REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET PO

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET LA RECHERCHE SCIENTIFIQUE

Université MOHAMED SEDDIK BENYAHIA-JIJEL

Faculté des Sciences et de la Technologie

Département Automatique

Projet de Fin d'étude

Pour l'obtention du Diplôme de Master en Sciences

Filière : Automatique

Option : Automatique et Informatique Industrielle

Thème

Sécurité des systèmes de Reconnaissance Biométrique Multimodale

Présenté par :

Mahadi MAHADJIR

Nassim MEZERREG

Encadrés par :

Dr.S. Biad

Soutenus le :15/06/2016 à 9h30 Devant le Jury Composé de :

❖ **Mr D. BOUTANA**	Prof. Université de Jijel	Président
❖ **M.KEMIHA**	Dr. Université de Jijel	Examinatrice

Année universitaire 2015/2016

بسم الله الرحمن الرحيم

REMERCIEMENT

Nulle œuvre n'est exaltante que celle réalisée avec le soutien moral et financier des personnes qui nous sont proches.

Avant tout nous remercions **ALLAH** de nous avoir donner force et courage pour continuer. C'est grâce à lui que notre chemin est éclairé pour finir ce modeste travail. Nous tenons à exprimer notre profonde reconnaissance à :

Notre encadreur **Dr.BIAD Souad** de nous avoir encadré, orienté, conseillé et corrigé tout au long de notre travail.

Nous remercions également le **membre de jury** qui ont accepté d'examiner et de juger notre travail. Nos vifs remerciements vont également à tous ceux qui ont de près ou loin contribuer à l'accomplissement de ce travail.

Notre reconnaissance s'adresse à nos **familles** qui ont su nous apporter sans relâche les soutiens durant toutes ces longues années d'études.

Nous tenons à exprimer notre gratitude envers Mr **Mohammed Maaradji** qui a mis à notre disposition le matériel nécessaire pour le bon déroulement de ce travail. Enfin, nous remercions également tous les **enseignants** qui ont assuré notre formation durant notre cycle universitaire.

Trouvez ici l'expression de nos profondes gratitudes et reconnaissances.

DEDICACES

Je dédie ce mémoire a :

- A ma Mère et Mon père, dont ce travail est le fruit de la rigueur de votre éducation. Vos prière et vos bénédiction m'ont été d'un grand secours pour mener à bien mes études. Aucune dédicace ne saurait être assez éloquente pour exprimer ce que vous méritez pour tous les sacrifices que vous n'avez cessé de me donner depuis ma naissance, durant mon enfance et même à l'âge adulte.
- A mes chers Sœurs et frères.
- A mes chers Oncles et Tantes.
- A toute la famille.
- A tous mes amis sans exception. Je ne peux trouver les mots justes et sincères pour vous exprimer mon affection et mes pensées, vous êtes pour moi des frères, sœurs et des amis sur qui je peux compter. En témoignage de l'amitié qui nous uni et des souvenirs de tous les moments que nous avons passé ensemble, je vous dédie ce travail et je vous souhaite une vie pleine de santé et de bonheur.
- Vous qui m'admirez tant soyez sûrs que ce travail est le résultat de votre confiance en moi. Soyez-en remerciés.

MAHADJIR Mahadi

DEDICACES

Je dédie ce mémoire a :

- A ma Mère et Mon père, dont ce travail est le fruit de la rigueur de votre éducation. Vos prière et vos bénédiction m'ont été d'un grand secours pour mener à bien mes études. Aucune dédicace ne saurait être assez éloquente pour exprimer ce que vous méritez pour tous les sacrifices que vous n'avez cessé de me donner depuis ma naissance, durant mon enfance et même à l'âge adulte.
- A mes chers frères.
- A toute la famille.
- A mes amis : **Hocine Zahar, Salah, Jonny, Oussama, Nouh, Kader, Yousri, Bachir, Hamza, Bader, Hichem** ainsi que tous les autres sans exception.Je ne peux trouver les mots justes et sincères pour vous exprimer mon affection et mes pensées, vous êtes pour moi des frères, sœurs et des amis sur qui je peux compter. En témoignage de l'amitié qui nous uni et des souvenirs de tous les moments que nous avons passé ensemble, je vous dédie ce travail et je vous souhaite une vie pleine de santé et de bonheur.
- Vous qui m'admirez tant soyez sûrs que ce travail est le résultat de votre confiance en moi. Soyez-en remerciés.

MEZERREG Nassim

Table des matières

Table des figures

Liste des tableaux

LISTE DES ABRÉVIATIONS

GDA (Generalized Discriminante Analysant)

NIST (National Institue of Standards)

FTE (Failure to Enroll)

FTC (Failure to capture)

TFA Taux de fausse Acceptation

TFR Taux de faux rejet

TEE Taux d'égale Erreur

ROC Receiver Operating Characteristic

CMC Cumulative Match Characteristic

KNN K Nearest Neighbord

SHA-1 Secure Hash Algorithm

ACP Analyse en Composante Discriminante

ALD Analyse linéaire discriminante

GDA Generalized Discriminante Analysis

FERET The facial Recognition Technology

FVC Fingerprint Verification Competition

TBC Taux de Bonne Classification

TFC Taux de Fausse Classification

INTRODUCTION GÉNÉRALE

La reconnaissance biométrique est en quelque sorte l'exploitation automatisée ou semi-automatisée de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité [AK10].

De nos jours, cette technologie est l'un des sujets les plus pertinents de XXIe siècle, et elle suscite une attention accrue. La croissance internationale des communications, tant en volume qu'en diversité (déplacements physiques, transactions financières, accès aux services...), implique le besoin de s'assurer de l'identité des individus. En effet, l'importance des enjeux peut motiver les fraudeurs à mettre en échec les systèmes de sécurité existants. Il existe donc un intérêt grandissant pour le développent des systèmes électroniques sécurisés d'identification et de reconnaissance.

Tout d'abord il est important de rappeler que les systèmes biométriques basés sur l'utilisation de l'une des modalités existantes [Cho14] comme (visage, iris, forme de la main, ADN...) ne sont toutes parfaites. Les principales contraintes liées à ce contexte sont dues à l'ergonomie et à l'acceptabilité de certaines modalités. Par exemple la reconnaissance de l'ADN ou de la rétine est généralement mal perçue par le public. Il existe d'autres modalités, moins intrusives, comme les biométries du visage, la reconnaissance automatique du locuteur (RAL) .... Ces modalités présentent l'avantage d'être naturelles aux êtres humains, tout en apportant un niveau de sécurité acceptable pour un certain nombre d'applications. De plus, le matériel nécessaire – caméra et microphone - est actuellement intégré à la plupart des systèmes sécurisés. Seulement elles présentent un faible score d'évaluation.

Afin d'augmenter les performances de tels systèmes et pouvoir ainsi envisager leurs utilisations à grande échelle, le couplage de plusieurs modalités paraît une voie prometteuse qui reste à valider . Ce travail porte sur la mise en œuvre d'un système de reconnaissance biométriques multimodales basés sur la reconnaissance de visage et de l'empreinte digitale.

Ainsi dans ce mémoire, nous abordons plusieurs points importants concernant la biométrie multimodale.

- Dans le premier chapitre nous allons mettre en relief quelques notions de base liées à la biométrie. Nous donnerons le principe de fonctionnement des systèmes biométriques, les diverses technologies et les outils utilisés pour mesurer leurs performances.
- Dans le deuxième chapitre nous présentons en détail le schéma général du système proposé ensuite nous mettons en avant l'utilisation des filtres de Gabor à divers niveaux du système biométrique multimodal et la classification des données.
- Dans le chapitre 3 nous présentons l'ensemble des étapes conduisant à l'obtention d'un système de reconnaissance multimodal performant et les résultats de tests.
  Et enfin nous exploitons le modèle théorique proposé dans le cadre de cette étude pour réaliser un système pratique de contrôle d'accès utilisant les données biométriques.

CHAPITRE 1

ETAT DE L'ART DE LA BIOMÉTRIE

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométriques informatisés.

Nous introduirons dans ce chapitre quelques notions et définitions de base liées à la biométrie. Nous donnerons le principe de fonctionnement des systèmes biométriques ainsi que les outils utilisés pour mesurer leurs performances.

La biométrie ou, plus précisément, la reconnaissance biométrique est en quelque sorte l'exploitation automatisée ou semi-automatisée de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité. Ainsi dans ce chapitre il est question de faire un état de l'art de la biométrie et les différentes modalités

1.1 Définition de la Biométrie

Le mot biométrie signifie « mesure + vivant » ou « mesure du vivant », et désigne dans un sens très large l'étude quantitative des êtres vivants, mais dans notre contexte, la reconnaissance et l'identification d'individus, il existe deux définitions principales qui se complètent :

1. La biométrie est la science qui étudie à l'aide de mathématiques, les variations biolo-

giques à l'intérieur d'un groupe déterminé.

2. Toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier l'identité qu'un individu affirme.

1.2 Modalités biométriques

Le terme **biométrie** regroupe en fait ce que l'on appelle des modalités biométriques; contrairement à ce que l'on possède et que l'on peut donc perdre (une clé) ou ce que l'on sait et que l'on peut donc oublier (un mot de passe), les modalités biométriques représentent ce que l'on est et permettent de prouver notre identité.

Pour que des caractéristiques collectées puissent être qualifiées de modalités biométriques, elles doivent être :

- *universelles* (on peut trouver chez tous les individus),
- *uniques* (permettre de différencier un individu par rapport à un autre),
- *permanentes* (autoriser l'évolution dans le temps),
- *enregistrables* (collecter les caractéristiques d'un individu avec son accord),
- *mésurable* mesurables (autoriser une comparaison future).

L'empreinte digitale, la géométrie de la main, l'iris, la rétine, le visage, l'empreinte palmaire, la géométrie de l'oreille, l'ADN, la voix, la démarche, la signature ou encore la dynamique de frappe au clavier sont autant de modalités biométriques différentes (figure 1.1).

FIGURE 1.1 – Différentes modalités biométriques

Biométrie	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptabilité	Côut
DNA	Haute	Haute	Haute	Faible	Haute	Faible	Côuteuse
Oreille	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Haute	nd
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Peu Côuteuse
Thérmo-visage	Haute	Haute	Faible	Haute	Moyenne	Haute	nd
Empreinte	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Peu Côuteuse
Démarche	Moyenne	Faible	Faible	Haute	Faible	Haute	nd
Géometrie Main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Peu Côuteuse
Veines Main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	nd
Iris	Haute	Haute	Haute	Moyenne	Haute	Faible	Peu Côuteuse
Frappe Clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Peu Côuteuse
Odeur	Haute	Haute	Haute	Faible	Faible	Moyenne	nd
Rétine	Haute	Haute	Moyenne	Faible	Haute	Faible	Très Côuteuse
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Peu Côuteuse
Voix	Moyenn	Faible	Faible	Moyenne	Faible	Haute	Peu Côuteuse

TABLE 1.1 – Comparaison des différentes technologies biométriques

1.3 Systèmes biométriques et modes de fonctionnements

Dans un système biométrique typique, il existe quatre modules principaux à savoir :

1. **module de capture :** acquiert les données biométriques d'un individu et cela (via un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc...)
2. **module d'extraction de caractéristiques :** considère en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe,
3. **module de correspondance :** compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux,
4. **module de décision :**vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s).

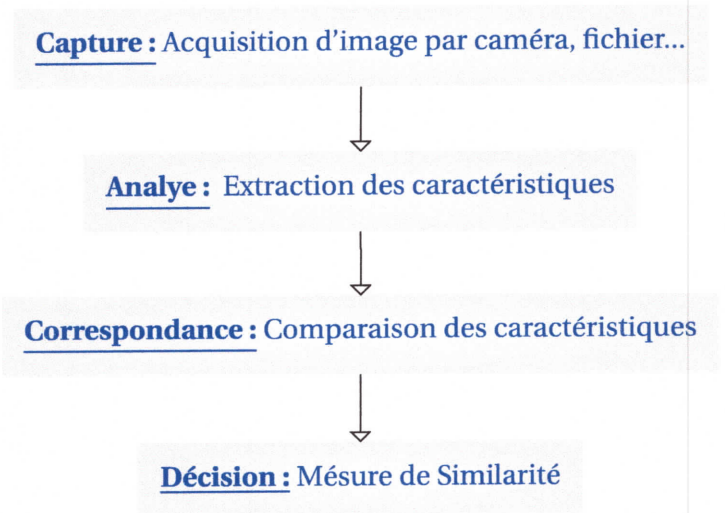

FIGURE 1.2 – Les modules d'un système biométrique

1.4 Modes de fonctionnement d'un système biométrique

Les systèmes biométriques peuvent fournir trois modes de fonctionnement, à savoir, l'enrôlement, l'authentification (ou vérification) et l'identification. Dans ce qui suit, les figures illustreront l'exemple d'un système biométrique utilisant l'empreinte digitale comme modalité.

1.4.1 Mode Enrôlement

L'enrôlement (Figure 1.3) est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données.

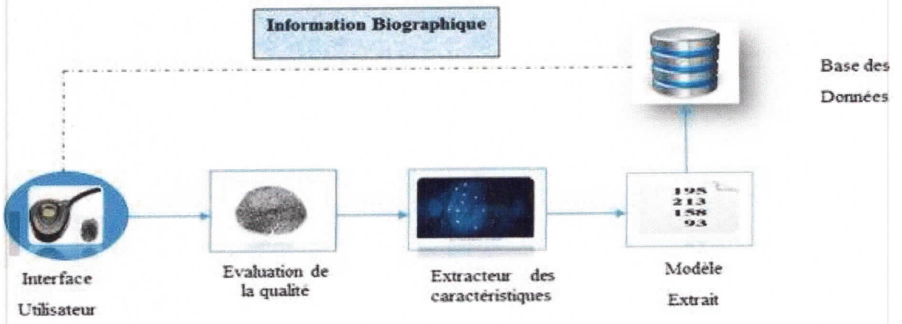

FIGURE 1.3 – Enrôlement d'une personne dans un système biométrique.

1. **mode authentification :** lorsqu'un système biométrique opère en mode authentification (figure 1.4), l'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non.

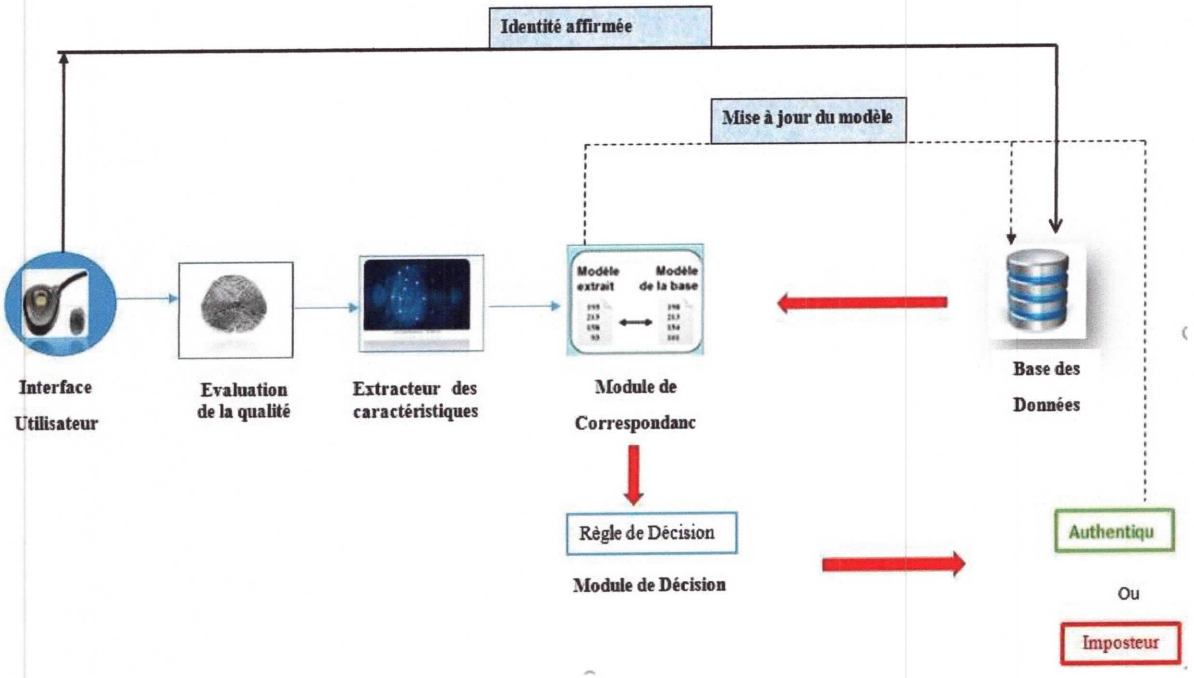

FIGURE 1.4 – Authentification d'un individu dans un système biométrique.

Pour illustrer ce principe, prenons la situation où un utilisateur ($M.X$) souhaite accéder à une salle sécurisée en entrant son code personnel d'identification (Code PIN) et en présentant une modalité biométrique. Le système acquiert alors les données biométriques et va les comparer uniquement avec le modèle enregistré correspondant à M.X. On parle alors de correspondance (1 : 1). Ainsi, si l'entrée biométrique de l'utilisateur et le modèle enregistré dans la base de données correspondant à l'identité affirmée possèdent un degré de similitude élevé, l'affirmation est validée et l'utilisateur est considéré comme étant un authentique. Dans le cas contraire, l'affirmation est rejetée et l'utilisateur est considéré comme étant un imposteur. En résumé, un système biométrique opérant en mode vérification répond à la question "Suis-je bien $M.X$?".

1.4.2 Mode Identification

Dans un système biométrique opérant en mode identification (figure 1.5), l'utilisateur ne dévoile pas explicitement son identité. Cependant, l'affirmation implicite faite par l'utilisateur est qu'elle est une des personnes déjà enrôlées par le système.

Ainsi, l'échantillon biométrique de l'individu est comparé avec les modèles de toutes les personnes de la base de données. On parle alors de correspondance (1 : N) La sortie du

système biométrique est constituée par l'identité de la personne dont le modèle possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée. Typiquement, si la plus grande similarité entre l'échantillon et tous les modèles est inférieure à un seuil de sécurité minimum fixé, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système. Dans le cas contraire, la personne est acceptée.

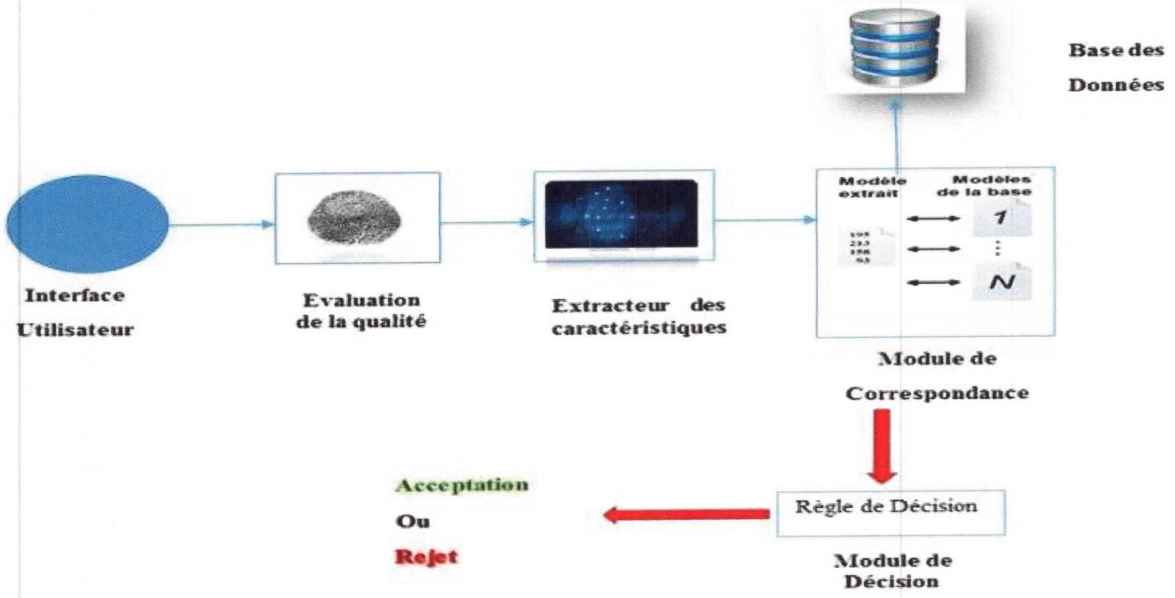

FIGURE 1.5 – Identification d'un individu dans un système biométrique.

Un exemple de système opérant en mode identification serait l'accès à un bâtiment sécurisé : tous les utilisateurs qui sont autorisés à entrer dans le bâtiment sont enrôlés par le système; lorsqu'un individu essaye de pénétrer dans le bâtiment, il doit d'abord présenter ses données biométriques au système et, selon la détermination de l'identité de l'utilisateur, le système lui accorde le droit d'entrée ou non. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ?

1.5 Pourquoi la multimodalité?

Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut garantir actuellement un excellent taux de reconnaissance avec des

systèmes biométriques unimodaux, basés sur une unique signature biométrique. De plus, ces systèmes sont souvent affectés par les problèmes suivants [JNR05] :

- **Bruit introduit par le capteur** du bruit peut être présent dans les données biométriques acquises, ceci étant principalement dû à un capteur défaillant ou mal entretenu. Par exemple, l'accumulation de poussière sur un capteur d'empreintes digitales, un mauvais focus de caméra entraînant du flou dans des images d'iris, etc. Le taux de reconnaissance d'un système biométrique est très sensible à la qualité de l'échantillon biométrique et des données bruitées peuvent sérieusement compromettre la précision du système [CDJ05].
- **Non-universalité :** si chaque individu d'une population ciblée est capable de présenter une modalité biométrique pour un système donné, alors cette modalité est dite universelle. Ce principe d'universalité constitue une des conditions nécessaires de base pour un module de reconnaissance biométrique. Cependant, toutes les modalités biométriques ne sont pas vraiment universelles. Le National Institute of Standards and Technologies (NIST) a rapporté qu'il n'était pas possible d'obtenir une bonne qualité d'empreinte digitale pour environ 2% de la population (personnes avec des handicaps liés à la main, individus effectuant de nombreux travaux manuels répétés, etc.) [JDN04]. Ainsi, de telles personnes ne peuvent pas être enrôlées dans un système de vérification par empreinte digitale.

  De la même manière, des personnes ayant de très longs cils et celles souffrant d'anormalités des yeux ou de maladies oculaires (comme certains glaucomes et cataractes) ne peuvent fournir des images d'iris, ou de rétine, de bonne qualité pour une reconnaissance automatique. La non-universalité entraîne des erreurs d'enrôlement ("Failure to Enroll" ou FTE) et/ou des erreurs de capture ("Failure to Capture" ou FTC) dans un système biométrique.
- **Manque d'individualité :**

  les caractéristiques extraites à partir de données biométriques d'individus différents peuvent être relativement similaires. Par exemple, une certaine partie de la population peut avoir une apparence faciale pratiquement identique due à des facteurs génétiques (père et fils, vrais jumeaux, etc.). Ce manque d'unicité augmente le taux de fausse acceptation ("False Accept Rate" ou FAR) d'un système biométrique.

- **Manque de représentation invariante :**
  les données biométriques acquises à partir d'un utilisateur lors de la phase de reconnaissance ne sont pas identiques aux données qui ont été utilisées pour générer le modèle de ce même utilisateur lors de la phase d'enrôlement. Ceci est connu sous le nom de "variations intra-classe". Ces variations peuvent être dues à une mauvaise interaction de l'utilisateur avec le capteur (par exemple, changements de pose et d'expression faciale lorsque l'utilisateur se tient devant une caméra), à l'utilisation de capteurs différents lors de l'enrôlement et de la vérification, à des changements de conditions de l'environnement ambiant (par exemple, changements en éclairement pour un système de reconnaissance faciale) ou encore à des changements inhérents à la modalité biométrique (par exemple, apparition de rides dues à la vieillesse, présence de cheveux dans l'image de visage, présence de cicatrices dans une empreinte digitale, etc.). Idéalement, les caractéristiques extraites à partir des données biométriques doivent être relativement invariantes à ces changements. Cependant, dans la plupart des systèmes biométriques, ces caractéristiques ne sont pas invariantes et, par conséquent, des algorithmes complexes sont requis pour prendre en compte ces variations. De grandes variations intra-classe augmentent généralement le taux de faux rejet ("False Reject Rate" ou FRR) d'un système biométrique.
- **Sensibilité aux attaques :** bien qu'il semble très difficile de voler les modalités biométriques d'une personne, il est toujours possible de contourner un système biométrique en utilisant des modalités biométriques usurpées. Des études [MMYH02] [VdPK00] ont montré qu'il était possible de fabriquer de fausses empreintes digitales en gomme et de les utiliser pour contrer un système biométrique. Les modalités biométriques comportementales telles que la signature et la voix sont plus sensibles à ce genre d'attaque que les modalités biométriques physiologiques.

Ainsi, à cause de tous ces problèmes pratiques, les taux d'erreur associés à des systèmes biométriques unimodaux sont relativement élevés, ce qui les rend inacceptables pour un déploiement d'applications critiques de sécurité. Pour pallier ces inconvénients, une solution est l'utilisation de plusieurs modalités biométriques au sein d'un même système, on parle alors de système biométrique multimodal.

1.6 Mesure de la performance d'un système biométrique :

Tout d'abord, afin de comprendre comment déterminer la performance d'un système biométrique, il nous faut définir clairement trois critères principaux à savoir :

1. **taux de faux rejet ("False Reject Rate" ou FRR) :** Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.
2. **taux de fausse acceptation ("False Accept Rate" ou FAR) :** Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.
3. **taux d'égale erreur ("Equal Error Rate" ou EER) :** Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où $FRR = FAR$, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations. La figure 1.6 illustre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs tandis que l'EER est représenté sur la figure 1.7.

   Selon la nature (authentification ou identification) du système biométrique, il existe deux façons d'en mesurer la performance :

   - Lorsque le système opère en mode authentification, on utilise ce que l'on appelle une courbe ROC (pour "Receiver Operating Characteristic" en anglais). La courbe ROC (figure 1.7) trace le taux de faux rejet en fonction du taux de fausse acceptation [PD02]. Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé.

   - En revanche, dans le cas d'un système utilisé en mode identification, on utilise ce que l'on appelle une courbe CMC (pour "Cumulative Match Characteristic" en anglais).

     La courbe CMC (figure 1.8) donne le pourcentage de personnes reconnues en fonction d'une variable que l'on appelle le rang [BK05]. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit, parmi deux images, celle qui correspond le mieux à l'image d'entrée, etc. On peut donc dire

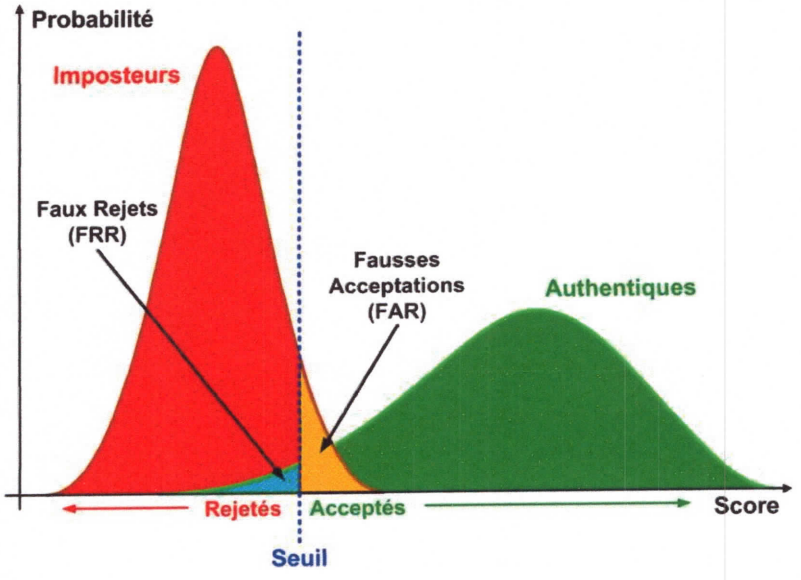

FIGURE 1.6 – Illustration du FRR et du FAR.

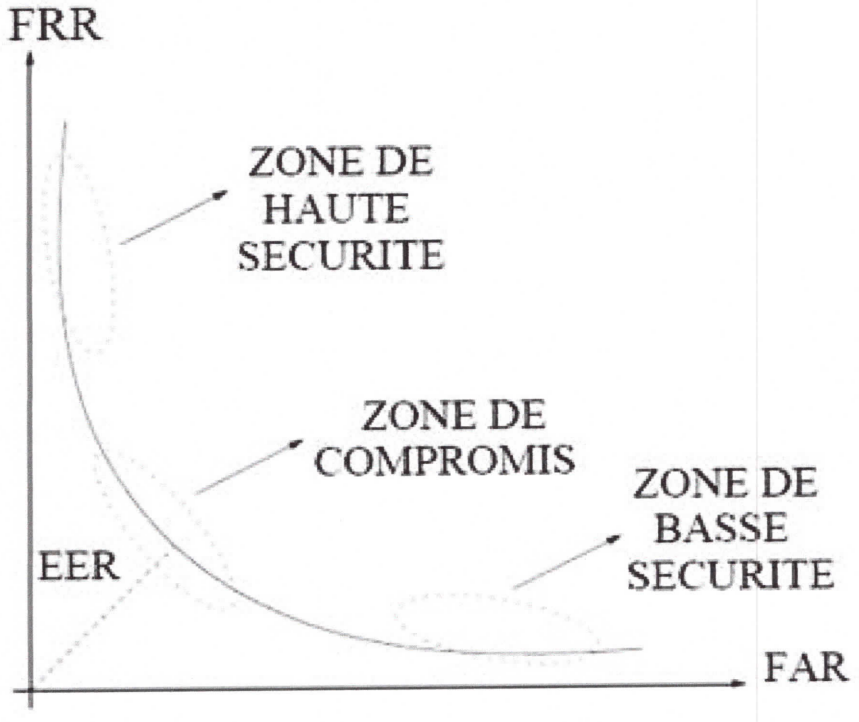

FIGURE 1.7 – Courbe ROC.

que plus le rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible.

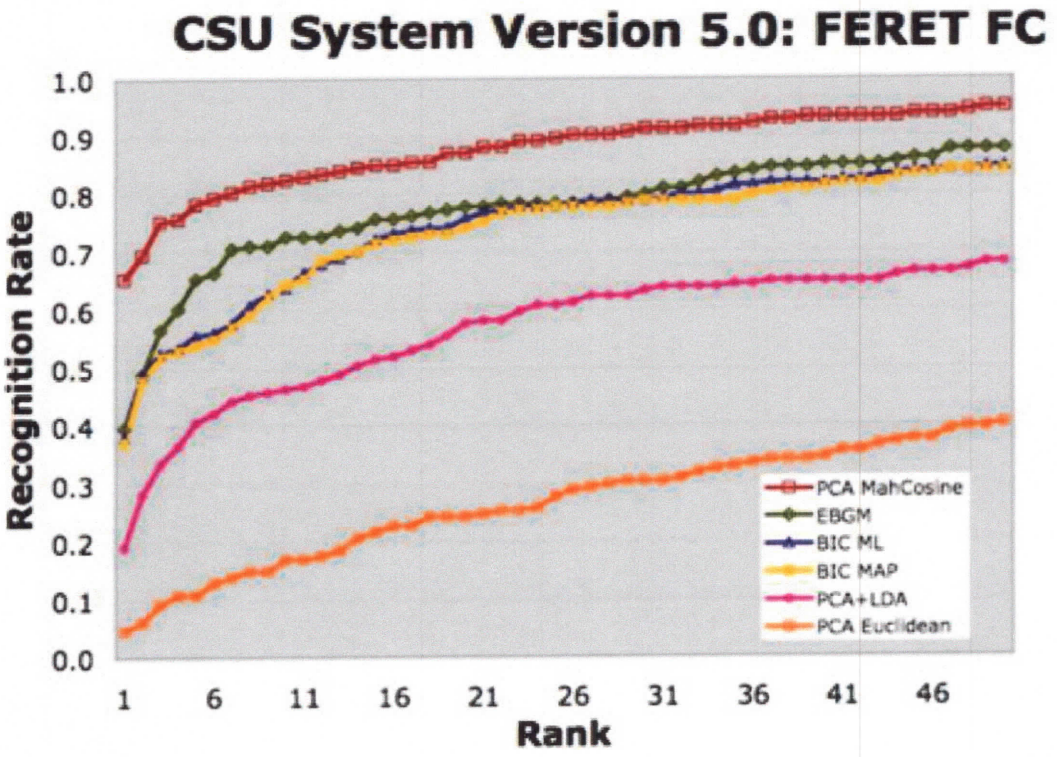

FIGURE 1.8 – Courbes CMC du CSU System 5.0 pour le "FERET Probe Set FC" et pour différents algorithmes de reconnaissance faciale.

Enfin, il faut savoir que la courbe CMC n'est qu'une autre manière d'afficher la per- formance d'un système biométrique et peut également être calculée à partir du FAR et du FRR. Une étude comparative précisant le lien entre les courbes CMC et ROC peut être trouvée dans [BCP+05].

1.7 Conclusion

Dans ce chapitre nous avons présenté en détail l'état de l'art de la biométrie. En effet nous avons commencé par quelques définitions ensuite l'importance de la multi-modalités dans les systèmes biométriques et enfin le mode de fonctionnement de ces derniers.

CHAPITRE 2

SYSTÈME PROPOSÉ

Le domaine de la vérification automatique des personnes est depuis quelques années en pleine expansion. En effet, le besoin d'accès sécurisés automatisés à des environnements physiques ou virtuels est croissant. Ces besoins requièrent des moyens fiables pour vérifier l'identité d'une personne qui se présente au système d'accès. Ce chapitre est consacré à la description du système sécurisé de reconnaissance biométrique proposé. Une présentation détaillée des différentes étapes de ce schéma est établie point par point en faisant apparaitre les caractéristiques de tous les outils utilisés.

2.1 Schéma général

Dans le cadre de cette étude, nous allons élaborer un système basé sur la reconnaissance biométrique (figure 2.1) et qui se compose de deux parties :

- **partie théorique :** le travail proposé dans cette section consiste à l'élaboration d'un système de reconnaissance biométrique multimodal basé sur la fusion des caractéristiques de l'empreinte digital et le visage. L'outil utilisé pour l'extraction de caractéristiques est le filtre de Gabor. Les filtres de Gabor sont connus comme un moyen d'analyse espace-fréquence très robuste. Ils permettent l'analyse des images suivant différentes résolutions et différents angles (section 2).
- **partie pratique :** cette partie consiste à la réalisation pratique d'un contrôle d'accès à un local en utilisant les données biométriques des personnes autorisées à accéder

à l'intérieur. Le schéma de cette application est illustré sur la figure 2.2.Il comporte :

- Un automate ACX 5740(Schneider Electric)
- Une carte magnétique
- Un lecteur de carte.

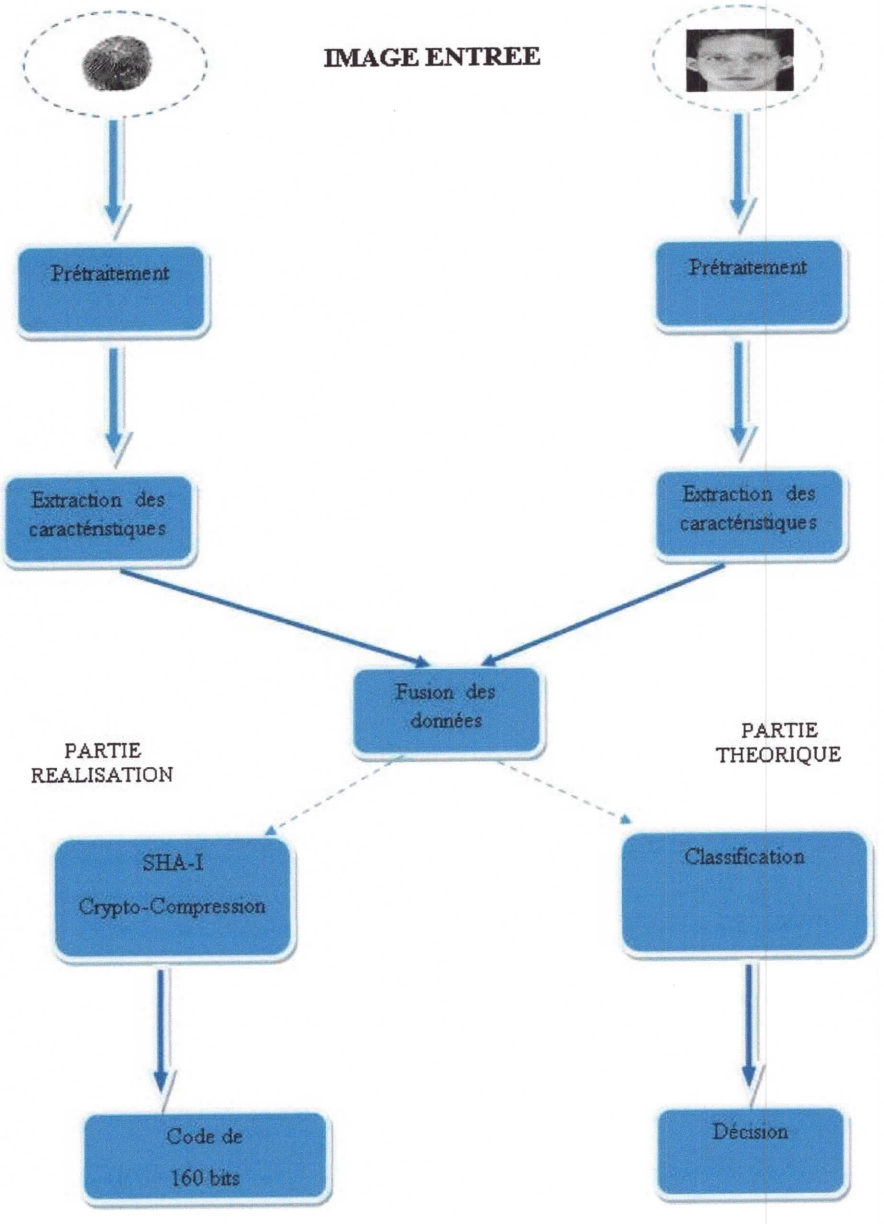

FIGURE 2.1 – Schéma du système proposé

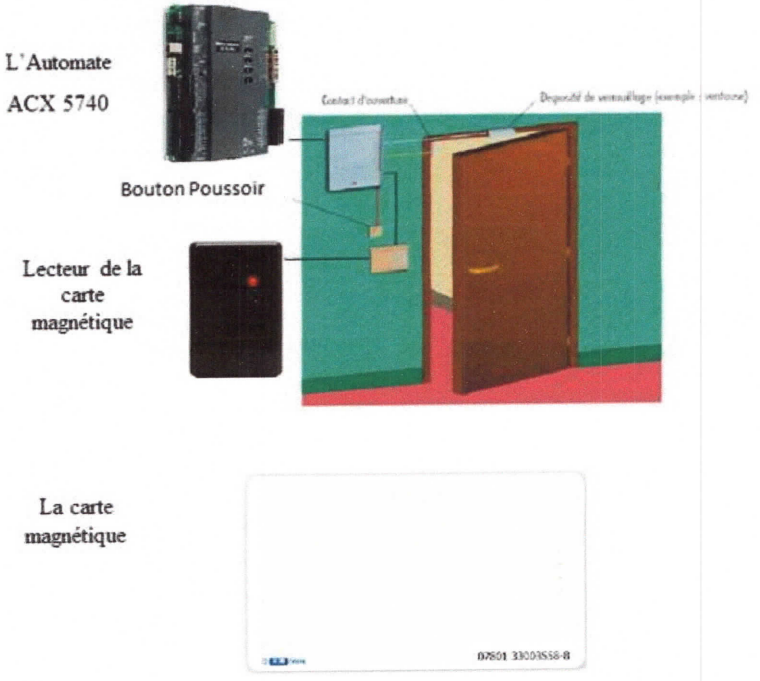

FIGURE 2.2 – Illustration du schéma d'application

2.1.1 Prétraitement

Le prétraitement peut être défini comme étant un ensemble d'opérations visant à rendre une image plus exploitable. Pour notre travail il sera question de quelques opérations parmi lesquelles on peut citer : l'égalisation,la détection des éléments(face/empreinte).

- **Détection du Visage :** La détection du visage est faite par la méthode de détection des éléments à savoir La méthode de Viola et Jones. C'est l'une des méthodes les plus connues et les plus utilisées, en particulier pour la détection de visages et la détection de personnes , proposée par les chercheurs Paul Viola et Michael Jones en 2001. Elle fait partie des toutes premières méthodes capables de détecter efficacement et en temps réel des objets dans une image. Inventée à l'origine pour détecter des visages. Sur la figure 2.1 est illustré un exemple d'application de la phase de prétraitement.

2.1.2 Extraction des caractéristiques

Dans cette étape le filtre de Gabor permet l'extraction des caractéristiques de l'image prétraitée. Il extrait les caractéristiques pertinentes et invariantes aux différentes transformations (rotation, changement d'échelle etc...)

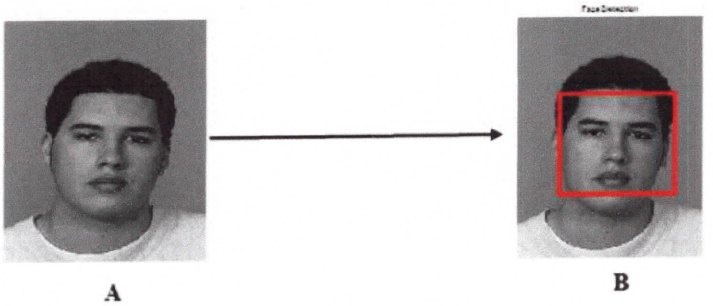

FIGURE 2.3 – Exemple d'application de la phase de prétraitement (*a*) image originale (*b*) visage détecté.

2.1.3 Fusion

Pour pouvoir utiliser plusieurs sources biométriques, il est nécessaire de les fusionner afin de générer une seule décision de reconnaissance. Cette fusion peut être faite à différents niveaux du processus biométrique : soit avant l'étape de classification ou bien après l'étape de la classification [MOZ11]. Dans le cadre de ce travail, nous avons fusionné nos données biométriques avant la phase de classification vue la richesse de l'information qu'on peut acquérir des modalités biométriques.

2.1.4 Classification

On se trouve confronté à la disponibilité d'une masse importante d'informations représentant les caractéristiques utiles pour la reconnaissance (les bancs de filtres de Gabor pour le visage et l'empreinte). Nous avons utilisé le classifieur KNN (K Nearest Neighbord) pour l'évaluation des performances du système proposé. C'est une méthode qui classifie des données non étiquetées en se basant sur leur similarité aux données d'apprentissage.

2.1.5 Crypto-compression

Cette étape garantie la sécurité du système et maintient la longueur de la signature fixe. Elle peut être assurée par les fonctions de hachage cryptographique comme, par exemple, la fonction de hachage cryptographique $SHA-1$ générant une signature de taille $160-bits$. Dans le cadre de notre travail nous allons utiliser l'algorithme $SHA-1$.

- **L'algorithme** $SHA-1$ le SHA en anglais (Secure Hash Algorithm) est une norme américaine pour le hachage. Ainsi le $SHA-1$ est une version améliorée de la précédente qui engendre un code de 160 bits à partir d'un message de longueur maximale de 2^{64} bits.

2.2 Filtres de Gabor

Les caractéristiques directement extraites par filtrage de Gabor, à partir des images, ont été largement utilisées dans plusieurs domaines tels que : la reconnaissance de formes, l'identification biométriques (empreintes digitales, iris, visage...), la segmentation de la texture. La puissance de cet outil réside dans ses propriétés de localisation optimale espace-fréquence. En fait, ces filtres minimisent d'une manière optimale le principe d'incertitude de Heisenberg [Dau85].

2.2.1 Définition

Les filtres de Gabor sont très utilisés pour l'extraction de caractéristiques. Le principe consiste en la sélection dans le domaine de Fourier de l'ensemble de fréquences qui compose la région à détecter ou extraire. Un filtre de Gabor est un filtre linéaire dont la réponse impulsionnelle est une sinusoïde modulée par une fonction gaussienne (également appelée ondelette de Gabor). Il porte le nom du physicien anglais d'origine hongroise Dennis Gabor [Ham14].

2.2.2 Expression unidimensionnelle

Au départ les ondelettes de Gabor ont été développées pour le cas unidimensionnel. Dans le domaine temporel, elles sont données par le produit d'une sinusoïde complexe et d'une enveloppe gaussienne :

$$g(x) = e^{2j\pi u_0+\phi}\, e^{\frac{(x-x_0)^2}{\sigma_x}} \tag{2.1}$$

2.2.3 Expression bidimensionnelle

La généralisation de cette ondelette pour le cas bidimensionnelle permet l'analyse de l'image suivant différentes résolutions et différents angles. En $2D$ c'est aussi une fonction à noyau gaussien modulée par une onde sinusoïdale plane complexe, donnée par l'équation (2.2) :

$$g(x,y) = \frac{1}{2\pi\sigma\beta} \exp^{\pi[\frac{(x-x_0)^2}{\sigma_x^2}+\frac{(y-y_0)^2}{\beta_x^2}]} \exp^{i(\xi_0 x+\upsilon_0 y)} \tag{2.2}$$

Ou x_0, y_0 est le centre de filtre de Gabor dans le domaine spatial, ξ_0 et υ_0 les fréquences spatiales du filtre, et σ_x et β_x les écart-type spatiaux de la gaussienne elliptique[Mel09]. Les bancs de filtres de Gabor sont alors obtenus ont faisant varier tous ces paramètres à savoir l'orientation, la fréquence, la phase de la sinusoïde, le support temporel et l'enveloppe gaussienne. Ce jeu de paramètres qui contrôlent cette ondelette, permet une analyse complète et l'extraction des caractéristiques pertinentes de l'image. L'équation générale faisant apparaitre tous ces paramètres en détail est donnée par l'équation (2.3) :

$$g(x,y,\theta,\lambda,\varphi,\sigma,\gamma) = exp^{(-\frac{x'^2+\gamma^2y'^2}{2\sigma^2})} exp^{(i(2\pi\frac{x'}{\lambda}+\varphi))} \tag{2.3}$$

avec : θ l'orientation de l'ondelette, λ la fréquence centrale, φ la phase de décalage, σ l'écart-type de l'enveloppe gaussienne, γ le rapport d'aspect spatial.

2.2.4 La fréquence de l'ondelette (λ)

Ce paramètre spécifie la longueur d'onde de la sinusoïde ou la fréquence centrale de l'ondelette. Plus cette longueur est grande plus les ondelettes sont sensibles aux variations d'intensités, et plus elle est petite plus les ondelettes sont sensibles aux contours [OUA11].

2.2.5 L'orientation de l'ondelette (θ)

L'orientation nous permet d'obtenir les angles auxquels l'image ou les contours doivent être sélectionnés. Le schéma proposé dans le cadre de cette étude utilise 40 filtres de Gabor

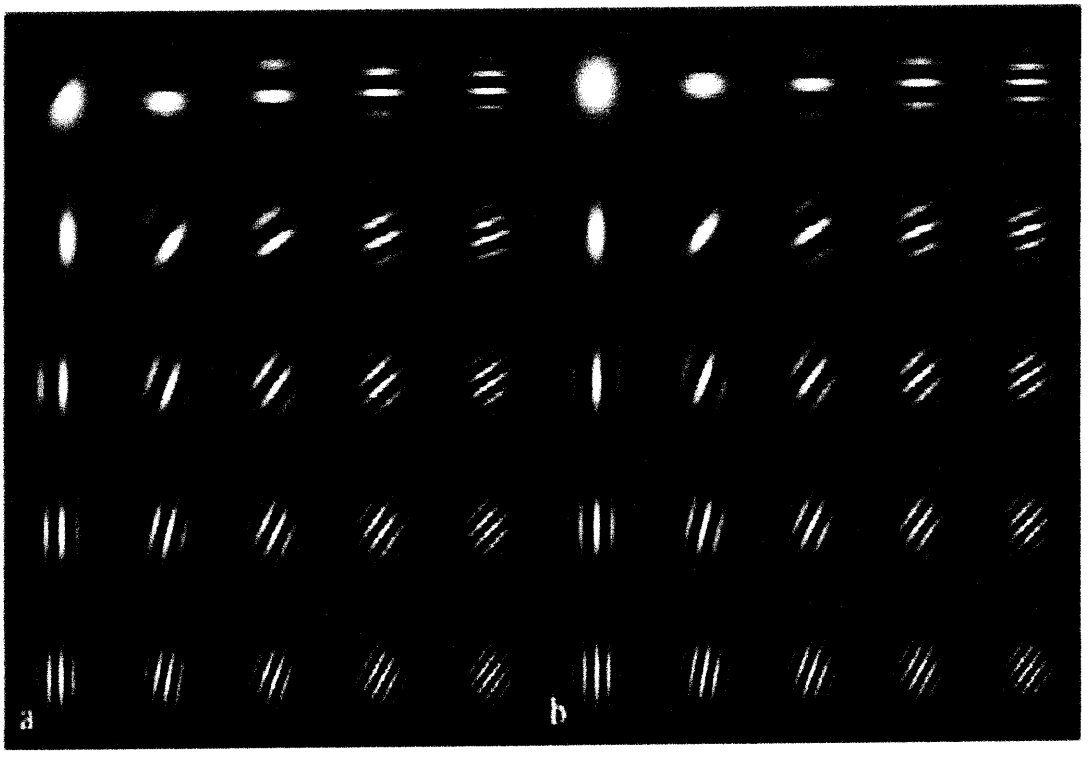

FIGURE 2.4 – Banque de Filtre de Gabor suivant plusieurs orientations :a et b

(figure 2.4) obtenus par le changement de fréquence (5 valeurs) et d'orientation de l'ondelette (8 valeurs). φ représente la phase de la sinusoïde. Elle vaut 0 ou $\frac{\pi}{2}$ selon que l'on veut la partie réelle ou imaginaire.

Le résultat de l'application de ce banc de filtre sur l'image de teste de la figure 2.3 est illustré par la figure 2.6.

Pour des images de taille 120 × 120 pixel comme le cas de la base utilisée dans notre étude, les caractéristiques extraites seront de taille 120 × 120 × 40, ce qui représente une très grande taille de données surtout lorsqu'on utilise une base de données de 100 images et plus. Alors la nécessité d'utiliser les méthodes de réduction de dimensionnalité est primordiale [HZAM13].

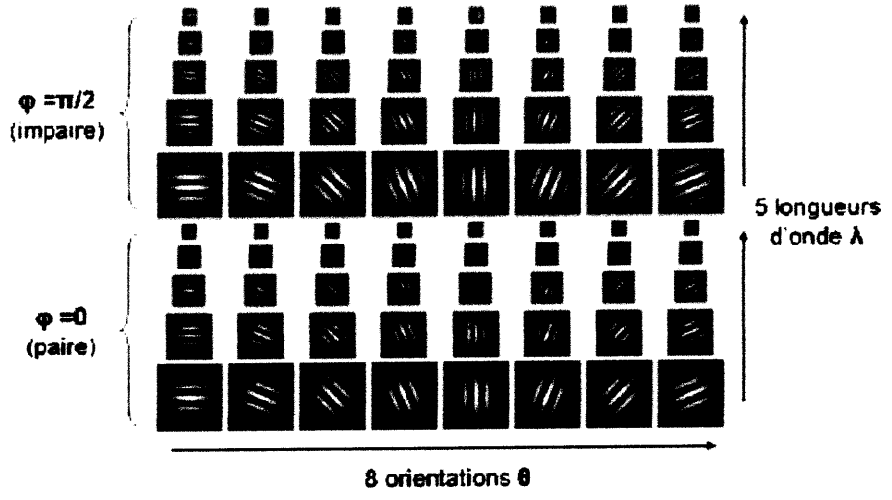

FIGURE 2.5 – Fréquence et Orientation de L'ondelette de Gabor

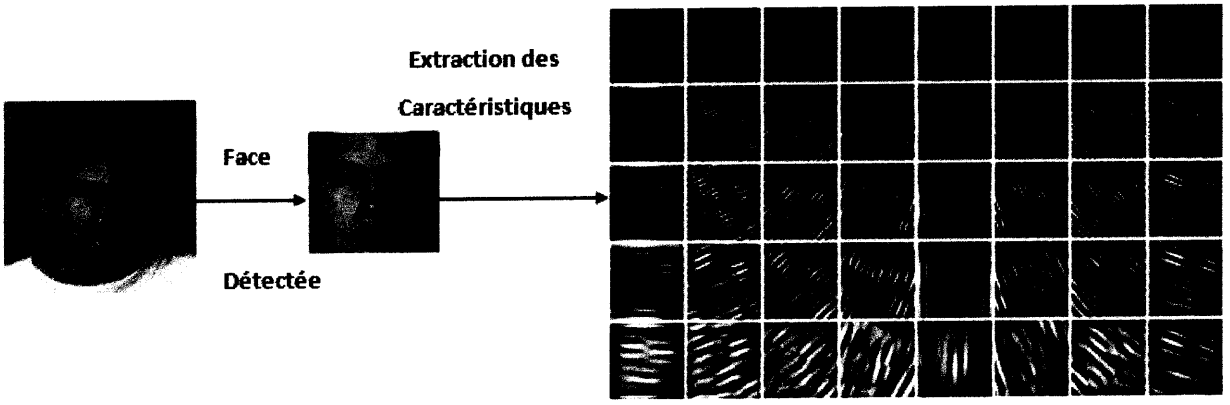

FIGURE 2.6 – Extraction des caractéristiques de l'image test

2.3 Méthodes de réductions de dimensionnalité

La réduction de dimension est une tâche importante dans les processus d'apprentissage car elle facilite la classification, la compression et la visualisation des données de grande dimension en atténuant les propriétés indésirables des espaces de grande dimension. En faite la plus part des méthodes de classification sont inutiles pour les grandes dimensions. C'est pour cela nous allons utilisés l'une de ces technique avant la phase de classification. Il existe deux types de techniques de réductions ; linéaires et non linéaires.

2.3.1 Techniques de réductions linéaires

L'idée principale des algorithmes linéaires de réduction de dimensionnalité est de trouver une transformation linéaire dans un nouvel espace de dimension significativement inférieur qui contient une grande part de l'information totale. Ceci est dans l'objectif de trouver une représentation discriminante des données afin de s'affranchir du fléau de la dimension.

2.3.1.1 Analyse en Composante Principale (ACP)

L'objectif de l'Analyse en Composantes Principales (ACP) est de revenir à un espace de dimension réduite par exemple figure 2.7 en déformant le moins possible la réalité. Il s'agit donc d'obtenir le résumé le plus pertinent possible des données initiales avec le minimum de perte d'information. Cette méthode est souvent utilisée afin d'extraire les caractéristiques essentielles dans l'authentification de visage.

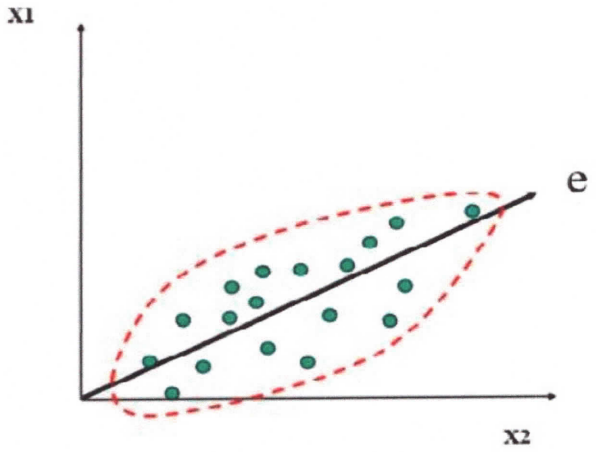

FIGURE 2.7 – Représentation de la méthode ACP

2.3.1.2 Analyse Discriminante Linéaire (ALD)

Contrairement à l'ACP, l'objectif de l'Analyse Linéaire Discriminante (ALD) est de réduire le nombre de dimensions tout en préservant au maximum les classes. Pour cela, elle cherche les axes tels que la projection des données dans l'espace engendré par ces axes

permette une plus grande séparation des classes [MOZ08]. L'ALD est utile particulièrement dans les cas où les fréquences interclasses sont inégales. La figure II-6 compare les axes choisis par la ALD et l'ACP pour les mêmes données..

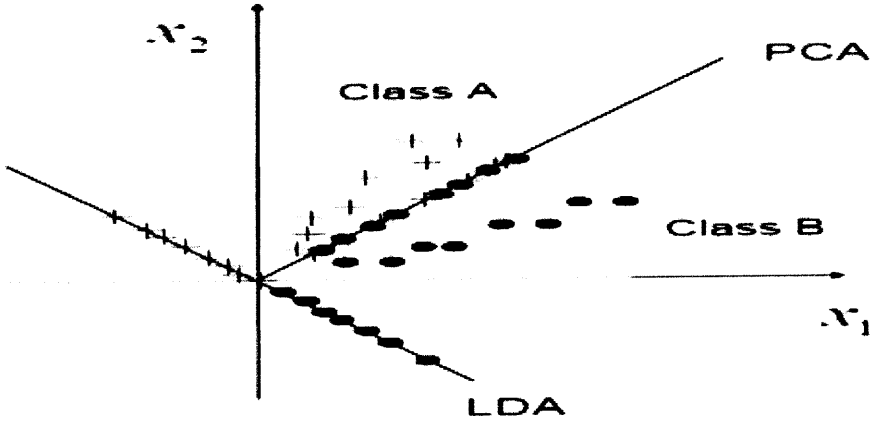

FIGURE 2.8 – Comparaison entre les projections de deux classe ("Classe 1" et "Classe 2")

2.3.2 Techniques de réductions non linéaires.

Les techniques non linéaires globales pour la réduction de la dimension sont des techniques qui visent à préserver les propriétés globales des données. Dans notre travail il est question d'utiliser l'une de ces méthodes.La sous-section présente une techniques non linéaires pour la réduction de la dimensionnalité (GDA).

2.3.2.1 GDA (Analyse discriminante généralisée)

Le **GDA** est une méthode conçue pour la classification non linéaire basé sur un noyau fonction φ qui transforme l'espace d'origine X à un nouvel espace de caractéristiques de dimension réduit $Z : \varphi : X \rightarrow Z$.En plus de cette réduction, cette méthode nous donne ainsi la dispersion au sein de l'intra-classe et l'extra-classe peuvent être calculée comme suit [HZAM13]

$$B^{\varphi} = \sum_{c=1}^{c} M_c m_c^{\varphi} (m_c^{\varphi})^T \tag{2.4}$$

$$W^{\varphi} = \sum_{c=1}^{c} \sum_{x \in X_c} \varphi(x)\varphi(x)^T \tag{2.5}$$

où m_c^{φ} est la moyenne de la classe x_c en Z et M_c le nombre d'échantillon appartenant à x_c.Ainsi le but du GDA est de trouver une matrice de projection U^{φ} qui maximise le rapport :

$$U_{opt}^{\varphi} = argmax \frac{|(U^{\varphi})^T B^{\varphi} U^{\varphi}|}{|(U^{\varphi})^T W^{\varphi} U^{\varphi}|} = [u_1^{\varphi}, ...u_N^{\varphi}] \tag{2.6}$$

Les vecteurs, U^{φ} peuvent être trouvé comme solution aux problèmes généralisés aux vecteurs propres :$B^{\varphi}U_i^{\varphi} = \lambda_i W_i^{\varphi} U_i^{\varphi}$.La formation vecteurs sont censés être centrée dans l'espace caractéristique Z.De la théorie des noyaux produits toute solution $U^{\varphi} \in Z$ doit se situer dans la portée de tous les échantillons de formation dans Z :

$$U^{\varphi} = \sum_{c=1}^{C} \sum_{i=1}^{M_c} \alpha_{ci} \varphi(x_{ci}) \tag{2.7}$$

Où α_{ci} sont des poids réels et x_{ci} est l'échantillon $i^{ème}$ de la classe c. La solution est obtenue en résolvant :

$$\lambda = \frac{\alpha^T KDK\alpha}{\alpha^T KK\alpha} \tag{2.8}$$

où $\alpha = \alpha_c, c = 1...C$ est un vecteur de poids avec $\alpha = \alpha_{ci}, i = 1...M_C$. La matrice de noyau $K(M \times M)$ se compose du point de produits non linéaire, à savoir :

$$K = (K_{KL})_K = 1...C, L = 1...C. \tag{2.9}$$

Où $K_{KL} = (K(x_{Ki}, x_{Lj}))_i = 1...M_k, j = L...M_L$ La matrice $D(M \times M)$ est un bloc de matrice diagonale de telle sorte que :

$$D = (D_c)_{c=1...C}. \tag{2.10}$$

Lorsque la $C^{ième}$ sur la diagonale possède tous les éléments égaux à $\frac{1}{M_c}$. Résoudre le problème de valeurs propres revient cherche les coefficients du vecteur α qui définissent les vecteurs de projection $U^{\varphi} \in Z$.La projection du vecteur de test x_{test} est calculé comme suit :

$$(U)^T \varphi(x_{test}) = \sum_{c=1}^{C} \sum_{i=1}^{M_C} \alpha_{ci} k(x_{ci}, x_{test}) \tag{2.11}$$

2.3.2.2 Schéma Fonctionnel du GDA

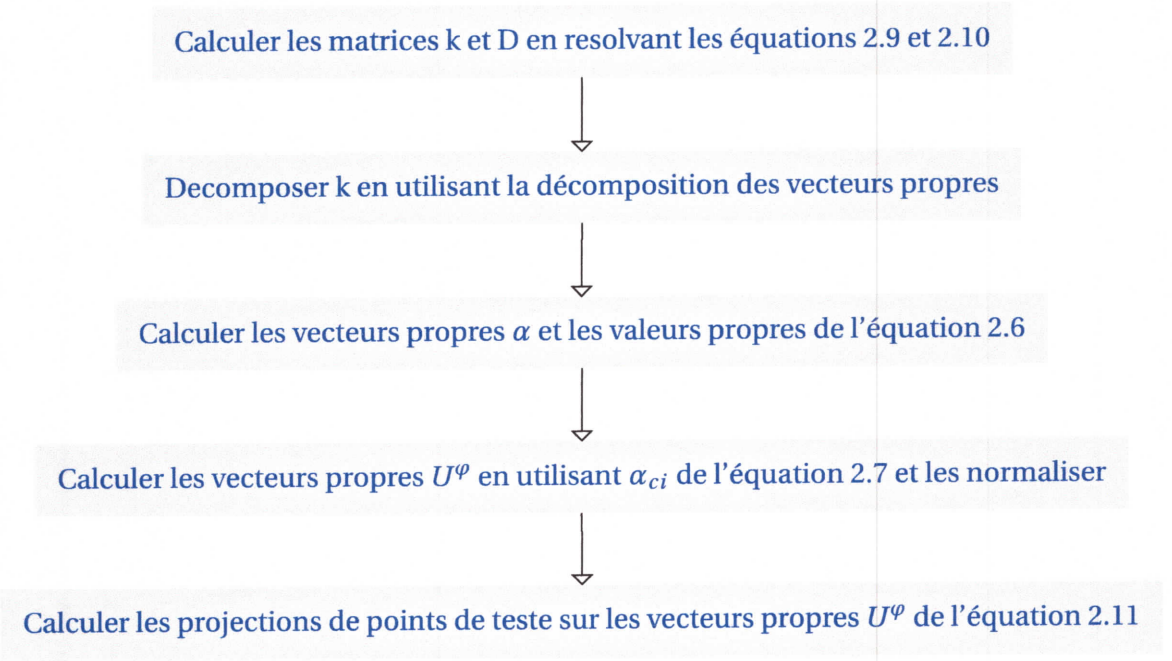

FIGURE 2.9 – Schéma Fonctionnel du GDA

2.4 Méthodes de Classification

Les méthodes de classification ont pour objectif d'identifier les classes auxquelles appartiennent des objets à partir de certains points descriptifs. Elles s'appliquent dans plusieurs domaines et conviennent en particulier au problème de la prise de décision automatique. Les méthodes utilisées pour la classification sont d'une grande variété, mais pour notre contexte nous utilisons Le K-NN.

2.4.1 Les K Plus Proches Proches Voisins.

La méthode des k plus proches voisins est une méthode d'apprentissage supervisé. En abrégé k-NN ou KNN, de l'anglais k-nearest neighbor. La méthode KNN est donc une méthode à base de voisinage, non-paramétrique (figure 2.10).

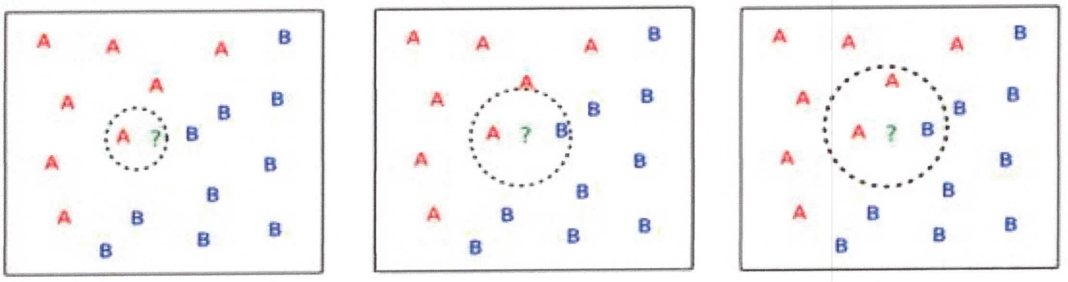

FIGURE 2.10 – Principe des K-NN (k Nearest Neighbor)

2.4.1.1 Règles des KNN

Le paramètre k doit être déterminé par l'utilisateur : $k \in N$.En classification binaire, il est utile de choisir k impair pour éviter les votes égalitaires. Le meilleur choix de k dépend du jeu de donnée. En général, les grandes valeurs de k réduisent l'effet du bruit sur la classification et donc le risque de sur-apprentissage, mais rendent les frontières entre classes moins distinctes. Il convient donc de faire un choix de compromis entre la variabilité associée à une faible valeur de k contre un 'oversmoothing' ou surlissage ($i.e$ gommage des détails) pour une forte valeur de k. Un bon k peut être sélectionné par diverses techniques heuristiques, par exemple, de validation-croisée. Nous choisirons la valeur de k qui minimise l'erreur de classification.La méthode KNN nécessite :

- Un entier K
- Une base d'apprentissage
- Une métrique pour la proximité

Exemple :

* Dans la figure de l'exemple, on a deux classes (verte et Rouge) et le but est de trouver la classe à laquelle appartient le point blanc, on prend ici $k = 3$.

* De 3 plus proches voisins, 2 appartiennent à la classe rouge et une à la classe verte, donc par déduction le point blanc est affecté à la classe rouge (représentant la classe majoritaire).

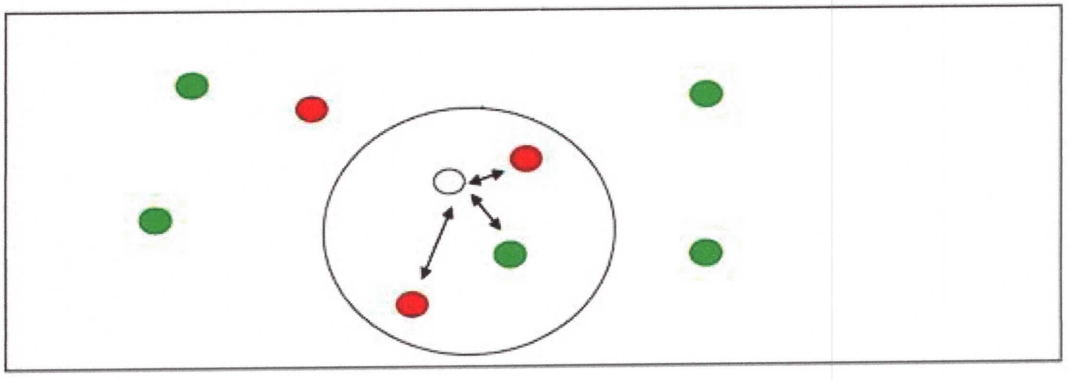

FIGURE 2.11 – Exemple sur la procédure de Sélection

2.4.1.2 Algorithme KNN.

La méthode du plus proche voisin est une méthode non paramétrique où une nouvelle observation est classée dans la classe d'appartenance de l'observation de l'échantillon d'apprentissage qui lui est la plus proche, au regard des covariables utilisées. La détermination de leur similarité est basée sur des mesures de distance. Formellement, soit l'ensemble de données à disposition ou échantillon d'apprentissage :

$$L = \{(y_i, x_i), i = 1, ..., n_L\} \tag{2.12}$$

Où $y_i \ni 1, ..., c$ dénote la classe de l'individu i et le vecteur $x_i = (x_{i1}, x_{ip})$ représente les variables prédicatrices de l'individu i. La détermination du plus proche voisin est basée sur une fonction distance arbitraire d (.). La distance euclidienne ou dissimilarité entre deux individus caractérisés par p covariables est définie par :

$$d((x_1, x_2, x_p)(u_1, u_2, u_p)) = \sqrt{(x_1 - u_1)^2 + (x_2 - u_2)^2 + (x_p - u_p)^2} \tag{2.13}$$

Ainsi, pour une nouvelle observation (y,x) le plus proche voisin $y_{(1)}x_{(1)}$ dans l'échantillon d'apprentissage est déterminé par :

$$d(x, x_{(}(1))) = min_i(d(x, x_i)) \tag{2.14}$$

Et $\hat{y} = y_{(}(1))$ la classe du plus proche voisin, est sélectionnée pour la prédiction de y. Les notations $x_{(j)}$ et $y_{(j)}$ représentent respectivement le $j^{ème}$ plus proche voisin de x et sa classe

d'appartenance. Parmi les fonctions distance types, la distance euclidienne est la plus utilisée et elle est définie comme suit :

$$d(x_i, x_j) = \sum_{s=1}^{P} (x_{is} - x_{js})^2)^{\frac{1}{2}} \tag{2.15}$$

On trouve aussi la distance de Minkowski :

$$d(x_i, x_j) = \sum_{s=1}^{P} (x_{is} - x_{js})^q)^{\frac{1}{q}} \tag{2.16}$$

2.5 Conclusion

Dans ce chapitre, nous avons présenté l'ensemble des étapes nécessaires pour la conception du système de reconnaissance biométrique proposé.Les différentes testes effectués pour l'évaluation de ce système seront présentés au chapitre suivant.

CHAPITRE 3

RÉSULTATS ET DISCUSSION

3.1 Introduction

Après avoir présenté les différentes notions et outils de bases utilisés au cours de cette étude dans les deux chapitres précédents, l'objectif du présent chapitre est de tester un système de reconnaissance biométrique multimodale proposé. Nous allons utilisé deux modalités biométriques à savoir le visage et l'empreinte.Tout d'abord nous allons d'abord vérifier les deux systèmes uni-modaux à base respectivement de modalité du visage et celle de l'empreinte.Ensuite nous optons pour la fusion de ces deux modalités.

3.2 Base de données

Dans notre travail nous avons choisi une collecte d'image de la base de données **FERET**(The Facial Recognition Technology). Cette dernière est une base de données uni-modale destinée à quantifier la performance des systèmes de reconnaissance faciale.Elle a été collectée sur 1199 personnes en plusieurs sessions entre août 1993 et juillet 1996. Pour certains volontaires, le temps séparant la première et dernière image acquise est supérieur à deux ans. Les images de cette base ont été collectées avec des conditions différentes d'expression, de pose, d'éclairage et d'âge.La figure 3.1 représente un extrait d'images de la base de données.

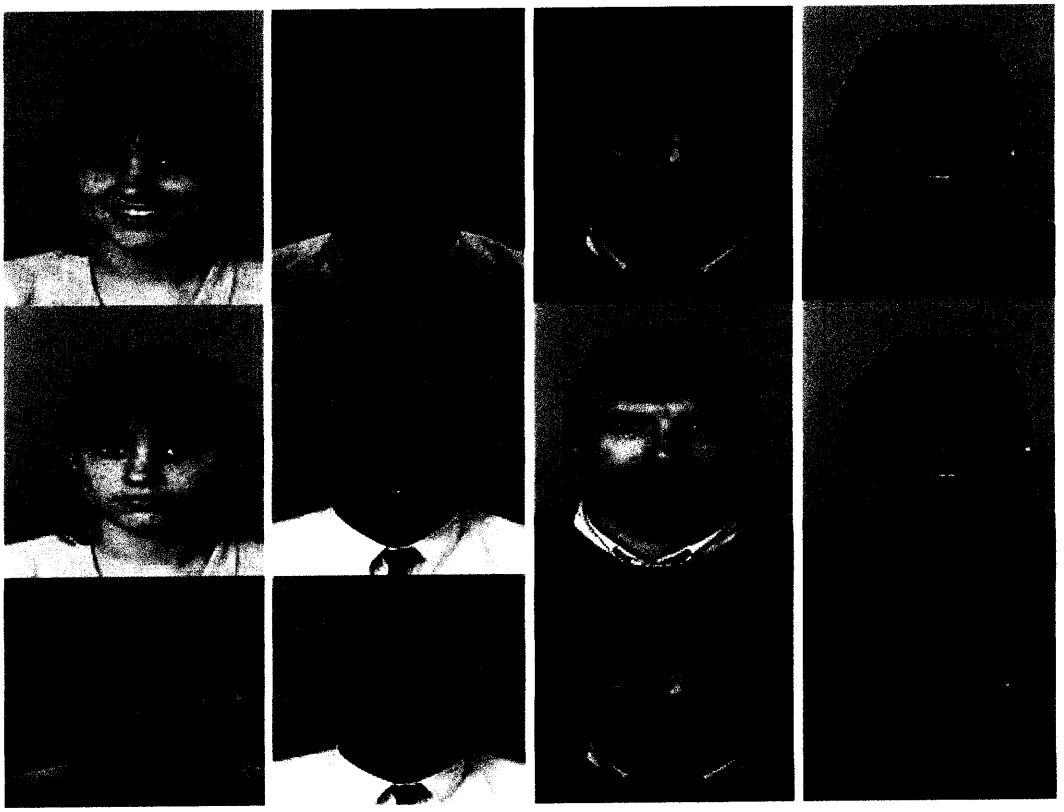

FIGURE 3.1 – Quelques Images de la base de données FERRET

Pour l'empreinte digitale nous avons utilisé la base de données $DB1$ qui a été utilisée dans la compétition *Fingerprint Vérification Competition*(FVC2002).Elle est composée de 100 personnes (8 images par personnes).la figure 3.2 illustre un exemple de cette base.

FIGURE 3.2 – Exemple de la base de données d'empreinte digitale FVC2002

3.3 Protocole d'évaluation

La comparaison des systèmes biométriques nécessite un protocole d'évaluation et une base de données bien défini. Le protocole d'évaluation assure que les systèmes biométriques sont testés sous les mêmes conditions.Le système de vérification compare les données de la personne aux données stockées correspondant à l'identité réclamée et par la suite calcule leur similitude.Pour ce faire, on procède par plusieurs étapes tels que : le prétraitement, l'extraction de caractéristiques,...etc.

Dans la suite nous allons détaillé ces différentes étapes.

3.4 Étape de Prétraitement

La phase de prétraitement est essentielle dans les systèmes de reconnaissance, elle a pour rôle de rendre une image exploitable. Pour cela nous avons jugé utile dans notre travail de prétraiter les images afin d'obtenir des meilleurs conditions pour un résultant satisfaisant et performant.Ainsi chaque modalité dispose différentes phases pour le prétraitement qui sont détaillées dans le paragraphe suivant.

3.4.1 Visage :

a. **La détection du visage :** Dans la partie précédente,nous avons souligné qu'il était nécessaire la prise en compte du prétraitement.Ainsi avant de passer au découpage ou élimination des informations inutiles,on a utilisé le célèbre outil de détection des objets à savoir la méthode de **Viola and Jones** [JV03].Cette méthode d'une précision nette nous permet d'avoir juste la région concernée.La figure 3.3 illustre un exemple d'étapes constituant cette méthode.

FIGURE 3.3 – Détection du Visage en utilisant la méthode Viola and Jones

Suite au résultat de l'étape précédente, Le découpage de l'image conserve le maximum d'informations intrinsèque de l'image et supprime les informations inutiles.Ainsi une fenêtre rectangulaire centrée autour des caractéristiques essentiels a été utilisée.La figure 3.4 est donnée en exemple :

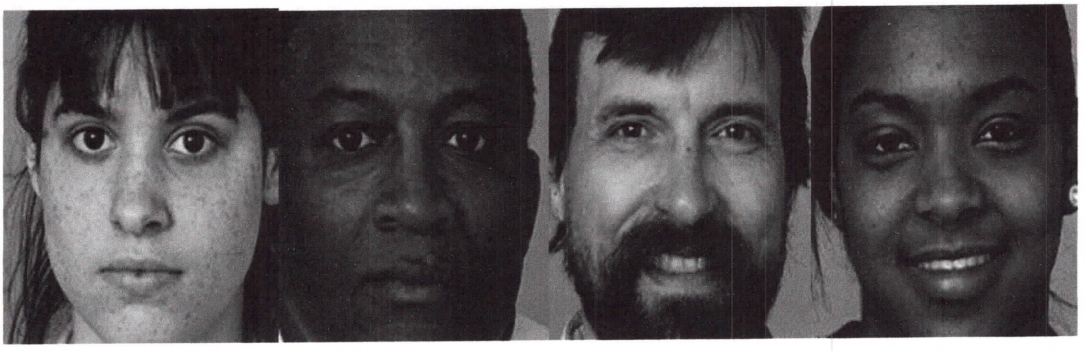

FIGURE 3.4 – Images après détection et coupage

3.4.2 Empreinte

Pour les empreintes digitales, il est aussi nécessaire de prétraiter les images et cela se réalise comme suit :

a. **Histogramme :** Il fait correspondre pour chaque intensité le niveau de gris correspondant. Les niveaux vont de 0 (noir absolu) à 255 (blanc absolu).

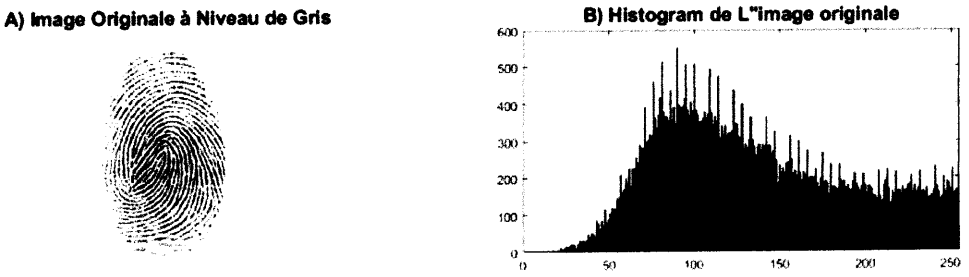

FIGURE 3.5 – A :Image Originale B :Histogramme de l'image

b. **Binarisation :**

La binarisation appelée aussi seuillage, est la technique de segmentation la plus simple. Les pixels de l'image sont partagés par un seuil T en deux classes. En général, ils sont représentés par une classe de pixels noirs et une autre classe de pixels blancs (voir image B de la figure 3.6).

c. **Détection :** Celle-ci nous permet juste de sélectionner la partie essentielle de l'image (voir image C de la figure 3.6).

d. **Découpage :**

La phase finale du prétraitement est le découpage de l'image comme nous le montre image D la figure 3.6 .

3.5 Étape d'extraction des caractéristiques

Comme nous l'avons souligné dans le chapitre précèdent, le **filtre de gabor** est utilisé dans le but de nous garantir l'extraction de caractéristiques pertinentes et invariantes aux différentes transformations à savoir la rotation, le changement d'échelle etc... En outre,grâce à ses bonnes performances en reconnaissance du visage et de l'empreinte digitale, ainsi que ses qualités propres : localisation précise en temps/fréquence et robustesse aux variations de contraste et de luminosité selon [BSC04]. Les caractéristiques à base du filtre Gabor sont directement extraites des images à niveaux de gris. Dans le domaine spatial, un filtre de gabor bidimensionnelle est une fonction de noyau Gaussien modulé par un complexe sinusoïdal onde plane. Dans notre travail nous utilisons quarante filtre de gabor en 5 fréquences

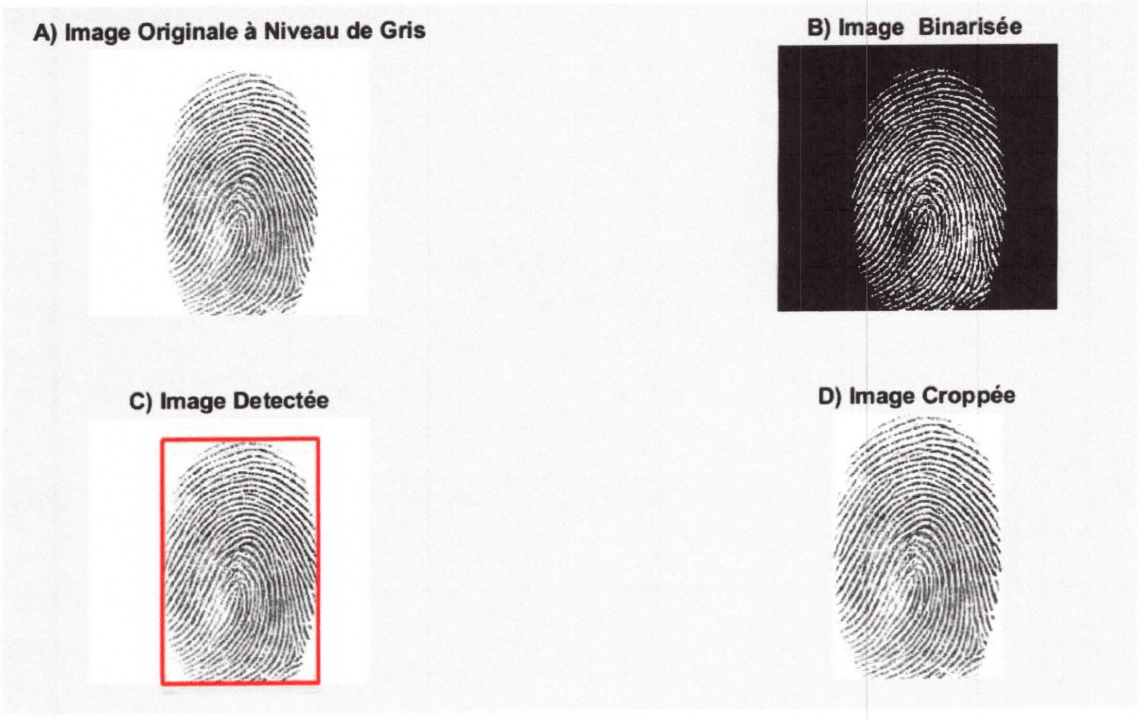

FIGURE 3.6 – Différents étapes du prétraitement de l'empreinte

et 8 orientations(voir figure 2.5 chapitre 2). L'extraction des caractéristiques des images s'effectue comme suit :

- Une fois que l'image d'entrée est pré-traiter,on convolue l'image de sortie avec une taille de 120×120 avec les quarante filtres de Gabor (5 longueurs d'ondes et 8 orientations) pour avoir une taille du vecteur caractéristique de $120 \times 120 \times 40 = 57600$.

3.6 Étape de Réduction de dimensionalité

Pour notre travail nous avons une grande taille de dimension des données augmentant ainsi le temps de calcul et conduisant à la diminution de performance du système. C'est dans ce sens que nous avons jugé utile l'utilisation d'un réducteur de dimensionalité à savoir le **GDA**(Generalized Discriminante Analysis). En utilisant ce dernier la taille extraites des caractéristiques (57600) est réduite à 200.

3.7 Création des matrices

L'utilisation de plusieurs images dans le processus de reconnaissance biométrique nécessite une organisation pour mieux gérer les données,c'est dans ce contexte qu'on a ordonnancé des vecteurs images côtes à côtes créant ainsi la matrice d'apprentissage.

3.8 Étape de classification

Les méthodes de classification, aussi appelées partition des données, permettent de grouper des objets dans des classes de manière à ce que les objets appartenant à la même classe sont plus similaires entre eux qu'aux objets appartenant aux autres classes.Dans ce travail nous avons utilisé le célèbre classifieur **K-NN** pour cette tâche. En effet la classification par **K-NN** est en réalité un apprentissage, il a ainsi donné des bon résultants. Ayant une base de données d'empreinte limitée, nous avons pris 50 personnes, chacune ayant 3 images d'empreintes et 3 du visage en tout 300 images. Le tableau suivant répresente le **TBC**(Taux de bonne Classification) et le **TFC**(Taux de fausse Classification).

Modalités	**Nombres d'images**	**TBC**	**TFC**
Visage	300	96%	4%
Visage	150	93%	7%
Empreinte	150	90%	10%
Visage+Empreinte	150(Empreinte+Visage)	92%	8%

TABLE 3.1 – Résultats des différents taux de classifications

Discussion

Pour la classification nous avons remarqué que plus la base de données est de grande dimension plus la classification est meilleure.

3.9 Évaluation en mode Vérification

La vérification a pour but de déterminer le minimum de ressemblance entre deux images et cela en calculant les distances entre les caractéristiques des images.Les distances utilisées au cours de cette étude, sont les normes **L1** et **L2** définie ci-dessous :

3.9.1 La norme L1 :

La norme L1 aussi appelée la distance de Manhattan est la somme de la différence entre les valeurs absolus des composantes des deux vecteurs A et B :

$$d1(A,B) = \sum_{i=1}^{N} |A_i - B_i| \tag{3.1}$$

3.9.2 La norme L2 :

Elle est aussi appelée la distance euclidienne, elle représente la somme de la différence au carré entre les composants des deux vecteurs A et B :

$$d2(A,B) = \sqrt{\sum_{i=1}^{N} (A_i - B_i)^2} \tag{3.2}$$

3.10 Calcul du seuil de décision

Dans n'importe quel système biométrique de vérification, d'identification ....etc,la notion du calcul du seuil de décision intervient.Ce dernier joue le rôle d'un arbitre décidant l'identité d'un client ou d'un imposteur. En ce fait nous utilisons des images classées en deux groupes (clients et imposteurs). Pour vérifier l'identité de deux groupes,on détermine le seuil tout en calculant les distances intra-classes et extra-classes. En d'autre terme la distance intra-classe reflète une comparaison entre des individus d'un même groupe(clients par exemple) et l'extra-classe pour des groupes différents,ce qui nous ramène à determiner le seuil de décision representant le centre entre la distance maximale intra-classe et celle minimale extra-classe. La figure 3.7 donne les différentes étapes de ce calcul d'une façon générale [Mus13].

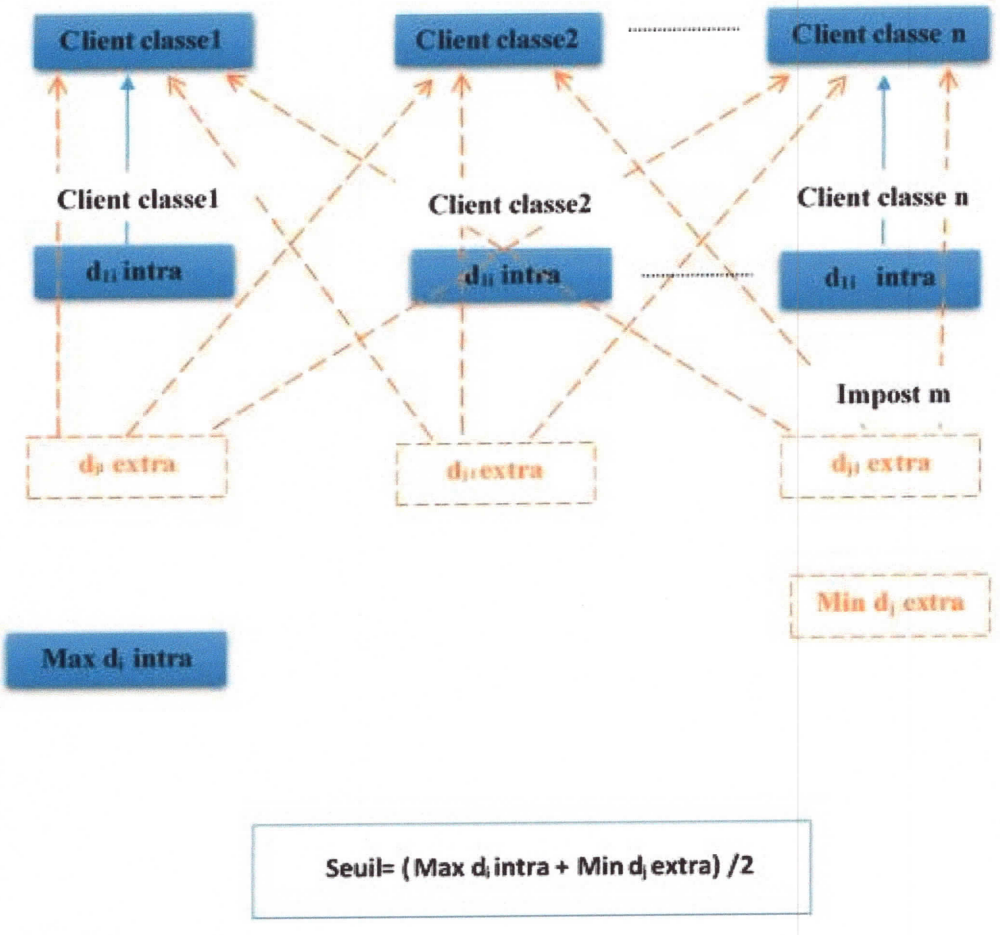

FIGURE 3.7 – Procédure de détermination du seuil

3.11 Résultats en mode vérification

Dans cette section, nous présentons les résultats obtenus concernant la reconnaissance biométrique multimodale basée sur les schémas précédents.

3.11.1 Protocole utilisé pour Le visage

Nous présentons ici les résultats obtenus en mode vérification. En effet notre travail a été effectué sur Matlab 2016*a* et que dans le mode vérification il est nécessaire d'avoir des personnes authentiques et imposteurs. Nous avons utilisé une base de données de 300 image appartenant à 100 personnes dont chacune ayant 3 images pour la classification. Ensuite pour passer au mode vérification ou pour le test de la vérification nous avons utilisé deux bases de 50 personnes (1 image par personne) dont l'une pour les clients et la deuxième pour les imposteurs. En mode vérification, un système biométrique doit vérifier l'identité d'une personne, il s'agit donc de comparer son image à celle de la personne qu'elle prétend être et qui se trouve dans la base.C'est donc une comparaison un à un. Ainsi l'image du candidat est comparé à tous les modèles d'images de la personne réclamée.

- **L'utilisation d'un seuil**

Pour tout système de reconnaissance biométrique en mode vérification, la phase de décision devient d'une importance capitale, car c'est à ce niveau que l'appartenance d'une image est vérifiée (personne connue ou inconnue), d'où la nécessité d'utilisation d'un seuil de décision, on prend le **TEE** lorsque **TFA=TFR**.

Résultats de La norme L1

Les figures 3.8, 3.9 et 3.10 représentent respectivement le **TEE** en fonction du **seuil** et le **TFR** en fonction du **TFA**.

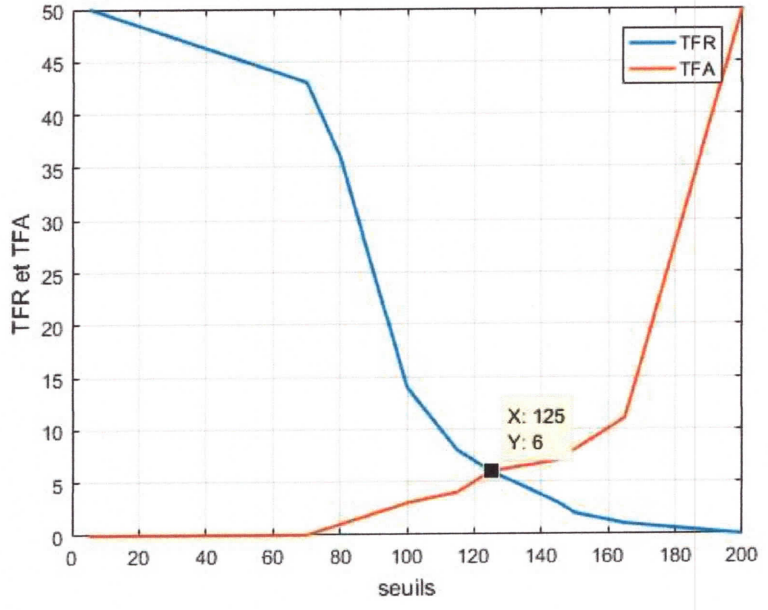

FIGURE 3.8 – TFR ET TFA en fonction de la valeur du seuil.

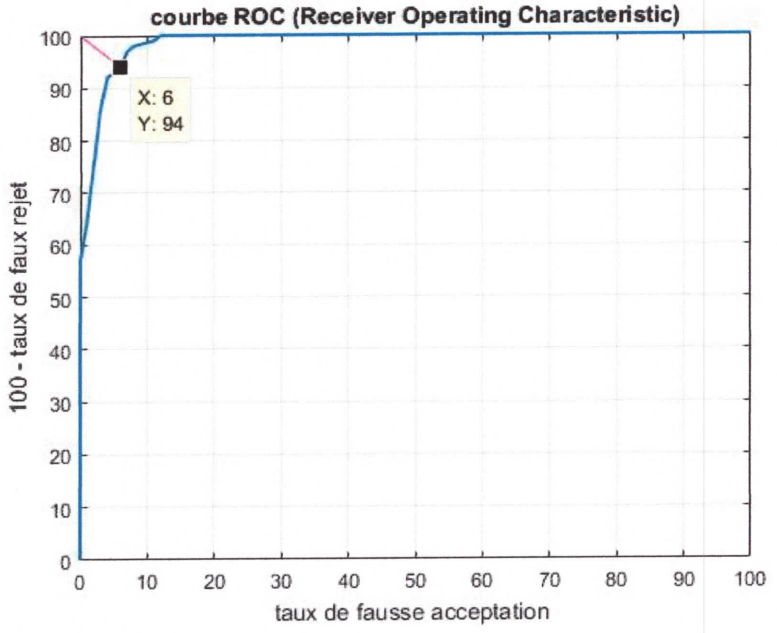

FIGURE 3.9 – Courbe ROC.

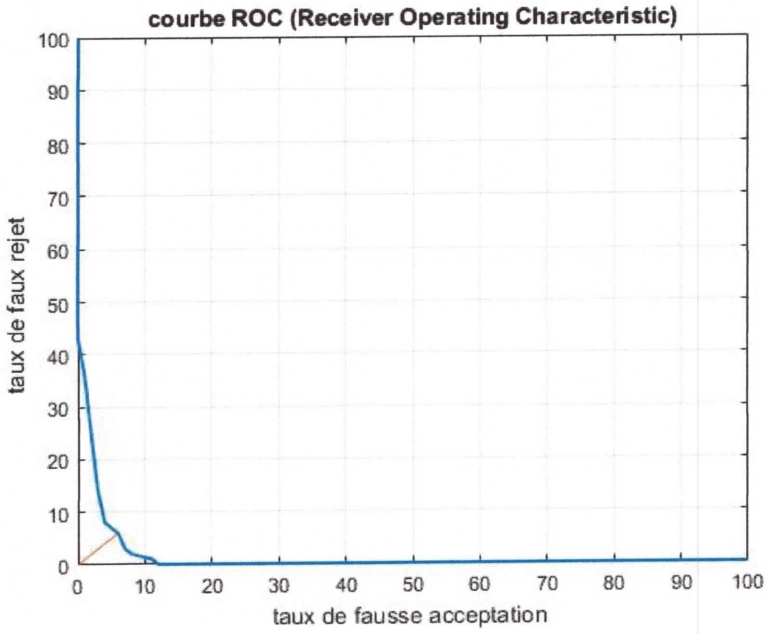

FIGURE 3.10 – Courbe ROC.

Résultats de la norme L2 :

Les figures 3.11, 3.12 et 3.13 représentent respectivement le **TEE** en fonction du **seuil** et le **TFR** en fonction du **TFA**.

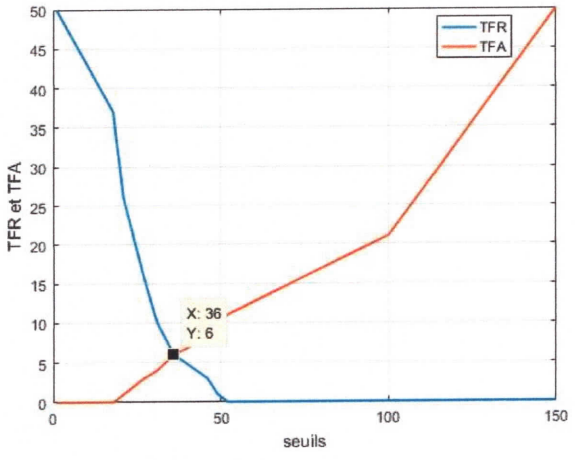

FIGURE 3.11 – TFR ET TFA en fonction de la valeur du seuil.

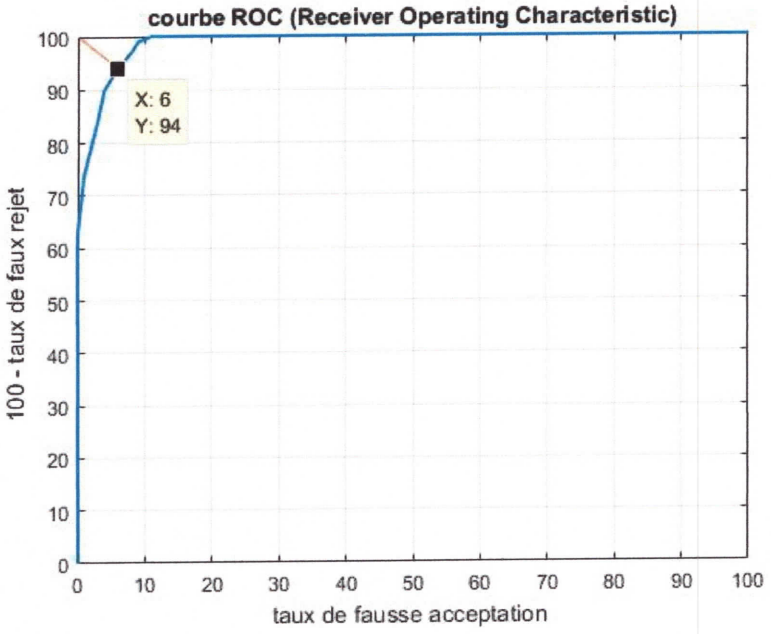

FIGURE 3.12 – Courbe ROC.

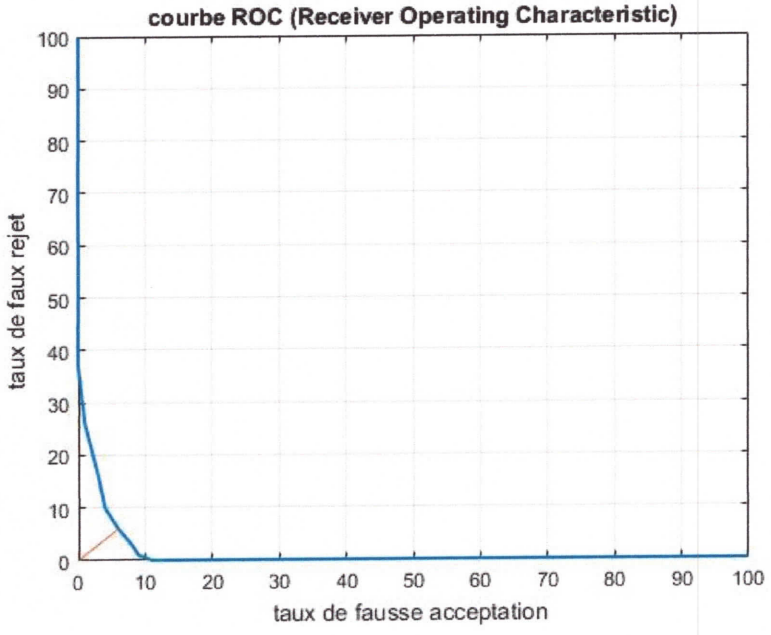

FIGURE 3.13 – Courbe ROC.

	TEE	TFA	TFR	SEUIL
L1	6%	6%	94%	125
L2	6%	6%	94%	36

TABLE 3.2 – Comparaison des différentes normes

Résultats de la comparaison des normes L1 et L2

Les figures 3.14,3.15 représentent le **TFA** en fonction du **TFR**.

3.11.2 Discussion des résultats

La méthode de vérification basé sur la norme **L1** donne un résultat de "**TEE**=6%" pour un "**seuil** =125" et l'évaluation par la courbe ROC montre que pour un **TFA** de 6% on a 94% de **TEE** (**Fig** 3.8,**Fig** 3.9).

Pour la deuxième norme **L2** on a obtenu des résultats pareils à celle de la norme **L1** sauf une différence au niveau du seuil avec une valeur de "**seuil** =36" (**Fig** 3.11,**Fig** 3.12). Nous remarquons que pour un seuil différent les deux normes **L1** et **L2** ont les mêmes coûts d'erreurs (figures 3.14 et 3.15).

D'après la définition présenté dans le chapitre1 (section 1.3 page13), on constate que la zone de basse de sécurité est presque nulle alors que que la zone de haute sécurité existe d'où la performance du système.

3.12 Protocole utilisé pour l'empreinte :

Pour l'empreinte, on a utilisé une base de données de 150 image appartenant à 50 personnes dont chacune ayant 3 images pour la classification. Ensuite pour passer au mode vérification nous avons utilisé deux bases de 50 personnes (1 image par personne) dont l'une pour les clients et la deuxième pour les imposteurs. Dans ce qui suit, les différents résultats obtenus sont illustrés par les figures 3.16, 3.17, 3.18.

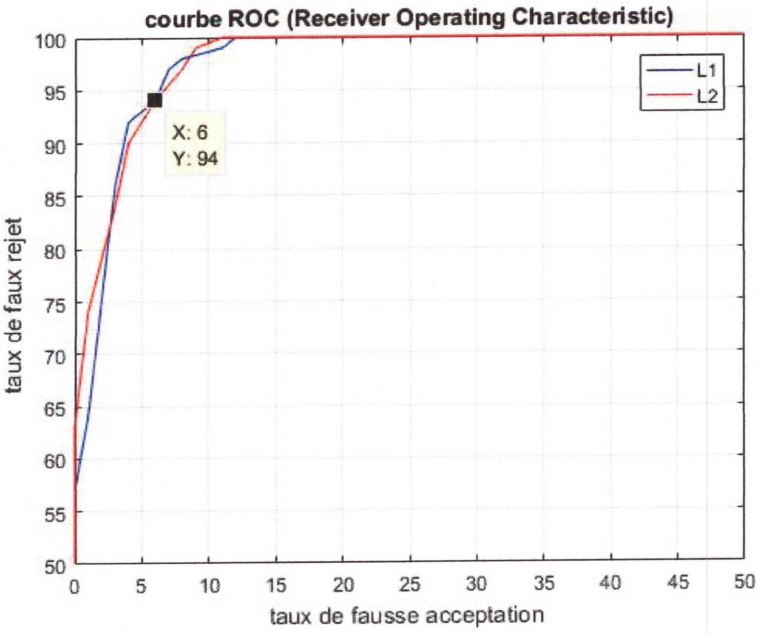

FIGURE 3.14 – Courbe ROC de la norme L1 et L2.

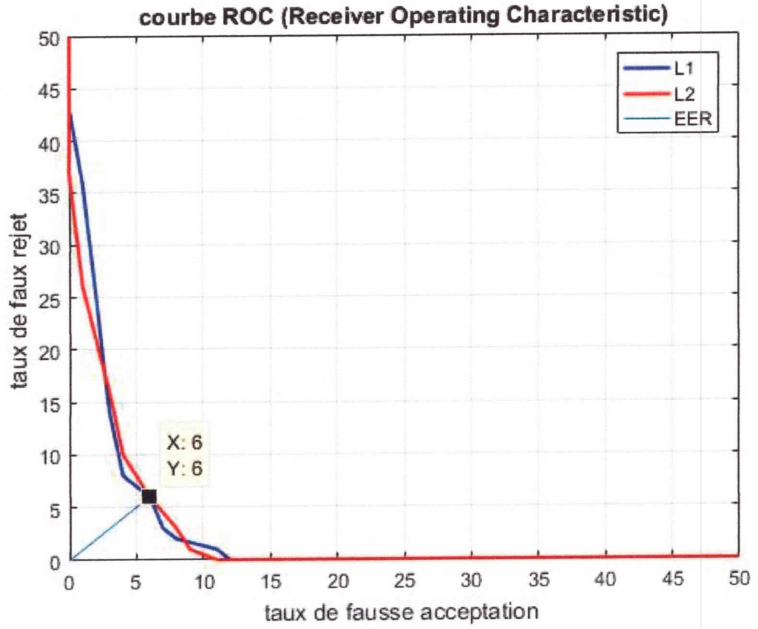

FIGURE 3.15 – Courbe ROC de la norme L1 et L2.

La norme L1 :

Les figures 3.16, 3.17 et 3.18 représentent respectivement le **TEE** en fonction du **seuil** et le **TFA** en fonction du **TFR** pour les tests d'empreintes.

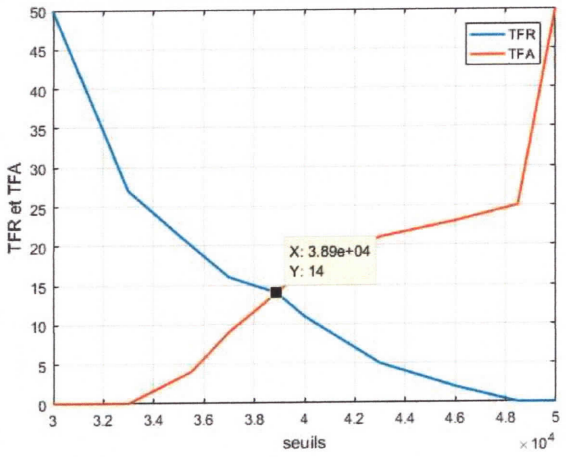

FIGURE 3.16 – TFR ET TFA en fonction de la valeur du seuil.

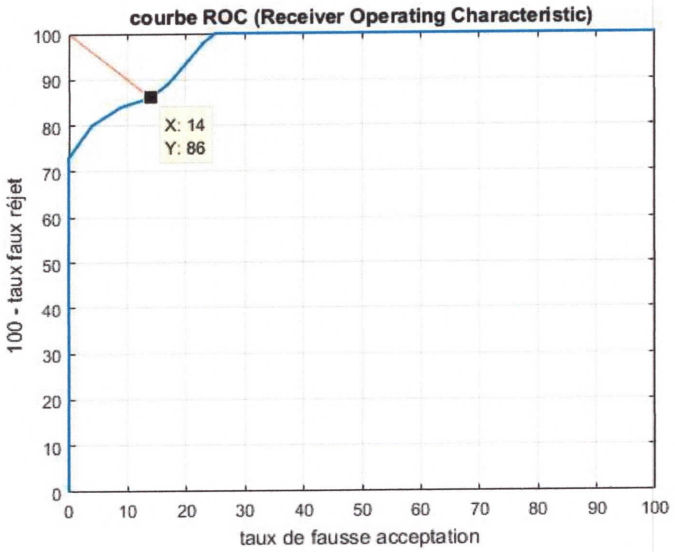

FIGURE 3.17 – Courbe ROC.

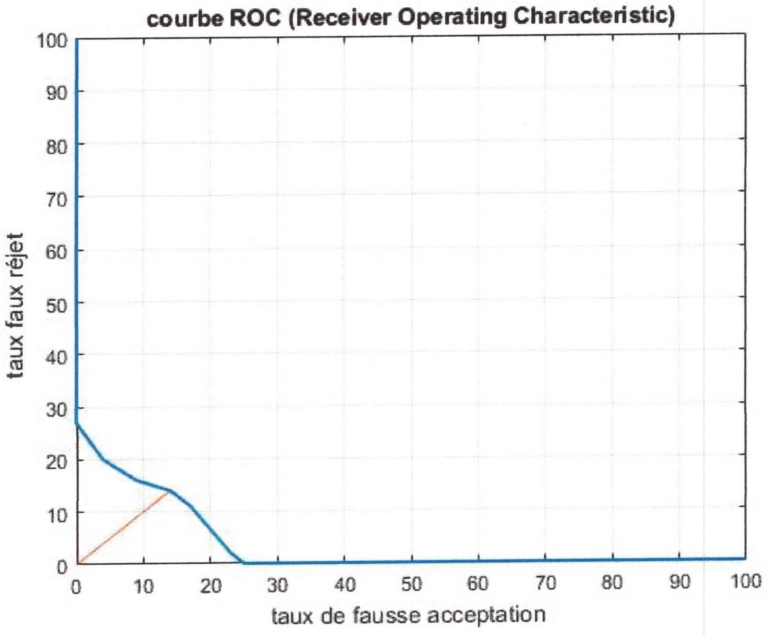

FIGURE 3.18 – Courbe ROC.

La norme L2 :

Les figures 3.19, 3.20 et 3.21 représentent respectivement le **TEE** en fonction du **seuil** et le **TFA** en fonction du **TFR**.

Résultats de la comparaison des normes L1 et L2

Les figures 3.22, 3.23 représentent le **TFR** en fonction du **TFA**. Vu les courbes de comparaison correspondant à L1 et L2, nous tirons comme conclusion que la distance L2 est meilleure que L1.

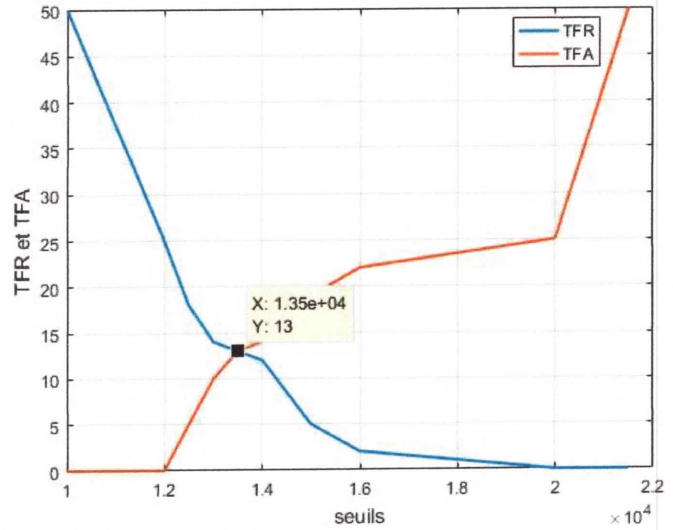

FIGURE 3.19 – TFR ET TFA en fonction de la valeur du seuil.

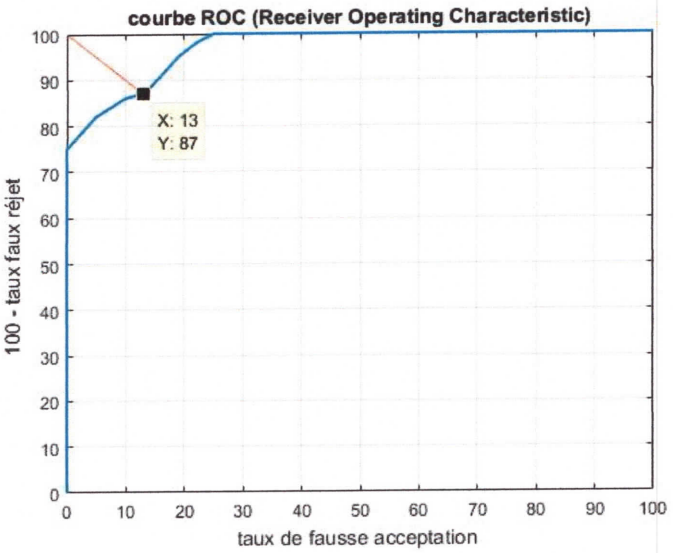

FIGURE 3.20 – Courbe ROC.

	TEE	TFA	TFR	SEUIL
L1	14%	14%	86%	38900
L2	13%	13%	87%	13500

TABLE 3.3 – Comparaison des différentes normes

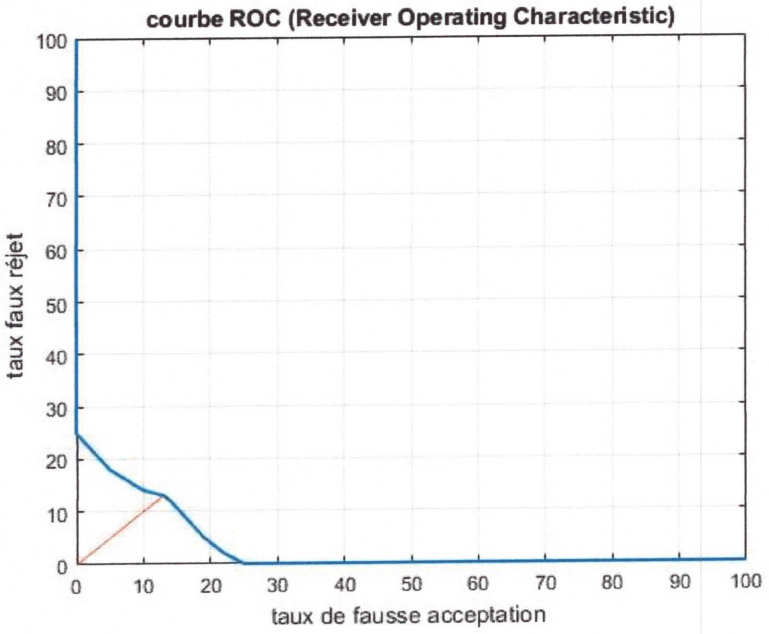

FIGURE 3.21 – Courbe ROC.

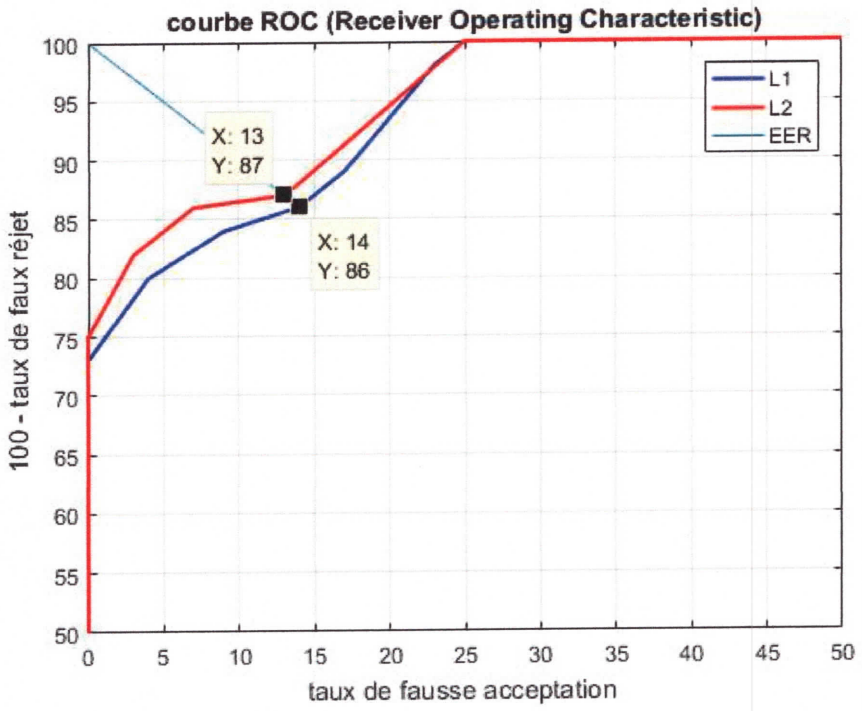

FIGURE 3.22 – Courbe ROC de la norme L1 et L2.

Discussion des résultats

La méthode de vérification basé sur la norme **L1** donne un résultat de "**TEE**=14%" pour un "**seuil** =38900" et l'évaluation par la courbe ROC montre que pour un **TFA** de 14% on a 86% de **TFR** (figures 3.16 et 3.17).

Pour la norme **L2** on a obtenu un résultat de "**TEE**=13%" pour un "**seuil** =13500" et l'évaluation par la courbe ROC montre que pour un **TFA** de 13% on a 87% de **TFR** (figures 3.19 et 3.20). D'après ces résultats, on peut constater que la norme **L2** donne des meilleurs taux d'évaluation pour le cas de l'empreinte.

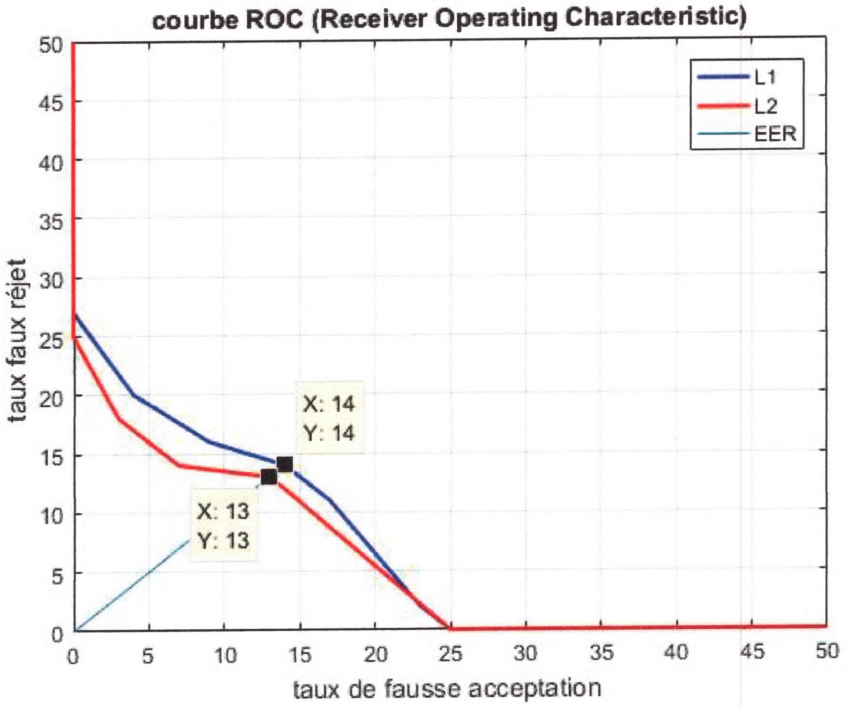

FIGURE 3.23 – Courbe ROC de la norme L1 et L2.

3.13 Fusion de deux modalités (Visage et Empreinte)

Courbe ROC de l'Empreinte,face et Fusion de l1 :

Les figures 3.24 et 3.25 représentent respectivement la courbe ROC et le **TFR** en fonction de **TFA** de la norme **L1**.

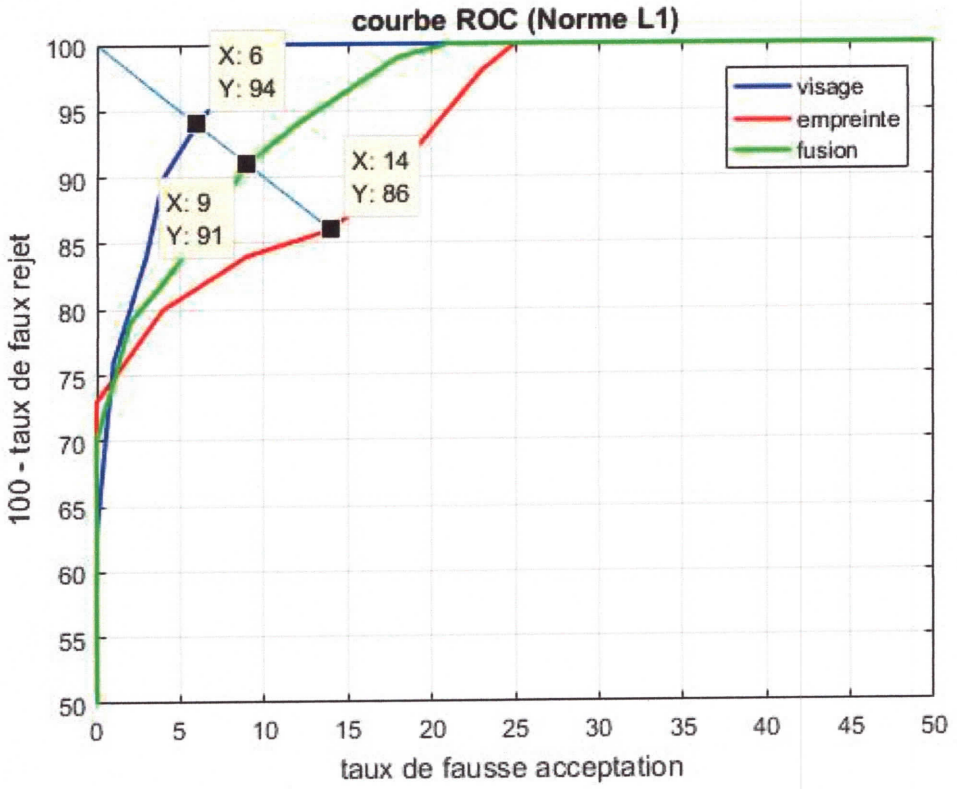

FIGURE 3.24 – Courbe de **TFR** en fonction de **TFA** de la fusion (L1).

	Visage	**Empreinte**	**Fusion**
100-TFR	94%	88%	91%
TFA	6%	14%	9%

TABLE 3.4 – Comparaison des différentes modalités selon la norme **L1**

Courbe ROC de l'empreinte,face et fusion de L2 :

Les figures 3.26 et 3.27 représentent respectivement la courbe ROC et le **TFR** en fonction de **TFA** de la norme **L2**.

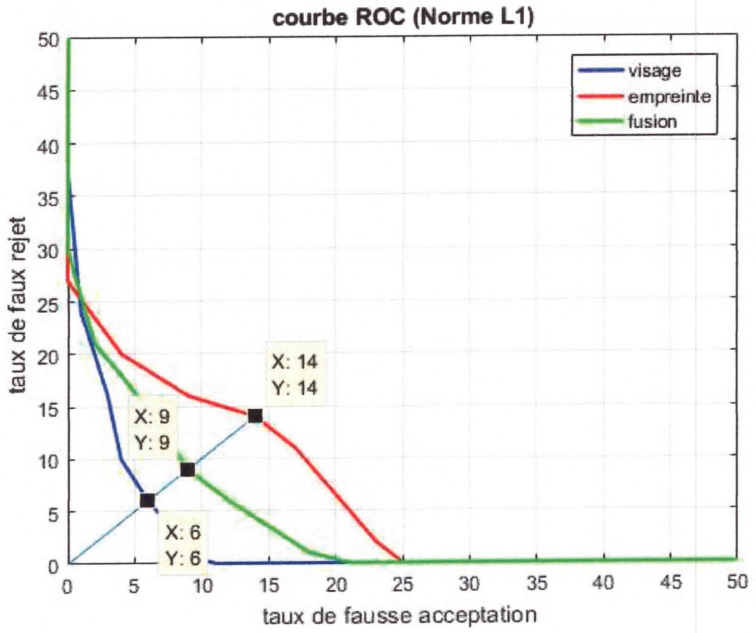

FIGURE 3.25 – Courbe ROC de la fusion de L1.

	Visage	**Empreinte**	**Fusion**
100-TFR	94%	87%	92%
TFA	6%	13%	8%

TABLE 3.5 – Comparaison des différentes modalités selon la norme **L2**

Discussion des résultats

Les figures précédentes regroupe d'une manière générale les résultats des différentes modalités et leur fusion. Ainsi on peut remarquer que la fusion de résultats de la modalité Visage avec celui de l'empreinte donne des résultats satisfaisant. Pour 92% de **TFR** pour la norme L2 contre 91% pour la norme L1, on constate que la norme L2 est meilleure que la norme L1.

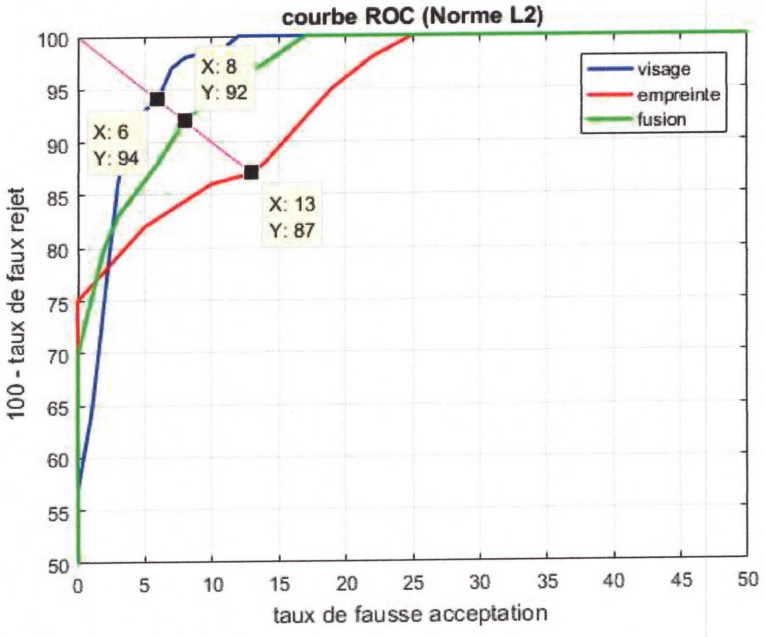

FIGURE 3.26 – Courbe de **TFR** en fonction de **TFA** de la fusion (L2).

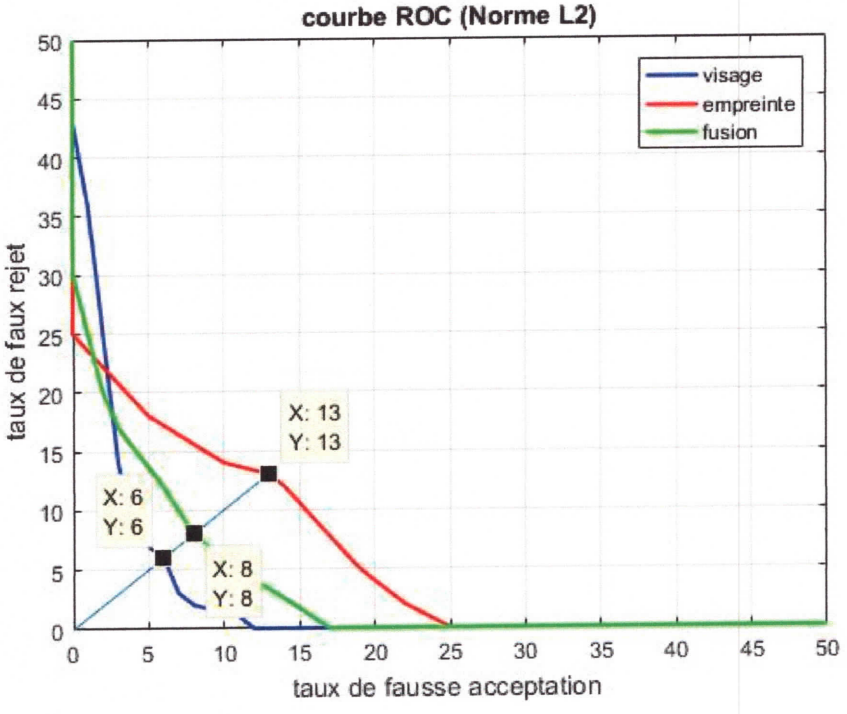

FIGURE 3.27 – Courbe ROC de la fusion de L2.

3.14 Conclusion :

Dans ce chapitre nous avons présenté les différents résultats de différentes modalités et leur fusion.

Nous avons d'abord tester le système uni-modale du Visage et de l'empreinte, puis nous les avons fusionné dans le but d'obtenir un système performant.

La fusion des deux modalités a permit d'améliorer d'avantage les résultats obtenus pour l'empreinte.

RÉALISATION

Cette partie est une étape qui nous permet d'implémenter la théorie à la pratique. A cet effet nous avons utilisé un automate pour la réaliser. Le protocole utilisé est le suivant :

1. Traiter les images de face et d'empreinte pour obtenir les 200 caractéristiques pour chacune d'elles.
2. Concaténer les 200 caractéristiques du visage avec celui de l'empreinte.
3. Faire la crypto-compression en utilsant le $SHA-1$ pour obtenir 160 bits (40 chiffres en hexadécimal).
4. Enfin coder les cartes magnétiques avec les 40 chiffres hexadécimaux.

3.14.1 La phase prétraitement :

3.14.1.1 Visage

Pour le visage, il faut d'abord convertir les images en couleur en niveaux de gris, ensuite procédé au prétraitement selon les étapes suivantes :

a. **Égalisation de l'image :** Elle a pour but d'accentuer le contraste de l'image (voir image B de la figure 3.28).

b. **Détection du Visage :**

Cette méthode d'une précision nette nous permet d'avoir juste la région concernée. (voir image C de la figure 3.28).

c. **Découpage :**

La phase finale du prétraitement est le découpage de l'image comme nous le montre la (voir image D de la figure 3.28).

3.14.1.2 Empreinte

Pour les empreintes digitales,les étapes suivantes sont nécessaire pour avoir une image exploitable :

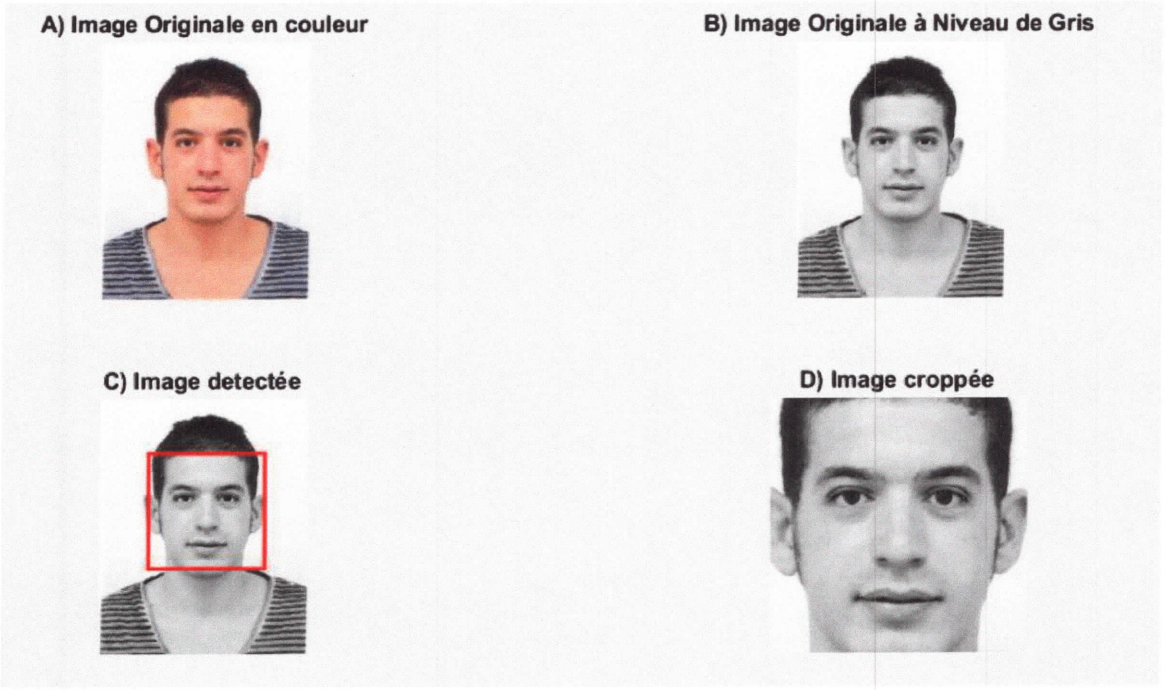

FIGURE 3.28 – Différents étapes du prétraitement du visage

a. **Binarisation :** La binarisation appelée aussi seuillage, est la technique de segmentation la plus simple. Les pixels de l'image sont partagés par un seuil T en deux classes. En général, ils sont représentés par une classe de pixels noirs et une autre classe de pixels blancs (voir image B de la figure3.29).

b. **Détection :** Celle-ci nous permet juste de sélectionner la partie essentielle de l'image (voir image C de la (**Fig** 3.29)).

c. **Découpage :**

La phase finale du prétraitement est le découpage de l'image comme nous le montre la figure 3.29 en D.

3.14.1.3 La signature digitales :

La derniere phase est l'étape de la crypto-compression où on a utilisé l'algorithme $SHA-1$. On obtient alors la signature des 40 chiffres en héxadecimal. Ci-dessous un exemple des 40 chiffres en héxadecimal.

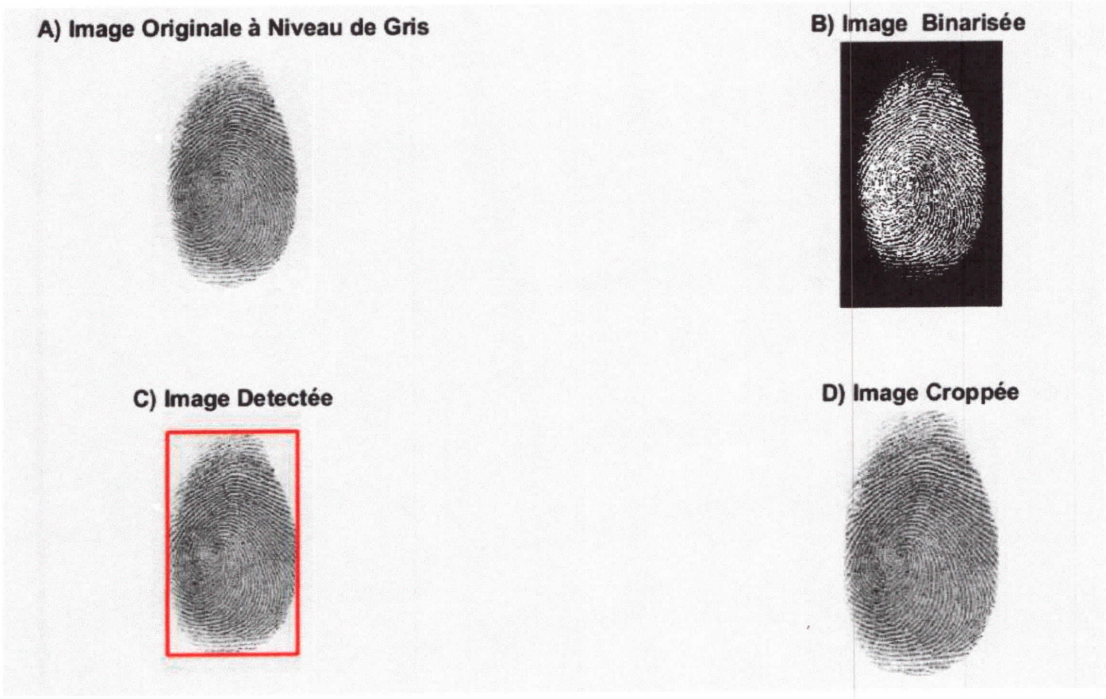

FIGURE 3.29 – Différents étapes du prétraitement de l'empreinte

Prénom/Nom	**Signature Digitale**
Cherriti Jonnaid	$54EF1DB6AC3A26C1ACD6EF1418B14620DFAAF350$

TABLE 3.6 – Exemple de signature digitale obtenue.

3.14.2 L'automate ACX5740

Cette réalisation est effectuée par un automate connu sous le nom d'**Andover Continuum**.Il est présenté dans la figure ci-dessous.

3.14.3 Câblage de l'automate :

Pour garantir la bonne alimentation de l'automate, il est nécessaire de l'alimenté par une source d'énergie fourni par un redresseur qui fournit une tension de $24V$ à la sortie lorsque l'entrée est soumise à $220V$.

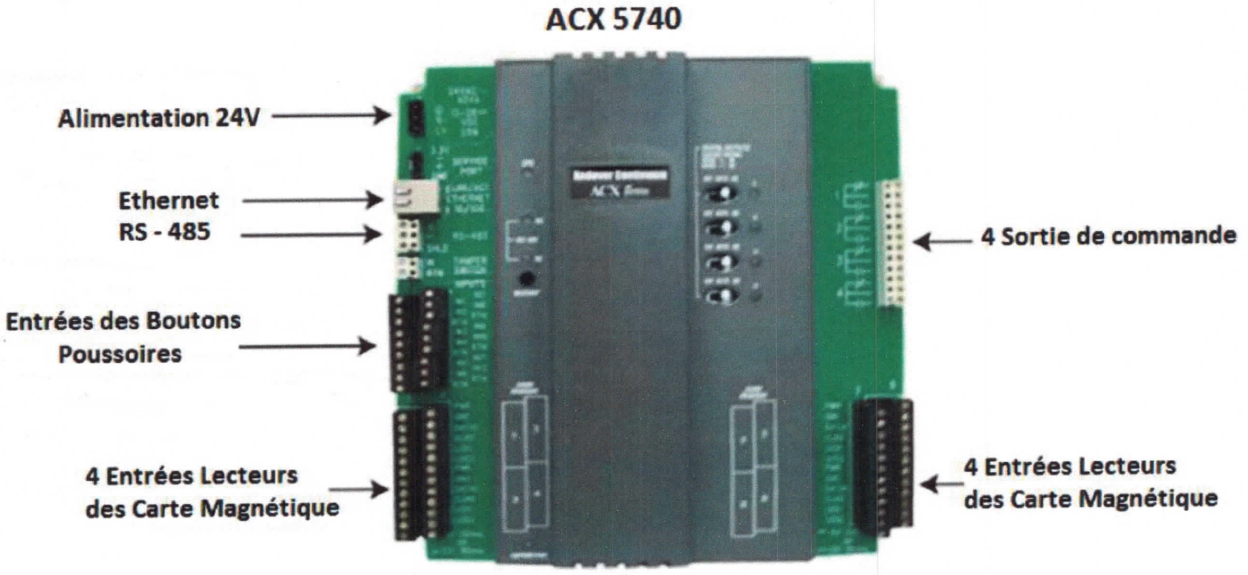

FIGURE 3.30 – Schéma de l'automate

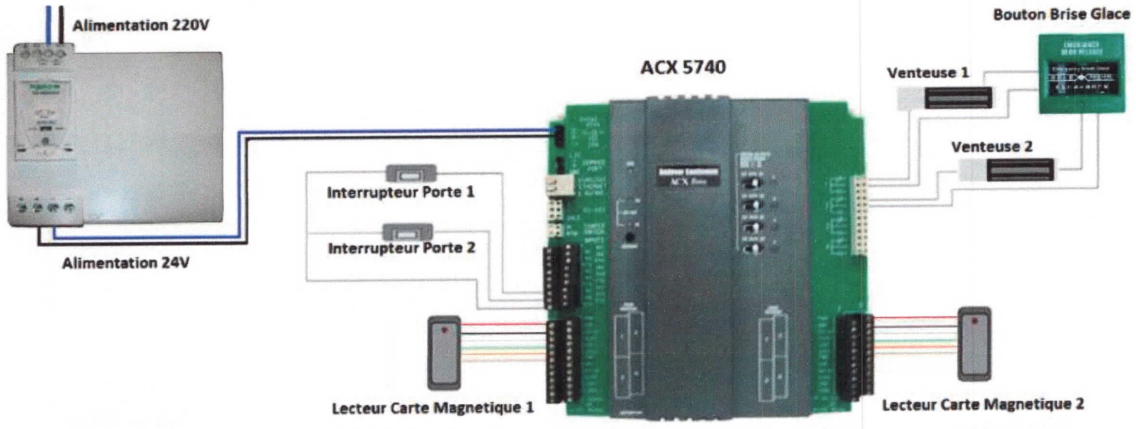

FIGURE 3.31 – Câblage de l'automate

3.14.4 Les salles à controller :

Le but de cette réalisation est de controller l'accès à deux salles à savoir :

- Une salle de réunion,
- Une salle de classe.

Les figures 3.32 et 3.33 représentent respectivement les différentes salles d'une façon générale et les portes à controller.

Et enfin nous avons clôturé par une partie destinée à la réalisation pratique pour valider la robustesse des résultats.

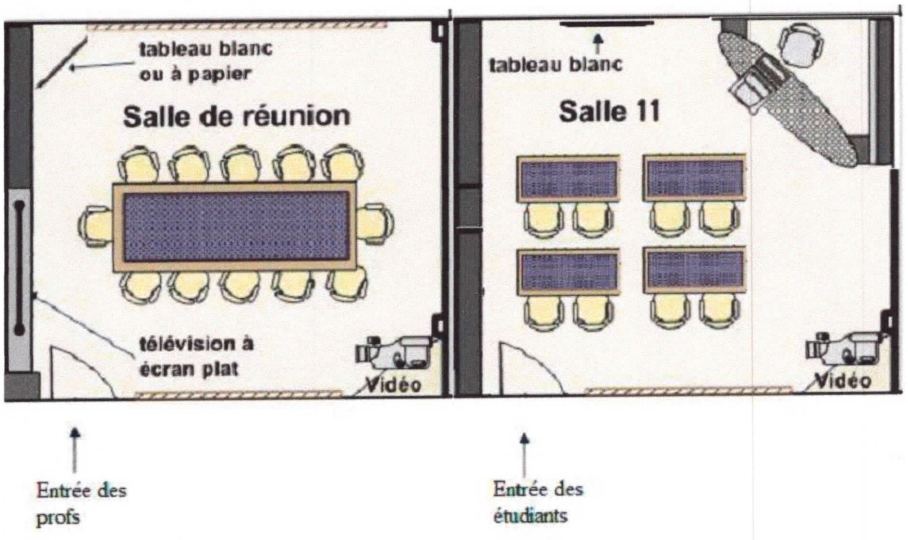

FIGURE 3.32 – Les salles d'accès

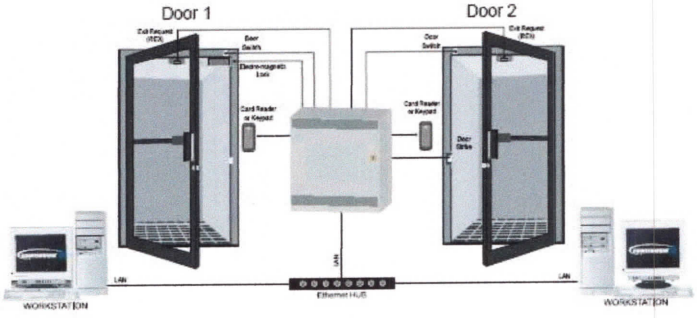

FIGURE 3.33 – Les portes à controller

CONCLUSION GÉNÉRALE

La biométrie est un domaine à la fois passionnant et complexe. Elle tente par des outils très évolués de faire la distinction entre les individus, nous obligeant à travailler dans un contexte de très grande diversité.

Ce manuscrit a été organisé en trois chapitres.Il a introduit les concepts généraux de la biométrie où nous avons présenté un état de l'art de cette dernière.

Les systèmes unimodaux ont toujours eu un niveau de sécurité moyen d'où la nécessité de fusionné plusieurs modalités. Dans ce travail, on a opté pour deux modalités biométriques à savoir : le visage et l'empreinte. Nous avons proposé un système de reconnaissance biométrique constitué principalement des étapes d'extraction de caractéristiques, de classification et de fusion de deux modalités. La fusion intervient dans le but d'améliorer les performances du système proposé. On s'est basé dans ce mémoire beaucoup plus sur l'étape d'extraction de caractéristiques. En effet cette dernière est effectué par un célèbre filtre à savoir le filtre de Gabor. Le choix de ce filtre comme extracteur est dû à ses propriétés de localisation optimale espace-fréquence. En fait, ces filtres minimisent d'une manière optimale le principe d'incertitude de Heisenberg [Ham14].

En ce qui concerne les techniques de classification, elles sont effectuées par le classificateur *K-NN* qui est détaillé dans le chapitre 2. Des tests ont été effectués et ont permis entre autres de confirmer la forme des courbes obtenue représentant la courbe ROC. A l'issue du travail réalisé, nous pouvons affirmer que les performances des systèmes multimodaux sont meilleures que celles des systèmes unimodaux.

Et enfin pour tester la robustesse de notre travail, nous avons exploiter le modèle théo-

rique proposé dans le cadre de cette étude en réalisant un système pratique de contrôle d'accès utilisant les données biométriques.

Tous les images et d'empreintes peuvent être soumises à différentes changements que ce soit standards (compression,rotation,...) ou malicieuses, alors et en perspectives nous proposons d'améliorer la robustesse du système proposé par l'ajout d'une étape garantissante cette performance à savoir la quantification.

BIBLIOGRAPHIE

[AK10] Lalita Acharya and Tomasz Kasprzycki. *La biométrie et son usage par l'État.* Bibliothèque du Parlement, 2010.

[BCP+05] Ruud M Bolle, Jonathan H Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. The relation between the roc curve and the cmc. In *Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on*, pages 15–20. IEEE, 2005.

[BK05] R Beveridge and M Kirby. Biometrics and face recognition. In *IS&T Colloquium*, page 25, 2005.

[BSC04] Dhruv Batra, Girish Singhal, and Santanu Chaudhury. Gabor filter based fingerprint classification using support vector machines. In *India Annual Conference, 2004. Proceedings of the IEEE INDICON 2004. First*, pages 256–261. IEEE, 2004.

[CDJ05] Yi Chen, Sarat C Dass, and Anil K Jain. Fingerprint quality indices for predicting authentication performance. In *Audio-and Video-Based Biometric Person Authentication*, pages 160–170. Springer, 2005.

[Cho14] Moujahdi Chouaib. Protection des systèmes de sécurité biométriques : Contributions à la protection des modèles biométriques. *Université Mohammed V-Agdal, Faculté des Sciences, Rabat*,2014.

[Dau85] John G Daugman. Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters. *JOSA A*, 2(7) :1160–1169, 1985.

[Ham14] Bourouina Rabeh Hamdellou, Haroun. Extraction et caractérisation de textures pour la classification des images, *Université de Jijel, Faculté de Science et Technologie département D'Electronique*,2014.

[HZAM13] Mohammad Haghighat, Saman Zonouz, and Mohamed Abdel-Mottaleb. Identification using encrypted biometrics. In *Computer analysis of images and patterns*, pages 440–448. Springer, 2013.

[JDN04] Anil K Jain, Sarat C Dass, and Karthik Nandakumar. Can soft biometric traits assist user recognition? In *Defense and Security*, pages 561–572. International Society for Optics and Photonics, 2004.

[JNR05] Anil Jain, Karthik Nandakumar, and Arun Ross. Score normalization in multimodal biometric systems. *Pattern recognition*, 38(12) :2270–2285, 2005.

[JV03] Michael Jones and Paul Viola. Fast multi-view face detection. *Mitsubishi Electric Research Lab TR-20003-96*, 3 :14, 2003.

[Mel09] Anouar Mellakh. *Reconnaissance des visages en conditions dégradées.* PhD thesis, Evry, Institut national des télécommunications, 2009.

[MMYH02] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamada, and Satoshi Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Electronic Imaging 2002*, pages 275–289. International Society for Optics and Photonics, 2002.

[MOZ08] Nicolas MOZIRET. *Revue des algorithmes PCA, LDA et EBGM utilises en reconnaissance 2D du visage pour la biometrie.* PhD thesis, Institut Superieur d'Electronique de Paris (ISEP), D'epartement d'Electronique, 2008.

[MOZ11] Nicolas MOZIRET. *Reconnaissance Biométrique par Fusion Multimodale du Visage et de lÍris.* PhD thesis, Ecole supérieur de Télécommunication PARISTech, 2011.

[Mus13] NASRI Mustapha. Transformations non lineaires kpca et klda pour l'authentification de visages, *Université d'Msila, Faculté de Science et Technologie département D'Electronique*,2013.

[OUA11] Abdelmalik OUAMANE. *Etude de la fusion de modalités pour l'authentification en biométrie (visage, voix).* PhD thesis, Faculté des sciences et de la technologie UMKBiskra, 2011.

[PD02] Florent Perronnin and Jean-Luc Dugelay. Introduction à la biométrie authentification des individus par traitement audio-vidéo. *TS. Traitement du signal,* 19(4) :253–265, 2002.

[VdPK00] Ton Van der Putte and Jeroen Keuning. Biometrical fingerprint recognition : don't get your fingers burned. In *Smart Card Research and Advanced Applications,* pages 289–303. Springer, 2000.