الجـــمـهوريـــــة الجـــــزائـرية الديمقـــراطيـــــة الشـــــعبيـــــة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــعليـــم العـــــــالي والبحـــــث العلـــــــمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــامعة أبي بكـر بلـــــــقـايد – تـلمســـــــــــــان –

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Télécommunication

Spécialité : Réseaux et Télécommunications (RT)

THEME

Utilisation de la biométrie pour la sécurité informatique

Réalisé par :

LIMAM Amira Hadjer **MADANI Wassila**

Soutenu en 06 juillet 2021 devant le Jury :

Mr. BOUACHA Abdelhafid	Professeur	Univ. Tlemcen	Président
Mr. IRID S.M.H.	MCA	Univ. Tlemcen	Examinateur
Mr. BOUABDELLAH Reda	MAA	Univ. Tlemcen	Encadrant
Mr. RAHMI Bachir	Doctorant	Univ. Tlemcen	Co-encadrant

Année universitaire 2020/2021

Dédicace

Je dédie ce modeste travail à :

« Ma mère Mme. **BOUHADJA Chahrazed »**
Celle que personne ne peut compenser les sacrifices qu'elle a consentis pour mon éducation et mon bien être, l'origine de ma réussite, votre soutien fut une lumière dans tout mon parcours. Autant de phrases et d'expressions aussi éloquentes soit elles ne sauraient exprimer ma gratitude envers vous, je vous dois ce que je suis aujourd'hui et ce que je serai demain.
Ce travail est pour vous.

« A mon grand-père Mr. **BOUHADJA Mohamed »**
Puisse dieu lui avoir en sa sainte miséricorde, j'espère qu'il apprécie cet humble geste comme preuve de reconnaissance de la part d'une fille qui a toujours prié pour le salut de son âme et que ce travail soit une prière pour son âme.

« A ma grand-mère Mme. **BOUHADJA Khadidja »**
Que ce travail soit l'expression des vœux que vous n'avez cessé de formuler dans vos prières.
Que Dieu vous préserve santé et longue vie.

« A mon frère et mes sœurs : **Asma, Fadela et Sara** »
Pour leur soutien et encouragement, puissent nos liens fraternels se consolider et se pérenniser encore plus.

« A ma nièce **Sirine** et mon neveu **Mohamed Chahine »**
Vous êtes mes plus beaux cadeaux, que dieu vous donne santé, bonheur, courage et réussite.

Je vous aime.

« A mes cousines **Amina** et **ibtisseme** »

« A tous mes enseignants du primaire au supérieur »
Pour leurs enseignements de qualité et leurs conseils qui nous ont permis de poursuivre notre cursus scolaire.

« A ma copine et mon binôme M^{lle}. **LIMAM Amira Hadjer »**
Pour son soutien moral, sa patience et sa compréhension tout au long de ce projet.

« A mes amies : **Asma, Chahinez, Chaimaa, Hadjer, Kawtar, Widad** et **Yousra** »

« A toute la promotion master 2 Réseaux et télécommunications »

« A vous chers lecteurs. »

Wassila

Dédicace

Tous les mots ne sauraient exprimer la gratitude, l'amour, le respect,
la reconnaissance, c'est tout simplement que :
Je dédie ce modeste travail à :

À Ma tendre Mère : Mme **Amar Belhadj Hasna**,
Tu représentes pour moi la source de tendresse
et l'exemple de dévouement qui n'a pas cessé de m'encourager.
Tu as fait plus qu'une mère puisse faire pour que ses enfants
suivent le bon chemin dans leur vie et leurs études.

À Mon très cher Père : Mr **Limam Noureddine**
Aucune dédicace ne saurait exprimer l'amour,
l'estime, le dévouement et le respect que j'ai toujours pour vous.
Rien au monde ne vaut les efforts fournis jour
et nuit pour mon éducation et mon bien être.

Ce travail et le fruit de tes sacrifices que tu as consentis
pour mon éducation et ma formation le long de ces années.

A ma belle-mère « **Asma** » et mon beau père « **Sidi Mohamed** »

À mes très chères sœurs : « **Wafaa, Ahlam, Ikram** »

A mon très cher frère :« **Djawed** »

A mon très cher fiancé « **Zine El Abidine** »

A mes très chères belles sœurs : « **Fatima** et **Ilham** », Et mon beau frére : « **Walid** »

A mes nièces et neveux :
« **Yassine, Rania, Sarah, Marwa, Yousra, Abdellah, Sidahmed,**
Wassim, Razane et Yassmine »

A ma très cher amie et mon binôme : « **Madani Wassila** »

A mes chers amis
et mes Collègues de l'Université

Et à tous ce qui ont enseigné moi au long de ma vie scolaire.
A tous ceux que je connais de près ou de loin et en particulier
ceux qui ont contribué à la réalisation de ce travail...

Amira Hadjer

Remerciement

On remercie tout d'abord **DIEU** le Tout-puissant de nous avoir donné le courage, la volonté, la patience, la santé et de nous avoir éclairci le chemin tout au long de notre vie.

Nous adressons toute notre reconnaissance et vifs remerciements à notre directeur de mémoire **Mr. Reda BOUABDALLAH** qui malgré son emploi du temps surchargé, a toujours été à l'écoute du moindre de nos besoins, pour sa qualité d'encadrement, sa patience, sa disponibilité et surtout ses judicieux conseils. Ce fut un honneur de travailler avec lui.

On tient également à remercier **Mr. Bachir RAHMI** pour son soutien, son encouragement et son guide. Cela n'aurait jamais été possible sans lui. Nous lui serons éternellement reconnaissantes.

Nous sommes sensibles à l'honneur que **Mr. Abdelhafid BOUACHA** professeur à l'université de Tlemcen, nous a fait de présider le jury de ce travail. Qu'il veuille accepter notre profond respect et notre immense estime.

Nous sommes particulièrement heureuses que **Mr. Mohamed el hadj Irid** maître assistant à l'université de Tlemcen, nous fasse l'honneur de faire partie du jury de ce mémoire. Qu'il trouve ici l'expression de nos sentiments les plus distingués.

On tient à reconnaitre notre gratitude envers nos enseignants qui ont si bien mené leur noble quête d'enseigner les bases de télécommunication. Nous les remercions pour le savoir qu'ils nous ont transmis.

Nous remercions nos parents, nos frères et sœurs pour leur présence et leur soutien. Nos amis, nos proches et toute personne qui a contribué de loin ou de près à la réalisation de ce travail.

Résumé

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques. Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance d'un individu dans un grand nombre d'applications diverses. La reconnaissance automatique de personnes a reçu beaucoup d'attention au cours des dernières années en raison de ses nombreuses applications dans différents domaines tels que les applications de sécurité. La reconnaissance faciale est l'une des meilleures modalités biométriques pour des applications liées à l'identification ou l'authentification de personnes. En effet, c'est la modalité utilisée par les humains. Elle est non intrusive et socialement bien acceptée.

Dans ce projet de fin d'étude, la technique **ACP** est utilisé pour un système d'identification de personnes par reconnaissance des visages humains, lors de ça, nous avons réalisé un programme **MATLAB** basé sur la technique des visages propres (eigenfaces) dans la base de données qu'on a créé, avec un taux de reconnaissance de 96%.

Mots clés : sécurité informatique, biométrie, reconnaissance faciale, visages propres, **ACP**.

Abstract

Biometrics is a measurement of biological characteristics for the identification or authentication of an individual based on some of his characteristics. This technique is increasingly used today to establish the recognition of an individual in a large number of diverse applications. Automatic recognition of people has received a lot of attention in recent years because of its many applications in different areas such as security applications. Facial recognition is one of the best biometric modalities for applications related to the identification or authentication of people. Indeed, It Is the modality used by humans. It Is non-intrusive and socially well accepted.

In This Project of end of study, the **PCA** technique Is used for a system of identification of people by recognition of the human faces, during That, we realized a **MATLAB** program based on the technique of the clean faces (eigenfaces) in the data base that we created, with a rate of recognition of 96%.

Keywords: IT Security, biometrics, facial recognition, eigenfaces, **PCA**.

الملخص

البيومترية هي مقياس للخصائص البيولوجية لتحديد أو مصادقة هوية الفرد بناءً على بعض خصائصه. تُستخدم هذه التقنية أكثر فأكثر اليوم لإثبات التعرف على هوية الأفراد في عدد كبير من التطبيقات المتنوعة. وقد حظي التعرف التلقائي على هوية الأشخاص باهتمام كبير في السنوات الأخيرة نظرًا لتعدد لتطبيقاته في مجالات مختلفة مثل تطبيقات الأمان، يعد التعرف على الوجه أحد أفضل الأساليب البيومترية للتطبيقات المتعلقة بتحديد هوية الأشخاص أو المصادقة عليها. في الواقع، هذه هي الطريقة التي يستخدمها البشر. إنها تمنع التطفل ومقبولة اجتماعيًا.

في نهاية هذه المذكرة، يتم استخدام تقنية PCA لنظام التعرف على الأشخاص من خلال التعرف على الوجوه البشرية. وخلال ذلك، قمنا بإنشاء برنامج MATLAB استنادًا إلى تقنية Eigenfaces في قاعدة البيانات التي أنشأناها بمعدل تعرف يصل إلى 96%.

الكلمات المفتاحية: الأمن المعلوماتي، البيومترية، التعرف على الوجوه، Eigenfaces، ACP.

Table de Matière

Chapitre 02

État de l'art de reconnaissance faciale et empreinte palmaire

Chapitre 03

Reconnaissance de visage par Eigenfaces

Chapitre 04

Résultats expérimentaux

Liste de figures

Liste des tableaux

Liste des Abréviations :

- **Abréviations :**

CLUSIF : Club de la Sécurité des systèmes d'Information Français.

RAND: Public Safety and Justice.

ADN: L'acide désoxyribonucléique.

FRR : Le taux de faux rejet**.**

FAR : Le taux de fausse acceptation.

EER : Le taux d'égale erreur.

AAM : La méthode des modèles actifs d'apparence.

SVM : Les machines à vecteurs de support.

***LBP* :** Les motifs binaires locaux.

LFA : L'analyse de caractéristiques locales.

EGM : Correspondance de graphe élastique.

EBGM : Correspondance graphique de l'Elastique Bunche.

LG-PCA : Algorithme Log Gabor de l'analyse en composantes principales.

LFA : L'analyse de caractéristiques locales.

LDA : L'analyse discriminante linéaire.

EFM : Modèle discriminant Linéaire amélioré de Fisher.

ICA : L'analyse en composantes indépendantes.

NMF : Factorisation non négative des matrices.

PCA : L'analyse en composantes principales.

K-PCA : Noyau de l'analyse en composantes principales.

K-LDA : Noyau de l'analyse discriminante linéaire.

RLDA : Régression de l'analyse discriminante linéaire.

DLDA : La directe de l'analyse discriminante linéaire.

BIC : Les approches Bayésiennes.

2-D PCA : L'analyse en composantes principales bidimensionnelle.

ADN : L'acide désoxyribonucléique.

CCD : Récepteurs à transferts de charge.

MATLAB : MATrix LABoratory.

- **Majuscules latines :**

A : Matrice.

C : Matrice de covariance.

D : Dimension de l'espace vectoriel.

$I_{i\_i}(m, n)$: Représentation matricielle d'une image de dimension m×n.

A^T **:** Transposé de la matrice U et A.

N : Nombre d'images d'apprentissage.

X : Représentation matricielle d'un ensemble d'images.

- **Minuscules Grecs :**

λi, μi : Valeurs propres.

- **Majuscules Grecs :**

Φ : Différence entre toutes images et image moyenne.

Ψ : Image moyenne de toutes images collectées.

Γi (m×n, 1) : Représentation vectorielle d'une image.

Introduction générale

Avec la croissance explosive des réseaux informatiques et le vol de données personnelles, le besoin de sécurité et d'identifier une personne devient de plus en plus nécessaire lors de la réalisation de diverses opérations comme les contrôles d'accès ou les paiements sécurisés. A ce jour, la saisie de codes alphanumériques reste la solution la plus courante. Bien que cette solution ait l'avantage d'être très simple, elle a le désavantage de ne pas reconnaitre si la personne qui a entré le mot de passe est bien celle qui prétend être. D'où, un nouveau type de méthodes est en train de naître qui est basé sur les caractéristiques physiques et comportementales de l'utilisateur tel que le visage, les empreintes palmaires et d'autres modalités. Cela semble être une solution évidente au problème ci-dessus : l'identité d'une personne est alors associée à ses caractéristiques, et non pas à ce qu'elle a ou ce qu'elle sait.

Ce système présente un grand nombre d'avantages par rapport à l'ancien système et il est largement répandu. Les caractéristiques biométriques doivent au moins assurer les clauses suivantes : l'universalité, l'unicité, la stabilité, l'acceptabilité et la non-reproductibilité.

La reconnaissance faciale sert à prendre ou capter la forme du visage d'un individu et d'extraire certaines informations pour la vérification de l'identité. Selon le système utilisé, veuillez suivre quelques instructions : L'individu doit être devant l'appareil ou il peut se déplacer à une certaine distance. Les données biométriques obtenues sont ensuite comparées avec celles de la base de données. Plusieurs méthodes ont été développées durant ces années parmi eux la méthode ACP.

Dans ce mémoire qui a pour but l'accomplissement d'un système de reconnaissance de visage avec la méthode ACP, qui est conçu pour être fiable et adapté aux environnements présentant une variabilité de luminosité, de posture, d'expressions faciales et la présence ou l'absence de composants structurels. Nous avons travaillé sur tous les niveaux du système : la détection, l'extraction des caractéristiques et la reconnaissance.

Nous avons essayé d'arriver à ce but à travers quatre chapitres, plusieurs notions et conceptions de la biométrie ont été traité :

Le premier chapitre : <<Introduction à la biométrie>>

Ce chapitre décrit la biométrie et ses modalités ainsi que leurs avantages et limites, ensuite il donne le principe de fonctionnement des systèmes biométriques et ses domaines d'applications.

Le deuxième chapitre : <<État de l'art de reconnaissance faciale et empreinte palmaire>>

Nous allons déterminer la place du visage et empreintes palmaires parmi les autres modalités, nous allons traiter par la suite leurs processus de fonctionnement tout en citant les méthodes utilisées.

Le troisième chapitre : <<la reconnaissance du visage par Eigenfaces>>

Ce chapitre présente la conception de notre système où nous allons décrire la méthode ACP, son objectif ainsi que son principe de fonctionnement.

Le quatrième chapitre : <<Résultat expérimentaux >>

Ce chapitre donne les résultats obtenus après la réalisation de notre système et l'exécution du programme qu'on a testé sur nous et nos proches.

Enfin, nous passerons en revue les principales contributions de ce mémoire et révélerons nos perspectives envisagées.

Chapitre 01

Introduction à la biométrie

1.1 Introduction

La technologie biométrique est de plus en plus utilisée dans les applications quotidiennes. Au fil de temps, l'être humain a essayé toujours et à chaque fois d'améliorer sa vie Dans plusieurs domaines surtout de vivre en sécurité (d'être sécurisé dans les lieux public, sécurisé de toute sorte de vol…). Avec le développement technologique rapide, la sécurité devient l'un des sujets les plus Préoccupants au sein de notre société et qui pose un délicat problème pour les citoyens, les entreprises et le gouvernement au niveau de la protection des informations et des données Sensibles contre le vol. Pour toutes ces raisons, il est obligatoire d'établir une nouvelle Technique de contrôle efficace, c'est pour cela la biométrie a été créer.

Dans ce chapitre, nous donnerons quelques concepts et définitions de base liés à la biométrie. Nous présenterons également le principe de fonctionnement du système biométrique, ses performances, ses différentes techniques ainsi que les systèmes multimodaux.

1.2 Définition de la biométrie

La biométrie est donnée par [1]: **« La biométrie s'applique à des particularités ou des caractères humains uniques en leur genre et mesurables, permettant de reconnaître ou de vérifier automatiquement l'identité ».**

La biométrie est une technologie complète qui vise à établir l'identité d'une personne en mesurant l'une des caractéristiques physiques d'une personne. Il peut y avoir plusieurs types de caractéristiques physiques, dont certaines sont plus fiables que d'autres, mais toutes ces caractéristiques doivent être inviolables et uniques pour représenter une personne.

En revanche, comme nous le verrons, les propriétés physiques sont loin d'être parfaites et précises, et nous avons rapidement atteint les limites de ces technologies.

Le mot **biométrie** est la traduction du mot anglais « **biométrics** », qui correspond à l'identification en français. Il fait référence à l'étude quantitative de la biologie au sens large, mais dans le contexte de la reconnaissance d'individus il est défini par [2]**:**

1. Selon le **CLUSIF** : la biométrie est la science qui étudie à l'aide des mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé.

2. Selon la **RAND** : la biométrie est définie comme toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier son identité.

1.3 Les propriétés d'une modalité biométrique

La vérification d'identité par la technologie biométrique est plus forte que l'utilisation de méthodes d'authentification conventionnelles (comme les cartes, les clés ou les mots de passe) car elle forme un lien puissant et durable entre la personne physique et son identité Les propriétés principales d'une modalité biométrique sont :

- **L'universalité** : Cela signifie que l'ensemble de la population doit avoir ce modèle (caractéristiques physiques ou comportementales).
- **L'unicité :** Signifie que deux personnes distinctes doivent posséder des caractéristiques biologiques différentes.
- **La stabilité :** C'est la stabilité dans le temps, la stabilité de chacun. La technologie biométrique utilisée comme moyen de vérification d'identité doit être relativement stable sur une période de temps, et surtout, une personne doit rester stable quel que soit l'environnement de collecte (conditions extérieures humaines, conditions émotionnelles humaines).
- **L'acceptabilité** et la facilité d'usage se rapportent aux contraintes liées à l'acquisition et l'utilisation d'une modalité biométrique.
- **La non-reproductibilité :** concerne la facilité ou non à falsifier une modalité Biométrique.

Toutes les technologies biométriques n'ont pas toutes ces caractéristiques, ou du moins ont ces caractéristiques à des degrés divers. Par conséquent, aucune technologie biométrique

n'est parfaite ou idéale, mais plus ou moins adaptée à l'application. Lors du choix d'un mode biométrique, un compromis est fait entre la présence ou l'absence de certains de ces attributs selon les besoins de chaque modalité.

Méthodes	**Exemples**	**Propriétés**
Ce que vous savez	• ID de l'utilisateur • Mot de passe • Code PIN	• Partagé • De nombreux mots de passe sont faciles à deviner • Oublié
Ce que vous avez	• Cartes • Badges • Clés	• Partagé • Peuvent être dupliqués • Perdus ou volés
Ce que vous savez et ce que vous avez	• Carte de guichet automatique • PIN	• Partagé • PIN un maillon faible (écrire le PIN sur la carte)
Quelque chose d'unique de l'utilisateur	• Empreinte digitale • Visage • Iris • La voix	• Impossible à partager • Répudiation peu probable • Falsification difficile • Ne peut être perdu ou volé

Tableau 1. 1: Propriétés d'une modalité biométrique [3]

1.4 Les différentes modalités biométriques

Il existe plusieurs techniques biométriques utilisées dans divers secteurs, on peut distinguer deux types : [4]

1.4.1 Modalités morphologiques (physiologiques)

Elles reposent sur la détermination des caractéristiques physiques spécifiques (uniques et permanentes) de chaque personne. On cite :

- L’empreintes digitales
- La géométrie de la main
- L’iris
- Le visage
- L'empreinte palmaire
- La Rétine

1.4.2 Modalités comportementales

Elles reposent sur l’analyse de certains comportements d’une personne.

- La signature
- La dynamique de frappe au clavier
- La Voix
- La Démarche

1.5 Description des principales techniques biométriques

1.5.1 l’empreinte digitale

L'utilisation des empreintes digitales pour l'identification est l'une des premières biométries, basée sur le fait que chacun possède une empreinte digitale unique. Le lecteur d'empreintes

digitales scanne et capte les éléments permettant de distinguer les empreintes digitales. Ces éléments sont appelés minuties.

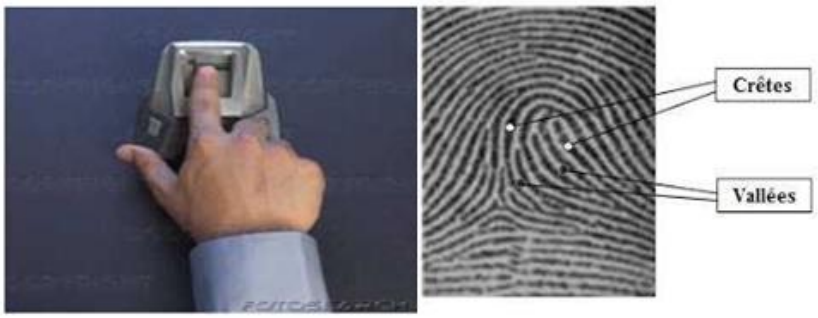

Figure 1. 1: Empreinte digitale

On différencie les individus à l'aide de leurs points singuliers, d'où on distingue deux types:

1.5.1.1 Les points singuliers globaux

- **Noyau ou centre** : lieu de convergences des stries.
- **Delta** : lieu de divergences des stries.

1.5.1.2 Les points singuliers locaux

Appelés aussi minuties. Les minuties sont des changements de continuité de l'empreinte digitale. Il existe plusieurs types de minuties : lac, bifurcation, delta ou impasse...etc. Généralement une quarantaine sont extraites de la zone scannée. Statistiquement il est impossible de trouver douze points identiques chez deux individus. Figure 1.2 [5]

Figure 1. 2: Les caractéristiques d'une empreinte digitale

1.5.2 L'Iris

L'iris est la partie colorée de l'œil qui entoure la pupille noire. La reconnaissance par l'iris est très utilisée dans les applications d'identification et de vérification suite à stabilité de sa forme, plus distinctive, et unique. Elle est extrêmement fiable mais les équipements d'acquisition sont coûteux. L'acquisition de l'iris est effectuée au moyen d'une caméra pour pallier aux mouvements inévitables de la pupille. Elle est très sensible (précision, reflet...) et relativement désagréable pour l'utilisation car l'œil doit rester grand ouvert et il est éclairé par une source lumineuse pour assurer un contraste correct. [6] [7]

Figure 1. 3: L'iris

1.5.2 La rétine

La rétine est la « pellicule photographique » de l'œil**.** Elle est constituée de 4 couches de cellules et est située au fond de l'œil. Les éléments qui permettent de distinguer deux rétines sont les veines qui les tapissent. La disposition de ces veines est stable et unique. La biométrie par la rétine procure également, un haut niveau en matière de reconnaissance. Cette technologie est bien adaptée pour des applications de haute sécurité (sites militaires et nucléaires, salles de coffres forts, etc.). La disposition des veines de la rétine assure une bonne fiabilité et une haute barrière contre la fraude. L'utilisateur doit placer son œil à quelques centimètres d'un orifice de capture situé sur le lecteur de rétine. Il ne doit pas bouger et doit fixer un point vert lumineux qui effectue des rotations. A ce moment, un faisceau lumineux traverse l'œil jusqu' aux vaisseaux sanguins capillaires de la rétine. Le système localise et capture ainsi environ 400 points de référence. Après la capture d'une image de la rétine, le logiciel du dispositif de lecture découpe un anneau autour de la fovéa. Il repère l'emplacement des veines et leur orientation. Puis il les codifie dans un gabarit. Les algorithmes de l'opération restent relativement complexes [5] [8]

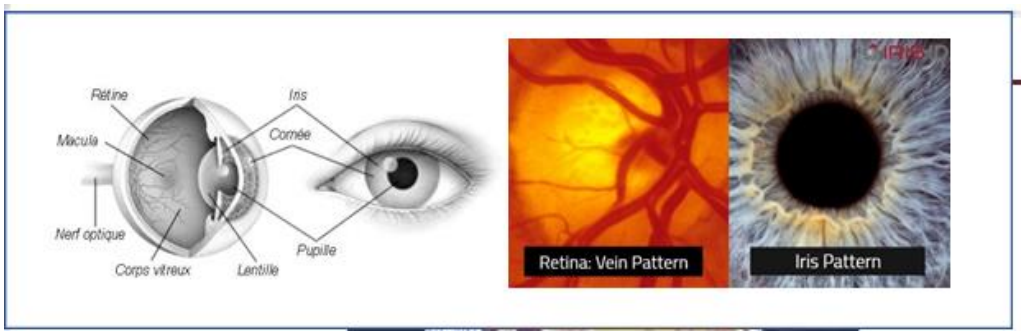

Figure 1. 4: La rétine

1.5.3 Le visage

Il s'agit de capter la forme du visage d'un individu et d'en extraire certaines informations jugées évidentes pour l'authentification. Selon le système utilisé, l'individu doit être positionné devant l'appareil où peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence. Au début des années 1970, la reconnaissance par le visage était principalement basée sur des attributs faciaux mesurables comme l'écartement des yeux, des sourcils, des lèvres, la position du menton, la forme, etc.

Depuis les années 1990, les différentes technologies utilisées exploitent toutes les découvertes effectuées dans le domaine du traitement d'image et de l'analyse de données [5]

La reconnaissance faciale est principalement utilisée comme système de surveillance ou de reconnaissance par les autorités ou les forces de police dans les lieux publics. C'est l'une des techniques les plus acceptables, mais elle nécessite un arrière-plan simple et fixe pour obtenir des résultats précis. [9]

Figure 1. 5: Le visage

1.5.4 La géométrie de la main

La géométrie de la main ou du doigt est une mesure automatisée de plusieurs dimensions, notamment la largeur de la main et des doigts et la longueur des doigts. C'est une technologie qui est rapide et bien développée et qui est facilement acceptée par les utilisateurs. Elle est n'est ni trop distinctive ni unique, ce qui la rend inadaptée pour des applications d'identification. Elle offre un taux d'erreur relativement haut et elle n'est pas utilisable avec des personnes jeunes ou âgées [6]

Figure 1. 6: La géométrie de la main

1.5.6 La voix

La voix humaine varie d'une personne à l'autre et peut se constituer de composantes physiologiques et comportementales. L'identification par la voix basée sur la forme et la taille des appendices (bouche, cavités nasales et les lèvres) utilisées dans la synthèse du son. La reconnaissance des locuteurs est plis utilisé par les téléphones, les corps policiers, les hôpitaux…etc [6].

Figure 1. 7: La voix

1.5.7 L'empreinte palmaire

Cette technique utilise la surface intérieure de la paume pour l'identification et/ou la vérification des personnes. Elle est bien adaptée pour les systèmes de moyenne sécurité telle que le contrôle d'accès physique ou logique [6].

Figure 1. 8: Empreinte palmaire

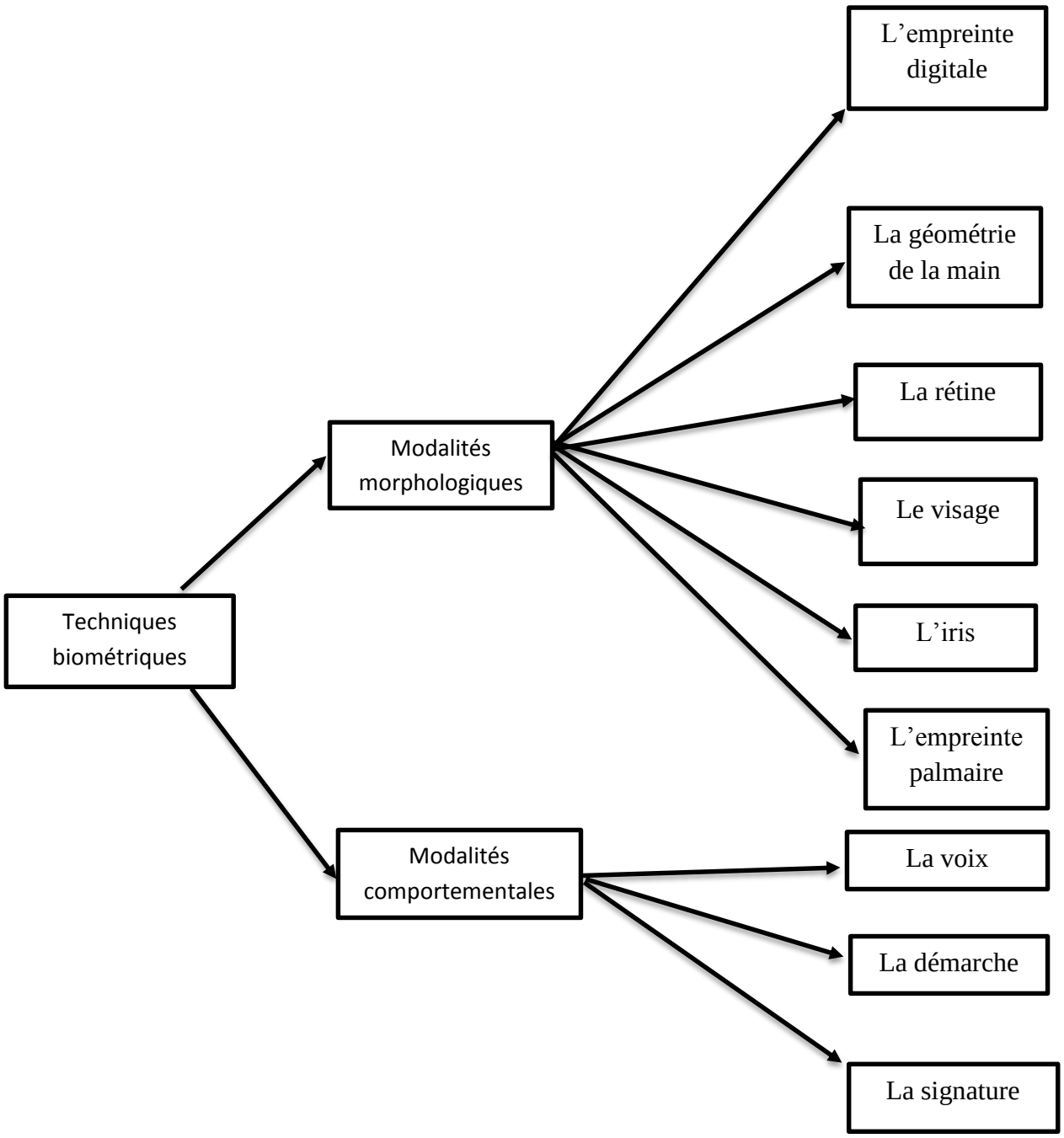

Figure 1. 9: Caractéristiques physiques des techniques biométriques

1.6 Les avantages et les inconvénients des techniques biométriques

Parmi les avantages et les inconvénients des modalités biométriques on peut citer :

Modalité	Avantages	Inconvénients
L'empreinte digitale	La technologie la plus éprouvée techniquement et la plus connue du grand public. Caractéristique difficile à dupliquer. La petite taille du lecteur facilite son intégration dans la majorité des applications (téléphones portables, PC). Faible coût des lecteurs grâce aux nouveaux capteurs de type "Chip silicium". Bon compromis entre le taux de faux rejet et le taux de fausse acceptation.	Acceptabilité moyenne de la part du grand publique. Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur). Certains systèmes peuvent accepter un moulage de doigt ou un doigt coupé (la détection du doigt vivant permet d'éviter ce type d'usurpation).
L'iris	Grande quantité d'information Contenue dans l'iris Vrais jumeaux non confondus	L'iris est aisément visibleet peut être photographié.Le problème de sécurité est alors lié aux vérifications effectuéeslors de la prise de vue.(Problème identique pourles empreintes, la voix, l'oreille, ... Mais moins pour la rétine).

La rétine	L'empreinte rétinienne est peu exposée aux blessures (coupure, brûlure,). Très difficile, voire impossible, de l'imiter. Les taux de faux rejet et de fausse acceptation sont faibles. Stable durant la vie d'un individu.	Système intrusif et mal accepté par le public, il faut placer l'œil près du capteur. Coût plus important que le coût des autres technologies. Modalité non adaptée pour un flux de passage important.
Le visage	Très bien accepté par le public Ne demande aucune action de l'usager (peu intrusive), pas de contact physique Technique peu coûteuse	Technologie sensible à l'environnement (éclairage, position, expression du visage...) Les vrais jumeaux ne sont pas différenciés Sensible aux changements (barbe, moustache, lunette...)
La géométrie de la main	Bien acceptée de la part des usagés. Très simple à utiliser. Le résultat est indépendant de l'humidité et de l'état de propreté des doigts.	Trop encombrant pour un usage sur le bureau, dans une voiture ou dans un téléphone. Risque de fausses acceptations pour des jumeaux ou des membres d'une même famille
La voix	Il est plus facile de protéger le lecteur que dans les autres technologies. Impossible d'imiter la voix. Non intrusif	Sensible à l'état physique et émotionnel de l'individu. Fraude possible par enregistrement. Sensible aux bruits ambiants Taux de faux rejets et fausses acceptations élevés

Tableau 1. 2: Les avantages et inconvénients des techniques biométriques **[5]**

1.7 Comparaison entre quelques techniques biométriques

Identifiant biométrique	Universalité	Caractère distinctif	Permanence	Facilité de saisie	Performance	Acceptabilité	Facilité de contournement
ADN	E	E	E	F	E	F	F
Oreille	M	M	E	M	M	E	M

Visage	E	F	M	E	F	E	E
Empreinte digital	M	E	E	M	E	M	M
Démarche	M	F	F	E	F	E	M
Géométrie de la main	M	M	M	E	M	M	M
Veines de la main	M	M	M	M	M	M	F
Iris	E	E	E	M	E	F	F
Dynamique de la frappe	F	F	F	M	F	M	M
Empreinte palmaire	M	E	E	M	E	M	M
Rétine	E	E	M	F	E	F	F
Signature	F	F	F	E	F	E	E
Voix	M	F	F	M	F	E	E

Tableau 1. 3: Tableau comparatif des différentes techniques biométriques **[6]**
Avec : (E : Elevé, F : faible et M : Moyen)

1.8 Les Systèmes biométriques et leurs modes de fonctionnements

1.8.1 Système biométrique

Un système biométrique est essentiellement un système de reconnaissance de formes qui fonctionne en acquérant des données biométriques à partir d'un individu, extrayant un ensemble de caractéristiques à partir des données acquises, et comparant ces caractéristiques contre la signature dans la base de données.

Il sert à vérifier l'identité d'une personne à l'aide d'une ou plusieurs modalités qui lui sont propres (voix, iris, empreintes digitales, visage …) [10].

1.8.2 Architecture d'un système biométrique

Un système biométrique comprend généralement 3 modules, grâce à ses 3 modules (apprentissage, identification, base de données), le système peut effectuer une vérification d'identité ou une identification. Il existe un quatrième module optionnel, le module

adaptateur.

:

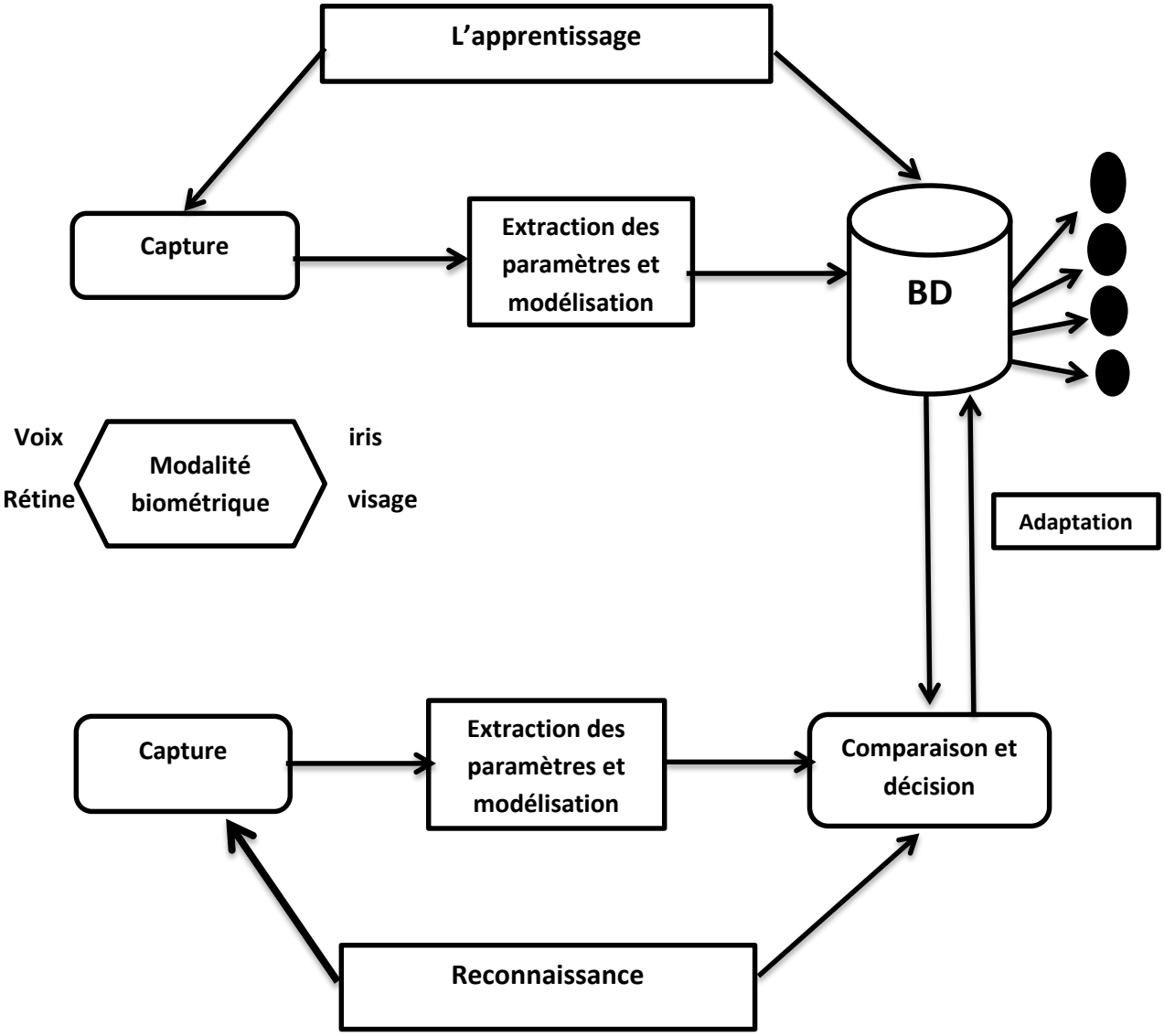

Figure 1. 10: Architecture d'un système biométrique

1.8.3 Modes de fonctionnements

Un système biométrique peut fonctionner selon trois modes :

1.8.3.1 Mode d'enrôlement

Est la phase préliminaire qui consiste en l'enregistrement des données biométriques d'une personne dans le système pour la première fois [11].

1.8.3.2 Mode d'authentification (ou vérification)

Le système répond simplement à la question « **Suis-je qui je prétends être ?** ». Il authentifie l'identité d'un individu en comparant sa caractéristique biométrique capturée avec la Template de l'identité prétendue qui est stockée dans le système. Dans un tel système, l'utilisateur devra entrer son identité et sa caractéristique biométrique, ce qui conduira à une seule comparaison la donnée capturée avec la donnée stockée, c'est une comparaison un à un **(1 :1).** Le résultat sera un rejet « la personne n'est pas qui elle prétend être » ou une acceptation « la personne est bien qui elle prétend être » [11].

1.8.3.3 Le mode d'identification

Le système répond plutôt à la question « Qui suis-je ? ». La reconnaissance de l'identité d'une personne se fera alors en cherchant dans toute la base de données du système une Template correspondante à la donnée biométrique capturée. Le système établit donc plusieurs comparaisons, c'est une comparaison du type un à plusieurs (1 : N) [11]

1.8.4 Décomposition en modules

Un système biométrique comporte quatre modules principaux [11].

1.8.4.1 Le module de capture

Qui capture la donnée biométrique d'un individu, au moyen d'un terminal de capture biométrique.

1.8.4.2 Le module d'extraction de caractéristiques

Dans lequel on traite la donnée biométrique acquise pour extraire les valeurs caractéristiques. Par exemple, la position et l'orientation.

1.8.4.3 Le module de comparaison et de prise de décision

Dans le quelles valeurs caractéristiques extraites sont comparées avec les Template stockés pour produire un résultat. Il détermine si le degré de similitude retourné par le module de comparaison est suffisant pour déterminer l'identité d'un individu.

1.8.4.4 Le module de base de données

Qui stocke les modèles biométriques des utilisateurs enrôlés. Le mode d'enregistrement est responsable d'inscrire les individus dans la base de données du système biométrique.

1.9 Les types de systèmes biométriques

1.9.1 Mono-modalité

La technologie d'identification biométrique monomode est une technologie utilisée pour authentifier les personnes sur la base d'une seule méthode d'identification biométrique. Avant de continuer à fournir des systèmes biométriques, il est nécessaire de choisir la méthode la plus adaptée à l'application.

1.9.2 Multimodalité

La reconnaissance biométrique multimodale consiste à combiner plusieurs systèmes de reconnaissance biométrique, ce qui augmente la quantité d'informations distinctives pour la personne à reconnaître. En fait, cela peut réduire certaines des limites des systèmes biométriques uni modaux. La multi modalité est une méthode alternative pour améliorer systématiquement les performances des systèmes biométriques.

1.10 Les performances des systèmes biométriques

Pour comprendre comment déterminer la performance d'un système biométrique, il nous faut définir clairement trois critères principaux [6]:

- Le premier critère s'appelle le taux de faux rejet (FRR) : Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.
- Le deuxième critère est le taux de fausse acceptation (FAR) : Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.
- Le troisième critère est connu sous le nom de taux d'égale erreur (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 1.11 montre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs.

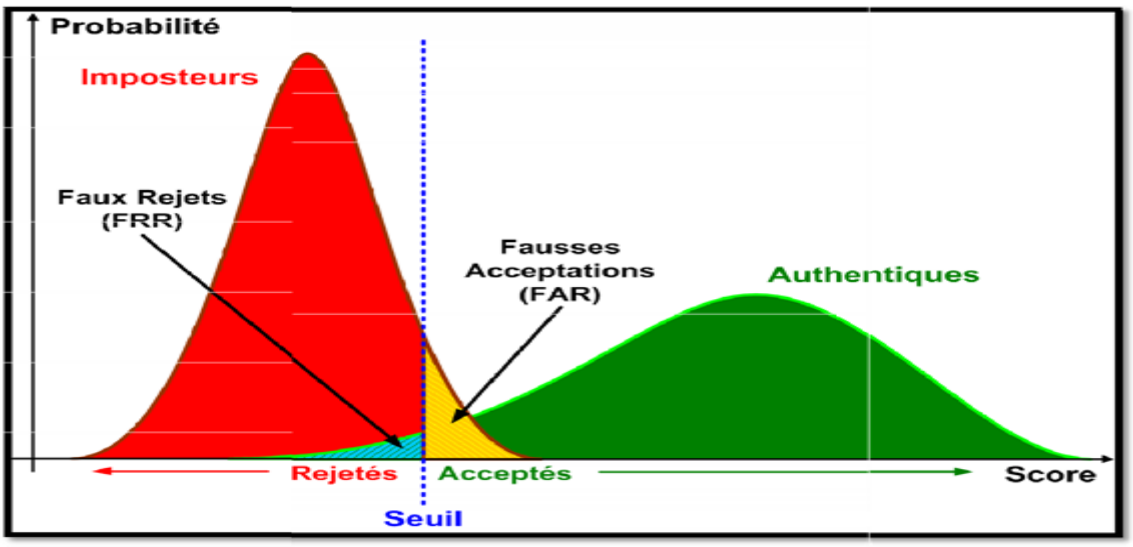

Figure 1. 11: Illustration du FRR et du FAR

1.11 Les applications de la biométrie

La technologie biométrique a été appliquée dans de nombreux domaines et ses applications sont divisées en trois catégories :

1.11.1 Applications commerciales

Telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'internet, la carte de crédit, le contrôle d'accès physique, le téléphone portable, la gestion des registres médicales, l'étude de distances, etc.…

1.11.2 Applications de gouvernement

Telles que la carte nationale d'identifications, le permis de conduite, la sécurité sociale, le contrôle de passeport, etc…

1.11.3 Applications juridiques

Telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc…

Figure 1. 12: Applications biométriques

1.12 Conclusion

Nous avons introduit dans ce premier chapitre la notion de la biométrie et ses différentes modalités utilisées dans les systèmes biométriques pour l'identification des personnes, les avantages et inconvénients de chaque modalité ainsi que la comparaison entre quelques techniques biométriques. Ensuite nous avons défini le système biométrique et son mode de fonctionnement, domaine d'application, l'architecture, les types de systèmes biométriques et leurs performances.

Nous présenterons dans le chapitre suivant un état de l'art sur la reconnaissance faciale et l'empreinte palmaire.

Chapitre 02

État de l’art de reconnaissance faciale et empreinte palmaire

2.1 Introduction

L'objectif de ce chapitre est de donner une vue générale des méthodes les plus courantes pour la reconnaissance de visage et d'empreinte palmaire.

La reconnaissance faciale est la technologie la plus acceptable en biométrie, elle a reçu de plus en plus d'attention dans le domaine de la recherche en raison de ses caractéristiques. En fait, le visage est naturel, non invasif et facile à utiliser. De nombreuses méthodes de reconnaissance faciale sont proposées depuis plus de trente ans, mais les systèmes de reconnaissance faciale sont encore complexes et posent un énorme défi aux chercheurs.

D'autre part, Les empreintes palmaires ont de nombreuses caractéristiques qui les distingue des autres modalités. Cela nous a poussé à lesss considérer comme un choix approprié pour notre étude. Nous avons présenté la reconnaissance palmaire, ses caractéristiques ainsi que son système de reconnaissance.

2.2 La reconnaissance de visage

Il existe de nombreuses raisons de choisir la reconnaissance faciale. Cela comprend les éléments suivants :

- Il ne nécessite aucune interaction physique pour le compte de l'utilisateur.
- Il est précis et permet des taux d'inscription et de vérification élevés.
- Il ne nécessite pas un expert pour interpréter le résultat de la comparaison.
- Il peut utiliser l'infrastructure de votre matériel existant, les caméras existantes et des dispositifs de capture d'image.
- Il est le seul biométrique qui vous permet d'effectuer l'identification passive dans de nombreux environnements (par exemple : identifier un terroriste dans un terminal de l'aéroport occupé).

La reconnaissance automatique de visage a pour but de reconnaitre l'identité d'un individu automatiquement à partir de l'image de visage. On peut distinguer deux types de reconnaissances :

2.2.1 Types de reconnaissance de visage

2.2.1.1 Reconnaissance par identification

La personne qui veut accéder au système sécurisé ne proclame pas son identité.

L'algorithme d'identification compare l'image en entrée avec tous les modèles pré-appris de toutes les personnes enregistrées. Il obtient un score et il prend une décision binaire (oui/non).

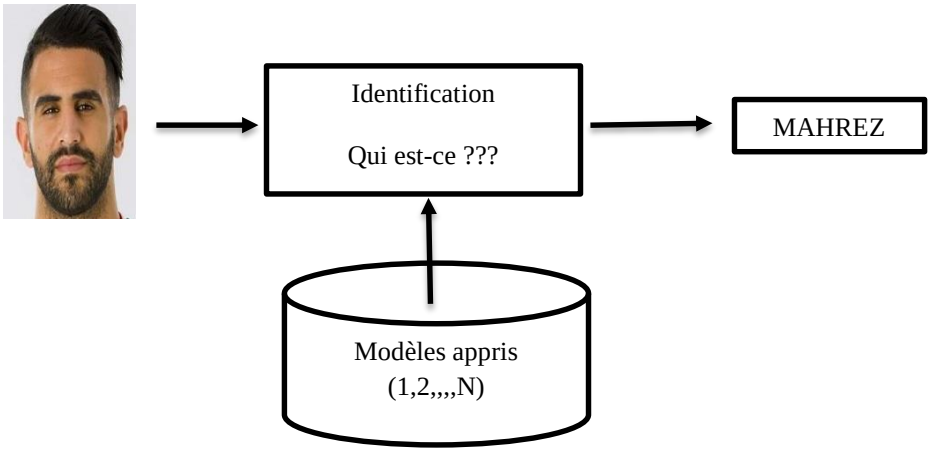

Figure 2. 1: Reconnaissance par identification

2.2.1.2 Reconnaissance par Vérification

La personne qui veut accéder au système proclame son identité. L'algorithme de vérification compare l'image en entrée avec le modèle pré-appris de cette personne. Ensuite Il prend une décision binaire (oui/non).

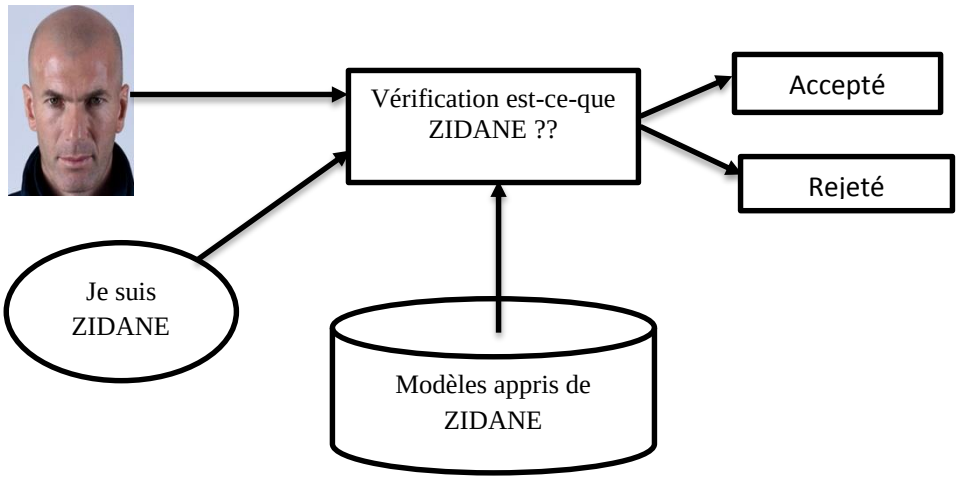

Figure 2. 2: Reconnaissance par vérification

2.2.2 Processus d'un système de reconnaissance de visage

Il y a plusieurs étapes dans ce processus, qui peuvent être illustrées par la figure suivante :

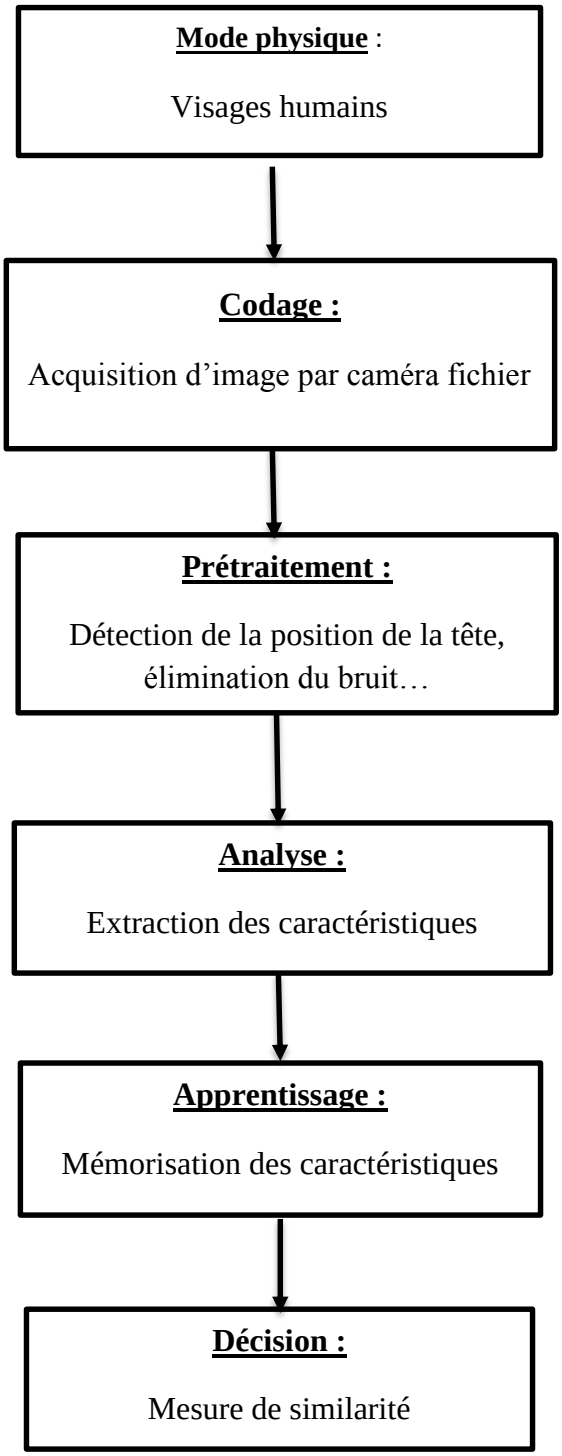

Figure 2. 3: Processus d'un système de reconnaissance de visage

Donc pour être identifié, l'image de la personne dans le système de reconnaissance faciale suit les étapes suivantes [6]:

2.2.2.1 Le mode physique (L’extérieur)

C’est le mode réel en dehors du système avant l’acquisition de l’image. Dans cette étape, on tient compte généralement de trois paramètres essentiels : l'éclairage, la variation de posture et l'échelle.

La variation de l'un de ces trois paramètres peut conduire à une distance entre deux images du même individu, supérieure à celle séparant deux images de deux individus différents, et par conséquence une fausse identification.

2.2.2.2 Acquisition de l’image

Cette étape consiste à utiliser un appareil photo ou à utiliser une caméra pour extraire dynamiquement l'image de l'utilisateur du monde extérieur. Après cela, l'image extraite sera numérisée, résultant en une représentation bidimensionnelle du visage, comportant une matrice en niveaux de gris. L'image de cette étape est dans son état d'origine, ce qui crée un risque de bruit et réduit les performances du système.

2.2.2.3 Prétraitements

La fonction de cette étape est d'éliminer les parasites causés par la qualité des équipements optiques ou électroniques lors de l'acquisition de l'image d'entrée, afin que seules les informations nécessaires soient conservées, préparant ainsi l'image pour la « prochaine étape ». Ceci est essentiel car vous n'obtiendrez jamais une image sans bruit en raison de l'arrière-plan et d'une lumière généralement inconnue. Il existe plusieurs types de traitement et d'amélioration de la qualité d'image, tels que : la normalisation, l'égalisation et le filtrage médian. Cette étape peut également inclure la détection et la localisation de visages humains dans l'image, notamment lorsque l'arrière-plan est très complexe.

2.2.2.4 Extraction de paramètres

En plus de la classification, l’étape de l’extraction des paramètres représente le cœur du système de reconnaissance, elle permet d’effectuer le traitement de l’image dans un autre

espace de travail plus simple et qui garantit une meilleure exploitation de données, et donc permettre l’utilisation, seulement, des informations utiles, discriminantes et non redondantes.

2.2.2.5 Classification (Modélisation)

Cette étape comprend la modélisation des paramètres extraits d'un visage ou d'un groupe de visages de l'individu en fonction des caractéristiques communes de l'individu. Un modèle est un ensemble d'informations utiles, différenciées et non redondantes permettant de caractériser un ou plusieurs individus similaires.

2.2.2.6 Apprentissage

C’est l’étape où on fait apprendre les individus au système. Il comprend des paramètres de mémoire, qui sont extraits et classés dans une base de données ordonnée pour faciliter l'étape de reconnaissance et de prise de décision. C'est une sorte de mémoire système.

2.2.2.7 Décision

Il s'agit de l'étape permettant de faire la distinction entre un système d'identification personnelle et un système de vérification. Dans cette étape, le système de reconnaissance comprend la recherche du modèle de visage le plus approprié en tant qu'entrée des visages stockés dans la base de données, qui est caractérisé par son taux de reconnaissance. En revanche, dans le système de vérification, il s'agit de déterminer si le visage d'entrée est bien le visage de l'individu revendiqué (modèle) ou un imposteur, qui se caractérise par son EER (égal taux d'erreur).

2.2.3 Principe de fonctionnement d’un système de reconnaissance de visage

La reconnaissance faciale automatique est principalement divisée en deux modules :

2.2.3.1 Module de détection/normalisation

Il est chargé de détecter et/ou de localiser le visage dans l'image ou la vidéo en effectuant une éventuelle normalisation pour restaurer le visage à la taille standard

2.2.3.2 Module de reconnaissance

Le module est divisé en trois étapes, c'est-à-dire que le prétraitement vise à segmenter l'image du visage en éliminant les artefacts, puis passe à la deuxième étape, l'extraction des caractéristiques, et la dernière étape consiste à combiner les empreintes biologiques testées avec toutes celles stockées dans une base de données (appelée galerie). Pour prendre enfin une décision sur l’appartenance d’un individu à l’ensemble des visages ou pas.

2.2.4 Organigramme des méthodes de reconnaissance faciale

Nous pouvons diviser les méthodes de reconnaissance faciale en trois catégories : les méthodes locales, les méthodes globales et les méthodes hybrides.

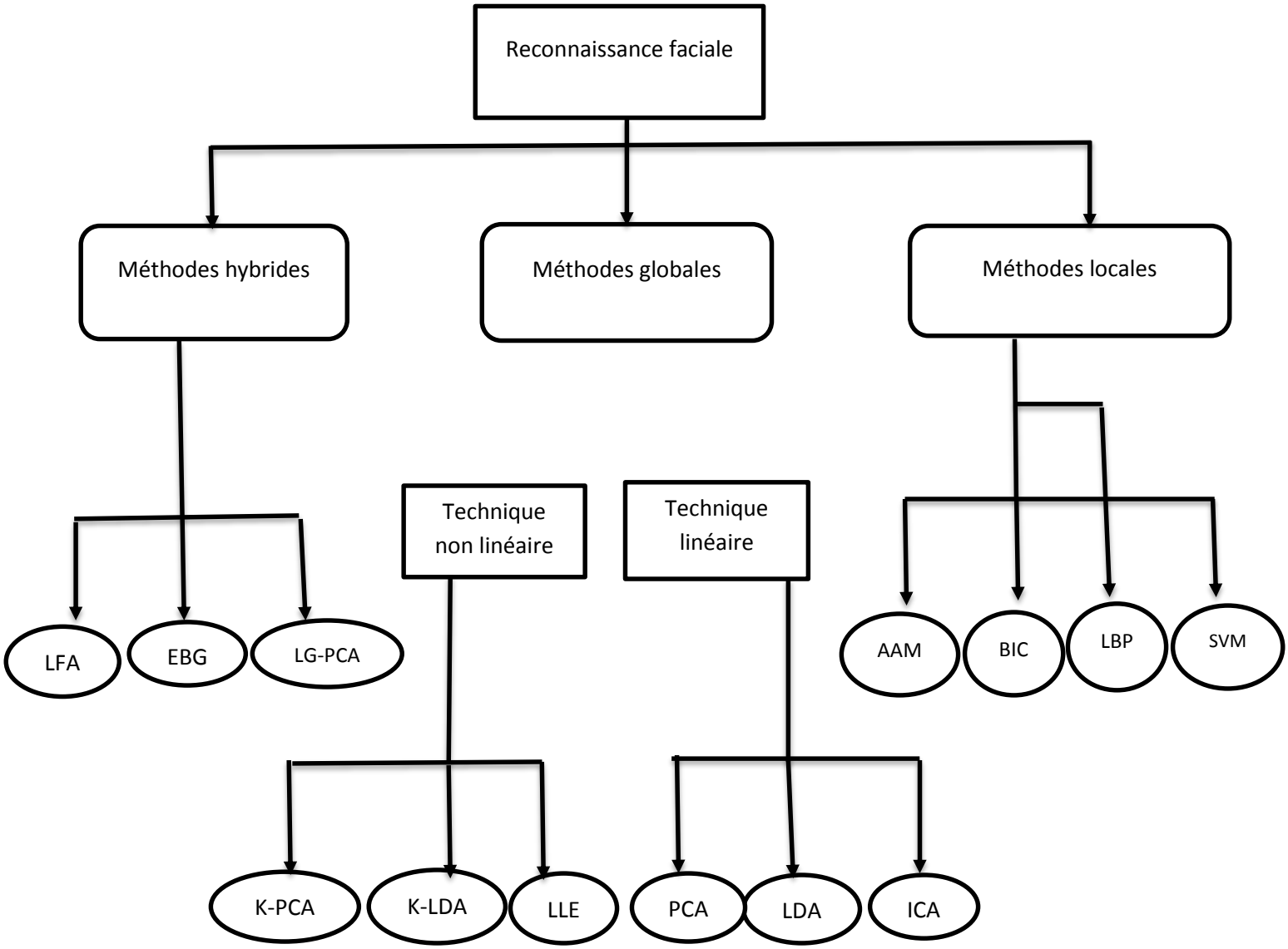

Figure 2. 4: Classification des algorithmes principaux utilisés en reconnaissance de visage

2.2.4.1 Méthodes globales

La méthode globale, également appelée méthode holistique, est un principe dans lequel toute la surface du visage est utilisée comme source d'information lorsque l'algorithme est entré, et les caractéristiques locales du visage, telles que les yeux et le nez, ne sont pas prises en compte. Ces technologies sont très réussies et bien documentées, elles offrent donc de très

bonnes performances. Mais le problème du stockage des informations extraites lors de la phase d'apprentissage reste le problème principal de cette méthode

Généralement, ces méthodes sont basées sur des techniques d'analyse statistique bien connues [12].

On distingue deux types de techniques dans l'approche globale : « les techniques linéaires » et « les techniques non linéaires » [6].

2.2.4.1.1 Les techniques linéaires

La technologie linéaire projette linéairement les données d'un espace de grande dimension (tel que l'espace de l'image d'origine) vers un sous-espace de faible dimension. Dans le sous-espace linéaire, la distance est utilisée pour comparer les vecteurs de données. La technique linéaire la plus connue est peut-être (ACP), également connue sous le nom de transformation de Karhunen-Loeve. Une autre méthode qui vise à représenter des visages sans utiliser le concept de classes est (NMF) ou (ICA).

Cependant, l'ACP classique doit convertir l'image du visage en un vecteur, ce qui détruit la structure géométrique de l'image. Afin de ne pas perdre l'information de voisinage lors du passage de l'image au vecteur, une méthode (2-D ACP) est étudiée. Cette méthode prend une image en entrée, et non plus un vecteur. Il existe d'autres techniques basées sur la décomposition linéaire, tel que (LDA) qui est l'une des méthodes de reconnaissance faciale les plus couramment utilisées, le modèle (EFM), le LDA direct (DLDA) et le RLDA (régression LDA).

2.2.4.1.2 Les techniques non linéaires

Afin de pouvoir traiter les problèmes non linéaires de la reconnaissance faciale, cette méthode linéaire a été étendue aux techniques non linéaires basées sur les concepts mathématiques du noyau ("**kernel**"), tels que le noyau PCA, le noyau LDA et le noyau ICA.

2.2.4.2 Méthodes locales

Les méthodes locales sont également appelées méthode à traits, géométriques, à caractéristiques locales, ou analytiques. L'analyse du visage humain est donnée par la description individuelle de ses parties et de leurs relations. Ce modèle convient à la manière avec laquelle l'être humain perçoit le visage, c'est à dire, à nos notions de traits de visage et de parties comme les yeux, le nez, la bouche, etc… [12].

Catégorie	Traits
Yeux	Forme, couleur, distance entre les yeux
Bouche	Gabarit, largeur, superficie de la bouche ouverte
Sourcils	Séparation, épaisseur
Cheveux	Intensité, forme, couleur
Lèvres	Largeur, forme, couleur
Joues	Intensité
Nez	Longueur, largeur
Distances	d (yeux, centre du nez), d (menton, bouche)…
Rapports	d (centre de la face, bouche)/d(menton, bouche)…

Tableau 2. 1: Traits utilisés pour identifier un visage par la méthode locale

Les approches Bayésiennes (comme la méthode BIC), (**SVM**), la méthode des (**AAM**) ou encore la méthode (**LBP**) ont été utilisées dans ce but.

Par rapport aux méthodes globales, l'avantage de toutes ces méthodes est qu'il est plus facile de modéliser les changements de pose, d'éclairage et d'expression. Cependant, ils sont plus lourds à utiliser, car ils nécessitent généralement de placer manuellement un certain nombre de points sur le visage, ce qui peut être fait automatiquement et de manière assez fiable par l'algorithme de détection.

2.2.4.3 Les méthodes hybrides

La méthode hybride associée les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurelles) avec l'extraction de caractéristiques d'apparence locale. La technologie hybride est similaire à la fonction du système visuel humain, qui peut améliorer la stabilité des performances de reconnaissance lorsque la posture, la lumière et les expressions faciales changent. Les caractéristiques

extraites par (LFA) et les ondelettes de Gabor, telles que (EGM) et (EBGM), et PCA (LG-PCA) sont des algorithmes hybrides typiques [6].

Le tableau 4 résume qualitativement les différences entre les deux types de caractéristiques [12].

Facteurs de variations	Caractéristiques locales	Caractéristiques globales
Illuminations	Très sensible	Sensible
Expressions	Non sensible	Sensible
Pose	Sensible	Très Sensible
Bruit	Très sensible	Sensible
Occlusion	Pas sensible	Très Sensible

Tableau 2. 2: Comparaison des méthodes basées sur les caractéristiques locales ou globales

Nous pouvons voir que les caractéristiques locales et globales réagissent différemment aux facteurs de variation. Par exemple, les changements d'illumination peuvent avoir plus d'influence sur les caractéristiques locales, tandis que les changements d'expression ont plus d'impact sur les caractéristiques holistiques. Ainsi, les méthodes hybrides peuvent constituer une approche efficace pour réduire la complexité des classificateurs et améliorer leur capacité de généralisation.

2.2.5 Principales difficultés de la reconnaissance de visage

Pour le cerveau humain, le processus de reconnaissance des visages humains est une tâche visuelle avancée. Bien que les humains puissent détecter et reconnaître sans effort les visages dans une scène, la construction d'un système automatisé pour effectuer de telles tâches est un sérieux défi. Ce défi devient encore plus important lorsque les conditions d'acquisition d'images varient considérablement. Il existe deux types de changements liés aux images faciales : inter-sujet et intra-sujet. En raison de la similitude physique entre les individus, les différences entre les sujets sont limitées. D'un autre côté, il existe de grandes différences au sein du corps principal. [13]

2.2.5.1 Changement d'illumination

Lors de la prise de vue, l'apparence du visage dans l'image variera considérablement en fonction de la lumière de la scène (voir Figure 2.5). Les changements de lumière rendent très difficile la reconnaissance des visages. En fait, les changements d'apparence du visage dus à l'éclairage sont parfois plus importants que les différences physiques entre les individus et peuvent conduire à une mauvaise classification des images d'entrée. Cela a été observé grâce aux expériences d'Adini et al., dans lesquelles l'auteur a utilisé une base de données de 25 individus. Par conséquent, la reconnaissance faciale dans des environnements non contrôlés est encore un domaine de recherche ouvert.

Figure 2. 5: Exemple de changement d'illumination

2.2.5.2 Variation de pose

Lorsqu'il y a un changement de posture dans l'image, le taux de reconnaissance faciale diminue fortement. Des tests d'évaluation développés sur la base de FERET et FRVT ont prouvé cette difficulté. Les changements de posture sont considérés comme le principal problème des systèmes de reconnaissance faciale. Lorsque le visage est sur le côté dans le plan image (direction <30°), il peut être normalisé en détectant au moins deux traits du visage (à travers les yeux). Cependant, lorsque la rotation est supérieure à 30°, la normalisation géométrique n'est plus possible (voir Figure 2.6).

Figure 2. 6: Exemple de variation de pose

2.2.5.3 Expressions faciales

L'expression faciale est un autre facteur qui affecte l'apparence du visage (voir la figure 2.7). La déformation faciale causée par les expressions faciales est principalement concentrée dans la partie inférieure du visage. Les informations faciales situées sur la partie supérieure du visage restent quasiment inchangées. L'identification est généralement suffisante. Cependant, comme les expressions faciales modifient l'apparence du visage, cela entraîne inévitablement une diminution du taux de reconnaissance. La reconnaissance des expressions faciales est un problème qui existe toujours et n'a pas été résolu. Les informations temporelles fournissent des connaissances supplémentaires importantes qui peuvent être utilisées pour résoudre ce problème.

Figure 2. 7: Exemple d’expressions faciales

2.2.5.4 Présence ou absence des composants structurels

La présence de composants structurels tels que des barbes, des moustaches ou des lunettes peut modifier considérablement les traits du visage, tels que la forme, la couleur ou la taille

du visage. De plus, ces composants peuvent masquer des traits faciaux de base, provoquant l'échec du système de reconnaissance. Par exemple, les lunettes opaques ne peuvent pas distinguer clairement la forme et la couleur des yeux, et la barbe ou la moustache peut changer la forme du visage.

Figure 2. 8: Exemple de présence ou absence des composants structurels

2.2.5.5 Les vrais jumeaux

Qui ont le même indicatif d'ADN, peuvent tromper les personnes qui ne les connaissent pas (les personnes familières avec les jumeaux ont reçu une grande quantité d'information sur ces derniers et sont donc beaucoup plus qualifies à distinguer les jumeaux.). Il est peu probable que la vérification automatique de visage, ne pourra jamais détecter les différences très subtiles qui existent entre les jumeaux.

Figure 2. 9: Exemple des vrais jumeaux

2.3 Reconnaissance par empreinte palmaire

L'empreinte palmaire a de nombreuse caractéristique qui les distingue des autres modalités. Cela nous a poussés à la considérer comme un choix approprié pour notre étude expérimentale qui est exposé dans ce chapitre. Ainsi, nous avons présentés la reconnaissance palmaire et ces caractéristiques et ce système de reconnaissance.

2.3.1 Définition d’une empreinte palmaire

Par définition, On appelle paume de la main la partie intérieure de la main (partie non visible lorsque la main est fermée) du poignet aux racines des doigts. Ainsi, l'empreinte palmaire n'est autre que l'impression (image) de la paume de la main faite par la pression de cette dernière sur une surface donnée. En d'autres termes, elle peut être définie comme étant le modèle de la paume de la main illustrant les caractéristiques physiques du motif de sa peau tel que les lignes (principales et rides), points, minutie et texture. [14]

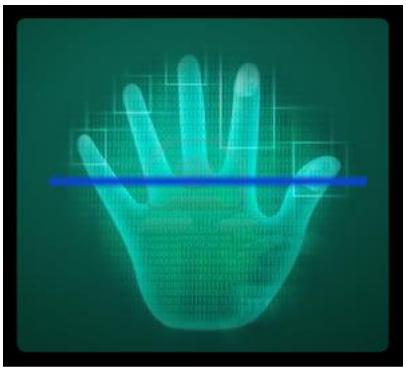

Figure 2. 10: Empreinte palmaire

2.3.2 Caractéristiques d’une empreinte palmaire

On distingue cinq types de caractéristiques qui nous permettent de reconnaitre les individus :

2.3.2.1 Caractéristiques géométriques

Selon la forme de la main, l'empreinte palmaire présente des caractéristiques géométriques telles que : la longueur, la largeur et la surface. [15] [16]

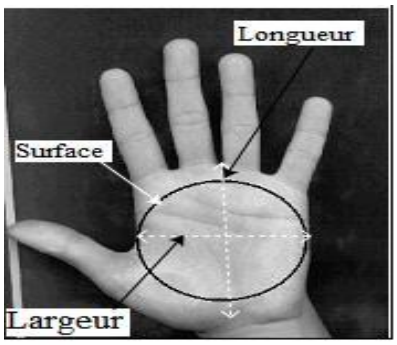

Figure 2. 11: Caractéristique géométrique de la paume de la main

2.3.2.2 Caractéristiques des lignes principales

L'empreinte palmaire est caractérisée par trois plis de flexion, dites lignes principales : la ligne de tête, la ligne de vie et celle du cœur. La Figure 2.11 montre les différents plis de la paume. [15]

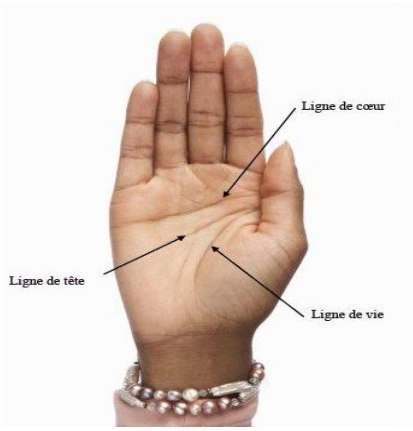

Figure 2. 12: Les différents plis de la paume de la main

Ces plis ne varient que peu à travers le temps. Ils sont faciles à extraire par des algorithmes de détection de contour. Leur positionnement et leur forme sont importants pour la reconnaissance. Mais ils sont génétiquement liés (2 jumeaux ont la même forme de plis de flexion) et restent peu distinctifs. Ainsi, seuls, ils ne peuvent pas fournir une information suffisante pour une reconnaissance efficace.

2.3.2.3 Les rides (Plis secondaires)

L'empreinte palmaire contient de nombreux autres plis qui diffèrent de ceux de flexion du fait qu'ils sont plus minces et plus irréguliers. Certains d'entre eux sont congénitaux, d'autres sont dus aux activités musculaires. Les lignes principales et les rides peuvent être observées facilement sur les images capturées à basse résolution. Comme les lignes principales seules ne fournissent pas une information distinctive suffisante, les rides jouent un rôle important dans la reconnaissance palmaire. Combinées aux lignes principales, elles fournissent une information distinctive pour la reconnaissance. [15]

Figure 2. 13: Les traits secondaires de la paume de la main

2.3.2.4 Les points de référence

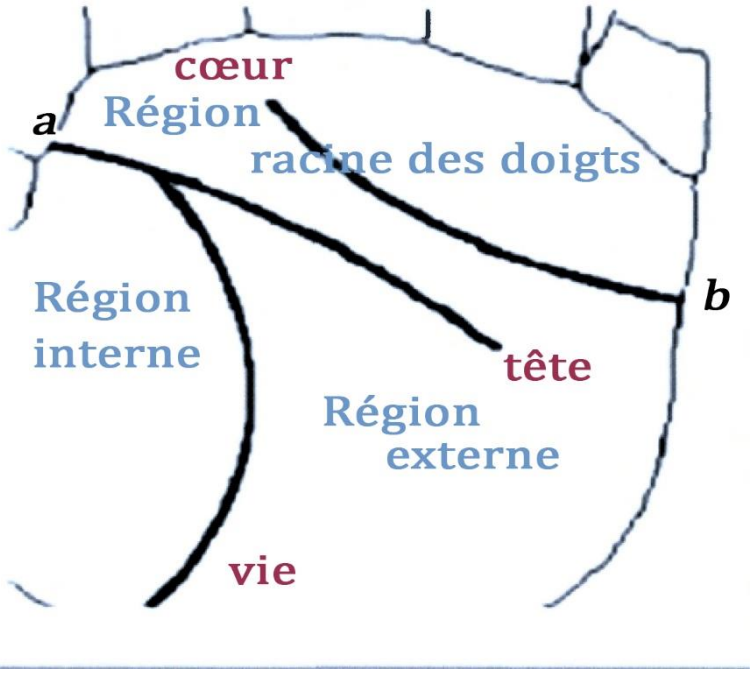

Figure 2. 14: Les points de référence de l'empreinte palmaire

Les points représentant les deux extrémités de la paume de la main sont appelés point de références. Ce sont les points a et b dans la Figure 15

La paume peut être devisée en trois régions selon les points de référence a et b ces régions sont :

- La région de la racine des doigts.
- La région interne.
- La région externe.

2.3.2.5 Les caractéristiques des minuties

Les minuties de l'empreinte palmaire sont généralement similaires aux minuties de l'empreinte digitale. Elles sont utilisées pour la reconnaissance et correspondent aux points suivants : Delta, Fin de ligne, Lac, Bifurcation [15].

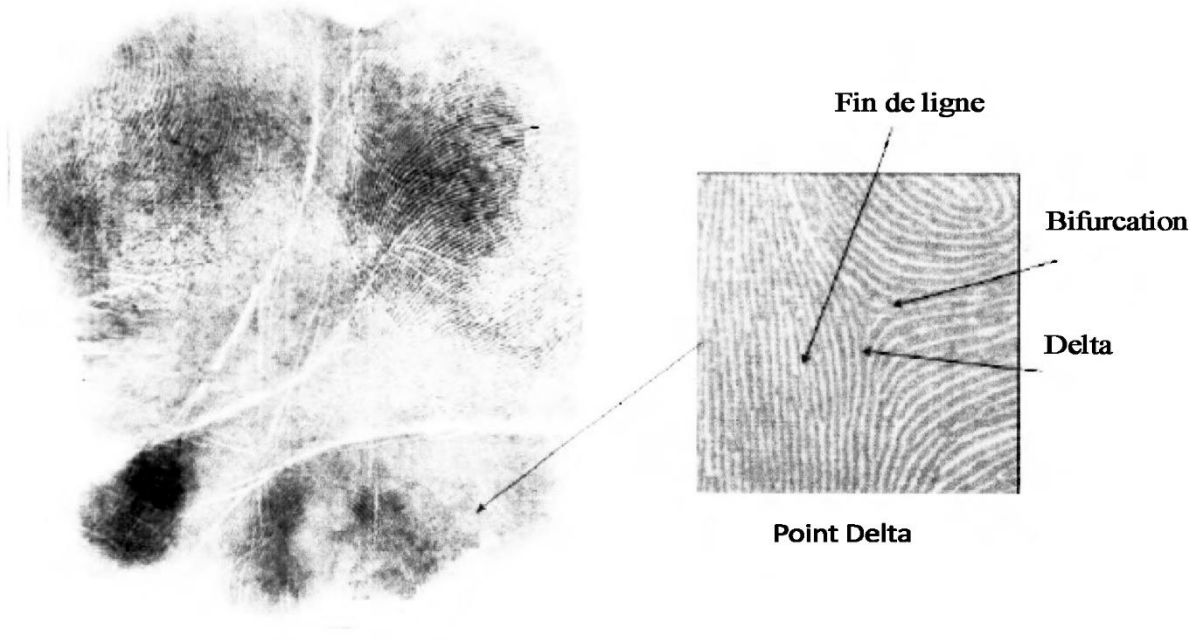

Figure 2. 15: Les minuties de la paume de la main

2.3.3 Caractéristiques d'identification par empreintes palmaires

On discrimine deux classes principales d'identification par empreinte palmaire : l'identification hors ligne et l'identification en ligne.

2.3.3.1 L'identification hors ligne

La recherche sur la reconnaissance d'empreintes palmaires hors ligne a été au centre de l'attention ces dernières années, dans laquelle tous les échantillons de palmiers sont fixés sur du papier puis transmis à un ordinateur via un scanner numérique (Figure 17). En raison de la haute résolution relative aux images d'empreintes palmaires hors ligne, certaines techniques d'empreintes digitales peuvent être utiles pour la reconnaissance d'empreintes palmaires hors ligne, où des lignes et des points de données ou des points singuliers peuvent être extraits. [17]

2.3.3.2 L’identification en ligne

Pour la reconnaissance d'empreintes palmaires en ligne, les échantillons d'images sont directement acquis via un équipement d'acquisition d'empreintes palmaires. Évidemment, la reconnaissance d'empreintes palmaires en ligne est plus adaptée aux applications en temps réel, c'est pourquoi nous nous intéressons à ce type de reconnaissance. Figure 17 Images de reconnaissance d'empreintes palmaires en ligne et hors ligne. [17]

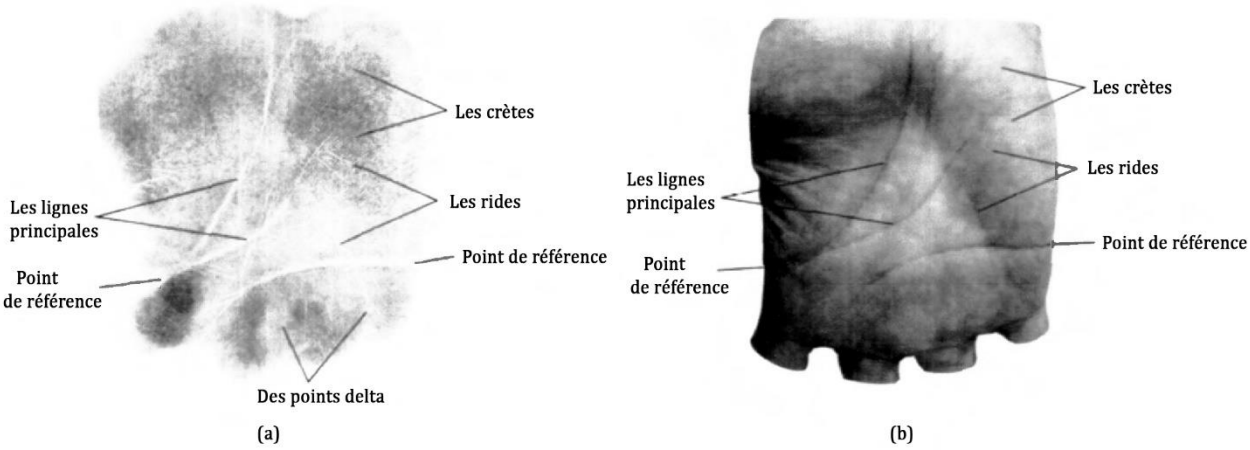

Figure 2. 16: Images d’identification par empreintes palmaires :
a) identification hors ligne **b)** identification en ligne

2.3.4 Capteur d’empreintes palmaires

Pour la reconnaissance complète en ligne d’une empreinte de la main, vous avez besoin d'un appareil spécifique qui doit acquérir plus rapidement les empreintes palmaires. La figure suivante montre un exemple d'un tel appareil :

Figure 2. 17: Capteur d'empreinte palmaire

2.3.5 Système de reconnaissance palmaire

2.3.5.1 Acquisition

Elle s'agit du premier processus des systèmes de reconnaissance des empreintes palmaires et elle s'agit de capturer l'image de la paume. Les chercheurs utilisent quatre types de capteurs différents pour recueillir les images d'empreintes palmaires : les scanners d'empreintes palmaires à base de **CCD**, les appareils photo numériques, les scanners numériques et les caméras vidéo. La figure 18 montre un scanner d'empreinte palmaire à base de **CCD** développé par l'Université polytechnique de Hong Kong. D'une manière générale, les scanners d'empreintes palmaires à **CCD** capturent des images d'empreintes palmaires de haute qualité et alignent les paumes avec précision puisque les scanners sont équipés de chevilles pour guider le placement des mains.

Les scanners numériques sont rentables pour collecter les images d'empreintes palmaires. Cependant, ils ne peuvent pas prendre en charge la vérification en temps réel en raison du temps de numérisation. Les appareils photo numériques et les caméras vidéo sont deux moyens de recueillir des images d'empreintes palmaires sans contact. La figure2.19(a) montre une image d'empreinte palmaire collectée par un scanner d'empreinte palmaire à **CCD**, et la figure 2.19(b) est une image d'empreinte palmaire collectée par un scanner numérique.

Figure 2. 18: Capteur d'empreinte palmaire

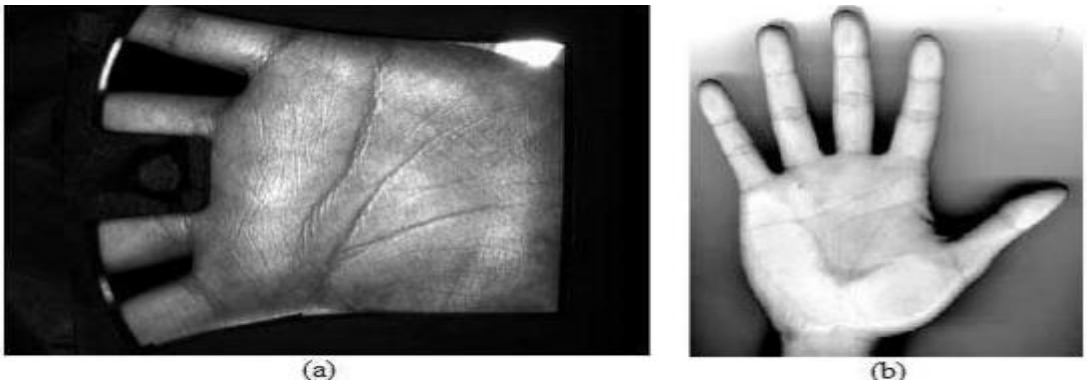

Figure 2. 19: Deux empreintes palmaires recueillies par :
(a) Un scanner d'empreintes palmaires à base de CCD **(b)** Un scanner numérique

2.3.5.2 Prétraitement

Le prétraitement est utilisé pour aligner différentes images d'empreintes palmaires et pour segmenter les parties centrales en vue de l'extraction de caractéristiques. La plupart des algorithmes de prétraitement utilisent les points clés entre les doigts pour établir un système de coordonnées.

Le prétraitement comprend généralement cinq étapes communes, (1) la binarisation des images de la paume, (2) l'extraction du contour de la paume et/ou des doigts, (3) la détection des points clés, (4) l'établissement d'un système de coordination et (5) l'extraction des parties

centrales. La figure (2.20) (a) illustre les points clés et la figure (2.20) (b) montre une image prétraitée.

Les deux premières étapes de tous les algorithmes de prétraitement sont similaires. Cependant, la troisième étape est mise en œuvre de différentes manières, notamment par tangente et par ondelettes. Toutes ces approches utilisent uniquement les informations sur les frontières des doigts.

Après avoir obtenu les systèmes de coordonnées, les parties centrales des empreintes de la main sont segmentées. La plupart des algorithmes de prétraitement segmentent des régions carrées pour l'extraction de caractéristiques. [18]

2.3.5.3 Extraction des caractéristiques

De nombreux travaux ont été réalisés pour développer des algorithmes d'extraction de caractéristiques. D. Zhang et al ont utilisé des caractéristiques de points et de lignes de référence pour un système de vérification d'empreintes palmaires. Li et al ont utilisé la transformée de Fourier pour l'extraction de caractéristiques d'empreintes palmaires. Kong et al ont proposé l'extraction de caractéristiques d'empreintes palmaires en utilisant des filtres de Gabor 2-D. Gan et al ont appliqué la transformée en ondelettes pour la reconnaissance des empreintes palmaires. Wu et al ont proposé une analyse de la texture des empreintes palmaires en utilisant la dérivée des filtres gaussiens. [18] [19]

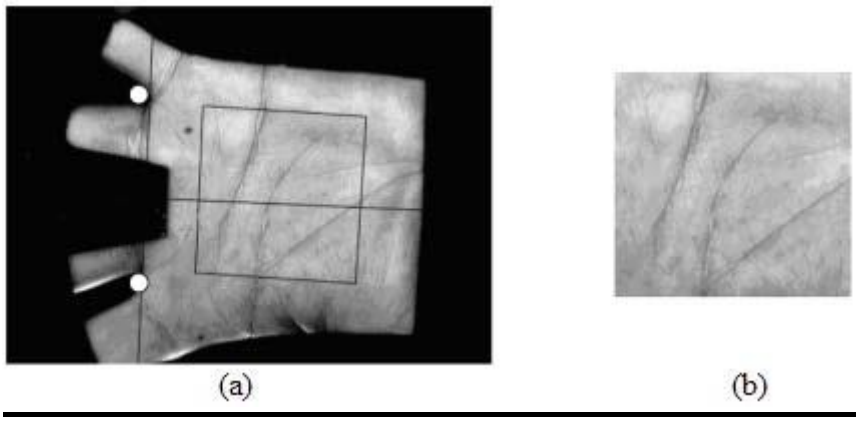

Figure 2. 20: Illustration du prétraitement
(a) Les points clés basés sur la limite du doigt
(b) Les parties centrales pour l'extraction des caractéristiques

2.3.5.4 Comparaison et classification

De nombreux travaux ont été consacrés à la comparaison des empreintes palmaires. De nombreux classificateurs existants, y compris les réseaux neuronaux, diverses mesures, dont la mesure du cosinus, la distance euclidienne pondérée, la distance euclidienne, la distance de Hamming et la distance du plus proche voisinage, ont été examinés.

Cette étape consiste à comparer les informations avec celles de la base de données, afin de déterminer l’identité de l’individu, il est autorisé à accéder. Si non le scanner vous rejette. [18] [20]

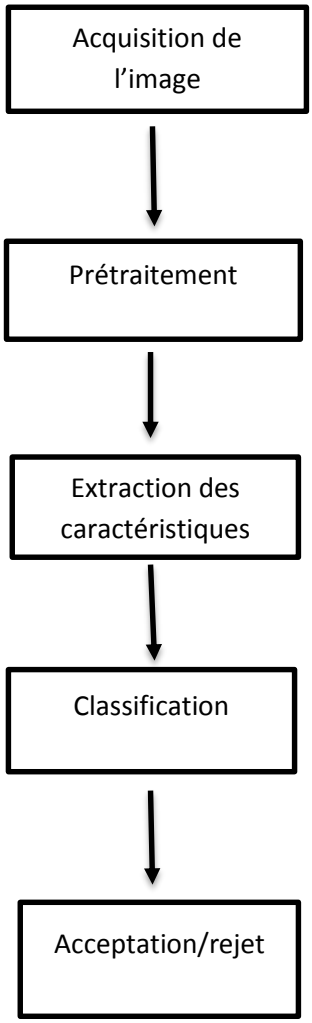

Figure 2. 21: Système de reconnaissance palmaire

2.4 Conclusion

Dans ce chapitre, on vient d'approfondir l'état de l'art de la reconnaissance faciale et des empreintes palmaires.

Dans la première partie, nous avons déterminé les techniques les plus populaires utilisées en reconnaissance du visage. Ensuite nous avons détaillé le processus de reconnaissance de

visage, son principe de fonctionnement ainsi que l’algorithme des méthodes de reconnaissance faciale. Enfin nous avons cité les différentes difficultés inhérentes à la reconnaissance de visages.

Dans la dernière partie, Nous avons défini l’empreinte palmaire, ces caractéristiques biométriques et les types de reconnaissance, et à la fin nous avons déterminé le processus de reconnaissance palmaire.

Chapitre 03

Reconnaissance de visage
par Eigenfaces

3.1 Introduction

La reconnaissance du visage a atteint un haut niveau de performances, même avec l'utilisation d'un seul exemple d'apprentissage. Dans les conditions actuelles des travaux sur la reconnaissance faciale, le système visuel humain reste encore le plus robuste face aux diverses variations pouvant altérer le processus d'identification : changement des conditions d'éclairage, variations de l'expression faciale, modifications de l'apparence du visage à travers la présence ou l'absence de lunettes, barbe, maquillage.

De nombreuses techniques ont été développées ces dernières années, nous avons cité les plus connues dans le chapitre précédant. Parmi elles, Eigenface, qui est une Technique particulièrement prise par les chercheurs de la communauté de la biométrie.

Nous commencerons d'abord par l'objectif de l'algorithme ACP. Puis nous détaillerons le principe de la méthode Eigenface. Ensuite nous présenterons son organigramme détaillé. Nous décrirons également ses avantages. Et enfin nous terminerons par une conclusion.

3.2 L'objectif de la méthode ACP

L'algorithme ACP, PCA en anglais est né des travaux de MA. Turk et AP. Pentland au MIT Media Lab, en 1991. Il est aussi connu sous le nom d'Eigenfaces car il utilise des vecteurs propres et des valeurs propres. L'objectif de cet algorithme est de capturer les changements dans une collection d'images faciales afin d'utiliser ces informations pour encoder et comparer les visages. Étant donné un ensemble d'images différentes de visages, la technologie recherche les composantes primordiales de la distribution du visage, puis utilise des vecteurs de caractéristiques pour les représenter. Chaque visage spécifique est ensuite estimé par approximation linéaire du vecteur caractéristique associé à la valeur caractéristique maximale.

3.3 Principe de la méthode eigenfaces

L'idée principale consiste à exprimer un nombre N d'images d'apprentissage selon une base de vecteurs orthogonaux particuliers, contenant des informations indépendantes d'un vecteur à l'autre.

Ces nouvelles données sont donc exprimées d'une manière plus appropriée à la reconnaissance du visage.

Nous voulons extraire l'information caractéristique d'une image de visage, pour l'encoder aussi efficacement que possible afin de la comparer à une base de données de modèles encodés de manière similaire. En termes mathématiques, cela revient à trouver les vecteurs propres de la matrice de covariance formée par les différentes images de notre base d'apprentissage.

Une image $\mathrm{I_i(m,n)}$ est traitée comme un vecteur $\Gamma_i(m \times n, 1)$ dans un espace vectoriel de grande dimension ($\mathrm{D = m \times n}$), par concaténation des colonnes.

Après avoir rassemblé nos M images dans une unique matrice, nous obtenons une matrice d'images Γ, ou chaque colonne représente une image Γ_i. [12]

$$\boldsymbol{\Gamma} = \begin{bmatrix} \mathbf{a_{1,1}} & \mathbf{b_{1,1}} & \cdots & \mathbf{z_{1,1}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a_{n,1}} & \mathbf{b_{n,1}} & \cdots & \mathbf{z_{n,1}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a_{1,m}} & \mathbf{b_{1,m}} & \cdots & \mathbf{z_{1,m}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a_{n,m}} & \mathbf{b_{n,m}} & \cdots & \mathbf{z_{n,m}} \end{bmatrix} \quad \textbf{(3.1)}$$

On calcule ensuite l'image moyenne Ψ de toutes les images collectées.

$$\boldsymbol{\Psi} = \frac{\mathbf{1}}{\boldsymbol{N}} \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{\Gamma_i} \quad \textbf{(3.2)}$$

Cette image peut être vue comme le centre de gravité du jeu d'images et qui est représenté par la figure 3.1.

Figure 3. 1 : Image moyenne

On ajuste ensuite les données par rapport à la moyenne.

L'image moyenne est alors soustraite de chaque image avec la formule suivante :

$$\mathbf{\Phi_i = \Gamma_i - \Psi,\ i = 1 \ldots N} \qquad \mathbf{(3.3)}$$

On calcule ensuite la matrice de covariance du jeu de données. Cette matrice peut être vue comme une matrice de moments d'ordre 2 :

$$\mathbf{C = \sum_{i=1}^{N} \Phi_i \Phi_i^T \quad \Phi_i^T = AA^T \qquad A = [\Phi_1 \Phi_2 \ldots \Phi_N]} \qquad \mathbf{(3.4)}$$

La prochaine étape consiste à calculer les vecteurs propres et les valeurs propres de cette matrice de covariance C de taille $(D \times D)$, c'est-à-dire de l'ordre de la résolution d'une image.

Le problème est que parfois, cela peut être difficile et très long.

En effet, si $D > N$ (si la résolution est supérieure au nombre d'images), il y aura seulement $N - 1$ vecteurs propres qui contiendront de l'information (les vecteurs propres restants auront des valeurs propres associées nulles). [21] [22]

Par exemple, pour 50 images de résolution 180x200, nous pourrions résoudre une matrice L de 50x50 au lieu d'une matrice de 36000x36000 pour ensuite prendre les combinaisons linéaires appropriées des images Φ_i. Le gain de temps de calcul serait considérable, nous passerions d'une complexité de l'ordre du nombre de pixels dans une image à celle de l'ordre du nombre d'images [12].

Les étapes du processus qui nous permettent d'avancer dans les calculs sont décrits ci-dessous :

Considérons les vecteurs propres e_i de C = AAT, associés aux valeurs propres λ_i.

On a:

$$\mathbf{Ce_i = \lambda_i e_i} \tag{3.5}$$

Les vecteurs propres v_i de L = A^TA, associés aux valeurs propres μ_i sont tels que :

$$\mathbf{Lv_i = \mu_i v_i} \tag{3.6}$$

Soit :

$$\mathbf{AA^T Av_i = A\mu_i v_i} \tag{3.7}$$

Comme C = AA^T, nous pouvons simplifier **:**

$$\mathbf{C(Av_i) = \mu_i (Av_i)} \tag{3.8}$$

De (3.5) et (3.6), nous voyons que Av_i et μ_i sont respectivement les vecteurs propres et les valeurs propres de C :

$$\begin{cases} \mathbf{e_i = Av_i} \\ \mathbf{\lambda_i = \mu_i} \end{cases} \tag{3.9}$$

Nous pouvons donc trouver les valeurs propres de cette énorme matrice C en trouvant les valeurs propres d'une matrice L beaucoup plus petite. Pour trouver les vecteurs propres de C, il suffit juste de multiplier les vecteurs propres de L par la matrice A.

Les vecteurs propres trouvés sont ensuite ordonnés selon leurs valeurs propres correspondantes, de manière décroissante. Plus une valeur propre est grande, plus la variance capturée par le vecteur propre est importante. Cela implique que la majeure partie des informations est contenue dans les premiers vecteurs propres.

3.3.1 Projection des images de visage

De façon imagée, les vecteurs propres de l'ensemble de ses six visages présentés dans la figure 3.3 s'obtiennent comme une combinaison linéaire des six visages initiaux. Puis, on obtient six images par la soustraction des valeurs propres par ces visages initiales et les prochains vecteurs propres s'obtiennent comme une combinaison linéaire de ses nouvelles images [23]

Figure 3. 2: Un ensemble de six visages

Les techniques d'interprétation d'ACP classiques peuvent être utilisées pour interpréter les vecteurs de caractéristiques d'un ensemble de visages. En particulier, il peut représenter la projection du visage sur un sous-plan bidimensionnel. Par exemple, la figure 3.4 montre Les six têtes du sous-plan formé par les vecteurs propres 2 et 3. Le deuxième vecteur de caractéristiques capture des informations liées au sexe du visage : il compare le visage masculin avec le visage féminin. Le troisième vecteur propre semble à opposer les cheveux longs aux cheveux courts.

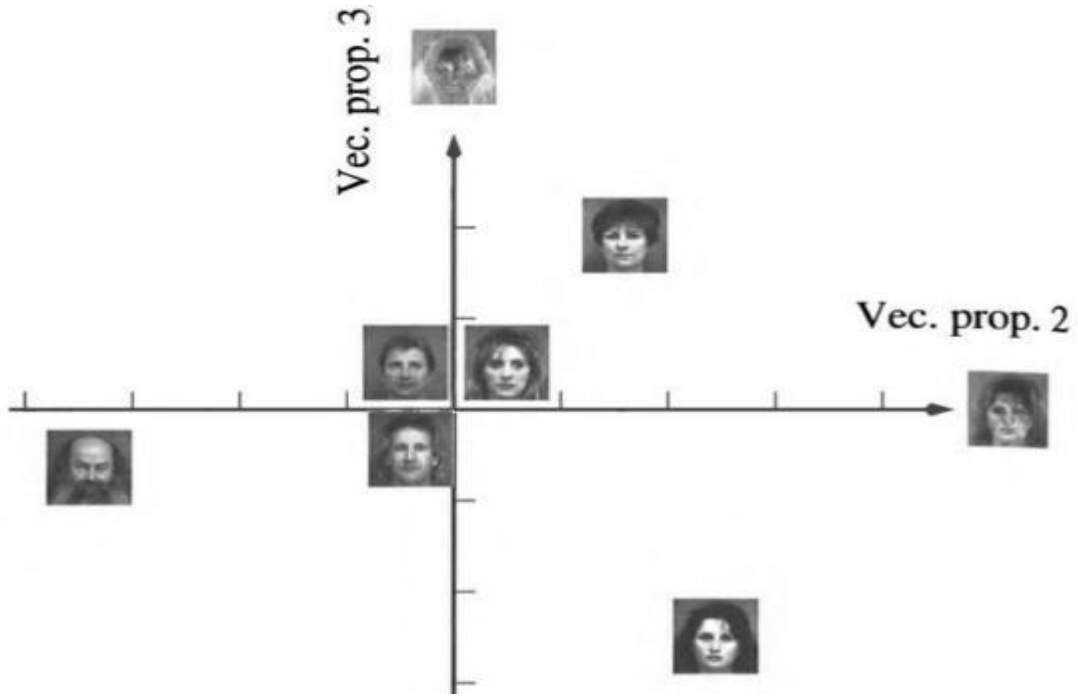

Figure 3. 3: Projection des six visages sur le sous-plan formé par les vecteurs propres 2 et 3

3.3.2 Phase d'apprentissage

La phase d'apprentissage correspondra à des personnes réelles qui seront enregistrées dans la base de données. Par conséquent, cette étape consiste à collecter un grand nombre d'images faciales pour constituer une base de données de départ. Tout d'abord, nous construisons une matrice contenant N images de la bibliothèque d'apprentissage, puis calculons l'image moyenne. Ensuite, nous réajustons les données liées à la moyenne pour pouvoir suivre de manière simple Le comportement des valeurs d'écart type, de variance et de covariance. On applique ensuite l'algorithme de reconnaissance globale à cette matrice réajustée.

Ce qu'il faut retenir, c'est que ces algorithmes fournissent en sortie ce que l'on appelle la matrice de projection G, ce qui est très utile dans la deuxième partie de la phase d'apprentissage. Cette étape consiste à projeter l'image apprise dans un espace vectoriel dont le vecteur est l'élément de notre matrice de projection G. Toutes ces projections sont finalement stockées dans une grande base de données. [24]

3.3.3 Phase de test

Lorsqu'une nouvelle image de la base de test est mise devant le système, on la soustrait par rapport à la moyenne, on la projette ensuite sur l'espace vectoriel relatif à la matrice de projection G afin de la comparer avec toutes les projections issues de la phase d'apprentissage et qui étaient stockées dans la base de données. Par le terme comparer, il faut exécuter un calcul de distance entre les projections vectorielles. Il semble logique que plus la distance entre deux projections est petite, plus ces deux projections se ressemblent. Ainsi le résultat de la reconnaissance est l'image de la base d'apprentissage qui ressemble le plus à la nouvelle image présentée au système [24].

3.3.4 Résumé de la méthode

Nous résumons les différentes étapes de l'eigenfaces comme suit :

L'apprentissage des visages propres s'effectue selon les étapes suivantes :

1- Collecte des M images faciales et construction de la matrice T de taille M, par concaténation des colonnes des images faciales. Prétraitement des images collectées.

2- Calcul du visage moyen en sommant les colonnes de la matrice T et en divisant le vecteur résultant par le nombre d'image d'entrée (M).

3- Soustraction du visage moyen de la matrice T pour obtenir la matrice A ; où chaque élément représente la variance des valeurs d'intensité de chaque pixel.

4- Calcul de la matrice.

5- Calcul des vecteurs propres de C' et les triés dans un ordre descendant selon les valeurs propres associées.

6- Calcul des vecteurs propres de la matrice de covariance C et obtention des visages propres en multipliant les vecteurs propres de C' par la matrice A.

7- Choix des K meilleur valeurs propres et les vecteurs propres associés.

8- Détermination du poids des images d'entrée en projetant chaque image dans l'espace visage.

Chaque visage est maintenant représenté par un vecteur qui est utilisé pour reconstruire les images.

9- Et enfin sauvegarde des calculs du visage moyen, des eigenfaces et du poids des images.

Les neuf étapes décrites transformeront une base de données d'images faciales en un ensemble de projections dans l'espace visage (face sace).

L'étape de reconnaissance peut être résumée comme suit :

1. Prétraitement de l'image d'entrée et soustraction du visage moyen.
2. Détermination du poids de l'image d'entrée par la projection de celle–ci dans l'espace visage en multipliant le vecteur résultant de l'étape (1) par les eigenfaces de la base de données.
3. Comparaison des résultats obtenus en utilisant des métriques telles que la distance Euclidienne. Nous allons décrire les différentes distances existantes dans la section suivante.

3.3.5 Mesure de distance

Lors de la phase de test, les visages appris, additionnés avec d'autres nouveaux visages qui sont généralement équivalents, sont reconstruits à partir des vecteurs propres déjà calculés. Un mécanisme de décision est ensuite mis en place pour décider quels visages parmi les visages reconstruits lors de la phase de test avaient été au préalable stocké en mémoire. L'algorithme le plus simple est l'algorithme du plus proche voisin. Il consiste à rechercher les visages les plus semblables aux visages tests sur l'hyperplan défini par les vecteurs propres (souvent, seuls les vecteurs propres ayant les plus grandes valeurs propres sont conservés). Ensuite, on calcule la distance euclidienne entre la projection du visage test et la projection de tous les visages appris. Si la distance entre le plus proche voisin (ou la distance moyenne entre les K plus proches voisins) et le visage test est inférieure à un seuil donné, le visage est classé comme connu, sinon il est classé comme inconnu [24].

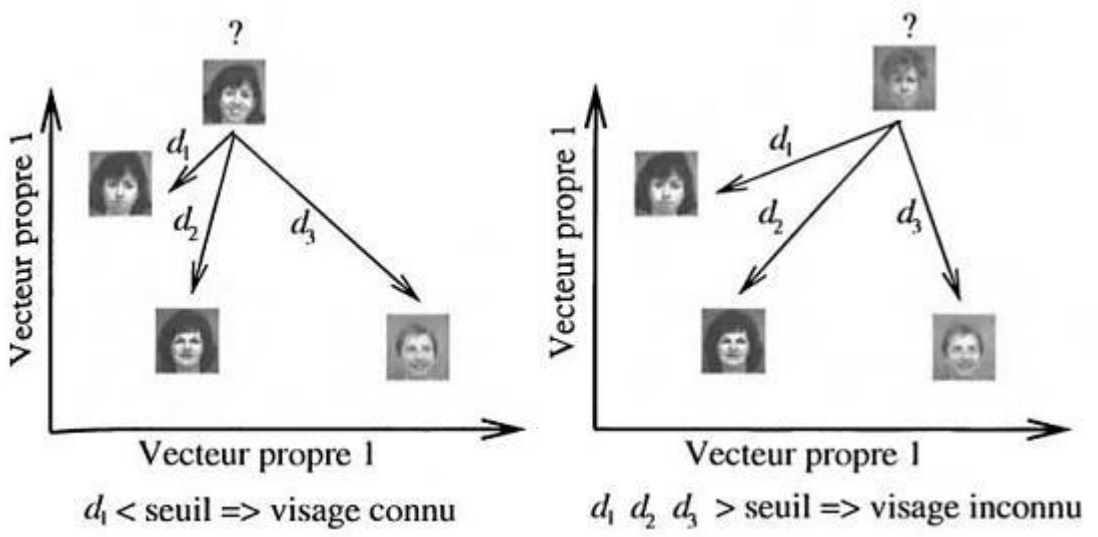

Figure 3. 4: Illustration de la simulation d'une tâche de reconnaissance à partir de l'algorithme

La mesure la plus couramment utilisée est la distance euclidienne. L'autre étant la distance de Mahalanobis. La distance de Mahalanobis offre généralement des performances supérieures. Faisons une brève digression et examinons ces deux mesures de distance simples.

3.3.5.1 Distance euclidienne

La distance euclidienne est probablement la métrique de distance la plus utilisée. Il s'agit d'un cas particulier d'une classe générale de normes et elle est donnée comme suit :

$$\|\boldsymbol{x}-\boldsymbol{y}\|_{\boldsymbol{e}}=\sqrt{|\boldsymbol{x_i}-\boldsymbol{y_i}|^{\boldsymbol{2}}} \qquad \textbf{(3.10)}$$

3.3.5.2 Distance de Mahalanobis

La distance de Mahalanobis est une meilleure mesure de distance lorsqu'il s'agit de problèmes de reconnaissance de formes. Elle prend en compte la covariance entre les variables et élimine donc les problèmes liés à l'échelle et à la corrélation qui sont inhérents à la distance euclidienne. Elle est donnée comme suit :

$$\boldsymbol{d(x,y) = \sqrt{(x-y)^T C^{-1}(x-y)}} \quad \textbf{(3.11)}$$

3.3.6 Organigramme détaillé de l'approche Eigenface

Notre organigramme est divisé en trois parties : la première partie est le prétraitement, puis la phase d'apprentissage, et enfin la phase de reconnaissance, où la distance euclidienne est réservée au calcul de la différence entre les poids de l'image à reconnaître et de l'image de la base de données. Ensuite, le programme affiche le plus proche.

3.3.6.1 Organigramme du prétraitement

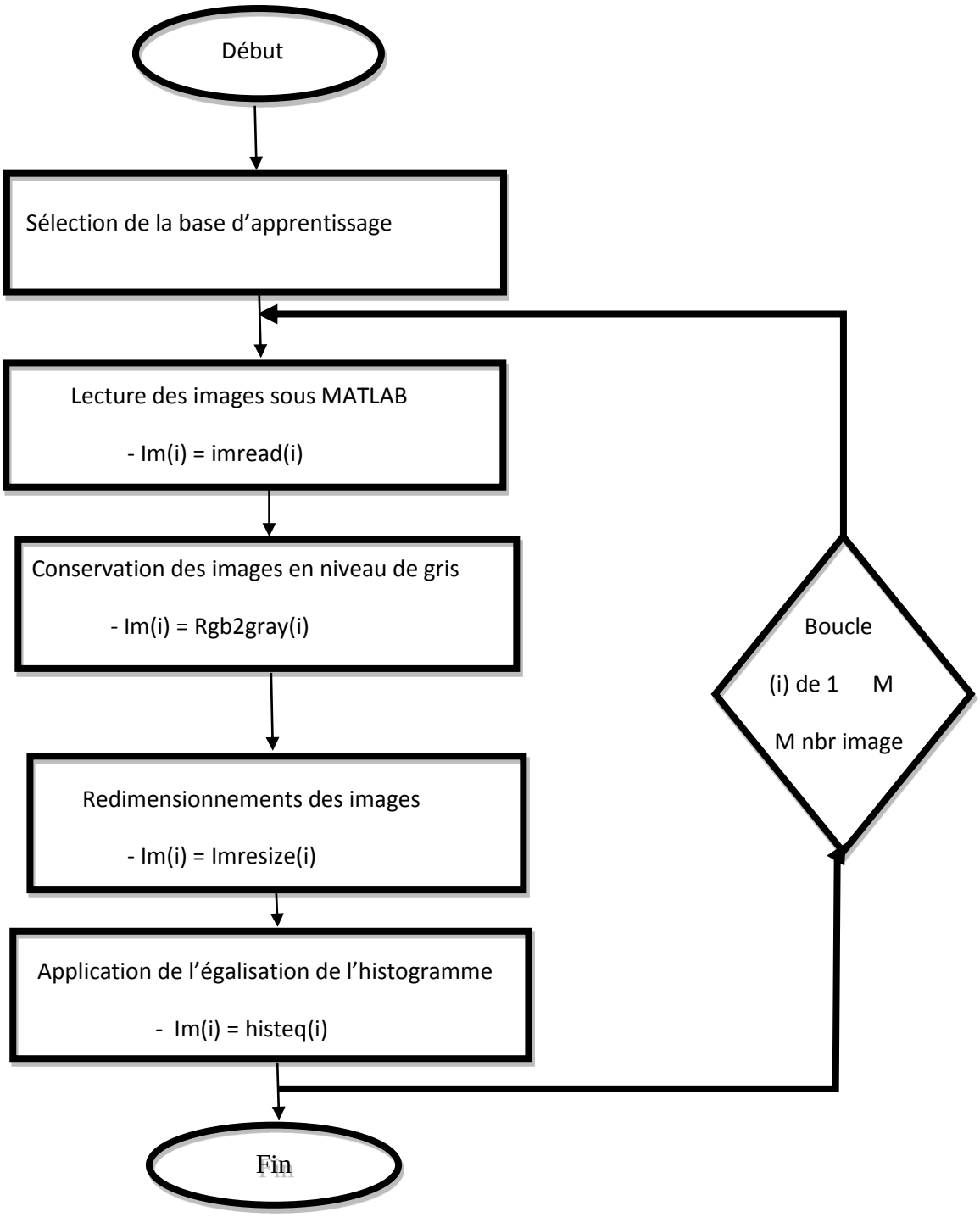

Figure 3. 5: Prétraitements

3.3.6.2 Organigramme de la phase d'apprentissage

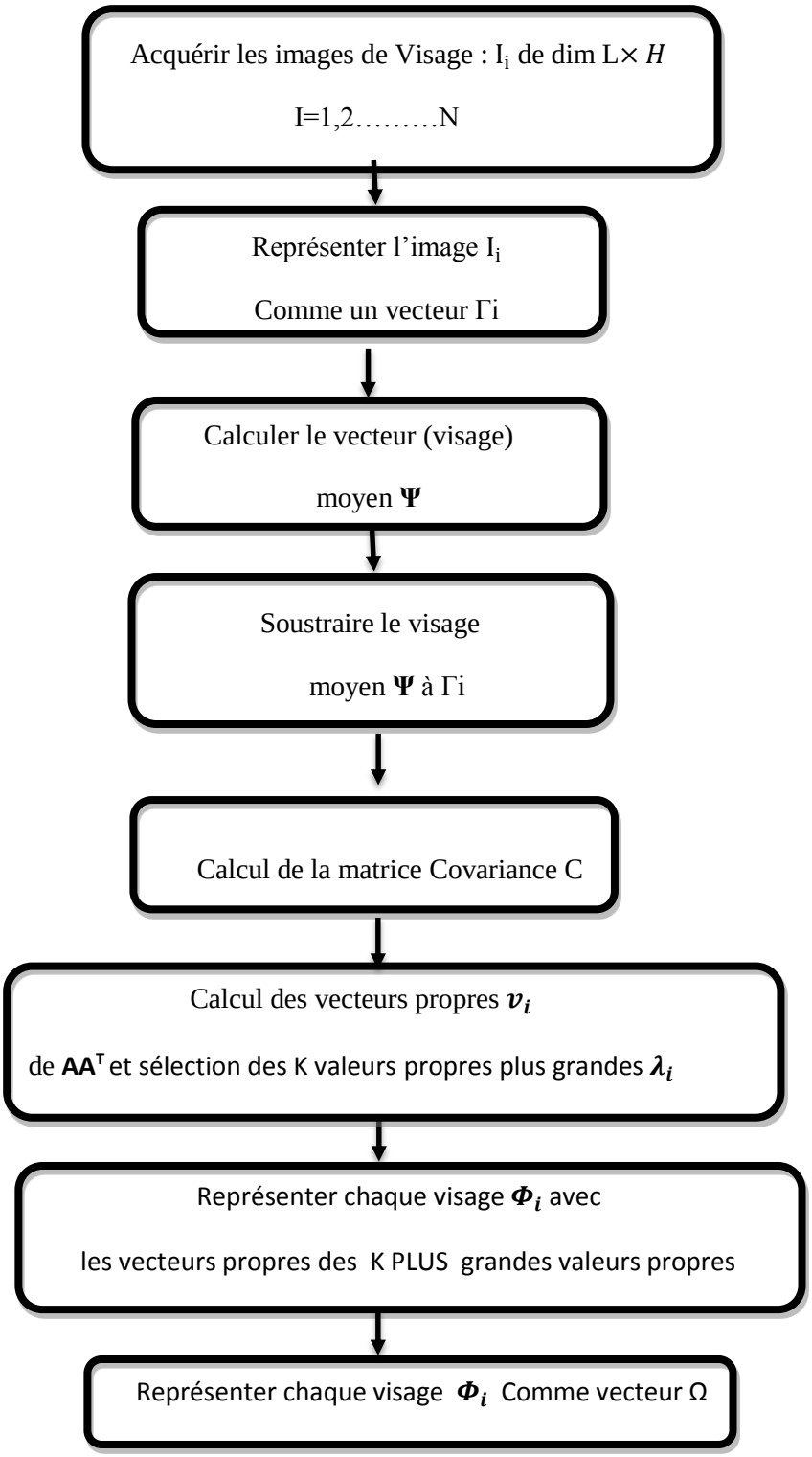

Figure 3. 6: Phase d'apprentissage

3.3.6.3 Organigramme de la phase d'identification

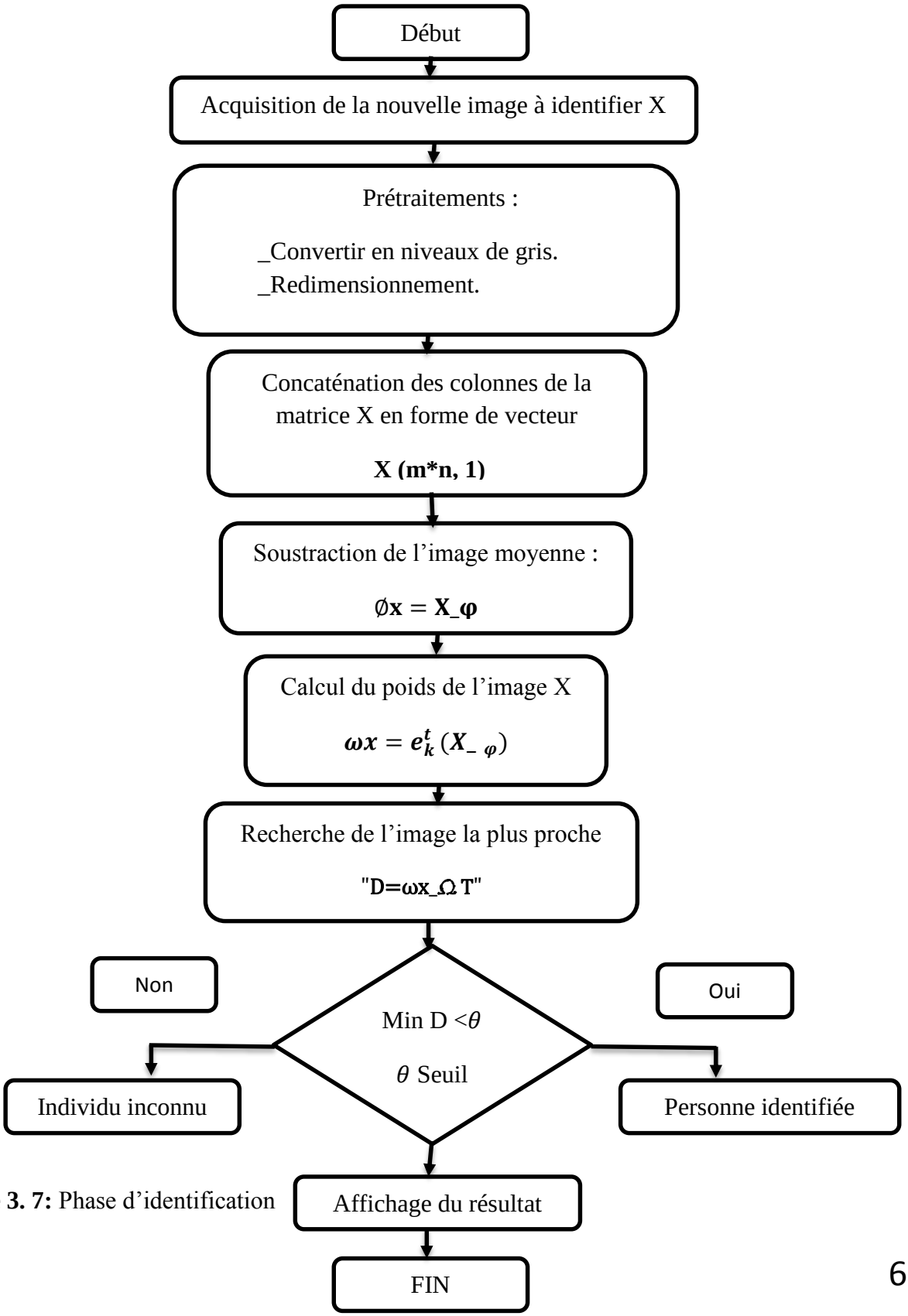

Figure 3. 7: Phase d'identification

3.4 Les avantages de la méthode Eigenface

- Les données d'intensité brutes sont utilisées directement pour l'apprentissage et la reconnaissance sans traitement significatif de bas niveau ou de niveau intermédiaire.
- Aucune connaissance de la géométrie des visages n'est requise
- La compression des données est obtenue grâce à la représentation de sous-espaces de faible dimension
- La reconnaissance est simple et efficace par rapport aux autres approche correspondante

3.5 Conclusion

Ce chapitre a été consacré en premier lieu à la présentation de la méthode de reconnaissance faciale choisie qui est « Eigenface ». Ensuite nous avons mis en évidence un organigramme détaillé de cette approche. Enfin nous avant donné un aperçu sur ses avantages.

Dans le dernier chapitre, nous utiliserons Matlab pour faire la conception de notre système de reconnaissance faciale.

Chapitre 04

Résultats expérimentaux

4.1 Introduction

Ce chapitre présente la partie la plus importante de notre projet, qui vise à apprendre à utiliser la technologie biométrique pour protéger l'information. Dans ce cadre, nous proposons un système d'identification. L'étude expérimentale de ce système est basée sur la reconnaissance faciale par la méthode ACP décrite dans le chapitre précédent. Elle est réalisée sur une base de données créée par nous-même. Afin d'évaluer l'efficacité de la méthode de recherche et les performances du système biométrique que nous avons proposé, et vu l'importance affectée à la modalité du visage ces dernières années, nous proposerons un système de reconnaissance faciale opérationnel avec des résultats expérimentaux.

4.2 Environnement du travail

Dans cette partie, nous présenterons le matériel et le logiciel utilisés dans notre travail.

4.2.1 Environnement matériel

Afin de mettre en œuvre ce projet, nous avons besoin d'un ensemble de matériel dont les caractéristiques sont les suivantes :

Un ordinateur ASUS avec les caractéristiques suivantes :

- Processeur : AMD E1-6010 APU avec AMD Radeon R2 Graphics 1.35GHz
- Mémoire installée (RAM) : 4 GO
- Type du système : système d'exploitation 64 bits.
- OS : Microsoft Windows 10

4.2.2 Environnement logiciel

Notre système a été développé sous l'environnement de Windows 10 avec le langage *MATLAB* version (R2015 b).

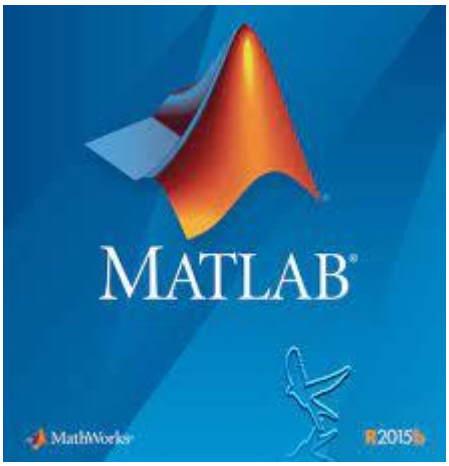

Figure 4. 1: Logo MATLAB

- **<u>Généralité sur Matlab :</u>**

Entre 1970 et 1990, de nombreux programmes informatiques interactifs sont apparus Sur le marché électronique notamment le programme MATLAB, conçu par « Cleve Moler » à la fin des années 1970. MATLAB « Matrix Laboratory » est un langage de développement informatique spécialement conçu pour les applications scientifiques, utilisé pour développer des solutions nécessitant une puissance de calcul très élevée, et permettant d'effectuer de multiples simulations basées sur des algorithmes d'analyse numérique. Comme il dispose de nombreux outils dont « Image Processing ToolBox », qui propose un ensemble d'algorithmes et d'outils de référence graphique pour traiter, analyser, visualiser et développer des algorithmes de traitement d'images [Matlab].

Autrement dit MATLAB est un système interactif et convivial de calcul numérique et de visualisation graphique destiné aux ingénieurs et scientifiques. Il possède un langage de programmation à la fois puissant et simple d'utilisation. Il permet d'exprimer les problèmes et solutions d'une façon aisée, contrairement aux autres langages de programmation.

Il s'impose dans le monde universitaire et industriel comme un outil puissant de simulation et de visualisation de problèmes numériques. Dans le monde universitaire, MATLAB est utilisé pour l'enseignement de l'algèbre linéaire, le traitement du signal, l'automatique, ainsi

que dans la recherche scientifique. Dans le domaine industriel, il est utilisé pour la résolution et la simulation de problèmes pratiques d'ingénierie et de prototypage [25].

4.3 Système de reconnaissance faciale

4.3.1 Conception

4.3.1.1 Principe de fonctionnement du système

Le problème de la reconnaissance faciale est défini tel qu'à partir de l'image du visage, la personne correspondante doit être identifiée. Pour ce faire, il est nécessaire d'obtenir une image de référence (images d'apprentissage) sous la forme d'une base de données de tous les visages connus du système. Chaque image est associée à un vecteur de propriétés qui varie d'une personne à l'autre. La reconnaissance consiste alors à comparer le vecteur caractéristique du visage à reconnaitre avec chaque vecteur de la base d'apprentissage. Autrement dit, trouver la personne dont le visage est le plus similaire à celui qu'on cherche à identifier.

La structure générale de notre système de reconnaissance de visage comporte deux phases :

- **Phase d'entrainement :** comme son nom l'indique, c'est la phase où le système apprend la personne à partir d'une ou plusieurs images, elle s'effectue en utilisant l'algorithme d'ACP. A la fin de cette étape, on aura pour chaque personne un modèle unique qui le caractérise.

- **Phase de test :** elle consiste à identifier une personne de la base de test à partir de celle qui se trouve dans la base d'entrainement.

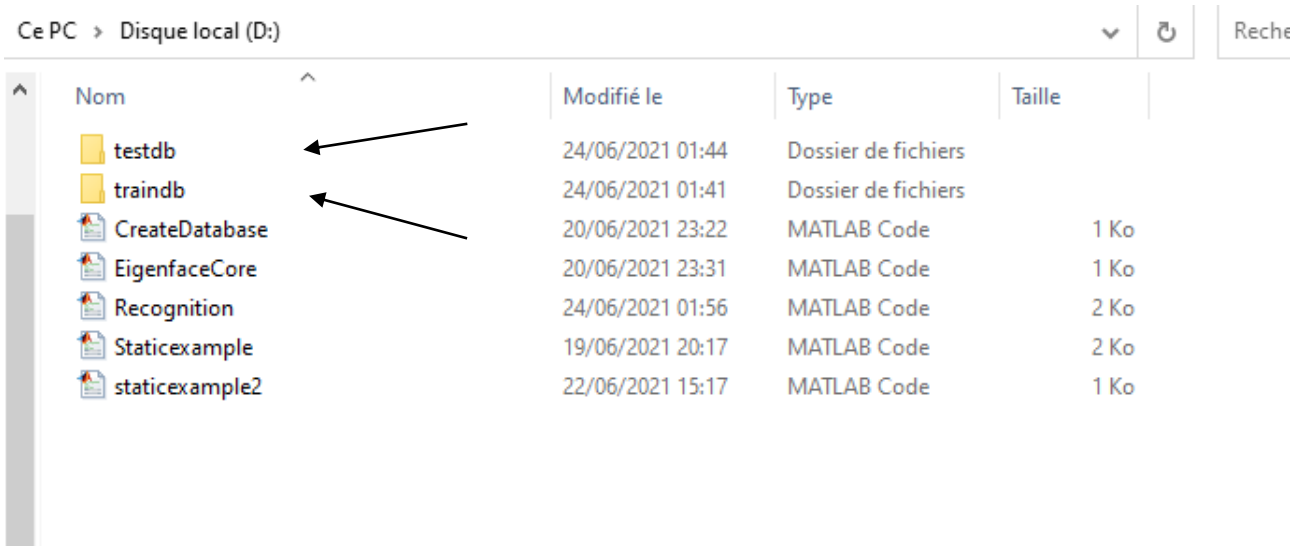

Figure 4. 2: Base de test et d'entrainement

Pour réaliser ce système on a créé notre propre base de données.

4.3.1.2 Création de la base de données

4.3.1.2.1 Prétraitement

La création de la base de données est l'étape initiale qui permet d'introduire les images d'entrainement, pour cela on a redimensionné ces images (180*200) pour qu'on puisse utiliser la méthode ACP. On a chargé l'ensemble des images dans MATLAB en utilisant la fonction « img = imread(str) ».

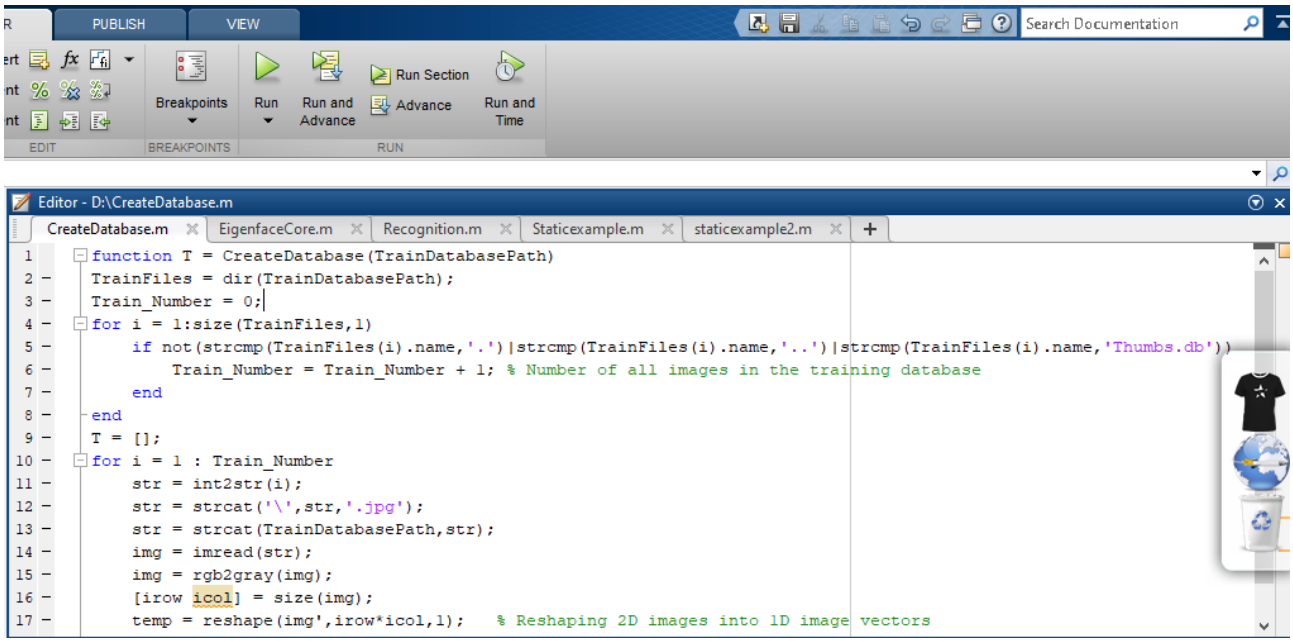

Figure 4. 3: Création de la base de données

4.3.1.2.2 Base d'entrainement (apprentissage)

La base de d'entrainement est composée de 7 images : les 6 premières images correspondent aux 3 individus avec 2 images pour chacun, avec des positions différentes par rapport à celles de la base de test. La 7 -ème image apparaitra lors du teste d'une image qui existe à la base de test et n'existe pas dans la base d'apprentissage.

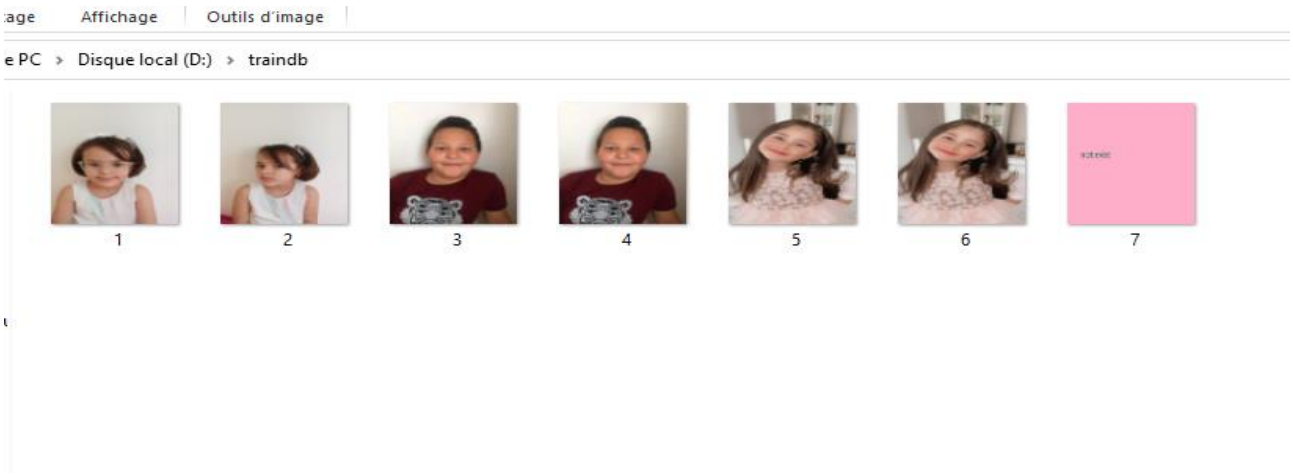

Figure 4. 4: Base d'entrainement

4.3.1.2.3 Base de test

La base de test est composée de 4 images de 4 individus différents, avec 1 image par individu d'où une image parmi eux n'existe pas dans la base d'entrainement.

Figure 4. 5: Base de test

4.3.1.2.4 Charger l'ensemble de données dans MATLAB

4.3.1.2.4.1 Base de données

Afin d'intégrer notre base de données dans Matlab on a utilisé la fonction :

```
function T = CreateDatabase(TrainDatabasePath)
```

Cette fonction remodèle toutes les images 2D de la base de données d'entraînement en vecteurs colonnes 1D. Ensuite, elle place ces vecteurs colonnes 1D dans une rangée pour construire la matrice 2D 'T'.

D'où :

TrainDatabasePath : est le Chemin de notre base de données d'entraînement.

T : Une matrice 2D, contenant tous les vecteurs d'image 1D Supposons que toutes les images P de la base de données d'entrainement ont la même taille de MxN. La longueur des vecteurs colonnes 1D est donc de MN et 'T'sera une matrice 2D MNxP.

La création de la base de données dans Matlab se fait comme suit :

- **Gestion des dossiers :** par la fonction : **TrainFiles =dir(CreateDatabase**

- **Construction d'une matrice 2D à partir de vecteurs d'image 1D :** par la fonction **: T= [ ],** selon les étapes suivantes :

➢ Appeler de la boucle ‘’For ‘‘ afin de parcourir le vecteur et effectuer à chaque pas toutes les instructions.

➢ Choisir le nom de chaque image dans les bases de données comme un numéro correspondant, par :

```
str = strcat(TrainDatabasePath,str)
```

➢ Lecture des images sous MATLAB avec la fonction :

```
img = imread(str)
```

➢ Convertir les images au niveau du gris par :

```
img = rgb2gray(img)
```

➢ Redimensionner les images 2D pour obtenir un nombre de lignes N1 et de colonnes N2 par :

```
[irow icol] = size(img)
```

➢ Remodeler les images 2D en vecteurs d'images 1D par :

```
temp = reshape(img',irow*icol,1)
```

4.3.1.2.4.2 Implémentation d’algorithme ACP

On a utilisé l'analyse en composantes principales pour déterminer les caractéristiques les plus discriminantes entre les images de visages, avec la fonction :

```
function [m, A, Eigenfaces] = EigenfaceCore(T)
```

Cette fonction obtient une matrice 2D, contenant tous les vecteurs d'image d'entraînement et renvoie 3 sorties qui sont extraites de la base de données d'entraînement.

D'où :

m : (M*Nx1) est la moyenne de la base de données d'entrainement.

Eigenfaces : (M*Nx(P-1)) est le vecteur propre de la matrice de covariance de la base de données d'entraînement.

A : (M*NxP) est la matrice de vecteurs d'image centrés.

T : est déjà définit précédemment.

L'implémentation d'algorithme ACP se fait selon les étapes suivantes :

- Calcul de l'image moyenne par :

```
m = mean(T,2);
Train_Number = size(T,2);
```

- Calcul de l'écart de chaque image par rapport à l'image moyenne :

```
A = [];
for i = 1 : Train_Number
    temp = double(T(:,i)) - m;
    A = [A temp];
end
```

- Calcul de substitut de la matrice de covariance C=A*A' qui est définit par L :

```
L = A'*A;
```

- Définir Les éléments diagonaux de D qui sont les valeurs propres de L=A'*A et de C=A*A', avec :

```
[V D] = eig(L)
```

- Triage et élimination des valeurs propres :

Toutes les valeurs propres de la matrice L sont triées et celles qui sont inférieures à un seuil spécifié, sont éliminées.

```
L_eig_vec = [];
for i = 1 : size(V,2)
    if( D(i,i)>1 )
        L_eig_vec = [L_eig_vec V(:,i)];
    end
end
```

- Calcul des vecteurs propres de la matrice de covariance 'C' par :

Les vecteurs propres de la matrice de covariance C (ou les "faces propres") peuvent être récupérés à partir des vecteurs propres de L.

```
Eigenfaces = A * L_eig_vec;
```

4.3.1.2.4.3 Etape de reconnaissance

En utilisant la fonction :

```
function OutputName = Recognition(TestImage, m, A, Eigenfaces,TrainDatabasePath)
```

Cette fonction compare deux visages en projetant les images dans le face space et en mesurant la distance euclidienne entre eux.

Avec : **TestImage :** est le chemin de l'image de test d'entrée

OutputName : est le Nom de l'image reconnue dans la base de données de formation

L'étape de reconnaissance se fait comme suite :

- **Projection de vecteurs d'image centrés dans l'espace des visages :**

Toutes les images centrées sont projetées dans l'espace des visages en les multipliant dans la base des faces propres.

Le vecteur projeté de chaque visage sera son vecteur caractéristique correspondant.

```
ProjectedImages = [];
TrainFiles = dir(TrainDatabasePath);
Train_Number = 0;
for i = 1:size(TrainFiles,1)
    if not(strcmp(TrainFiles(i).name,'.')|strcmp(TrainFiles(i).name,'..')|strcmp(TrainFiles(i).name,'Thumbs.db'))
        Train_Number = Train_Number + 1;
for i = 1 : Train_Number
    temp = Eigenfaces'*A(:,i);
    ProjectedImages = [ProjectedImages temp];
end
```

- **Extraction des caractéristiques PCA de l'image de test par :**

```
InputImage = imread(TestImage);
temp = InputImage(:,:,1);
[irow icol] = size(temp);
InImage = reshape(temp',irow*icol,1);
Difference = double(InImage)-m;
ProjectedTestImage = Eigenfaces'*Difference;
```

D'où : « **`ProjectedTestImage = Eigenfaces'*Difference`** » est le Vecteur de caractéristiques de l'image de test

- **Calcul des distances euclidiennes :**

Les distances euclidiennes entre l'image test projetée et la projection de toutes les images d'entraînement centrées sont calculées par :

```
Euc_dist = [];
for i = 1 : Train_Number
    q = ProjectedImages(:,i);
    temp = ( norm( ProjectedTestImage - q ) )^2;
    Euc_dist = [Euc_dist temp];
end
```

[MW1]

L'image test est supposée avoir une distance minimale avec l'image correspondante dans la base de données d'entraînement.

```
disp(Euc_dist)
[Euc_dist_min , Recognized_index] = min(Euc_dist);
disp(Euc_dist_min)
```

Après nous avons comparé la distance minimale de l'image test avec les images d'entrainement par un seuil d=1.582e^{+16}, si la distance minimale entre l'image test et une ou plusieurs images d'entrainement est inférieure par rapport au seuil, notre système va connaitre l'image par la distance euclidienne parmi les distances calculées.

Sinon, le système va classer l'image test comme une image inconnue.

```
if Euc_dist_min < 1.582e+16
    OutputName = strcat(int2str(Recognized_index),'.jpg');
else
    OutputName = strcat(int2str(Train_Number),'.jpg');
```

4.3.2 Réalisation

4.3.2.1 1er cas

Pour tester le bon fonctionnement de notre système de reconnaissance, on a utilisé la fonction staticexample2.m qui montre l'utilisation des fonctions présentée précédemment.

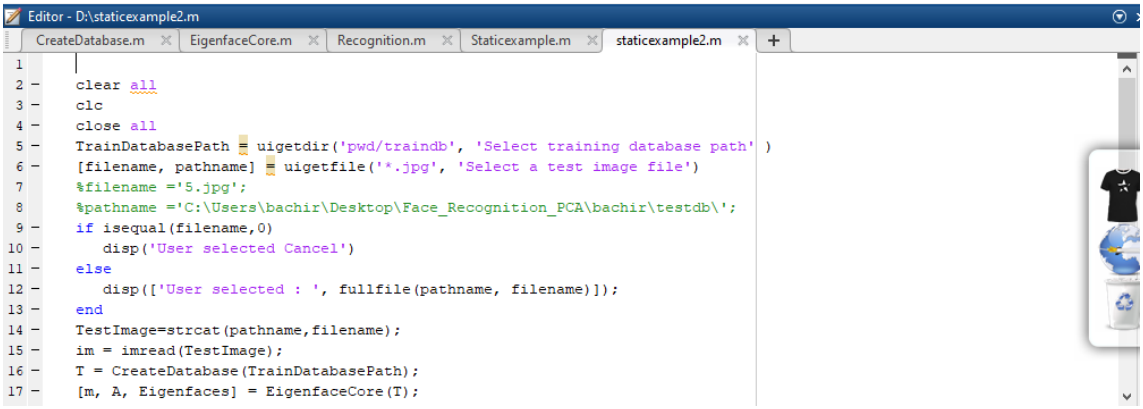

Figure 4. 6: La fonction « staticexample2 » de test

Après l'exécution de cette fonction, une fenêtre apparait pour sélectionner le chemin de la base d'entrainement.

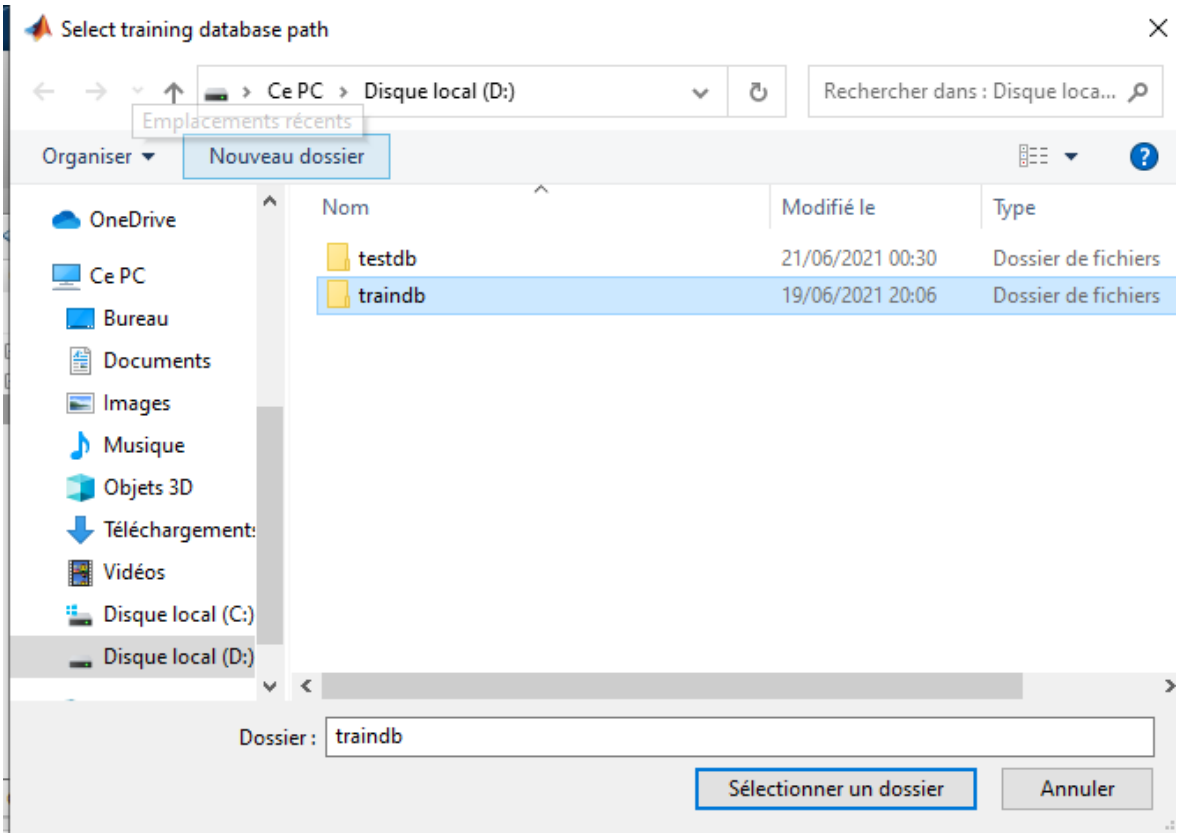

Figure 4. 7: Chemin de base d'entrainement

Après la sélection du dossier de la base d'entrainement, une autre fenêtre apparait pour sélectionner le dossier du test.

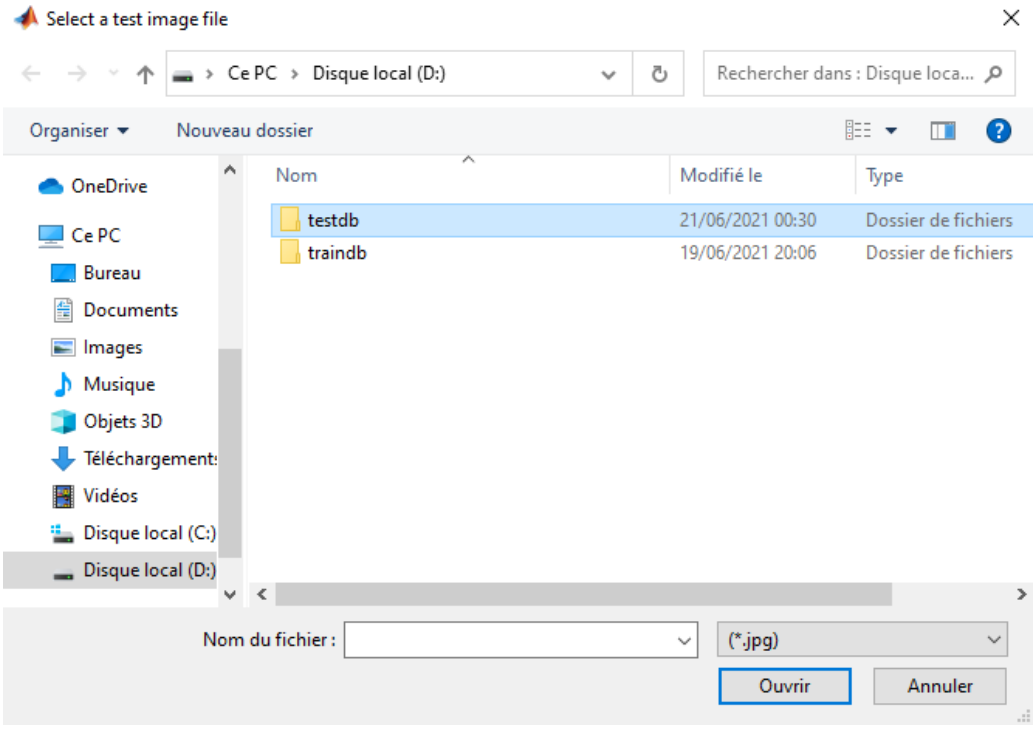

Figure 4. 8: Chemin de la base de test

Après avoir cliqué sur le bouton ‘ouvrir’, on peut accéder au contenu du fichier pour choisir une image à tester.

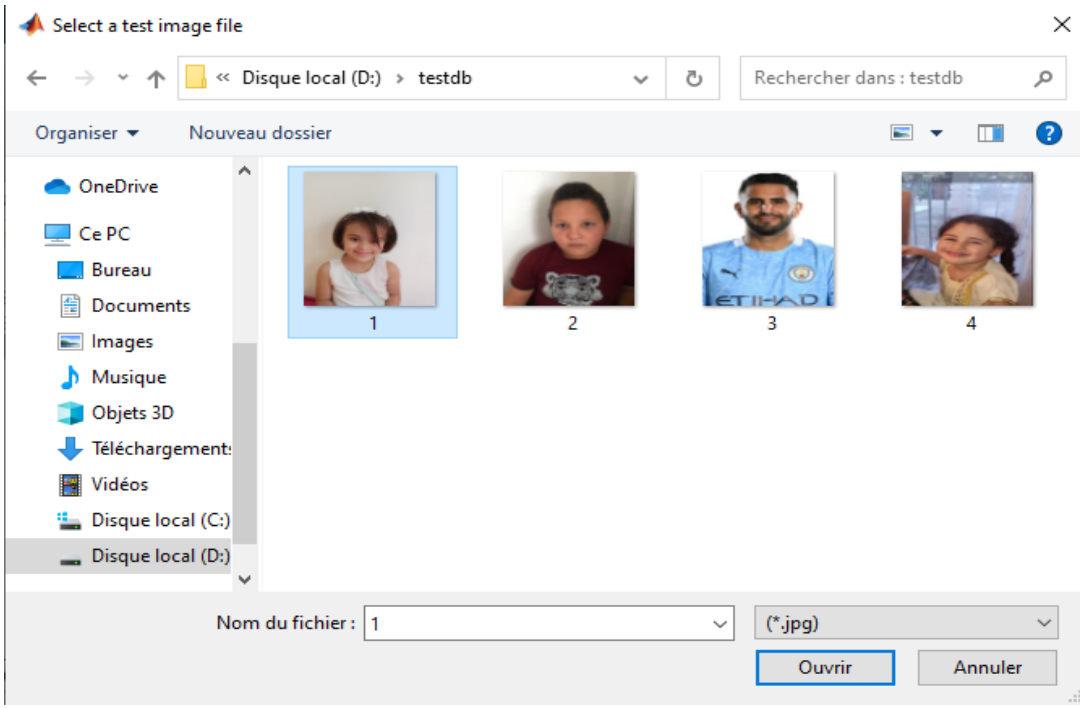

Figure 4. 9: Contenu du fichier test

Après avoir choisi l'image, le programme va effectuer les opérations nécessaires pour connaitre la personne, et après l'exécution on remarque l'apparition d'une phrase dans la fenêtre de commande disant « you are in the database ». Voici les résultats expérimentaux avec la même pose et avec variation de pose.

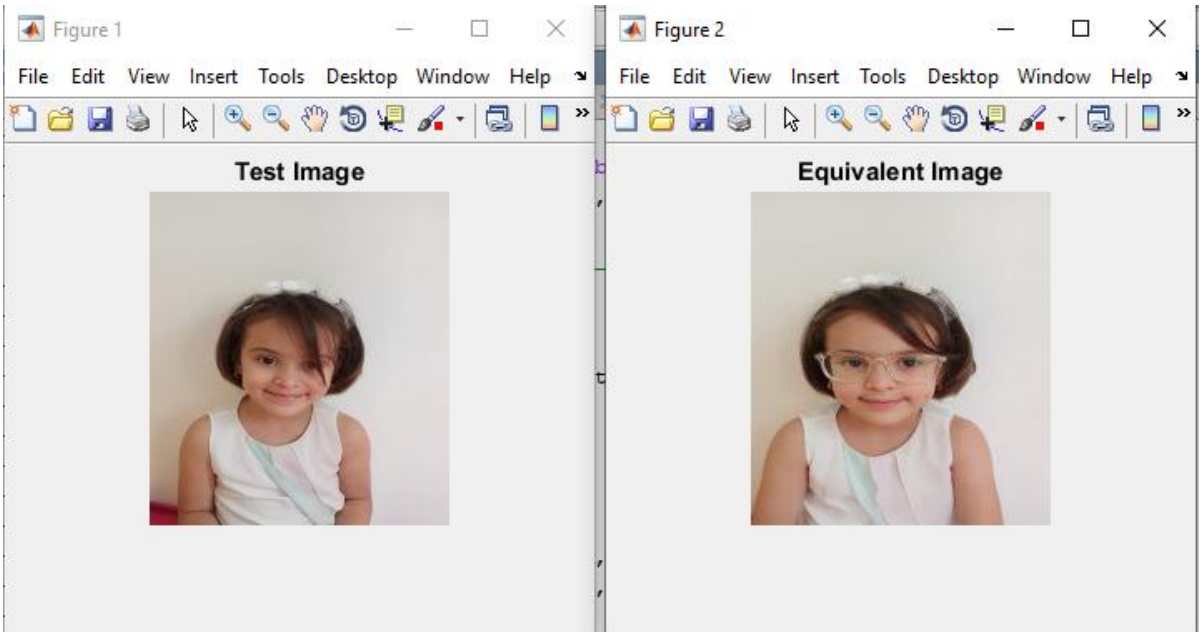

Figure 4. 10: Résultats obtenus avec la même pose

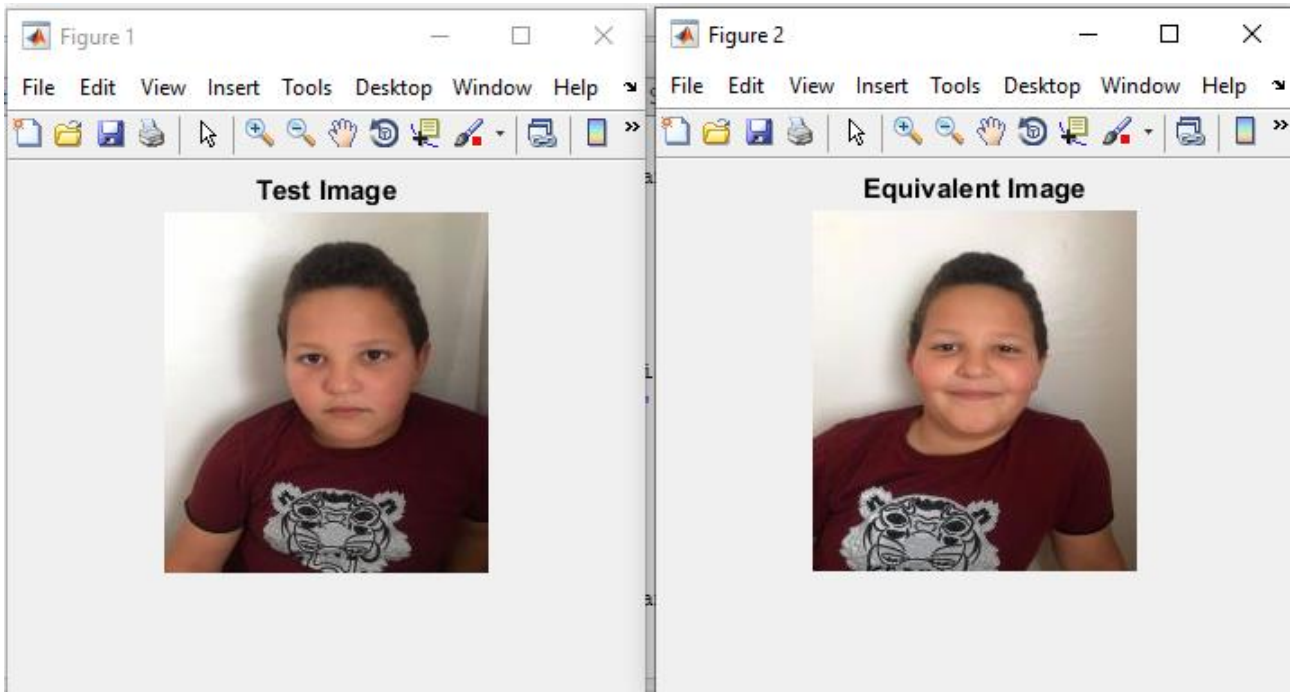

Figure 4. 11: Résultats obtenus avec variation de pose

Le programme a calculé les distances des images. Après avoir obtenu plusieurs distances inférieures au seuil donné, le programme a choisi l'image avec la plus petite distance euclidienne.

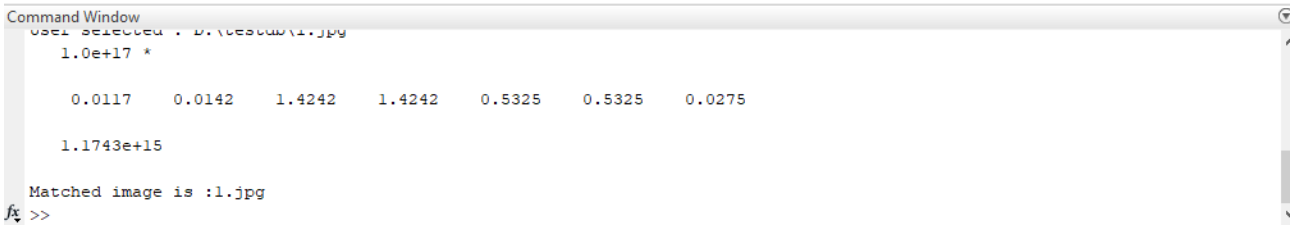

Figure 4. 12: Distances euclidiennes obtenues

- **Comparaison des distances avec le seuil (d= $1.582e^{+16}$) :**

Images	**Image.1**	**Image.2**	**Image.3**	**Image.4**	**Image.5**	**Image.6**	**Image.7**
Distances	**$1.17e^{+15}$**	**$1.42e^{+15}$**	**$1.42e^{+17}$**	**$1.42e^{+17}$**	**$5.32e^{+16}$**	**$5.32e^{+16}$**	**$2.75e^{+15}$**

Tableau 4. 1: Comparaison des distances euclidiennes des images pour le 1er cas

La distance **$1.17e^{+15}$** correspond à la première image dans la base d'apprentissage. Le schéma en bas montre les étapes que notre programme a suivi pour connaitre la bonne personne

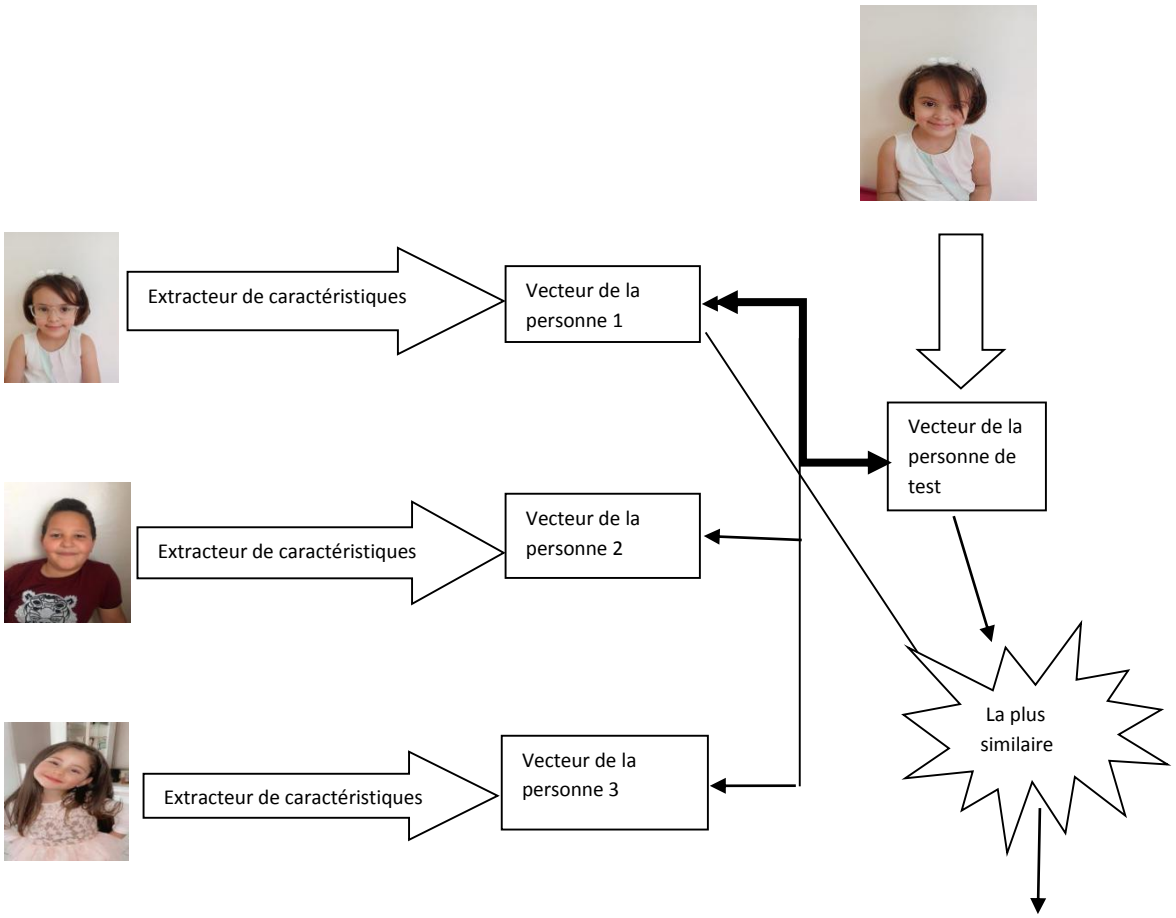

Figure 4. 13: Schéma synoptique de reconnaissance de visage avec la méthode ACP

4.3.2.2 2ème cas

Dans le deuxième cas, nous allons tester notre programme sur une image qui n'existe pas dans la base d'entrainement. On va suivre les mêmes étapes citées précédemment et les résultats de cette exécution vont être présentés par la suite.

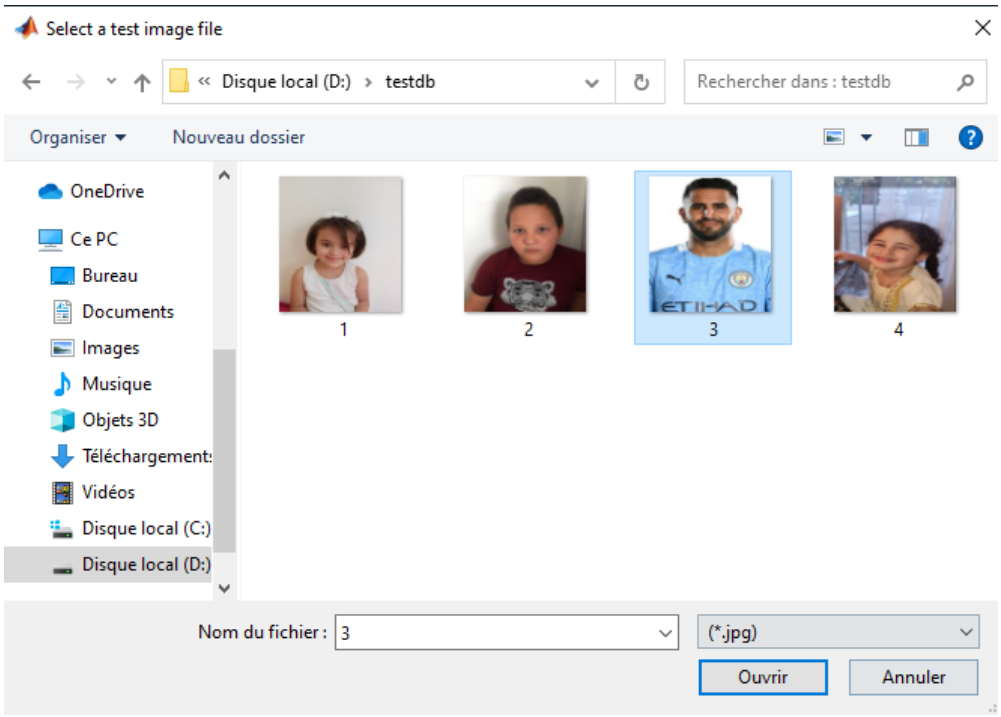

Figure 4. 14: Base de test

Nous avons choisi la troisième photo qui n'est pas connue par notre système. Ce dernier a calculé les distances euclidiennes qui sont affichées dans la fenêtre de commande en bas :

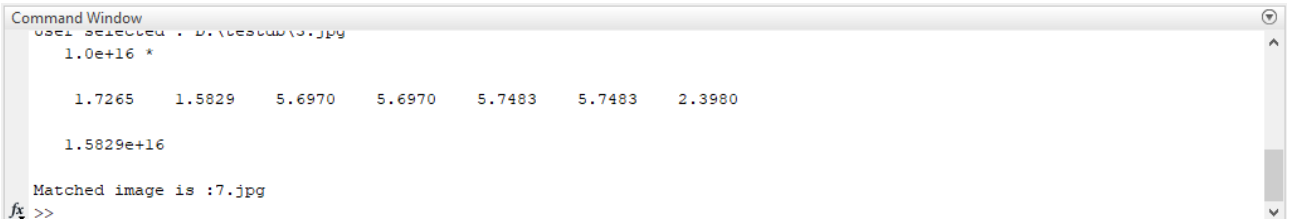

Figure 4. 15: Distances euclidiennes calculées

Le tableau ci-dessous montre l'approche des distances euclidiennes des images avec la distance donnée auparavant.

Images	Image.1	Image.2	Image.3	Image.4	Image.5	Image.6	Image.7
Distances	$1.7265e^{+16}$	$1.5829e^{+16}$	$5.670e^{+16}$	$5.6970e^{+16}$	$5.7483e^{+16}$	$5.7483e^{+16}$	$2.3980e^{+16}$

Tableau 4. 2: Comparaison des distances euclidiennes des images pour le 2ème cas

Comme la figure 4.15 et le tableau 4.2 montrent, toutes les distances calculées sont supérieures au seuil donné (**d= 1.582e^{+16}),** donc le programme va afficher la septième image de la base d'apprentissage, et une phrase s'affichera dans la fenêtre de commande disant « sorry you are not in the data base », ce qui nous montre que l'image de test n'existe pas dans la base d'apprentissage.

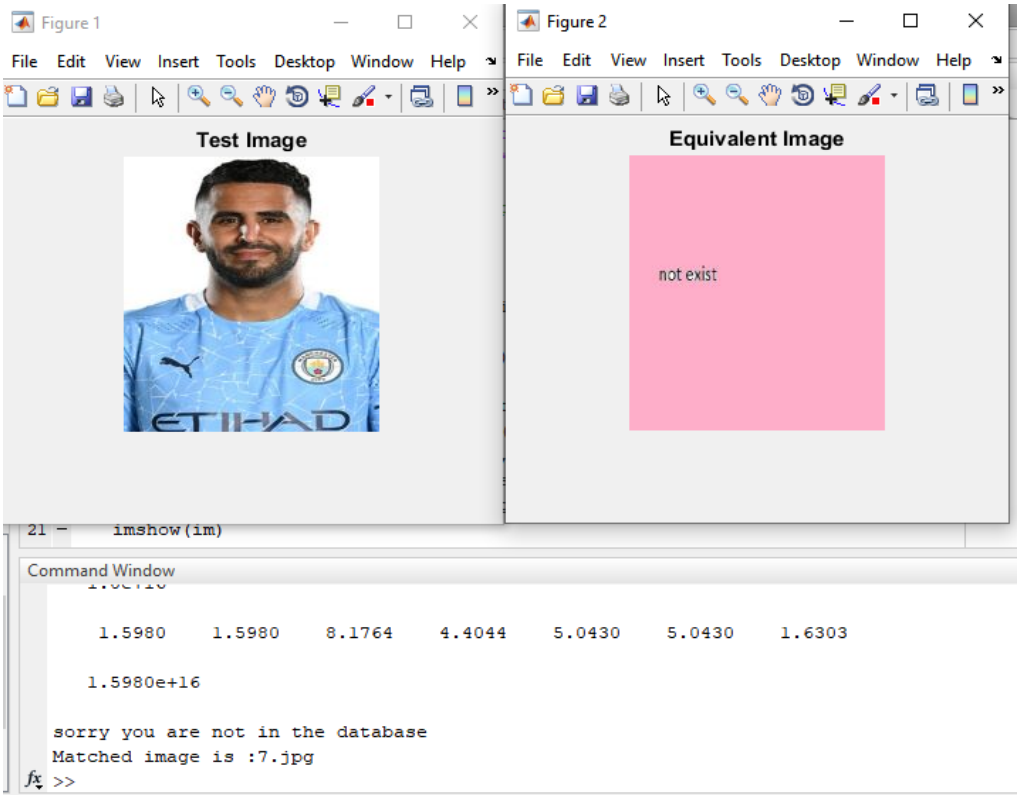

Figure 4. 16: Résultat obtenu

4.4 Conclusion

Dans ce chapitre, nous utilisons l'analyse en composantes principales pour implémenter un système de reconnaissance faciale. Le système reconnaît avec succès les visages humains et fonctionne mieux dans différentes conditions d'orientation du visage. L'algorithme a été testé sur notre propre base de données et implémenté à l'aide de MATLAB. Ces recherches nous ont permis de mieux comprendre le logiciel MATLAB, notamment dans le domaine du calcul matriciel, vectoriel et des distances euclidiennes. Des tests sur des images avec

différentes poses montrent que cette méthode classe bien les visages. Nous avons pu tester la robustesse du programme pour 4 personnes, et on peut dire qu'il est très fiable et acceptable.

Conclusion générale

L'identification biométrique est l'utilisation de caractéristiques physiques, comportementales ou biologique pour identifier des personnes. Le visage est considéré comme la modalité la plus utilisée pour la reconnaissance biométrique due à son unicité. Les systèmes de reconnaissance automatique des visages sont souvent développés dans les applications de télésurveillance et l'accès à des endroits sécurisés. Ce travail s'inscrit dans le domaine de la reconnaissance automatique des visages, qui consiste à vérifier l'identité d'une personne à partir de son image. La biométrie reste toujours un domaine de recherche car la finalité recherchée et espérée n'est pas encore satisfaisante. Chaque système a soit un temps de traitement trop lent, soit la précision n'est pas assez satisfaisante. Mais au moins certains systèmes biométriques sont plus approuvables que d'autres, selon l'application. Elle est de plus en plus appliquée dans la réalité grâce à ses avantages, c'est un domaine qui est passionnant et complexe à la fois.

Dans ce projet, nous nous intéressons au problème de la reconnaissance faciale. Notre travail comprend le développement d'un algorithme puissant conçu pour reconnaître les individus par ses traits de visage en utilisant la méthode « Eigenface » basée sur l'analyse en composantes principales (**ACP**). L'ACP est une méthode mathématique qui peut être utilisée pour simplifier un ensemble de données et réduire sa taille. Il est utilisé pour représenter efficacement des images de visage et peut reconstruire grossièrement des images de visage à partir d'un petit ensemble de poids et d'images de visage standard.

Nous avons avisé dans le premier chapitre que la variation de pose et d'éclairage présentent des défis lors de l'identification ce qui motivent les chercheurs. La présentation du technique ACP dans le troisième chapitre nous montre que cette technique est l'un des algorithmes mathématiques utilisés pour simplifier l'ensemble de données tout en réduisant sa taille. Cette dernière a été utilisée sur une base de données que nous avons créée, qui contient une gamme d'images différentes de quatre personnes dans des positions dissemblables.

Grace aux résultats obtenus au dernier chapitre, nous concluons que la technique ACP est une méthode très efficace pour identifier les personnes à travers les traits du visage. Nous avons constaté que le taux de reconnaissance de notre système est assez élevé. Les résultats découverts nous permettent de prédire dans le futur un algorithme qui correspond à l'algorithme ACP en termes de qualité, mais il est plus rapide et utilisable en pratique.

En guise de perspectives, une étude étendue peut être envisager pour la réalisation d'un système de reconnaissance avec des performances assez hautes, l'autre étude consiste à appliquer ce système à une autre base de données avec plus de personnes et avec un fort changement d'éclairage et de positions.

Bibliographie

[1] G.Roethenbaugh, «"In Introduction to biometrics and General History",» chez *Biometric Explained*, 1998.

[2] B. Ibtissam, «Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus.,» In Oran, 2015.

[3] J. H. R. M. Nalini K.Ratha, «Enhacing security and privacy in biometrics-based authentication systems,» *IBM systems journal,* vol. 40, p. 3, 2001.

[4] T. B. P. K. e. K. P. M. FAISAL, «Reconnaissance de la paume de la main. Ecole nationale Supérieure d‟ Informatique (ESI),» Oued-Smar, Alger, 2010.

[5] S. E. e. S. A. ZITOUNI, «"Authentification et identification biométrique des personnes par les empreintes palmaires.",» 2016.

[6] Y. Y. I. e. a. BOUSSAFEUR, «La biométrie multimodale basée sur la fusion de la reconnaissance de visage et l'empreinte palmaire.,» 2017.

[7] w. J. ". H. J. G. a. A. John D, «Biometrics: A look at facial recognition.,» 2003.

[8] T. R. S. K. K. e. T. P. H. BORAH, «Retina recognition system using adaptive neuro fuzzy inference system,» 2015.

[9] A. MURHULA, « Conception et mise en place d'une plateforme de sécurisation par synthese et reconnaissance biométrique de documents de traffic.,» 2015.

[10] G. e. D. L. HAYET, «Dévelopement d'un system biométrique pour la reconnaissance de visage, basé sur l'opérateur binair local (LBP) et ses variantes,» 2018.

[11] H. e. Z. N. KHIAT, «La reconnaissance faciale en utilisant l'analyse en composantes principales.,» 2017.

[12] R. V. Eric, «RECONNAISSANCE FACIALE PAR METHODE ACP HYBRIDE,» 2016.

[13] H. OUAMANE, « Identification de reconnaissance faciale avec des expressions,» 2012.

[14] A. M. T. S. &. K. A. Kumar, «Anatomy of Hand. Dans: Encyclopedia of Biometrics. s.l.:Springer,» 2009.

[15] Z. B. A. e. a. BENHEMIMED, «Reconnaissance de l'empreinte palmaire pour des applications civiles et criminalistiques.,» 2018.

[16] D. D. ZHANG, «Palmprint authentication. Springer Science & Business Media,» 2004.

[17] B. M. Boukhari Wassila, «Identification Biométrique des Individus par leurs Empreintes Palmaires « Palmprints » : Classification par la Méthode des Séparateurs à Vaste Marge (SVM)».

[18] V. H. M. L. T. G. Mouad M.H.Ali, « Palmprint Recognition Process and Techniques,» *International Journal of Applied Engineering Research ISSN 0973-4562,* vol. 13, n° %110, 2018.

[19] W. K. J. Y. a. M. W. Zhang, «online palmprint identification,» *IEEE transactions on pattern analysis and machine intelligence,* vol. 25, n° %19, 2003.

[20] W. L. a. D. Z. J. You, «hierarchical palmprint identification via multiple feature extraction,» *PERGAMON pattern recognition,* 2002.

[21] S. BOUDJELLAL, «Détection et identification de personne par méthode biométrique,» 2012.

[22] B. e. F. S. ABDESSETTAR, «Extraction des caractéristiques pour l'analyse biométrique d'un visage.,» ouargla, 2014.

[23] H. e. V. ABDI, «Dominique. Mathématiques pour les sciences cognitives,» 2006.

[24] N. H. B. Abdelouahid, «Reconnaissance de visage par réseau de neurones,» Laboratoire de recherche Informatique et Télécommunications, UNIVERSITÉ MOHAMMED V, 2014-2015.

[25] MARTAJ, Nadia et MOKHTARI, Mohand. Stateflow. In : *MATLAB R2009, SIMULINK et STATEFLOW pour Ingénieurs, Chercheurs et Etudiants*. Springer, Berlin, Heidelberg, 2010. p. 513-586.