République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohamed Seddik Benyahia de Jijel
Faculté des Sciences Exactes et informatique
Département d'Informatique

Mémoire de fin d'étude

pour l'obtention du diplôme Master de Recherche en Informatique

Option : ***Informatique Légale et Multimédia***

Thème

Cryptosystème biométrique pour la protection du template d'empreinte digitale

Présentés par :
MERICHE Madina.
BOUNAR Salah.

Encadré par :
Melle.BIROUK Wafa

Promotion : 2020.

Résumé

Les cryptosystèmes biométriques représentent les technologies émergentes de protection des modèles biométriques améliorant l'acceptation de biométrie. Les systèmes d'authentification d'empreintes digitales enregistrent généralement les données extraites de l'empreinte digitale en tant que modèle de minutie dans la base de données. Ainsi, si les points de minutie d'un utilisateur sont divulgués, l'empreinte digitale peut être générée à partir d'eux. Par conséquent, la sécurisation des informations extraites de l'empreinte digitale est nécessaire.
Ce travail vise à la construction d'un cryptosystème biométrique qui utilise les informations de localisation des points de minutie (minuties voisines) pour protéger le template d'empreinte digital sauvegardé dans la base de données.
Mots clés : biométrie, clé, cryptosystèmes biométriques, protection du template biométriques.

Abstract

Biometric cryptosystems represent emerging technologies for the protection of biometric models improving the acceptance of biometrics. Fingerprint authentication systems usually save the data extracted from the fingerprint as a thoroughness template in the database. Thus, if a user's minutiae points are disclosed, the fingerprint can be generated from them. Therefore, securing the information extracted from the fingerprint is necessary.
This work aims at the construction of a biometric cryptosystem which uses the location information of the minutiae points (neighboring minutiae) to protect the digital empriente template saved in the database.
Keywords : biometrics, key, biometric cryptosystems, biometric template protection.

Table des matières

Table des matières **1**

Liste des tableaux **4**

Table des figures **6**

Liste des abréviations **7**

Introduction générale **8**

1 La biométrie et Les empreintes digitales **10**

1.1 Introduction 10

1.2 Biométrie 10

1.2.1 Définition de la biométrie 10

1.2.2 Système biométrique et leur mode de fonctionnement 10

1.2.2.1 Mode d'enrôlement 11

1.2.2.2 Mode de vérification 11

1.2.2.3 Mode d'identification 12

1.2.3 Modalités biométriques 13

1.2.3.1 Modalités morphologiques 13

1.2.3.2 Modalités biologiques 13

1.2.3.3 Modalités comportementales 14

1.2.4 Architecture d'un système biométrique 15

1.2.4.1 Module de capture : 15

1.2.4.2 Module de traitement du signal : 15

1.2.4.3 Module du stockage : 15

1.2.4.4 Module de similarité : 15

1.2.4.5 Module de décision : 16

1.2.5 Performance d'un système biométrique : 16

1.2.6 Applications d'un système biométrique 18

1.3 Reconnaissance des empreintes digitales : 19

1.3.1 Empreinte digitale : 19

1.3.2 Caractéristiques d'une empreinte digitale : 19

1.3.2.1 Représentation globale 20
1.3.2.2 Représentation locale 21
1.3.3 Structure d'un système de reconnaissance d'empreintes digitales : . . 22
1.3.3.1 L'acquisition de l'image d'empreinte 22
1.3.3.2 Pré-traitement 23
1.3.3.3 Extraction des caractéristiques 23
1.3.3.4 Post-traitement 28
1.3.4 Comparaison des empreintes digitales 31
1.3.4.1 Approches basées sur la corrélation 31
1.3.4.2 Approches basées sur les crêtes 32
1.3.4.3 Approches basées sur les minuties 32
1.4 Conclusion 32

2 Cryptosystémes biométriques 33
2.1 Introduction 33
2.2 Cryptosystème biométrique 33
2.2.1 Protection du modèle biométrique 33
2.2.2 Classification des cryptosystèmes biométriques 33
2.2.2.1 Cryptosystèmes biométriques de liaison de clés 34
2.2.2.2 Cryptosystèmes biométriques de génération de clés 34
2.2.3 les méthodes de cryptosystéme biométrique 35
2.2.3.1 Fuzzy commitment 35
2.2.3.2 Fuzz vault 36
2.2.3.3 Schémas de Quantization 37
2.2.3.4 Méthode cryptosystème biométrique basé sur les minuties voisinages 38
2.2.4 Avantage des cryptosystèmes biométriques 38
2.3 Méthode de cryptosystème biométrique basé sur les minuties voisinages . . . 39
2.3.1 Prétraitement 40
2.3.2 Extraction de points des minuties 41
2.3.3 Génération de modèles sécurisés(gabarit) 41
2.3.4 Comparaison 45
2.4 Conclusion 46

3 Tests et résultats expérimentaux 47
3.1 Introduction 47
3.2 Environnement de développement 47
3.2.1 Matériel 47
3.2.2 Software 47
3.3 Présentation de l'application 49

3.3.1 Base de donnée utilisée 49
3.3.2 Les attaques acceptables utilisés 50
3.3.3 Interface graphique 51
3.4 Tests et évaluations 56
3.4.1 Evaluation des performances 56
3.4.2 Sécurité 59
3.5 Conclusion 60

Conclusion générale **61**

Bibliographie **62**

Liste des tableaux

3.1 Caractéristiques des machines utilisés 47
3.2 Paramètre utilisé pour chaque manipulation 50
3.3 La moyenne de similarité pour chaque paramètre de Rotation 56
3.4 La moyenne de similarité pour chaque paramètre de Shearing 56
3.5 La moyenne de similarité pour chaque paramètre de Compression 57
3.6 La moyenne de similarité pour chaque paramètre de Bruit Gaussien 57
3.7 La moyenne de similarité pour chaque paramètre de Scaling 57
3.8 La moyenne générale de la mesure de similarité pour chaque attaque. 58
3.9 Les résultats de P_{TPR} et P_{FPR} par rapport au différents seuils 60

Table des figures

1.1 Enrôlement dans un système biométrique. 11
1.2 Authentification d'un individu dans un système biométrique. 12
1.3 Identification d'un individu dans un système biométrique. 12
1.4 Différentes modalités biométriques 14
1.5 Part de marché comparatif par technologie biométrie 15
1.6 Architecture complète d'un système biométrique. 16
1.7 Illustration du FRR et du FAR 17
1.8 Courbes DET. 18
1.9 Quelques applications de la biométrie. 19
1.10 Les vallées (valleys) et les crêtes (ridges) sur une empreinte. 19
1.11 Caractéristiques d'une empreinte digitale. 20
1.12 Les principales classes d'empreintes digitales selon la classification de Galton-Henry 21
1.13 Représentation des vecteurs de terminaison et de bifurcation. 21
1.14 Architecture générale d'un système complet de reconnaissance d'empreintes. 22
1.15 Principe du pré-traitement de l'image. 23
1.16 La phase d'extraction de la signature 24
1.17 Le champ d'orientation d'une image d'empreinte digitale 24
1.18 Résultats de de binarisation 26
1.19 Résultats de de squelettisation 27
1.20 Les différentes représentations du squelette. 28
1.21 Exemples de détermination du type de minutie en fonction du calcul de CN. 28
1.22 Exemples de détermination du type de minutie en fonction du calcul de CN. 29
1.23 Validation des terminaison détéctes : vrai terminaison(a), branche parasite(b), segment trop court(c) 29
1.24 Définitions associée a une bifurcation lors de la phase de validation. 30
1.25 Résultat de la phase d'élimination des fausses minuties. 31
1.26 Les différentes positions de même doigt. 31

2.1 Mode de fonctionnement général d'un schéma de liaison de clé 34
2.2 mode de fonctionnement général d'un schéma de génération de clé 35
2.3 Schéma de fuzzy commitment. 36

2.4 Schéma de fuzzy vault. 37
2.5 Schéma de Quantization proposée. 38
2.6 Datagrame des étapes de la technique proposée. 40
2.7 Le résultat obtenu après le pré-traitement. 41
2.8 Résultat de l'extraction de points des minuties. 41
2.9 Algorithme 1 : Calcul du modèle utilisateur sécurisé 42
2.10 Génération d'un emplacement modifié m_i avec m_j le plus proche à l'aide des touches utilisateur p_0 et q_0. 43
2.11 les emplacements modifiés pour les points de minutie d'un empreinte digitale. 43
2.12 les emplacements modifiés pour les points de minutie d'un empreinte digitale. 44
2.13 Calcul de la clé s_0 de 48 bits en utilisant p_0, q_0 et r_0. 45

3.1 Logo Python 48
3.2 Une partie de la base de données utilisée 50
3.3 La représentation de page d'accueil 51
3.4 La représentation de la page principale 52
3.5 La barre de menus de la page principale 52
3.6 Fenêtre pour l'evaluation des performances 53
3.7 Fenêtre pour l'evaluation des performances (Taux) 53
3.8 Résultat de l'evaluation des performances 54
3.9 le résultat obtenu de la la partie d'image originale et la partie d'image attaquée. 55
3.10 Les résultats sauvegardés 55
3.11 Évaluation de performance par les différentes attaques. 59
3.12 Évaluation de TPR et FPR par rapport aux différentes seuils. 60

Liste des abréviations

PIN Personal Identification Number

ADN Acide désoxyribo Nucléique

TFR Taux Faux Rejet

FRR False Reject Rate

FR False Reject

TFA Taux Fausse Acceptation

FAR False Accepte Rate

FA False Accepte

TEE Taux Erreur Egal

GAR Genuine Accept Rate

TPR True Positive Rate

FPR False Positive Rate

JPEG Joint Photographic Experts Group

Introduction générale

Dans le monde automatisé actuel, les résultats de diverses avancées technologiques ont rendu la vie humaine très confortable. Grâce à ces progrès, l'authentification humaine est également devenu automatisée de nos jours. Par conséquent, le rôle joué par le système d'authentification automatisé est extrêmement important. L'informatisation du système d'authentification a fait de la sécurité un souci, dans le cas où un imposteur est authentifié par l'authentification système, cela peut entraîner d'énormes pertes et il devient difficile de suivre le défaillant.

Les systèmes d'authentification automatisés traditionnels sont basé sur des jetons (cartes d'identité ou nom d'utilisateur) et quelques connaissances (par exemple, mot de passe) connu uniquement de l'utilisateur. Ces techniques sont devenus très populaires ; cependant, il existe divers obstacles et limitations, par exemple, le mot de passe d'un utilisateur peut être ignoré, spéculé ou volé, de plus, les jetons d'un utilisateur peuvent être partagé, perdu ou volé. Si un imposteur a les informations d'identification d'un utilisateur ou si un utilisateur a partagé ses informations d'identification avec quelqu'un, alors dans ce cas, le système d'authentification traditionnel ne peut pas différencier qu'il s'agit d'un utilisateur authentique ou de quelqu'un d'autre. Ces inconvénients sont pris en compte en utilisant un système d'authentification qui repose sur la biométrie.

La biométrie est la science de établir l'identité de la personne en fonction d'attributs physiques ou comportementaux tels que l'empreinte digitale, le visage, la veine, l'oreille et iris, etc. Les systèmes biométriques sont basés sur le principe que les attributs physiques et comportementaux peuvent être uniques associé à un individu. La cryptographie vise à garantir le secret et l'authenticité du message. La clé cryptographique utilisée pour sécuriser les informations pendant le cryptage et le décryptage sera généralement longue et très difficile à retenir. La protection de la confidentialité de cette clé est une préoccupation majeure. Cela peut être résolu efficacement par les cryptosystèmes biométriques. Ce dernier combinent la biométrie et la cryptographie pour bénéficier de points forts des deux domaines. Dans de tels systèmes, alors que la cryptographie offre des niveaux de sécurité élevés, la biométrie apporte la non-répudiation et élimine le besoin de se souvenir des mots de passe ou de porter des jetons. Au lieu de stocker des données cryptographiques, les clés seront générées dynamiquement à l'aide de la biométrie pour sécuriser le modèle et le système biométrique.

Les systèmes d'authentification biométrique basés sur les empreintes digitales stockent

généralement les données de caractéristiques biométriques d'un utilisateur directement comme modèle de minuties, cependant, il est observé à travers diverses études qu'en utilisant les données des points de minutie, la reconstruction de l'empreinte d'origine est possible. L'empreinte digitale d'un humain est liée en permanence à son corps qui ne peut pas être changé, donc si une empreinte digitale d'un humain est compromis, alors, dans ce cas, ce sera un dommage permanent. Par conséquent, il est nécessaire de sécuriser les fonctionnalités d'empreinte digitale d'un utilisateur. Différentes méthodes présentées pour la protection des données biométriques d'un utilisateur Parmi ces méthodes on trouve les cryptosystèmes biométriques. Soit une clé numérique est solidement liée aux données biométriques d'un utilisateur ou elle est générée en utilisant les données biométriques d'un utilisateur.
Dans ce mémoire, nous présentons un cryptosystème biométrique qui utilise les informations de localisation des points de minutie pour construire un modèle hautement sécurisé pour un utilisateur. Pour chaque point de minutie, un emplacement modifié sécurisé est généré en utilisant les informations de ses minuties voisines et un jeu de clés. Dans ce contexte, ce manuscrit est composé de trois chapitres encadrés par une introduction générale et une conclusion générale. :

- ✓ **Le premier chapitre** en introduisant la notion de la biométrie et les applications qui en découlent. Nous insistons plus particulièrement sur l'utilisation des empreintes digitales, où nous détaillons les différentes étapes qui composent son système complet de reconnaissance.

- ✓ **Le deuxième chapitre** est consacré à introduire le concept des cryptosystèmes biométriques, leur classifications et leurs différentes méthodes,ensuite nous détaillons les différents principes et étapes de la méthode proposée, qui utilise les informations de localisation des points de minuties pour construire un modèle hautement sécurisé.

- ✓ **Le troisième chapitre** est consacré essentiellement à la présentation de différentes interfaces de l'application réalisée, ainsi que les résultats des tests effectués sur cette application.

Enfin, nous terminons par une conclusion dans laquelle nous dressons un bilan et une synthèse du travail effectué, et nous discutons un ensemble de perspectives qui peuvent être considérées comme des directions de recherche future.

Chapitre 1

La biométrie et Les empreintes digitales

1.1 Introduction

La biométrie est une technique naissante qui nous permet de vérifier l'identité d'un individu en employant un ou plusieurs de ses caractéristiques personnelles. Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance des personnes dans un grand nombre d'applications diverses.
Dans ce chapitre nous commençons par présenter la biométrie de manière générale ainsi que les diverses applications qui en découlent, en focalisant plus particulièrement sur l'utilisation des empreintes digitales, ou nous détaillons les différentes étapes qui composent son système complet de reconnaissance.

1.2 Biométrie

1.2.1 Définition de la biométrie

Le terme de biométrie est originaire d'une contraction des deux anciens termes grecs : « bios » qui signifie : la vie « métrique » qui se traduit par : mesure.C'est-à-dire « mesure du vivant ». La biométrie consiste à vérifier ou déterminer l'identité d'un individu à partir de ses caractéristiques biologiques (comme l'ADN), comportementales (comme la voix) ou morphologiques (comme l'empreinte digitale).

Les techniques biométriques permettent la mesure et la reconnaissance de ce que l'on est, à la différence d'autres techniques de même finalités, mais permettant de mesurer ou vérifier ce que l'on possède (cadre, badge, document..) ou ce que l'on sait (mot de passe, code pin..)[1].

1.2.2 Système biométrique et leur mode de fonctionnement

Un système biométrique est un système de reconnaissance des formes qui procède en premier par l'acquisition des données biométriques de l'individu à reconnaître, puis extrait des caractéristiques à partir de celles ci, enfin il compare ces caractéristiques avec les modèles de la

base de données. Selon le contexte de l'application, un système biométrique peut fonctionner soit en mode d'enrôlement, de vérification ou d'identification[2].

1.2.2.1 Mode d'enrôlement

L'enrôlement est la première phase de tout système biométrique. Il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois. Pendant l'enrôlement, la caractéristique biométrique est mesurée en utilisant un capteur biométrique afin d'extraire une représentation numérique[3]. Cette représentation est ensuite réduite, en utilisant un algorithme d'extraction bien défini, afin de réduire la quantité de données à stocker pour ainsi faciliter la vérification et l'identification. le modèle biométrique retenu, est stocké dans une base de données centrale.(voir **la figure 1.1**)

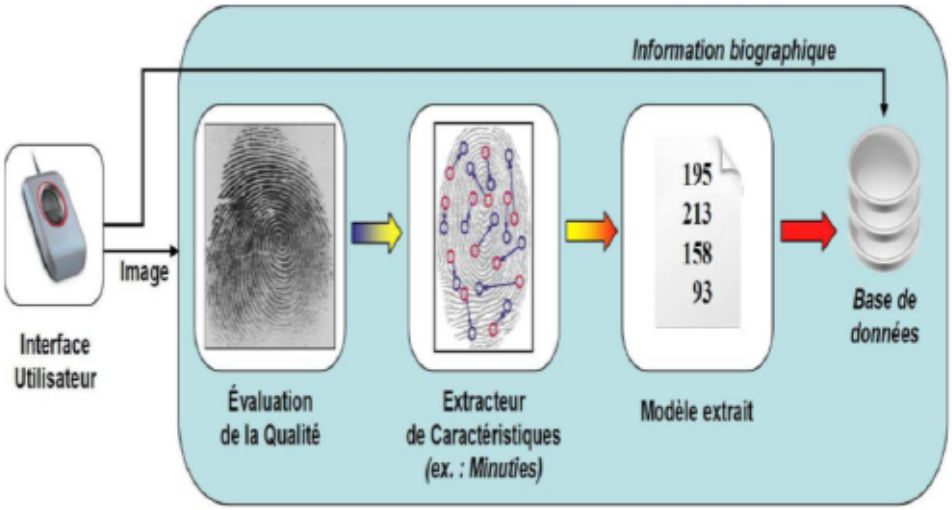


FIGURE 1.1 – Enrôlement dans un système biométrique.

1.2.2.2 Mode de vérification

Le système vérifie l'identité d'une personne en comparant les données biométriques acquises avec celles stockées dans la base de données. Dans un tel système, la personne revendique une identité, généralement via un code PIN (Personal Identification Number), un nom d'utilisateur, une carte à puce,etc. le système effectue alors une comparaison afin de déterminer si la déclaration est vraie ou non. La vérification de l'identité est généralement utilisée pour empêcher que plusieurs personnes n'utilisent la même identité[3].**la figure 1.2**

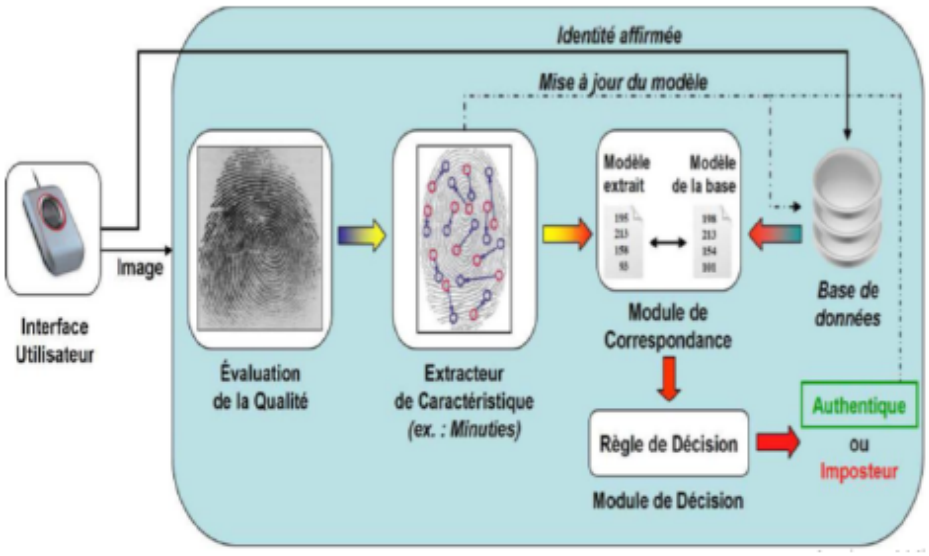


FIGURE 1.2 – Authentification d'un individu dans un système biométrique.

1.2.2.3 Mode d'identification

le système cherche à reconnaître un individu en comparant son modèle avec tous les modèles existants dans la base de données pour une éventuelle correspondance. Par conséquent, le système effectue une comparaison, du modèle de la personne, avec plusieurs modèles pour établir son identité. Ici l'individu n'a pas à revendiquer une identité. L'identification de l'identité est généralement utilisée pour empêcher qu'une personne n'utilise plusieurs identités[3].(voir **la figure 1.3**)

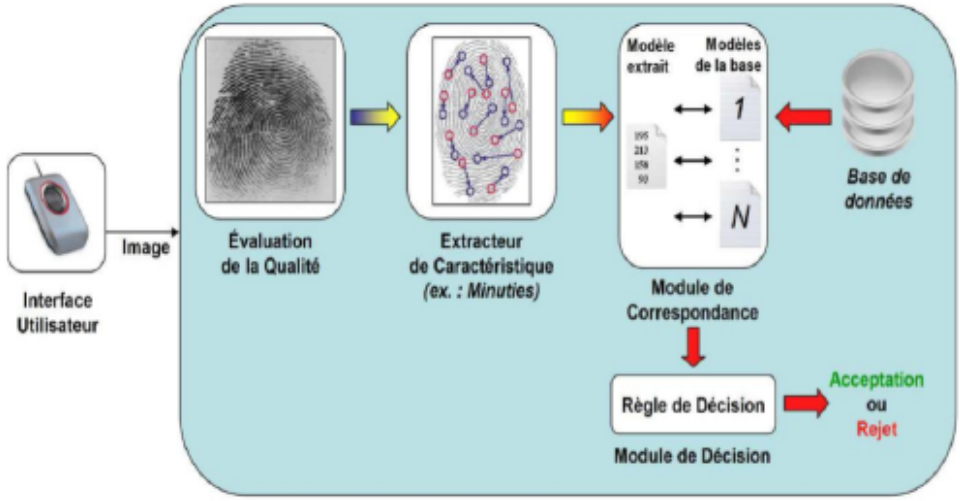


FIGURE 1.3 – Identification d'un individu dans un système biométrique.

1.2.3 Modalités biométriques

l'identification biométrique repose sur l'exploitation de caractéristiques humaines bien particulières qui constituent les différentes modalités biométriques[4]. ces modalités biométriques illustrées à **la figure 1.4** , sont regroupées en trois catégories :

1.2.3.1 Modalités morphologiques

Pour cette catégorie, l'authentification s'effectue à partir de caractéristiques physiques qui sont propres à chaque individu. On peut citer en particulier les empreintes digitales, le visage, l'iris, la rétine,..etc.

Les empreintes digitales : ce procédé est le plus répandu et le plus ancien, la donnée de base est le dessin représenté par les crêtes et sillons de l'épiderme (jonctions, terminaisons aveugles, croisements). Une empreinte est caractérisée par une centaine de points particuliers (appelés minuties),Les minuties représentent les fins de crêtes, les bifurcations, les lacs, les lots et les points qui composent l'empreinte digitale. La combinaison des minuties est quasi infinie[1].

Le visage : est la biométrie la plus commune et la plus populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle. Les caractéristiques jugées significatives pour la reconnaissance du visage sont : les yeux, la bouche et le tour du visage. Le problème de cette méthode vient des possibles perturbations pouvant transformer le visage (maquillage, faible luminosité, présence d'une barbe ou des lunettes, expression faciale inhabituelle, changement avec l'age, etc).[5]

L'iris : est la région, sous forme d'anneau, située entre la pupille et le blanc de l'oeil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. La reconnaissance de l'iris est développée dans les années 80 c'est pour cela elle est une technologie plus récente. l'image de l'iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place a une courte distance de l'appareil[6].

La rétine : La reconnaissance de la rétine permet d'observer les ramifications vasculaires qui tapissent le fond de l'oeil (surface interne antérieure) et qui sont uniques pour chaque personne. L'utilisateur doit placer son oeil face a un orifice de capture situé sur le dispositif d'acquisition, Le capteur enregistre la disposition des veines dans l'oeil en balayent la rétine a l'aide d'un faisceau lumineux dans le globe oculaire. Cette technique requiert une collaboration étroite de la part de l'utilisateur, car il doit placer son oeil extrêmement près de la caméra[**?**]7

1.2.3.2 Modalités biologiques

L'authentification s'effectue à partir d'éléments biologiques tels que la salive, ADN (Acide désoxyribo Nucléique), le sang. Elles sont très complexes à mettre en oeuvre et sont réservées exclusivement pour des applications judiciaires.

L'ADN : est l'outil d'identification par excellence, plusieurs états à travers le monde possédent ou programment la mise sur pied d'une base de données génétique et projettent de l'egiférer sur ce plan. L'analyse des empreintes génétiques est une méthode d'identification d'individus extrêmement précise, elle est issue directement de l'évolution de la biologie moléculaire.[5]

1.2.3.3 Modalités comportementales

L'authentification se base sur la différence comportemental d'un individu, tels que la démarche, la signature, la dynamique de frappe au clavier, la voix.

La démarche :Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps..etc), en analysant des séquences d'images. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle[1].

La signature : toute personne a son propre style d'écriture. A partir de la signature d'une personne, nous pouvons définir un modèle qui pourra être employé pour son identification. La signature étant utilisée dans beaucoup de pays comme élément juridique ou administratif, elle est utilisée pour justifier la bonne fois d'une personne ou pour la confondre devants des documents préalablement signés. la signature est examinée sous la forme d'une trace statique de stylo sur le papier. Sous forme numérisée, la géométrie statique de la signature ne suffit pas a garantir l'unicité de son auteur[8].

La voix : La biométrie de la voix traite des données qui proviennent à la fois de facteurs physiologiques dépendants de l'âge, du sexe, de la tonalité, de l'accent et de facteurs comportementaux comme la vitesse et le rythme. Ils ne sont en général pas imitables. C'est la seule technique qui permette à l'heure actuelle de reconnaître une personne à distance et qui est en général bien accepté par les usagers[5].

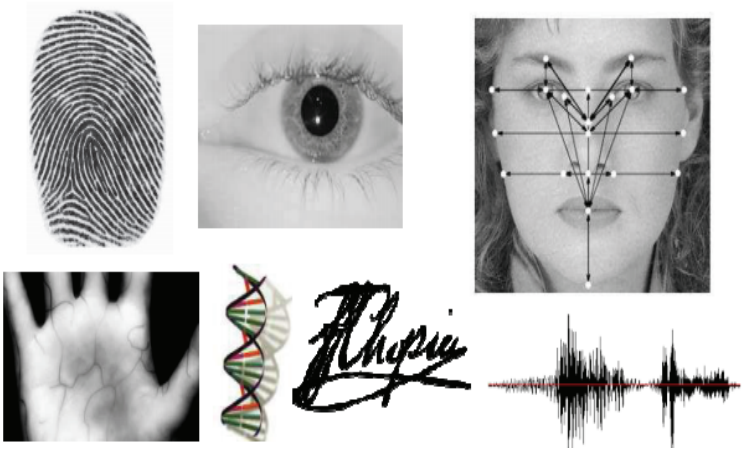


FIGURE 1.4 – Différentes modalités biométriques

Parmi les nombreuses méthodes d'identification biométrique l'utilisation des empreintes digitales est la méthode la plus aboutie avec 59% de parts de marché, nous y reviendrons

plus en détail dans la section suivante. Néanmoins d'autres méthodes commencent à trouver leur place sur le marché de la biométrie (voir **la figure 1.5**) :

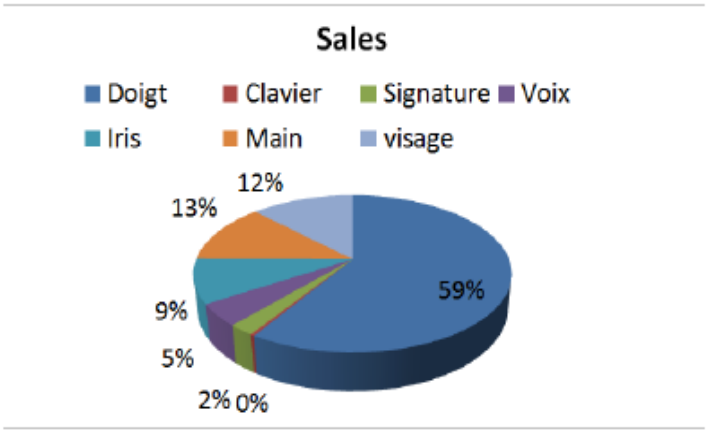


FIGURE 1.5 – Part de marché comparatif par technologie biométrie

1.2.4 Architecture d'un système biométrique

L'architecture d'un système biométrique contient cinq modules comme le montre **la figure 1.6** :

1.2.4.1 Module de capture :

qui consiste à acquérir les données biométriques afin d'extraire une représentation numérique. Cette représentation est ensuite utilisée pour l'enrôlement, la vérification ou l'identification. Il s'agit d'un capteur biométrique qui peut être de type sans ou avec contact.

1.2.4.2 Module de traitement du signal :

qui permet de réduire la représentation numérique extraite afin d'optimiser la quantité de données à stocker lors de la phase d'enrôlement, ou pour faciliter le temps de traitement pendant la phase de vérification et l'identification. Ce module peut avoir un test de qualité pour contrôler les données biométriques acquises.

1.2.4.3 Module du stockage :

qui contient les modèles biométriques des utilisateurs enrôlés du système.

1.2.4.4 Module de similarité :

qui compare les données biométriques extraites par le module d'extraction de caractéristiques a un ou plusieurs modèles préalablement enregistrés. Ce module détermine ainsi le degré de similarité (ou de divergence) entre deux vecteurs biométriques.

1.2.4.5 Module de décision :

qui détermine si l'indice de similarité retourné est suffisant pour déterminer l'identité d'un individu.[9]

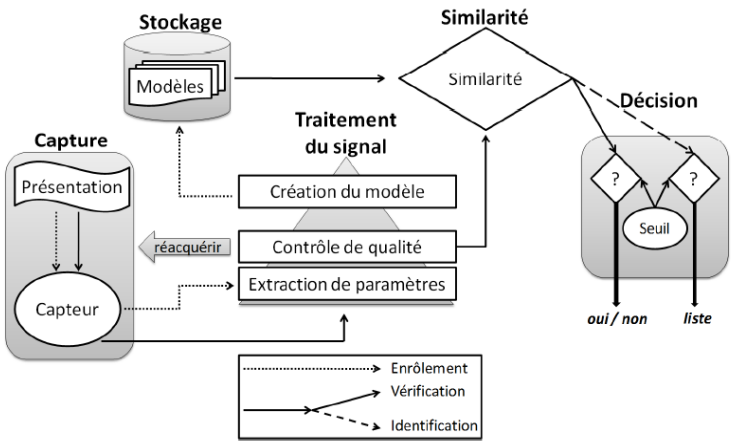


FIGURE 1.6 – Architecture complète d'un système biométrique.

1.2.5 Performance d'un système biométrique :

En biométrie, chaque système est en face de deux populations :

1. Les clients appartenant au système, ceux qui sont autorisés à pénétrer dans la zone protégée.
2. Les imposteurs n'appartenant pas au système, mais généralement qui essayent de rentrer.

Pour évaluer les performances d'un système biométrique plusieurs mesures sont employées :

✓ **Le taux de faux rejets (TFR)** : ("False Reject Rate"ou FRR), c'est la possibilité que le système produise un faux rejet. Ce taux représente le pourcentage des personnes censées être reconnues mais qui sont rejetées par le système.

$$TFR = \frac{\text{nombre de client rejeté(FR)}}{\text{tenombre total d'acces clientsxt}} \tag{1.1}$$

✓ **Le taux de fausse acceptation (TFA)** ("False Accepte Rate" ou FAR) : est la probabilité qu'un système biométrique identifie de manière incorrecte une personne ou ne réussisse pas à rejeter un imposteur. Il mesure le pourcentage d'intrants non valides qui sont acceptés à tort. Il est 'également connu sous le nom de 'taux de faux Positif".

$$TFA = \frac{\text{nombre imposteurs acceptés (FA)}}{\text{nombre total d'acces imposteurs}} \tag{1.2}$$

✓ **Le taux d'erreur (TEE)**("Equal Error Rate" ou EER) : ce taux est calculé à partir des deux premiers critères et constitue un point de mesure performance courant. Ce point correspond au lieu où FRR = FAR, c'est- à -dire le meilleur compromis entre le faux rejet et la fausse acceptation.

$$TEE = \frac{\text{nombre de fausses acceptations (FA) + nombre de faux rejets (FR)}}{\text{nombre totale d'acces}} \tag{1.3}$$

✓ **GAR** :«Genuine Accept Rate» c'est le taux des véritables clients acceptés par le Système biométrique. GAR est calculé par l'équation :

$$TFA = GAR(T) = 1 - FRR(T) \tag{1.4}$$

La relation entre FAR et FRR et le seuil T sont montrés sur **la Figure 1.7** où on constate que si on choisit le seuil T faible, le système laissera passer tous les gentils utilisateurs (clients), mais il laissera passer aussi les imposteurs facilement ce qui donne un système de faible sécurité. Et si on choisit le seuil T fort, le système bloquera les imposteurs mais malheureusement bloquera aussi quelques clients.

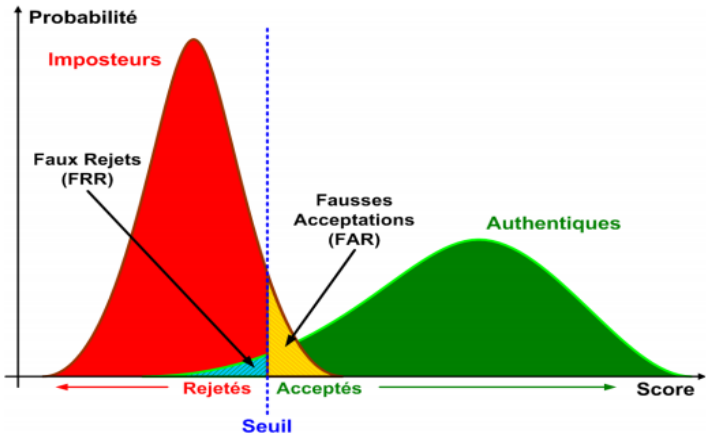


FIGURE 1.7 – Illustration du FRR et du FAR .
[29]

La courbe DET est la liaison entre le FAR et le FRR pour différentes valeurs de seuil comme montre **la Figure 1.8** .

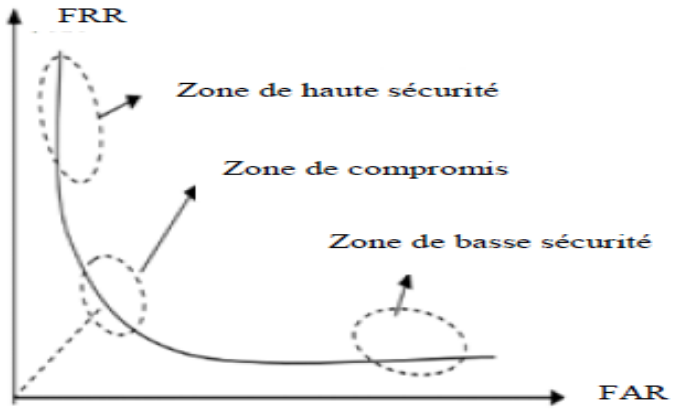


FIGURE 1.8 – Courbes DET.

Comparaison des performances Le vrai taux positif (TPR) P_{TPR} et le taux de faux positifs (FPR) P_{FPR} ont été calculés comme suit [28] :

$$T_{TPR} = \frac{\text{n similaire}}{\text{N identique}} \tag{1.5}$$

$$T_{FPR} = \frac{\text{n distinct}}{\text{N identique}} \tag{1.6}$$

Où n similaire est le nombre des paires d'images visuellement identiques correctement identifiées comme des images similaires, N identique est le nombre total de paires d'images visuellement identiques, n distinct est le nombre des paires d'images distinctes considérées par erreur comme des images similaires, et N différent est le nombre total de paires d'images différentes. Il est clair que le TPR et le FPR sont respectivement des indicateurs de robustesse et de discrimination.

1.2.6 Applications d'un système biométrique

Les techniques biométriques sont appliquées dans plusieurs domaines et leurs champ d'application couvrent potentiellement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes[1]. Les applications de la biométrie peuvent être divisées en trois groupes principaux **figure 1.9** :

- **Applications commerciales** : telles que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.
- **Applications gouvernementales** : telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc.

- **Applications légales** : telles que l'identification de corps, la recherche criminelle, l'identification de terroriste, etc.

FIGURE 1.9 – Quelques applications de la biométrie.

1.3 Reconnaissance des empreintes digitales :

1.3.1 Empreinte digitale :

L'empreinte digitale se compose d'un ensemble de lignes localement parallèles dessinées sur l'épiderme appelées "les stries"(ou les crêtes qui sont les reliefs en contacts avec la surface au toucher) et des creux entre les stries appelées "les vallées" (ou les sillons), (**Figure 1.8**).

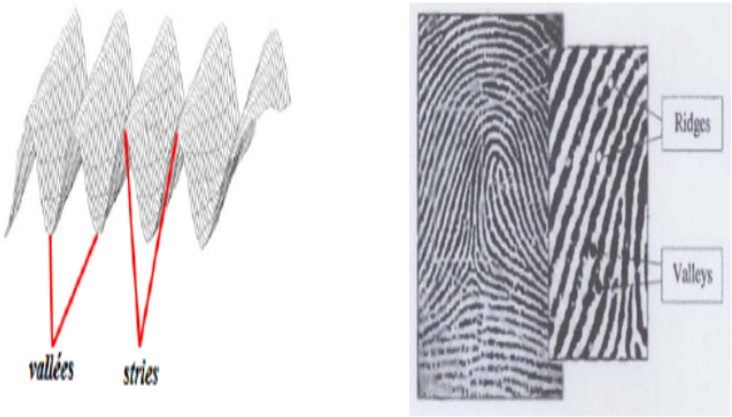


FIGURE 1.10 – Les vallées (valleys) et les crêtes (ridges) sur une empreinte.

1.3.2 Caractéristiques d'une empreinte digitale :

Plusieurs représentations des empreintes digitales sont proposées, et elles sont classifiées dans deux types principaux : représentation locale et représentation globale. La représentation

globale est un attribut entier du doigt et la représentation locale se compose de plusieurs composants, chaque composant typiquement dérivé d'une région dans l'espace limitée de l'empreinte digitale. Généralement, des représentations globales sont employées pour la classification d'empreinte digitale et des représentations locales sont employées pour la comparaison d'empreinte digitale.

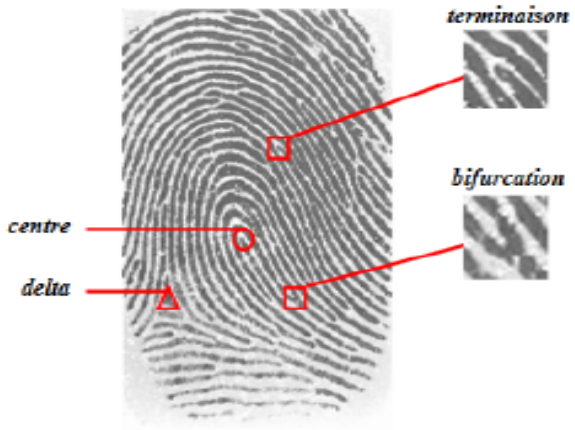


FIGURE 1.11 – Caractéristiques d'une empreinte digitale.

1.3.2.1 Représentation globale

chaque empreinte digitale a un ensemble des points singuliers globaux qui sont les centres et les deltas, symbolisés respectivement par θ et $\triangle$. Le centre est le lieu de convergence des stries (il est aussi appelé le core), alors que le delta correspond au lieu de divergence. La position et le nombre de ces points permettent la classification des empreintes digitales, c'est ainsi que Francis Galton les a subdivisées en trois grandes familles[10] :

- ✓ **Les Boucles (Loops)** une empreinte est de classe boucle si ses stries rentrent d'un côté et ressortent du même côté et si elle possède un point singulier de type boucle et un point singulier de type delta. Les boucles représentent 65% des empreintes des doigts humains.
- ✓ **Les Spires (Whorls)** une empreinte appartient à la classe spire si elle possède au moins une strie qui fait 360°. Elle peut aussi contenir jusqu'à deux régions singulières de type boucles et deux régions singulières de type deltas. Les spires représentent 30% des empreintes des doigts humains.
- ✓ **Les Arches (Archs)** : une empreinte est de classe arche si elle possède des stries qui rentrent d'un côté et ressortent du côté opposé et si elle ne contient ni boucle ni delta comme points singuliers. Les arches ne représentent que 5% des empreintes des doigts humains.

Edward Henry les a classées en six sous-classes principales : arche, boucle à gauche (left loop), boucle à droite (right loop), arche penchée (tented arch), spires et spires imbriquées ou boucles jumelles[11] (**figure 1.12**)

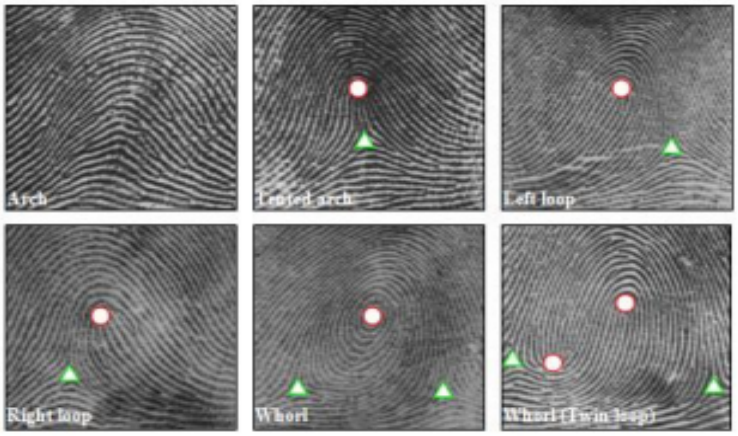


FIGURE 1.12 – Les principales classes d'empreintes digitales selon la classification de Galton-Henry .

1.3.2.2 Représentation locale

Il s'agit des caractéristiques les plus utilisées "les minuties" (littéralement : petits détails), qui sont en fait les points d'irrégularités qui se trouvent sur les lignes capillaires. Nous pouvons distinguer jusqu'à seize types de minuties différentes , mais dans les algorithmes on n'en s'intéresse qu'aux deux types suivants parce qu'ils sont facilement détectables :

- ✓ **La bifurcation** c'est le point où la strie se divise en deux.
- ✓ **La terminaison** c'est le point où la strie s'arrête .

En fait les autres types de minuties ne sont que les résultats des combinaisons des minuties de terminaison et de bifurcation. Par exemple, les boucles peuvent être visualisées en tant que deux bifurcations. Chaque minutie est représentée par les cordonnées (x, y) de sa position dans l'image, et l'angle Θ qui est la direction associé à la strie (**la figure 1.13**). Donc chaque minutie de l'empreinte est repérée par un vecteur de la forme[12] : (Type de minutie, x, y,Θ).

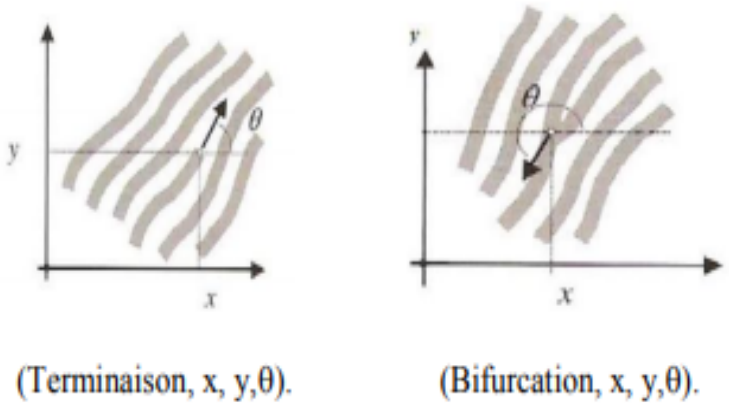


FIGURE 1.13 – Représentation des vecteurs de terminaison et de bifurcation. [30]

1.3.3 Structure d'un système de reconnaissance d'empreintes digitales :

Un système automatique complet de reconnaissance d'empreintes digitales est une chaîne de processus qui à partir du doigt d'un utilisateur en entrée renvoie un résultat en sortie, permettant ainsi à l'utilisateur d'accéder ou non à des éléments nécessitant une protection. La réalisation d'un tel système a fait l'objet de très nombreuses recherches et des méthodes très différentes de traitement ont été proposées. Cependant ces systèmes répondent toujours à la même structure (**figure 1.14**) :

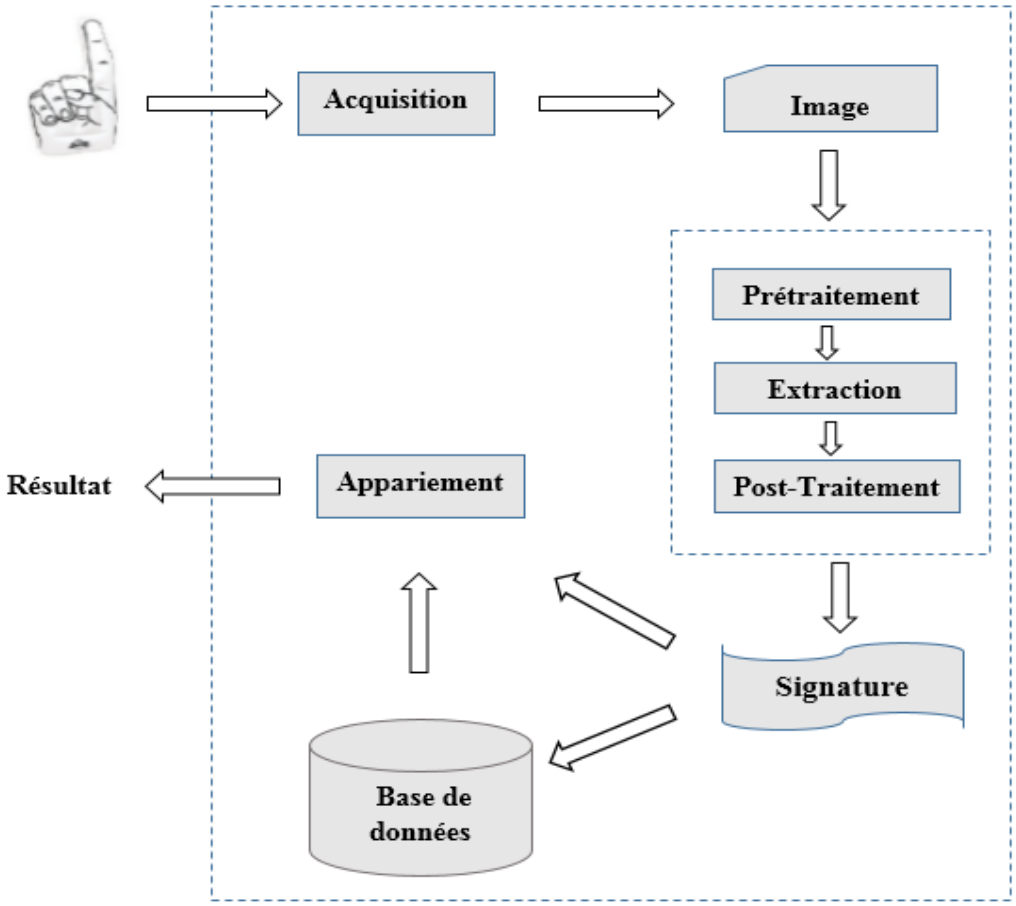


FIGURE 1.14 – Architecture générale d'un système complet de reconnaissance d'empreintes.

1.3.3.1 L'acquisition de l'image d'empreinte

La première phase d'un système de reconnaissance consiste à obtenir une image de l'empreinte du doigt.

La capture de l'image d'une empreinte digitale consiste à trouver les lignes tracées par les crêtes (en contact avec le capteur) et les vallées (creux). L'image d'une empreinte est acquise par des procèdes directs (online) ou indirects (offline) :

L'acquisition directe : ce sont les capteurs, où on peut citer :

Les capteurs optiques (les plus répondus, dont le principe de fonctionnement est le même que celui du scanner ainsi ses prix acceptables), les capteurs thermiques, les capteurs à ultrasons qui sont assez chers, les capteurs intégrés au silicium .

L'acquisition indirecte : où il existe 2 méthodes :

- ✓ **L'empreinte acquise par encre** : après l'avoir enduit d'encre, le doigt est imprimé sur un bout de papier. Ce papier passe ensuite au scanner standard pour être numérisé.
- ✓ **les empreintes latentes** : elles sont formées suite à une légère trace laissée sur un objet due à la sécrétion constante de la sueur. Les services de sécurité décèlent ce genre de détails sur les lieux du crime à l'aide d'une poudre spéciale.

1.3.3.2 Pré-traitement

La reconnaissance d'une empreinte digitale est directement liée à la qualité de l'image obtenue au moyen du capteur. Ainsi dans la plupart des cas, un pré-traitement (**figure 1.16**) est nécessaire pour améliorer la qualité de l'image. Pour limiter les calculs des étapes suivantes du système l'image brute de l'empreinte est filtrée. Une opération de filtrage utilisant les caractéristiques locales de l'empreinte est ensuite appliquée à l'image de manière à améliorer sa qualité en éliminant le bruit[13].

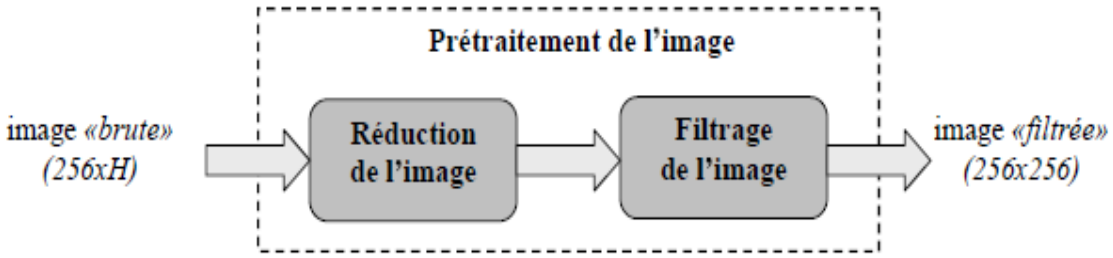


FIGURE 1.15 – Principe du pré-traitement de l'image.

1.3.3.3 Extraction des caractéristiques

La méthode classique : La méthode la plus répandue consiste à extraire les minuties à partir d'un squelette de l'image. Comme le montre la **figure 1.17** l'image est d abord préparée à l'étape d'extraction au moyen d une binarisation et d'une squelettisation, ensuite un fichier signature est extrait de l'empreinte après la détection et l'extraction des minuties[13].

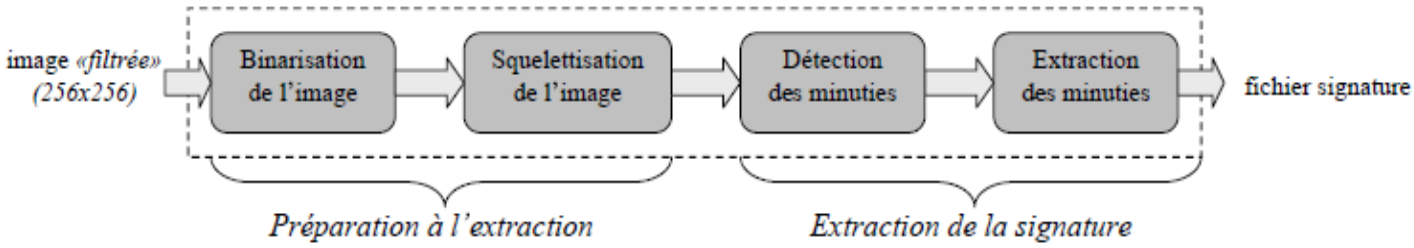


FIGURE 1.16 – La phase d'extraction de la signature

Estimation de champ d'orientation : Le champ d'orientation d'une image d'empreintes digitales représente la nature intrinsèque d'empreintes digitales (**figure 1.18**). C'est un étage essentiel pour déterminer les rides d'empreintes digitales et pour trouver la région d'intérêt d'image d'empreintes digitales, Il existe plusieurs méthodes pour estimer le champ d'orientation des images d'empreintes digitales. **Anil Jain** et **al** ont proposés une méthode efficace pour estimer le champ d'orientation d'une image.

FIGURE 1.17 – Le champ d'orientation d'une image d'empreinte digitale

L'idée principale de cette méthode est que l'image d'impatience digitale se divise en plusieurs fenêtres de taille WxW[32]. Pour tout pixel dans chaque fenêtre, on calcule les gradients Gx et Gy et puis on calcule l'orientation locale de ce pixel en utilisant la formule suivante :

$$v_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} (2G_x(u,v)G_y(u,v)) \tag{1.7}$$

$$v_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} (2G_x^2(u,v) - G_y^2(u,v)) \tag{1.8}$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}(\frac{v_x(i,j)}{v_y(i,j)}) \tag{1.9}$$

Avec : W : la taille de la fenêtre locale
G_x et G_y : sont les grandeurs de gradient dans des directions de x et de y respectivement
(i, j) : est l'orientation locale du pixel (i, j).

Segmentation : Après avoir estimé le champ d'orientation d'une image d'empreintes digitales, un algorithme de segmentation qui est basé sur le niveau de certitude du champ d'orientation est employé pour localiser la région d'intérêt dans l'image d'empreintes digitales[32]. Le niveau de certitude du champ d'orientation au pixel (i, j) est défini comme suit :

$$CL(i,j) = \sqrt{\frac{1}{w^2}\frac{v_x^2(i,j) + v_y^2(i,j)}{v_e(i,j)}} \tag{1.10}$$

Tel que :

$$v_e(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} (2G_x^2(u,v) + G_y^2(u,v)) \tag{1.11}$$

Avec :
W : la taille de la fenêtre locale.
Gx et Gy : les grandeurs de gradient dans des directions de x et de y respectivement.
CL (i, j) : l'orientation locale du pixel (i, j).
Pour chaque pixel, si son niveau de certitude du champ d'orientation est inférieur d'un certain seuil T, il est marqué comme pixel de fond. Sinon il est marqué comme un pixel de la région d'intérêt.

La Binarisation : Pour permettre la squelettisation, l'image doit d'abord être binarisée, c'est-à-dire que l'image en 256 niveaux de gris dont nous disposons à ce stade est transformée en image binaire où les pixels noirs correspondent aux stries et les pixels blancs aux vallées[14]. Pour effectuer ce traitement la valeur de chaque pixel P(x, y) est comparée à un seuil T et si cette valeur est supérieure au seuil le pixel prend la valeur de un (noir), sinon il prend la valeur de zéro (blanc),(**figure 1.18**).

$$P(X,Y) = \{\ 1 \text{ si } P(x,y) \geqslant T$$
$$\{0 \text{ si } P(X,y) \leqslant T$$

FIGURE 1.18 – Résultats de de binarisation

La squelettisation : Pour faciliter l'extraction des minuties l'image doit être squelettisée : une suite d'opérations morphologiques d érosion va réduire l'épaisseur des stries jusqu'à ce que cette dernière soit égale à un pixel tout en conservant la connexité des stries (c'est-à-dire que la continuité des stries doit être respectée, il ne faut pas introduire de trous). Nous avons utilisé l'algorithme de Rosenfeld[15] pour sa simplicité. Pour chaque pixel p_0 on considère son voisinage immédiat de 8 pixels $P_i, i \in [1..8]$. Pour l'algorithme de squelettisation on considère les définitions suivantes :

1. P_0 est un point frontière Nord si $P_2 = 0$
2. P_0 est un point frontière Est si $P_4 = 0$
3. P_0 est un point frontière Sud si $P_6 = 0$
4. P_0 est un point frontière Ouest si $P_8 = 0$
5. P_0 est un point 8-terminal si un seul de ses voisins est noir ($\exists i \in [1..8], p_i = 1$), il s'agit d'une minutie de type terminaison .
6. P_0 est un point 8-isolé si aucun de ses voisins n'est noir ($\forall i \in [1..8], p_i = 0$)
7. P_0 est un point 8-simple si la connexité de ses 8 voisins n'est pas altérée quand on le transforme en pixel blanc.

P_1	P_2	P_3
P_8	P	P_4
P_7	P_6	P_5

La squelettisation consiste à répéter les opérations d'érosion suivantes jusqu'à ce que plus aucun pixel ne soit changé :

- **Etape 1** : tous les pixels noirs vérifiant (1) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Nord) .
- **Etape 2** : tous les pixels noirs vérifiant (2) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Est)
- **Etape 3** : tous les pixels noirs vérifiant (3) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Sud) .
- **Etape 4** : tous les pixels noirs vérifiant (4) et (7) et ne vérifiant pas (5) et (6) sont changés en pixels blancs (érosion des points frontières Ouest). La propriété (7) peut être ignorée dans les étapes d'érosion car bien qu'un point unique corresponde à une minutie sa présence à ce stade du traitement est très probablement due à un résidu de bruit, il vaut donc mieux l effacer. Il est à noter que plus l'épaisseur des stries sera importante et plus le processus sera long. La **figure 1.20** montre le résultat obtenu à partir d'une image binaire filtrée.

FIGURE 1.19 – Résultats de de squelettisation

La détection des minuties : Les deux étapes de préparation à l extraction (binarisation et squelettisation) ont grandement facilité cette phase. En effet nous disposons maintenant d'une image binaire squelettisée : un pixel noir prend la valeur 1, un pixel blanc prend la valeur 0 et la largeur des stries est égale à 1 pixel. Si l'on calcule le nombre de transitions divisé par 2 entre un pixel blanc et un pixel noir pour chaque point du squelette, on obtient le nombre CN de stries partant de ce point (Crossing Number) et nous pouvons donc déterminer simplement le type d'un pixel[13] (voir **figure 1.21**).

Ainsi pour chaque pixel P appartenant à une strie (c'est-à-dire pour chaque pixel qui prend la valeur de 1), le calcul de CN peut prendre cinq valeurs :

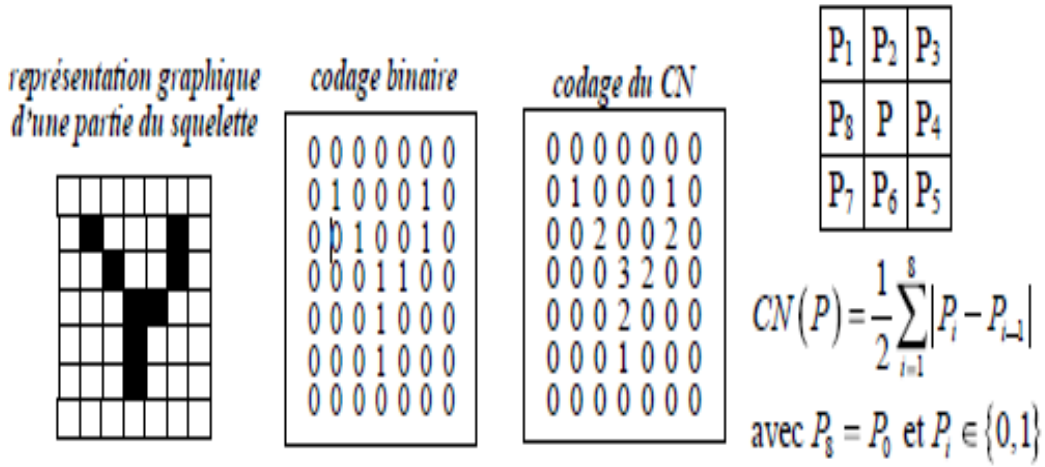


FIGURE 1.20 – Les différentes représentations du squelette.

— CN (P) =0 : dans ce cas il s'agit d'un pixel isolé et nous n'en tenons pas compte, car même si ce type de minutie existe, il est très rare et à ce stade du traitement il est probablement dû à un résidu de bruit.
— CN (P)=1 : dans ce cas nous avons à faire à une minutie de type terminaison.
— CN (P)=2 : c'est le cas le plus courant, le pixel se situe sur une strie, il n'y a pas de minutie.
— CN (P)=3 : nous sommes en présence d'une bifurcation triple.
— CN (P)=4 : nous sommes en présence d'une bifurcation quadruple. Ce type de minutie étant assez rare il est probablement dû au bruit que nous l'ignorons.

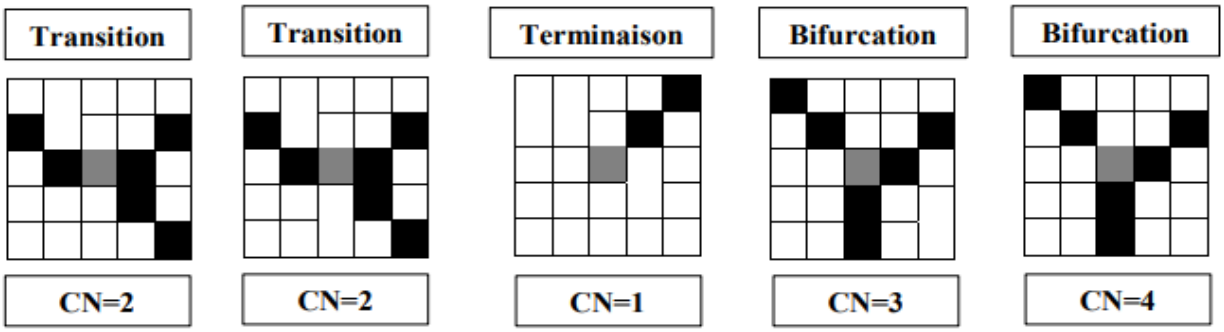


FIGURE 1.21 – Exemples de détermination du type de minutie en fonction du calcul de CN.

1.3.3.4 Post-traitement

L'objectif de ce processus est d'éliminer au maximum les fausses minuties tout en conservant les vraies détectées. Pour cela, on utilise des considérations empiriques[16],[17] basées sur le fait que la distance entre deux minuties voisines est toujours supérieure à un certain seuil. En effet, pratiquement, il est extrêmement rare de trouver deux vraies minuties très

proches, par contre on a quasiment toujours une concentration locale de plusieurs fausses minuties.

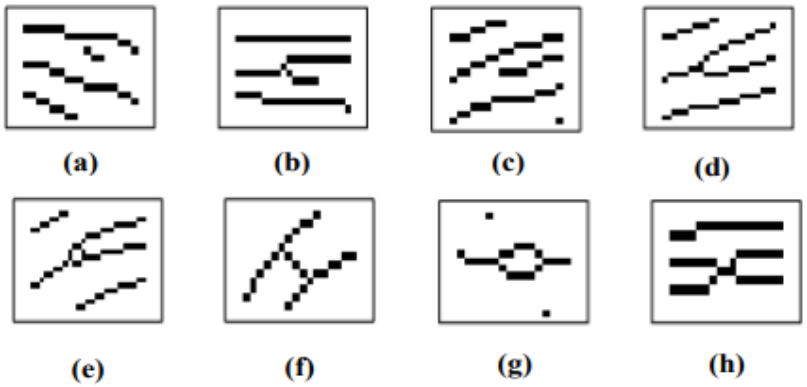


FIGURE 1.22 – Exemples de détermination du type de minutie en fonction du calcul de CN.

Traitement des terminaisons détectées

Pour éliminer les fausses terminaisons, nous suivons les règles suivantes : S'il existe un bloc adjacent au bloc contenant la terminaison T (XT ; YT) et appartenant au bord de l'image, alors T est une fausse minutie et nous élimine.

Pour les terminaisons restantes T, on parcourt la strie qui lui est associée sur une distance maximum K1, jusqu'à atteindre le point A.

FIGURE 1.23 – Validation des terminaison détéctes : vrai terminaison(a), branche parasite(b), segment trop court(c)

Traitement des bifurcations détectées

Lorsqu'on détecte un point B candidat pour le titre de bifurcation (CN (B)=3), on parcourt les trois stries qui lui sont associées sur une distance maximum de K jusqu'à atteindre trois points A_1, A_2 et A_3 (**Figure 1.25**). Plusieurs cas peuvent se produire et ils sont traités dans l'ordre suivant :

— $d < K_1$, $d < K_2$, $d < K_3$ la zone circulaire de centre B et de rayon K1 contient au moins quatre minuties. On considère alors que nous sommes dans une zone très bruitée (regroupement important) et que B est une fausse bifurcation.

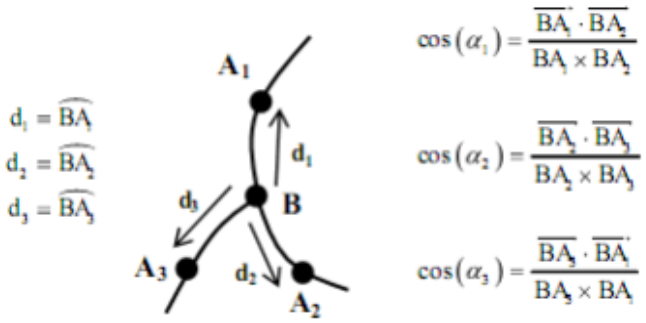


FIGURE 1.24 – Définitions associée a une bifurcation lors de la phase de validation.

CN (A_1)=1, CN (A_2)=1, CN (A_3)=1 : au moins une des stries mène à une terminaison. On est dans le cas d'une branche parasite, le point B et les terminaisons atteints ne sont pas validés.

— A_1= A_2 ou $A_2 = A_3$ où $A_3 = A_1$: deux des stries mènent au même point. On est dans le cas d'un îlot , le point B et la bifurcation atteinte ne sont pas validés.

— Nous avons deux des stries qui mènent à deux bifurcations A_1 et A_2 (CN (A_1) =3, CN (A_2)=3). Dans ce cas, on calcule la différence angulaire $\alpha 1$ ainsi que la distance $\| \overline{A_1A_2}\|$ entre les deux bifurcations rencontrées. Si les conditions $|\cos(\alpha 1)| > \cos(\Pi \div 4)$ et $\| \overline{A_1A_2}\| \leq \lambda$ (B correspond à la distance inter-strie locale du bloc contenant B) sont réunies, alors on est dans le cas d'un triangle et on considère que B est une vraie bifurcation tandis que A1 et A2 sont des fausses.

— Une seule des stries mène à une bifurcation A1 (CN (A_1) = 3). On calcule les différences angulaires $\alpha 1$ et $\alpha 2$ ainsi que la distance entre A1 et B.$|\cos(\alpha 2)| > \cos(\Pi \div 4), |\cos(\alpha 1)| > \cos(\Pi \div 4)$ et $|BA_1| \leq \lambda$ alors on est dans le cas d'un pont et A_1 et B sont considérés comme de fausses minuties.

— Dans tous les autres cas, le point B est validé en tant que vraie bifurcation. La **figure 1.26** du processus d'extraction des minuties ainsi que la phase d'élimination des fausses terminaisons et bifurcations.

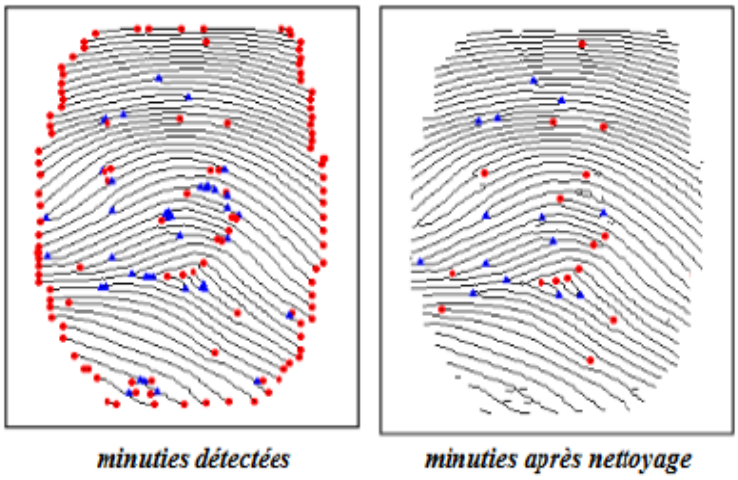


FIGURE 1.25 – Résultat de la phase d'élimination des fausses minuties.

1.3.4 Comparaison des empreintes digitales

La comparaison des empreintes digitales consiste à réaliser un accord entre la signature à identifier et les signatures stockées dans la base de données. Cependant cette tâche n'est pas facile[18], notamment à cause de la variabilité dans les différentes impressions d'une même empreinte (variation intra-classe)**figure 1.27**.

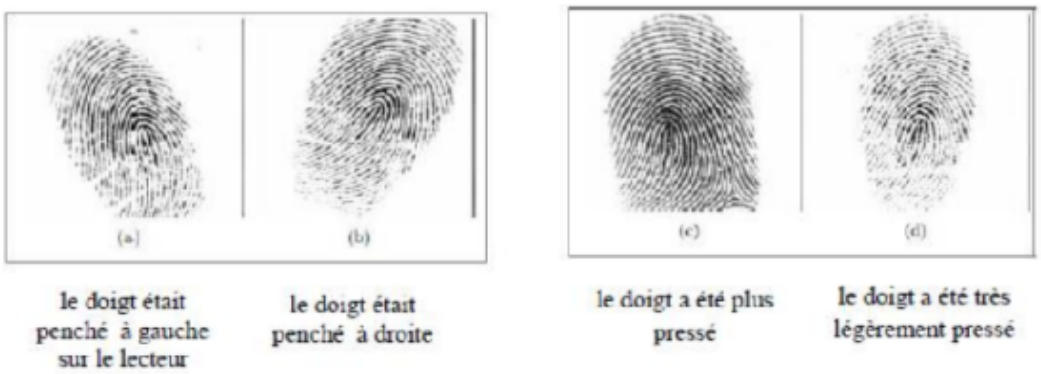


FIGURE 1.26 – Les différentes positions de même doigt.

Il existe plusieurs approches classifiées en 3 catégories principales :

1.3.4.1 Approches basées sur la corrélation

Cette approche est basée sur la corrélation des pixels de deux empreintes digitales, Elle consiste à comparer tout simplement les matrices de pixels des images de deux empreintes, et calculer la corrélation de pixels.

1.3.4.2 Approches basées sur les crêtes

Dans cette approche, on utilise des caractéristiques extraites des crêtes (orientation, texture, forme de ride, etc.) pour comparer les empreintes digitales. L'avantage de cette approche est que les caractéristiques de crêtes peuvent être extraites plus exactement, cependant les distinctions de ces caractéristiques sont faibles.

1.3.4.3 Approches basées sur les minuties

C'est l'approche la plus utilisée dans la littérature, des minuties sont extraites à partir des deux empreintes digitales et stockées sous forme d'un ensemble de points dans le plan de deux dimensions. L'assortiment basé sur minuties essentiellement se compose de trouver l'alignement entre les minuties du motif et les minuties d'entrée. Le résultat est le nombre maximum des pairs de minuties.

1.4 Conclusion

Dans ce premier chapitre, nous avons présenté une vue générale de la biométrie, un survol sur quelques techniques biométriques, ainsi que l'architecture d'un système biométrique, ses applications et ses avantages. Ensuite, nous avons entamé d'une façon détaillée la technique à utiliser dans notre travail et qui est celle de l'empreinte digitale, où nous avons spécifié les caractéristiques d'une empreinte digitale, la structure générale d'un système de reconnaissance d'empreintes digitales, ainsi que les différentes approches de comparaison pour déterminer la correspondance entre deux empreintes.

Dans le chapitre suivant, nous allons présenter les cryptosystémes biométriques et ses méthodes, en détaillant la technique proposé et qui est notre intérêt dans ce mémoire.

Chapitre 2

Cryptosystémes biométriques

2.1 Introduction

Dans ce chapitre, nous allons présenter le concept des cryptosystèmes biométriques, leur classifications et leurs différentes méthodes,ensuite nous détaillons les différents principes et étapes de la méthode proposée.

2.2 Cryptosystème biométrique

Les cryptosystèmes biométriques combinent la cryptographie et la biométrie pour bénéficier des atouts des deux domaines. Dans de tels systèmes, alors que la cryptographie fournit des niveaux de sécurité élevés et ajustables, la biométrie apporte la non-répudiation et élimine le besoin de se souvenir des mots de passe ou de porter des jetons, etc.[20]
Les cryptosystèmes biométriques sont conçus pour lier en toute sécurité une clé numérique à une clé biométrique ou pour générer une clé numérique à partir d'une clé biométrique.[21]

2.2.1 Protection du modèle biométrique

Les cryptosystèmes biométriques libèrent des clés cryptographiques qui sont associées aux traits biométriques des utilisateurs enregistrés. Par conséquent, les cryptosystèmes biométriques offrent des solutions pour sécuriser la gestion des clés basée sur la biométrie ainsi que la protection des modèles biométriques. Puisque l'authentification est effectuée indirectement en vérifiant les validités de clé, le système n'a pas besoin de stocker les modèles biométriques d'origine. De plus, la plupart des cryptosystèmes biométriques fournissent des mécanismes pour mettre à jour ces clés à tout moment afin que les utilisateurs puissent appliquer différentes clés à différentes applications.

2.2.2 Classification des cryptosystèmes biométriques

Les cryptosystèmes biométriques sont classés comme systèmes de liaison de clé et de génération de clé en fonction de la façon dont le croquis sécurisé est obtenu. Le croquis sécurisé est une information publique sur les caractéristiques biométriques stockées dans les bases de données lors de l'inscription.[20]

2.2.2.1 Cryptosystèmes biométriques de liaison de clés

Les données auxiliaires sont obtenues en liant une clé choisie à un modèle biométrique. À la suite du processus de liaison, une fusion de la clé secrète et du modèle biométrique est stockée en tant que données auxiliaire. En appliquant un algorithme de récupération de clé approprié, les clés sont obtenues à partir des données auxiliaires lors de l'authentification[22]. Étant donné que les clés cryptographiques sont indépendantes des fonctionnalités biométriques, elles sont révocables tandis qu'une mise à jour de la clé nécessite généralement une réinscription afin de générer de nouvelles données auxiliaires. Le mode de fonctionnement général d'un schéma de liaison de clé est illustré sur la **figure 2.1** :

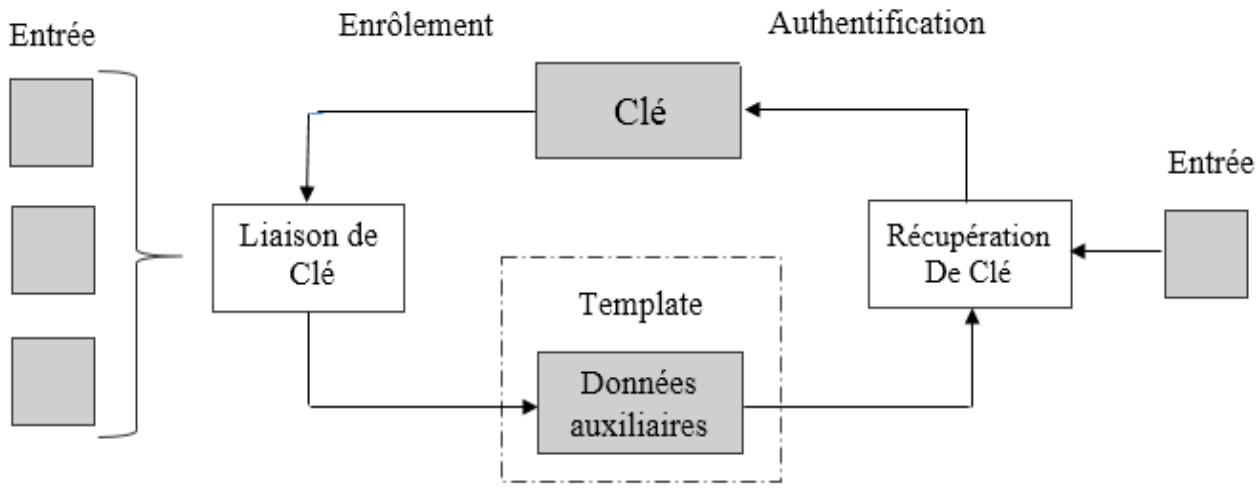


FIGURE 2.1 – Mode de fonctionnement général d'un schéma de liaison de clé

2.2.2.2 Cryptosystèmes biométriques de génération de clés

Si l'esquisse sécurisée est dérivée uniquement du modèle biométrique et que la clé cryptographique est directement générée à partir des données d'aide et des fonctionnalités biométriques de requête, alors on parle de cryptosystèmes biométriques de génération de clé. Les données auxiliaires sont appliquées pour récupérer le modèle biométrique d'origine[21]. Le mode de fonctionnement général d'un schéma de génération de clé est illustré sur la **figure 2.2** :

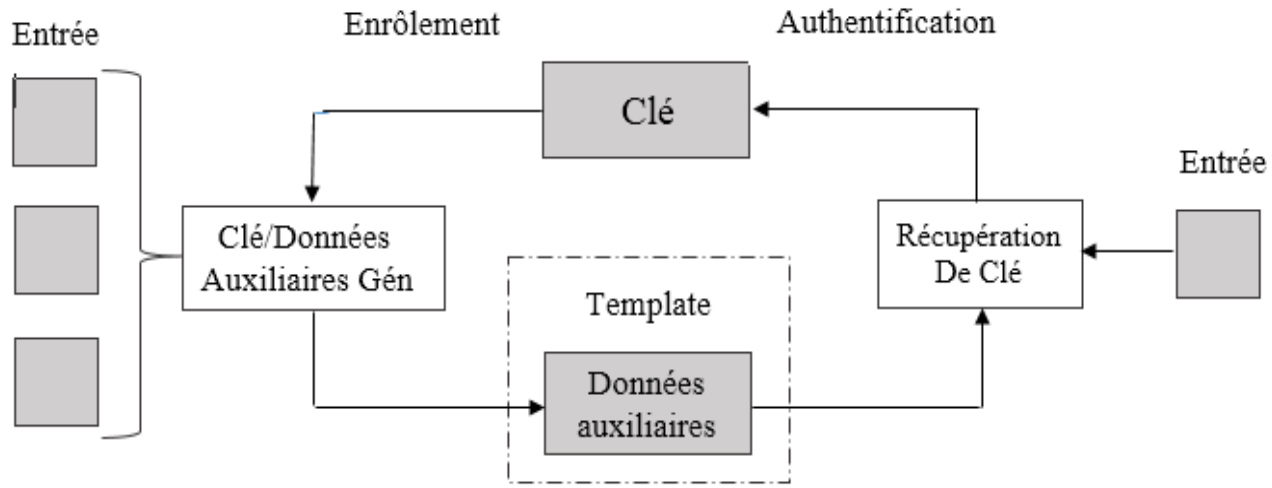


FIGURE 2.2 – mode de fonctionnement général d'un schéma de génération de clé

2.2.3 les méthodes de cryptosystéme biométrique

2.2.3.1 Fuzzy commitment

Le principe de cette méthode est d'utiliser la donnée biométrique courante pour recalculer une valeur qui servira ensuite pour l'authentification de l'utilisateur[25]. Plus formellement, la méthode dite du fuzzy commitment se décompose en deux étapes : enrôlement puis authentification. Traditionnellement en biométrie, l'étape d'enrôlement consiste à relever plusieurs fois la donnée biométrique de l'utilisateur (son empreinte par exemple) afin de constituer une valeur de référence. L'étape d'authentification consiste ensuite à comparer la valeur courante à la valeur de référence pour déterminer si l'utilisateur est bien celui attendu. La méthode dite du fuzzy commitment suit ces deux étapes sauf que la valeur de référence stockée n'est pas une donnée biométrique et ne permet pas de retrouver la donnée biométrique utilisée pour la générer. Pour cela, le fuzzy commitment utilise un ensemble de mots de code dans $\{0,1\}^n$ et une fonction de hachage H (**figure 2.3**).

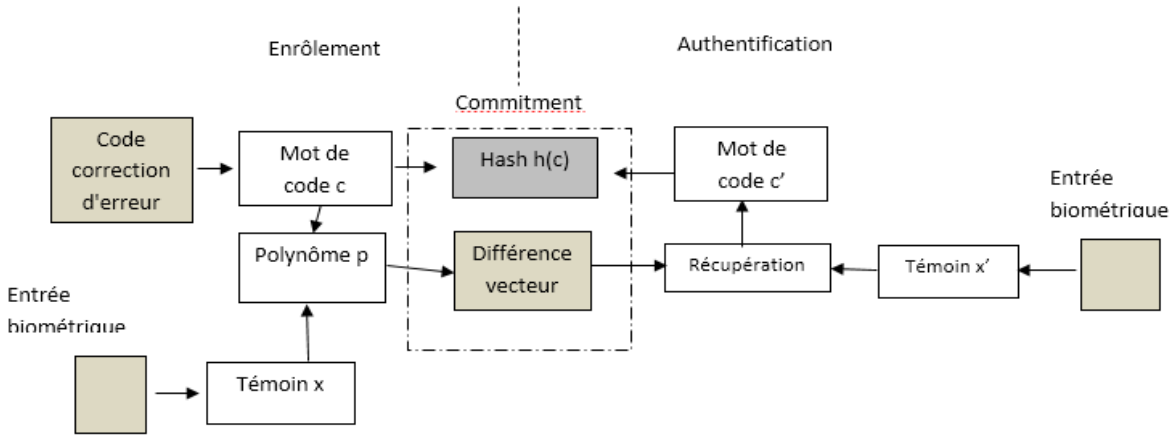


FIGURE 2.3 – Schéma de fuzzy commitment.
[31]

— **Enrôlement :** Un utilisateur **U** présente son empreinte biométrique représentée sous la forme d'une suite **x** de **n** bits. Le système choisit aléatoirement un mot de code $c \in \{0,1\}^n$ et calcule $(c-x, H(c))$. Le fuzzy commmitment de l'utilisateur **U** est le couple $(c-x, H(c))$. Cette donnée est stockée, le reste est effacé. A la fin de cette étape, le système authentifiera comme étant **U** tout utilisateur capable de produire une empreinte biométrique permettant de retrouver le mot de code **c**.

— **Authentification :** Supposons qu'un utilisateur se présente sous l'identité de **U** et que son signal biométrique courant soit **x'**. Le système utilise **x'** pour vérifier l'engagement $(c-x, H(c))$. Pour cela,il faut tout d'abord calculer $(c-x)+x'$. Si l'utilisateur était bien celui qu'il prétend être, alors son empreinte biométrique courante **x'** devrait être proche de son empreinte biométrique de référence **x** et par voie de conséquence $(c-x)+x'$ devrait être proche de **c**, au sens de la métrique de Hamming.Si la distance entre $(c-x)+x'$ et **c** est inférieure à la distance du code, alors le mot de code **c'**, le plus proche de $(c-x)+x'$ est égal à **c**. Pour cela, il suffit de vérifier que $H(c') = H(c)$ où **c'** est le mot de code le plus proche de $(c-x)+x'$.

2.2.3.2 Fuzz vault

Les auteurs proposent une méthode appelée fuzzy vault[26]. L'authentification d'un utilisateur repose, là encore, sur sa capacité à présenter une donnée biométrique permettant de retrouver un secret, le secret en question est un polynôme **P** de degré **n**. Lors de l'étape d'enrôlement, le système calcule un fuzzy vault **V** , littéralement coffre fort flou, à partir de **P** et de l'ensemble des minuties de l'empreinte de l'utilisateur. L'utilisateur est authentifié lorsqu'il est possible de retrouver **P** à partir de **V** et des minuties apparaissant dans son empreinte courante(**Figure 2.4**).

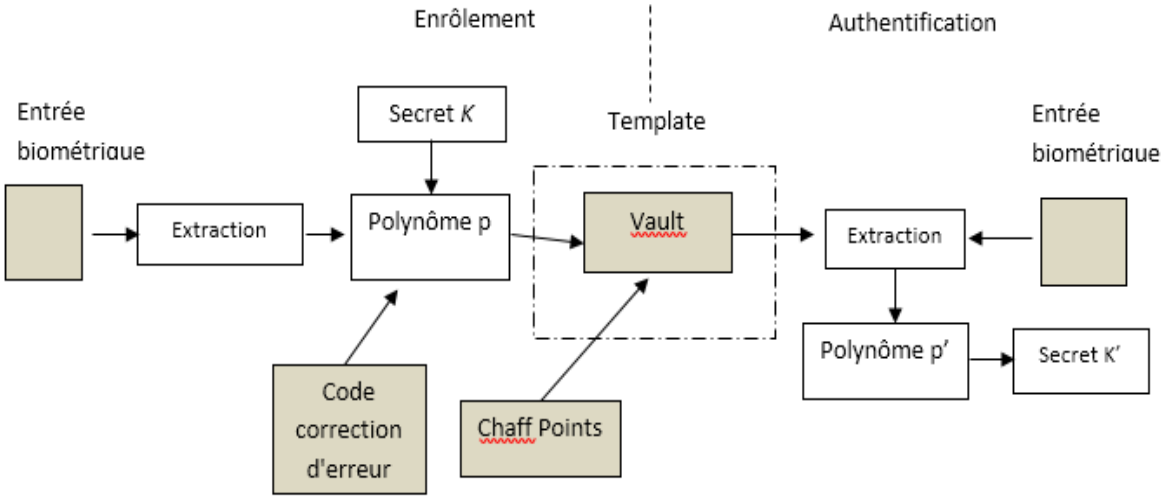


FIGURE 2.4 – Schéma de fuzzy vault.
[31]

Plus précisément, l'algorithme de Juels et Sudan peut se présenter comme suit :

— **Enrôlement :** Considérons un utilisateur **U**, l'ensemble des minuties $\{a_i\}_{1\leqslant i\leqslant t}$ apparaissant dans l'image de son empreinte digitale et un polynôme **P** de degré **k** où $t > k$. Nous calculons tout d'abord l'ensemble des points $R_1 = \{(a_i, P(a_i)\}_{1\leq i\leq t}$. Nous générons ensuite un second ensemble de points $R2 = \{(x_j, y_j\}_{1\leq j\leq n}$ tels que $x_j \neq a_i$ et $y_j \neq P(a_i)$ pour tout $1 \preceq i \preceq t$ et tout $1 \preceq j \preceq n$. L'ensemble R_2 est destiné à brouiller l'information venant de R_1. Le coffre-fort flou de l'utilisateur **U** est l'ensemble $V_U = R_1 \cup R_2$. Cet ensemble est rendu publique, le reste est effacé.

— **Authentification :** Lorsqu'un utilisateur souhaite s'authentifier en temps que **U**, il présente son empreinte digitale et nous extrayons l'ensemble des minuties $\{b_i\}_{1\preceq i\preceq t'}$ de l'image acquise. Nous sélectionnons ensuite dans V_U l'ensemble des points de la forme (x, y) où x est proche d'une valeur b_i. Si l'empreinte proposée est suffisamment proche de l'empreinte de l'utilisateur **U** alors ce procédé, un cryptosystème biométrique pour l'authentification permet de retrouver suffisamment de points de R_1 pour pouvoir reconstruire **P** par interpolation de Lagrange. Si c'est le cas, l'utilisateur est authentifié en tant que **U**.

2.2.3.3 Schémas de Quantization

Au sein de ce groupe de schémas, les données auxiliaires sont construites de manière à aider à quantifier les caractéristiques biométriques afin d'obtenir des clés stables(**Figure 2.5**).

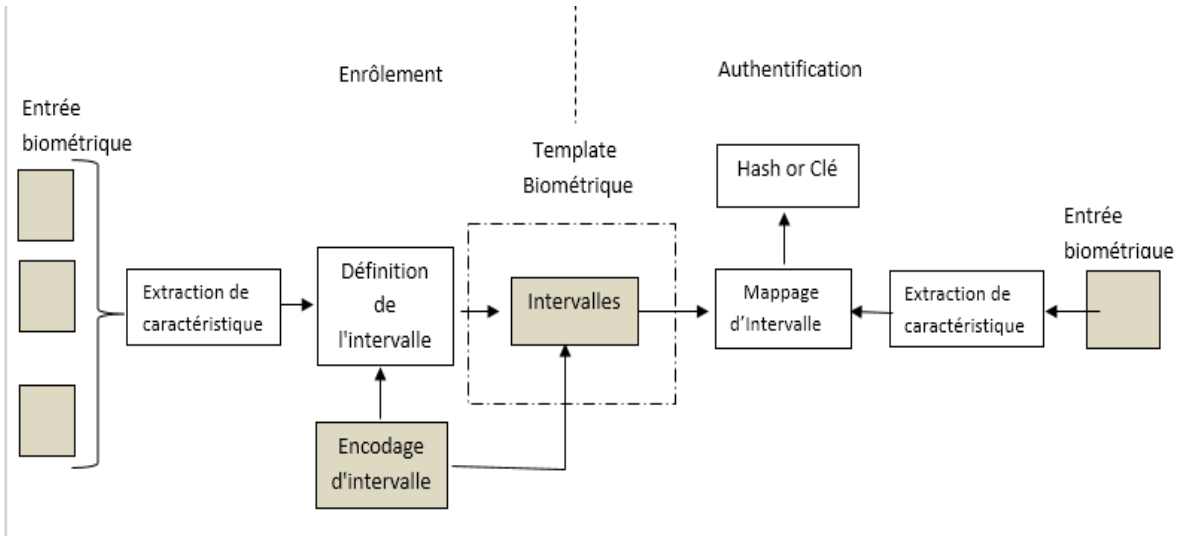


FIGURE 2.5 – Schéma de Quantization proposée.

Mode de fonctionnement :
dans le schéma[27] de quantification généraux, qui ont été appliqués aux caractéristiques biométriques physiologiques et comportementales, traiter les vecteurs de caractéristiques à partir de plusieurs échantillons de recrutement et dérivez des intervalles appropriés pour chaque élément de caractéristique (des vecteurs de caractéristiques à valeur réelle sont nécessaires). Ces intervalles sont codés et stockés en tant que données d'assistance. Au moment de l'authentification, là encore, les caractéristiques biométriques d'un sujet sont mesurées et mappées dans les intervalles précédemment définis, générant un hachage ou une clé. Afin de fournir des clés ou des hachages pouvant être mis à jour, la plupart des schémas fournissent un codage paramétré des intervalles.

2.2.3.4 Méthode cryptosystème biométrique basé sur les minuties voisinages

est une technique qui utilise les informations de localisation des points de minutie pour construire un modèle hautement sécurisé pour un utilisateur. Pour chaque point de minutie, un emplacement modifié sécurisé est généré en utilisant les informations de ses minuties voisines et un jeu de clés. Nous allons détaillées les étapes de cette méthode dans la section suivants.

2.2.4 Avantage des cryptosystèmes biométriques

Les cryptosystèmes biométriques offrent plusieurs avantages par rapport aux systèmes biométriques[19] conventionnels. Les principaux avantages peuvent être résumés comme suit :

— **Protection du gabarit :** dans les systèmes cryptographiques biométriques, le gabarit biométrique d'origine est masqué de sorte qu'une reconstruction est difficilement réalisable.

— **Libération de clé dépendante de la biométrie :** les cryptosystèmes biométriques fournissent des mécanismes de libération de clé basés sur la présentation de données biométriques.
— **Révocabilité des modèles biométriques :** plusieurs instances de modèles sécurisés peuvent être générées en liant ou en générant différentes clés.
— **Sécurité accrue :** les cryptosystèmes biométriques empêchent plusieurs types traditionnels d'attaques contre les systèmes biométriques (par exemple, les attaques de substitution).
— **Meilleure acceptation sociale :** en raison des avantages de sécurité mentionnés ci-dessus, l 'acceptation sociale des applications biométriques devrait augmenter.

2.3 Méthode de cryptosystème biométrique basé sur les minuties voisinages

Pour disposer un système d'authentification d'empreintes digitales hautement sécurisé, nous besoin de générer un modèle sécurisé pour un utilisateur. En utilisant les données extrait de l'empreinte digitale de l'utilisateur, un modèle sécurisé est généré et stocké dans la base de données, qui est également utilisée pour l'authentification. Parmi diverses fonctionnalités d'empreintes digitales, la technique utilise des points singuliers et des informations de points de minuties pour construire un modèle utilisateur sécurisé, à l'aide d'un jeu de clés utilisateur p_0, q_0, r_0.[23]
Comme représenter à la **La figure 2.6**, notre Schéma est composé de quatre étapes :

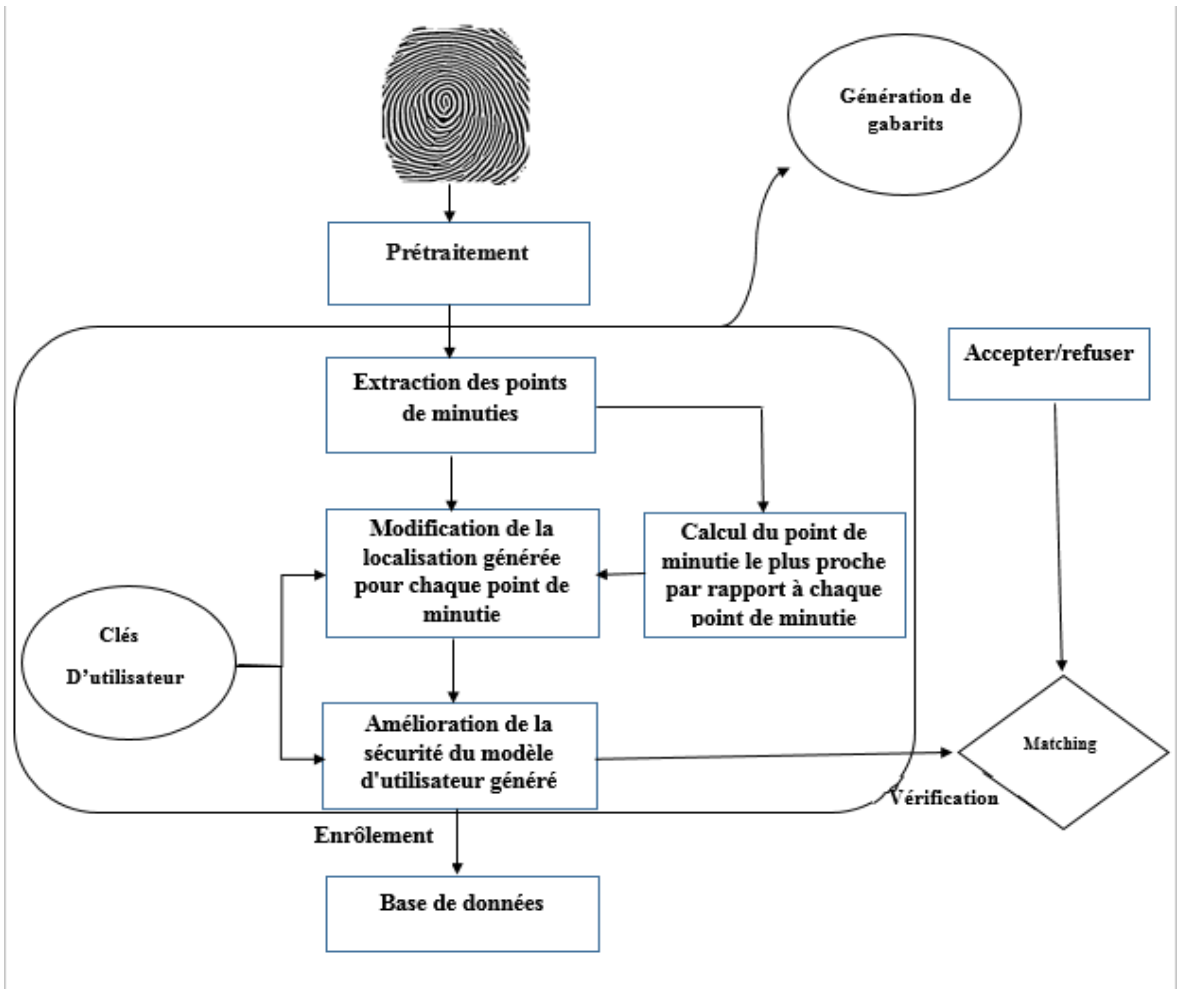


FIGURE 2.6 – Datagrame des étapes de la technique proposée.

2.3.1 Prétraitement

Initialement, l'empreinte digitale est capturée à l'aide de capteurs. Pour améliorer la qualité d'image nous utilisons le filtre de Gabor. Ce dernier est une opération de traitement d'images numériques qui consiste à appliquer des opérateurs afin de faire des transformations sur toute l'image ou à une partie d'elle pour améliorer la qualité visuelle de cette dernière.[24](**Figure 2.7**)

$G(x, y, \theta, f) = e^{-\frac{1}{2}(\frac{x_\theta^2}{\sigma_x^2}) + (\frac{y_\theta^2}{\sigma_y^2})}\cos(2\pi f x_\theta)$

avec : $x_\theta = \text{x } \cos\theta + \text{y } \sin\theta$

et : $y_\theta = \text{ycos}\theta + \text{xsin}\theta$

où θ est l'orientation de la sinusoïde, f sa fréquence et σ_x (respectivement σ_y) l'écart type de la gaussienne selon l'axe des abscisses.

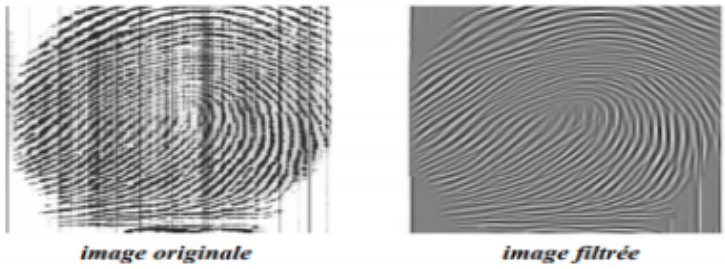


FIGURE 2.7 – Le résultat obtenu après le pré-traitement.

2.3.2 Extraction de points des minuties

A partir de l'image filtrée, sont extraites de diverses informations présentes dans l'empreinte digitale, nous avons vu dans le chapitre 1, l'extraction des minuties.(**figure 2.8**).

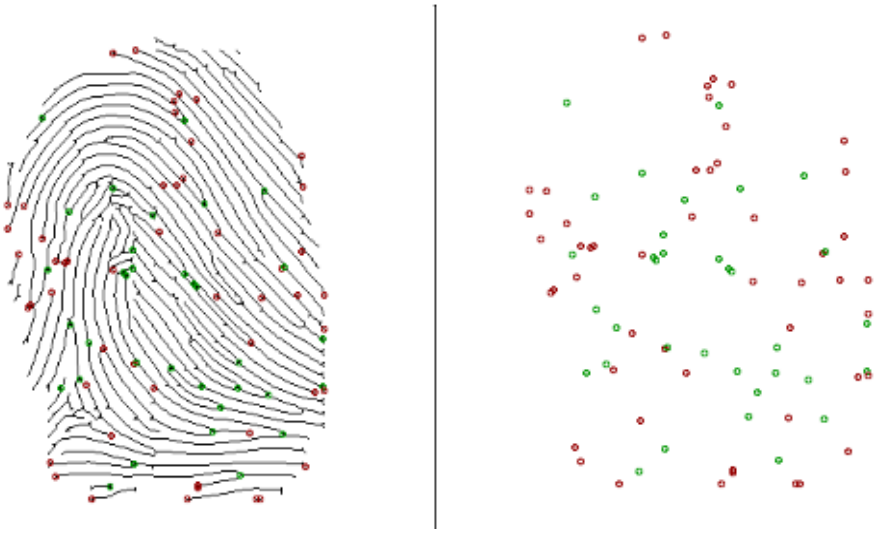


FIGURE 2.8 – Résultat de l'extraction de points des minuties.

2.3.3 Génération de modèles sécurisés(gabarit)

Les emplacements des points de minutie et leur orientation sont aléatoires. Habituellement, le modèle utilisateur est directement stocké dans la base de données dans la forme des points de minutie avec leurs attributs (tels que l'emplacement, type et orientation). L'empreinte digitale originale d'un utilisateur peut être reconstruite. Donc pour éviter cela au lieu de stocker directement les points de minutie avec leurs attributs, la technique proposée stocke les emplacements modifiés de points de minuties. Ces emplacements modifiés sont obtenus par modifier l'emplacement d'origine des points de minuties à l'aide d'un jeu de clés utilisateur ainsi qu'en utilisant l'emplacement des minuties voisines points (Ce processus est décrit dans le cadre de l'algorithme 1 (**La figure 2.9**) de l'étape 5 à l'étape 22.).

1: **Input:** *Minutiae points locations* (x_1, y_1), (x_2, y_2), ..., (x_n, y_n) *and key-set* $\{p_0, q_0, r_0\}$
2: **Output:** *secured user template (UT)*
3: /* *Computation of key* s_0 *for user template security enhancement* */
4: $s_0 = \lfloor p_0 \rfloor + \lfloor q_0 \rfloor \times (2^{16}) + \lfloor r_0 \rfloor \times (2^{32})$
5: /* *Secured template generation, from step 6 to step 22* */
6: **for** $i = 1$ to n **do**
7: $\quad dis_i = \infty$
8: $\quad$ **for** $k = 1$ to n **do**
9: $\quad\quad$ **if** $i \neq k$ **then**
10: $\quad\quad\quad dis = \sqrt{(x_i - x_k)^2 + (y_i - y_k)^2}$
11: $\quad\quad\quad$ **if** $dis_i > dis$ **then**
12: $\quad\quad\quad\quad dis_i = dis$
13: $\quad\quad\quad\quad j = k$
14: $\quad\quad\quad$ **end if**
15: $\quad\quad$ **end if**
16: $\quad$ **end for**
17: $\quad$ /* *Computation of modified locations* */
18: $\quad x'_i = x_i + (p_0 \times \cos(q_0 + tan^{-1}(\frac{y_i - y_j}{x_i - x_j})))$
19: $\quad y'_i = y_i + (p_0 \times \sin(q_0 + tan^{-1}(\frac{y_i - y_j}{x_i - x_j})))$
20: $\quad$ /* *Reducing translation due to intra-subject variance* */
21: $\quad x'_i = x'_i - x_{sing}$
22: $\quad y'_i = y'_i - y_{sing}$
23: $\quad$ /* *Security enhancement of the user template* */
24: $\quad \begin{bmatrix} x'_i \\ y'_i \end{bmatrix} = \begin{bmatrix} cos(r_0) & -sin(r_0) \\ sin(r_0) & cos(r_0) \end{bmatrix} \times \begin{bmatrix} x'_i \\ y'_i \end{bmatrix}$
25: $\quad x'_i = x'_i + (s_0 \times \cos(r_0))$
26: $\quad y'_i = y'_i + (s_0 \times \sin(r_0))$
27: **end for**
28: /* *abscissae of the secured user template* */
29: $UT(1, :) = \{x'_1, x'_2, ..., x'_n\}$
30: /* *ordinates of the secured user template* */
31: $UT(2, :) = \{y'_1, y'_2, ..., y'_n\}$

FIGURE 2.9 – Algorithme 1 : Calcul du modèle utilisateur sécurisé

Supposons qu'il y ait n points de minutie obtenus à partir d'une empreinte digitale, $m_i = \{x_i, y_i, \theta_i, type_i\}$, où x_i est la valeur en abscisse, y_i est la valeur ordonnée, θ_i est la valeur d'orientation, et $type_i$ représente le type de minutie (bifurcation de crête ou début / fin de crête). Pour générer les emplacements modifiés d'un point de minutie m_i, la technique proposée utilise uniquement l'emplacement d'un point de minutie (valeur d'abscisse x_i et ordonnée y_i).

Pour un point de minutie m_i, soit m_j (valeur d'abscisse x_j et valeur d'ordonnée y_j) le point de minutie le plus proche au point de minutie m_i, maintenant en utilisant les clé utilisateur q_0 et p_0 et le point de minutie m_j, pour modifier l'emplacement m_i. Comme montre la **figure 2.10**, un emplacement modifié correspondant à un point de minutie m_i est généré en calculant x'_i et y'_i. Les valeurs de x'_i et y'_i sont obtenues à partir de l'emplacement d'origine du point de minutie m_i (x_i, y_i) et m_j (x_j, y_j) à l'aide de p_0 et q_0. les valeurs x'_i et les valeurs y'_i sont

calculées comme suit :

$$x'_i = x_i + (P_0 \times \cos(q_0 + \tan^{-}1\frac{y_i - y_j}{x_i - x_j})) \tag{2.1}$$

$$y'_i = y'_i + (P_0 \times \sin(q_0 + \tan^{-}1\frac{y_i - y_j}{x_i - x_j})) \tag{2.2}$$

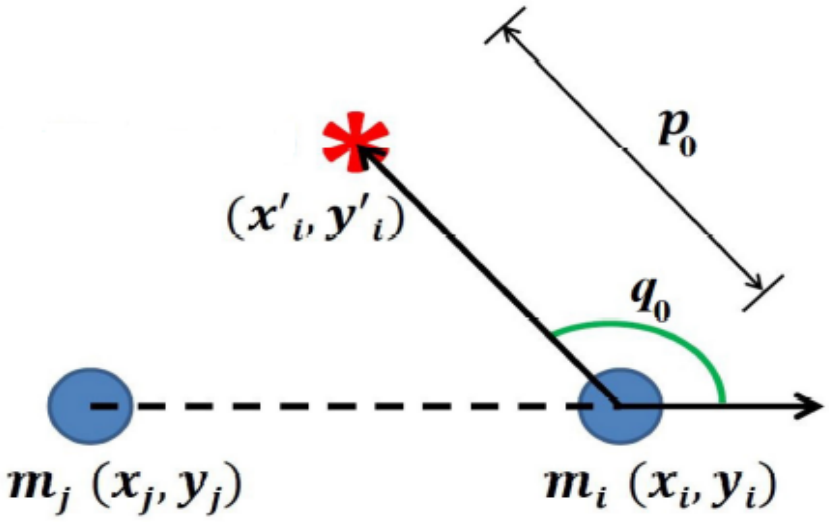


FIGURE 2.10 – Génération d'un emplacement modifié m_i avec m_j le plus proche à l'aide des touches utilisateur p_0 et q_0.

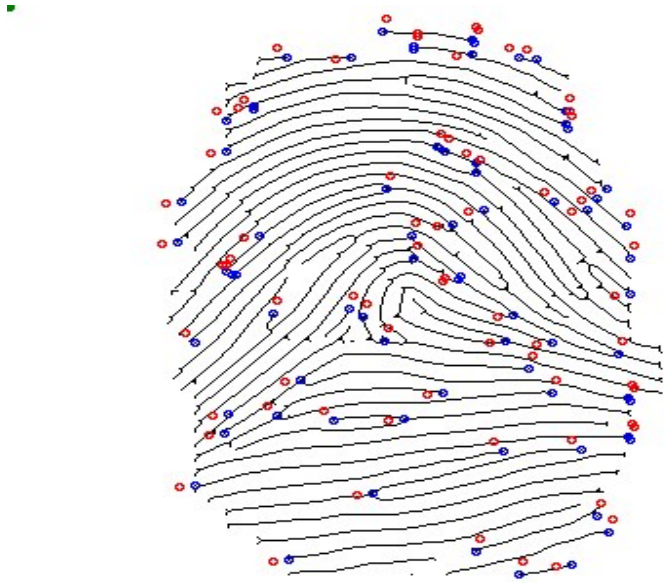


FIGURE 2.11 – les emplacements modifiés pour les points de minutie d'un empreinte digitale.

En raison de la variance intra-sujet, il existe un problème de traduction. Pour réduire les effets de la traduction, on utilise l'emplacement du point singulier (x_{sing} étant la valeur

d'abscisse et y_{sing} la valeur d'ordonnée d'un point singulier). Tous les emplacements modifiés des points de minuties sont traduits de telle sorte que l'emplacement du point singulier devienne l'origine (**La figure 2.12** a et b).
Cela se fait de la manière suivante :

$$x'_i = x'_i - x_{sing} \tag{2.3}$$

$$y'_i = y'_i - y_{sing} \tag{2.4}$$

Pour chaque point singulier présent dans une empreinte digitale, un ensemble des emplacements modifiés correspondants des points de minuties sont générés. En d'autres termes, on peut dire que pour chaque point singulier d'une empreinte digitale, un modèle d'utilisateur est généré et enregistré dans une base de données lors du processus d'enregistrement. Au moment de la vérification, tous ces modèles sont comparés avec le modèle de requête.

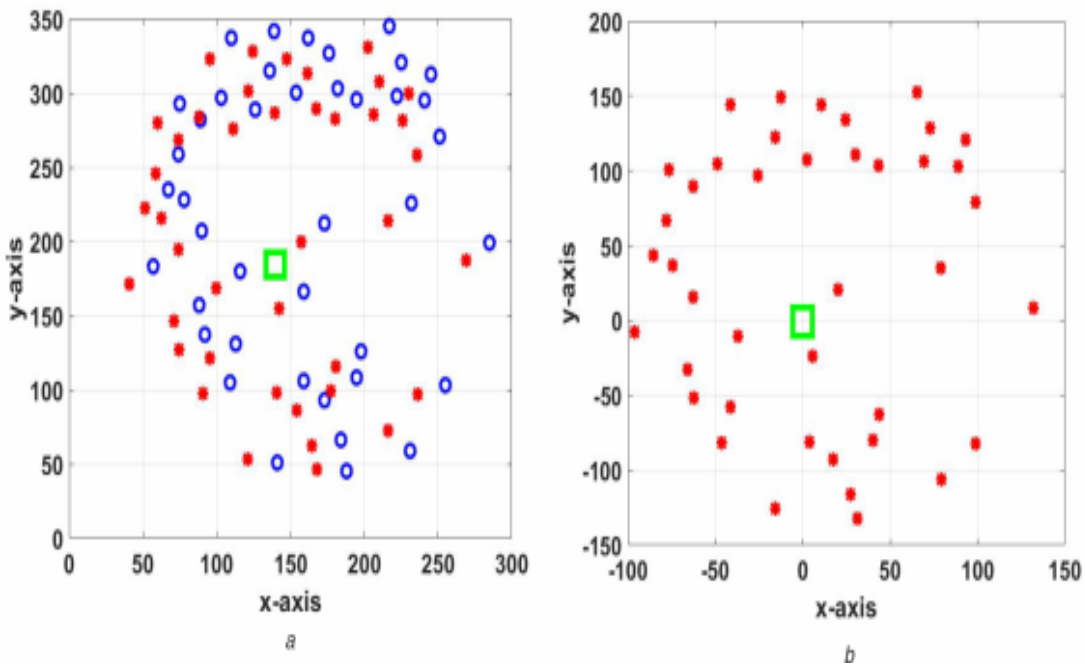


FIGURE 2.12 – les emplacements modifiés pour les points de minutie d'un empreinte digitale.

Amélioration de la sécurité du modèle utilisateur généré Le modèle d'utilisateur sécurisé généré à la dernière étape est encore amélioré en utilisant r_0 et s_0.
s_0 est un entier de 48 bits généré à l'aide de valeurs intégrales de p_0, q_0 et r_0 :

— les 16 premiers bits (à partir du bit le moins significatif) sont des valeurs intégrales de p_0.
— du 17 au 32 bits (à partir des bits les moins significatifs) sont des valeurs intégrales de q_0 .
— les 16 derniers bits (du bit le moins significatif) sont des valeurs intégrales de r_0.

comme le montre **la figure 2.13**. Tous les emplacements modifiés sont tournés de l'angle de r_0 par rapport à l'origine, puis traduits par des unités s_0 à partir de l'origine, ce qui fait un angle r_0 par rapport à l'axe des abscisses.

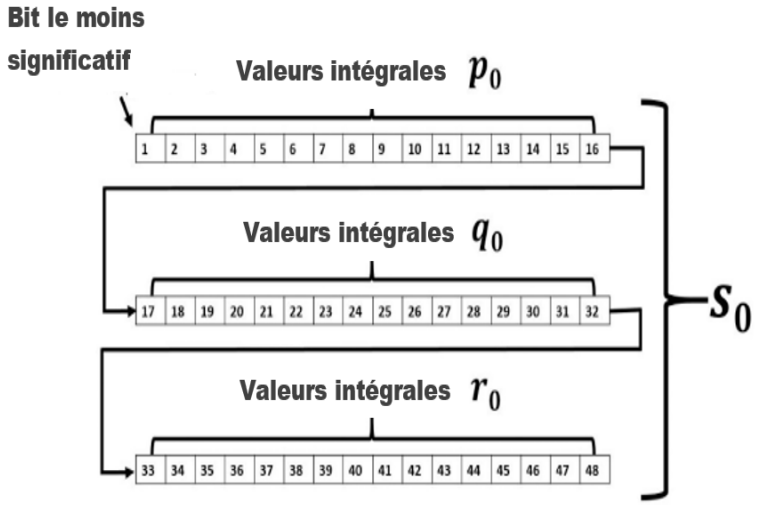


FIGURE 2.13 – Calcul de la clé s_0 de 48 bits en utilisant p_0, q_0 et r_0.

les valeurs des abscisses des emplacements modifiés sont augmentées de $s_0 \times cos(r_0)$ et la valeur des ordonnées de $s_0 \times sin(r_0)$.les emplacements sont les suivants :

$$S_0 = \lfloor p_0 \rfloor + \lfloor q_0 \rfloor \times (2^{16}) + \lfloor r_0 \rfloor \times (2^{32}) \tag{2.5}$$

$$x'_i = x'_i + (s_0 \times \cos(r_0)) \tag{2.6}$$

$$y'_i = y'_i + (s_0 \times \sin(r_0)) \tag{2.7}$$

Enfin, ces emplacements modifiés et améliorés de sécurité généré à l'aide d'attributs de points de minutie, de point singulier et le jeu de clés d'utilisateurs sont stockés dans la base de données en tant que modèle utilisateur pour la vérification d'un utilisateur à l'avenir.

2.3.4 Comparaison

Le point singulier qui est présent à l'endroit le plus proche par rapport au centre d'une image d'empreinte digitale de requête est sélectionné, et en l'utilisant, un seul modèle d'utilisateur est construit au moment de la vérification.
Ce gabarit est comparé à tous les gabarits qui sont présents dans la base de données par la distance Hausdorff
tel que : $s^{(1)} = s_1^{(1)}, s_2^{(1)}, .., s_n^{(1)}$ et $s^{(2)} = s_1^{(2)}, s_2^{(2)}, .., s_m^{(2)}$ être deux signatures, la distance de Hausdorff est défini comme :

$H_d(s^{(1)}, s^{(2)}) = max\{max\{d(n, s^{(2)}) : n \in s^{(1)}\}, max\{d(m, s^{(1)}) : m \in s^{(2)}\}\}$
où $d(n, s^{(1)}) = min\{d(n, m) : m \in s^{(1)}\}$

2.4 Conclusion

Dans ce chapitre nous avons vue les cryptosystèmes biométriques et ses méthodes, ainsi ses avantages ensuite nous avons détaillé les différents principes et étapes de la méthode proposée, qui utilise les informations de localisation des points de minuties pour construire un modèle hautement sécurisé. La performance de la méthode proposée est évaluée en l'appliquant sur une base de donnée, où les résultats obtenus seront analyser, chose qui sera abordé dans le chapitre suivant.

Chapitre 3

Tests et résultats expérimentaux

3.1 Introduction

Après avoir présenté dans le chapitre précédent les différentes étapes de la conception de la méthode proposée "Cryptosystème biométrique basé sur les minuties voisinages", nous présentons dans ce chapitre un aperçu général sur la phase pratique de notre travail.
Le but de ce projet est de construire pour la sécurisation de notre base de données d'empreinte digitale en appliquant certaine manipulation acceptable comme la rotation, le bruit, nous mettons en évidence les raisons de nos choix technique, les testes sur l'application et les résultats obtenue
Nous résumons cette mise en ouvre en trois parties :

- Environnement de développement
- Présentation l'application
- Tests et évaluation

3.2 Environnement de développement

3.2.1 Matériel

Nous avons utilisés deux machines avec les caractéristiques suivantes :

Caractéristiques	**Machine1**	**Machine2**
Processeur	1.80 GHz Intel core i3-CPU	2.40 GHz Intel core i5-6200U
RAM	3.00 GO	400 GO
Carte graphique	Intel(R) HD Graphics 4000	Intel(R) HD Graphics 4000
Système d'exploitation	Windows 7 64 Bits	Windows 7 64 Bits

Table 3.1 – Caractéristiques des machines utilisés

3.2.2 Software

L'environnement logiciel utilisé pour la réalisation de notre application est : Python

FIGURE 3.1 – Logo Python

Nous avons utilisés la version Python 2.7 comme langage de programmation, parmi les raisons de cette utilisation :

— Python fonctionne sur différentes plateformes (Windows, Mac, Linux).
— Il a une syntaxe simple claire, respecte les standards du domaine. Similaire a la langue anglaise.
— langage peut être traite de manière procédurale, de manière orientée objet ou de manière fonctionnelle.

Modules et bibliothèques Une bibliothèque est une ensemble de fonctions. Elles sont regroupées et mises à disposition afin de pouvoir être utilisées sans avoir à les réécrire.
Celles-ci permettent de faire : du calcul numérique, du graphisme, de la programmation internet ou réseau, du formatage de texte, de la génération de documents...
Parmi les différentes bibliothèques utilisés dans notre application :

Module PIL :
La bibliothèque PIL (Python Imaging Librairie) permet la manipulation de tout type d'images et fournit quelques fonctions de traitement d'images de base.

Numpy :
Numpy est une bibliothèque numérique apportant le support efficace de larges tableaux multidimensionnels, et de routines mathématiques de haut niveau.

OpenCV :
Cette bibliothèque permet de manipuler les structures de base, réaliser des opérations sur des matrices, dessiner sur des images, sauvegarder et charger des données.

Matplotlib :
Matplotlib est une bibliothèque destinée à tracer et visualiser des données sous formes de graphiques.

TKinter :
Tkinter (de l'anglais Tool kit interface) est la bibliothèque graphique libre d'origine pour le

langage Python, permettant la création d'interfaces graphiques. Elle vient d'une adaptation de la bibliothèque graphique Tk écrite pour Tcl.

SciPy :

La librairie SciPy contient de nombreuses boites à outils consacrées aux méthodes de calcul scientifique. Ses différents sous-modules correspondent à différentes applications scientifiques, comme les méthodes d'interpolation, d'intégration, d'optimisation, de traitement d'image, de statistiques, de fonctions mathématiques spéciales, etc.

os :

fonctions permettant d'interagir avec le système d'exploitation.

math

toutes les fonctions utiles pour les opérations mathématiques (cosinus,sinus,exp, etc.).

random :

Des fonctions permettant de travailler avec des valeurs aléatoires.

3.3 Présentation de l'application

Le but de notre travail est de tester la performance de notre algorithme (cryptosystème biométrique basé sur les minuties voisinages) contre quelques attaques acceptables, sur une base d'image d'empreinte digitale, nous pouvons mesurer la performance de cet algorithme.

3.3.1 Base de donnée utilisée

Pour évaluer la méthode proposée dans ce mémoire nous l'avons appliqué sur certain images (80 images) de la base FVC 2002, la résolution de ces images est (388×374) ainsi que son format est TIFF. Il existe dans cette base de données huit échantillons par doigt ce qui permet aux algorithmes de comprendre les variations entre les doigts correspondants. La **figure 3.2** suivante montre une partie de cette base de données :

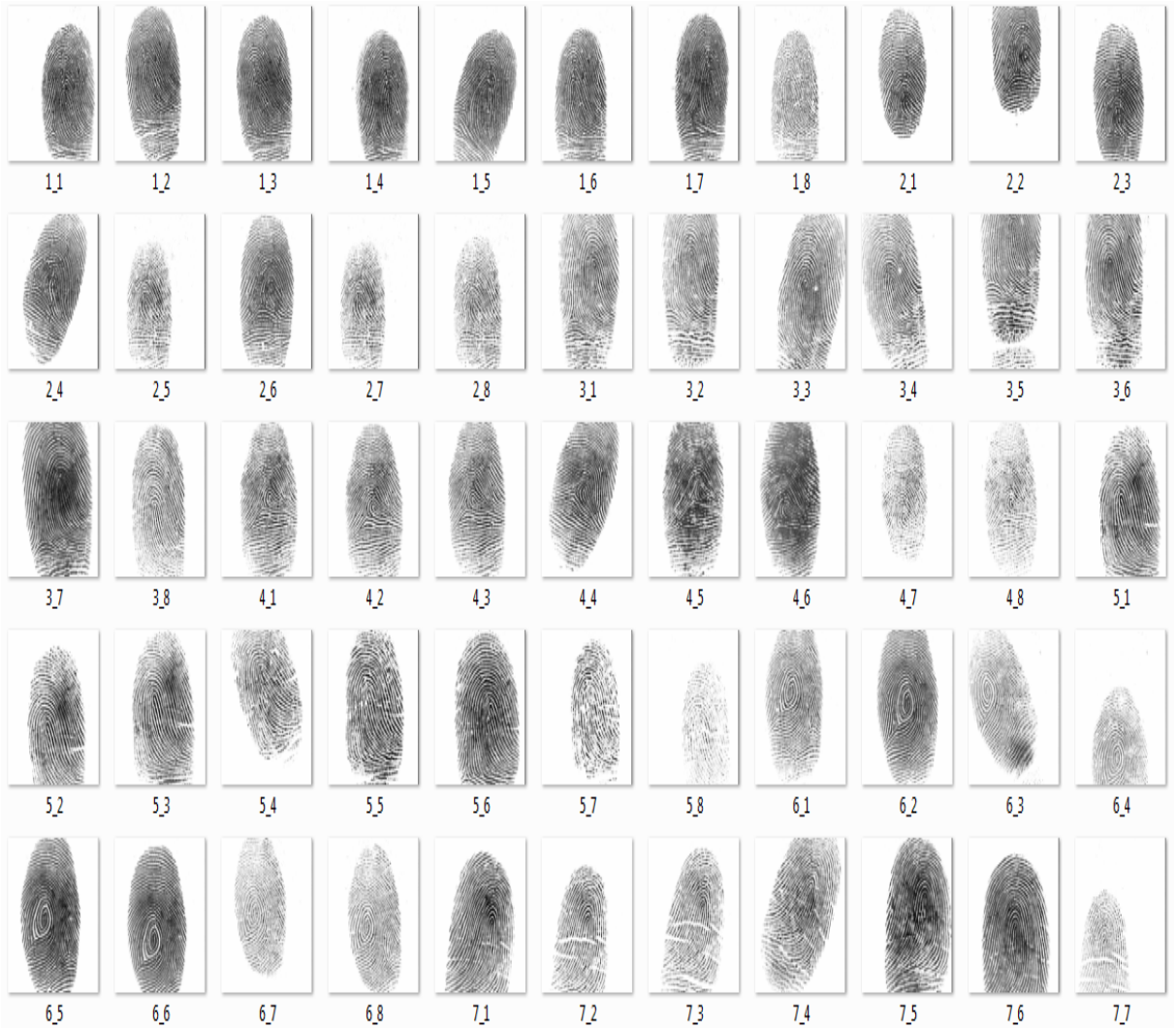


FIGURE 3.2 – Une partie de la base de données utilisée

3.3.2 Les attaques acceptables utilisés

Nous appliquons quelques manipulations acceptables tel que la rotation, shearing, la compression, bruits gaussien et scaling. Le **tableau 3.2** montre les paramètres de chaque attaque :

Attaque	Paramètre
Scaling	**0.5** 0.7 1 1.2 1.5
Rotation	**5** ±10 ±15 ±30 ±45 ±90
Shearing	0.01 0.03 **0.05** 0.07 0.09
Compression JPEG	**10** 20 30 40 50 60 70 80 90
Bruit Gaussien	0.001 **0.005** 0.010 0.015 0.020 0.025 0.030 0.035

TABLE 3.2 – Paramètre utilisé pour chaque manipulation

— Pour calculer le TPR et FPR, nous appliquons les attaques présentées dans le **tableau 3.2** sur la base d'image (80 empreintes), en utilisant le paramètre en gras pour chaque

attaque.

3.3.3 Interface graphique

Dans cette partie, nous allons présenter les différentes phases de la réalisation de notre projet, Après le lancement de l'application la fenêtre d'accueil s'affiche :

FIGURE 3.3 – La représentation de page d'accueil

l'interface graphique est composée de deux bouton comme illustre **la figure 3.3** Ci-dessus :

— **Le bouton Exit** :pour quitter l'application.

— **le bouton Next :** pour accéder à la page principale.

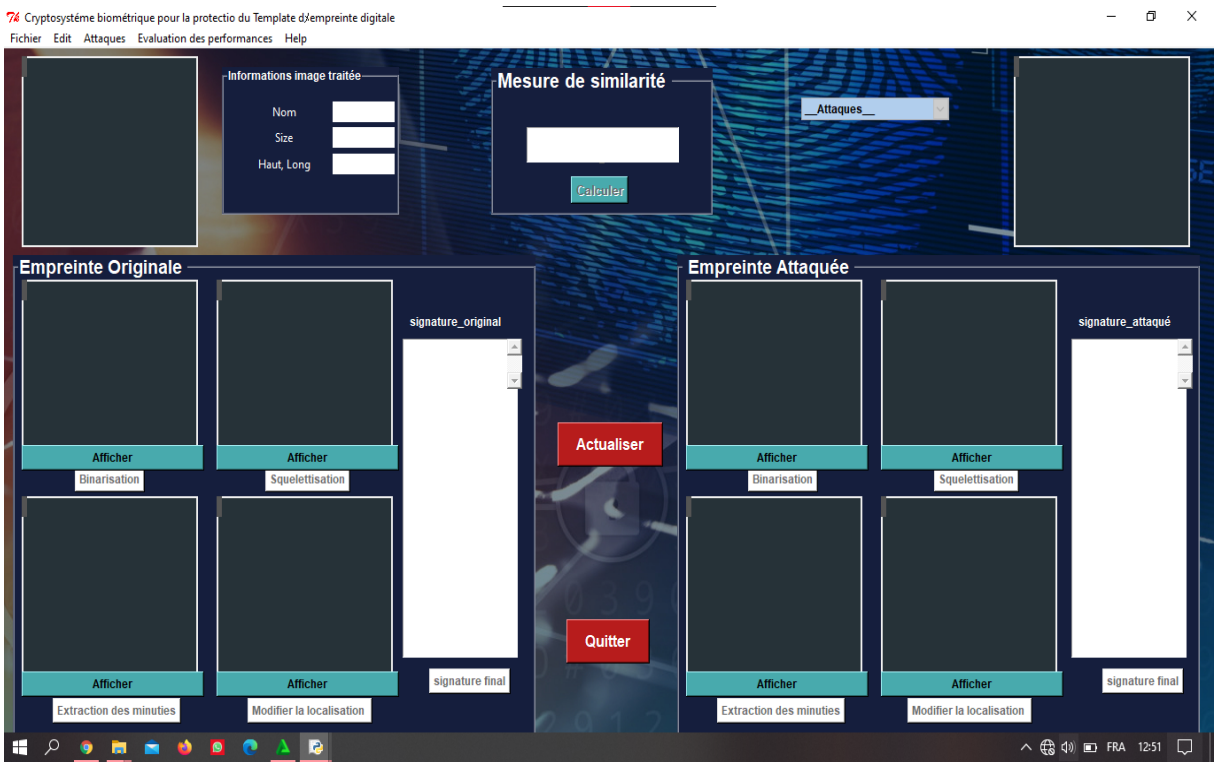


FIGURE 3.4 – La représentation de la page principale

La barre des menus de l'interface graphique (**Figure 3.4**) est contient :

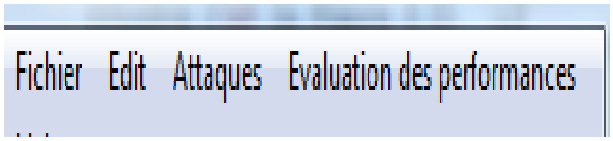


FIGURE 3.5 – La barre de menus de la page principale

- **Ficher :** contient Ouvrir image originale (permet d'ouvrir une image pour la traité), Réinitialiser et Fermer.
- **Edit :** le menu Edit contient Actualiser et Supprimer.
- **Attaques :** le menu Attaques permet de choisir une attaque parmi les cinq attaques (Rotation,Shearing, Compression, Bruit gaussien, Scaling).
- Evaluation des performance :permet d'afficher une fenêtre, elle est décomposée sur deux pages pour la performance et le Taux.

FIGURE 3.6 – Fenêtre pour l'evaluation des performances

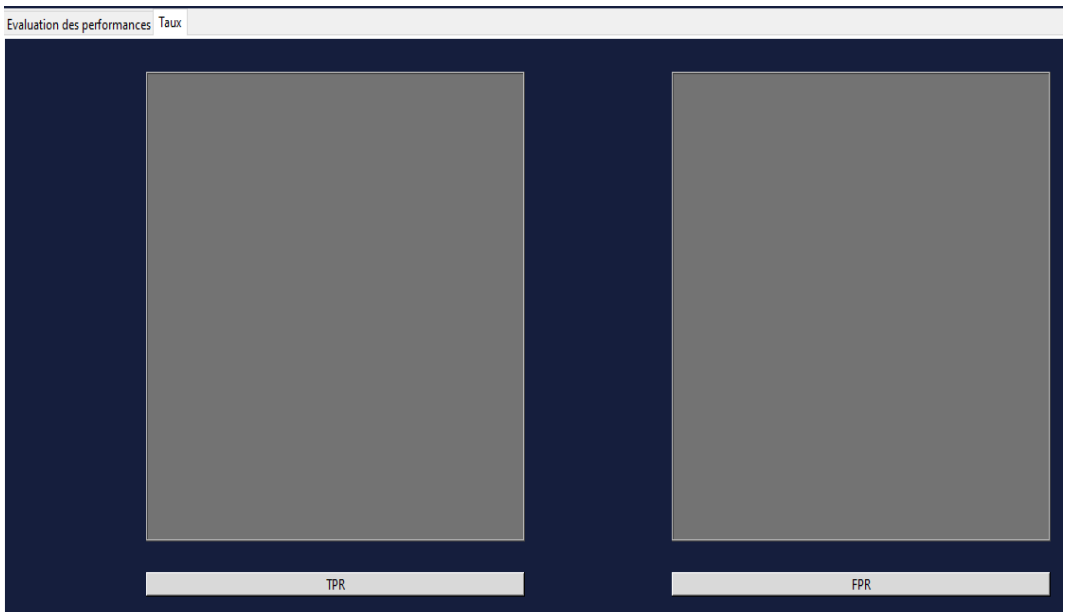


FIGURE 3.7 – Fenêtre pour l'evaluation des performances (Taux)

La **figure 3.8** montre les résultat obtenu de l'evaluation de performance :

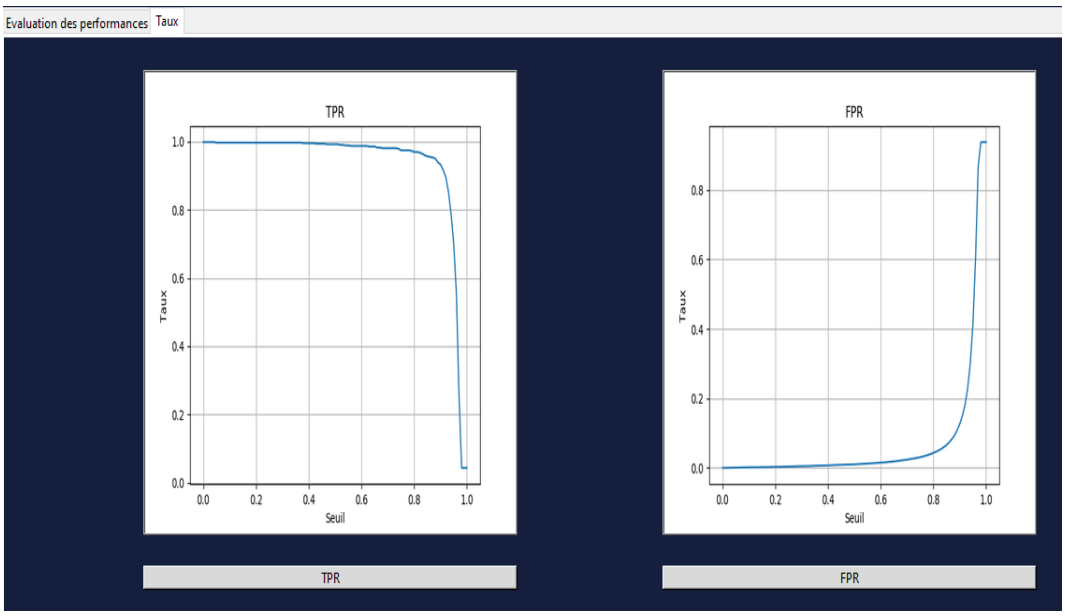


FIGURE 3.8 – Résultat de l'evaluation des performances

L'interface graphique (**figure 3.4**) est composée de trois parties (Empreinte originale, Empreinte attaquée, et mesure de similarité). Pour les deux premières étapes nous avons les boutons suivants :

— **Bouton Binarisation :** il sera actif que lorsque l'image originale est affichée pour la partie d'image originale, et lorsque l'attaque est choisi pour la partie d'image attaquée, il suffit de cliquer sur ce bouton pour obtenir l'image binarisée.
— **Bouton Squelettisation :** il sera actif que lorsque l'image binarisée est affichée, il suffit de cliquer sur ce bouton pour obtenir l'image squelattisée.
— **Bouton Extraction des minuties :** il suffit de cliquer sur ce bouton pour obtenir l'ensemble des minuties extraits.
— **Bouton décomposition :** il sera actif que lorsque les minuties sont extraits, il suffit de cliquer sur ce bouton pour obtenir la modification des minuties
— **Bouton Signature** : il sera actif que lorsque la est faite, il suffit de cliquer sur ce bouton pour obtenir la signature.
— **Bouton Afficher :** permet d'afficher les chaque image traité.

la **Figure3.8** montre les résultats obtenu les étapes de l'empreint original et attaqué.

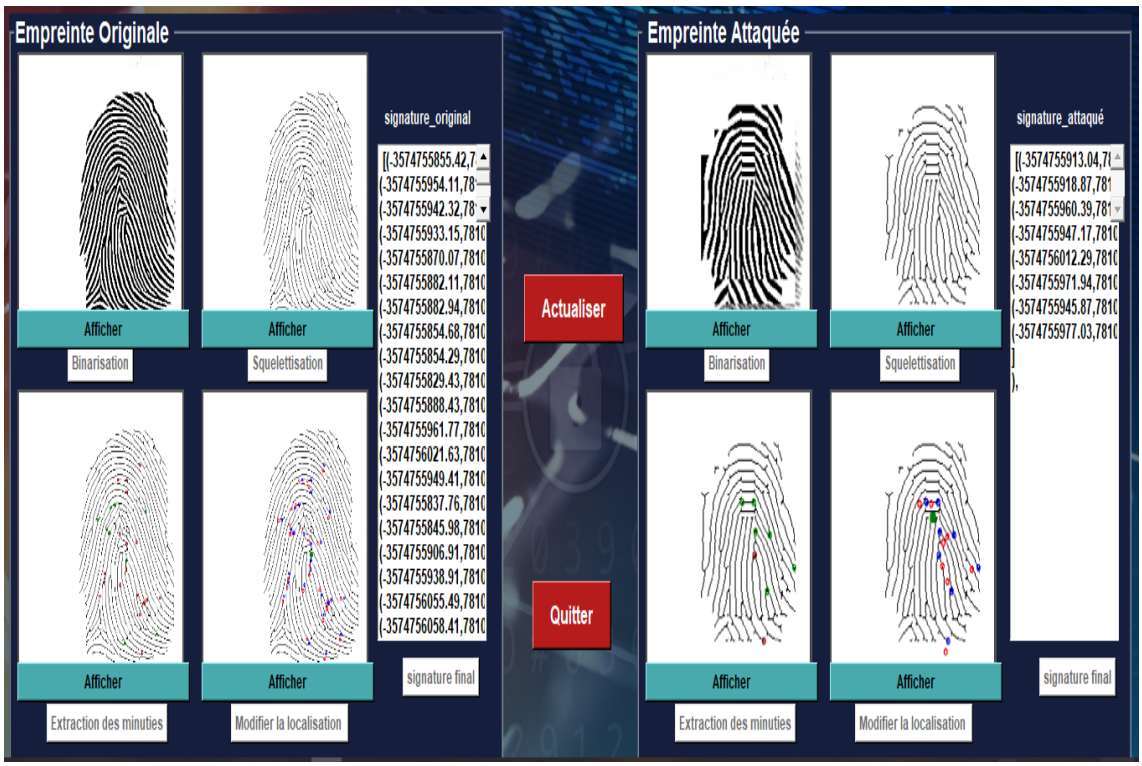


FIGURE 3.9 – le résultat obtenu de la la partie d'image originale et la partie d'image attaquée.

la partie trois de l'interface est la mesure de similarité pour calculer la distance entre la signature d'image originale et la signature attaqué, il suffit de cliquer sur le bouton calculer.

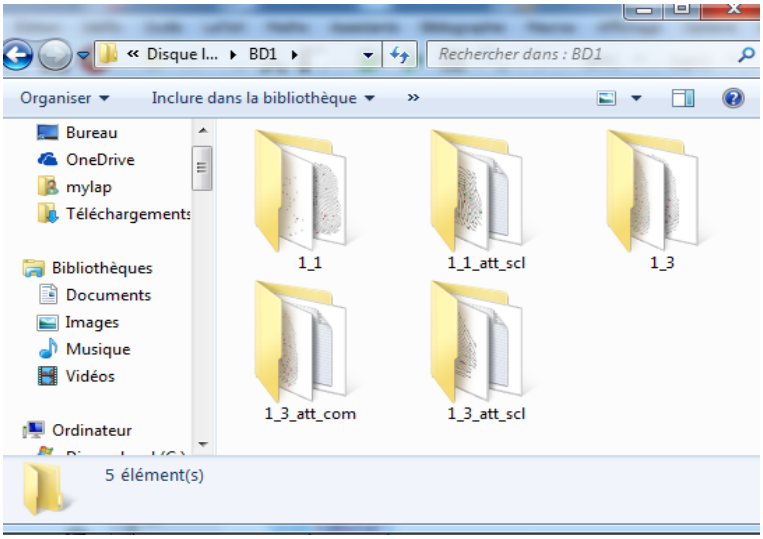


FIGURE 3.10 – Les résultats sauvegardés

3.4 Tests et évaluations

3.4.1 Evaluation des performances

Pour évaluer la performance de notre méthode contre les différentes manipulations acceptables et qui sont : la rotation, shearing, compression, bruit gaussien et scaling, nous calculons la mesure de similarité entre la signature de chaque image d'empreinte originale et sa signature attaqué, pour chaque paramètre d'attaque, ensuite nous calculons la moyenne de cette mesure. Notre teste est appliqué sur 80 images choisies de la base FVC2002, puis nous comparons les résultats avec notre seuil choisi (0.5).
Les résultat obtenus pour chaque attaque sont illustré dans les tableaux suivants :
Rotation :

Attaque	**Paramètre**	**Moyenne de Mesure**
Rotation	5	0.623
	10	0.589
	15	0.572
	30	0.5
	45	0.299
	90	0.501

TABLE 3.3 – La moyenne de similarité pour chaque paramètre de Rotation

Shearing :

Attaque	**Paramètre**	**Moyenne de Mesure**
Shearing	0.01	1.608
	0.03	1.042
	0.05	1.121
	0.07	1.197
	0.09	1.0764

TABLE 3.4 – La moyenne de similarité pour chaque paramètre de Shearing

Compression :

Attaque	Paramètre	Moyenne de Mesure
Compression	10	0.635
	20	0.642
	30	0.697
	40	0.671
	50	0.648
	60	0.671
	70	0.698
	80	0.697
	90	0.719

TABLE 3.5 – La moyenne de similarité pour chaque paramètre de Compression

Bruit Gaussien :

Attaque	Paramètre	Moyenne de Mesure
Bruit Gaussien	0.001	1.222
	0.005	0.972
	0.010	1.248
	0.015	1.139
	0.020	1.230
	0.025	1.172
	0.030	0.831
	0.035	1.260

TABLE 3.6 – La moyenne de similarité pour chaque paramètre de Bruit Gaussien

Scaling :

Attaque	Paramètre	Moyenne de Mesure
Scaling	0.5	0.351
	0.7	0.545
	1	0.598
	1.2	0.598
	1.5	0.421

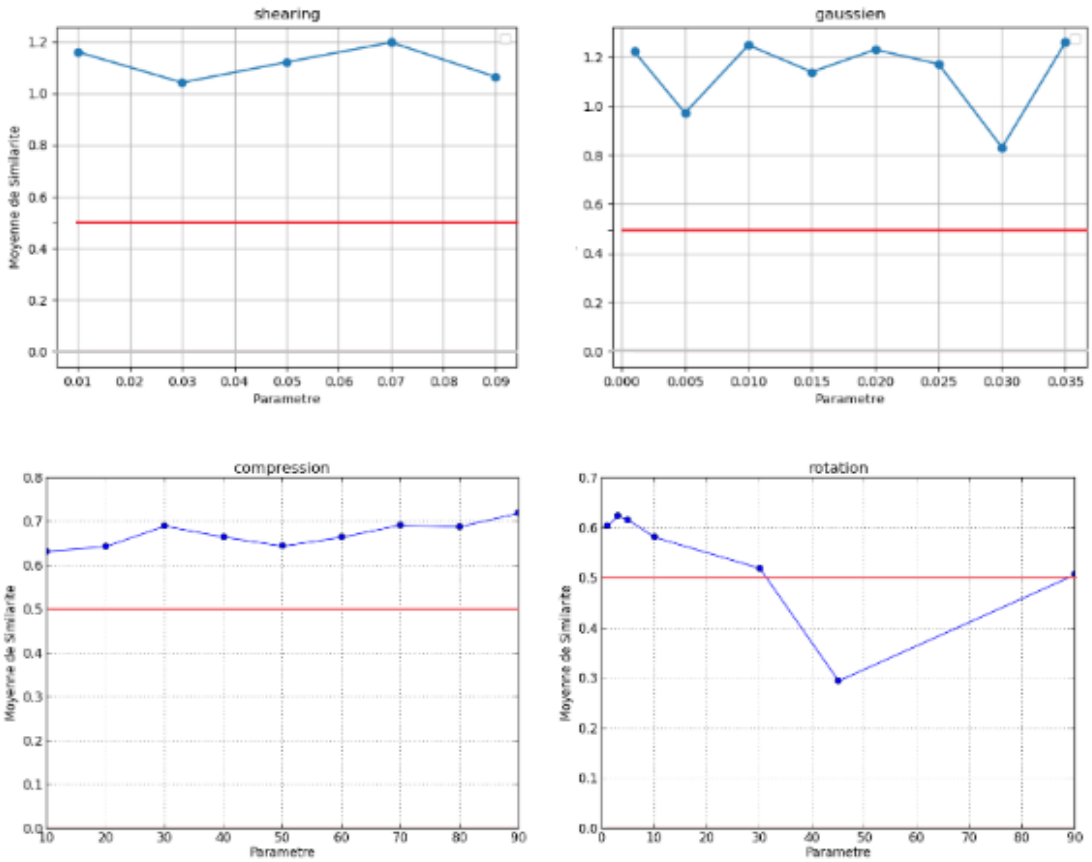
TABLE 3.7 – La moyenne de similarité pour chaque paramètre de Scaling

La moyenne de mesure de similarité générale pour toutes les attaques sont illustré dans le tableau suivant :

Attaque	**Moyenne global de similarité**
Rotation	0.505
Shearing	1.116
Compression	0.675
Bruit Gaussien	1.287
Scaling	0.502

TABLE 3.8 – La moyenne générale de la mesure de similarité pour chaque attaque.

Nous avons représentés les résultats sous forme des courbes. Les figures suivantes montrent les différentes courbes représentatives de la performance de notre méthode :



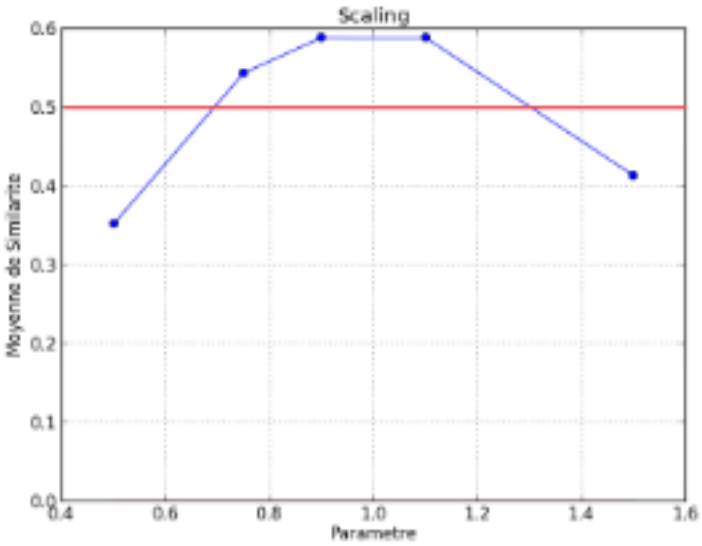


FIGURE 3.11 – Évaluation de performance par les différentes attaques.

Les résultats expérimentaux montrent que notre méthode est robuste, la moyenne de mesure de similarité calculée entre la signature des images originaux et la signature des images attaquées est supèrieure à 0.5 pour la totalité des manipulations, sauf dans le cas de la rotation 45, de scaling 0.5 et 1.5 ne donne pas des bons résultats (Moyenne de similarité 0.5), aussi la moyenne globale de mesure pour toutes les attaques est supérieure à 0.5. Donc la méthode proposée est robuste contre les attaques acceptables.

3.4.2 Sécurité

— **Le TPR (True positifs rate) :** pour calculer le TPR nous testons la mesure de similarité entre la signature de chaque image d'empreinte originale et les signatures de cette image avec un paramètre standard pour chaque attaque, donc nous calculons la distance entre la signature d'une image et les cinq signature manipulés de cette dernière, nous comparons le résultats avec certains seuils, dans ce cas nous obtenons le nombre de paire d'image visuellement identique considérées comme des images similaire (N similaire). Le nombre total de paires d'image visuellement identique est 400 (n identique).

— **Le FPR (False positifs rate) :** Pour calculer le FPR . Nous calculons la mesure de similarité entre la signature d'un échantillons d'empreinte original est les 72 signatures attaqués (nous ne comparons pas avec les échantillons de la même personne), les résultats obtenus nous lui comparons avec les différents seuils, nous obtenons le nombre de paires d'images différentes considérées comme des images similaires(N distinct) pour chaque seuils. Le nombre total de paires d'images différentes est 28800 (n différent).

Le **tableau 3.9** montre les résultats obtenu pour le P_{TPR} et P_{FPR} pour des différents seuils :

Seuils	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
P_FPR	0.00	0.00	0.005	0.013	0.021	0.037	0.045	0.051	0.172	0.97
P_TPR	1.00	1.00	1.00	0.995	0.993	0.991	0.982	0.975	0938	0.042

TABLE 3.9 – Les résultats de P_{TPR} et P_{FPR} par rapport au différents seuils

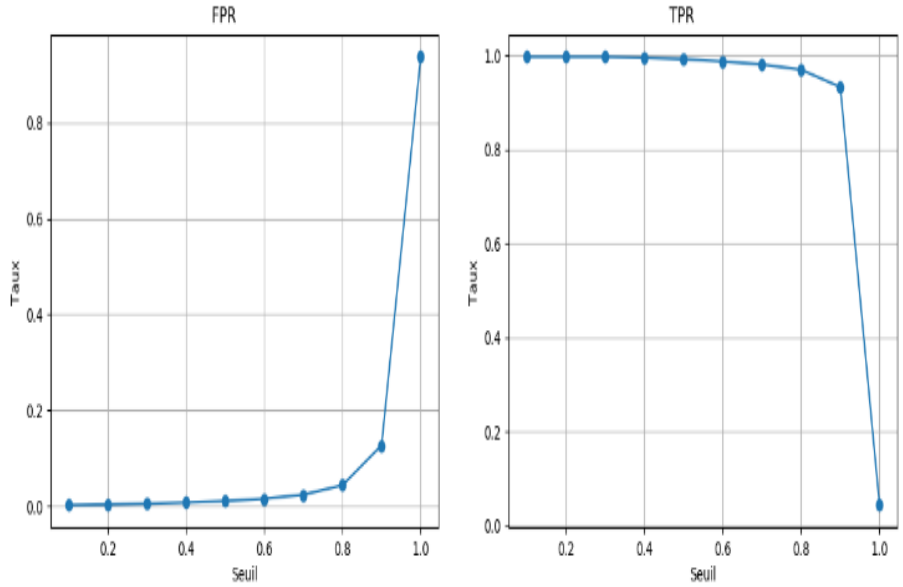


FIGURE 3.12 – Évaluation de TPR et FPR par rapport aux différentes seuils.

Les résultats montrent que le TPR et FPR est acceptable. en outre dans notre méthode le résultat avec une valeur proche à 1 est meilleur que celui avec un petit TPR, de même, la méthode avec un petit FPR est plus performante que avec un grand FPR.

3.5 Conclusion

Nous conclu d'après les différents tests effectués sur notre système pour évaluer ses performances à travers les différentes attaques appliquées sur les images d'empreintes digitales, que notre méthode est robuste contre quelques attaques acceptables.Également nous concluons que notre méthode ne donne pas des bons résultats dans le cas de la rotation 45, scaling 0.5 et 1.5. les résultats et leur analyse montrent l'efficacité de la technique proposée en termes de performance.

Conclusion générale et perspectives

L'objectif principale de ce travail était l'application de l'une des approches de cryptosystéme biométrique pour la protection du template d'empreinte digitale. Le travail réalisé dans ce mémoire a abouti à la création d'une application permettant d'appliquer un algorithme pour protégé le template d'empreinte digitale pour garantir leur sécurité contre les différentes modifications acceptable comme la compression, shaering, bruit gaussien, scaling et la rotaion.

Nous avons vu les étapes utilisées dans le système de reconnaissance biométrique d'empreinte digitale pour l'identification et l'authentification. Ensuite, notre travail a essentiellement consisté par la description introduire le concept des cryptosystèmes biométriques, leur classifications et leurs différentes méthodes. La deuxième section du chapitre nous avons présenté la technique pour construire un modèle utilisateur hautement sécurisé en utilisant les données extraites de l'empreinte digitale grâce à la génération d'emplacements modifiés correspondant aux points de minutie d'une empreinte digitale.

Enfin,nous conclu que notre méthode appliqué dans ce mémoire est robuste et peut gérer les variations dues à les différents manipulations acceptables (la rotation, shearing, bruit gaussien, compression et scaling) sur le capteur d'empreintes digitales. Les résultats obtenues montrent l'efficacité de la technique proposée en termes de sécurité et performance.

Bibliographie

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

[2] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1) :4–20, 2004.

[3] James L Wayman. Fundamentals of biometric authentication technologies. *International Journal of Image and Graphics*, 1(01) :93–113, 2001.

[4] S Pankanti, NK Ratha, AW Senior, RM Bolle, and JH Connell. Guide to biometrics, 2004.

[5] Samir AKROUF. *Une approche multimodale pour l'identification du locuteur.* PhD thesis, 2014.Université FERHAT ABBAS-SETIF

[6] Abderahmane BENAGGA and Lina TELIB. Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt.Université KASDI MERBAH OUARGLA 2016.

[7] Anis Chaari. *Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée.* PhD thesis, 2009.Université d'Evry Val d'Essonne

[8] Arun Kumar Yadav and KS Grewal. A comparative study of different biometric technologies. *International Journal of Computer Science & Communication*, 5(1), 2014.

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

[10] Francis Galton. *Finger prints.* Macmillan and Company, 1892.

[11] Anil K Jain, Sarat C Dass, and Karthik Nandakumar. Can soft biometric traits assist user recognition ? In *Biometric technology for human identification*, volume 5404, pages 561–572. International Society for Optics and Photonics, 2004.

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

[13] Nicolas Galy. *Etude d'un système complet de reconnaissance d'empreintes digitales pour un capteur microsystème à balayage*. PhD thesis, Institut National Polytechnique de Grenoble-INPG, 2005.

[14] Mehmet Sezgin and Bülent Sankur. Survey over image thresholding techniques and quantitative performance evaluation. *Journal of Electronic imaging*, 13(1) :146–166, 2004.

[15] Renato Stefanelli and Azriel Rosenfeld. Some parallel thinning algorithms for digital pictures. *Journal of the ACM (JACM)*, 18(2) :255–264, 1971.

[16] ZhaoQi Bian, David Zhang, and Wei Shu. Knowledge-based fingerprint post-processing. *International journal of pattern recognition and artificial intelligence*, 16(01) :53–67, 2002.

[17] Seonjoo Kim, Dongjae Lee, and Jaihie Kim. Algorithm for detection and elimination of false minutiae in fingerprint images. In *International Conference on Audio-and Video-Based Biometric Person Authentication*, pages 235–240. Springer, 2001.

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

[19] Christian Rathgeb and Andreas Uhl. The state-of-the-art in iris biometric cryptosystems. *State of the art in Biometrics*, pages 179–202, 2011.

[20] Jisha Nair BJ. A review on biometric cryptosystems. *International Journal of Latest Trends in Engineering and Technology (IJLTET)*.

[21] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. *EURASIP Journal on advances in signal processing*, 2008 :1–17, 2008.

[22] Umut Uludag, Sharath Pankanti, Salil Prabhakar, and Anil K Jain. Biometric cryptosystems : issues and challenges. *Proceedings of the IEEE*, 92(6) :948–960, 2004.

[23] Syed Sadaf Ali, Iyyakutti Iyappan Ganapathi, and Surya Prakash. Robust technique for fingerprint template protection. *IET Biometrics*, 7(6) :536–549, 2018.

[24] Stéphane Mallat. *Une exploration des signaux en ondelettes*. Editions Ecole Polytechnique, 2000.

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

[26] Ari Juels. M. sudan a fuzzy vault scheme. In *Proceedings of the 2002 IEEE International Symposium on Information Theory*, volume 408, 2002.

[27] Jean-Paul Linnartz and Pim Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In *International Conference on Audio-and Video-Based Biometric Person Authentication*, pages 393–402. Springer, 2003.

[28] Salil Prabhakar. *Fingerprint classification and matching using a filterbank*. Michigan State University. Department of Computer Science & Engineering, 2001.

[29] Florent Perronnin and Jean-Luc Dugelay. Introduction à la biométrie-authentification des individus par traitement audio-vidéo. *Traitement du signal*, 19(4), 2002.

[30] James L Wayman, Anil K Jain, Davide Maltoni, and Dario Maio. *Biometric systems : Technology, design and performance evaluation*. Springer Science & Business Media, 2005.

[31] Christian Rathgeb and Andreas Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(1) :3, 2011.

[32] Bukasa Tshibuabua Patrick Gérard, Patrick Kande Ngalamulume Gérard. Conception et réalisation d'un systÃ¨me de vote électronique pour le parlement : "cas du sénat congolais".Université de Kinshasa RDC 2011.