correspondante est donnée par la formule :

$$\frac{1}{1+d} * 10 \tag{4.3}$$

Cette mesure est comparée à un seuil de décision fixé en avance pour répondre à la question : « **acceptée ou rejetée ?** ».

4.2.2 Architecture du système biométrique multimodal avec protection

L'architecture de notre système de reconnaissance biométrique multimodal avec protection est illustrée dans la figure 4.4

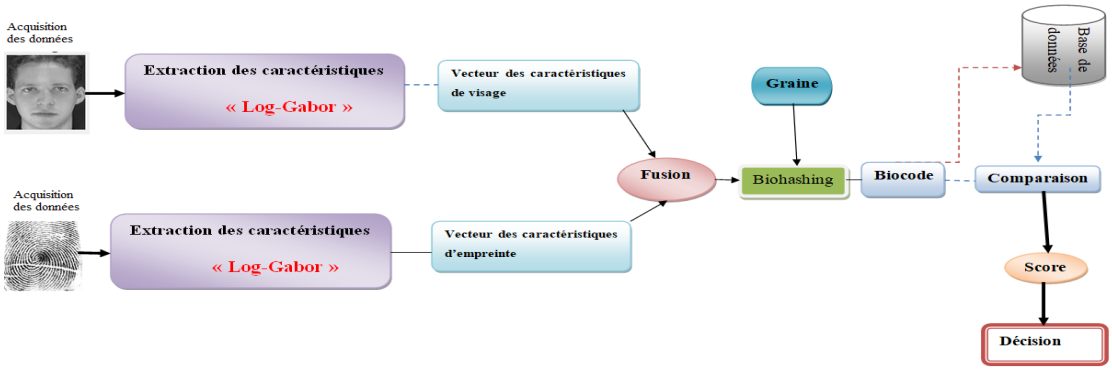


FIGURE 4.4 – Architecture du système biométrique multimodal avec protection

Les modules d'acquisition des données, extraction des caractéristiques, comparaison et décision sont les mêmes qui nous avons utilisé dans le système précédent.

Dans ce système biométriques multimodal(avec protection) nous ajoutons la phase de protection à l'aide de l'utilisation de l'approche de transformation des caractéristiques inversible « Biohashing », et dans cette méthode plus que le vecteur des caractéristiques est long, plus que le système est plus sécurisé, c'est pour cela nous avons choisi la fusion au niveau des caractéristiques pour obtient un vecteur long.

4.2.2.1 La phase de protection(Biohashing)

Dans cette étape, nous avons sécurisé le vecteur de caractéristiques extrait par la phase d'extraction des caractéristiques. Pour cela, nous avons appliqué une méthode révocable très populaire, basée sur la transformation des caractéristiques inversible « **Biohashing** ».

1. **La biohashing**

   La BioHachage a été proposé en 2003 pour la reconnaissance faciale [Goh 2003] puis en 2004 pour les empreintes digitales [Teoh 2004]. Lors de la phase d'enrôlement, l'utilisateur présente son empreinte et son visage et la clé secrète stockée sur une clé USB, une carte à puce ou plus généralement un token. Des paramètres sont extraits de l'empreinte et visage (par exemple à l'aide d'un filtres Log-Gabor) sous forme de deux vecteurs, après nous avons fusionner ces vecteurs pour donner un seul vecteur de caractéristiques.
   La fonction de transformation prend comme entrée ce vecteur et la clé secrète pour générer un BioCode binaire. Ce BioCode est ensuite stocké dans la base de données.

Lors de la phase de vérification, un nouveau BioCode est calculé et comparé au BioCode de référence. La transformation comporte deux étapes : la projection de la donnée biométrique originale par une matrice pseudoaléatoire orthonormale (générée à partir de l'aléa stocké sur le token), suivie d'une quantification en fonction d'un seuil prédéfini[Cherrier 2012], (comme présenté dans le chapitre 03).

2. Algorithme du Biohashing

L'algorithme Biohashing est appliqué aux données biométriques représentées par un vecteur à valeur réelle de longueur fixe et génère un modèle binaire appelé BioCode de longueur inférieure ou égale à la taille d'origine.
L'algorithme de Biohashing transforme le modèle biométrique C = (C1, . . ., Cn) dans un modèle binaire appelé BioCode B = (B1, . . ., Bm), avec $m <= n$, comme suit :

Algorithme 2 : Processus de protection par la BioHashing [Belguechi 2015]

Input : C : le vecteur moyenne de l'utilisateur U de taille n;
S : La clé sous forme d'une nombre aléatoire attribué à l'utilisateur U;
Output : B : Biocodede taille m avec m<n;
1 Générer à partir de S une matrice aléatoire uniforme $R_n * m$ (n lignes m colonnes);
2 Contrôler que les vecteurs de R sont linéairement indépendant sinon aller à 1;
3 Appliquer le processus de Gam-Schimidt pour transformer R en une matrice orthonormée;
4 Projeter le vecteur C sur la nouvelle matrice R :

$$[C_1, C_2, ..., C_n] \begin{pmatrix} r_{11} & ... & r_{1m} \\ \vdots & \ddots & \vdots \\ r_{r1n} & ... & rrnm \end{pmatrix} = [w_1, w_2, ..., w_m]$$

5 Binarisation de W à partir de seuil $\tau b = 0$ pour obtenir le biocode $B = \{b_1, b_2, ..., b_n\}$ tel que :

$$b_i = \begin{cases} 0 & Si \quad w_i \leq \tau_b \\ 1 & Si \quad w_i > \tau_b \end{cases}$$

6 effacer le vecteur C et sauvegarder le vecteur B comme référence de l'utilisateur U;

Dans notre travail nous avons en entrée un vecteur de taille 1104 et après l'application de la fonction Biohashing, nous obtient un biocode de même taille que le premier vecteur (1104).

4.3 Implémentation et résultat expérimental

4.3.1 Les bases de données

1. **Base de données du Visage (ORL [1])**

Conçu par AT & T laboratoires de l'université de Cambridge en Angleterre, la base ORL (Olivetti Research Laboratory) est une base de donnée de référence pour les systèmes de reconnaissances automatiques des visages, il a été recueillie entre 1992 et avril 1994.

Cette base contient 400 images, représentant les visages de 40 personnes, chacune dispose 10 vues différentes, avec des changements de pose, d'éclairage, d'expressions faciales (expression neutre, sourire et yeux fermés) et des occultations partielles par les lunettes mais toujours sur un fond foncé. Ces images ont été collectées à des dates différentes, elles sont de taille 112 * 92 pixels. Dans notre travail, nous avons sélectionné 8 images pour chaque personne, totalisant 320 images. la figure 4.5 représente un extrait de cette base.

Figure 4.5 – Extrait de la base ORL

1. https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html

2. **Base de données d'empreinte digitale (URU4000)**

La sous base de données d'empreinte digitale utilisé dans cette application est de SDUMLA-HMT [Yilong 2011]. Elle comprend de vraies données (images de taille 294*356 pixels) multimodaux de 106 personnes, acquis par 5 capteurs différents à chaque personne. Pour une seule personne il a enregistré 6 doigts (3 doigts pour chaque main), chaque doigt acquis 8 fois. la figure 4.6 représente un extrait de cette base est donné.

Figure 4.6 – Extrait de la base URU4000 [Yilong 2011]

Dans notre travail nous avons choisi les empreintes acquissent à l'aide du capteur URU4000 développé par Zhongkong Inc, nous avons sélectionné 40 personnes (1er doigt de la main droit) , chaque personne a 8 images, totalisant 320 images.

3. **Base de données multimodale**

À partir des bases de données ORL et URU4000, nous avons formé une base de données multimodale virtuelle. Nous avons élaboré un corpus de 640 images (2 modalités * 40 personnes * 8 images pour chaque personne).

Séparation de la basse donnée

Notre base de données est divisée en deux parties : une base pour effectuer l'apprentissage et l'autre pour tester les techniques et déterminer leurs performances, il n'y a pas une règle pour déterminer ce partage. Notre base a été scindée de la façon suivante :

- **Images d'apprentissages :** La première, la troisième, la cinquième, et la Septième image pour chaque modalité de chaque personne servent pour la phase d'apprentissage.
- **Images de tests :** Les 4 images restantes (2,4, 6, 8) de chaque individu nous ont servi pour la réalisation des différents tests.

4.3.2 Environnement du travail

Dans cette section, nous présenterons les environnements matériel et logiciel de notre travail.

Environnement matériel

Pour réalisé cette application nous avons utilisé un équipement, configurées comme suit :

Modèle	Processeur	RAM	Disque Dur	SE
ASUS K756U	Intel® core(TM) i5-6200U CPU @230GHZ 240GHZ	8.0 GO	1000 GO	Windows 10 64 bit

Environnement logiciel

Le nom MATLAB [2] vient de l'anglais MATrix LABoratory, une traduction littérale nous amène à voir MATLAB comme un laboratoire pour manipuler des matrices. En effet, MATLAB permet de manipuler des matrices, de tracés de courbes, de résolution de systèmes et d'algorithmes de calculs numériques, de créer des interfaces utilisateurs, et peut d'interagir avec d'autres langages comme le C, C++, Java, et Fortran.
MATLAB est un environnement très performant, permet l'exécution de tâches nécessitant une grande puissance, comprend de nombreuses fonctions plus spécifiques regroupées dans des TOOLBOX (que l'on peut traduire par "boîte à outils").
Version utilisé : Lors du développement de notre application, nous avons utilisé MATLAB R2015a comme un outil logiciel.

4.3.3 Présentation de l'application

Interface principale de l'application

La figure 4.7 présente la fenêtre principale de notre application, elle est composée de deux systèmes :

- Système multi-biométrique sans protection.
- Système multi-biométrique avec protection.

2. http://nte.mines-albi.fr/MATLAB/co/Generalites.htmlfr.slideshare.net

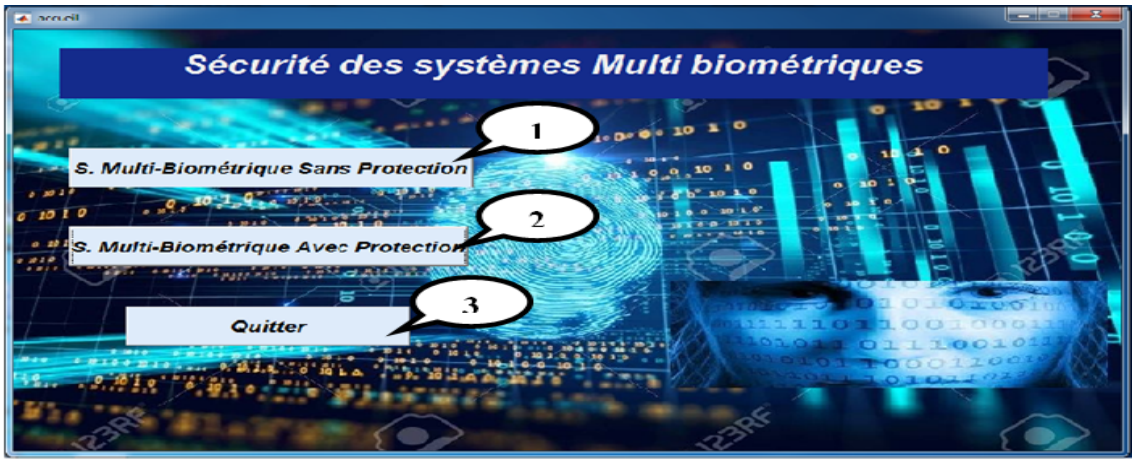


Figure 4.7 – interface principale de l'application

1. Affiche l'accueil du Système multi-Biométrique sans protection
2. Affiche l'accueil du Système multi-Biométrique avec protection
3. fermer la fenêtre.

Système multi-Biométrique avec protection

On doit présenter notre système multi-biométrique avec protection proposé.

Interface d'accueil

La figure 4.8 présente la fenêtre d'accueil de notre système.

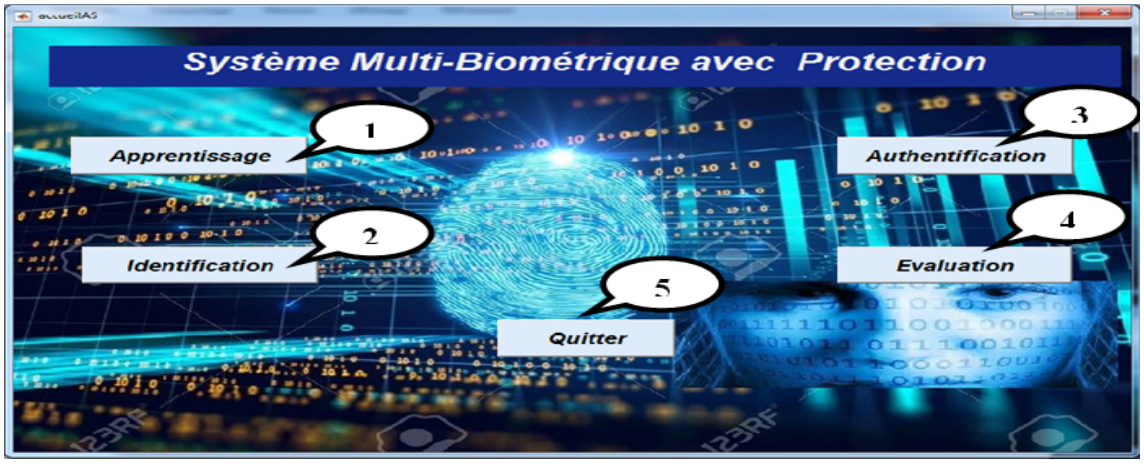


Figure 4.8 – Accueil du système multi-biométrique avec protection

1. Afficher la fenêtre d'apprentissage.

2. Afficher la fenêtre d'identification.
3. Afficher la fenêtre d'authentification.
4. Afficher la fenêtre d'évaluation.
5. Fermer la fenêtre et retourne à la fenêtre principale.

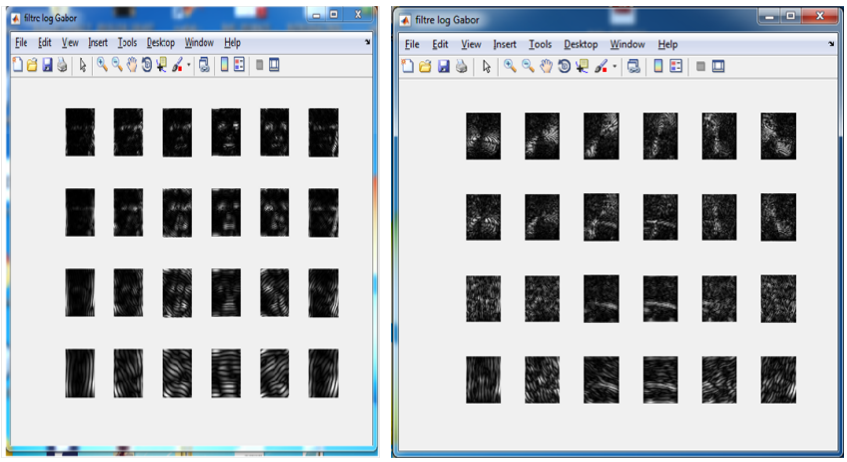
Interface d'apprentissage

La figure 4.9 présente la phase d'apprentissage (enrôlement) dans la quelle nous avons ajouté des individus dans la base de données.

Figure 4.9 – interface d'apprentissage

1. Charger le visage de la nouvelle personne qui nous voulons ajouter dans la base.
2. Charger l'empreinte digitale de la nouvelle personne qui nous voulons ajouter dans la base.
3. Entrée l'identifiant de la personne.
4. Lancement du processus d'apprentissage dans le quel nous avons extraies les caractéristiques de la personne et l'enregistrer dans la base de données.
5. Vidé tous les champs
6. Fermer la fenêtre et retourne à la fenêtre Accueil

Avant l'enregistrement du BioCode dans la base de données un filtre de Log-Gabor a été appliqué sur ces deux modalités (voir figure 4.10), puis le système génère une clé et appliqué la BioHashing.



(a) filtres log Gabor du visage (b) filtres log Gabor d'empreinte

Figure 4.10 – Filtre Log-Gabor

Après l'enregistrement une boite d'information est affiché figure 4.11

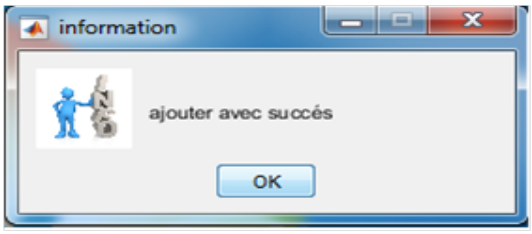


Figure 4.11 – enregistrement avec sucés

Interface d'identification

La figure 4.12 présente la phase de reconnaissance « Identification » dans le quel nous avons identifié les personnes.

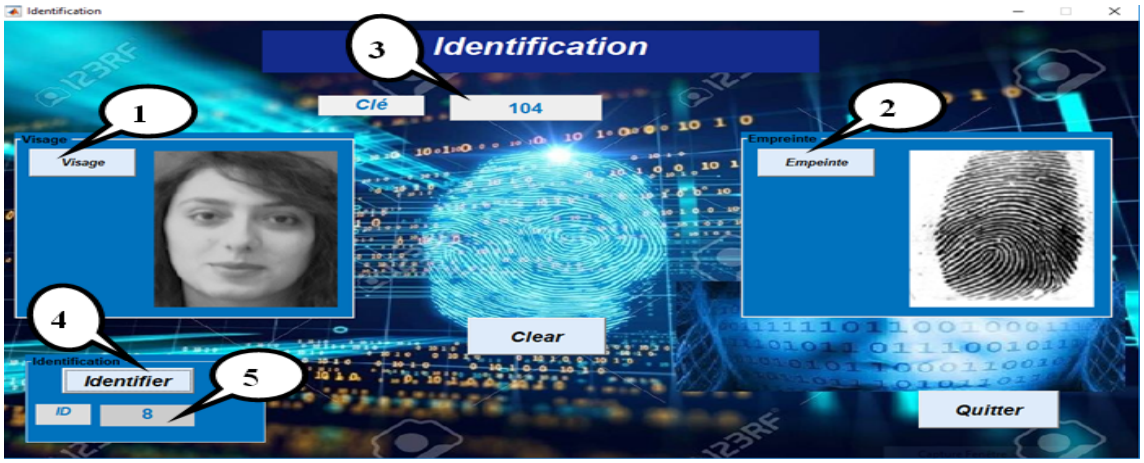


Figure 4.12 – Interface d'identification

1. Charger le visage de la personne qui nous voulons identifier
2. Chargé l'empreinte digitale de la personne
3. Entrée la clé
4. Lancement du processus d'identification dans le quel nous avons testé si cette personne est appartient à ce système ou non.
5. Affichage du résultat.

On a 2 cas :

1 Dans le cas d'un client, le champ « 5 » = identifiant de cette personne et une boite d'information s'affiche figure 4.13.

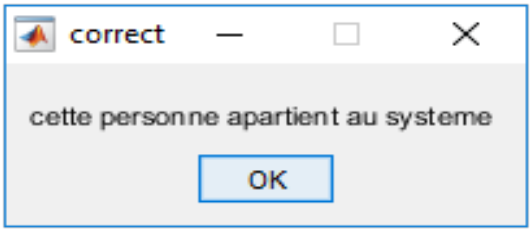


Figure 4.13 – personne accepté (client)

2 Dans le cas d'un imposteur, le champ « 5 » = 0 et une boite d'information s'affiche figure 4.14

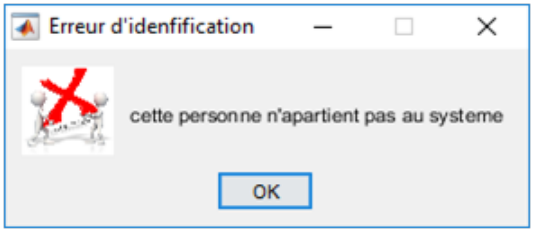


Figure 4.14 – personne refusé (imposteur)

Interface d'authentification (vérification)

La figure 4.15 présente la phase de reconnaissance « vérification » dans le quel nous avons authentifié les personnes.

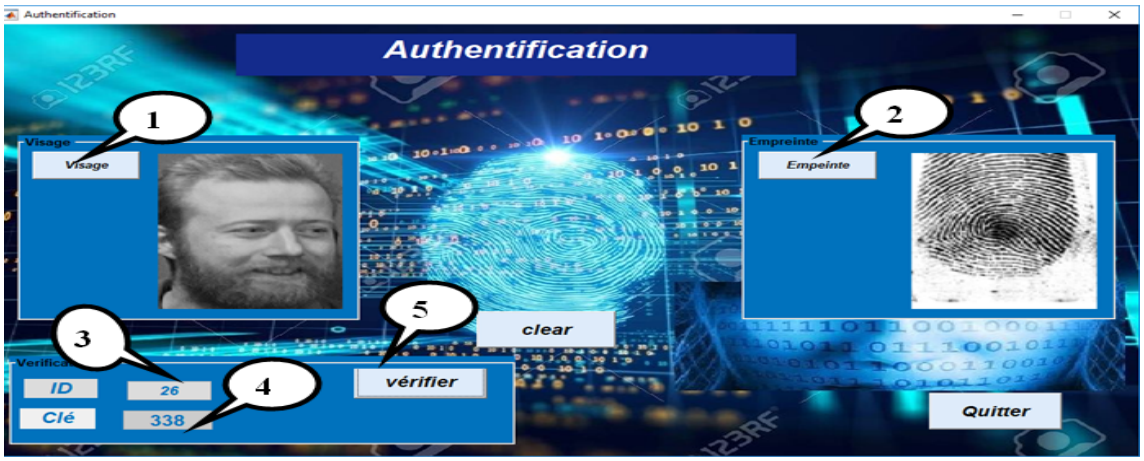


Figure 4.15 – Interface d'authentification

1. Charger le visage de la personne qui nous voulons vérifier
2. Chargé l'empreinte digitale de la personne.
3. Entrée l'identifiant (ID) pour la vérification.
4. Entrée la clé.
5. Lancement du processus de vérification dans le quel nous avons testé si cette personne est un client ou imposteur.

On a 2 cas :

1 Dans le cas d'un client, une boite d'information doit être affiché figure 4.16.

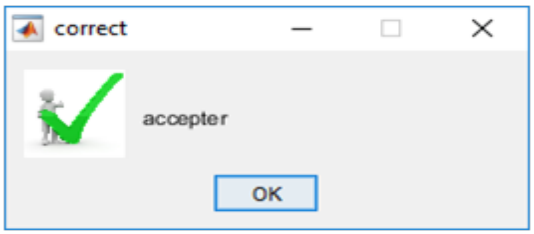


Figure 4.16 – personne accepté (client)

2 Dans le cas d'un imposteur, une boite d'information doit être affiché figure 4.17.

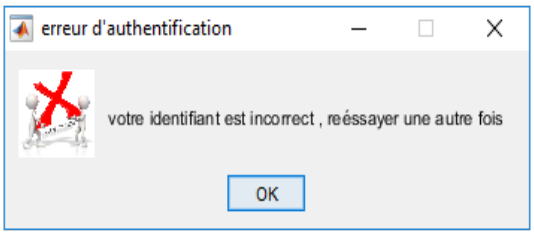


Figure 4.17 – personne refusé (imposteur)

Système multi-Biométrique sans protection

Ce système contient les mêmes phases qui nous avons présentées dans le système précédent sans appliquer l'étape de protection, la figure 4.18 présente la fenêtre d'accueil de ce système.

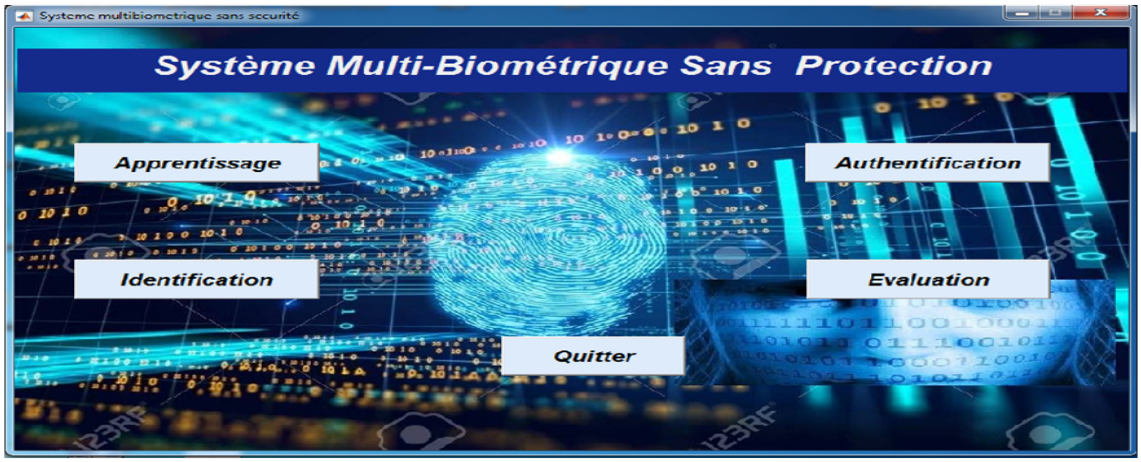


Figure 4.18 – Interface d'accueil du système multi-biométrique sans protection

- **Apprentissage :** la déférence dans cette phase on applique seulement le filtre Log-Gabor sur les deux modalités puis on enregistre le vecteur dans la base.

- **Identification :** dans cette phase on charge le visage et l'empreinte digitale puis lancé le processus d'identification. N'ont pas besoin d'entrée la clé de chaque individu comme le premier système pour confirmer leur identité.
- **Authentification :** pour la vérification aussi on charge le visage, l'empreinte digitale et entré l'identifiant puis lancé le processus de vérification.

4.4 Évaluation de performance

Dans cette partie, nous intéressons tout d'abord à présenter et discuter les différents résultats de taux de reconnaissance obtenus par le système biométrique multimodal sans protection et le système biométrique multimodal avec protection dans le quel, on va tester l'utilité de l'algorithme de protection.

Dans l'identification, les performances des systèmes proposés est représenté sous forme de courbe **CMC**. Et dans la vérification les performances des systèmes proposés est représenté sous forme de courbe **ROC** et **FAR vs FRR** et le taux d'erreur égal **(EER)**.

1. Courbe CMC

Pour présenter la performance de la phase d'identification de deux systèmes, on utilise la courbe CMC (Cumulative Match Caractéristique) qui affiche le taux d'identification en fonction de rang, les figures 4.19 et 4.20 illustres les courbes de CMC pour les deux systèmes.

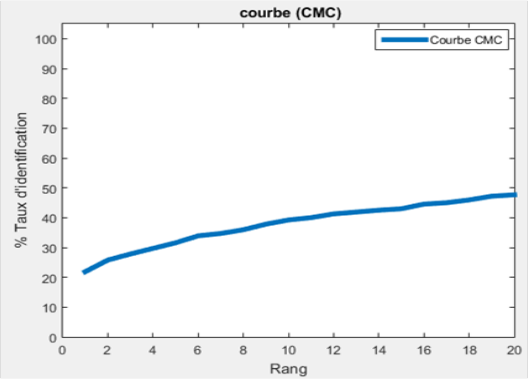


Figure 4.19 – courbe CMC du système biométrique multimodal sans protection

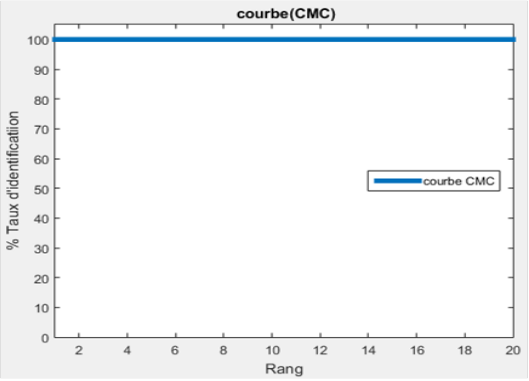


Figure 4.20 – courbe CMC du système biométrique multimodal avec protection

On remarque que la première courbe qui corresponde au système sans protection, le taux d'identification ne dépasse pas 50%, après plusieurs test nous avons choisis la valeur 0.4 pour le seuil de décision. Contrairement au système avec protection qui nous a donné un résultat parfait 100% à cause de la phase de protection qui nous avons appliqué ainsi que le bon choix du seuil=0.51.

2. Distributeur de scores

La figure 4.21 et figure 4.22 illustres les courbes de distribution des scores authentiques et imposteurs dans les systèmes biométriques multimodaux sans protection et avec protection.
D'après ces courbes nous avons déterminé les meilleurs seuils pour les deux systèmes.

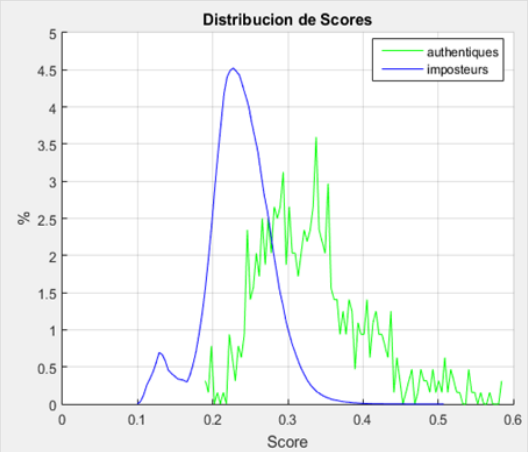


Figure 4.21 – Distribution des scores authentique et imposteurs du système biométrique multimodal sans protection

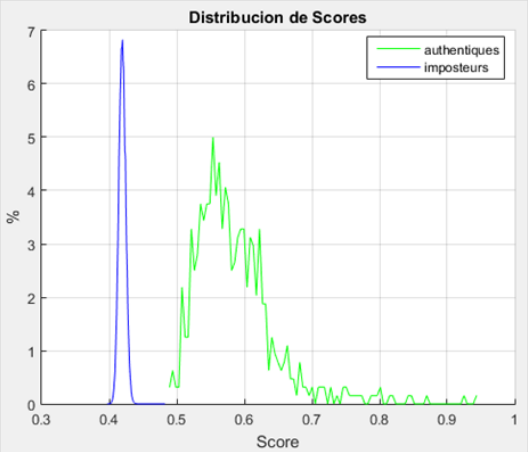


Figure 4.22 – Distribution des scores authentique et imposteurs du système biométrique multimodal avec protection

3. Courbe FAR vs FRR

Les figures 4.23 et 4.24 illustres la distribution des scores du FAR et du FRR pour tous les seuils de décision possibles. Nous reportons les deux systèmes, le système biométrique multimodal avec protection et le système biométrique multimodal sans protection pour analyser l'impact du choix du seuil de décision. Le point d'intersection entre les deux courbes FAR et FRR représente l'EER.

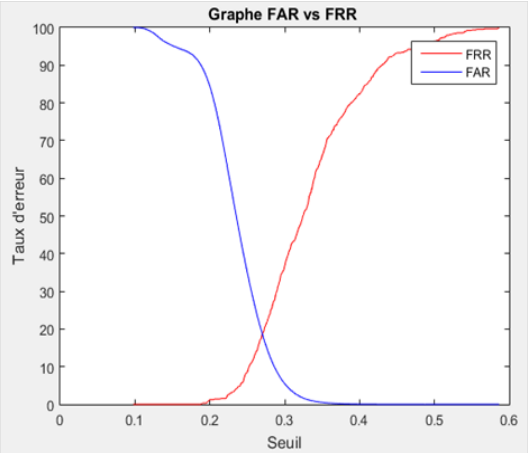


Figure 4.23 – Variation des FRR et FAR en fonction du seuil de décision du système biométrique multimodal sans protection

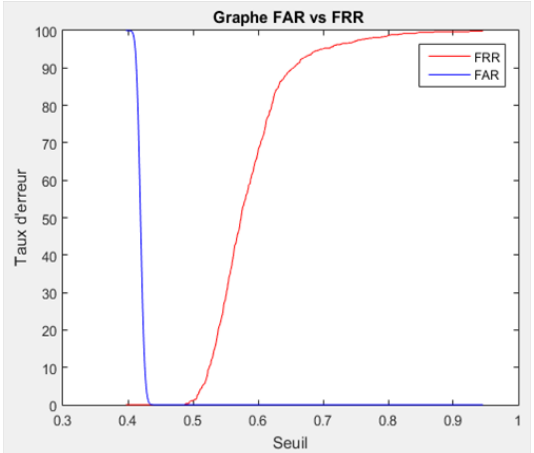


Figure 4.24 – Variation des FRR et FAR en fonction du seuil de décision du système biométrique multimodal avec protection

4. Courbe ROC

Les figures 4.25 et 4.26 illustres les courbes ROC pour les deux systèmes On remarquant que le taux de véritable accepter (GAR) est égale à 100% dans le système biométrique multimodal avec protection par contre dans le système biométrique multimodal sans protection le GAR $< 70\%$.

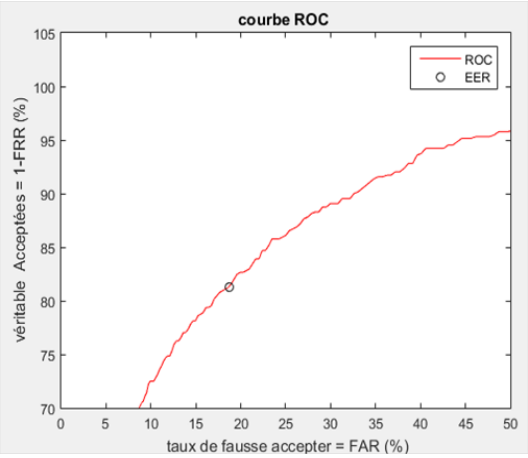


Figure 4.25 – courbe ROC du système biométrique multimodal sans protection

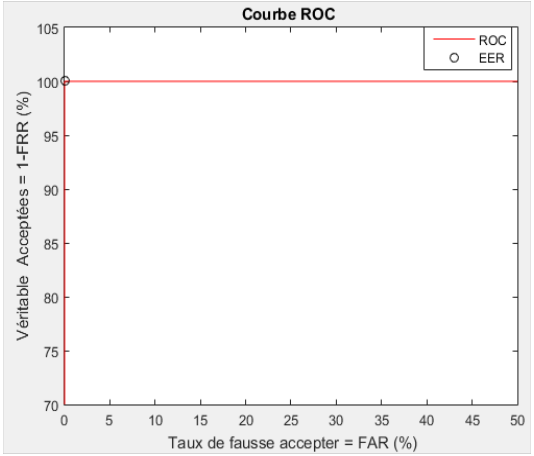


Figure 4.26 – courbe ROC du système biométrique multimodal avec protection

Le tableau 4.4 illustre une comparaison entre le système biométrique multimodal sans protection et le système biométrique multimodal avec protection en terme de valeur EER.

Système	**seuil**	**EER %**
S. sans protection	0.28	18.679%
S. avec protection	0.487	0%

Table 4.1 – comparaison de performance entre les deux systèmes

À travers cette comparaison, notre système biométrique multimodal avec protection par l'utilisation de l'approche de la biohashing a donné de meilleurs résultats atteint EER=0% par rapport à 18.679% par l'autre système (sans protection).

4.5 Conclusion

Ce chapitre est consacré à la conception des systèmes biométriques multimodaux avec et sans protection, nous avons implémenté la méthode de la biohashing pour sécurisé notre système. Ensuite, on a exposé les résultats de performance obtenu lors de la phase du test d'évaluation de nos systèmes notamment le taux d'erreurs EER.
Les résultats obtenus justifient l'efficacité de notre système biométrique multimodal avec protection basé sur la méthode de la biohashing.

Conclusion Générale

La biométrie consiste à l'utilisation des caractéristiques physiologiques ou comportementales, afin de déterminer l'identité des individus. La multi-biométrie devenue un domaine de recherche très actif durant ces dernières années, il consiste à concaténer plusieurs modalités pour améliorer les performances de l'authentification et dont un système efficace, fiable et rapide.

Les systèmes multi biométriques souffrent de vulnérabilités. Néanmoins, les données biométriques brutes sont directement stockées dans la base, peuvent être compromises, ceci entraine l'impossibilité d'utiliser ces données vue qu'elles ne sont pas révocables. Il devient indispensable d'assurer la sécurité et l'intégrité des systèmes multi biométriques et la confidentialité des utilisateurs, avec des schémas de protection des modèles multi biométriques sécurisés et révocables.

L'étude présentée dans le cadre de ce modeste mémoire apporte une solution de sécurisation des systèmes multi-biométrique en utilisant la méthode de transformation des caractéristiques inversible « Biohashing ». Cette méthode protège le modèle multi-biométrique révocable et nous a donnés des résultats fiables. Nous avons implémenté un système basé sur la combinaison de deux modalités visage et empreinte digitale au niveau des caractéristiques avec une extraction basé sur le filtre Log-Gabor.

Afin de concevoir notre système biométrique multimodal avec protection. En premier lieu, nous avons donné un aperçu sur des concepts généraux de la biométrie, puis nous avons présenté la biométrie multimodale, les différents niveaux et techniques de fusions possibles, par la suite un état de l'art sur la protection des systèmes multi biométriques. Enfin, nous avons implémenté et testé notre système multi biométrique avec protection par un autre système qu'est sans protection afin dévaluer

leur performance, En effet on a arrivé à un taux d'erreur de 0% par rapport à 18.679 % par l'autre système (sans protection).

Nous clôturons notre mémoire par perspectives, il est souhaitable d'implémenter l'approche du Biohashing avec une méthode hybride de fusion des données par exemple au niveau des caractéristiques et au niveau de score. Ainsi penser à adapter notre système biométrique multimodal avec protection pour d'autres types de données biométriques.

Bibliographie

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

[Amirthalingam 2014] Amirthalingam, G. Improving the Multibiometric Recognition Based on Fuzzy Vault Scheme Using Multiple Polynomials.European Journal of Scientific Research ISSN 1450-216X / 1450-202X Vol.117 No.4 January, 2014, pp.585-594 http ://www.europeanjournalofscientificresearch.com.

[Ammour 2018] Ammour, B., Bouden, T. & Boubchir, L. Face–iris multi-modal biometric system using multi-resolution Log-Gabor filter with spectral regression kernel discriminant analysis, 2018.

[Argyropoulos 2010] Argyropoulos, S., Tzovaras, D. , Ioannidis, D.,Damousis, Y., Michael G. Strintzis, Martin Braun and Serge Boverie « Biometric template protection in multimodal authentication systems based on error correcting codes » Journal of Computer Security 18, 2010, 161–185, DOI 10.3233/JCS-2010-0369 IOS Press.

[Ari 1999] Ari Juels et Martin Wattenberg ; A fuzzy commitment scheme.In Proceedings of the 6th ACM conference on Computer and communications security,CCS '99, pages 28–36, New York, NY, USA. ACM. 1999, (Cité en pages 52 et 53.).

[ARTABAZ 2011] ARTABAZ, S. BIOMÉTRIE MULTIMODALE .(Mémoire magister, Ecole nationale Supérieure en Informatique Oued-Smar Alger, 2011.

[Barigou 2013] Barigou, F. contribution à la catégorisation de textes et à l'extraction d'information.(Thèse doctoral, université d'Oran, 2013.

[BARKA 2016] BARKA , K. & BOUKHRIS Y. Système d'identification biométrique à base d'un modèle flou, Mémoire master academique, université KASDI MERBAH OUARGLA,2016.

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

[Belguechi 2015] Belguechi, R. O. (2015). Sécurité des systèmes biométriques : révocabilité et protection de la vie privée, Doctoral dissertation, Ecole nationale Supérieure en Informatique Alger, 2015.

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

[Beulah 2014] Beulah, I. M., and Rani, L. Ensuring Privacy and Renewability Using Helper Data Systems on Multibiometric Cryptosystems, 2014.

[BOUTELLAA,] BOUTELLAA, E. Système biométrique de vérification de signatures manuscrites en ligne, Mémoire magister, Ecole nationale Supérieure d'informatique (E.S.I)Oued-Smar Alger.

[Bringer 2008] Bringer, J., Chabanne, H., Cohen, G. , Kindarji, B. et Zemor, G. Theoretical and Practical Boundaries of Binary Secure Sketches. IEEE Transactions on Information Forensics and Security, 2008, vol. 3, no. 4, pages 673–683. (Cité en page 54.).

[Bringer 2017] Bringer, J., Morel, C., and Rathgeb, C. Security analysis and improvement of some biometric protected templates based on Bloom filters. Image and Vision Computing, 2017, 58, 239-253.

[Canuto 2013] Canuto, A. M., Pintro, F., and Xavier-Junior, J. C. Investigating fusion approaches in multi-biometric cancellable recognition. Expert Systems with Applications, 2013, 40(6), 1971-1980.

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

[Chidemyan 2015] Chidemyan, S. S. Palm vein and fingerprint based multimodal fuzzy vault scheme.Proceedings of the YSU, Physical and Mathematial Scineces, Issue 1, 2015, Pages 41–46.

[Christian 2001] Christian Rathgeb et Andreas Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, vol. 2011, no. 1, pages 1–25, 2011. (Cité en pages 41, 43, 44, 47, 48 et 52.).

[Damasceno 2015] Damasceno, M., Canuto, A.M.P and Norman Poh « Multi-Privacy Biometric Protection Scheme using Ensemble Systems" CNPq'2015, Conselho Nacional de Desenvolvimento Cientifico e Tecnologico - Brazil, 2015.

[Dasgupta 1999] Dasgupta, S. and Gupta, A. An elementary proof of the Johnson-Lindenstrauss Lemma, UTechnical Report TR-99-006, International Computer Science Institute, Berkeley, CA, 1999.

[DEHACHE 2014] DEHACHE, I., & SOUICI-MESLATI, L. A. B. I. B. A. Une Approche Multimodale Pour La Vérification Biométrique. Courrier du Savoir, 2014, vol. 12.

[Dessimoz 2007] Dessimoz, D., Richiardi, J., Champod, C., & Drygajlo, A. Multimodal biometrics for identity documents (). Forensic science international, 2007 167(2-3), 154-159.

[Dinca 2017] Dinca, L. M., and Hancke, G. User-Centric Key Entropy : Study of Biometric Key Derivation Subject to Spoofing Attacks. Entropy, 2017, 19(2), 70.

[DJILI 2016] DJILI, A., & MAHDADI, D. E. Reconnaissance de personnes utilisant la multi-représentation de l'iris, Mémoire master academique, université KASDI MERBAH OUARGLA, 2016.

[Dwivedi 2019] Dwivedi, R., & Dey, S. A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. Applied Intelligence, 2019, 49(3), 1016-1035.

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

[Faundez 2005] Faundez-Zanuy, M. Data fusion in biometrics, in Aerospace and Electronic Systems Magazine, IEEE 2005, vol.20, no.1, pp.34-38.

[Fedias 2013] Fedias, M. (2013). Combinaisons de données d'espaces couleurs et de méthodes de vérification d'identité pour l'authentification de visages, Doctoral dissertation, Université Mohamed Khider-Biskra, 2013.

[Feng 2006] Feng Hao, R. Anderson et J. Daugman. Combining Cryptography with Biometrics Effectively. IEEE Transactions on Computers, 2006, vol. 55, no. 9, pages 1081–1088. (Cité en pages 52 et 53.).

[Ferguson 2010] Ferguson, N., Schneier, B. et Kohno, T. Cryptography Engineering, Design Princi, Wiley Online Library, 2010.

[Fischer 2009] FISCHER, S., REDONDO, R., et CRISTOBAL, G. How to construct log-Gabor Filters ? Instituto de Optica (CSIC). Serrano 121, 28006 Madrid, Spain, 2009.

[Gabor 1946] Gabor, D. Theory of Communication. J. Inst. Electr. Eng., 93 :429457, 1946.

[Geetha 2013] Geetha, K., & Radhakrishnan, V. Multimodal biometric system : A feature level fusion approach. International journal of computer applications, 2013, vol. 71, no 4.

[Geethanjali 2012] Geethanjali, N., Thamaraiselvi, K., and Priyadharshini, R. Feature level fusion of multibiometric cryptosystem in distributed system. International Journal of Modern Engineering Research (IJMER), 2012, vol. 2, no 6, p. 4643-4647.

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

[Giot 2012] Giot, R., Rosenberger, C., & Dorizzi, B. Reconnaissance du genre par analyse de dynamique de frappe au clavier sur texte libre. In : 7ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2012). 2012. p. 111-118.

[Goh 2003] Goh, A. and Ngo, C. Computation of cryptographic keys from face biometrics. In : IFIP International Conference on Communications and Multimedia Security. Springer, Berlin, Heidelberg, 2003. p. 1-13.

[Gomez 2017] Gomez-Barrero, M., Maiorana, E., Galbally, J., Campisi, P., and Fierrez, J. Multi-biometric template protection based on Homomorphic Encryption. Pattern Recognition, 2017, 67, 149-163A.

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

[Hili 2016] Hili, N. K. Biométrie multimodale basée sur l'iris et le visage, Doctoral dissertation, Université Paris-Saclay ; Université de Tunis El Manar, 2016.

[Ismail 2015] Ismail, S., Ali, F. H. H. M., and Aljunid, S. A. A New Hybrid Approach for Securing Multibiometric Templates Based on Cancelable and Fuzzy Commitment Scheme, 2015.

[Jain 2004] Jain, A. K., Ross, A., & Prabhakar, S. An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 2004, 14(1).

[Jain 2005] Jain, A., Nandakumar, K., & Ross, A. Score normalization in multimodal biometric systems. Pattern recognition, 2005, 38(12), 2270-2285.

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

[Jain 2008] Jain, A. k., Nandakumar, K. & Nagar,A. Biometric Template Security.EURASIP Journal on Advances in Signal Processing, 2008 no. 1, pages 1–17.(Cité en pages 1, 2, 10, 23, 24, 35, 41, 43, 44, 47, 48, 51, 52, 54 et 101.).

[Jegede 2018] Jegede, A., Udzir, N. I., Abdullah, A., & Mahmod, R. Revocable and Non-Invertible Multibiometric Template Protection based on Matrix Transformation. Pertanika Journal of Science & Technology, 2018, 26(1).

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

[Juels 2002] Juels, A. et Sudan, M. A fuzzy vault scheme. In Proceedings of IEEE International Symposium on Information Theory, 2002, pages 408. (Cité en pages 52 et 53.).

[Kanade 2010] Kanade, S.,Petrovska-Delac-etaz, D. and Dorizzi, B. Obtaining Cryptographic Keys Using Feature Level Fusion of Iris and Face Biometrics for Secure User Authentication. In IEEE CVPR Workshop on Biometrics, (June 2010).

[Karthi 2013] Karthi, G., and Azhilarasan, M. Hybrid multimodal template protection technique using fuzzy extractor and random projection. IJRCCT, 2013, 2(7), 381-386.

[Kaur 2008] Kaur, M., Singh, M., Girdhar, A., & Sandhu, P. S. Fingerprint verification system using minutiae extraction technique. World Academy of Science, Engineering and Technology, 2008, 46, 497-502.

[Kelkboom 2009] Kelkboom, E.,Zhou, X., Breebaart, J., Veldhuis, R. and Busch,C. (2009). "Multi-algorithm fusion with template protection," in Biometrics : Theory, Applications, and Systems, BTAS'09. IEEE 3rd International Conference on. IEEE, 2009, pp. 1–8.

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

[Kumar 2016] Kumar, A., and Kumar, A. A Cell-Array-Based Multibiometric Cryptosystem. IEEE access, 2016, 4, 15-25.

[Lahbib 2012] Lahbib, W., Algorithme Knn (k narres neighbours, ou k plus proches voisins), Ecole supérieur de commerce (ESC), (déc, 2012).

[Lalithamani 2015] Lalithamani, N., and Sabrigiriraj, M. Palm and hand vein-based fuzzy vault generation scheme for multibiometric cryptosystem. The Imaging Science Journal, 2015, 63(2), 111-118.

[Lam 1995] Lam, L., & Suen, C. Y. Optimal combinations of pattern classifiers. Pattern Recognition Letters, 1995, vol. 16, no 9, p. 945-954.

[Lim 2017] Lim, M., Mai, G., H., and Yuen, P. C. Binary feature fusion for discriminative and secure multi-biometric cryptosystems. Image and Vision Computing, 2017, vol. 58, p. 254-265.

[Liu 2001] Liu, S., & Silverman, M. A practical guide to biometric security technology. IT Profesional, 2001, 3(1), 27-32.

[Lu 2014] Lu, L., and Peng, J. Finger multi-biometric cryptosystem using feature-level fusion. International Journal of Signal Processing, Image Processing and Pattern Recognition, 2014, 7(3), 223-236.

[Maiorana 2011] Maiorana, E., Campisi, P., and Neri, A. Cancellable biometrics for on-line signature recognition. In New Technologies for Digital Crime and Forensics : Devices, Applications, and Software, 2011, (pp. 290-315). IGI Global.

[Maltoni 2003] Maltoni,D., Maio, D. , Jain, A. k. et Prabhakar, S. Handbook of fingerprint recognition. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.(Cité en pages 18, 31, 47, 58, 100 et 102.).

[Meenakshi 2010] Meenakshi, V. S., and Padmavathi, D. G. 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, 2010, 7(5), 1694-0814.

[Merkle 2012] Merkle, J., Kevenaar, T., and Korte, U. Multi-modal and multi-instance fusion for biometric cryptosystems. In Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the (pp. 1-6). IEEE (2012, September).

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

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

[Nagar 2012] Nagar, A., Nandakumar, K., and Jain, A. K. Multibiometric cryptosystems based on feature-level fusion. IEEE transactions on information forensics and security, 2012, 7(1), 255-268.

[Nandakumar 2005] Nandakumar, K. Integration of multiple cues in biometric systems Doctoral dissertation, Michigan State University. Department of Computer Science and Engineering, 2005

[Nandakumar 2008] Nandakumar, K. and Jain,A. K. Multibiometric template security using fuzzy vault. In : 2008 IEEE Second International Conference on Biometrics : Theory, Applications and Systems. IEEE, 2008. p. 1-6.

[Nanni 2006] Nanni, L., & Lumini, A. Empirical tests on biohashing. Neurocomputing, 2006, 69(16-18), 2390-2395.

[Navin 2005] Navin,G., BEBIS, G., et NEFIAN, A. Face recognition experiments with random projection. In : Biometric Technology for Human Identification II. International Society for Optics and Photonics, 2005. p. 426-438. (Cité en page 44.).

[Paul 2012] Paul, P., and Gavrilova, M. Multimodal cancelable biometrics. In : 2012 IEEE 11th international conference on cognitive informatics and cognitive computing. IEEE, 2012. p. 43-49.

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

[Pillai 2010] Pillai,J.K. Patel, V.M. Chellappa R. et Ratha, N.K. Sectored Random Projections for Cancelable Iris Biometrics. In Acoustics Speech and Signal Processing (ICASSP), IEEE International Conference on, 2010, pages 1838–1841,(Cité en page 44.).

[POP 2008] POP, Eugen LUPU Petre G. Multimodal biometric systems overview. Acta Technica Napocensis Electronics and Telecommunications, 2008, vol. 49, no 3.

[Ratha 2001] Ratha, N. K., Connell, J. H., & Bolle, R. M. Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 2001, 40(3), 614-634 Cité en pages 10, 12, 24, 35, 43 et 47.

[Ratha 2006] Ratha, N., Connell, J., Bolle, R. M., & Chikkerur, S. Cancelable biometrics : A case study in fingerprints. In 18th International Conference on Pattern Recognition (ICPR'06), (2006, August), Vol. 4, pp. 370-373). IEEE (Cité en pages 7, 33, 43, 47 et 49.).

[Ratha 2007] Ratha, N.K., Chikkerur, S., Connell, J.H. et Bolle, R.M. Generating Cancelable Fingerprint Templates. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 2007, vol. 29, no. 4, pages 561–572. (Cité en pages 47, 49, 97 et 101.)

[Rathgeb 2011] Rathgeb, C., & Uhl, A. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011(1),pages 1–25, 2011. (Cité en pages 41, 43, 44, 47, 48 et 52.).

[Rathgeb 2012] Rathgeb, C., & Busch, C. Multi-biometric template protection : Issues and challenges. In : New Trends and Developments in Biometrics. IntechOpen, 2012.

[Rathgeb 2014] Rathgeb, C., and Busch, C. Cancelable multi-biometrics : Mixing iris-codes based on adaptive bloom filters. Computers & Security, 2014, vol. 42, p. 1-12.

[Rathgeb 2015] Rathgeb, C., Gomez-Barrero, M., Busch, C., Galbally, J., and Fierrez, J. (2015, March). 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 (pp. 1-6). IEEE.

[Ross 2006] ROSS, Arun, NANDAKUMAR, Karthik, et JAIN, A. K. Information fusion in biometrics, in chapter 2. Handbook of Multibiometrics, International Series on Biometrics, 2006, vol.6.

[Ruud 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. (Cité en pages 28, 41 et 47.)

[Sankareswar 2015] Sankareswari, K., and Jothi, S. A. Hybrid Approach for Securing Biometric Templates such as fingerprint images and iris codes.Using Visual Cryptography. International Journal of Advance Research in Computer Science and Management Studies, 2015.

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

[Schneier 1995] Schneier,B. Applied cryptography (2nd ed.) : protocols, algorithms,and source code in c. John Wiley & Sons, Inc., New York, NY, USA, 1995. (Cité en pages 28 et 51.).

[Shanthini 2012] SHANTHINI, B. et SWAMYNATHAN, S. Multimodal biometric-based secured authentication system using steganography. Journal of Computer Science, 2012, vol. 8, no 7, p. 1012.

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

[Stokkenes 2016] Stokkenes, M., Ramachandra, R., Sigaard, M. K., Raja, K., Gomez-Barrero, M., and Busch, C. Multi-biometric template protection—A security analysis of binarized statistical features for bloom filters on smartphones. In : 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA). IEEE, 2016. p. 1-6.

[Sujitha 2019] SUJITHA, V. et CHITRA, D. A Novel Technique for Multi Biometric Cryptosystem Using Fuzzy Vault. Journal of medical systems, 2019, vol. 43, no 5, p. 112.

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

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

[Teoh 2008] Teoh, A. B., Kuan, Y. W., and Lee, S. Cancellable biometrics and annotations on biohash. Pattern recognition, 2008, vol. 41, no 6, p. 2034-2044.

[THANKI 2015] THANKI, R. M., and BORISAGAR, K. R. Analysis and Enhancement of Security in Multibiometric System Using CS Theory Based Watermarking Techniques.October 2015,https ://www.researchgate.net/publication/283255058.

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

[Xu 1992] XU, Lei, KRZYZAK, Adam, et SUEN, Ching Y. Methods of combining multiple classifiers and their applications to handwriting recognition. IEEE transactions on systems, man, and cybernetics, 1992, vol. 22, no 3, p. 418-435.

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

[Yang 2012] Yang, B., Busch, C.,Groot,K. H Xu and Raymond N. J. Veldhuis « Performance Evaluation of Fusing Protected Fingerprint Minutiae Templates

on the Decision Level » Sensors (Basel). 12(5) : 5246–5272.Published online 2012 Apr 26. doi : 10.3390/s120505246.

[Yevgeniy 2008] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin et Adam Smith. (Mars 2008). Fuzzy Extractors : How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Computing, 2008, vol. 38, no. 1, pages 97–139. (Cité en page 54.).

[Yildiz 2017] Yildiz, M., Yanikoğlu, B., Kholmatov, A., Kanak, A., Uludağ, U., and Erdoğan, H. (2017). Biometric layering with fingerprints : template security and privacy through multi-biometric template fusion. The Computer Journal, 2016, vol. 60, no 4, p. 573-587.

[Yilong 2011] Yilong Yin, Lili Liu, and Xiwei Sun. Sdumla-hmt : a multimodal biometric database. In Chinese Conference on Biometric Recognition, pages 260–268. Springer, 2011.

[You 2019] You, L., & Wang, T. A novel fuzzy vault scheme based on fingerprint and finger vein feature fusion. Soft Computing, 2019, vol. 23, no 11, p. 3843-3851.

[Zewail 2003] Zewail, R., SEIF, A., SAEB, M., et al. Iris identification based on log Gabor filtering. In : 2003 46th Midwest Symposium on Circuits and Systems. IEEE, 2003. p. 333-336.

[ZITOUNI 2016] ZITOUNI, S. & SACI A. Authentification et Identification biométrique des personnes par les empreintes palmaires, UNIVERSITE KASDI MERBAH OUARGLA, 2016