REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université de Mohamed El-Bachir El-Ibrahimi - Bordj Bou Arreridj

Faculté *des Sciences et de la technologie*

Département d'Électromécanique

Mémoire

Présenté pour obtenir

LE DIPLOME DE MASTER

FILIERE : ELECTROMECANIQUE

Spécialité : ELECTROMECANIQUE

Par :

- **Maiza Abderraouf**
- **Belhoul Brahim**

Intitulé

Etude et simulation d'un système biométrique effaçable multimodal

Soutenu le : 25 /06/2023

Devant le Jury composé de :

Nom & Prénom	*Grade*	*Qualité*	*Etablissement*
M. Zaoui Fares	*MCB*	*Président*	*Univ-BBA*
M. Bekkouche.Tewfik	*MCA*	*Encadreur*	*Univ-BBA*
M. Ben gueddouj Abdellah	*MCB*	*Examinateur*	*Univ-BBA*

Année Universitaire 2022/2023

Remerciements

Le grand remerciement revient à dieu qui nous a donné la force et le courage à réaliser et terminer ce modeste travail.

Nous tenons à remercier très vivement notre encadreur Monsieur ***Bekkouche Tewfik****, enseignant à l'université Mohamed El Bachir El Ibrahimi Bordj Bou Arreridj, nous le remercions de nous avoir toujours poussé vers l'avant, pour toute la confiance qu'il nous porte, pour sa grande disponibilité inconditionnelle, ses conseils avisés, et ses encouragements. Ses nombreuses idées furent un soutien très précieux.*

Nous remercions nos amis et collègues de l'université, pour l'ambiance conviviale qu'ils ont contribué à entretenir, les bons moments passés en leur compagnie et leur sympathie.

A tous ceux qui nous avons eu la chance de travailler avec ou que, nous avons eu l'honneur de côtoyer avant et pendant mon mémoire, et à tous nos professeurs de l'Université de Mohamed El Bachir El Ibrahimi Bordj Bou Arreridj.

Enfin, nous remercions chaleureusement tous les membres de nos familles et tous nos amis pour leur soutien et leurs encouragements.

DEDICACE

Je dédie ce mémoire :

À mes très chers parents pour leur soutient durant toute ma vie d'étudient et sans eux je ne serai jamais devenu ce que je suis.

*À toute ma famille. À mon encadreur « **Bekkouche Tewfik** ».*

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

À tous mes amis (es) sans aucune exception.

Collègues de la promotion 2022/2023

Spécialité : ELECTROMECANIQUE.

À toute personne ayant contribué à ce travail de près ou de loin.

Maiza Abderraouf.

DEDICACE

Je dédie ce mémoire :

À mes très chers parents pour leur soutient durant toute ma vie d'étudient et sans eux je ne serai jamais devenu ce que je suis.

*À toute ma famille. À mon encadreur « **Bekkouche Tewfik** ».*

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

À tous mes amis (es) sans aucune exception.

Collègues de la promotion 2022/2023

Spécialité : ELECTROMECANIQUE.

À toute personne ayant contribué à ce travail de près ou de loin.

Brahim

Table des matières

Chapitre 1

Chapitre 2

Chapitre 3

List de figures :

Liste des tableaux :

Introduction

Introduction

La Biométrie est dérivée de deux mots grecs à savoir. Bio signifie vie et métrique signifie mesurer. Il existe plusieurs traits ou caractéristiques tels que le doigt, le visage, l'oreille, l'iris, la démarche, qui sont les plus largement utilisés en biométrie. La technologie biométrique a été largement utilisé dans plusieurs applications telles que le contrôle d'accès, le contrôle de l'immigration dans les frontières, identification des cadavres, surveillance, secteur médecine légale, ordinateur humain interaction, analyse du comportement, etc… [1].

Avec le développement des capacités des appareils électroniques et des technologies de communication, l'utilisation de la biométrie comme moyen de vérification et d'identification des individus s'est développée énormément. La biométrie peut être physique comme les empreintes digitales, les empreintes palmaires ou les images faciales, ou comportementale comme la voix et la démarche. Chaque personne a une biométrie unique qui la distingue. La biométrie ne peut pas être remplacée lorsqu'elle est compromise. Par conséquent, il est préférable de protéger ou de remplacer la biométrie par des formulaires annulables générés par des méthodes non réversibles. Il existe deux directions principales de la protection biométrique, à savoir le bio-cryptage et la biométrie révocable.

Diverses méthodes ont été introduites pour protéger le modèle biométrique. Certains s'appuient sur une seule biométrie pour le processus de vérification dans ce qu'on appelle la biométrie monomodale. Les empreintes digitales, l'iris et les images faciales sont les éléments biométriques les plus couramment utilisés dans les systèmes de vérification monomodaux. Cette stratégie de vérification biométrique monomodale est peu fiable. Par conséquent, pour assurer un processus de vérification fiable, des données de la biométrie multimodale peuvent être collectées et utilisées pour rendre les systèmes plus sûrs, tels que les empreintes digitales avec des images d'iris, de visages, etc... [2].

Introduction

La protection des bases de données consiste à sécuriser les informations stockées dans une base de données contre les accès non autorisés, les altérations ou les suppressions malveillantes.

Le mémoire est organisé autour de trois chapitres, dans le premier chapitre, nous verrons des généralités sur la biométrie, dans le deuxième chapitre, nous aborderons la protection des bases de données biométriques. Quant au chapitre 3, nous passons à la partie pratique, par la proposition d'un algorithme de protection d'une base de données biométrique multimodale sous environnement Matlab. Cet algorithme est inspiré d'un article scientifique apparu en septembre 2022 et intitulé « Cancelable biometric system for IOT applications based on optical double random phase encoding » [3]. Enfin, nous clorons ce mémoire par une conclusion et des perspectives.

Chapitre 1
Généralités sur la biométrie

1.1 Introduction

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques. Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance d'un individu dans un grand nombre d'applications diverses. Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut garantir actuellement un excellent taux de reconnaissance avec des systèmes biométriques uni-modaux basés sur une unique signature biométrique. De plus, ces systèmes sont souvent affectés par les problèmes tels que le bruit introduit par le capteur, la non-universalité, le manque d'individualité et de représentation invariante ainsi que la sensibilité aux attaques. Ainsi, à cause de tous ces problèmes pratiques les taux d'erreur associés à des systèmes biométriques uni-modaux sont relativement élevés ce qui les rend inacceptables pour un déploiement d'applications critiques de sécurité. Pour pallier à ces inconvénients, une solution est l'utilisation de plusieurs modalités biométriques au sein d'un même système, on parle alors de système biométrique multimodal. Dans ce mémoire, nous avons présenté un système multimodal combinant les informations issues de visage et de l'empreinte palmaire. [8]

1.2 Définition de la biométrie

La biométrie peut être dénie comme étant la reconnaissance automatique d'une personne en utilisant des traits distinctifs, une autre définition de la biométrie et tous car athéistiques physiques ou traits personnels automatiquement mesurables, robustes et distinctives qui peuvent être utilisées pour identier un individu ou pour vérifier l'identité prétendue d'un individu... [5]

Il y a trois possibilités pour prouver son identité

1. Ce que l'on possède (carte, badge, document) ;
2. Ce que l'on sait (un nom, un mot de passe) ;
3. Ce que l'on est (empreintes digitales, main, visage, voix, ADN, signature, . . .) - Il s'agit de la biométrie.

1.3 Les types de systèmes biométriques

1.3.1 Mono-modalité

La biométrie monomodale est une technologie d'authentification de personne en se basant Sur une seule modalité biométrique. Avant de procéder à proposer un système biométrique, il est nécessaire de choisir la modalité la plus appropriée à l'application. [9]

1.3.2 Multi-modalité

La biométrie multimodale consiste à combiner plusieurs systèmes biométriques, ce qui permet l'augmentation de la quantité d'informations discriminante des personnes à identifier. En effet, elle

permet de diminuer certaines limitations des systèmes biométriques uni-modaux. La multi-modalité est une alternative qui permet d'améliorer de manière systémique la performance d'un système biométrique. [10]

1.4 La biométrie monomodal

Il existe aujourd'hui plusieurs choix pour les sécurités des systèmes. La biométrie est la plus utilisée dans des applications de la vie courante. Si à ses débuts au 19ème siècle les données biométriques étaient traitées manuellement, aujourd'hui, avec les traitements informatiques, les systèmes biométriques sont automatisés Nous ne décrivons ici que les modalités les plus communes, à savoir le visage, la parole, les empreintes digitales, le contour de la main et l'iris de l'÷il, laissant de côté d'autres modalités moins classiques (veines de la main, ADN, odeur corporelle, forme de l'oreille, des lèvres, rythme de frappe sur le clavier, démarche...). Dans ce chapitre, nous allons d'abord présenter le cadre général d'utilisation de la biométrie ainsi que la structure, les avantages des systèmes biométriques [4].

1.4.1 Différentes modalités biométriques

Aucune biométrie unique ne pouvant répondre efficacement aux besoins de toutes les applications d'identifications [4].

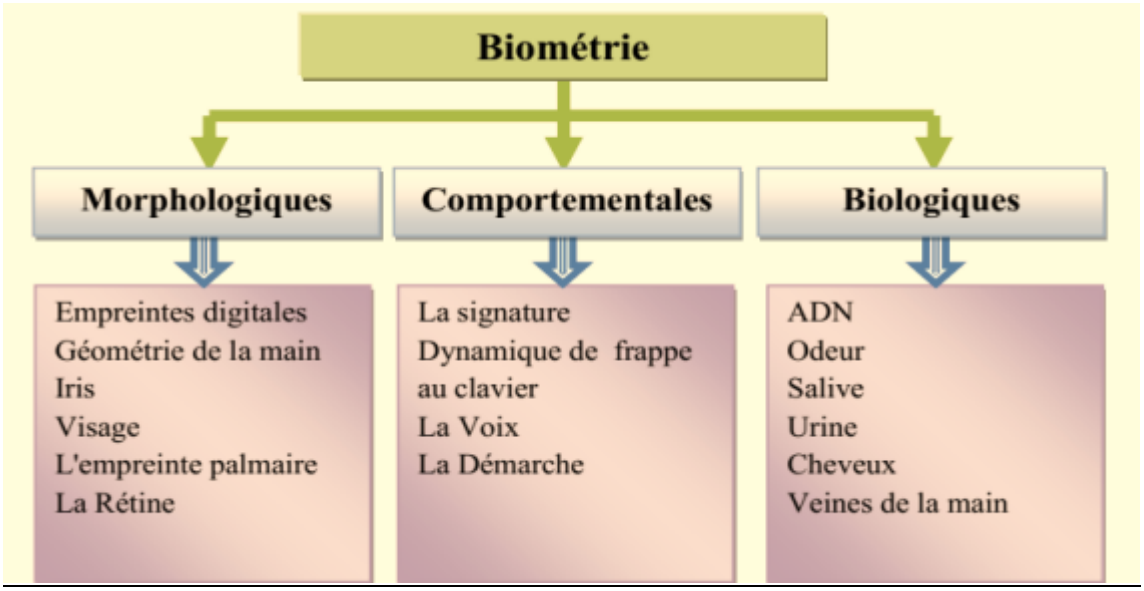


Figure 1. 1 : Les modalités biométriques

1.4.2 Les modalités biométriques

Les techniques utilisées dans la technologie biométrique peuvent être réparties en trois groupes comme nous l'avons dit ci haut et chaque groupe est constitué de quelques modalités biométriques. Dans cette section, nous allons essayer de voir les modalités biométriques que nous pouvons retrouver dans chaque groupe, leurs avantages et inconvénients les unes des autres.

A. La modalité morphologique

Cette technique fait allusion d'une manière générale aux formes et aspect extérieurs d'un être vivant et ces formes peuvent être de plusieurs types. Ceux qui sont utiles à la technologie biométrique sont empreinte digitale, main, voix, iris, rétine etc.

A.1 L'empreinte digitale

C'est une technique biométrique ancienne qui est généralement très connue par la plupart des gens [14]. Elle peut être définie comme une impression produite par la transpiration, la graisse, ou l'encre qui sont présentés dans la partie supérieure de chaque doigt de la main d'un être humain. Ces empreintes sont uniques pour chaque individu.

Figure 1.2 : Les parties de la minutie

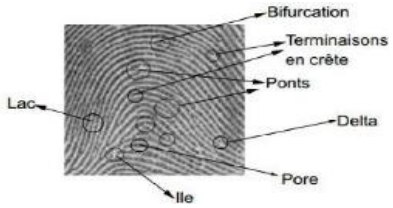


Figure 1.3 *:* L'empreinte digitale

A.1.2 Avantages et inconvénients de l'empreinte digitale

Avantages

- Facile à utiliser.
- La technologie la plus connue et éprouvée par le public.
- Faible coût.
- Traitement rapide.
- Petite taille de lecteur.
- Un bon compromis entre le taux de faux rejet et le taux de fausse acceptation [15].

Inconvénients

- Acceptabilité moyenne.
- Possibilité d'attaque.
- Certains systèmes peuvent accepter un moulage de doigts ou un doigt coupé.

A.2 Géométrie de la main

Chaque personne possède une forme propre de sa main. C'est une technique biométrique basée sur la mesure de la position et la taille des doigts placés sur une surface plane [16]. L'acquisition d'une image de la main est obtenue à l'aide d'un scanner spécialisé.

Figure 1.4 : Géométrique de la main [8]

A.2.1 Avantages et inconvénients de l'identification de la géométrie de la main

Avantages

- Utilisation simple.
- Bonne acceptabilité par les individus.
- Moins coûteuse que les empreintes digitales.
- Pas d'effet en cas d'humidité des doigts.

Inconvénients

- Risque de fausse acceptation pour des jumeaux ou des membres de la même famille.
- Trop encombrant pour un usage sur le bureau ou un téléphone.
- Modification de la forme des doigts avec le vieillissement [15].

A.3 La géométrie de l'oreille

L'oreille humaine a été utilisée comme un moyen de reconnaissance en médecine légale, et son morphologique extérieur est relativement stable durant une période de temps qui est acceptable pour les applications biométriques. Les approches de reconnaissance d'oreille sont basées sur la correspondance de la distance entre les différents points de référence de l'oreille. L'oreille humaine possède une richesse d'information qui se situe sur une surface 3D incurvée, cette richesse d'information a attiré l'attention des scientifiques légaux [17].

Figure 1.5 : Système de reconnaissance biométrique de l'oreille

A.3.1 Avantages et inconvénients de la reconnaissance biométrique de l'oreille

Avantages

- Une technique efficace, car il n'existe pas deux formes d'oreilles identiques.
- Très acceptable.

Inconvénients

- Il n'existe encore aucune application commerciale [18].

A.4 Le visage

Galton instaura dès le 19^{em} siècle dans ses ouvrages, avait publié ce que devrait la reconnaissance faciale actuelle. Ce n'est qu'à partir du milieu des années 80, lorsque la puissance des ordinateurs est devenue suffisante, que les recherches les plus poussées ont commencé. La reconnaissance se base sur les caractéristiques jugées significatives comme l'écart entre les yeux, la forme de la bouche, le tour de visage, la position des oreilles, l'écartement des narines ou encore la largeur de la bouche peuvent permettre d'identifier un individu. Cette méthode consiste à décomposer le visage selon plusieurs images en différents nuages des gris. Chaque image met en évidence une caractéristique particulière comme le montre l'image ci-dessous :

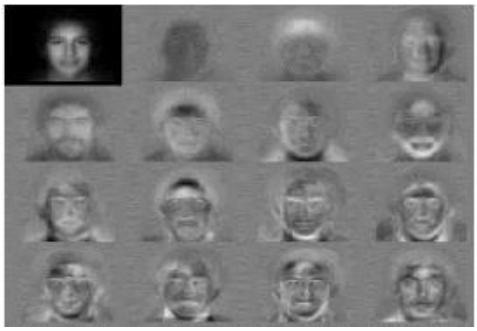


Figure 1.6 *: L*a décomposition du visage en plusieurs images gris

A.4.1 Avantages et inconvénients de reconnaissance de visage

Avantages

- Peu encombrant.
- Utilisation simple.
- Bonne acceptabilité.
- Peu coûteuse.

Inconvénients

- Problème de distinguer les vrais jumeaux.
- Peu d'efficacité.
- Sensibilité à la variation de l'éclairage et au changement de la position du visage [15].

A.5. Reconnaissance par analyse de l'Iris

C'est un voile très fin formé de lamelles pigmentaires qui donnent la couleur des yeux. L'identification par l'iris utilise plus de paramètres par rapport aux autres méthodes d'identification. Cette technique biométrique est employée dans le secteur financière, dans les hôpitaux et les grands aéroports [19].

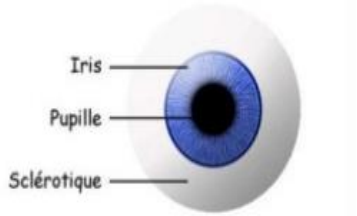


Figure 1.7 : L'iris

A.5.1 Avantages et inconvénients de la reconnaissance par iris

Avantages

- Distinguer les vrais jumeaux.
- Grande quantité d'information contenue dans l'iris.
- Fiabilité et durabilité.

Inconvénients

- Aspect psychologiquement invasif de la méthode.
- Coûteuse.
- Contraintes d'acquisition.
- Faible acceptabilité [15].

A.6 La reconnaissance par l'analyse de la rétine

La rétine est la couche sensorielle de l'œil qui permet la vision. Cette zone est parcourue par des vaisseaux sanguins qui émergent au niveau de la papille optique, où l'on distingue l'artère et la veine centrale de la rétine qui se divisent elles-mêmes en artères et veines de diamètre plus faible pour vasculariser les cellules qui permettent la vision.

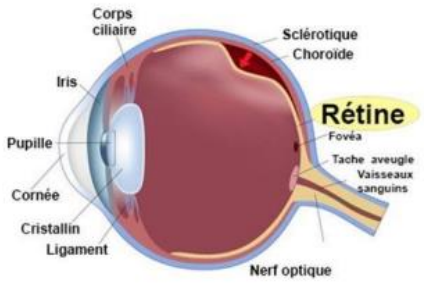


Figure 1.8 : La rétine

A.6.1 Avantages et inconvénients d'identification par rétine

Avantages

- La rétine est stable durant la vie d'un individu.
- Très efficace.
- La rétine est différente chez les vrais jumeaux.
- Haute sécurité.

Inconvénients

- Système intrusif car il faut placer l'œil près du capteur.
- Mal acceptée par le public.
- Un coût important [15].

B. Les modalités comportementales

B.1 La dynamique de frappe au clavier

C'est une propriété comportementale propre à chaque individu. Il s'agit d'une graphologie des temps modernes car on écrit plus souvent avec un clavier qu'avec un stylo. Les éléments principaux analysés par cette modalité sont : la vitesse de frappe, la suite de lettre, le temps de frappe, les pauses, etc. [20].

Figure 1.9 : La dynamique de frappe au clavier

B.1.1 Avantages et inconvénients de reconnaissance basée sur dynamique de frappe au clavier

Avantages

- Identification d'une personne à distance à partir de son ordinateur.
- Mise en œuvre rapide pour un grand nombre d'utilisation.
- Non intrusif, geste naturel pour une personne.

Inconvénients

- Dépend de l'état physique, émotion, fatigue, etc.
- Sensibilité à la différence entre les claviers [15].

B.2 La voix

La voix d'une personne peut être considérée comme la combinaison des caractéristiques morphologiques et comportementales. La voix est caractérisée par une intensité, une fréquence et une tonalité que l'on peut analyser par un microphone et à l'aide d'un traitement informatique. On peut isoler deux voix qui semblent être identiques pour l'oreille. L'aspect comportemental de la parole peut changer au cours du temps à cause de l'âge, l'état de santé et les émotions [21].

Figure 1.10 : Spectre d'un signal voix

B.2.1 Avantages et inconvénients d'identification vocale

Avantages

- Non intrusive.
- Facilité de protéger le lecteur.
- Seule information utilisable via le téléphone.
- Impossible d'imiter la voix.
- Sécurité d'une conversation téléphonique.

Inconvénients

- Taux élevé de faux de rejets et de fausses acceptations.
- Sensibilité aux bruits ambiants [15].

B.3 La signature électronique

Chaque personne est caractérisée par sa façon d'écriture unique. A partir de sa signature on peut définir un modèle qui pourra être utilisé pour l'identification des personnes [22].

Figure 1.11 : La signature électronique

B.3.1 Avantages et inconvénients d'identification basée sur la signature électronique

Avantages

- Bonne acceptabilité.
- La signature peut être conservée.
- Facile à utiliser.
- Elle implique la responsabilité de l'individu.

Inconvénients

- Sensibilité aux émotions de la personne.
- Besoin d'une tablette graphique.
- Non utilisable pour le contrôle d'accès en extérieur [15].

B.4 Analyse de la démarche

C'est une technique de reconnaissance biométrique utilisée à distance pour identifier et distinguer une personne grâce à sa manière de marcher et de bouger. En fait, chaque personne montre plusieurs traits tout en marchant tel que le maintien du corps, la position des genoux et les chevilles, la distance entre les deux pieds ce qui permet de l'identifier [22].

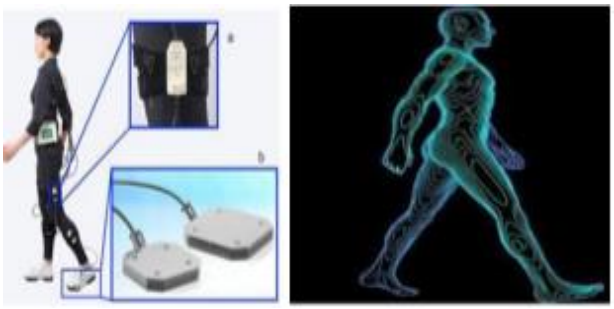


Figure 1.12 : Analyse de la démarche

B.4.1 Avantages et inconvénients de l'analyse de la démarche

Avantages

- Possibilité de suivre un individu pendant une longue durée.

Inconvénients

- Faible acceptabilité par les gens.
- Elle dépend du choix des chaussures et la nature d'habillement [15].

C. Modalité biologiques

C.1. Analyse de l'ADN

ADN (acide désoxyribonucléide) présent dans les cellules du corps, il est spécifique pour chaque individu. C'est une analyse du patrimoine génétique qui permet une identification à partir des cheveux, fragment de peau, d'une trace de sang et d'une goutte de salive. De plus l'ADN contient plus d'information sur l'identité des personnes [18].

Figure 1.13 : Système de reconnaissance basé sur l'ADN

C.1.1 Avantages et inconvénients de système de la reconnaissance d'ADN

Avantages

- Unique et permanant.
- Possibilité de différencier les individus à haute précision.
- Facile à obtenir.

Inconvénients

- Coûteux.
- Pour avoir les résultats, il faut attendre une longue durée.
- Facile à être volé [15].

C.2 La reconnaissance de thermographie faciale

Une caméra infrarouge capte la quantité de chaleur émise par les différentes parties du visage qui caractérise chaque personne. Contrairement à la biométrie faciale, la capture peut se faire dans des

états d'éclairages différents. Donc on peut l'utiliser dans l'obscurité ou de mauvaises conditions de visibilité [18].

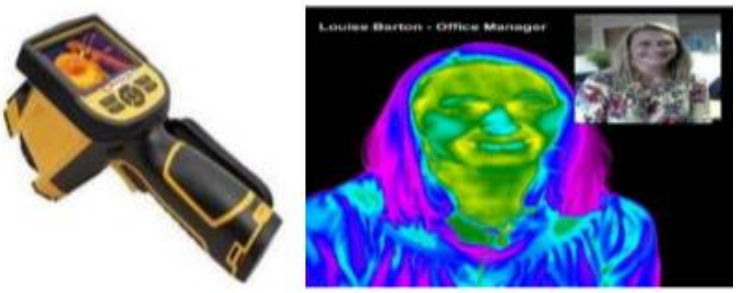


Figure 1.14 : Thermo-gamme faciale

C.2.1 Avantages et inconvénients de la thermo-gamme faciale

Avantages

- Faire une différence entre les vrais jumeaux.

Inconvénients

- Sensibilité aux émotions et à la température corporelle.
- Coûteuse [15].

1.5 La biométrie multimodale

La biométrie multimodale, qui consiste à combiner plusieurs systèmes biométriques, est de plus en plus étudiée. En effet elle permet de réduire certaines limitations des systèmes biométriques, comme l'impossibilité d'acquérir les données de certaines personnes ou la fraude intentionnelle, tout en améliorant les performances de reconnaissance. Ces avantages apportés par la multi-modalité aux systèmes biométriques "monomodaux" sont obtenus en fusionnant plusieurs systèmes biométriques. La première partie de ce travail est basée sur l'étude de méthodes de fusion de scores issus de systèmes biométriques. En un premier temps, des méthodes de fusion, largement utilisées dans le domaine de la biométrie multimodale, sont comparées sur une base de données de grande taille dont la qualité dégradée reflète les applications réelles de mobilité (par exemple la reconnaissance sur un terminal ou un téléphone mobile). Dans un deuxième temps, nous proposons une approche originale : une stratégie séquentielle de fusion. Le principe de cette stratégie séquentielle est de fusionner les systèmes successivement afin de n'utiliser, pour chaque personne, que la quantité d'information suffisante pour prendre la décision. Cette stratégie permet de garder des performances équivalentes aux systèmes fusionnant tous les systèmes mais elle permet surtout de réduire une contrainte importante des systèmes multimodaux : le coût (en termes de temps de traitement) et la difficulté d'utilisation due à l'accumulation des modalités. Dans une deuxième

partie, nous |présenterons des mesures de dépendance statistique et particulièrement une mesure de dépendance basée sur l'entropie : l'information mutuelle [7].

1.5.1 Définition de la biométrie multimodale

La biométrie multimodale est la combinaison de plusieurs modalités biométriques différentes, en augmentant la quantité d'informations discriminante de chaque personne et cela pour améliorer les performances de reconnaissance [11].

1.5.2 Différents systèmes multimodaux

On peut différencier 5 types de systèmes multimodaux selon les systèmes qu'ils combinent [12].

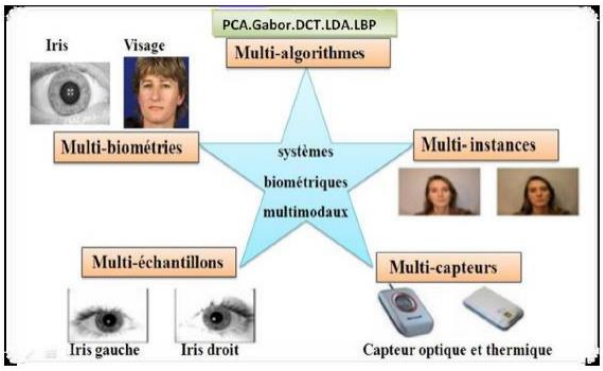


Figure 1.15 : Les différents systèmes multimodaux [11]

1.5.2.1 Multi-échantillons

Un unique capteur peut être utilisé pour acquérir plusieurs échantillons du même trait biométrique dans le but de prendre en compte les variations qui peuvent se produire au sein de ce trait, ou pour obtenir une représentation plus complète du caractère sous-jacent. Par exemple, un système de reconnaissance faciale peut capturer (et enregistrer) le profil frontal du visage d'une personne ainsi que les profils gauches et droits afin de tenir compte des variations de la pose faciale [11].

1.5.2.2 Multi-capteurs

Dans ces systèmes, un même trait biométrique est analysé à l'aide de plusieurs capteurs afin d'extraire diverses informations provenant de l'enregistrement des images. Par exemple un système peut enregistrer le contenu de la texture 2D du visage d'une personne avec une caméra CCD et la forme de la surface 3D du visage avec une autre gamme de capteurs dans le but de procéder à la reconnaissance. Dans ce cas, c'est l'introduction des capteurs 3D servant à mesurer la variation de la surface du visage qui est responsable de l'augmentation du coût du système biométrique multimodal [11].

1.5.2.3 Multi-algorithmes

Dans ces systèmes, les mêmes données biométriques sont traitées à travers plusieurs algorithmes. Par exemple, des algorithmes d'analyse de texture et de minuties peuvent être associés pour traiter la même image d'empreinte digitale afin d'extraire diverses caractéristiques qui peuvent améliorer la performance du système [11].

1.5.2.4 Multi-instances

Ces systèmes utilisent tout simplement plusieurs instances d'un même trait biométrique. Par exemple, les iris gauches et droits d'un individu peuvent être utilisés afin de vérifier son identité [11].

1.5.2.5 Multi-biométries

Les systèmes multi-biométries (ou multi-caractères) utilisent l'information de plusieurs modalités biométriques différentes combinées pour la réalisation de la reconnaissance des individus [11].

1.5.3 Architecture d'un système multimodal

Le système multimodal se réfère à la combinaison de deux ou plusieurs systèmes biométriques en acquérant les informations qui seront traitées par la suite. Ces deux procédures peuvent se faire simultanément (architecture parallèle) ou en série (architecture série).

1.5.3.1 L'architecture en parallèle

Est la plus utilisée car elle permet d'utiliser toutes les informations disponibles au même temps (l'acquisition ou traitement simultanément) et donc d'améliorer les performances du système. 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 [13].

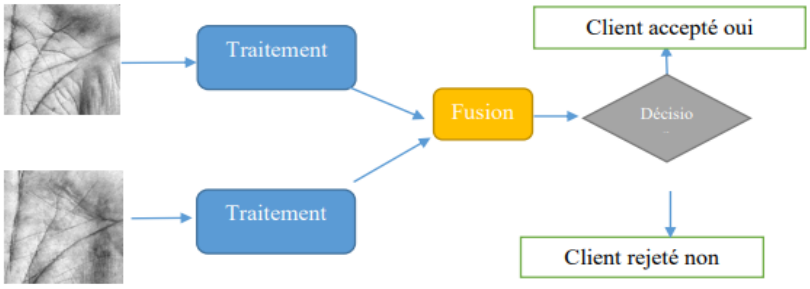


Figure 1.16 : Architecture de fusion en parallèle [13]

1.5.3.2 L'architecture en séries

La multi modalité est utilisée pour donner une alternative pour les personnes ne pouvant pas utiliser l'empreinte digitale. Pour la majorité des individus seule l'empreinte est acquise et traitée mais pour

ceux qui ne peuvent pas être ainsi authentifiés on utilise un système à base d'iris alternativement [13].

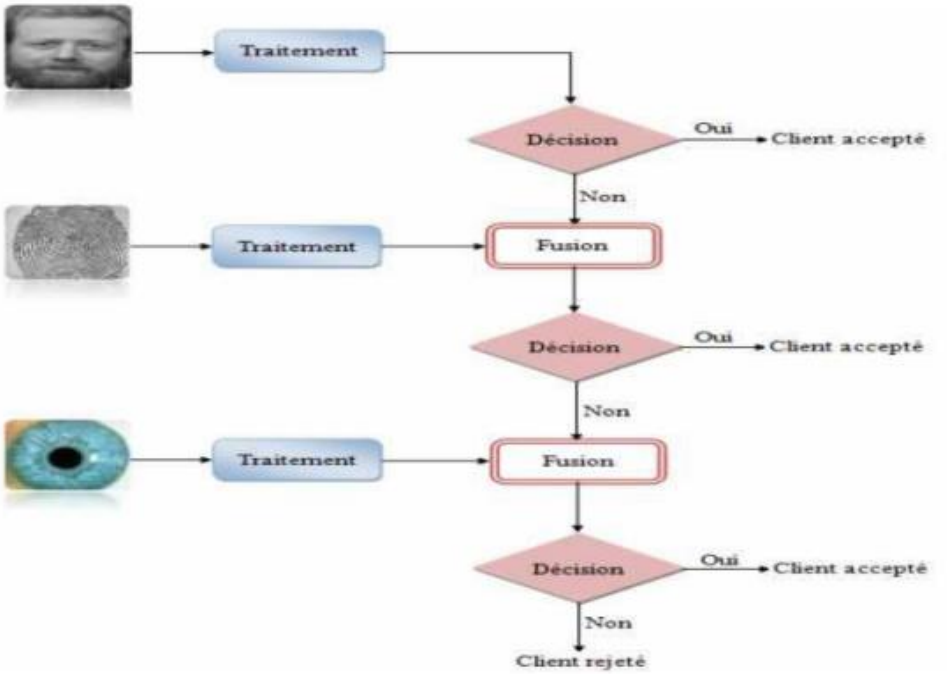


Figure 1.17 : Architecture de fusion en série [13]

1.6 Comparaison entre quelques techniques biométriques

Identifiant biométrique	Universalité	Caractère distinctif	Permanence	Facilité de saisie	Performance	Acceptabilité	Facilité de contournement
ADN	E	E	E	E	E	F	F
Oreille	M	M	E	M	M	E	M
Visage	E	F	M	E	F	E	E
Empreinte digitale	M	E	E	M	E	M	M
Démarche	M	F	F	E	F	E	M
Géométrie de la main	M	M	M	E	M	M	M
Veines de la main	M	M	M	M	M	M	F
Iris	E	E	E	M	E	F	F
Dynamique	F	F	F	M	E	M	M

de la frappe							
Empreinte palmaire	M	E	E	M	E	M	M
Rétine	E	E	M	F	E	F	F
Signature	F	F	F	E	F	E	E
Voix	M	F	F	M	F	E	E

Tableau 1.1 : Tableau comparatif des différentes techniques biométriques. (E : Elevé, F : faible et M : Moyen) [23]

1.7 Les Systèmes biométriques et leurs modes de fonctionnements

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Selon le contexte de l'application, le système biométrique fonctionne suivant trois modes : l'enrôlement, la vérification et l'identification [24].

1.7.1 Le mode d'enrôlement

C'est la première phase de tout système biométrique, pendant laquelle les caractéristiques biométriques d'un individu sont enregistrées dans la base de données pour la première fois.

Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données. Qui sera utilisée plus tard dans la phase d'authentification. Pendant l'enrôlement on extrait des caractéristiques biométriques en utilisant des algorithmes adéquats, ces caractéristiques seront réduites par la suite pour minimiser la quantité de données a stockée en facilitant ainsi la vérification et l'identification.

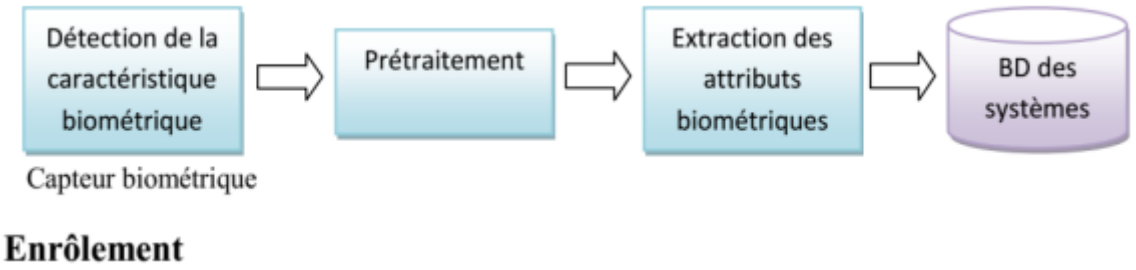


Figure 1.18 : Enrôlement d'une personne dans un système biométrique [25]

1.7.2 Le mode d'authentification (vérification)

Lorsqu'un système biométrique opère en **mode authentification** (Figure 19), l'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non.

Le système biométrique demande à l'utilisateur son identité et essaye de répondre à la question, « est-ce la personne X ? ». Dans une application de vérification l'utilisateur annonce son identité par l'intermédiaire d'un mot de passe, d'un numéro d'identification, d'un nom d'utilisateur, ou toute

combinaison des trois. Le système sollicite également une information biométrique provenant de l'utilisateur, et compare la donnée caractéristique obtenue à partir de l'information entrée, avec la donnée enregistrée correspondante à l'identité prétendue, c'est une comparaison un à un (1 :1). Le système trouvera ou ne trouvera pas d'appariement entre les deux. La vérification est communément employée dans des applications de contrôle d'accès et de paiement par authentification [25] [26].

L'authentification par la biométrie est plus forte que celle utilisant les moyens classiques d'identification tels que les cartes, clés ou mots de passe car elle constitue un lien fort et permanent entre une personne physique et son identité.

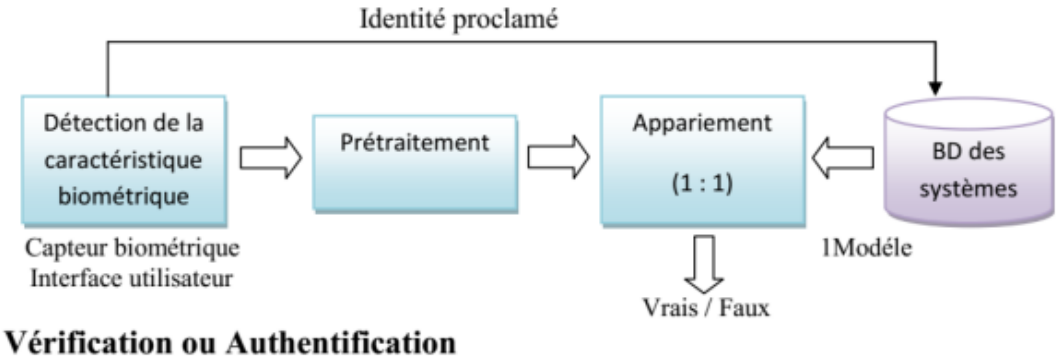


Figure 1.19 : Authentification d'un individu dans un système biométrique [25]

1.7.3 Le mode d'identification

Elle permet d'établir l'identité d'une personne à partir d'une base de données, le système biométrique pose et essaye de répondre à la question, « qui est la personne X ? », il s'agit d'une comparaison du type un contre plusieurs [27].

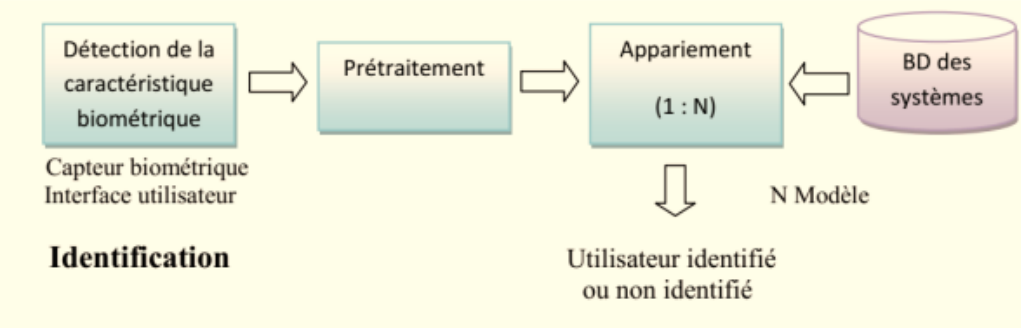


Figure 1. 20 : Identification d'un individu dans un système biométrique [27]

1.8 Conclusion

Dans ce chapitre nous avons donné une présentation générale de la biométrie et ses différentes modalités utilisées dans les systèmes biométriques pour l'identification des personnes, les avantages et inconvénients de chaque modalité ainsi que la comparaison entre quelques techniques biométriques. Nous avons défini le système biométrique et son mode de fonctionnement, domaine d'application, les types de systèmes biométriques et leurs performances. Enfin nous présenté la biométrie multimodale qui est le domaine d'étude de ce mémoire.

Chapitre 2

La protection des bases de données biométriques multimodales

Chapitre 2 : La protection des bases de données biométriques multimodales

2.1 Introduction

La protection des bases de données biométriques multimodales est une question cruciale car ses bases de données contiennent des informations sensibles sur les caractéristiques physiques uniques des individus, telles que les empreintes digitales, l'iris, les visages, les empreintes vocales, etc. Ces informations peuvent être utilisées à des fins d'identification et d'authentification, mais peuvent également être utilisées à des fins malveillantes telles que la fraude, le vol d'identité et l'espionnage.

Pour protéger les bases de données biométriques multimodales, plusieurs mesures peuvent être mises en place, notamment :

- Cryptage : Les données biométriques peuvent être cryptées de manière à ce qu'elles ne soient accessibles qu'aux personnes autorisées. Le cryptage est une méthode de sécurité qui convertit les données en un code qui ne peut être compris que par les personnes qui ont la clé de décryptage.
- Authentification : La base de données biométrique doit être protégée par des méthodes d'authentification robustes, telles que des mots de passe forts, des codes PIN et/ou l'utilisation de la biométrie elle-même pour accéder aux données.
- Contrôle d'accès : Le contrôle d'accès est une méthode de sécurité qui permet de contrôler l'accès à la base de données biométrique en limitant l'accès aux personnes autorisées.
- Stockage sécurisé : La base de données biométrique doit être stockée dans un environnement sécurisé qui limite les risques d'attaques physiques ou électroniques.
- Surveillance et suivi : Les activités sur la base de données biométrique doivent être surveillées et suivies en temps réel pour détecter toute activité suspecte ou malveillante.
- Formation et sensibilisation : Les personnes qui ont accès à la base de données biométrique doivent être formées et sensibilisées à la sécurité des données pour comprendre les risques potentiels et les mesures de sécurité nécessaires pour protéger les données.

En fin de compte, la protection des bases de données biométriques multimodales nécessite une approche multicouche, qui combine des mesures techniques, organisationnelles et humaines pour assurer la sécurité des données. La biométrie comprend tout un ensemble de technologies et procédés de reconnaissance, d'authentification et d'identification des personnes à partir de certaines de leurs caractéristiques physiques ou comportementales.

Ces dernières années, avec la large application de la technologie d'identification biométrique, les gens sont de plus en plus préoccupés par la sécurité de leur propre biométrie. Dans les deux cas, tant que vous fournissez vos propres informations biométriques, ces informations biométriques

risquent d'être copiées et détournées. De plus, la biométrie humaine ne change généralement pas et, une fois divulguée, elle ne peut pas être modifiée ou réinitialisée comme un mot de passe. Lorsque les mêmes informations biométriques sont appliquées à plusieurs systèmes d'information, la fuite d'informations biométriques dans un système affectera la sécurité des autres systèmes [32].

Pour protéger les bases de données biométriques multimodales, plusieurs mesures peuvent être mises en place.

2.2 Méthodes générales des modèles biométriques annulables

Les modèles biométriques annulables sont des modèles de reconnaissance biométrique qui permettent aux utilisateurs de révoquer ou de réinitialiser leurs identités biométriques en cas de violation de leur vie privée ou de vol de leurs données biométriques. Voici quelques méthodes de génération de modèles biométriques annulables [33].

2.2.1 Méthodes des cryptographies

L'importance de la cryptographie a été comprise dès les premiers réseaux informatiques. En fait, les ordinateurs communiquaient sur des réseaux ouverts. Bien que ce type de réseau ait bien servi pendant longtemps, il a également permis les espionnages de données. Cependant, vu que les services financiers étaient les premiers à être menacés, il était urgent de trouver un moyen pour garder les informations secrètes. C'est là qu'apparaît le rôle de la cryptographie [34]. Il y a plusieurs techniques, ces techniques sont divisées en divers types tels que la cryptographie visuelle, le hachage d'image, la signature de connaissances, l'elliptique Cryptographie de courbe (ECC), Chaos, Stéganographie, engagement flou et chiffrement de Hill. Ensuite, nous décrivons chacune de ces techniques.

2.2.1.1 La cryptographie visuelle

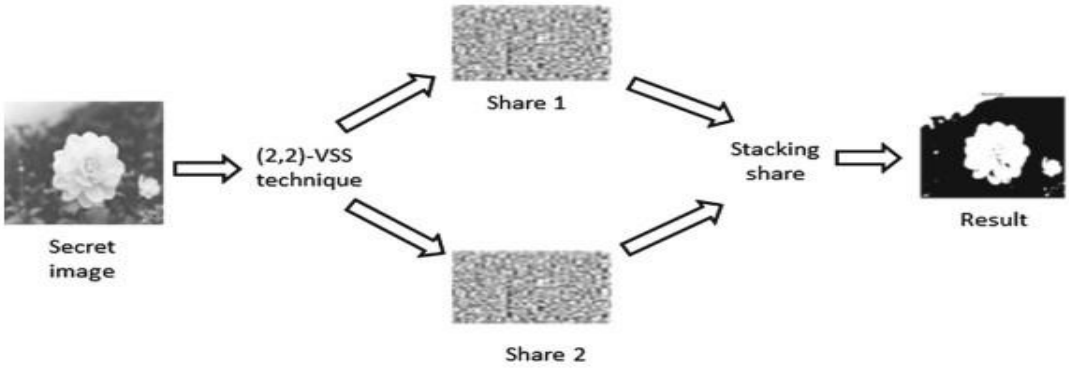


Figure 2.1 : La cryptographie visuelle d'une image d'entrée et transformée en une autre image crypte résultat

Dans la cryptographie visuelle, une image d'entrée est transformée en une autre image en exploitant le système visuel humain comme le montre la Figure 2.1. L'image binaire secrète est divisée en n patchs non chevauchants connus sous le nom de partages secrets visuels (VSS) et ces partages sont stockés dans Une base de données décentralisée [35].

2.2.1.2 La segmentation d'image

C'est une méthode bien connue d'authentification des images basées sur le contenu. En effet, elle détermine un vecteur d'entités appelé une signature binaire courte qui caractérise indépendamment l'image sans distorsion significative de son contenu [36].

2.2.1.3 Biohashing

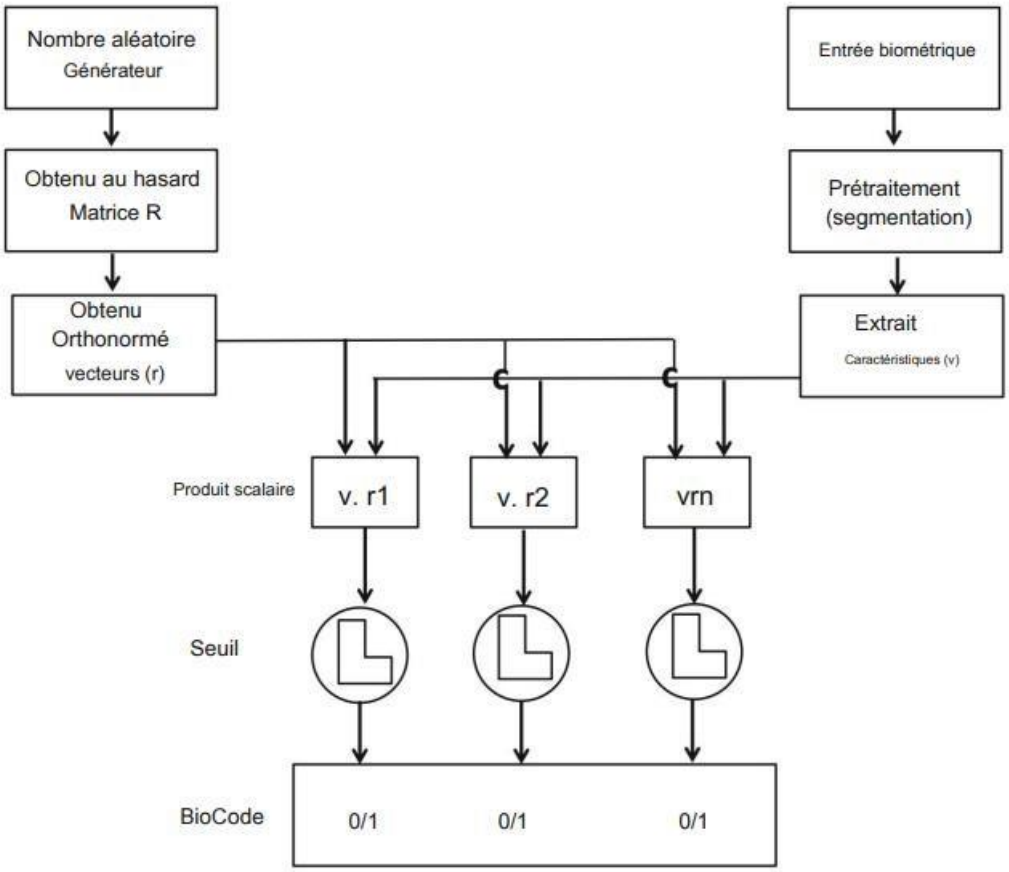


Figure 2.2 : Représentation schématique de la méthode BioHashing

C'est une fonctionnalité de procède d'extraction dans laquelle la conservation en ondelettes est utilisée pour extraire la caractéristique biométrique a partir des données biométriques saisies En utilisant un nombre aléatoire nominal (TRN) de l'utilisateur, des vecteurs pseudos aléatoires Perpendiculaires binaires sont génères, Ou le produit scalaire de la caractéristique et de tous les vecteurs aléatoires est calculé. Enfin, la discrimination binaire est appliquée pour calcule un modelé de hachage binaire de n bites (c) en utilisant l'équation ci-dessous :

$$c = Sig\ (\sum xbi - \Omega) \qquad (2.1)$$

Sig est défini comme une fonction de signal.

Ω est un seuil défini empiriquement qui ne s'applique qu'à l'utilisateur titulaire du TRN Base Bio Hashing est une variante de Bio Hashing qui utilise un seul trait biométrique, tel qu'une empreinte digitale ou une image faciale, comme entrée dans la fonction de hachage. Le code de hachage généré par la fonction est utilisé comme modèle de référence d'un individu [37].

2.2.1.4 La segmentation sensible à la zone

C'est une méthode de segmentation d'images qui utilise des informations de position et de forme pour diviser une image en plusieurs zones ou régions. Cette méthode est souvent utilisée pour traiter des images qui contiennent des objets de différentes tailles ou formes, ou lorsque l'on souhaite identifier des zones d'intérêt spécifiques dans une image.

La segmentation sensible à la zone peut être effectuée à l'aide de plusieurs techniques, notamment :

- Segmentation basée sur la région : cette technique divise l'image en régions homogènes en termes de couleur, de texture ou de propriétés géométriques. Chaque région est ensuite étiquetée en fonction de sa propriété dominante.
- Segmentation basée sur l'arbre de décision : cette technique utilise un arbre de décision pour décider si un pixel appartient à une certaine zone ou non. L'arbre de décision est construit en utilisant des caractéristiques telles que la couleur, la texture, la forme, etc.
- Segmentation basée sur les contours : cette technique utilise les contours de l'image pour diviser l'image en régions. Les régions sont obtenues en traçant les contours de l'image à différents niveaux de seuillage [34].

En utilisant la segmentation sensible à la zone, il est possible d'obtenir des résultats plus précis et cohérents dans des scénarios où la segmentation basée sur des seuils fixes ne fonctionne pas bien. Cette méthode peut être utilisée dans de nombreux domaines, tels que la reconnaissance de forme, la vision par ordinateur, la médecine, etc.

2.2.1.5 La technologie de signature des connaissances

C'est une méthode permet à une partie de convaincre les autres parties de sa connaissance d'une certaine valeur, de sorte qu'aucune information utile ne soit divulguée. Habituellement utilisé pour la confirmation Membres du groupe dans les signatures de groupe.

La technologie de codage de courbe elliptique (ECC) est utilisée pour obtenir une entrée stable à partir de données biométriques utilisées pour créer des paramètres de sécurité pour la courbe elliptique, divers.

Des études sur l'ECC ont conclu que la difficulté de résoudre un problème logarithmique discret de la courbe elliptique est très difficile en ce qui concerne la taille de la clé utilisée. Cette propriété

rend ECC est un très bon choix pour le processus de cryptage / décryptage par rapport aux autres cryptages Techniques qui sont linéairement ou semi-difficiles de manière significative [34].

En cryptographie_symétrique, le chiffre de Hill est un modèle simple d'extension du chiffrement affine à un bloc. Ce système étudié par Lester_S._Hill[1], utilise les propriétés de l'arithmétique modulaire et des matrices [38]. Comme illustrer dans les figures a et b et c.

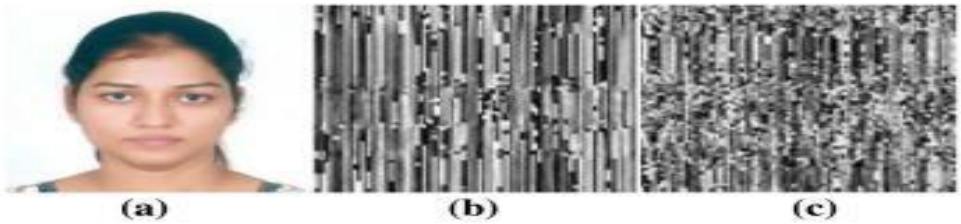


Figure 2.3 : Image d'entrée (a) , image cryptée (b), image décryptée (c)

2.2.2 Méthodes fondées sur la conversion

La transformation non inversible est l'une des premières méthodes de génération de modèles biométriques annulables. Dans cette méthode, les modèles biométriques originaux sont transformés en appliquant Différentes transformations, par exemple cartésiennes, polaires, etc... In Cartésien transformation, Les positions minutieuses sont mesurées en coordonnées rectangulaires par rapport à la position du Point singulier en alignant l'axe des x avec son orientation. Le système de coordonnées est divisé en cellules de taille fixe. La transformation provoque des changements dans les positions des cellules. Dans la transformation polaire, les positions minutieuses sont mesurées dans la coordonnée polaire par rapport à la position centrale. Les angles sont mesurés par rapport à l'orientation du noyau. Par conséquent, L'espace de coordonnées est divisé en régions polaires [35]. La transformée de Hadamard est une transformation orthogonale non sinusoïdale dont le fondement Réside dans les fonctions de Walsh. Les fonctions de Walsh sont des formes d'onde rectangulaires ou carrées avec des valeurs de +1 ou −1. La matrice de Hadamard est définie comme une matrice dont les éléments sont +1 et −1 et Ses vecteurs de ligne sont orthogonaux par paires. La transformation de Hadamard est divisée en deux types Hadamard partiel et (42) Hadamard complet. Le premier est non inversible tandis que le plus tard est inversible dans la nature. Le travail de recherche (Wang et Hu 2013) utilise la transformation partielle de Hadamard qui peut être formé en sélectionnant un certain nombre de lignes à partir de Full Hadamard Transforme [38].

2.2.3 Méthodes basées sur les filtres

Le filtre biométrique annulable est une méthode basée sur l'enveloppement. Bloom Filtres est une structure de données probabiliste peu encombrante qui représente un groupe pour prendre en charge les requêtes d'adhésion. Rose La conversion basée sur le filtre de tout vecteur d'entités binaires génère des éléments irréversibles Modèles de données biométriques [36] utilisé le filtre Bloom avec

voûte floue pour empêcher les attaques par correspondance croisée dans le système biométrique annulable. Filtre Bloom adaptatif Est une autre variante des filtres Bloom. Filtre Bloom adaptative est une autre variante des filtres Bloom. Rathgeb et al. (2014) ont utilisé le filtre Adaptive Bloom pour générer un alignement gratuit Iris annulable Modèle biométrique. Cette approche perme protection dans les modèles biométriques, génère des données biométriques compressées et réduit le temps de calcul tout en maintenant les performances de reconnaissance biométrique [37].

Les filtres Log Gabor sont largement utilisés dans divers travaux de recherche pour l'extraction de caractéristiques en raison de à une meilleure information spatiale et temporelle. Kaur et Khanna (2017a) ont utilisé des filtres log-Gabor avec projection aléatoire pour générer des vecteurs d'entités annulables. Dans cette approche, les auteurs ont utilisé le salage de la magnitude log-Gabor extraite avec des diagrammes de phase du signal biométrique qui entraîne la génération de Non [38].

2.2.4 Méthodes hybrides

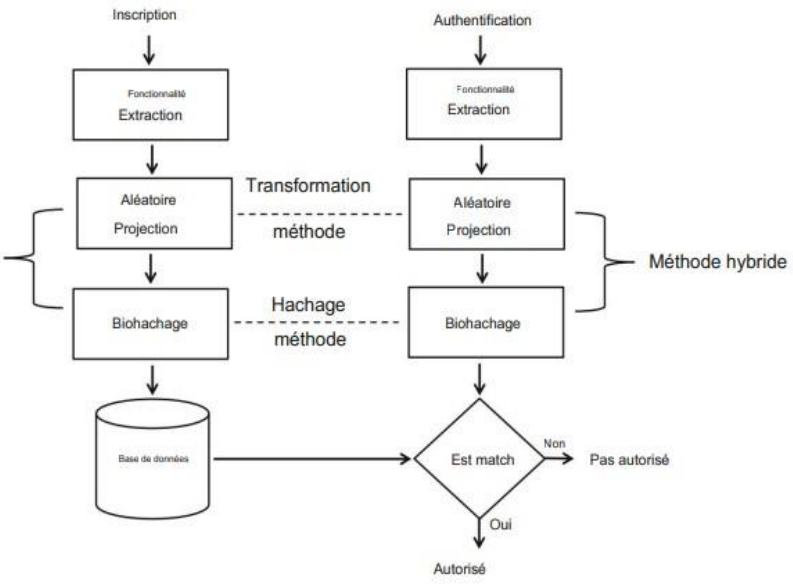


Figure 2.4 : Un exemple de méthode hybride

Les méthodes hybrides ont tendance à combiner deux méthodes ou plus pour générer un modèle biométrique annulable, par exemple une combinaison de méthodes de cryptographie et de transformation, comme illustré à la Figur 2.4 Les phases d'annulation, de discriminabilité et de sécurité constituent la partie principale de cette méthode [39] ont utilisé la projection aléatoire avec Fuzzy Vault pour générer des modèles d'empreinte vocale.

2.2.5 Méthodes basées sur la biométrie multimodale

La biométrie multimodale combine plusieurs traits biométriques avec divers algorithmes d'extraction de caractéristiques pour générer des modèles plus sécurisés. La multimodalité peut être

obtenue en combinant plusieurs traits biométriques tels que la prise de plusieurs biométries pour, par exemple. Iris, visage, empreinte digitale du même utilisateur pour la reconnaissance d'identité. Le principal avantage du système biométrique multimodal est qu'il est bon en termes de fiabilité, de précision, d'attaques frauduleuses, de sensibilité au bruit et plus sûr que la biométrie unimodale.
Système. Diverses méthodes ont été suggérées dans la littérature pour la biométrie multimodale ont suggéré des systèmes biométriques annulables de premier ordre, de deuxième ordre et multi ordres. Dans la méthode de premier ordre, le modèle annulable est généré en utilisant n'importe quelle technique de génération de modèle biométrique annulable une fois, tandis que dans la méthode de second ordre, deux techniques de génération de modèle biométrique annulable sont appliquées séquentiellement. Dans la méthode Multi ordre, les techniques de génération de modèles biométriques annulables sont appliquées plusieurs fois, ce qui peut être la même technique avec des paramètres différents ou des techniques complètement différentes. En fonction du nombre de fois où la méthode de génération de modèles biométriques annulables est appliquée, nous pouvons atteindre une sécurité élevée, mais au prix d'une complexité de calcul accrue [40].

2.2.6 Autres méthodes

Bio Convolions est également une approche basée sur la transformation non inversible principalement caractérisée par trois transformations Baseline Mixant et Shirtings. [41]. Cette approche peut être appliquée à diverses modalités biométriques, par exemple la parole, dans lesquelles l'analyse spectrale ou temporelle du signal vocal crée des séquences discrètes. De même, en cas de reconnaissance de signature et d'écriture manuscrite, où les séquences extraites sont basées sur la position du stylet et la quantité de pression et d'inclinaison appliquée.
Les permutations aléatoires sont une autre méthode de protection de modèle biométrique dans laquelle les valeurs de gris de l'image biométrique sont réorganisées avant un traitement ultérieur [42] ont utilisé l'analyse en composantes principales à permutation aléatoire (RP-PCA) et l'ACP Bidimensionnelle à permutation aléatoire (RP-2DPCA) pour générer des modèles annulables pour le visage, l'iris et l'oreille.
Deux méthodes populaires dans cette catégorie sont largement utilisées pour générer des modèles d'iris annulables, à savoir (i) GRAY-COMBO (ii) BIN-COMBO Dans GRAY-COMBO, le vecteur de caractéristiques binaires d'une image Iris est décalé de manière circulaire dans la direction horizontale à l'aide d'un décalage aléatoire, puis ces deux lignes sélectionnées au hasard sont ajoutées ou multipliées à l'aide de l'opérateur d'addition et de multiplication, comme illustré à la Fig. 5. Dans BIN- COMBO, le processus de décalage horizontal des lignes est le même, après quoi les lignes sélectionnées au hasard sont combinées avec les opérateurs XOR et XNOR. Le principal

avantage de cette méthode est que la quantité d'informations nécessaires à la reconnaissance est réduite. La principale limite de cette méthode est la bonne qualité des images de l'iris [43].

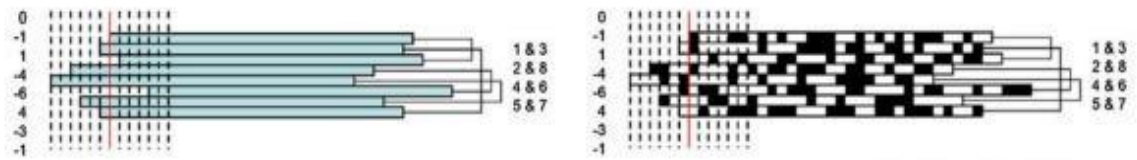


Figure 2.5 : Méthodes GRAY-COMBO (à gauche) et BIN-COMBO (à droite)

2.3 Mesures de performance

Les mesures de performance nous fournissent un outil utile pour analyser la capacité d'un algorithme. Diverses mesures de performance sont utilisées pour comparer les algorithmes ou les méthodes en fonction d'un domaine ou d'un domaine de recherche particulier. Ici, nous fournissons un examen complet des mesures de performance utilisées dans la reconnaissance biométrique annulable.

2.3.1 Mesures de performance pour la vérification

Deux caractéristiques biométriques appartiennent au même utilisateur ou non sont déterminées par le score de similarité. L'appariement de deux échantillons d'un même utilisateur est appelé appariement authentique ou véritable. L'appariement entre deux échantillons générés par deux utilisateurs différents est appelé appariement imposteur. Les scores sont utilisés pour exprimer la similarité entre un modèle de requête et un modèle authentique [44].

Une valeur plus élevée du score signifie une plus grande similitude entre eux. Une valeur seuil η est définie pour le processus de reconnaissance. Un système biométrique attribue à toutes les tentatives un score de groupe fermé de [0, 1]. La valeur de score 1 indique généralement une correspondance complète et 0 représente aucune correspondance. La valeur du seuil est prise très soigneusement, si elle est définie sur 0, alors les utilisateurs authentiques et intrus sont tous deux authentifiés par le système. S'il est défini sur 1, il devrait y avoir un risque qu'aucun ne soit authentifié par le système. Ainsi, la valeur de seuil doit être choisie très soigneusement dans un groupe fermé de 0 et 1. Un score d'intrus qui dépasse le seuil η connu sous le nom de False Accept (False Match), tandis qu'un score authentique qui tombe en dessous du seuil η connu sous le nom de False Reject (False Non correspondre). Les faux positifs (FP) signifient que les scores d'imposteur dépassent le seuil, les faux négatifs (FN) indiquent les scores d'utilisateurs authentiques inférieurs au seuil. Vrai négatif (TN) montre vraiment.

2.3.2 Mesures de performance pour l'identification

Les mesures de performance de vérification, le nombre de mesures d'identification est faible. Les chercheurs ont généralement utilisé le taux d'identification/reconnaissance, la précision, la précision de la classification, le temps de formation et le temps de test comme mesures de performance pour l'identification.

Taux d'identification ou taux de reconnaissance : Le taux d'identification est une estimation de la probabilité qu'un sujet soit correctement identifié au moins au rang-k [45].

Précision : C'est le rapport entre les vrais cas (à la fois vrais positifs et vrais négatifs) à tous cas possibles.

Précision de classification : La précision de classification Ai d'un programme individuel i dépend du nombre d'échantillons correctement classés (vrais positifs plus vrais négatifs) et est évaluée par la formule :

$$A_i = \frac{t}{n} \times 100 \qquad (2.1)$$

Où t est le nombre d'échantillons de cas correctement classés et n est le nombre total d'échantillons de cas.

2.3.3 Autres mesures de performance

Au cours de nos recherches, nous avons étudié que certains chercheurs utilisent des mesures de performance spécifiques pour leurs travaux de recherche, par exemple ont utilisé le rapport pic sur lobe latéral (PSR), qui est le rapport entre la moyenne du pic et l'écart type. Où la moyenne et l'écart type sont calculés dans une région angulaire centrée sur le pic et ont utilisé des équations de mélange de noyaux gaussiens et de champ de potentiel électrique pour générer un modèle d'empreinte digitale annulable. La performance est totalement basée sur la rapidité avec laquelle l'intrus peut trouver les valeurs des variables utilisées dans ces équations. Génèrent des modèles d'empreintes palmaires annulables. En cela, pour améliorer les performances du code Palmhash, un PRN à valeur gaussienne est utilisé à la place du code Palmhash avec un PRN à trois valeurs. Nous avons également observé que certains chercheurs n'utilisaient aucune mesure de performance pour leurs travaux de recherche. La majorité de ces travaux incluent une technique basée sur le cloud pour le stockage de modèles biométriques annulables et une technique de génération de clé stable à partir de données biométriques bruyantes.

2.4 Attaques contre la biométrie annulable

Diverses attaques sont possibles sur le système biométrique annulable, c'est-à-dire au niveau du capteur, au niveau de l'application et au niveau de la base de données. Dans une situation, lorsque le

système prend conscience qu'un intrus tente d'accéder au système, il peut modifier la fonction de transformation intermédiaire et générer des modèles erronés [46].

Dans la deuxième situation, le système bloquera ce compte et plus tard, lorsque l'utilisateur authentique tentera d'accéder au compte, il recevra un message d'alerte concernant ses informations d'identification, et enfin un nouveau modèle sera délivré à l'utilisateur authentique. Nous avons étudié divers types d'attaques existaient dans la littérature à savoir. Force brute, attaque via la multiplicité, jeton perdu, basé sur un dictionnaire, usurpation d'identité, intrusion, cryptanalyse, escalade, attaque inverse et pré-image

- Dans une attaque par force brute
- Dans l'attaque par jeton perdu
- Dans l'attaque de violation de la vie privée
- L'attaque de pré-image sur un système biométrique tente de trouver des échantillons biométriques très similaires à usurper

2.5 bases de données utilisées dans la biométrie annulable

Lorsqu'un algorithme est comparé à d'autres algorithmes, nous avons besoin d'un ensemble standard d'images. Plusieurs chercheurs se sont efforcés de développer divers ensembles d'images appelés bases de données. Les performances des algorithmes biométriques annulables sont testées sur une grande variété de bases de données. Ici, nous fournissons un examen complet des bases de données utilisées par divers chercheurs dans la reconnaissance biométrique annulable [47].

2.5.1 Bases de données de visages

2.5.1.1 La base de données PIE (pose, illumination, expression)

a été créée à l'université Carnegie Mellon (CMU) en 2000 avec 13 poses différentes, 43 conditions d'éclairage différentes et 4 expressions différentes. Il se compose de 41 368 images de 68 personnes dans diverses conditions. Le principal inconvénient de cette base de données est ce nombre limité de personnes prises pour des images sous une seule session d'enregistrement avec peu d'expressions [48].

2.5.1.2 La base de données CMU Multi PIE

Surmonte le problème qui se pose avec CMU PIE. Cette base de données contient 750 000 images de 337 personnes. La base de données se compose d'images couleur haute résolution dans deux formats, à savoir. JPG (groupe photographique commun pour les images haute résolution) ou PNG (groupe réseau portable pour les images multi-vues). Les images ont été prises sous 15 points de

vue et 19 conditions d'éclairage avec différentes expressions faciales, qui nécessitent 305 Go d'espace de stockage [49].

2.5.1.3 RA

Cette base de données formée par Aleix Martinez et Robert Benavente. Les images de cette base de données incluent l'expression faciale, l'illumination et l'occlusion. La base de données se compose de plus de 4000 images de 126 personnes parmi lesquelles 70 hommes et 56 femmes sont inclus. Chaque image a la taille de 768 × 576 pixels [50].

2.5.1.4 FÉRET

La base de données de la technologie de reconnaissance faciale a été collectée en 15 sessions et 1564 séries. Cette base de données contient 14126 images couleur de 1199 peuples. Deux visages, deux illuminations et entre 9 et 20 variations de pose sont prises lors de la constitution de cette base de données. Pour maintenir la cohérence, toute la base de données est formée dans le même environnement et dans les mêmes conditions de configuration physique.

2.5.1.5 BERC

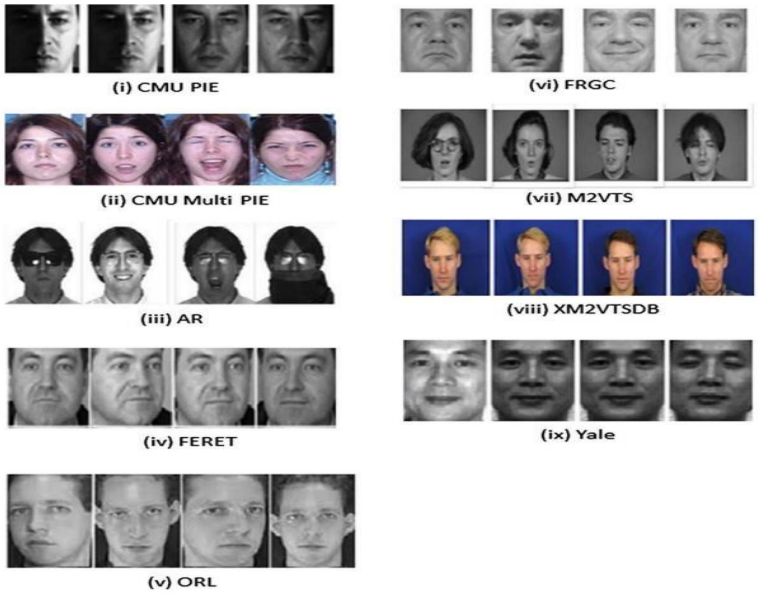


Figure 2.6 : Exemples d'images de bases de données de visages

La base de données BERC a été formée par le Bio-metrics Engineering Research Center. La base de données se compose de 5238 images de 390 sujets dans le groupe d'âge de 3 à 83 ans. Les images sont de très haute résolution 3648 × 2736 pixels par rapport à toutes les autres bases de données. Les images sont prises sous la même lumière, expression faciale, éclairage et occlusion avec/sans lunettes. Cette base de données s'est formée au laboratoire de recherche Olivetti, anciennement nommé American Tele phone & Telegraph Company. Cette base de données contient 400 images

de 40 sujets avec une résolution de 92 × 112. Certaines personnes photographiées à des moments différents et avec des variations d'expression faciale, par ex. en changeant l'éclairage, les yeux ouverts et fermés, avec/sans sourire, présence/ absence de lunettes

2.5.2 Bases de données Iris

2.5.2.1 ITI Delhi

Base de données Iris de l'Institut indien de technologie collectée au laboratoire de recherche biométrique en 2007. Cette base de données contient un total de 1120 images de 224 sujets, dont 176 hommes et 48 femmes. Les images de la base de données ont une résolution de 320 × 240 pixels prises auprès des étudiants et du personnel âgé de 14 à 55 ans de l'IIT Delhi dans un environnement intérieur.

2.5.2.2 CASIA Ver1, Ver2, Ver3

Cette base de données porte le nom de l'Institut d'automatisation du Centre de recherche sur la biométrie et la sécurité (CBSR) de l'Académie chinoise des sciences (CASIA), en Chine. Cette base de données a trois versions. CASIA-IrisV1 se compose de 756 images de 108 yeux avec une résolution de 320×280. VALID est également une base de données multimodale, composée de 530 images de 106 sujets (5 images par sujet) avec une résolution de 720 × 576 pixels. Certaines images sont prises dans un scénario de bureau réel sans bruit, les autres sont dans un éclairage différent et avec un bruit acoustique. CASIA-IrisV3 se compose de 22 035 images d'iris de plus de 700 sujets de même résolution de 640 × 480 [51].

2.5.2.3 GLACE NIST

National Institute of Standards and Technologie (NIST) pour l'Iris Challenge Evaluation (ICE) formé de 2 953 images avec une résolution de 480 × 640 pixels de 244 yeux différents

5.2.4 EC

La base de données Casia-BioSecure est divisée en deux parties : BioSecureV1 et CasiaV2. Cette base de données se compose d'un total de 2953 images de 244 iris différents avec une résolution de 640 × 240 pixels.

Ces images sont capturées dans différentes sessions, illumination et avec/sans lunettes.

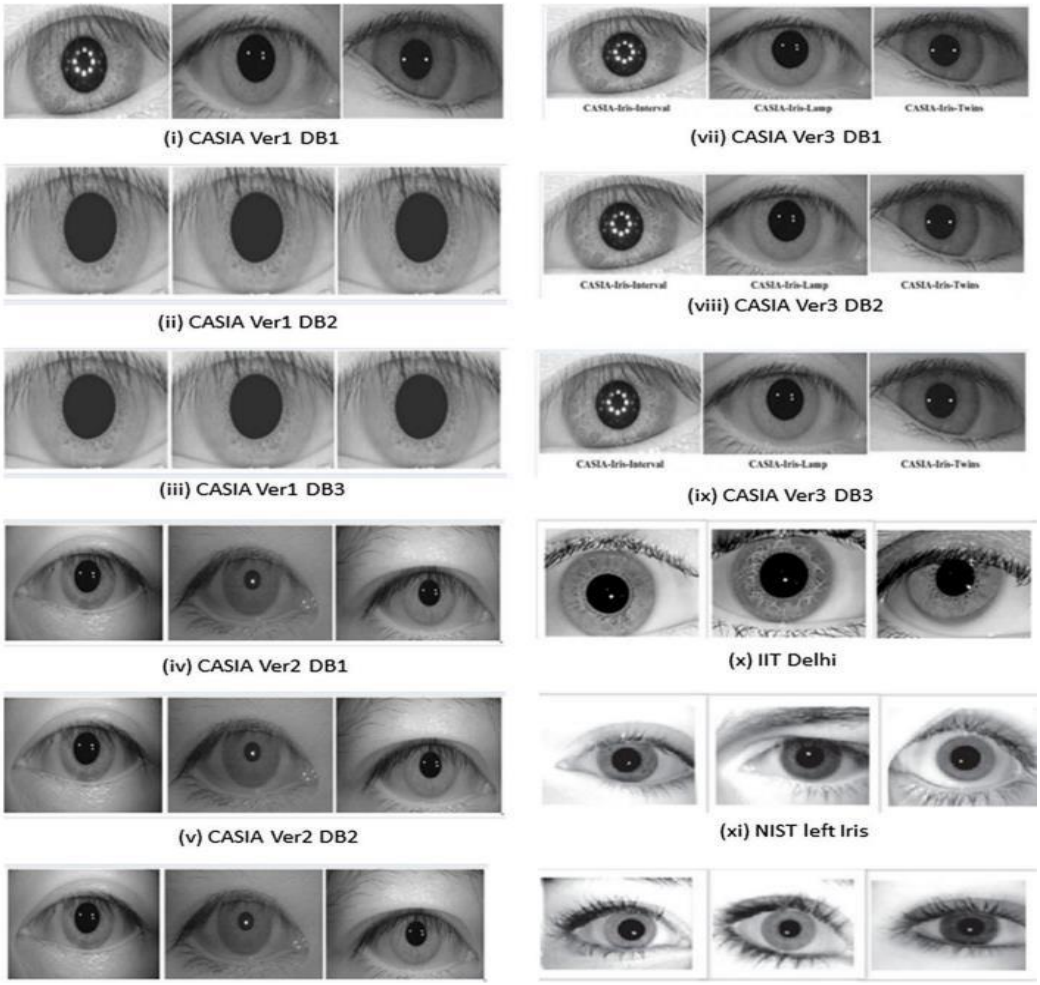


Figure 2.7 : Exemples d'images es bases de données CASIA, IIT Delhi, NIST Iris

2.5.3 Bases de données vocales

2.5.3.1 TIMIT

La base de données Texas Instruments (TI) du Massachusetts Institute of Technology (MIT) comprend 6300 phrases prononcées par 630 locuteurs (10 échantillons de chaque locuteur), dont 430 hommes et 192 femelles. La base de données se compose de 2 dialectes de l'anglais américain, lus par 630 locuteurs, 450 phrases phonétiquement compactes et 1890 phrases phonétiquement diverses. Il comprend également des transcriptions orthographiques, phonétiques et de mots ainsi qu'un fichier de forme d'onde vocale 16 bits, 16 kHz pour chaque énoncé [52].

2.5.3.2 Vidimt

Cette base de données contient 43 vidéos de personnes et les enregistrements audio correspondants avec un total de 430 (10 enregistrements/personne). Cette base de données enregistrée en 3 sessions, en plus des phrases, les personnes ont été invitées à tourner la tête en séquence (gauche, droite, retour au centre, haut, puis bas et enfin retour au centre) à chaque session. Les données vidéo

de chaque personne sont stockées dans une séquence d'images jpeg de 512 × 384 pixels. L'audio correspondant est stocké avec un fichier wav 16 bits et 32 kHz.

Section ID	Sentence ID	Sentence text
Session 1	Sa1	She had your dark suit in rensy wash water all year
	Sa2	Don ‘t ask me to carry an oil rag like that
	Si1398	Do they make class binsed decisions ?
	Si2028	He took hismaske from his forehead and threw it ,unexpeetedly ,across the deek
	Si768	Make lid for sugar bowl the same as jar lids omitting design disk
	Sx138	The clumsy custemer spilled some expensive perfume
doSession 2	Sx228	The viewpoint overlooked the ocean
	Sx318	Please dig my potatoes up before frost
Session 3	Sx408	I’d ride the subway. But I haven’t enough change
	Sx48	Grandmother outgrew her upbringing in petticoats

Tableau 2.1 : Exemple les basses des donnes vocales

2.5.4 Bases de données d'empreintes digitales

2.5.4.1 CVF

Le concours de vérification des empreintes digitales est un concours international axé sur l'évaluation des logiciels de vérification des empreintes digitales. FVC a 3 versions FVC2000, FVC2002 et FVC2004 avec 4 bases de données à savoir les bases de données DB1, DB2, DB3, DB4. FVC 2002 contient un total de 800 images de 110 personnes avec 500 dpi chacune.

2.5.4.2 IBM-99

La base de données optique International Business Machine contient un total de 376 images (188 × 2) de 188 paires d'empreintes digitales d'utilisateurs, chaque image avec 512 dpi.

2.5.5 Base de données des signatures

2.5.5.1 MCYT

Ministerio de Ciencia y Technologie, Ministère espagnol des sciences et de la technologie La base de données bimodale MCYT comprend un total de 16500 images de 330 sujets, chaque image ayant une taille de 300 × 300. Ils ont utilisé un dispositif de capture capacitif basé sur CMOS et un dispositif de capture optique avec une résolution de 500 ppp [53].

Figure 2.8: Exemple MCYT signature

2.5.6 Base de données d'empreintes palmaires

2.5.6.1 Poly U

La base de données Palm-print Version 2 de l'Université polytechnique de Hong Kong (Poly U) se compose de 600 images en niveaux de gris de 100 utilisateurs (6 images palmaires/utilisateur), la taille de l'image d'origine est de 384 × 284 pixels à 75 dpi. À partir d'une empreinte palmaire orientée, une taille d'image de 128 × 128 est recadrée [54].

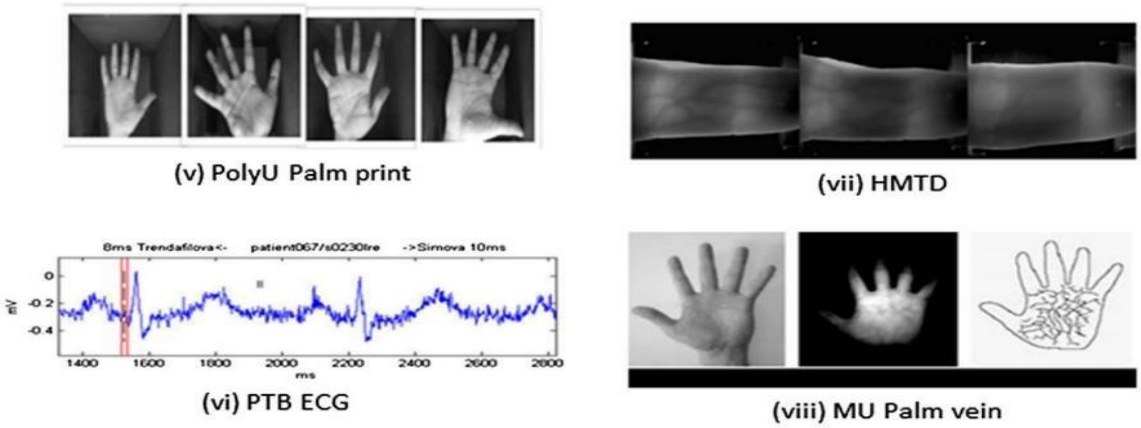


Figure 2.9: Exemple de base de données poly u

2.6 Conclusion

En conclusion, La protection des bases de données biométriques multimodales est un sujet critique et complexe qui nécessite une attention particulière pour garantir la sécurité et la confidentialité des informations sensibles. Les données biométriques sont des informations personnelles hautement confidentielles, et leur utilisation doit être réglementée par des lois et des normes de sécurité strictes. Pour protéger les bases de données biométriques, il est essentiel de mettre en place des mesures de sécurité appropriées telles que la cryptographie, la gestion des accès et l'authentification forte. De plus, la sensibilisation et la formation des utilisateurs sur les risques liés à la sécurité des

données biométriques sont également des facteurs clés pour garantir la protection des bases de données.

En fin de compte, la protection des bases de données biométriques multimodales est essentielle pour garantir la confidentialité et la sécurité des informations personnelles sensibles. Les organisations doivent être vigilantes pour garantir que les données biométriques sont stockées et utilisées de manière responsable et conforme aux réglementations en vigueur [55].

Chapitre 3

Implémentation d'un algorithme de protection d'une base de données biométrique multimodale sous environnement Matlab

Chapitre3 : Implémentation d'un algorithme de protection d'une base de données biométrique multimodale sous environnement Matlab

3.1 Introduction

Dans ce chapitre, nous procédons à l'implémentation d'un algorithme de protection d'une base de données biométrique multimodale sous environnement Matlab ou ce qu'on appelle (Cancellable biometrics). Cette implémentation s'articule autour d'un article scientifique intitulé : **' Cancelable biometric system for IoT applications based on optical double random phase encoding'** apparu dans le journal Optics Express · September 2022. Nous avons utilisé deux modalités biométriques à savoir le visage et l'empreinte digitale [31].

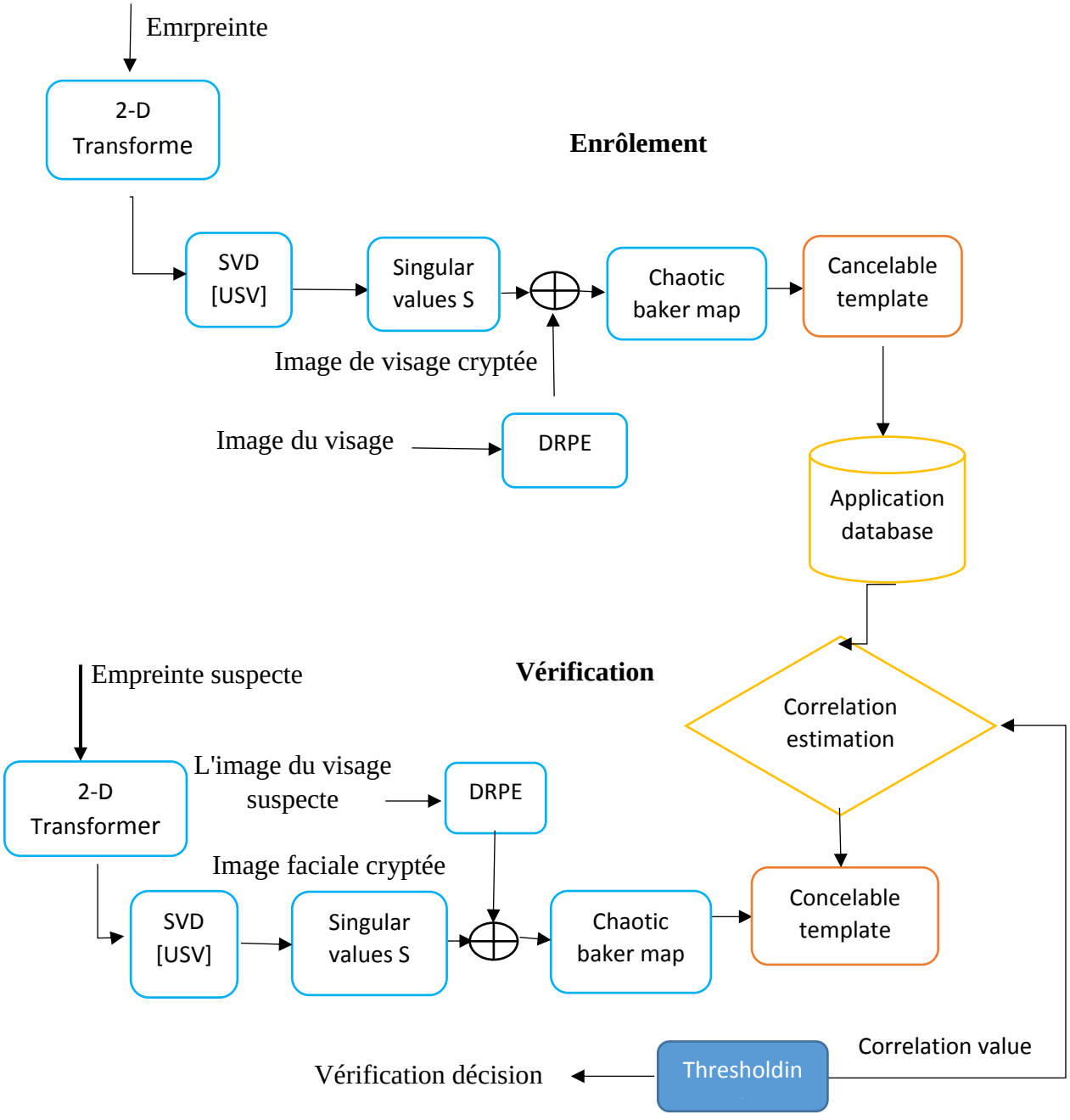


Figure 3.1 : Système de protection proposé de la base de donnés biométrique

La Figure 1.3 ci-dessous illustre le système de protection proposé de la base de données multimodale constituée des deux modalités (empreinte digitale-visage). Ce schéma est subdivisé en deux parties distinctes : la partie **'enrôlement'** et la partie **'vérification'**

3.2 Notions préliminaires

3.2.1 Cryptage à base de la Double Random Phase Encoding (DRPE)

C'est un cryptage d'images qui s'effectue dans le domaine fréquentiel à base des transformées comme la transformée de Fourier discrète (DFT), la transformée de Fourier fractionnaire (frFT) etc. Cette technique consiste à multiplier l'image originale élément par élément par un masque ayant le module égale à 1 est une phase générée aléatoirement entre 0 et 2 π, puis la résultante est transformée au domaine fréquentiel par le biais de la transformée de Fourier discrète . Le résultat obtenu est multiplié par un deuxième masque généré aussi aléatoirement puis transformé au domaine spatial par le biais de la transformée de Fourier discrète inverse (IDFT) pour donner l'image cryptée **Figure 3.2.**

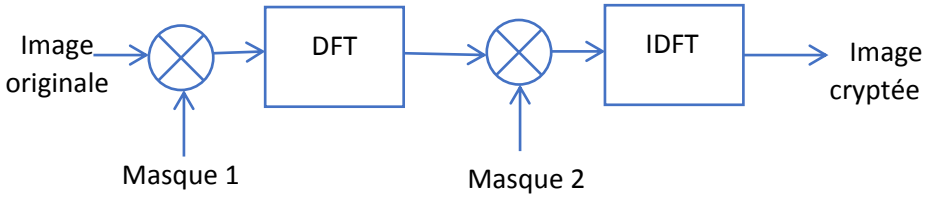
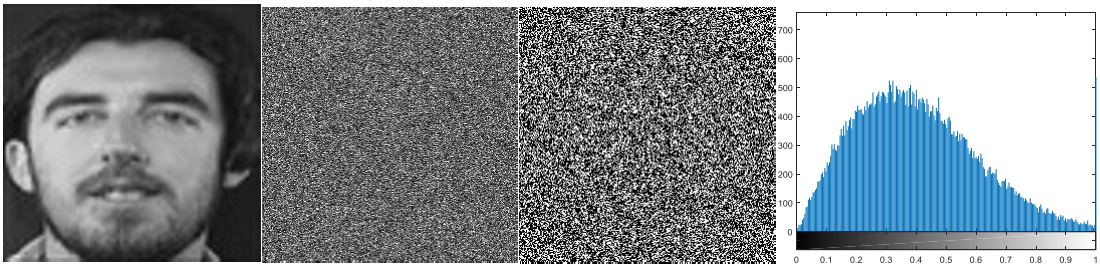
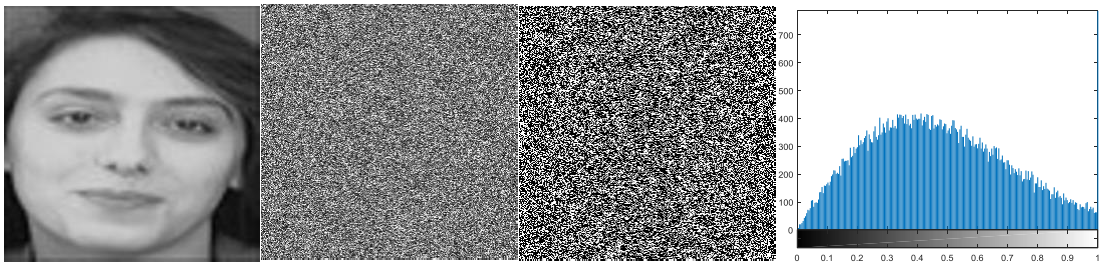


Figure 3.2 : Cryptage d'images par DRPE



(a)



(b)

Figure 3.3 : Processus de cryptage d'images par DRPE-Image originale-Phase de l'image cryptée-Histogramme de l'image cryptée.

3.2.2 Décomposition en valeurs singulières (SVD)

En mathématiques, le procédé d'algèbre linéaire de décomposition en valeurs singulières (ou SVD, de l'anglais singular value decomposition) d'une matrice est un outil important de factorisation des matrices rectangulaires réelles ou complexes. Ses applications s'étendent du traitement du signal aux statistiques, en passant par la météorologie. Le théorème spectral énonce qu'une matrice normale peut être diagonalisée par une base orthonormée de vecteurs propres. On peut voir la décomposition en valeurs singulières comme une généralisation du théorème spectral à des matrices arbitraires, qui ne sont pas nécessairement carrées.

Soit M une matrice $m \times n$ dont les coefficients appartiennent au corps K, où $K = \mathbb{R}$ ou $K = \mathbb{C}$. Alors il existe une factorisation de la forme

avec U une matrice unitaire $m \times m$ sur K, Σ une matrice $m \times n$ dont les coefficients diagonaux sont des réels positifs ou nuls et tous les autres sont nuls, et $V*$ est la matrice adjointe à V, matrice unitaire $n \times n$ sur K. On appelle cette factorisation la décomposition en valeurs singulières de M.

- La matrice V contient un ensemble de vecteurs de base orthonormés de Kn, dits « d'entrée » ou « d'analyse » ;
- La matrice U contient un ensemble de vecteurs de base orthonormés de Km, dits « de sortie » ;
- La matrice Σ contient dans ses coefficients diagonaux les valeurs singulières de la matrice M, elles correspondent aux racines des valeurs propres de .
- Une convention courante est de ranger les valeurs $\Sigma i, i$ par ordre décroissant. Alors, la matrice Σ est déterminée de façon unique par M (mais U et V ne le sont pas) [28].

Exemple : Soit la matrice a =

224	24	120	48
52	181	206	227
255	38	23	43
206	218	83	4

La décomposition de la matrice a en valeurs singulières est donnée ci-dessous

u =				s =				v =			
-0.4530	0.2942	-0.4967	-0.6794	514.3866	0	0	0	-0.6837	0.7015	-0.1738	0.1008
-0.5592	-0.7924	-0.1815	0.1624	0	270.3011	0	0	-0.4828	-0.2915	0.8115	0.1530
-0.4216	0.5044	-0.2757	0.7012	0	0	147.5562	0	-0.4375	-0.3763	-0.2488	-0.7779
-0.5516	0.1761	0.8027	-0.1428	0	0	0	56.2927	-0.3286	-0.5304	-0.4994	0.6011

Tableau 3.1 : La décomposition de la matrice a en valeurs singulières.

Si nous voulons récupérer la matrice a, nous procédons comme suit :

a = u.s.v'=

224.0000	24.0000	120.0000	48.0000
52.0000	181.0000	206.0000	227.0000
255.0000	38.0000	23.0000	43.0000
206.0000	218.0000	83.0000	4.0000

3.2.3 Carte chaotique de Baker

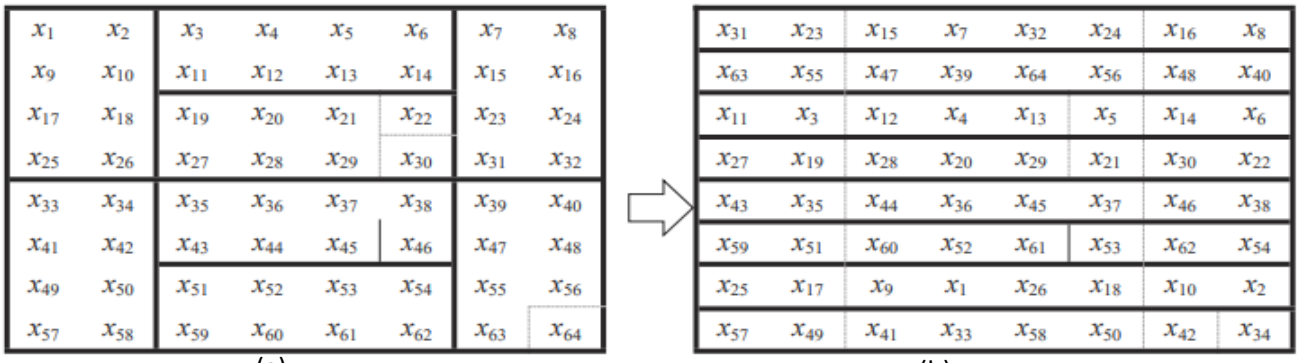


Figure 3.4 : Processus de permutation par la carte de Baker chaotique d'une matrice 8×8

La permutation par la carte chaotique de Baker consiste à découper une image en des blocks de 8×8 selon le modèle de la Figure 3.4 (a), puis transformer ces blocks en des lignes de 8 éléments comme illustré dans la Figure 3.4 (b).

3.3 Procédure d'enrôlement

La procédure d'enrôlement passe par les étapes suivantes :

1. Soit I la matrice empreinte digitale de dimensions $\times N$.
2. La matrice I est décomposée par le biais de la fonction SVD en trois composantes différentes.

$$SVD(I) = USV^T \tag{3.1}$$

3. L'image de visage cryptée (F_{en}) est additionnée à la matrice S.

$$L = S + F_{en} \tag{3.2}$$

4. La matice (L) obtenue à son tour est aussi décomposée utilisant la SVD.

$$SVD(L) = U_L S_L V_L^T \tag{3.3}$$

5. Utilisant la matrice S_L, la matrice I_m tatouée est obtenue selon la formule suivante :

$$I_m = US_L V^T \tag{3.4}$$

6. Finalement, la matrice $I_m$obtenue est encryptée par le biais de la fonction chaotique Baker map, pour donner la matrice résultante I_r, qui sera stockée dans la base de données biométrique annulable.

3.4 Résultats de simulation obtenus

La simulation est faite dans l'environnement Matlab 2016a et les modalités biométriques utilisés sont pris des bases de données DB1-B [29] pour les empreintes digitales et ORL data base [30] pour les visages respectivement.

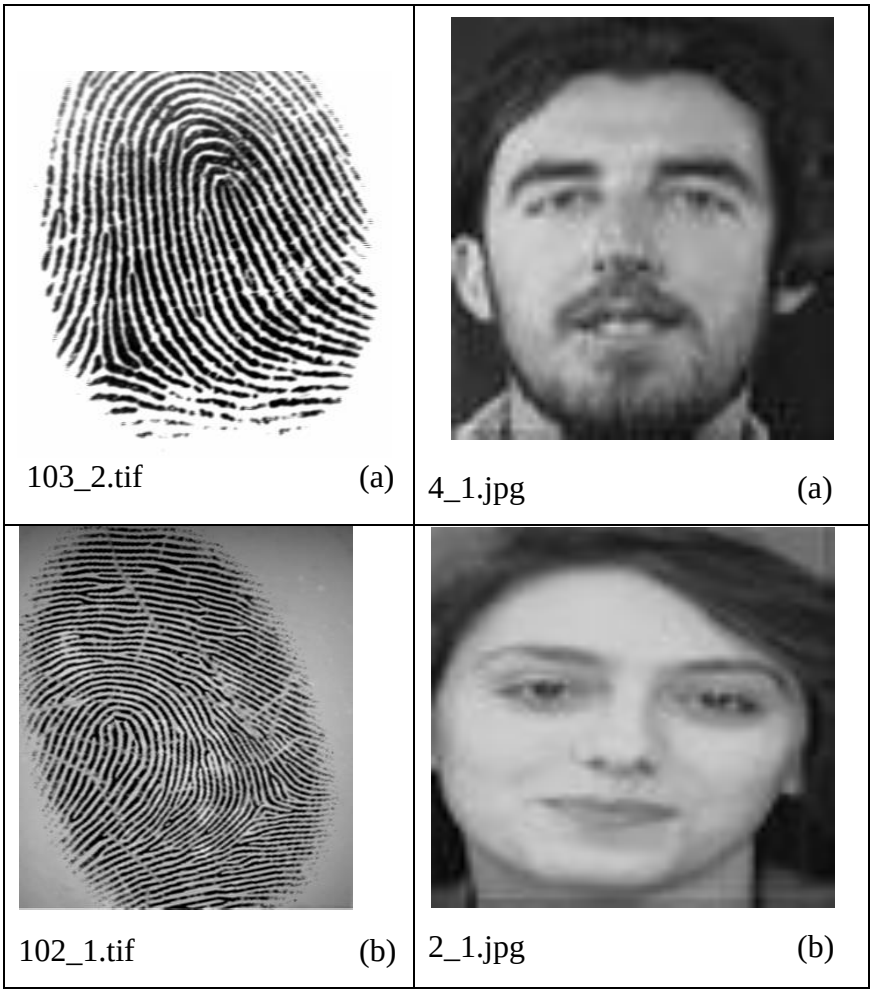


Figure 3.5 : Les deux modalités biométriques (empreinte-visage) utilisées dans la simulation.

Les résultats de simulation de l'algorithme proposé pour les paires (empreinte-visage) c. à. d (103_2.tif-4_1.jpg), (102_1.tif-2_1.jpg) respectivement sont donnés dans la figure ci-dessous :

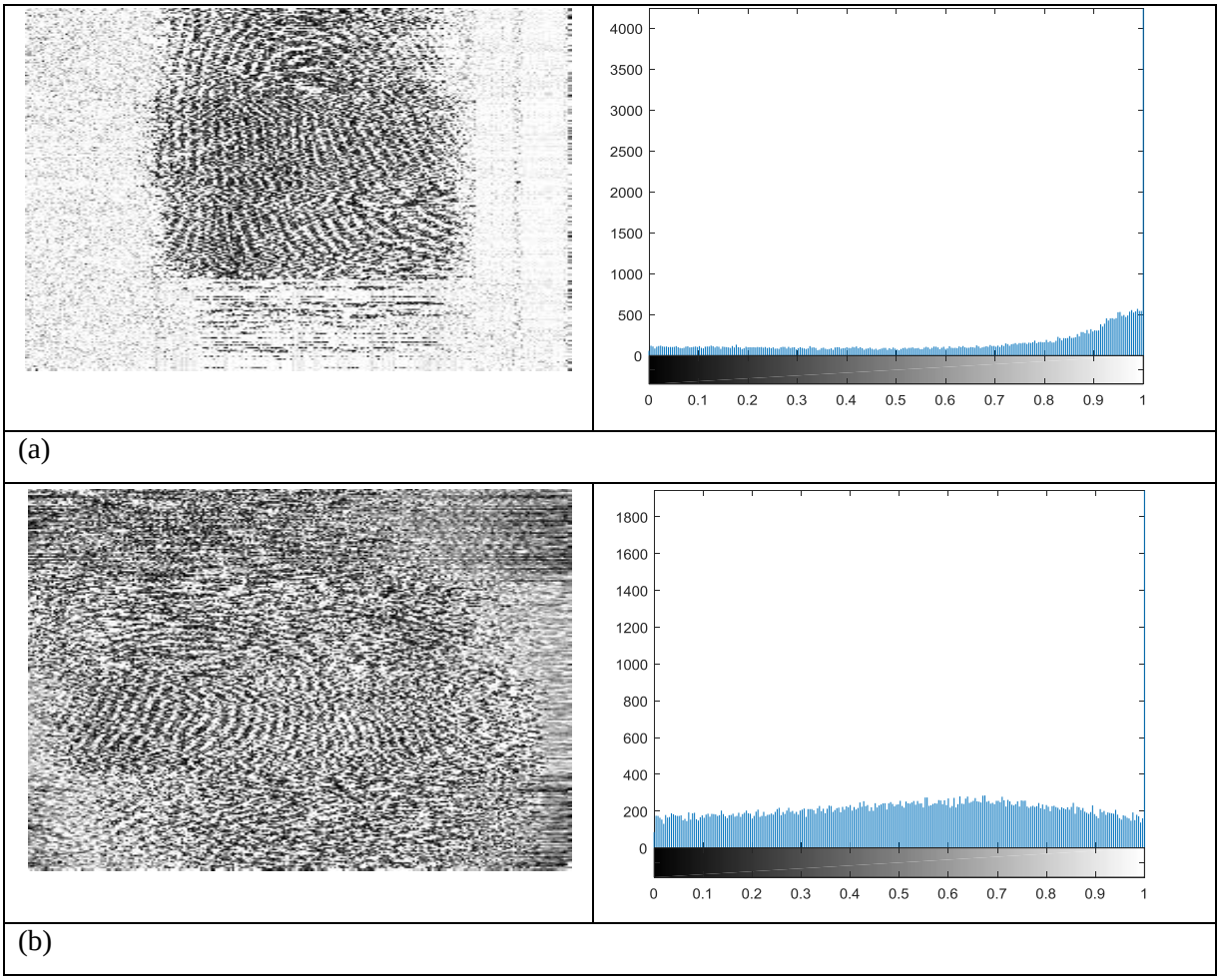


Figure 3.6 : Résultats de simulation (a) de cryptage de la paire (103_2.tif-4_1.jpg), Et (b) cryptage de la paire (102_1.tif-2_1.jpg).

3.5 Procédure de vérification

La procédure vérification consiste à faire passer la modalité multimodale suspecte par le même algorithme, puis le comparer avec la même modalité existant au niveau de la base de données.

La comparaison s'effectue moyennant deux métriques à savoir le taux de corrélation et le SNR (Signal to Noise Ratio).

$$cr = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \tag{3.5}$$

$$SNR = 10\log_{10}\frac{\sum_{i=1}^{Q} V_0^2(i)}{\sum_{i=1}^{Q}(v_0(i) - v_c(i))^2} \tag{3.6}$$

Paire	(103_2.tif-4_1.jpg) avec(103_2.tif-4_1.jpg)	(103_2.tif-4_1.jpg) avec(102_1.tif-2_1.jpg)	(102_1.tif-2_1.jpg) avec(102_1.tif-2_1.jpg)	(102_1.tif-2_1.jpg) avec(103_2.tif-4_1.jpg)
Corrélation	1	0.0022	1	0.0042
SNR (dB)	0	3210.21	0	3215.15

Tableau 3.2 : Résultats de comparaison entre les paires utilisant la corrélation et le SNR

3.6 Conclusion

En conclusion, l'implémentation d'un algorithme de protection d'une base de données biométrique multimodale sous environnement Matlab est un processus possible mais crucial qui nécessite une bonne compréhension des concepts de sécurité informatique et de traitement d'image.

Le développement de cet algorithme implique plusieurs étapes, telles que la collecte de données, le prétraitement des images, l'extraction des caractéristiques, la création d'une base de données, la mise en place d'un système d'authentification (vérification) et la mise en place de mécanismes de sécurité pour protéger la base de données. En somme, les résultats obtenus sont satisfaisants, en effet, lors de la vérification, nous avons effectué une comparaison entre la personne suspecte et son modalité stockée dans la base de données, puis nous décidons s'il est authentique ou non.

Conclusion générale

Conclusion générale

Les bases de données biométriques que ce soit uni-modale ou multimodale ne sont pas à l'abri d'attaques non autorisées. Or, la protection de ces bases de données devient une nécessité absolue. Plusieurs techniques de protection ont vu le jour en littérature. Parmi les techniques utilisées, nous citons entre autres celle constituée d'une transformation et de cryptage. Cette protection est subdivisée en deux phases distinctes, la phase d'enrôlement qui est en quelque sorte la construction de la base de données sécurisée, et la phase de vérification de l'authenticité de la personne en question. C'est dans ce contexte que nous avons implémenté l'algorithme [31], qui consiste à utiliser deux modalités le visage et l'empreinte. Le visage est crypté dans le domaine fréquentiel par le biais de la DRPE, basée essentiellement sur la transformée de Fourier fractionnaire. En revanche l'empreinte est transformée par le biais de la SVD. Les deux résultantes sont additionnées, puis la somme est permutée utilisant la carte de Baker pour donner naissance à la base de données sécurisée. Quant à la phase de vérification, il s'agit de faire passer la paire de modalité (visage-empreinte) suspecte par le même processus d'enrôlement et la comparer avec celle existante dans la base de données. Enfin prendre la décision si la suspecte est authentique ou non.

L'implémentation de cet algorithme est faite sous l'environnement Matlab 2016a, les bases de données sont celle d'ORL pour les visages et DB1 pour les empreintes. Les résultats de simulation sont satisfaisants et ont montré l'efficacité de l'algorithme proposé dans la protection de la base de données construite moyennant les mesures de performance comme le PSNR et le taux de corrélation.

En perspective, nous comptons développer nos propres algorithmes plus performants et plus efficaces.

Référence

References

[1] https://www.researchgate.net/publication/363952162?fbclid=IwAR2DE57TriDyAIZo-F6ZOkErfRrvt3pMfE16Bo2S7RuWWFj6l-iO7jK7Iys

[2] https://www.researchgate.net/publication/336386976?fbclid=IwAR1bNULEArMTVmoVxX1vFAAbGi8t2JXDYtLdT74S2mkAZadm7CYcFWNxZWU

[3] G.salama,S.El – Gazar et all "Cancelable biometric system for IOT applications based on optical double random phase encoding "

[4] Mémoire en vue de l'obtention du diplôme de Master en Informatique Titre :Identication et reconnaissance biométrique par l'utilisation des empreintes palmaires par une approche hiérarchique. Présenté Par Rima Khelif & Asma Saidani Soutenu le /09/2021 Devant le jury composé de : encadreur Dr Abdelouahab Attia Université de BBA ... ... Promotion : 2020/2021

[5] jr. Christopher horn Julius gatune D. John. Woodward and aryn thomas. biometrics a look at facial recognition. 2003.

[6] Memoire Online > Projet de mise en place d'un système de sécurité biométrique basé sur la reconnaissance d'iris embarqué dans un gab. par Benito Lubuma Use of Biometrics for the Regeneration of Revocable Crypto-biometric Keys

Université de Kinshasa - Lincecié en Genié Informatique 2014

[7 Use of Biometrics for the Regeneration of Revocable Crypto-biometric Keys

Par Mohamed Amine Hmani

[8] géométrique de la main http://biometrics.over blog.com/pages/La_geometrie_de_la_main-2019-7-29.html

[9] Identification de personne par fusion de différentes modalités biométriques » H. Guesmi 2014.

[10] "Introduction à la biométrie : Authentification des individus par traitement audio-video", Florent PERRONNIN, Jean-Luc DUGELAY,Institut Eurocom, MultiMedia Communications Department, Revue Traitement du signal, Vol.19, N°4, 2002.

[11] Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris, Nicolas Morizet. 2009.

[12] Identification de personne par fusion de différentes modalités biométriques » H. Guesmi 2014.

[13] "La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance", Melle Lorène ALLANO., 2009.

[14] F. Peronin, J.L. Dugelay: « An introduction to biometrics Audio and Video-Based Person Authentification ». Revue Traitement du Signal, Vol.19, No.04, 2002.

[15] T. Autret, R. Bergeron, M. Collignon, M.A. Couwez, A. Denis, J.C. Gandois, G. Khouberman, M. Lecherc, J.Y. Martin : « Techniques de contrôle d'accès par biométrie ». Dossier Technique de la Commission de Sécurité Physique, Clusif, (France), 2003.

[16] P. Varchol and D. Levicky: «Using of Hand Geometry in Biometric Security Systems ». Radioengineering. Vol.16, No.04, pp.82-87, 2007.

[17] B. Arbab-Zavar and M.S. Nixon: « On Guided Model-Based Analysis for Ear Biometrics ». Computer Vision and Image Understanding (Elsevier). Vol.115, No.04, pp.487- 502, 2011.

[18] I. Benchennane : « Etude et mise au point d'un procédé biométrique multimodale pour La reconnaissance des individus ». Thèse de doctorat, Université d'Oran Mohamed Boudiaf (Algérie), 2016.

[19] T. Hafs : « Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne ». Thèse de doctorat, Université Badji Mokhtar-Annaba (Algérie), 2016.

References

[20] A.K. Jain, A. Ross, S. Prabhakan: « An Introduction to Biometric Recognition ». IEEE Transactions on Circuits and systems for video technology, Vol. 14, No. 1, pp.04-20, Janvier 2004.

[21] S. Chantaf : « Biométrie par signaux physiologiques ». Thèse de doctorat, Université Paris Est Creteil (France). Soutenue le 02/05/2011.

[22] R.D. Seely, M. Goffredo, J.N. Carter, and M.S. Nixon: « View Invariant Gait Recognition ». In M. Tistarelli, S.Z. Li, and R. Chellapa, editors: ‘’Handbook of Remote Biometrics for Surveillance and Security’’. Springer Verlag (Advances in Pattern Recognition Series), London (UK), 2009.

[23] « A system for automated iris recognition », Proc. Of second IEEE Workshop on Applications of Computer Vision, pp. 121-128, R.P. Wilds, December 1994.

[24] «A practical guide to biometric security technology», IEEE Computer society, IT Pro – security. S.Liu, M. Silveman, January - February, 2001.

[25] «Biometrics a Look at Facial Recognition”, documented briefing by RAND Public Safety and Justice for the Virginia State Crime Commission, John D.Woodward, Jr., Christopher Horn, Julius Gatune, and Aryn Thomas, 2003.

[26] “Introduction à la biométrie : Authentification des individus par traitement audio-video”, Florent PERRONNIN, Jean-Luc DUGELAY,Institut Eurocom, MultiMedia Communications Department, Revue Traitement du signal, Vol.19, N°4, 2002.

[27] "Biométrie pour l’Identification", Rapport final, Institut de la Francophonie pour l'Informatique, DANG Hoang, Hanoï, Vietnam, 07 – 2005.

[28] Décomposition en valeurs singulières — Wikipédia (wikipedia.org)

[29] https://paperswithcode.com/dataset/orl

[30] http://www.comp.polyu.edu.hk/~csajaykr/myhome/data
base_request/ContactlessFP/

[31] G. M. Salama, S. E. Gazar, and Al, “Cancelable biometric system for IoT applications based on optical double random phase encoding,”Optics Express, Vol. 30, No. 21 , 37816, 10 Oct 2022.

[32] Thèse de doctorat en Informatique et réseaux
Soutenue le 01-02-2011
à Evry, Institut national des télécommunications , dans le cadre de École doctorale Informatique, télécommunications et électronique de Paris , en partenariat avec Université Pierre et Marie Curie (Paris ; 1971-2017) (Université) .

[33] : IEEE, pp 5232–5235 Ahmad T, Hu J (2010) Génération de modèles biométriques annulables à l'aide d'une ligne de projection. Dans : 11e International

[34] https://fr.wikipedia.org/wiki/Office_qu%C3%A9b%C3%A9cois_de_la_langue_fran%C3%A7aise

[35] Kaur H, Khanna P (2016) Protection des modèles biométriques à l'aide de la biométrie annulable et de la cryptographie visuelle Kim Y

[36] Conférence internationale sur la reconnaissance des formes (ICPR), vol 24. IEEE, pp 3108–3113 Kim Y,

[37] dey N, Nandi B, Dey M, Biswas D, Das A, Chaudhuri SS (2013) Génération de code BioHash à partir des caractéristiques de l'électrocardiogramme. Dans: Advance computing conference (IACC), vol 3.

[38] https://www.bing.com/search?q=le+chiffre+de+Hill&cvid=bc2b06e0343a4d80bfc6c92233021268&aqs=edge.69i57.1219j0j1&FORM=ANAB01&PC=EDGEDSE#:~:text=https%3A//fr.wikipedia.org/wiki/Chiffre_de_Hill

[39] (2017b) Cryptage biométrique non inversible pour générer des modèles biométriques annulables

References

Actes du Congrès mondial sur l'ingénierie et l'informatique, vol 1, pp 1–4 Kaur H, Khanna P (2019) Méthode de distance aléatoire pour générer des caractéristiques biométriques annulables unimodales et multimodales. IEEE Trans Inf Forensics Secur 14(3):709–719 Kelkboom EJ, Zhou X, Breebaart J, Veldhuis RN, Busch C (2009) Fusion

[40] Wang S, Hu J (2013) Une méthode basée sur la transformation Hadamard pour la conception de modèles d'empreintes digitales annulables. Yang K, Du Y, Zhou Z, Belcher C (2010) Méthode de reconnaissance de l'iris annulable basée sur le descripteur de Gabor. Dans : IEEE In : Congrès international sur le traitement des images et du signal (CISP), vol 3(no 6).

[41] im H, Nguyen MP, Chun SY (2017) Biométrie ECG annulable à l'aide de GLRT et amélioration des performances à l'aide d'un filtre guidé avec signal de guidage irréversible. Dans : Conférence internationale annuelle de la société d'ingénierie en médecine et biologie (EMBC), vol 39. IEEE, pp 454–457 Kong A, Cheung KH, Zhang D, Kamel M, You J

[42] Kaur H, Khanna P (2017a) Fonctionnalités annulables utilisant des filtres log-Gabor pour l'authentification biométrique. Multimed Tools Appl 76(4) :4673–4694 Kaur H, Khanna P

[43] Ghany KK, Hefny HA, Hassanien AE, Ghali NI (2012) Une approche hybride pour la sécurité des modèles biométriques. Dans : Actes de la conférence internationale 2012 sur les avancées dans l'analyse et l'exploration des réseaux sociaux (ASONAM 2012)

[44] Système d'authentification d'utilisateur biométrique multimodal annulable avec coffre flou. Dans : Conférence internationale sur la communication par ordinateur et l'informatique (ICCCI)

[45] Génération de modèles d'empreintes palmaires annulables à l'aide d'un modèle binaire local et d'une projection aléatoire. Dans : Conférence internationale sur la technologie signal-image et les systèmes basés sur Internet (SITIS), vol 13. IEEE, pp 203–209

[46] Issac CM, Kanaga EG (2017) Sondage sur les algorithmes de classification et les caractéristiques des signaux cérébraux adaptés à l'authentification biométrique annulable. Dans : Conférence internationale IEEE sur l'intelligence computationnelle et la recherche informatique (ICCIC).

[47] Bringer J, Chabanne H, Kindarji B (2009) Identification anonyme avec biométrie annulable. Dans : Actes du symposium international sur le traitement et l'analyse d'images et de signaux, vol 6. IEEE, pp 494–499 Bringer J, Chabanne H, Morel C (2014) Le mélange n'est pas suffisant : analyse de sécurité des codes d'iris annulables basés sur un secret permutation. Dans : Conférence conjointe internationale sur la biométrie (IJCB). IEEE, pp 1–8 Camenisch J, Stadler M (1997) Schémas de signature de groupe efficaces pour les grands groupes.

[48] IEEE, pp 1–4 Izu T, Sakemi Y, Takenaka M, Torii N (2014) Une attaque par usurpation contre un schéma d'authentification biométrique annulable. Dans : Conférence internationale sur les réseaux d'information avancés et les applications (AINA), vol 28. IEEE, pp 234–239

[49] H, Khanna P (2019) Méthode de distance aléatoire pour générer des caractéristiques biométriques annulables unimodales et multimodales. IEEE Trans Inf Forensics Secur 14(3):709–719 Kelkboom EJ, Zhou X, Breebaart J, Veldhuis RN, Busch C (2009) Fusion

[50] a été créée à l'université Carnegie Mellon (CMU)

[22] Ali MA, Tahir NM (2018) Technique biométrique annulable pour la reconnaissance de l'iris. Dans : Symposium IEEE sur les applications informatiques et l'électronique industrielle (ISCAIE). IEEE, pp 434–437 Andalib AS, Abdulla-Al-Shami

References

[51] M (2013) Un nouveau schéma de génération de clé pour les cryptosystèmes biométriques utilisant des minuties d'empreintes digitales. Dans : 2e Conférence internationale sur l'informatique, l'électronique et la vision (ICIEV).

[52] :Choudhury B, Then P, Raman V, Issac B, Haldar MK (2016) Biométrie de l'iris annulable basée sur des schémas de masquage de données. Dans : Conférence étudiante IEEE sur la recherche et le développement (SCOReD). IEEE, pages 1 à 6

[53] : Lee C, Choi JY, Toh KA, Lee S, Kim J (2007) Modèles d'empreintes digitales annulables sans alignement basés sur des Lumini A, Nanni L (2007) Un biohachage amélioré pour l'authentification humaine. Motif reconnu 40(3):1057– Patel VM, Ratha NK, Chellappa R (2015) Biométrie annulable :

Un examen. Signal IEEE ProcessMag 32(5) :54– informations minutieuses. IEEE Trans Syst Man Cybern B Cybern 37(4):980–992

[54] : Leng L, Zhang JS, Khan MK, Bi X, Ji M (2010) Palmcode annulable généré à partir de filtres Gabor aléatoires pour la protection des empreintes palmaires. Dans : International conference of image and vision computing New Zealand, vol 25. IEEE, pp 1–6

[55] : Maiorana E, Campisi P, Ortega-Garcia J, Neri A (2008) Biométrie annulable pour la reconnaissance de signature basée sur HMM. Dans : Conférence internationale sur la biométrie : théorie, applications et systèmes, vol 2. IEEE, pp 1–6

Résumé

Résumé

La biométrie est une technologie utilisée pour mesurer et analyser les caractéristiques physiques ou comportementales uniques d'un individu, afin de l'identifier de manière fiable. Les bases de données biométriques multimodales stockent les informations biométriques provenant de différentes modalités, comme les empreintes digitales et les traits du visage, pour augmenter la fiabilité et l'exactitude de l'identification biométrique. La protection de telles bases de données est cruciale pour prévenir l'accès non autorisé et les abus potentiels des données biométriques sensibles. Pour protéger les bases de données biométriques multimodales, plusieurs mesures de sécurité peuvent être mises en place. Tout d'abord, l'accès physique et logique à la base de données doit être restreint et contrôlé. Ensuite, des techniques de cryptage doivent être utilisées pour sécuriser les données biométriques stockées. Le cryptage garantit que les informations biométriques ne peuvent être lues ou comprises que par des personnes autorisées possédant la clé de déchiffrement appropriée. L'implémentation d'un algorithme de protection d'une base de données biométrique multimodale dépendra des spécificités de l'environnement DRPE (Développement Rapide de Produit Electronique) et la SVD est une technique de décomposition matricielle qui permet de réduire la dimensionnalité des données, d'extraire les caractéristiques principales et d'effectuer diverses opérations mathématiques sur les matrices. En outre, L'algorithme de protection devrait inclure des techniques de cryptage solides pour protéger les données biométriques stockées dans cryptage.

Mots clés : Biométrie multimodale, DRPE, SVD, Cryptage, La protection de telles bases de données.

ملخص

القياسات الحيوية هي تقنية تُستخدم لقياس وتحليل الخصائص الطبيعية أو السلوكية الفريدة للفرد ، من أجل التعرف عليها بشكل موثوق. تخزن قواعد البيانات البيومترية متعددة الوسائط معلومات القياسات الحيوية من طرائق مختلفة ، مثل بصمات الأصابع وميزات الوجه ، لزيادة موثوقية ودقة التعرف على القياسات الحيوية. تعد حماية قواعد البيانات هذه أمرًا بالغ الأهمية لمنع الوصول غير المصرح به وإساءة الاستخدام المحتملة لبيانات القياسات الحيوية الحساسة. لحماية قواعد البيانات البيومترية متعددة الوسائط ، يمكن تنفيذ العديد من التدابير الأمنية. أولاً ، يجب تقييد الوصول المادي والمنطقي إلى قاعدة البيانات والتحكم فيه. بعد ذلك ، يجب استخدام تقنيات التشفير لتأمين البيانات الحيوية المخزنة. يضمن التشفير أن المعلومات البيومترية لا يمكن قراءتها أو فهمها إلا من قبل الأشخاص المصرح لهم باستخدام مفتاح فك التشفير المناسب. يعتمد تنفيذ خوارزمية الحماية لقاعدة بيانات المقاييس الحيوية متعددة الوسائط على مواصفات بيئة(تطوير المنتجات الإلكترونية السريعة) اما تقنية تحلل المصفوفة فهي تجعل من الممكن تقليل أبعاد البيانات و استخراج الميزات الرئيسية و إجراء عمليات حسابية مختلفة على المصفوفات.
. يجب أن تتضمن خوارزمية الحماية تقنيات تشفير قوية لحماية بيانات القياسات الحيوية المخزنة في قاعدة البيانات

. البيانات البيومترية متعددة الوسائط ,تطوير المنتجات الإلكترونية السريعة , القياسات الحيوية: **كلمات البحث**

ABSTRACT

Biometrics is a technique used to measure and analyze the unique natural or behavioral characteristics of an individual, in order to reliably identify them. Multimedia biometric databases store biometric information from various modalities, such as fingerprints and facial features, to increase the reliability and accuracy of biometric identification. Protecting these databases is critical to prevent unauthorized access and potential misuse of sensitive biometric data. To protect multimedia biometric databases, several security measures can be implemented. First, physical and logical access to the database must be restricted and controlled. Then, encryption techniques must be used to secure the stored vital data. Encryption ensures that biometric information can only be read or understood by persons authorized to use the appropriate decryption key. The implementation of the protection algorithm for the multimedia biometric database will be based on the specification of the DRPE (Rapid Electronic Product Development) environment. SVD is a matrix decomposition technique that makes it possible to reduce the dimensions of data, extract key features and perform various calculations on matrices. In addition. The protection algorithm must include strong encryption techniques to protect the biometric data stored in the database.

Key words : Multimodal Biometrics, SVD, DRPE, protect multimedia biometric databases.