REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
Université YAHIA FARES de MEDEA

Mémoire de Fin d'Études

Pour l'obtention du Diplôme
De Master en Génie Électrique et Informatique

Option : Systèmes Intelligents et Communicants

THEME

RECONAISSANCE BIOMETRIQUE DU VISAGE PAR L'ANALYSE EN COMPOSANTES PRINCIPALES

Réalisé par :

MORAKECHI RAZIKA

Encadré par :

Dr. Mohamed SOLTANE

Année universitaire :2011/2012

Remerciements

Remerciements

Au terme de ce travail, nous tenons à remercier en premier lieu ➢Dieu➢ qui nous a donné la force pour achever ce travail.

Je remercie vivement notre promoteur Dr. Soltane Mohamed, pour son suivi, son aide et son soutien documentaire et moral et pour ses conseils précieux et tous les Enseignants qui ont contribués à ma formation durant mon cycle universitaire.

Je remercie ma famille et en particulier ma mère et mon père qui m'a donné l'éducation sans laquelle je n'en serais pas là aujourd'hui.

Sans oublier de remercier toute personne qui, d'une manière ou d'une autre, m'a aidé a l'élaboration de ce travail.

Dédicace

Dédicace

Je dédie Ce travail
A' Mes très chers parents, mon père qui fait beaucoup Pour nous
Ma mère qu'elle a beaucoup sacrifie pour moi et qu'elle n'a jamais cessée de m'encourager.

A mon cher mari et mon enfant Islam
A mes sœurs Amina, Marwa, Kawthar
Et en particulier A' ma très chère sœur Khadidja
ET à mon cher frère amine
ET toute ma famille.
A tous mes amis proches.

Résumé :

Ce travaille consiste à appliquer la biométrie du visage pour la reconnaissance des personnes, en utilisant une méthode globale qui s'appelle l'analyse en composantes principales PCA, implémentée par le logiciel Matlab.

On a travaillé sur la base de données ORL qui contient 40 personnes, chaque personne à 10 visages différents, l'apprentissage est appliqué sur 2 visages pour chaque personne (80 visages) et les autres visage (320 visages) pour le test.

Mots clés : biométrique, PCA, visage, base de donnée ORL, ROC ;

ملخص :

هذا العمل ينطوي عل تطبيق القياسات الحيوية للتعرف على وجوه الأشخاص باستخدام نهج شامل يسمى تحليل المكونات الرئيسية (PCA). يستخدم في البرمجة لغةMATLAB.

عملنا كان على قاعدة البيانات ORL التي تحتوي على 40 فرد، لكل فرد 10 صور لوضعيات مختلفة، يتم تطبيق التعلم على صورتين لكل شخص (80 صورة) والصور الأخرى (320 صورة) للاختبار.

Abstract :

This work is to apply biometrics for face recognition people use a holistic approach called principal components analysis (PCA) is used in our application programming language Matlab.

We worked on the ORL database which contains 40 individuals, each at 10 different faces, learning is applied on two faces for each person (80 faces) and other faces (320 faces) for the test.

Word keys : biometric; PCA;face; data base ORL; ROC

Table des matières

Remerciements i

Dédicace ii

Résumé iii

Table des matières iv

Table des figures vi

Introduction générale 1

Chapitre 1:les systèmes biométriques

1.1. Introduction 3

1. 2. les systemes biométriques 5

1.3. types de biométrie 8

1.4 systeme à technologie multiples 8

1.5 description des principales techniques biométriques 9

1.6. Quelque Avantages et Inconvénients 12

1.7. Mesure des performances d'un système biométrique 13

1.8. Application des systèmes biométriques 15

1.9. Conclusion 17

Chapitre 2:La reconnaissance du visage

2.1. Introduction 18

2.2. La place de la reconnaissance de visage parmi les autre techniques biométriques 18

2.3. Les étapes de reconnaissence de visage 19

2.4. Mode de reconnaissence 24

2.5. Les méthodes de reconnaissence de visage 25

2.6. Aventages et inconvénientes 29

2.7. Utilisations actuelles de reconnaissence de visage 31

2.8. Concluion 31

Chapitre 3 : Analyse en composentes principales

3.1. Introduction 32

3.2. Analyse en composent principale 32

3.3. Comment procédes pour accélérer les calculs 36

3.4. Quelques exemple réels d'application.....40

3.5. Conclusion.....42

Chapitre 4: Implémentation et résultats

4.1. Introduction 43

4.2. qu'est_ce_qui Matlab ? 43

4.3. Pour quoi utiliser Matlab.....43

4.4. Base de donnee 43

4.5. Phase d'enrolement 45

4.6. Phase d'identification.....48

4.7. Test d'identification 50

4.8. Phase de verification 54

4.9. Test de vérification.....55

4.10.Performance de système 58

4.11.Conclusion.....62

Conclusion générale.....63

Bibliographie.....65

Table des figures

1.1.Differentes modalités biométrique…….....4

1.2. Architecture generale des systemes biométriques.....5

1.3.Enrolement d'une personne dans un système biométrique.....6

1.4. Authentification d'une personne dans un système biométrique 6

1.5. Identification d'une personne dans un système biométrique.....7

1.6.Ilustration duFAR et FRR 14

1.7.Courbe ROC 15

2.1.Les étapes de reconnaissence de visage 19

2.2.Détection du visage.....20

2.3.Schéma d'identification.....22

2.4 .Schéma de vérification 29

2.5.Une classification des algorithmes principeaux.....33

3.1.phase d'apprentissage d'un système de reconnaisence du visage par l'ACP 33

3.2 .phase dereconnaissence d'un système de reconnaisence de visage par l'ACP.....33

3.3 .Passage d'un visage vers un vecteur 34

3.4.Image moyenne et les 15visages propres 37

3.5.Image resultat 39

4.1 .Exemples d'images des deux personnes.....44

4.2 .la base de données ORL 45

4.3 .Normalisation des figures de la base ORL 46

4.4 .Affichage la liste des personnes de la base ORL 47

4.5 .l'image moyenne et les images propres.....48

4.6 .la procedure d'identification.....49

4.7 .l'image de test et l'image construite par le systeme.....50

4.8 .Personne identifie.....51

4.9 .Resultat d'identification 51

4.10. l'image test et l'image construit par le systeme 52

4.11 . Personne non identie 53

4.12 .Résultat d'identification rejetée 53

4.13.La procedure devérification.....54

4.14 .Comparaison entre le visage d'entrée et le visage de la base de donnée 55

4.15 .Résultat authentique du système de vérification 56

4.16 .Comparaison entre le visage d'entrée et le visage de la base de donnée 57

4.17 . Résultat du système de vérification.....57

4.18 .Le courbe ROC/seuil=0.29 59

4.19 .Le courbe ROC/seuil=0.08 60

4.20 . Le courbe ROC/seuil=0.03 61

Bibliographies

[1] S. GUERFI ABABSA: Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D: PhD Thesis de l'Université Evry Val d'Essonne 2008

[2] N.MORIZET: Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris. PhD d'Ecole Nationale Supérieure des Télécommunications Spécialité : Signal et Images, 18 Mars 2009.

[3]M. Chassé, Analyste en informatique: La biométrie au Québec : Les enjeux. Document d'analyse Juillet 2002.

[4] B. Dorizzi, Techniques et Usages Biométriques, GET/INT Evry,2004.

[5] S. Chikkerur, ONLINE FINGERPRINT VERIFICATION SYSTEM, Master of Science,June 2005.

[6]S. craipeau,Gerarddubey,Xavier cuchet,la biométrie,projetincitatif GET 2003.

[7] A.CHAARI, Nouvelle approche d'identification dans les bases de données Biométriques basée sur une classification non supervisée, PhD Thesis2009.

[8]O. PAPINI,Biométrie, Université de la méditerranée2003.

[9]http\biometrie_online.Net

[10] J.Colineau, S. Delaître, Johan d'Hose, SantaRossi GdRISIS ,Reconnaissance du visage 2D-3D THALES Research & Technology 2005.

*[11]*http://fr.wikipedia.org/w/index.php?title=D%C3%A9tection_de_visage&oldid69908711.

[12] F.MESSAOUDI and Mohamed BENYETTOU, Fusion de Biométries Visage et Démarche, Laboratoire de Modélisation et Optimisation des Systèmes Industriels (LAMOSI).

[13] M.Benkiniouar, Mohamed Benmohamed, Méthodes d'identification et de reconnaissance de visages en temps réel basées surAdaBoost2003.

[14] A.Mignon Frédéric Jurie, Reconnaissance de visages : une méthode originale combinant analyse discriminante logistique et distance sur graphe, GREYC – CNRS / ENSICAEN / Université de Caen.

[15] A.Mellakh, Reconnaissance des visages en conditions dégradées, Thesis de l'université d'Evry-Val d'Essonne, 2009.

[16]W. Hizem. Capteur Intelligent pour la Reconnaissance de Visage., Thèse TELECOMMUNICATIONS 2009.

[17] S.Craipeau,G.dubey,X.guchet,La Biométrie,Raport final,fivrier2004.

[18] http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html.

[19] Club de sécurité des systèmes d'information français, Techniques de contrôle d'accès par biométrie,juin2003.

[20] R.Youmaran, M.Bouchard,Introduction à Matlab, ELG 3520 "Analyse de signaux et de systèmes"2003.

Résumé :

Ce travaille consiste à appliquer la biométrie de visage pour la reconnaissance des personnes, utilisent une méthode globale qui s'appelle l'analyse en composants principales (implémenté par le langage de programmation Matlab.

On a travaillé sur la base de données ORL qui contient 40 personnes, chaque personne à 10 visages différents, l'apprentissage est appliqué sur 2 visages pour chaque personne (80 visages)et les autres visage(320 visages)pour le test.

ملخص :

هذا العمل ينطوي عل تطبيق القياسات الحيوية للتعرف على وجوه الأشخاص باستخدام نهج شامل يسمى تحليل المكونات الرئيسية (PCA). يستخدم في البرمجة لغةMATLAB.

عملنا كان على قاعدة البيانات ORL التي تحتوي على 40 فرد، لكل فرد 10 وجوه مختلفة، يتم تطبيق التعلم على وجهين لكل شخص (80 وجه) والوجوه أخرى (320 وجه) للاختبار.

Abstract :

This work is to apply biometrics for face recognition people use a holistic approach called principal components analysis (PCA) is used in our application programming language Matlab.

We worked on the ORL database which contains 40 individuals, each at 10 different faces, learning is applied on two faces for each person (80 faces) and other faces (320 faces) for the test.

Introduction Générale

De nos jours on parle de plus en plus de l'insécurité dans divers secteurs ainsi que des moyens informatiques à mettre en œuvre pour contrer cette tendance : le contrôle d'accès aux ordinateurs, l'e-commerce, les opérations bancaires basés sur l'identification du demandeur, etc. Il existe traditionnellement deux manières d'identifier un individu. La première méthode est basée sur une connaissance à priori "knowledge-based" de la personne telle que, par exemple, la connaissance de son code PIN qui permet d'activer un téléphone portable. La seconde méthode est basée sur la possession d'un objet "token-based". Il peut s'agir d'une pièce d'identité, d'une clef, d'un badge, etc. Ces deux modes d'identification peuvent être utilisés de manière complémentaire afin d'obtenir une sécurité accrue comme dans le cas de la carte bleue. Cependant, elles ont chacune leurs faiblesses. Dans le premier cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. De plus une personne sur quatre seulement fait l'effort d'appliquer les consignes de sécurité avant de retirer de l'argent (regarder derrière soi, cacher le clavier avec sa main lors de la saisie du code secret, etc.). Dans le second cas, le badge (ou la pièce d'identité ou la clef) peut être perdu ou volé. Les caractéristiques biométriques sont une solution alternative aux deux modes d'identification précédents. L'avantage de ces caractéristiques biométriques est d'être universelles, c'est-à-dire présentes chez toutes les personnes à identifier. D'autre part, elles sont mesurables et uniques : deux personnes ne peuvent posséder exactement la même caractéristique. Elle sont aussi permanentes ce qui signifie qu'elles ne varient pas ou peu au cours du temps. L'intérêt des applications utilisant la biométrie se résume en deux classes : faciliter le mode de vie, éviter la fraude.

La reconnaissance faciale fait partie des techniques biométriques. On remarque que dans la vie quotidienne chacun de nous identifie tout au long des journées différentes visages. Ainsi lorsque nous rencontrons une personne, notre cerveau va chercher dans notre mémoire et vérifier si cette personne est répertoriée ou non. La difficulté de la reconnaissance de visage par ordinateur varie énormément suivant que les conditions d'acquisition. Dans un environnement contrôlé, des paramètres tels que l'arrière plan, la direction et l'intensité des sources lumineuses, l'angle de la prise de vue, la distance de la caméra au sujet sont des

paramètres maîtrisés par le système. Dans un environnement non contrôlé, une série de prétraitements sont souvent nécessaires avant de faire la reconnaissance à proprement parler. Il faut tout d'abord détecter la présence ou l'absence de visage dans l'image. Le visage doit ensuite être segmenté. Enfin, si nous travaillons sur un flux vidéo, le système doit suivre le visage d'une image à la suivante [1].

Ce travaille est organisée de la manière suivant :

Dans le chapitre 1 nous présentons une description générale des déférents systèmes biométrique et comment mesuré les performances d'un système biométrique.

Dans le chapitre 2 nous détaillons la reconnaissance par visage, les étapes et les méthodes de reconnaissance.

Dans le chapitre 3 nous étudions l'approche globales de la reconnaissance de visage et en particularité l'algorithme de l'analyse de composants principales.

Dans le chapitre 4 nous présentons une application de reconnaissance de visage utilisons la méthode d'analyse des composants principales, faire des tests de vérification et d'identification et voire des expériences montre l'influence du paramètre seuil sur le résultat de reconnaissance.

Les Systèmes Biométriques

1.1. Introduction :

La biométrie consiste à identifier une personne à partir d'une ou de plusieurs caractéristiques physiologiques (empreintes digitales, visage, iris, contour de la main, etc.), Ou comportementales (signature, démarche, etc.). Etymologiquement, la biométrie humaine est synonyme d'anthropologie physique. Une autre définition de la biométrie est donnée par Roethenbaugh : « 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 ».

Pourquoi la Biométrie : Besoins accrus en termes de sécurité, Les systèmes de vérification standards : cartes à codes, badges magnétiques présentent des inconvénients : perte, vol, falsification. L'usage de la biométrie reste encore très limité: problème d'acceptabilité, de performances, d'usages, de législation [2].
Un système de contrôle biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à un individu [3].

Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométriques informatisés. Il existe plusieurs caractéristiques physiques uniques pour un individu, ce qui explique la diversité des systèmes appliquant la biométrie, selon que l'on prend en compte [1][4] :

- L'empreinte digitale
- La géométrie de la main
- L'iris
- La rétine
- Le visage
- La dynamique de frappe au clavier
- La reconnaissance vocale
- La dynamique des signatures
- L'ADN ….

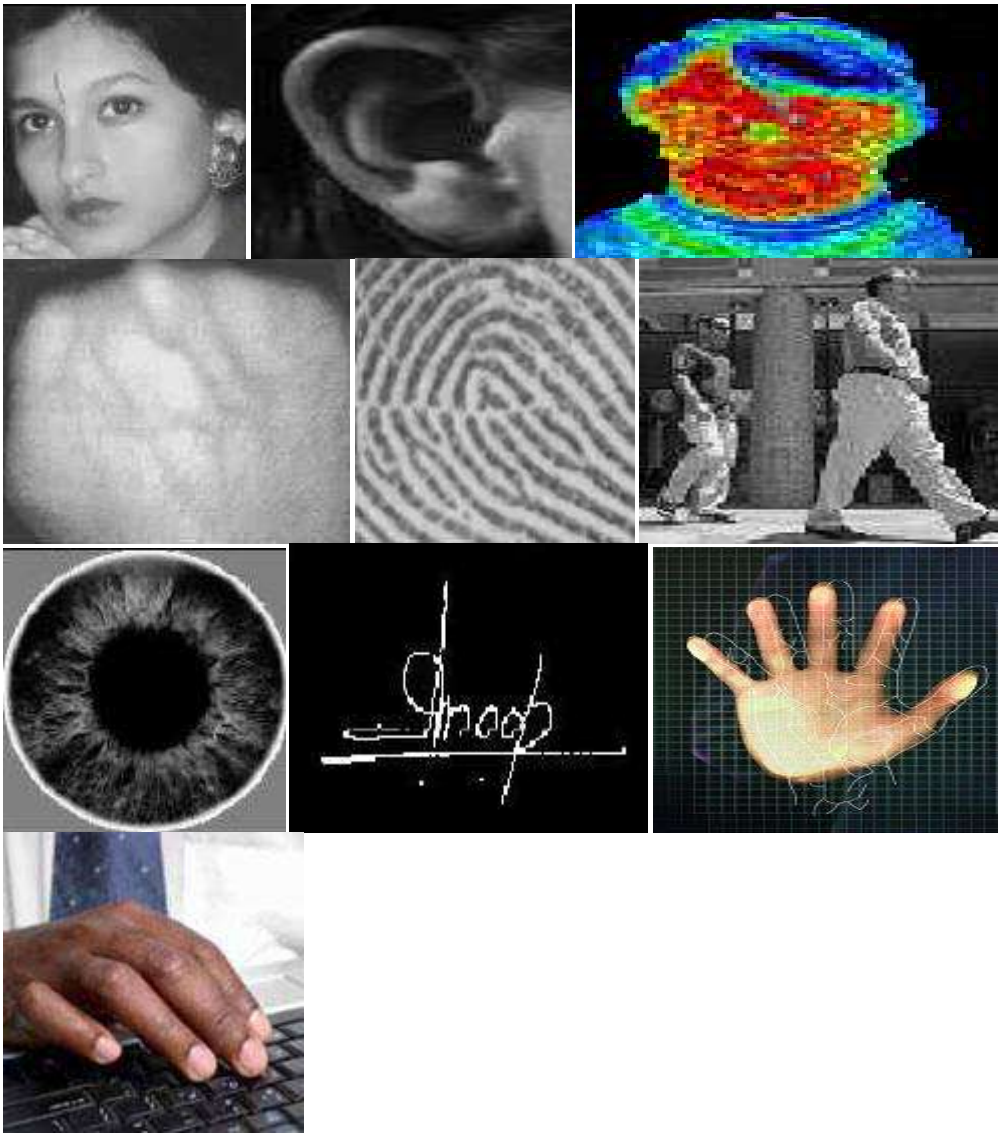


Figure 1. 1: Différentes modalités biométriques [2].

Physiologiques: Visage, Oreille, visage infrarouge, veine de la main, Empreintes digitales, iris, géométrie de la main.
Comportementales : démarche, signature, la dynamique de frappe au clavier.

1.2. Les systèmes biométriques :

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Selon le contexte de l'application, un système biométrique peut fonctionner en mode d'enrôlement ou en mode de vérification ou bien en mode d'identification :

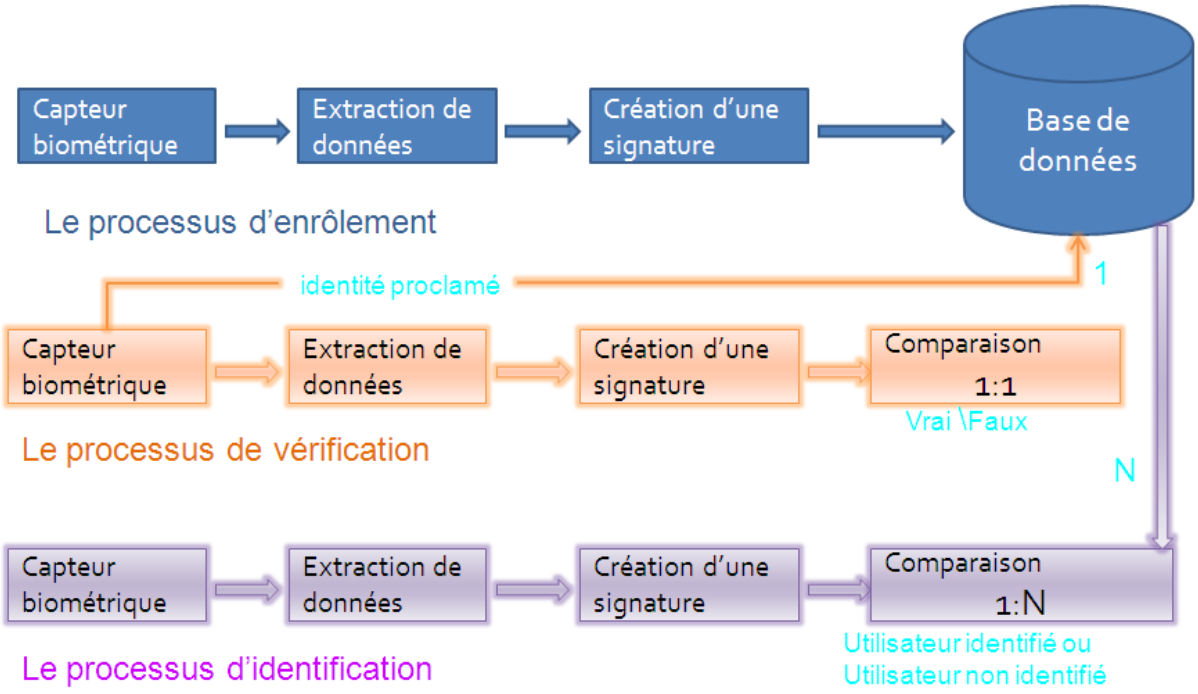


Figure 1. 2: Architecture général d'un système biométrique [5].

L'enrôlement est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques (signatures) sont capturées et enregistrées dans un dépôt de données central ou parfois sur un support portable [3]. Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données [2].

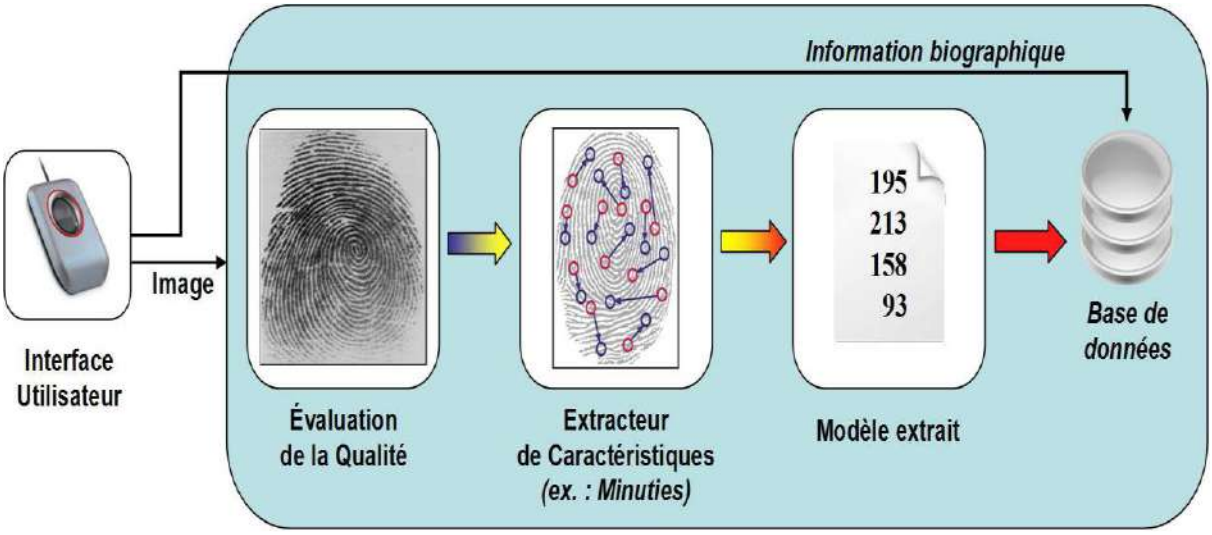


Figure 1. 3 : Enrôlement d'une personne dans un système biométrique [2].

Lorsqu'un système biométrique opère en mode authentification (Figure 1.4), l'utilisateur Affirme son identité et le système vérifie si cette affirmation est valide ou non.

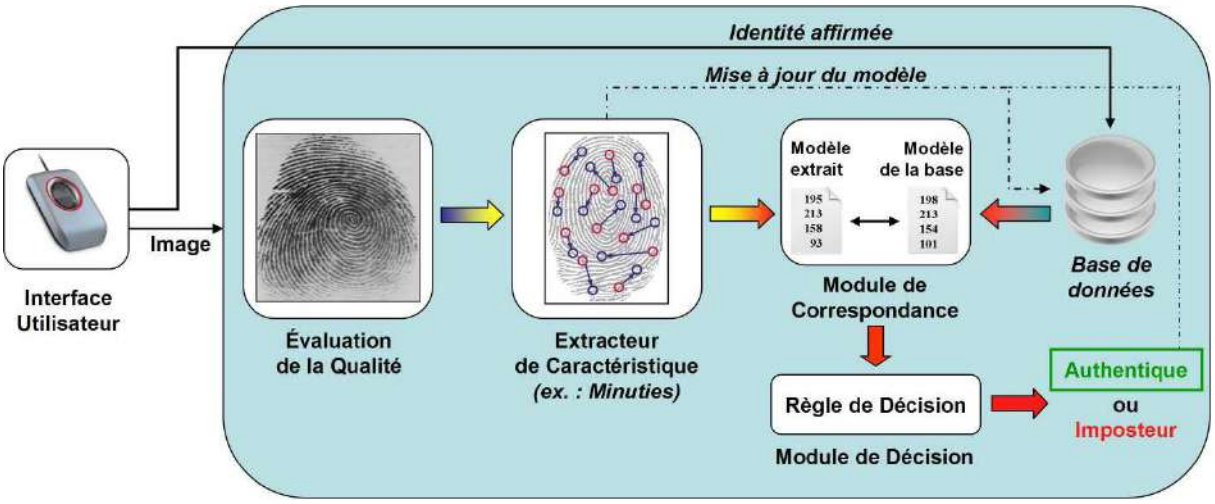


Figure 1. 4: Authentification d'un individu dans un système biométrique [2].

Pour illustrer ce principe, prenons la situation où un utilisateur (M. X) souhaite retirer de l'argent à un distributeur de billets en entrant son code personnel d'identification (code PIN) et en présentant une modalité biométrique. Le système acquiert alors les données biométriques et va les comparer uniquement avec le modèle enregistré correspondant à M. X. On parle alors de correspondance 1:1. Ainsi, si l'entrée biométrique de l'utilisateur et le modèle enregistré dans la base de données correspondant à l'identité affirmée possèdent un degré de similitude élevé,

l'affirmation est validée et l'utilisateur est considéré comme étant un authentique. Dans le cas contraire, l'affirmation est rejetée et l'utilisateur est considéré comme étant un imposteur. En résumé, un système biométrique opérant en mode vérification répond à la question "Suis-je bien M. X?" [2].

Dans un système biométrique opérant en mode identification (Figure. 1.5), l'utilisateur ne dévoile pas explicitement son identité. Cependant, l'affirmation implicite faite par l'utilisateur est qu'elle est une des personnes déjà enrôlées par le système. Ainsi, l'échantillon biométrique de l'individu est comparé avec les modèles de toutes les personnes de la base de données. On parle alors de correspondance 1:N. La sortie du système biométrique est constituée par l'identité de la personne dont le modèle possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée. Typiquement, si la plus grande similarité entre l'échantillon et tous les modèles est inférieure à un seuil de sécurité minimum fixé, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système. Dans le cas contraire, la personne est acceptée[2][3].

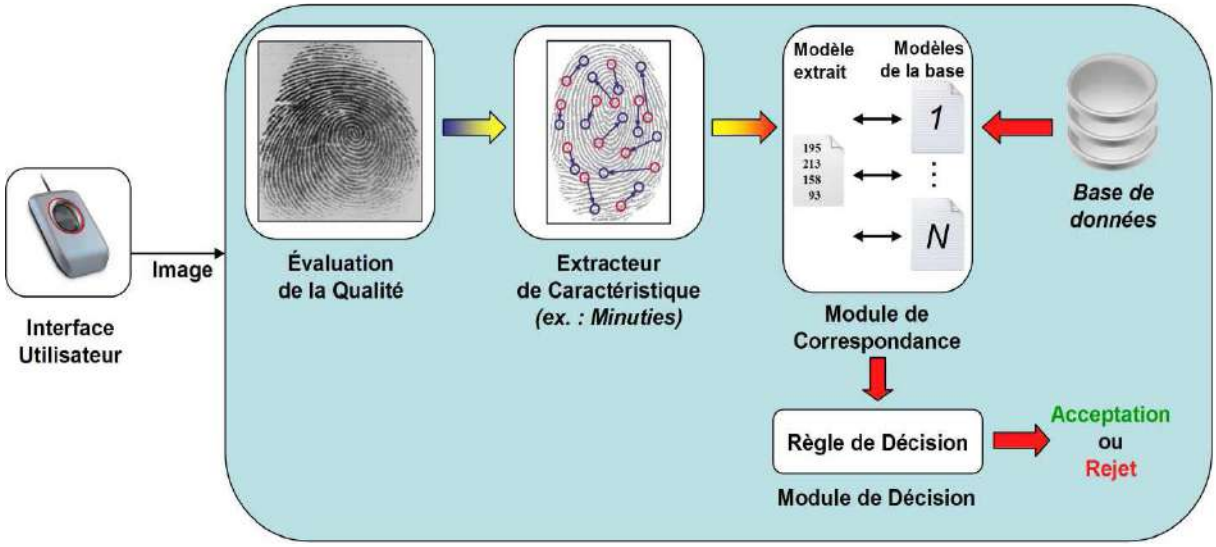


Figure 1. 5 : Identification d'un individu dans un système biométrique [2].

Un exemple de système opérant en mode identification serait l'accès à un bâtiment sécurisé : tous les utilisateurs qui sont autorisés à entrer dans le bâtiment sont enrôlés par le système ; lorsqu'un individu essaye de pénétrer dans le bâtiment, il doit d'abord présenter ses données biométriques au système et, selon la détermination de l'identité

de l'utilisateur, le système lui accorde le droit d'entrée ou non. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ?"[2].

1.3. Types de la biométrie :

Les systèmes biométriques sont généralement classés par l'industrie dans deux grandes catégories : la biométrie morphologique ou physiologique (en anglais : physiological) et la biométrie comportementale (en anglais : behavioral).

La biométrie morphologique est basée sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine et de l'iris de l'oeil.

La biométrie comportementale, quant à elle, se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, l'empreinte de sa voix, sa démarche et sa façon de taper sur un clavier.

À l'instar de la Commission Nationale de l'Informatique et des Libertés (CNIL) de France, il convient d'ajouter à ces deux catégories l'étude des traces biologiques regroupant de façon non exhaustive l'analyse de l'ADN, du sang et des odeurs. De nouvelles techniques sont en développement et il ne serait pas surprenant que plusieurs de celles-ci s'ajoutent dans les années à venir à celles déjà commercialisées ou mentionnées ci-dessus. À titre d'exemple, mentionnons la forme de l'oreille et la thermographie faciale [3].

1.4. Systèmes à technologies multiples :

Plusieurs techniques biométriques peuvent être utilisées dans un même système. Il existe par exemple un système combinant la reconnaissance de la voix avec la reconnaissance de l'écriture (signature). Les systèmes biométriques peuvent aussi s'utiliser en conjugaison avec d'autres systèmes ou d'autres technologies. Il existe des systèmes où l'image de l'empreinte digitale du pouce est emmagasinée sur une carte à microprocesseur et l'activation de cette carte nécessite l'utilisation d'un mot de passe. Ces technologies sont appelées multimodales [3].

1.5. Description des principales techniques biométriques commercialisée :

1.5.1 Empreintes digitales :

L'identification à l'aide des empreintes digitales est chargée d'histoire. Il s'agit de la plus vieille technique biométrique déjà utilisée par les Chinois il y a un millénaire, ensuite remise à jour par le Britannique Galton il y a un siècle. Elle est depuis largement utilisée par l'ensemble des forces de l'ordre de la planète. Soutenue par l'apport des nouvelles technologies, son utilisation n'est désormais plus confinée à la chasse aux criminels.Selon le International Biometric Group (IBG), l'empreinte digitale avec 48,8 % des revenus dominait le marché de la biométrie en 2000.

1.5.2 Forme de la main ou des doigts de la main :

Si l'une des premières formes de mesures biométriques fut la dactyloscopie, la reconnaissance de la forme de la main est considérée, quant à elle, comme l'ancêtre des technologies biométriques. À la fin des années soixante, Robert P. Miller déposa un brevet pour un appareil permettant de mesurer des caractéristiques de la main et de les enregistrer pour comparaison ultérieure. Quelques années plus tard, Identité, le premier système commercial basé sur cette technique, était installée dans une firme d'investissements de Wall Street.

Selon l'International Biométrique Group (IBG) la forme de la main occupait 10,4 % du marché des technologies biométriques en 2000.

1.5.3 visage :

Le développement de systèmes biométriques basés sur la reconnaissance du visage est des plus récents. En 1982, les chercheurs Hay et Young dans un ouvrage intitulé The Human Face mentionnent que l'humain, pour reconnaître un visage, utilise les caractéristiques globales et locales qui le composent. Par la suite, différentes recherches furent effectuées afin de voir si cette capacité de reconnaissance pouvait être reproduite informatiquement. Ces recherches donnèrent naissance à plusieurs techniques de reconnaissance du visage dont les plus répandues sont les visages propres et son dérivé le feature analysis. C'est à partir des travaux du professeur Teuvo Kohonen (1989), chercheur en réseaux neuronaux de l'Université d'Helsinki, et des travaux de Kirby et Sirovich21 (1989) de l'Université Brown du Rhode Island, que fut mis au point par le MIT un système de reconnaissance du visage nommé eigenface.

La reconnaissance de la forme du visage occupait en 2000 selon IBG 15,4 % du marché de la biométrie.

1.5.4 Balayage de la rétine :

En 1936, le Dr Carleton Simon et le Dr Isadore Goldstein eurent l'idée d'utiliser la rétine de l'oeil à des fins d'identification après qu'ils aient vu une photographie des vaisseaux sanguins d'une rétine. Ils établirent que ces vaisseaux sont uniques pour chaque personne. Vingt ans plus tard, le Dr Paul Tower, dans une étude sur les jumeaux identiques, confirma cette unicité. Au milieu des années soixante-dix, cette idée fut reprise dans le but de mettre au point un système d'identification biométrique commercialisable. Cette technologie, probablement à cause de son coût élevé, est peu répandue et sa part de marché n'est pas répertoriée dans les études de marché d'IBG.

1.5.5 Reconnaissance de l'iris :

L'idée d'utiliser l'iris de l'œil pour identifier les personnes fut proposée par l'ophtalmologiste Frank Burch en 1936. Deux autres membres de cette profession, Aran Safir et Leonard Fom, déposèrent un brevet concernant cette technologie en 1987. En 1989, ils demandèrent l'aide du professeur John Daugman de l'Université de Cambridge pour qu'il confectionne une méthode de calcul (algorithme) permettant d'utiliser cette technologie, travail complété en 1994. Les premières applications commerciales furent livrées quelques années plus tard.Malgré qu'elle soit récente, cette technologie biométrique détenait selon IBG 6,2 % des parts du marché en 2000.

1.5.6 Reconnaissance de la voix :

C'est en 1962 que Lawrence Kersta, un ingénieur du Bell Laboratoires, établit que la voix de chaque personne est unique et qu'il est possible de la représenter graphiquement. La voix est constituée de composantes physiologiques et comportementales. À cette époque, des travaux sur la voix furent aussi menés par des entreprises comme IBM et Texas Instruments et plusieurs corps policiers s'y intéressèrent. Dans les années quatre-vingt, plusieurs entreprises développèrent des systèmes de reconnaissance de la voix pour les corps policiers et les agences d'espionnage. Au début des années quatre-vingt-dix, le gouvernement américain demanda à ces entreprises de mettre au point un système pour le marché commercial.
Selon IBG, cette technologie biométrique détenait 4,3 % du marché en 2000.

1.5.7 Reconnaissance de l'écriture (signature) :

Dès 1929, Osborn établit que l'écriture dépend de plusieurs facteurs caractéristiques. Pour imiter une signature, il faut donc non seulement imiter la forme de l'écriture mais aussi tenir compte de ces facteurs reliés notamment à la vitesse, aux conditions environnantes et à la dextérité musculaire. Par la suite, diverses techniques de reconnaissance de la signature furent mises au point au bénéfice notamment des banques et des corps policiers. De façon non exhaustive, différents travaux, dont ceux de A.J. Mauceri (1965), de R.N. Nagel et A. Rosenfeld (1977) et de N.M. Herbst et C.N. Liu (1977) menèrent graduellement au dépôt d'une centaine de brevets de reconnaissance dynamique de la signature. Cette technologie représentait 2,7 % du marché de la biométrie en 2000 selon IBG.

1.5.8 Dynamique de frappe au clavier :

Durant la seconde guerre mondiale, les services secrets militaires savaient distinguer les messages en code morse de l'ennemi par ce qu'ils appelaient « Fist of the sender » ou l'écriture de l'expéditeur. En fait les militaires mesuraient le rythme de frappe pour déterminer qui était l'envoyeur. Au début des années quatre-vingt, la US National Science Fondation commanda une étude afin d'établir si cette particularité pouvait être Utilisée pour identifier des personnes par le rythme de frappe sur un clavier. À cette Époque, le National Bureau of Standards américain effectuait aussi une étude concluant à L'existence de caractéristiques uniques lorsqu'une personne tape sur un clavier. Elle confiale mandat au Stanford Research Institute (SRI) qui travailla sur la problématique Jusqu'en 1985 et développa une technologie biométrique basée sur la dynamique de frappe au clavier. Selon IBG, cette technologie occupait 0,4 % du marché de la biométrie en 2000.

1.5.9 Forme des veines de la main :

Ce système a été inventé par l'ingénieur britannique Joe Rice en 1984. Avant de commercialiser la découverte, une étude fut commandée à Cambridge Consultants afin d'établir que les veines de la main sont uniques pour chaque individu [3].

Le développement de ces techniques dans le domaine de la sécurité signale le passage de système d'identification des personnes jusqu'à présent centrés sur la

recherche d'informations administratives du système organisé auteur de la saisie et du stockage d'informations [6].

1.6. Quelque Avantages et Inconvénients :

Le tableau suivant illustre quelque avantages et inconvénient des différentes techniques biométrique.

Table 1.1 : Avantages et inconvénients des technologies biométriques [7].

Techniques	Avantages	Inconvénients
Empreintes digitales	• Cout. • Facilité de mise en place. • Talle du capteur.	• Qualité optimale des appareils de mesure. • Acceptabilité moyenne. • Possibilité d'attaque (rémanence de l'empreinte…).
Forme de la main	• Très ergonomique. • Bonne acceptabilité.	• Système encombrant. • Cout. • Perturbation par des blessures et l'authentification des membres des mêmes familles.
Visage	• Cout. • Peut encombrant. • Bonne acceptabilité.	• Jumeaux. • Psychologie, religion. • Déguisement. • Vulnérable aux attaques.
Rétine	• Fiabilité. • Pérennité.	• Cout. • Acceptabilité faible. • Installation difficile.
Iris	• Fiabilité.	• Acceptabilité très faible. • Contraintes d'éclairage.
Voix	• Facile.	• Vulnérable aux attaques.
Signature	• Ergonomie.	• Dépendent de l'état émotionnel de la personne. • Fiabilité
Frappe au clavier	• Ergonomie.	• Dépendent de l'état physique de la personne.

1.7. Mesure de la performance d'un système biométrique :

Un système biométrique n'utilise pas toute l'information contenue dans l'image ou le signal capté, il en extrait certaines caractéristiques, ce qui réduit la qualité d'informations, donc la capacité du système à reconnaitre l'unicité d'une donnée, puis il effectue un calcul et obtient un résultat à partir des données recueillies.

Sa robustesse dépend du nombre de critères retenus et de la méthode de modalisation(ou de calcul) utilisée [3] :

- ***Les difficultés rencontrées***

- variabilité intra-classe, similarité interclasse
- Segmentation
- Bruit d'acquisition
- Performances des systèmes (taux d'erreur, vitesse)
- Individualité des caractéristiques biométriques
- Fusion de plusieurs modalités biométriques
- Attaques sur les systèmes biométriques
- Problèmes éthiques

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

1. Le premier critère s'appelle le taux de faux rejet ("False Reject Rate" ou FRR). Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système,

2. Le deuxième critère est le taux de fausse acceptation ("False Accept Rate" ou FAR).Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système,

3. Le troisième critère est connu sous le nom de taux d'égale erreur ("Equal Error Rate" ou EER). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses Acceptations [2][8].

La figure 1.6. Illustre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs tandis que l'EER est représenté sur la figure 1.6.

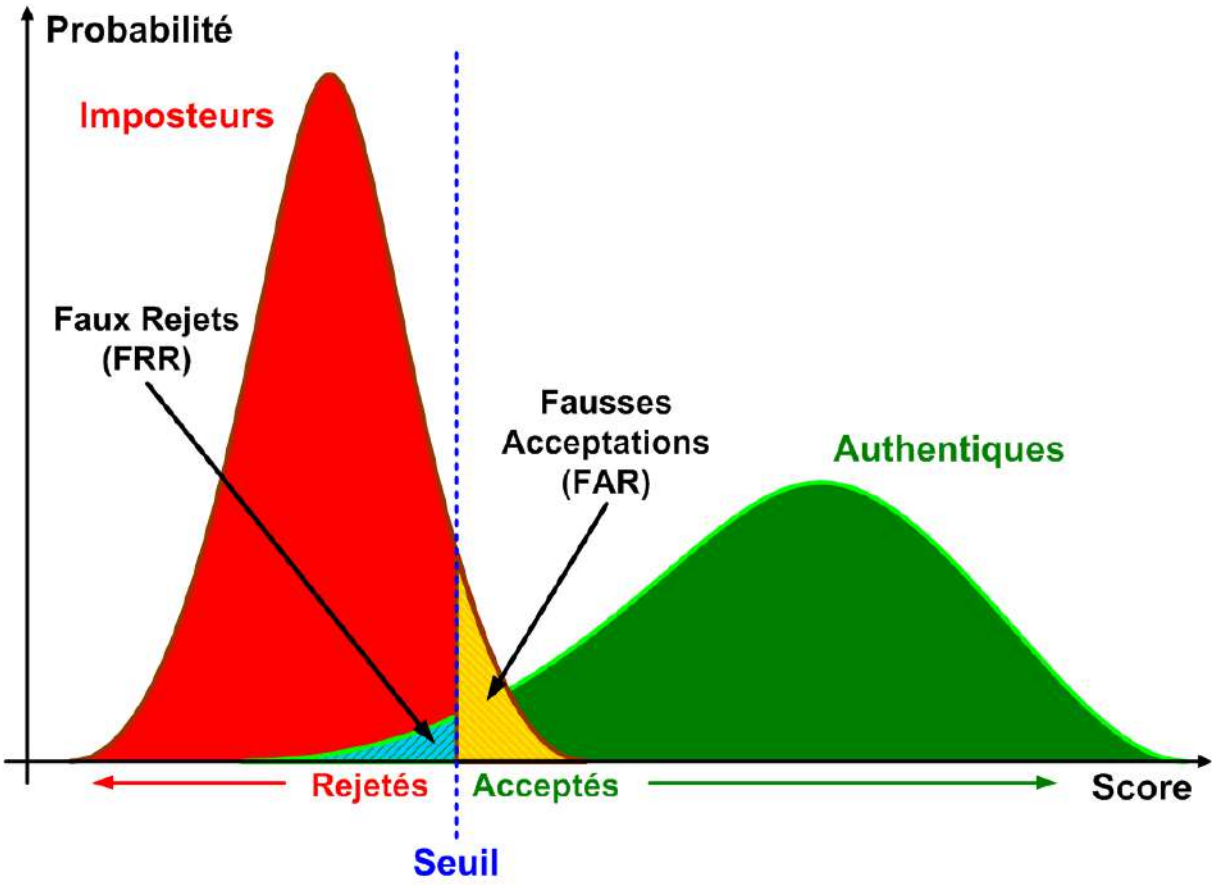


Figure1.6: illustration du **FRR** et du **FAR [2]**

Pour mesuré la performance du système, on utilise ce que l'on appelle une courbe ROC (pour "Receiver Operating Characteristic" en anglais). La courbe ROC (Figure. 1.7) trace le taux de faux rejet en fonction du taux de fausse acceptation Plus cette courbe tend à épouser la forme du repère, plus le système est Performant, c'est-à-dire possédant un taux de reconnaissance global élevé [2].

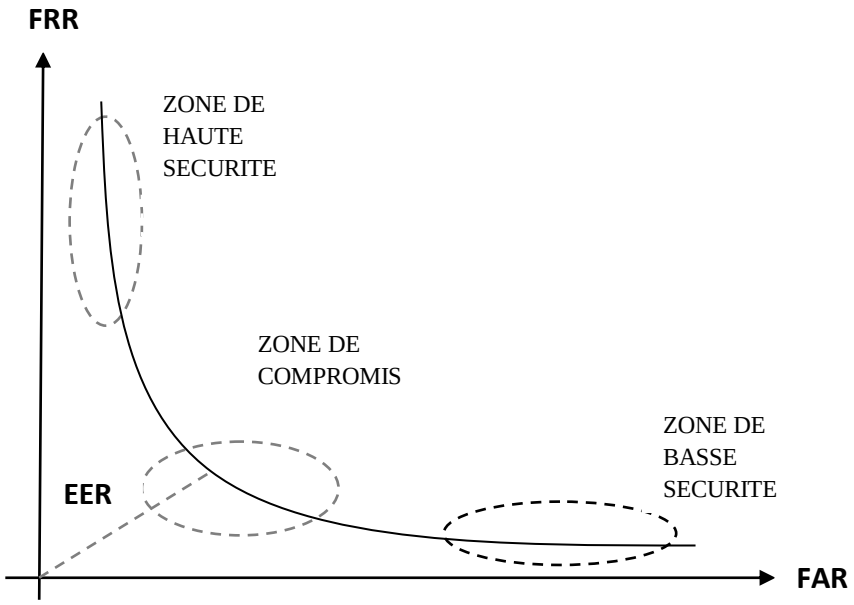


Figure1.7 : Courbe ROC [2].

1.8. Applications des systèmes biométriques :

Les applications de la biométrie peuvent être divisées en trois groupes principaux :

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

De nos jours les systèmes biométriques sont de plus en plus utilisés dans des applications civiles. Par exemple, le dispositif de Schiphol Privium à l'aéroport d'Amsterdam, utilise un capteur de l'iris pour accélérer la procédure de contrôle des passeports et des visas .Les passagers insèrent leur carte dans un lecteur et se mettent en face d'un appareil-photo ; ce dernier acquiert l'image de l'oeil. Des processus de traitement d'images sont alors lancés afin de localiser l'iris et de calculer une signature appelée « Iriscode » Une fois l'Iriscode calculé, il est comparé aux données stockées dans la carte pour identifier le passager. Un dispositif semblable est également employé pour vérifier l'identité des employés de l'aéroport qui travaillent dans des secteurs de haute sécurité. Un autre exemple d'utilisation à grande échelle de la reconnaissance faciale est celui de la ville de Newham, dans la banlieue de Londres. Il s'est vu décerner le trophée Big Brother Award en 1998 par l'organisation non gouvernementale Privacy International.

A en croire les perspectives de l'International Biometric Group, le marché de la sécurité des biens et des personnes ne s'est jamais aussi bien porté. En 2005, le marché représentait environ 1,8 milliard de dollars et pourrait atteindre les 5 milliards en 2008. Les technologies les plus répandues sont les empreintes digitales (48% du marché), la morphologie faciale (15,4% du marché), la géométrie de la main (11%), l'iris (9%), la reconnaissance vocale (6%), la rétine, la morphologie des oreilles ainsi que la radiographie dentaire. Notons que les techniques comportementales (comme la démarche, le sourire, le mouvement des yeux, etc.) ont quand à elles du mal à s'imposer.

1.9. Conclusion :

Ce chapitre a présenté un aperçu général, d'une part, quelques notions et définitions de base liées à la biométrie et d'autre part le principe de fonctionnement des systèmes biométriques ainsi que les outils utilisés pour mesurer leurs performances.

L'objectif du chapitre suivant est de présenter en détails le technique de la reconnaissance de visage parmi les autres techniques biométriques, car elle constitue l'objectif de ce travaile.

La reconnaissance du visage

2.1. Introduction :

La reconnaissance de visage est une tâche que les humains effectuent naturellement et sans effort dans leurs vies quotidiennes. La grande disponibilité d'ordinateurs puissants et peu onéreux ainsi que des systèmes informatiques embarqués ont suscité un énorme intérêt dans le traitement automatique des images et des vidéos numériques au sein de nombreuses applications, incluant l'identification biométrique, la surveillance, l'interaction homme-machine et la gestion de données multimédia. La reconnaissance faciale, en tant qu'une des technologies biométriques de base, a pris une part de plus en plus importante dans le domaine de la recherche, ceci étant dû aux avances rapides dans des technologies telles que les appareils photo numériques, Internet et les dispositifs mobiles, le tout associé à des besoins en sécurité sans cesse en augmentation [9].

2.2. La place de la reconnaissance du visage parmi les autres techniques biométriques :

Les empreintes digitales sont les caractéristiques biométriques les plus communément Utilisées pour la reconnaissance de criminels. Le premier système automatique d'authentification utilisant les empreintes digitales a été commercialisé au début des années soixante. D'autres parts, plusieurs études ont démontré que l'iris est la caractéristique la plus fiable car la texture de l'iris reste stable au cours de la vie.Toutefois, ces méthodes présentent l'inconvénient majeur d'être intrusives, ce qui limite énormément leurs domaines d'applications. De plus, une méthode comme l'identification de l'iris reste contraignante pour les utilisateurs qui n'apprécient pas de placer leur oeil devant un appareil. A l'inverse, des systèmes d'identification basés sur l'analyse des images de visage ne présentent aucune contrainte pour les utilisateurs. La reconnaissance faciale est une modalité qui peut être implémentée de manière indépendante des autres modalités biométriques, elle est souvent utilisée dans des applications de surveillance. La reconnaissance faciale offre plusieurs avantages : le système de capture (c.à.d les caméras) est facile à installer, il est accepté dans les lieux

publics ce qui permet d'avoir des bases de données de plus en plus grandes et ainsi d'améliorer les performances de la reconnaissance [1]. Le visage occupe la seconde place en biométrie [10].

2.3. Les étapes de reconnaissance du visage:

La reconnaissance automatique de visage s'effectue en trois étapes principales :
(1) détection de visages, (2) extraction et normalisation des caractéristiques du visage, (3) identification et/ou vérification (voir figure 2.1). Certaines techniques de traitements d'images peuvent être communes à plusieurs étapes. Par exemple, l'extraction des caractéristiques faciales (yeux, nez, bouche) est utilisée aussi bien pour la détection que pour l'identification de visages. Par ailleurs, les étapes de détection de visage et d'extraction de caractéristiques peuvent être exécutées simultanément. Cela dépend notamment de la nature de l'application, de la taille de la base d'apprentissage, et des conditions de prise de vue (bruit, occultation, etc.). Enfin, les techniques de traitement utilisées dans chaque étape sont très critiques pour les applications biométriques, et doivent, par conséquence, être optimisées pour améliorer les performances du système global, Cette technologie nous aide à éviter qu'une personne puisse avoir deux cartes d'identité ou usurpe l'identité d'une autre personne.

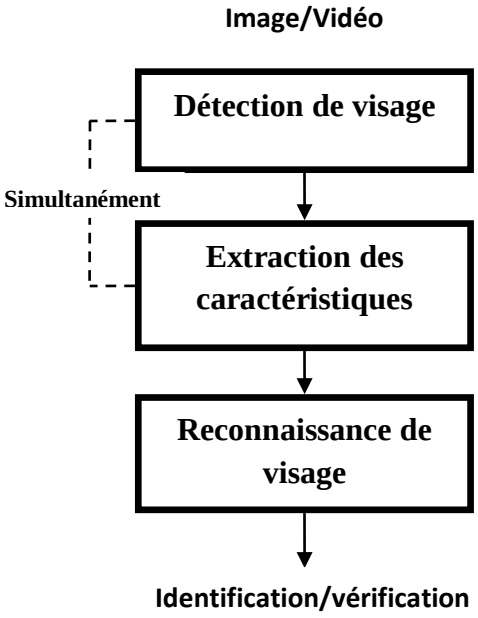


Figure 2. 1. : Les étapes de la reconnaissance de visage [1].

Dans ce qui suit nous allons détailler chaque étape du système de reconnaissance de visage, et nous présenterons les déférentes modes et méthodes de la reconnaissance de visage [1].

2.3.1. Détection de visage :

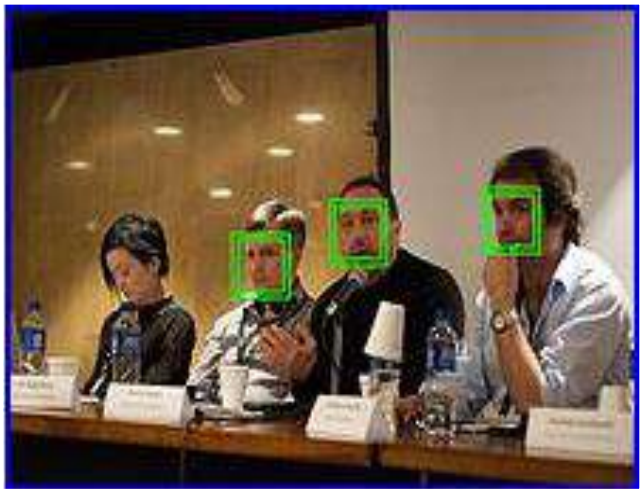


Figure 2. 2. : Détection de visage [11].

La détection de visage est un domaine de la vision par ordinateur consistant à détecter un visage humain dans une image numérique. C'est un cas spécifique de détection d'objet, où l'on cherche à détecter la présence et la localisation précise d'un ou plusieurs visages dans une image. C'est l'un des domaines de la vision par ordinateur parmi les plus étudiés, avec de très nombreuses publications, brevets, et de conférences spécialisées. La forte activité de recherche en détection de visage a également permis de faire émerger des méthodes génériques de détection d'objet.

La détection de visage a de très nombreuses applications directes en vidéo-surveillance, biométrie, robotique, commande d'interface homme-machine, photographie, indexation d'images et de vidéos, recherche d'images par le contenu, etc... Elle permet également de faciliter l'automatisation complète d'autres processus comme la reconnaissance de visage ou la reconnaissance d'expressions faciales [1], 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..[9].

2.3.2. Extraction de caractéristiques du visage :

L'extraction des caractéristiques telles que les yeux, le nez, la bouche est une étape prétraitement nécessaire à la reconnaissance faciale. On peut distinguer deux pratiques différentes : la première repose sur l'extraction de régions entières du visage, elle est souvent implémentée avec une approche globale de reconnaissance de visage. La deuxième pratique extrait des points particuliers des différentes régions caractéristiques du visage, tels que les coins des yeux, de la bouche et du nez. Elle est utilisée avec une méthode locale de reconnaissance et aussi pour l'estimation de la pose du visage. Par ailleurs, plusieurs études ont été menées afin de déterminer les caractéristiques qui semblent pertinentes pour la perception, la mémorisation et la reconnaissance d'un visage humain. par exemple, les caractéristiques pertinentes rapportées sont : les cheveux, le contour du visage, les yeux et la bouche. Cette étude a également démontré le rôle important que joue le nez dans la reconnaissance faciale à partir des images de profil. En effet, dans ce cas de figure, il est évident que la forme distinctive du nez est plus intéressant que les yeux ou la bouche les auteurs ont particulièrement établi que la partie supérieure du visage est plus utile pour la reconnaissance faciale que la partie inférieure [1].

2.3.3. La reconnaissance de visage :

Le module de reconnaissance exploite les caractéristiques du visage ainsi extraites pour créer une signature numérique qu'il stocke dans une base de données. Ainsi, à chaque visage de la base est associée une signature unique qui caractérise la personne correspondante, Un être humain moyen atteint un taux de reconnaissance de 99% peut on atteindre ce taux ou le dépasser avec un système informatique [13]. D'une manière générale, nous posons le problème comme celui de l'apprentissage d'une distance entre visages [14], La reconnaissance d'un visage requête est obtenue par l'extraction de la signature requête correspondante et sa mise en correspondance avec la signature la plus proche dans la base de données. Beaucoup de connaissances dans les domaines de la reconnaissance des formes, du traitement d'images, des statistiques ont été appliquées au domaine de la reconnaissance du visage [15], la reconnaissance dépend du mode de comparaison utilisé : vérification ou identification [1].

2.3.3.1. Identification :

Dans les années 90, le but de la recherche dans ce domaine se concentrait sur L'identification des visages enregistrés dans de bonnes conditions [15].

Ayant un flux d'image, ou une image qui contient un visage, l'identification est la reconnaissance à partir d'une base de données sans autre connaissance a priori de l'identité de la personne .cette tache donne lieu à une comparaison de type 1 to N :On compare une image de flux avec les images enregistrées dans la base de donnée (figure 2.3).Une application est la reconnaissance de personne « dangereuses » enregistrées dans une Watch List. Cette application sujette à des contraintes de temps de calcul d'où l'enregistrement de caractéristiques du visage au lieu de l'image entière .Aussi l'enregistrement d'une base de donnée du visage est conditionné, en France par l'autorisation de la CNIL (commission nationale informatique et liberté) qui cautionne la protection des donnée personnelles cette autorisation n'est donnée qu'en fonction du fort besoin de sécurité par l'application [16].

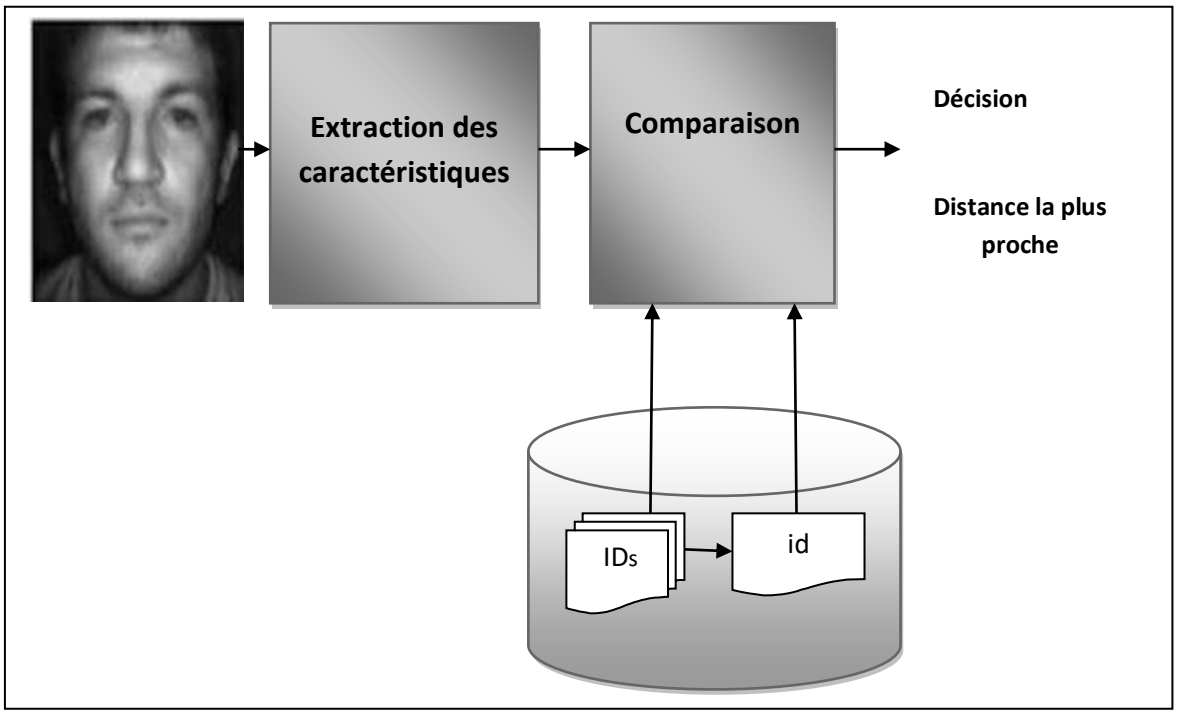


Figure 2. 3 : Schéma d'identification du visage [16].

2.3.3.2. Vérification :

Ayant un flux d'image ,ou une image qui contient un visage, vérification est la reconnaissance à partir d'une image de référence enregistrée au préalable dans une puce ou un fichier c'est une vérification de l'identité revendiquée c'est-à-dire que la personne décline au préalable son identité (figure 2.4) .Cette tache donne lieu à une comparaison 1 to1 ,Une des applications est le contrôle ou vérification d'identité à l'entrée des états unis par exemple (FC le nouveau passeport biométrique).la référence biométrique peut alors être enregistrée dans une base de données mais aussi sur une carte à puce détenue par le personne .dans ce cas la CNIL émet un avis moins restrictif à l'utilisation de la biométrie .Ainsi on peut trouver des appareils électroniques personnels utilisant la biométrie tels que les ordinateurs portables, les coffres, les téléphones etc[16].

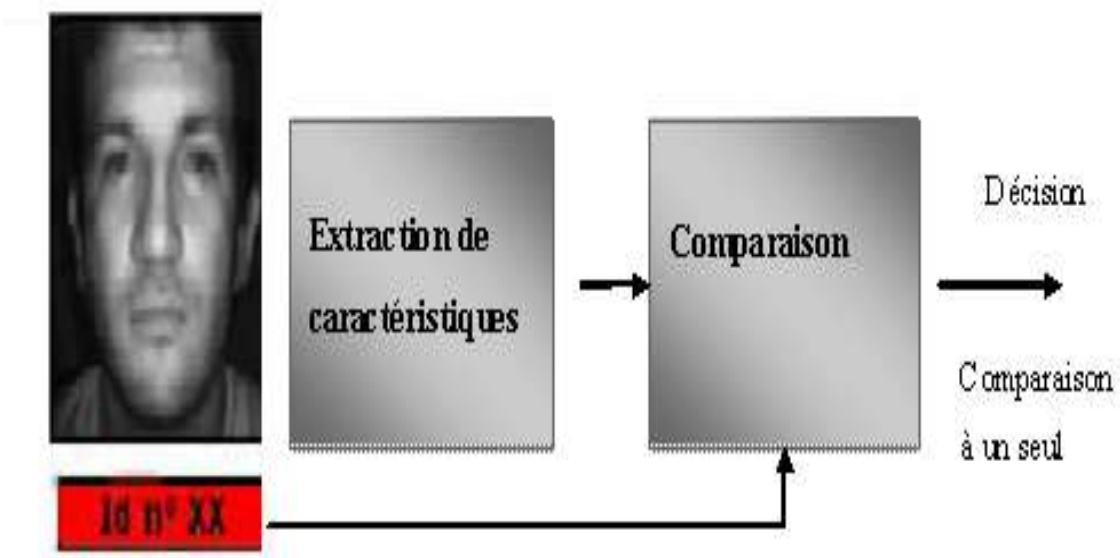


Figure 2. 4 : Schéma de vérification du visage [16].

2.4. Mode de reconnaissance :

Suivant l'application traitée, un système biométrique peut fonctionner suivant un mode de reconnaissance positif ou négatif:

- ✓ Dans une reconnaissance positive, le système permet de déterminer si la personne est celle qu'elle prétend être, de manière implicite ou explicite. Le but d'une reconnaissance positive est d'empêcher plusieurs personnes d'utiliser la même identité. Par exemple, si une personne unique est autorisée à entrer dans une certaine zone sécurisée, le système lui donnera exclusivement l'accès. Si le système arrive à faire correspondre la signature enregistrée de cette personne à la signature extraite de la biométrie acquise, cela correspond à une acceptation, et sinon à un rejet;

- ✓ Pour une demande de reconnaissance négative, le système permet de déterminer si la personne correspond à ce qu'elle nie être de manière explicite ou implicite. L'objet de la reconnaissance est négatif pour empêcher une seule personne d'utiliser de multiples identités. Par exemple, pour une application de prestations sociales, le système enregistre dans sa base de données les personnes qui ont déjà bénéficié de prestations. Si une personne malhonnête souhaite recevoir les prestations une deuxième fois en se proclamant comme étant une tierce personne, le système doit vérifier si celle-ci correspond à un des bénéficiaires enregistrés dans la base de données. Si le système arrive à faire correspondre la signature extraite de la biométrie acquise de cette personne avec une des signatures de la base de données, cela correspond à un rejet, et sinon à une acceptation. Notons que les méthodes traditionnelles d'authentification, telles que les mots de passe, les codes PIN, les clés, les jetons peuvent être utilisées uniquement pour une reconnaissance positive. La reconnaissance négative, quant à elle, ne peut être établie que par la biométrie. En outre, la reconnaissance positive peut fonctionner aussi bien en mode de vérification ou d'identification, mais les applications qui nécessitent une reconnaissance négative ne peuvent être déployées qu'en mode d'identification: en fait, le système doit parcourir la totalité de ses bases de données pour prouver que les données saisies ne sont pas présentes.

2.5. Les méthodes de reconnaissance de visage :

Les méthodes de reconnaissance de visage peuvent être séparées en deux grandes familles, les méthodes globales (ou holistiques) et les méthodes locales, basées sur des modèles. Le choix a été fait de se concentrer sur ces deux types d'approches fondamentale et de n'aborder ni les réseaux neuronaux (plus adaptés à la détection des visages), ni les modèles cachés de Markov (plus utilisés en reconnaissance de la parole) car ces deux dernières techniques rencontrent des problèmes lorsque le nombre d'individus augmente (les calculs deviennent très importants) ; de plus elles ne conviennent pas pour les systèmes de reconnaissance basés sur une seule "image modèle" car de nombreuses images par personne sont nécessaires pour entraîner les systèmes afin de configurer leurs paramètres de façon "optimale". Cependant, on pourra se référer aux travaux des équipes françaises du LE2I et du GIPSA qui les ont respectivement appliquées aux images de visage et aux signaux de parole [2].

2.5.1. Méthodes globales

Les méthodes globales sont basées sur des techniques d'analyse statistique bien connues. Il n'est pas nécessaire de repérer certains points caractéristiques du visage (comme les centres des yeux, les narines, le centre de la bouche, etc.) à part pour normaliser les images. Dans ces méthodes, les images de visage (qui peuvent être vues comme des matrices de valeurs de pixels) sont traitées de manière globale et sont généralement transformées en vecteurs, plus faciles à manipuler.

L'avantage principal des méthodes globales est qu'elles sont relativement rapides
A mettre en œuvre et que les calculs de base sont d'une complexité moyenne. En revanche, elles sont très sensibles aux variations d'éclairement, de pose et d'expression faciale. Ceci se comprend aisément puisque la moindre variation des conditions de l'environnement ambiant entraîne des changements inéluctables dans les valeurs des pixels qui sont traités directement.

Ces méthodes utilisent principalement une analyse de sous-espaces de visages. Cette expression repose sur un fait relativement simple : une classe de "formes" qui nous intéresse (dans notre cas, les visages) réside dans un sous-espace de l'espace de l'image d'entrée.

Par exemple, considérons une petite image de 64×64, en niveaux de gris codés sur 8 bits (donc de 0 à 255). Cette dernière possède 4096 pixels qui peuvent exprimer un grand nombre de classes de formes, comme des arbres, des maisons ou encore des visages. Cependant, parmi les 256^4096 > 10^9864 "configurations" possibles, seulement une petite quantité peut correspondre à des visages. Ainsi, la représentation de l'image originale est très redondante et la dimensionnalité de cette représentation pourrait être grandement réduite si l'on se concentre uniquement sur les formes qui nous intéressent. L'utilisation de techniques de modélisation de sous-espace a fait avancer la technologie de reconnaissance faciale de manière significative[2].

Nous pouvons distinguer deux types de techniques parmi les méthodes globales : les techniques linéaires et les techniques non linéaires.

Les techniques linéaires projettent linéairement les données d'un espace de grande dimension (par exemple, l'espace de l'image originale) sur un sous-espace de dimension inférieure. Malheureusement, ces techniques sont incapables de préserver les variations non convexes des variétés (géométriques donc au sens mathématique du terme) de visages afin de différencier des individus. Dans un sous-espace linéaire, les distances euclidiennes et plus généralement les distances de Mahalanobis qui sont normalement utilisées pour faire comparer des vecteurs de données, ne permettent pas une bonne classification entre les classes de formes "visage" et "non-visage" et entre les individus eux-mêmes. Ce facteur crucial limite le pouvoir des techniques linéaires pour obtenir une détection et une reconnaissance du visage très précises.

La technique linéaire la plus connue et sans aucun doute l'analyse en composantes principales (PCA), également appelée transformée de Karhunen-Loeve. Le PCA fut d'abord utilisé afin de représenter efficacement des images de visages humains En 1991, cette technique a été reprise dans le cadre plus spécifique de la reconnaissance

faciale sous le nom de méthode des Eigenfaces . Cependant, le PCA classique nécessite que les images de visage soient mises sous formes de vecteurs, ce qui a pour effet de détruire la structure géométrique de l'image. Pour ne pas perdre les informations de voisinage lors du passage de l'image en vecteur, une méthode PCA bidimensionnelle (2-D PCA a été étudiée. Cette méthode prend en entrée des images et non plus des vecteurs.

Il existe d'autres techniques également construites à partir de décompositions linéaires comme l'analyse discriminante linéaire (LDA) ou encore l'analyse en composantes indépendantes (ICA) Tandis que le PCA construit un sous-espace pour représenter de manière "optimale"(mathématiquement parlant) seulement "l'objet" visage, le LDA construit un sous-espace discriminant pour distinguer de façon "optimale" les visages de différentes personnes. Elle permet donc d'effectuer une véritable séparation de classes .Des études comparatives (par exemple, montrent que les méthodes basées sur le LDAdonne généralement de meilleurs résultats que les méthodes basées sur le PCA[2].

L'algorithme ICA, quant à lui, est une généralisation de l'algorithme PCA avec lequel il coïncide dans le cas de données gaussiennes. L'algorithme ICA est basé sur le concept intuitif de contraste et permet d'éliminer la redondance statistique des données de départ. Ce dernier a été rendu célèbre notamment avec l'expérience de la "cocktail party" qui met en avant la résolution d'un problème de séparation (dé corrélation) de sources audio. Bartlett et al. Ont fourni deux architectures différentes pour l'ICA : une première architecture (ICA I) qui construit une base d'images statistiquement indépendantes et une deuxième architecture (ICA II) qui fournit une représentation en code factoriel des données.

Bien que ces méthodes globales linéaires basées sur l'apparence évitent l'instabilité des toutes premières méthodes géométriques qui ont été mises au point, elles ne sont pas assez précises pour décrire les subtilités des variétés (géométriques) présentes dans l'espace de l'image originale. Ceci est dû à leurs limitations à gérer la non-linéarité en reconnaissance faciale : les déformations de variétés non linéaires peuvent être lissées et les concavités peuvent être remplies, causant des conséquences défavorables. Afin de pouvoir traiter ce problème de non-linéarité en reconnaissance faciale, de telles

méthodes linéaires ont été étendues à des techniques non linéaires basées sur la notion mathématique de noyau (“kernel”) comme le Kernel PCA et le Kernel LDA ,Ici, une projection non linéaire (réduction de dimension) de l’espace de l’image sur l’espace de caractéristiques (“feature space”) est effectuée ; les variétés présentes dans l’espace de caractéristiques résultant deviennent simple, de même que les subtilités des variétés qui sont préservées. Bien que les méthodes basées sur le noyau peuvent atteindre une bonne performance sur les données d’entraînement, il ne peut pas en être de même pour de nouvelles données en raison de leur plus grande flexibilité ; contrairement aux méthodes linéaires [2].

2.5.2. Méthodes locales

Les méthodes locales, basées sur des modèles, utilisent des connaissances a priori que l’on possède sur la morphologie du visage et s’appuient en général sur des points caractéristiques de celui-ci. Kanade présenta un des premiers algorithmes de ce type en détectant certains points ou traits caractéristiques d’un visage puis en le comparant avec des paramètres extraits d’autres visages. Ces méthodes constituent une autre approche pour prendre en compte la non-linéarité en construisant un espace de caractéristiques local et en utilisant des filtres d’images appropriés, de manière à ce que les distributions des visages soient moins affectées par divers changements. Les approches Bayesiennes (comme la méthode BIC) les machines à vecteurs de support (SVM) la méthode des modèles actifs d’apparence (AAM) ou encore la méthode “local binary pattern” (LBP) ont été utilisées dans ce but.

Toutes ces méthodes ont l’avantage de pouvoir modéliser plus facilement les variations de pose, d’éclairage et d’expression par rapport aux méthodes globales. Toutefois, elles sont plus lourdes à utiliser puisqu’il faut souvent placer manuellement un assez grand nombre de points sur le visage alors que les méthodes globales ne nécessitent de connaître que la position des yeux afin de normaliser les images, ce qui peut être fait automatiquement et de manière assez fiable par un algorithme de détection.

2.5.3. Méthodes hybrides

Les méthodes hybrides permettent d’associer les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurales) avec l’extraction de caractéristiques d’apparence locales. Elles permettent d’augmenter la stabilité de la performance de reconnaissance lors de changements de

pose, d'éclairement et d'expressions faciales. L'analyse de caractéristiques locales (LFA) et les caractéristiques extraites par ondelettes de Gabor (comme l'Elastic Bunch Graph Matching, EBGM), sont des algorithmes hybrides typiques.

Plus récemment, l'algorithme LogGabor PCA (LG-PCA) effectue une convol- ution avec des ondelettes de Gabor orientées autour de certains points caractéristiques du visage afin de créer des vecteurs contenant la localisation et la valeur d'amplitudes énergétiques locales ; ces vecteurs sont ensuite envoyés dans un algorithme PCA afin de réduire la dimension des données.

La figure 2.5 fournit une classification des algorithmes principaux de reconnaissance faciale.

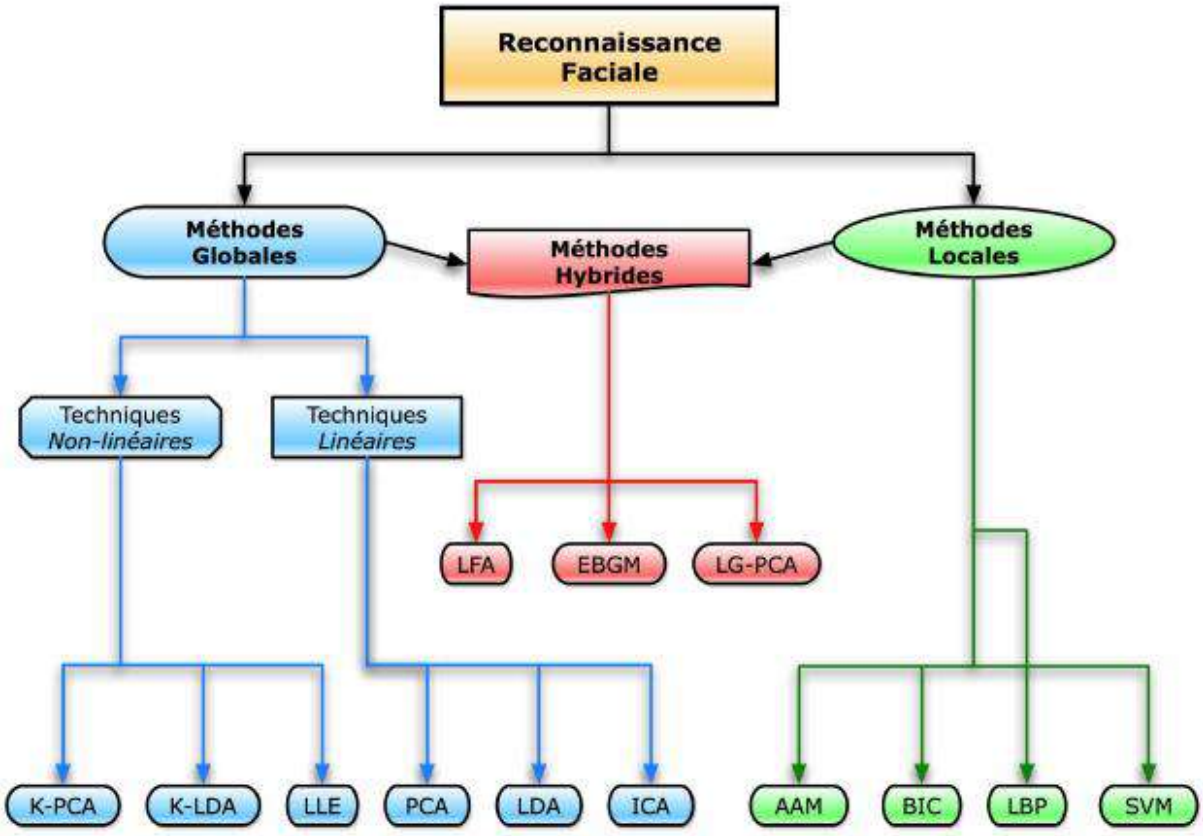


Figure 2. 5 : Une classification des algorithmes principaux utilisés en reconnaissance faciale [2].

2.6. Avantage et Inconvénient :

On trouve quelque avantage et inconvénient dans la reconnaissance de visage, comme l'illustre de la table2.1 :

Table 2.1 : Avantage et Inconvénient de la reconnaissance du visage.

Avantages	Inconvénients
-technique peu couteuse, peu en comburante. -absence de contact avec le capteur, méthode non intrusive pour la personne ; pas de risques pour la santé.	-Les vrais jumeaux ne sont pas différencies. -psychologiquement, certaines personnes rejettent leur image photographique (refus de son image, ajout d'accessoires, rôle, religion, critique de la qualité de la camera, etc.), l'image est considérée comme trop personnelle Peu être utilisée. -en tant que contrôle d'accés, le visage n'est pas, traditionnellement, reconnu comme un mécanisme fiable d'authentification. (put être dupé par l'utilisation de maquillage ou d'un masque en silicone). -dans l'état des systèmes actuels, technique trop sensible au changement d'échelle(taille du visage ou distance de caméra),présence d'arrière plan non stationnaire, changement de position lors de l'acquisition de l'image(inclinaison de la tête ou expression). -tous élément tel que lunettes de soleil, chapeau, moustache, barbe, piercing, blessure peut causer des anomalies avec des systèmes d'identification du visage.

2.7. Utilisations actuelles de la reconnaissance du visage :

La reconnaissance du visage est utilisée comme système de surveillance ou d'identification par les autorités ou les corps policiers principalement dans les lieux publics, les aéroports, les frontières, les casinos, les plages, les guichets automatiques et les laboratoires.

2.8. Conclusion :

Nous présentons dans ce chapitre quelques notions et définitions de base liées à la biométrie de visage. Nous donnerons les étapes et les méthodes de reconnaissance de visage, avantages et inconvénients ainsi que l'utilisation actuelle de la reconnaissance de visage.

L'objectif du chapitre suivant est de présenter en détails la méthode PCA pour la reconnaissance de visage parmi les autres méthodes.

Analyse en Composantes Principales (PCA)

3.1. Introduction :

Plusieurs approches pour la reconnaissance du visage ont été présentées dans le chapitre 2. il y a deux grandes familles : les algorithmes basés sur les approches globales par réduction d'espace et les algorithmes basés sur les approches par points caractéristiques. Nous allons limiter à la première famille étant donné que nous allons utiliser dans notre travail une méthode globale. Nous présenterons donc l'algorithme de réduction d'espace l'ACP [2].

3.2. Analyse en Composantes Principales (PCA) :

L'algorithme PCA ou KL (Karhunen-Loëve) [15] est né des travaux de M. A. Turk et A. P. 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 (respectivement Eigenvectors et Eigenvalues en anglais)[2].

L'idée principale (réduction d'espace) consiste à exprimer M images de départ selon une base de vecteurs orthogonaux particuliers - les vecteurs propres - contenant des informations indépendantes d'un vecteur à l'autre. Les données originales seront donc exprimées d'une manière plus appropriée à la reconnaissance du visage [2][15].

En théorie de l'information, nous voulons extraire l'information caractéristique d'une Image du 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.

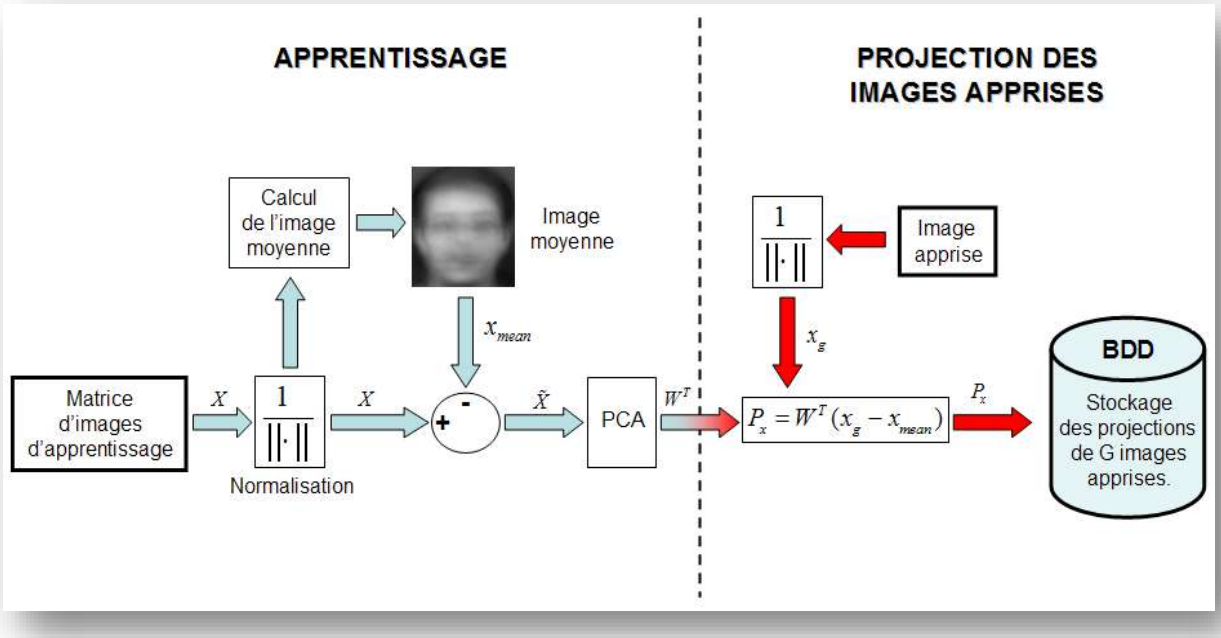


Figure 3.1: Phase d'apprentissage d'un système de reconnaissance de visage utilisant l'ACP [2].

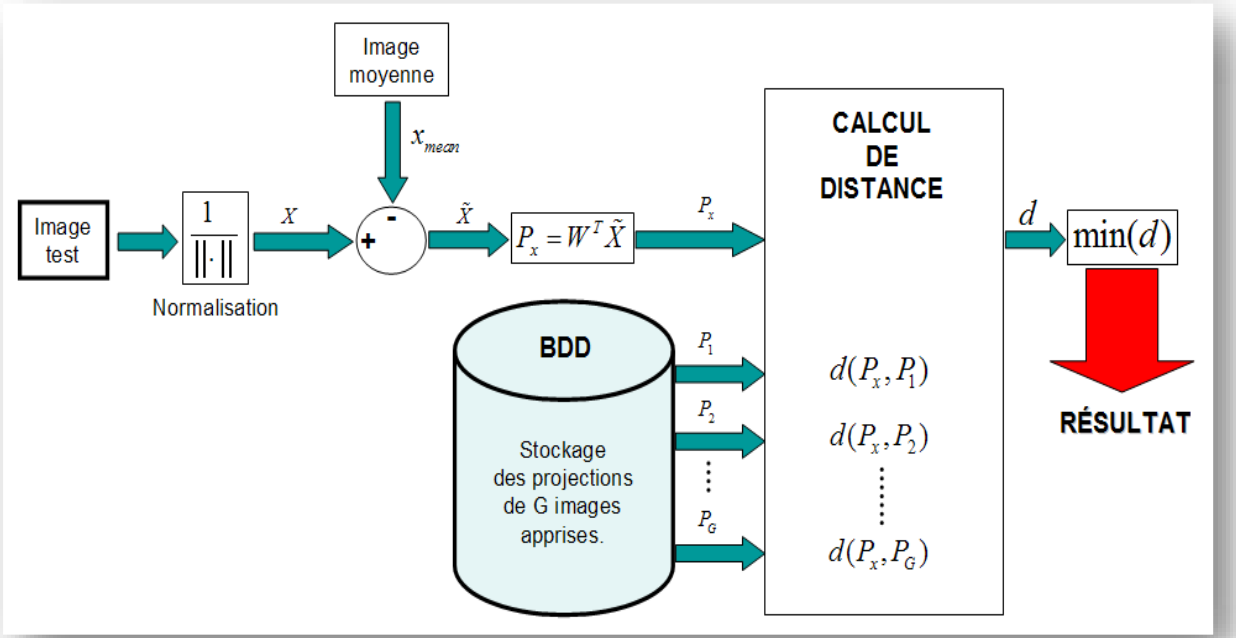


Figure 3.2 : Phase de reconnaissance d'un système de reconnaissance de visage utilisant l'ACP [2].

-Une image Ii(m,n) est traitée comme un vecteur vi(m×n,1) dans un espace vectoriel de grande dimension (N = m × n), par concaténation des colonnes (figure3.3).

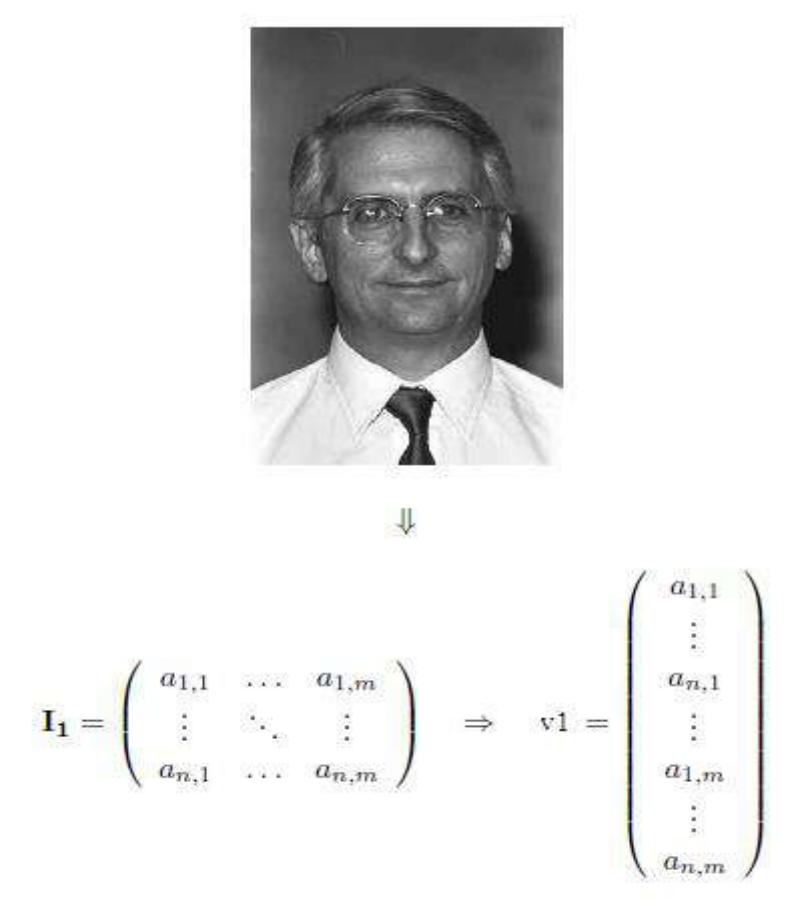


Figure 3.3 : Passage d'une image vers un vecteur dans un espace vectoriel de grande dimension.

Les coefficients ai,j représentent les valeurs des pixels en niveau de gris, codés de 0 à 255.

Après avoir rassemblé les M images dans une unique matrice, nous obtenons une matrice d'images V, où chaque colonne représente une image vi :

$$V = \begin{bmatrix} a_{1,1} & b_{1,1} \cdots & z_{1,1} \\ \vdots & \ddots & \vdots \\ a_{n,m} & b_{n,m} \cdots & z_{n,m} \end{bmatrix}$$

On calcule ensuite l'image moyenne Moy de toutes les images collectées. Cette image est toujours unique pour la même base de données et peut être vu comme le centre de gravité du jeu d'images :

$$Moy = \frac{1}{M} \sum_{i=1}^{M} v_i$$

On ajuste ensuite les données par rapport à la moyenne. L'image moyenne est alors soustraite de chaque image avec la formule suivante :

$$I_{\underset{i}{moy}} = v_i - Moy \quad , i = 1 \dots M$$

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

$$C = \sum_{i=1}^{M} I_{\underset{i}{moy}} \; I_{\underset{i}{moy}}^{T} = AA^T, A = [I_{\underset{1}{moy}} \; I_{\underset{2}{moy}} \dots I_{\underset{m}{moy}}]$$

La prochaine étape consiste à calculer les vecteurs propres et les valeurs de cette matrice de covariance C de taille (N × N), c'est-à-dire de l'ordre de la résolution d'une image.Le problème est que cela peut parfois être très difficile et très long ! En effet, si N > M (si la résolution est supérieure au nombre d'images), il y aura seulementM − 1 vecteurs propres qui contiendront de l'information (les vecteurs propres restants auront des valeurs propres associées nulles). Par exemple, pour 100 images de résolution 320×240, nous pourrions résoudre une matrice L de 100 × 100

au lieu d'une matrice de 76800 × 76800 pour ensuite prendre les combinaisons linéaires appropriées des images Imoy i.

Le gain de temps de calcul serait considérable ! Typiquement, nous passerions d'une complexité de l'ordre du nombre de pixels dans une image à une complexité de l'ordre du nombre d'images.

3.3. Comment procéder pour accélérer les calculs :

Considérons les vecteurs propres ei de $C = \mathrm{A}\mathrm{A}^{\mathrm{T}}$, associés aux valeurs propres λi :

$$\boldsymbol{C}e_i = \boldsymbol{\lambda_i e_i}$$

Les vecteurs propres vi de $L = A^T A$, associés aux valeurs propres μi sont tels que :

$$\boldsymbol{L}v_i = \mu_i v_i$$

Soit :

$$A^T A v_i = \mu_i v_i$$

En multipliant à gauche par A des deux côtés de l'égalité, nous obtenons :

$$AA^T A v_i = A\mu_i v_i$$

Puisque :$\boldsymbol{C} = AA^T$, nous pouvons simplifier :

$$\boldsymbol{C}(Av_i) = \mu_i(Av_i)$$

Nous voyons qu'Avi et μi sont respectivement les vecteurs propres et les valeurs propres de C :

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

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 pré-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.

Une part de la grande efficacité de l'algorithme PCA vient de l'étape suivante qui consiste à ne sélectionner que les k meilleurs vecteurs propres (ceux avec les k plus grandes valeurs propres). On définit alors un espace vectoriel engendré par ces k vecteurs propres, que l'on appelle l'espace des visages Ev ("Face Space").

Les images originales peuvent être reconstituées par combinaison linéaire de ces vecteurs propres. Les représentations graphiques de ces vecteurs rappellent un peu des images fantômes, chacune mettant en avant une partie du visage, on les appelle eigenfaces (figure3.4).

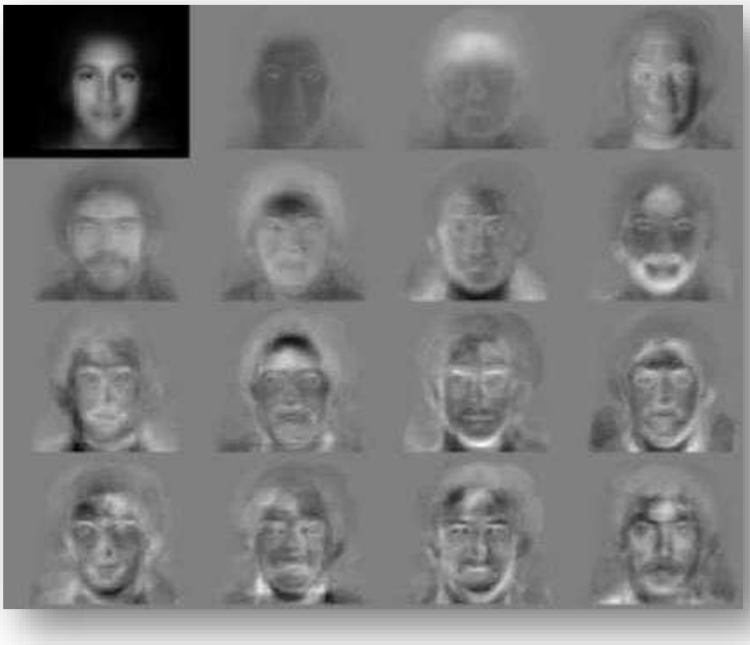


Figure 3.4 : Image moyenne et les 15 eigenfaces [2].

Nous allons maintenant projeter nos images de départ sur Ev. Une image vi est alors transformée en ses composantes eigenfaces par une simple opération de projection vectorielle:

$$\omega_k = e_k^T(v_i - Moy), k = 1 \dots M'$$

Les vecteurs ωk sont appelés poids et forment une matrice $\Omega^T = [\omega 1, \omega 2, \dots \omega M']$ qui décrit la contribution de chaque eigenface dans la représentation de l'image d'entrée. La matrice Ω^T est alors utilisée pour trouver quelle est, parmi un nombre pré-défini de classes, celle qui décrit le mieux une image d'entrée.

La méthode la plus simple pour déterminer quelle classe de visage fournit la meilleure description d'une image d'entrée est de trouver la classe de visage k qui minimise la distance euclidienne.

$$\varepsilon_k^2 = ||\Omega - \Omega_k||^2$$

où Ω_k est un vecteur qui décrit la k^e classe de visage.

Un visage appartient à une classe k quand le minimum εk est en dessous d'un certain seuil θ_ε.

Dans le cas contraire, le visage est classé comme étant inconnu et peut éventuellement être utilisé pour créer une nouvelle classe de visage. La création de la matrice de poids Ω_k est équivalent à la projection du visage original sur Ev. Puisque la distance ε entre l'image de visage et Ev est simplement le carré de la distance entre l'image d'entrée réajustée par rapport à la moyenne [2].

$$I_{moy} = V - Moy \quad et \quad I_{\substack{moy \\ f}} = \sum_{i=1}^{M} \omega_i e_i$$

, sa projection sur Ev est :

$$\varepsilon^2 = ||I_{moy} - I_{\substack{moy \\ f}}||^2$$

Il y a alors quatre possibilités pour une image d'entrée d'être reconnue ou non (Figure3.5).

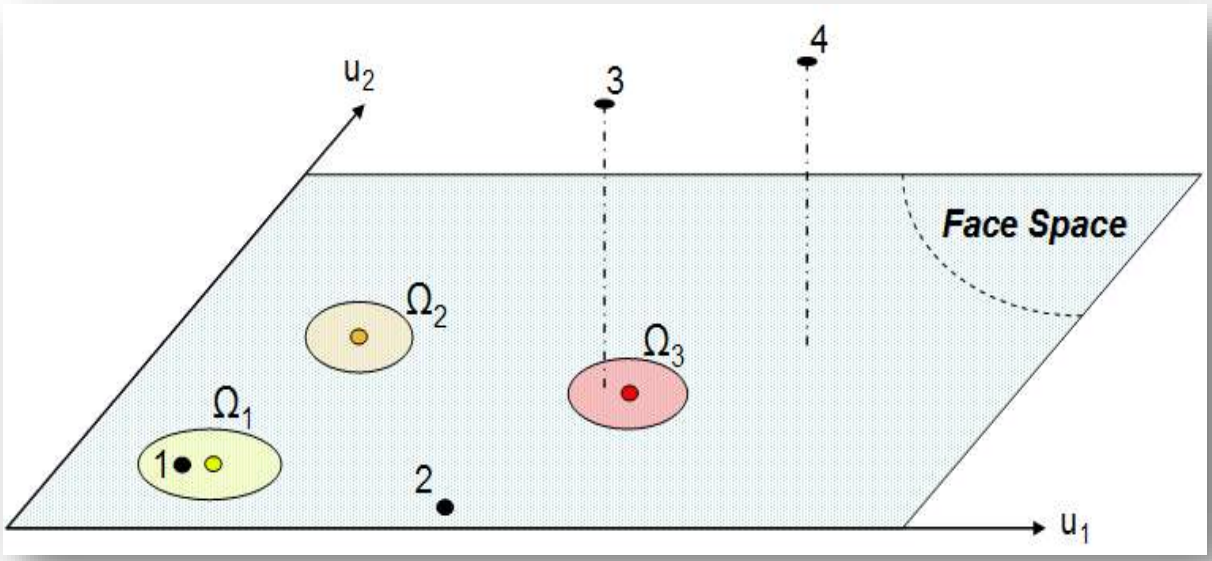


Figure 3.5 : Image résultat [2].

Une version simplifiée de Ev illustrant les quatre résultats de la projection d'une image sur Ev. Dans ce cas, il y a deux vecteurs propres (u1 et u2) et trois classes d'individus connus (Ω1, Ω 2, Ω 3) [2].

Dans le cas 1, un individu est reconnu et identifié. Dans le cas 2, un individu inconnu est présent. Les deux derniers cas (3 et 4) indiquent que l'image n'est pas une image de visage. Pour le cas 3, l'image est éloigné de Ev mais la projection est proche d'une classe connue, on parle alors de fausse acceptation. Ces remarques sont résumées dans le tableau table 3.1.

Table 3.1 : Les quatre possibilités qui apparaissent lors de la phase de reconnaissance [2].

	Espace des Visage (Ev)	**Classe de Visage**
Cas 1	proche	proche
Cas 2	proche	éloigné
Cas 3	éloigné	proche
Cas 4	éloigné	éloigné

3.4. Quelques exemples réels d'application :

La fonction première de l'analyse en composantes principales est une de réduction des données. On peut imaginer de nombreuses situations où les chercheurs sont aux prises avec un nombre très élevé de variables à considérer simultanément. Par exemple, la mise au point d'un instrument de mesure portant sur un construit théorique le moindrement complexe nécessite généralement une cueillette de données réparties sur une bonne centaine d'items. La recherche de Saintonge et Lachance (1995) illustre bien cette situation. Leur étude porte sur la validation d'une adaptation canadienne-française du SITA, un test de séparation individuation à l'adolescence développé initialement par Levine, Green et Millon (1986). Les auteurs ont administré le SITA comportant 103 items à un groupe de 424 jeunes âgé(e)s entre 12 et 22 ans. L'analyse en composantes principales a permis d'épurer l'instrument et de le réduire à une version comportant 52 items regroupés en 9 échelles. Saintonge et Lachance (1995) ont ensuite poursuivi leur analyse de cette version épurée du SITA en démontrant qu'il existait des différences significatives entre gars et filles (et entre adolescents plus âgés et plus jeunes) sur un certain nombre des neuf échelles identifiées par l'analyse en composantes principales.

Voici un deuxième exemple d'étude mettant à profit l'analyse en composantes principales. Carey, Faulstich, Gresham, Ruggiero et Enyart (1987) ont administré le « Children's Depression Inventory CDI » développé par Kovacs (1985) à un groupe de 153 jeunes patients hospitalisés pour soins psychiatriques de même qu'à un groupe témoin de 153 enfants provenant de la population générale. Le CDI comporte 27 items, mais l'ACP a permis de mettre en évidence deux ou trois composantes principales représentant de façon parcimonieuse une portion significative de la variance du test initial. La réduction des 27 items en un nombre limité de composantes a alors permis aux chercheurs de procéder à une analyse de fonctions discriminantes où il a été démontré que les composantes du CDI permettent de discriminer de façon adéquate les enfants appartenant au groupe clinique de ceux constituant le groupe témoin.

Terminons avec ce troisième exemple de recherche où l'on retrouve une application représentative de l'ACP. Ossenkopp et Mazmanian (1985) voulaient prédire la réponse physiologique au froid chez des rats soumis à une exposition de quatre heures en froid extrême. L'ensemble de leurs variables prévisionnelles était composé de 19 variables comportementales et physiologiques. Plutôt que d'utiliser ces 19 variables dans une analyse de régression multiple, ils ont d'abord procédé à une analyse en composantes principales qui leur a permis d'extraire 5 composantes représentant une proportion importante de la variance des mesures initiales. L'analyse de régression multiple a ensuite été menée en utilisant comme variables prévisionnelles les scores obtenus sur les cinq composantes extraites.

Les trois exemples que nous venons de citer ont en commun d'utiliser l'analyse en composantes principales dans une perspective de réduction des données et dans les trois cas on peut observer que les données ainsi réduites (les composantes) sont soumises à des analyses ultérieures. Ainsi, Saintonge et Lachance (1995) ont utilisé les composantes extraites en ta nt que variables dépendantes dans des analyses de variance et de tests t. Carey et al. (1987) quant à eux ont procédé à une analyse de fonctions discriminantes en se servant des composantes extraites pour définir leurs fonctions. Enfin, Ossenkopp et Mazmanian (1985) ont créé leur équation de régression multiple en utilisant comme variables prévisionnelles les scores obt nus préalablement par l'analyse en composantes principales.

Les trois exemples précédents illustrent parfaitement bien la définition de l'ACP telle qu'on la retrouve dans le « Dictionary of statistics and methodology » .

3.5. Conclusion :

En résumé, l'algorithme PCA est une méthode globale utilisant en premier lieu les niveaux de gris des pixels d'une image. Sa simplicité à mettre en œuvre contraste avec une forte sensibilité aux changements d'éclairement, de pose et d'expression faciale. Le principe selon lequel on peut construire un sous-espace vectoriel en ne retenant que les « meilleurs »vecteurs propres, tout en conservant beaucoup d'information utile, fait du PCA un algorithme efficace et couramment utilisé en réduction de dimensionnalité. Enfin, l'étude théorique de l'algorithme PCA est très pédagogique et permet d'acquérir de solides bases pour la reconnaissance 2D du visage. C'est un algorithme incontournable!

Implémentation et Résultat

4.1. Introduction :

Dans cette partie on propose une application pour la reconnaissance de visage, utilisant l'algorithme de l'analyse des composantes principale qui a été bien détaillé dans le chapitre précédant. Dans notre application on utilise le langage Matlab.

4.2. Qu'est-ce que c'est Matlab :

Matlab est un logiciel commercial développé par Math works Inc ,est un outil très efficace qui est largement utilisé pour le calcul numérique et la visualisation graphique[17],développé à l'origine pour le calcul matriciel (le nom Matlab est dérivée de cette représentation «matrix laboratory». il contient des bibliothèques(toolbox) qui répondent à des besoins spécifiques :analyse numérique, traitement du signal, traitement d'image, etc.

4.3. Pourquoi utiliser Matlab :

Matlab est déjà en usage dans de nombreux établissements.il est utilisé dans la recherche scientifique dans le milieu universitaire et industriel.les solutions prototype sont généralement obtenues plus rapidement dans Matlab que dans d'autre langages de programmation. Matlab est rapide, car les routines de base dans Matlab sont affinées pour les différentes architectures informatiques.

4.4. Base de données :

Nos expériences ont été exécutées sur des images frontales de visage de la base de données ORL [18]. ORL94 « ormerly 'The ORL Database of Faces' » est une base de données enregistrée spécifiquement pour évaluer les exécutions des approches biométriques à la vérification d'identité. Elle contient 10 images par visage de 40 personnes. Les images de format pgm 92x112 pixels organisé dans 40 dossiers nommé sx, chaque une à10 visage nommé y.pgm ou y indique le numéro d'image.

Il n'est pas suffisant d'utiliser la même base de données pour pouvoir honnêtement comparer des résultats. Il est nécessaire également de définir un protocole de test. Dans notre travail la base de données est scindée en deux ensembles : ensemble d'apprentissage et l'ensemble de test. L'ensemble d'apprentissage contient 2 images de chaque personne (80 images), utilisé comme ensemble de référence. Il sert d'ensemble de base, maintenant ainsi l'information concernant les personnes connues du système et permet de fixer les paramètres du système de reconnaissance de visages. l'ensemble de test contient les autres images des personnes (320 images), permet de tester le système en lui présentant des images de personnes lui étant totalement inconnues.

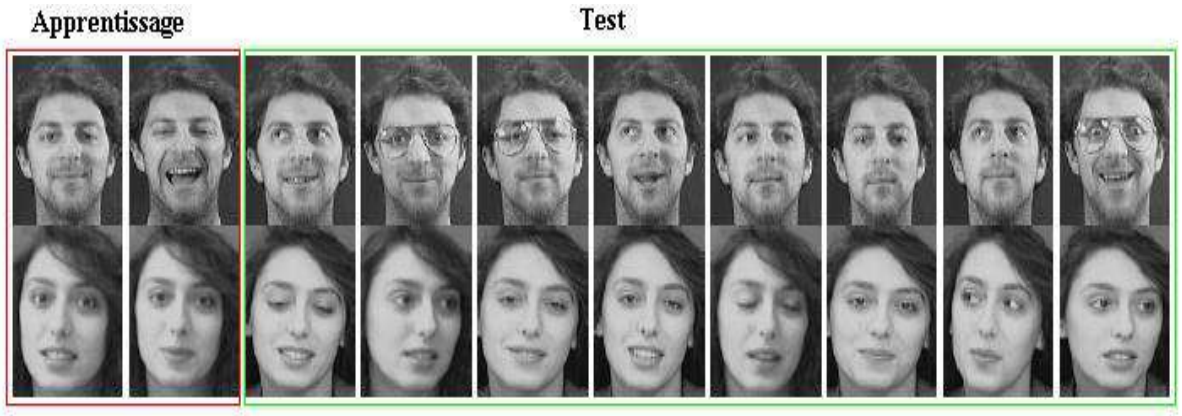


Figure 4.1 : Exemples d'images de deux personnes provenant de la base de données du laboratoire AT & T de l'université de cambridge.

4.5. Phase d'enrôlement :

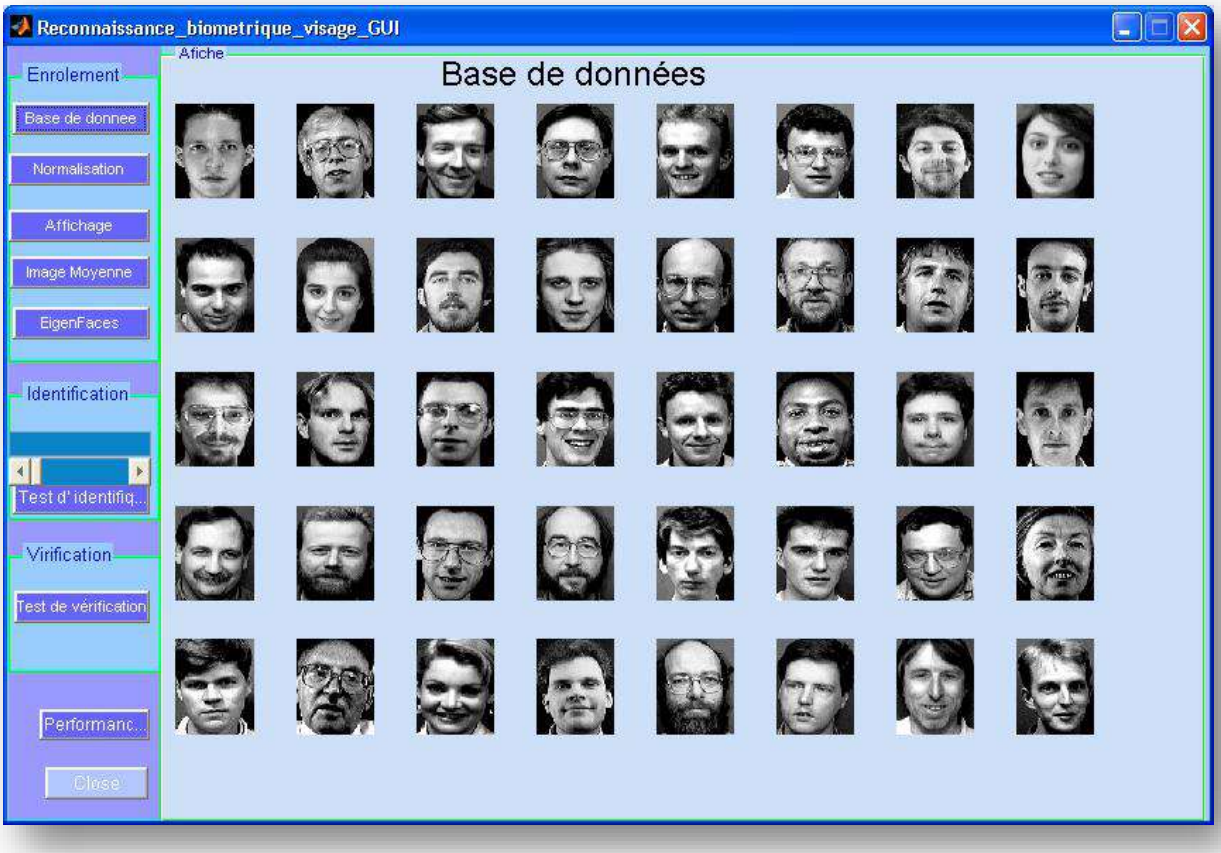


Figure4.2 : la base de données.

Pour l'apprentissage on utilise 2 images pour chaque personnes de la base, chaque image traitée comme un vecteur de 10304 (M=92*112) valeurs, puis rassemblé les 80 images dans une unique matrice, nous obtenons une matrice d'images V (10304*80), où chaque colonne représente une image.

On calcule ensuite l'image moyenne Moy de toutes les images collectées. Cette image peut être vu comme le centre de gravité du jeu d'images :

$$Moy = \frac{1}{M}\sum_{i=1}^{M} v_i$$

On ajuste ensuite les données par rapport à la moyenne. L'image moyenne est alors soustraite de chaque image avec la formule suivante :

$$I_{\substack{moy \\ i}} = v_i - Moy \quad , i = 1 \dots M$$

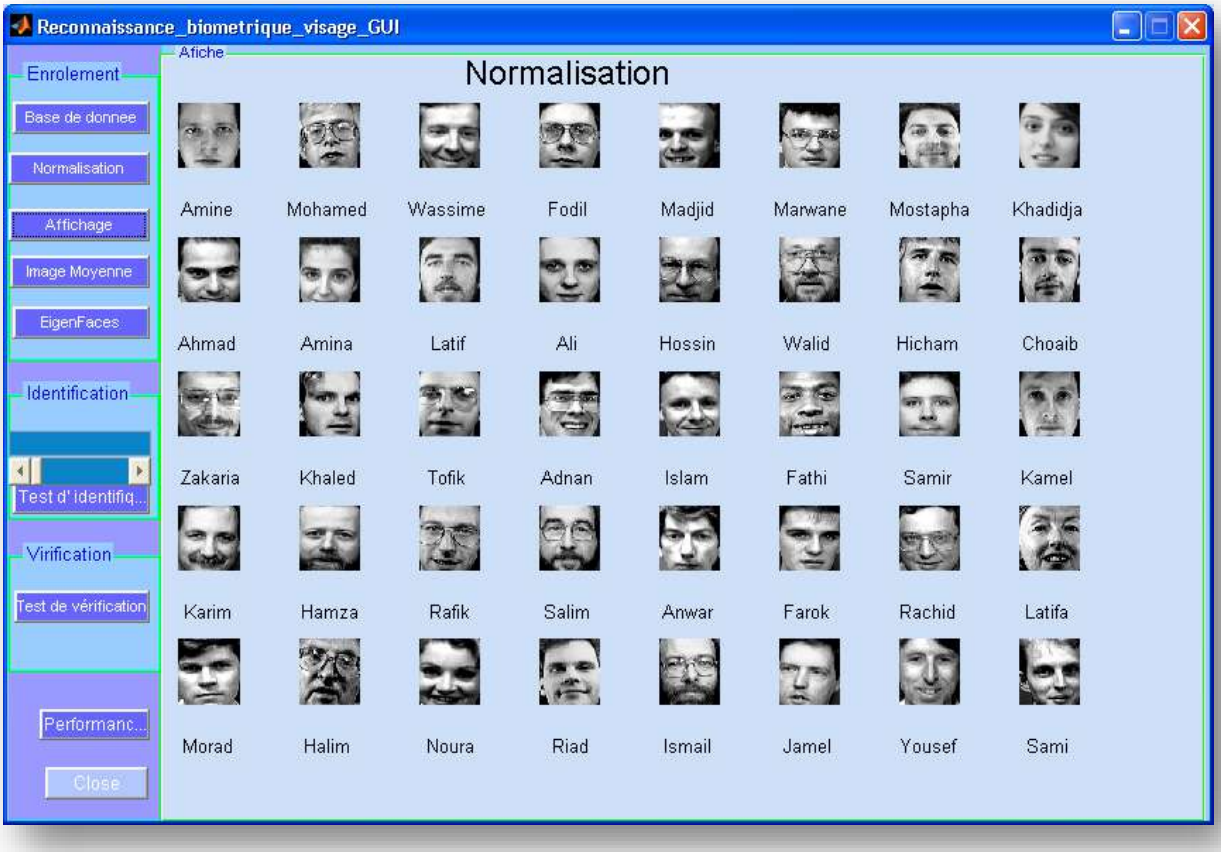


Figure4.3 : Normalisation de la base de donnée ORL.

On réduit la talle des images pour centré l'extraction d'information (figure4.3) et Pour la simplification on donne un nom, prénom, matricule et date de naissance à chaque personne (figure4.4).

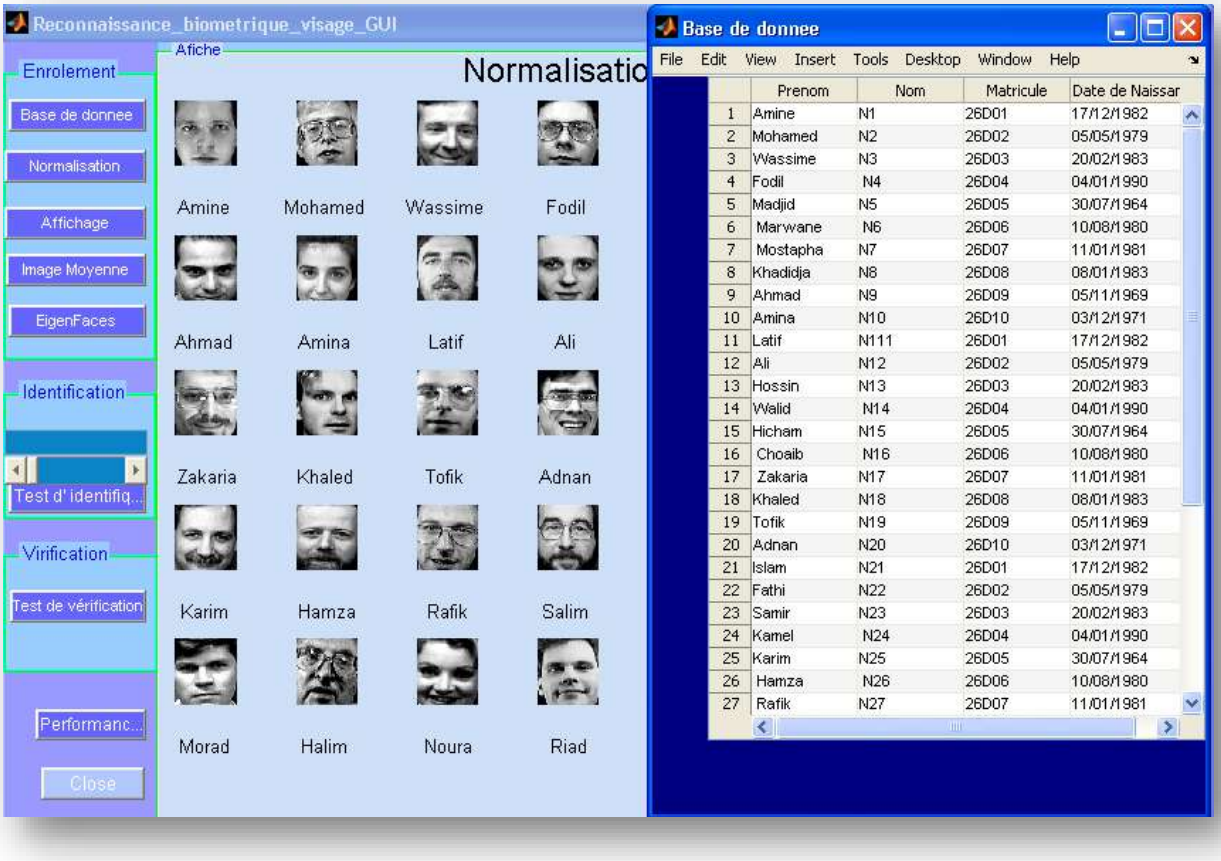


Figure4.4 : Affichage de la base de donnée ORL.

La prochaine étape consiste à calculer les vecteurs propres et les valeurs propres et affiche l'image moyenne et les 80eigenface.

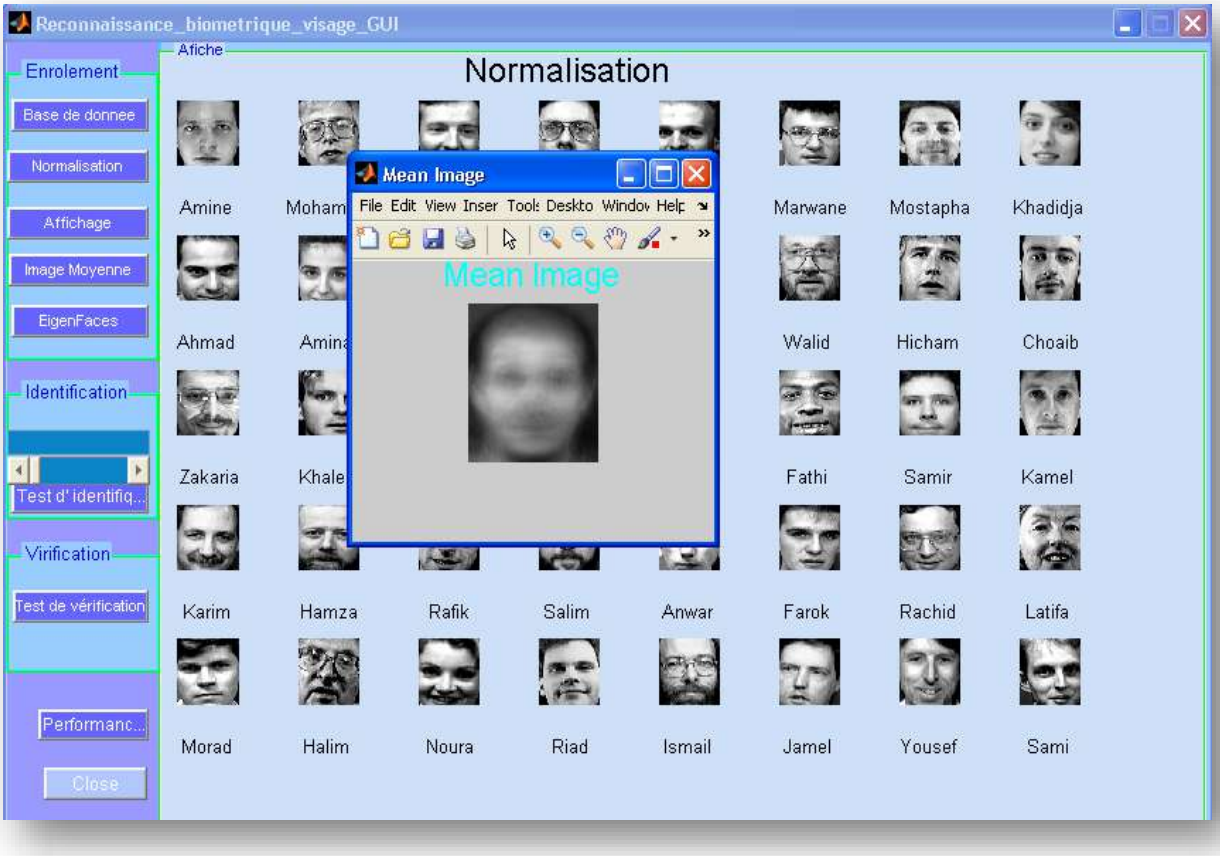


Figure4.5 : l'image moyenne et les images normaliseé.

4.6. Phase d'Identification :

Un système d'identification reconnaît un individu par une recherche sur l'ensemble de la base des modèles. Il effectue une comparaison un à plusieurs (on note généralement 1:80) pour établir l'identité de l'individu.aprée le calcule de la différence (distance) entre le poids de visage chosée et les 80 poids de la base de donné, on choisie le visage d'individu de plus petite distance trouvée. Le système doit établir l'identité d'un individu ou inférer que le sujet n'est pas enregistré dans la base de données du système

Le système choisi l'image la plus proche à l'image d'entrée et affiché puis le calcule de la probabilité, si la probabilité supérieur au seuil choisie donc le résultat de système est : « OK la personne acceptée » et si la probabilité est inferieur donc le résultat de système est : «NO la personne rejetée » (figure 4.6).

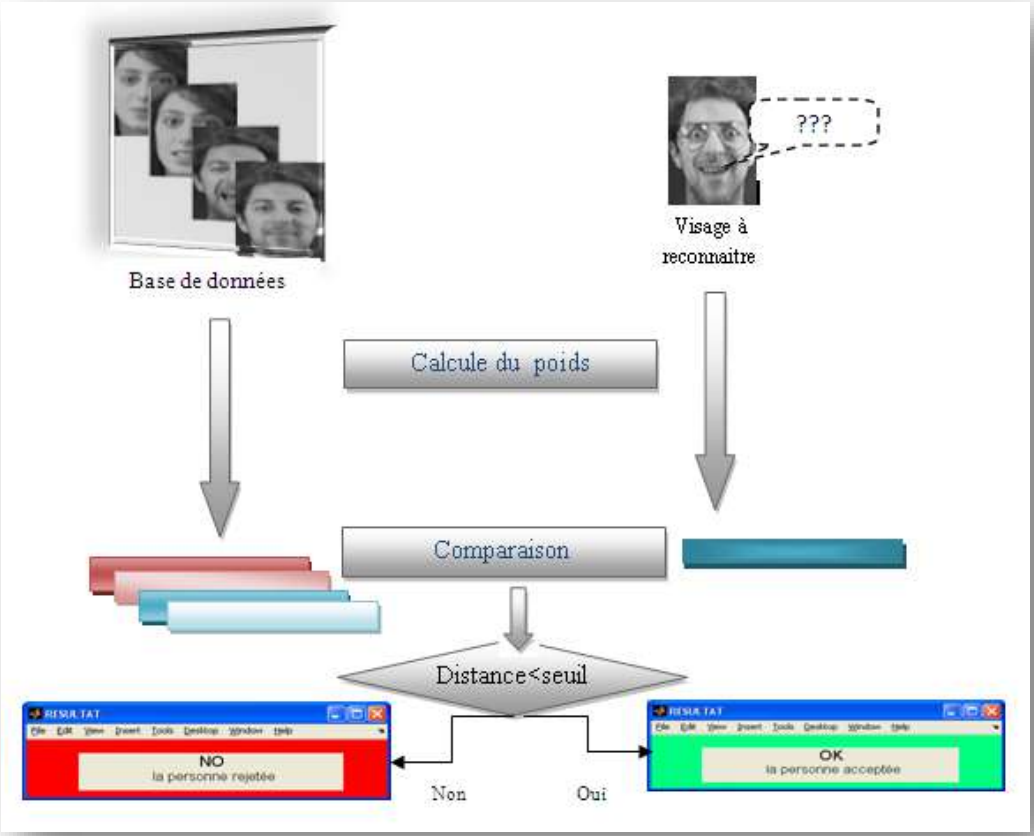


Figure 4.6 : la procédure d'identification.

4.7. Test d'identification :

Avant de faire un test d'identification on choisir un seuil égal à 0.16, et ouvrir une visage à reconnaitre, et les figure suivant montre le procédure d'identification.

① **Test 1 :**

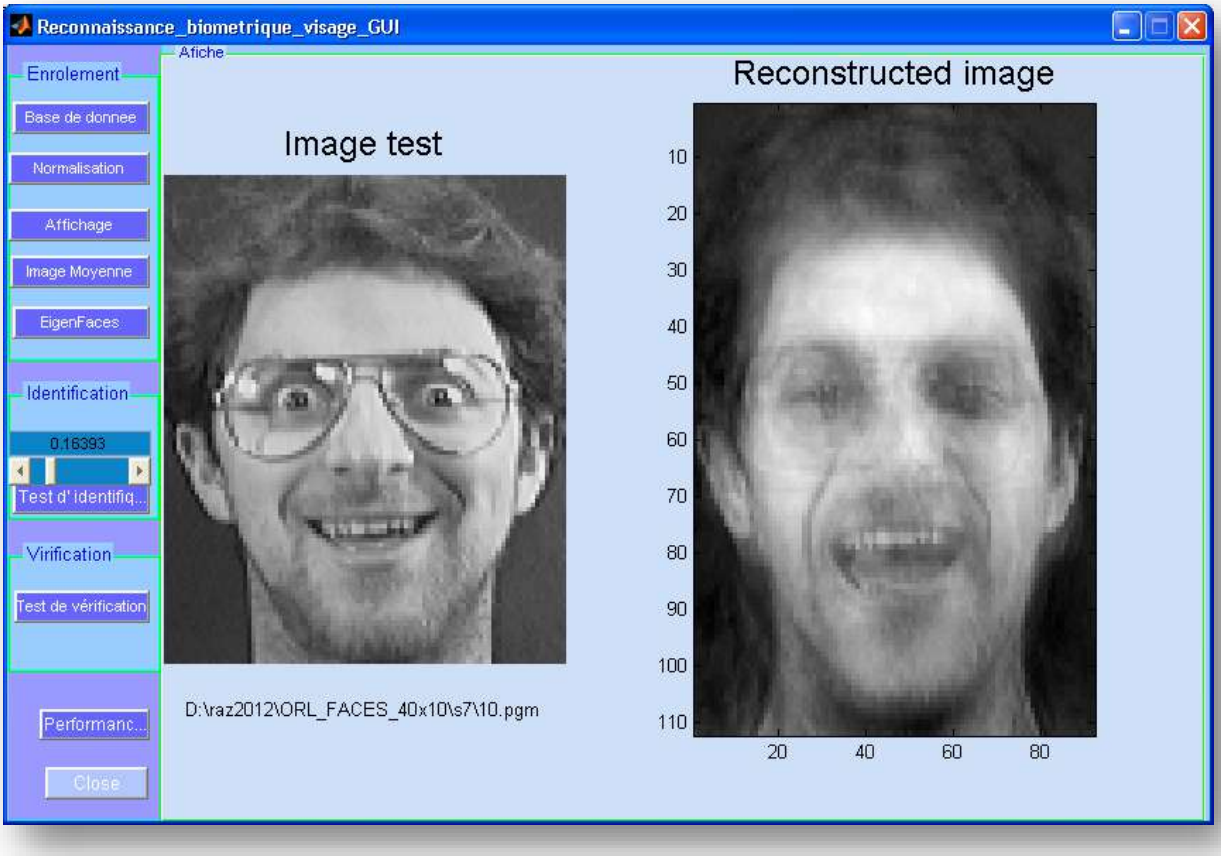


Figure 4.7 :l'image test et l'image construite par le système.

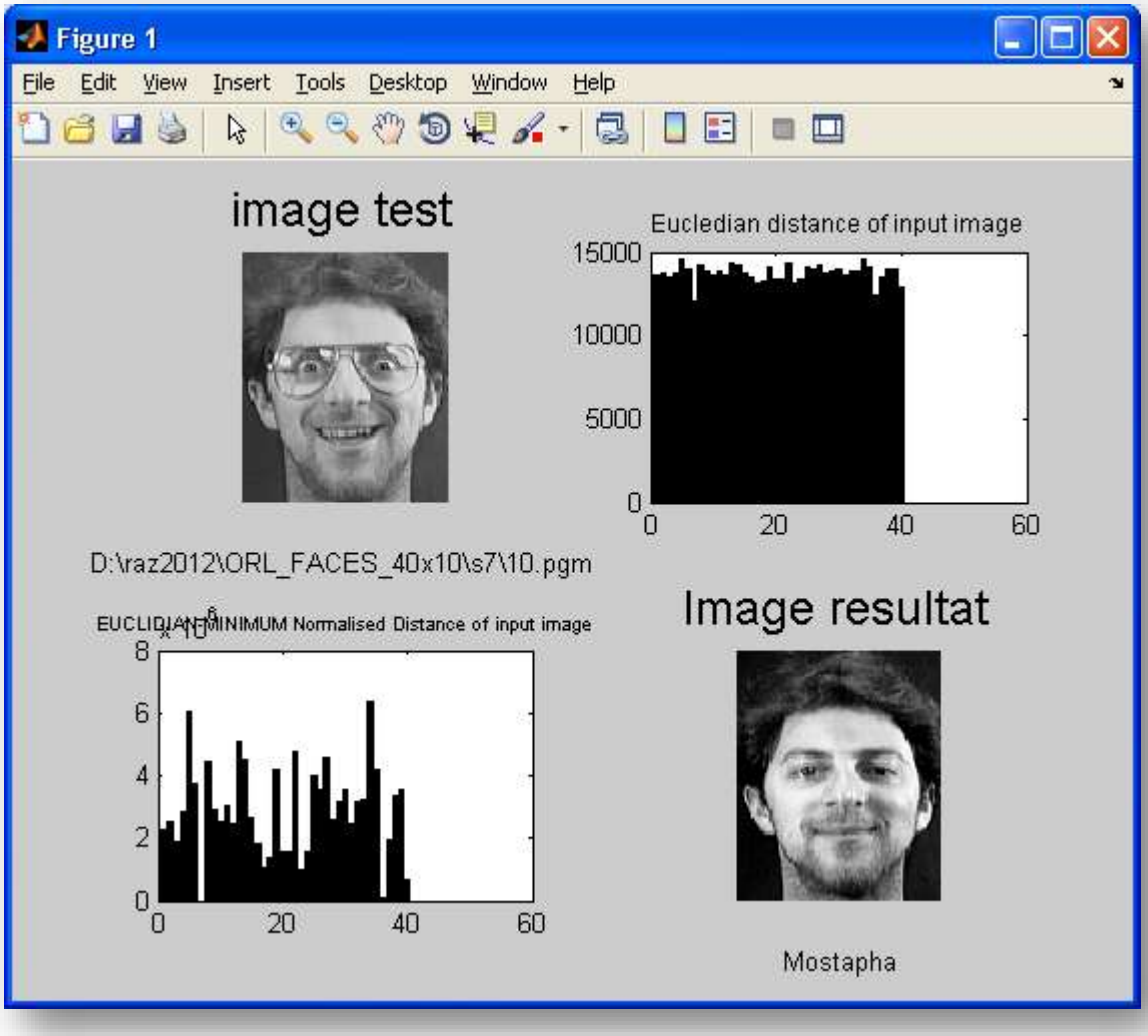


Figure 4.8 : personne identifie.

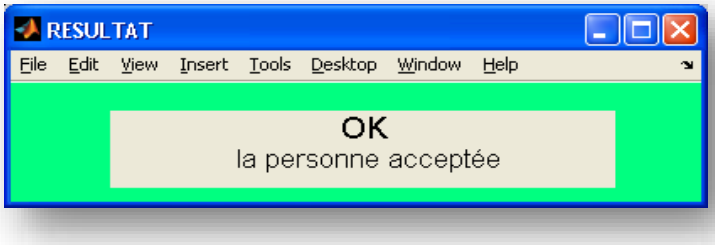


Figure4.9 : Résultat d'identification de système.

① **Test 2 :**

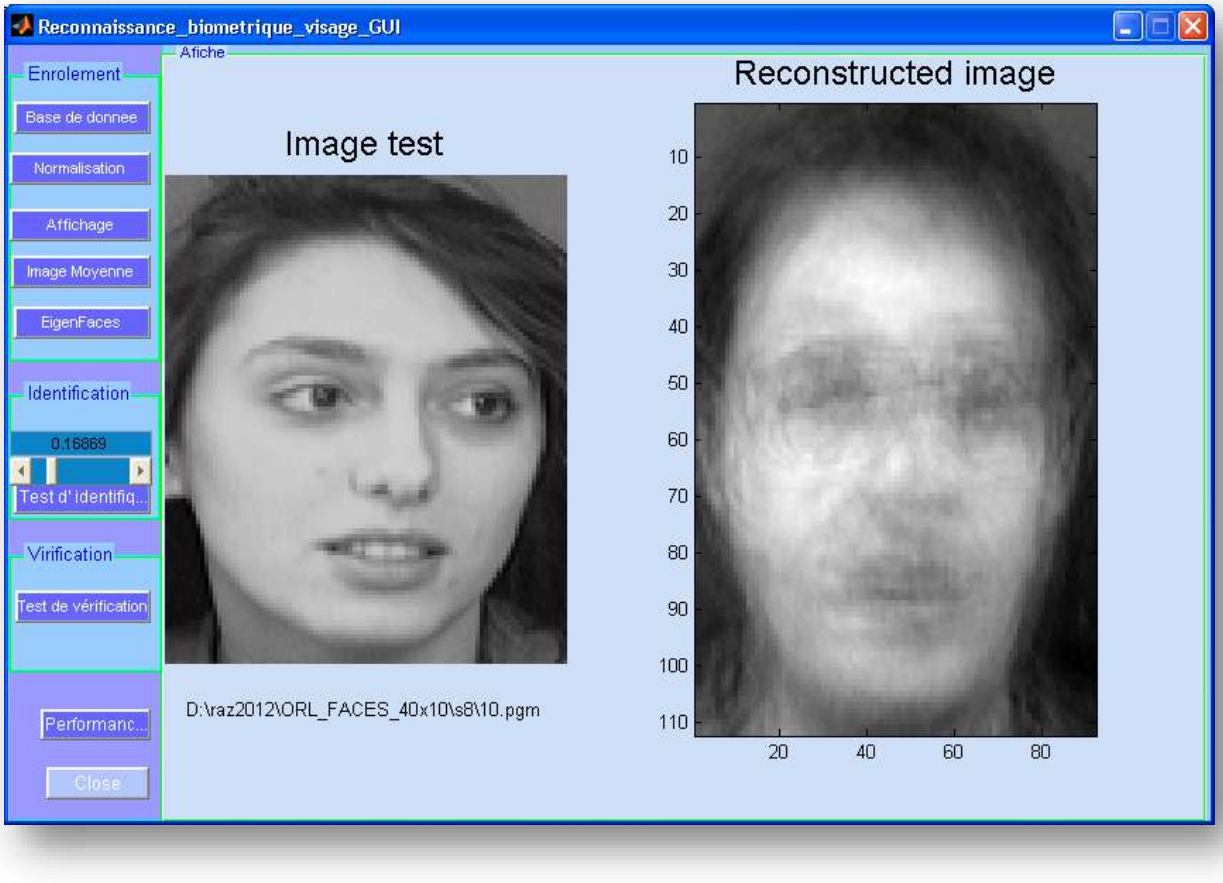


Figure 4.10 :l'image test et l'image construite par le système.

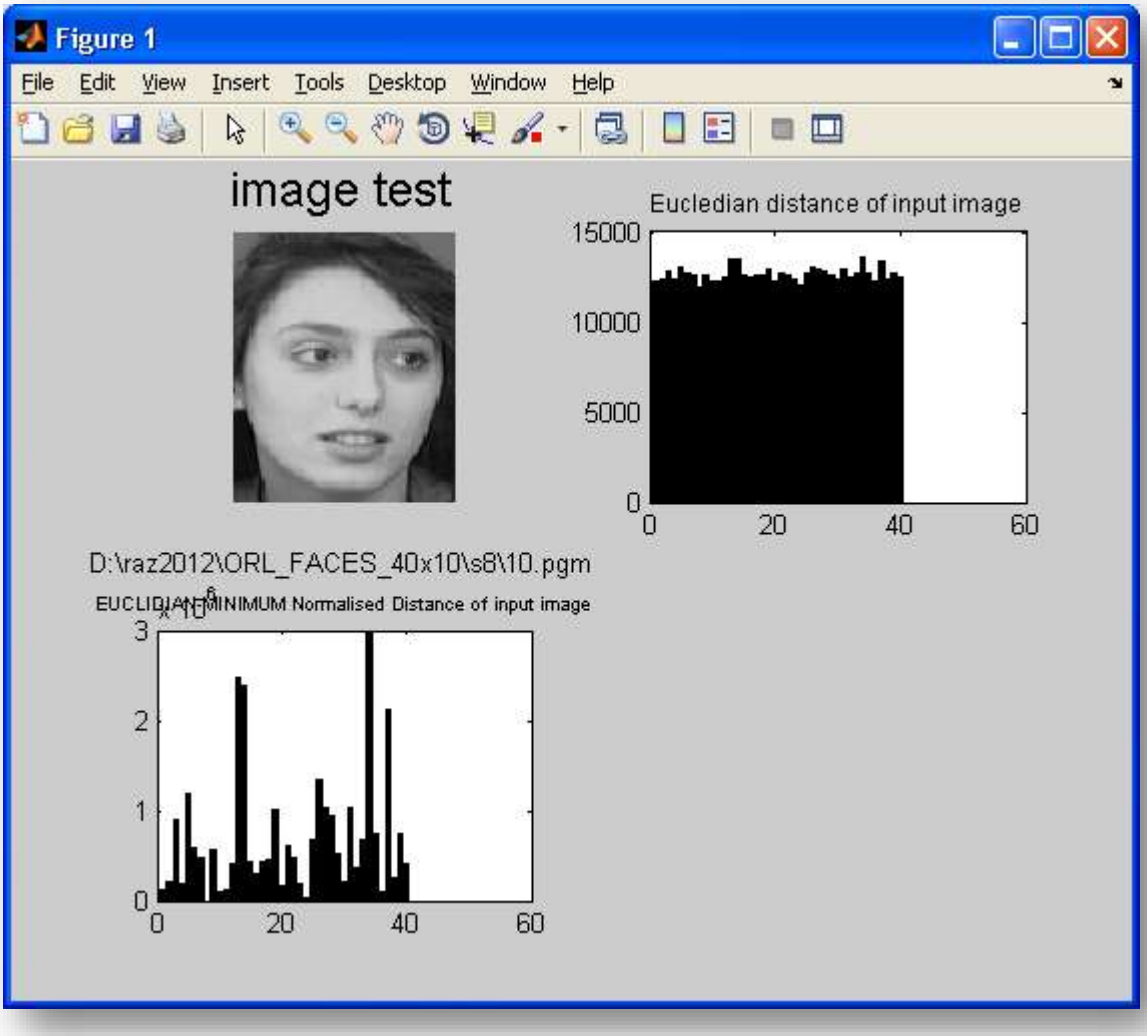


Figure 4.11 : personne non identifie.



Figure4.12: Résultat d'identification rejetée FR avec un seul égal à 0.16.

4.8. Phase de Vérification :

Un système de vérification vérifie l'identité d'une personne en comparant la signature biométrique extraite avec son propre modèle biométrique préenregistré dans le système. Il effectue une comparaison un à un (on note généralement 1:1) pour déterminer si l'identité revendiquée par l'individu est vraie. Un système d'authentification accepte ou rejette la demande d'un utilisateur : suis-je ce que je prétends être ?

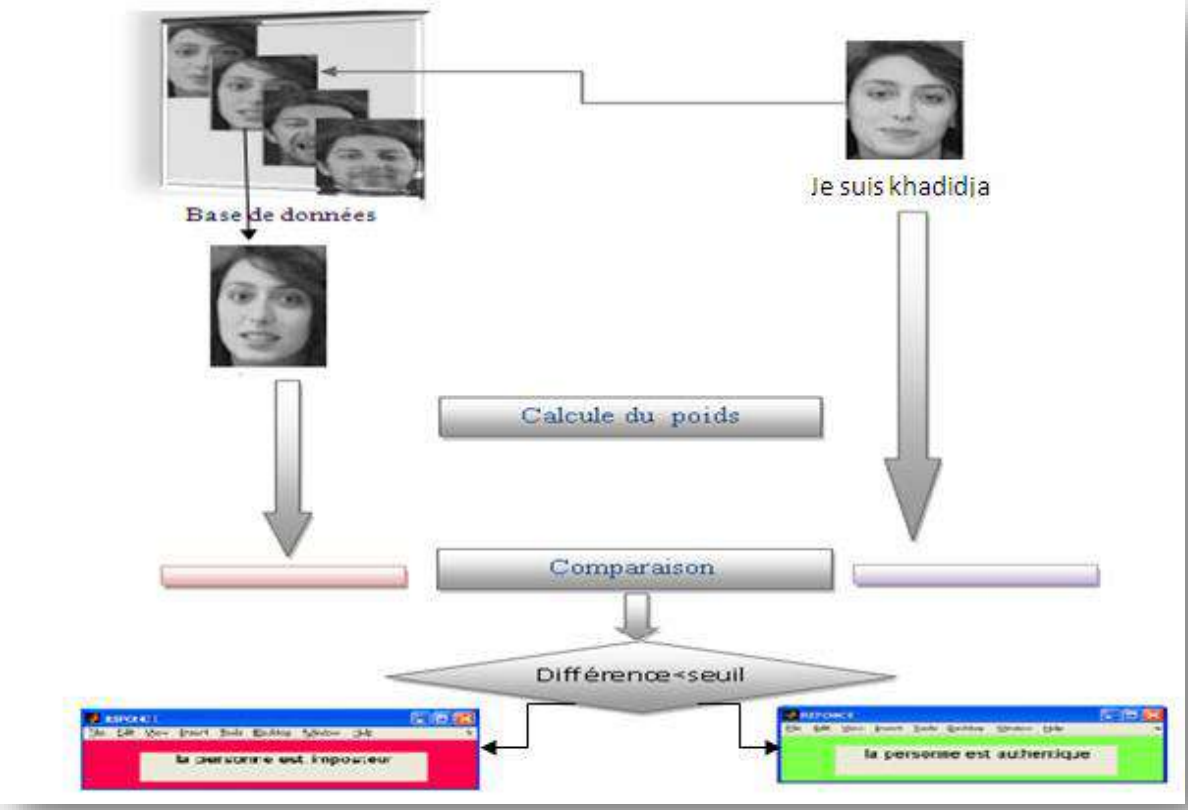


Figure 4.13 : la procédure de vérification.

4.9. Test de vérification :

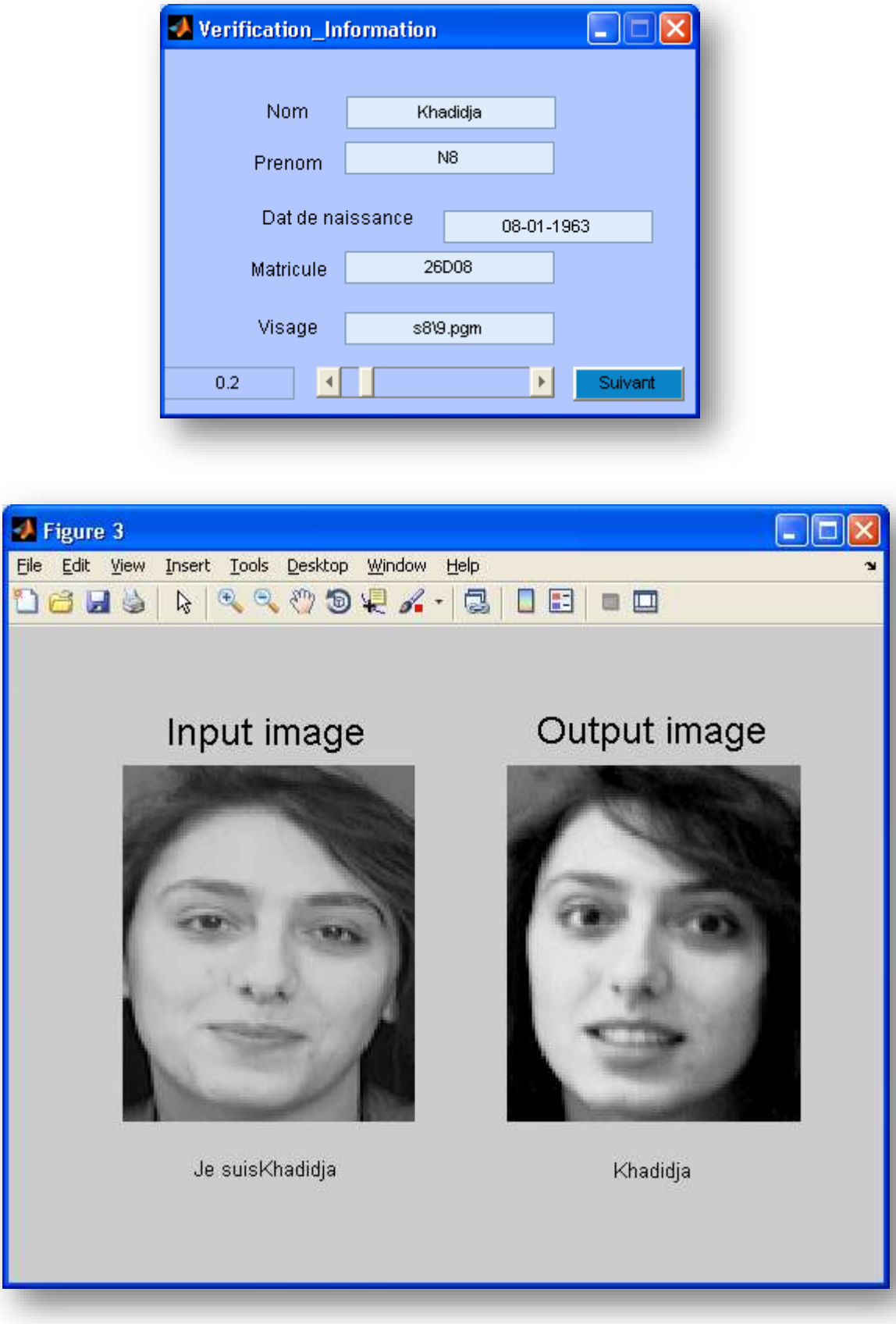


Figure 4.14 : Comparaison entre le visage d'entré et le visage de la base de donné.

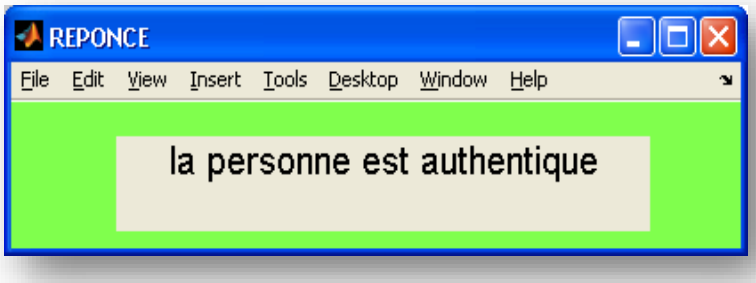
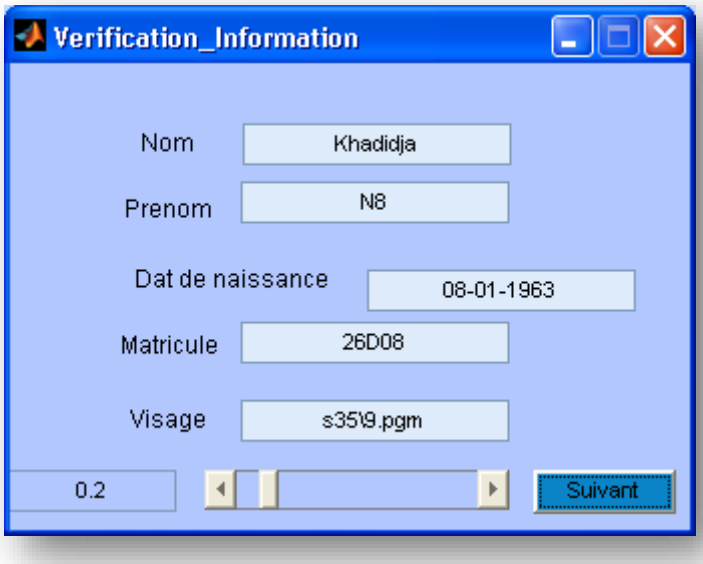


Figure 4.15: Résultat authentique du système de vérification.



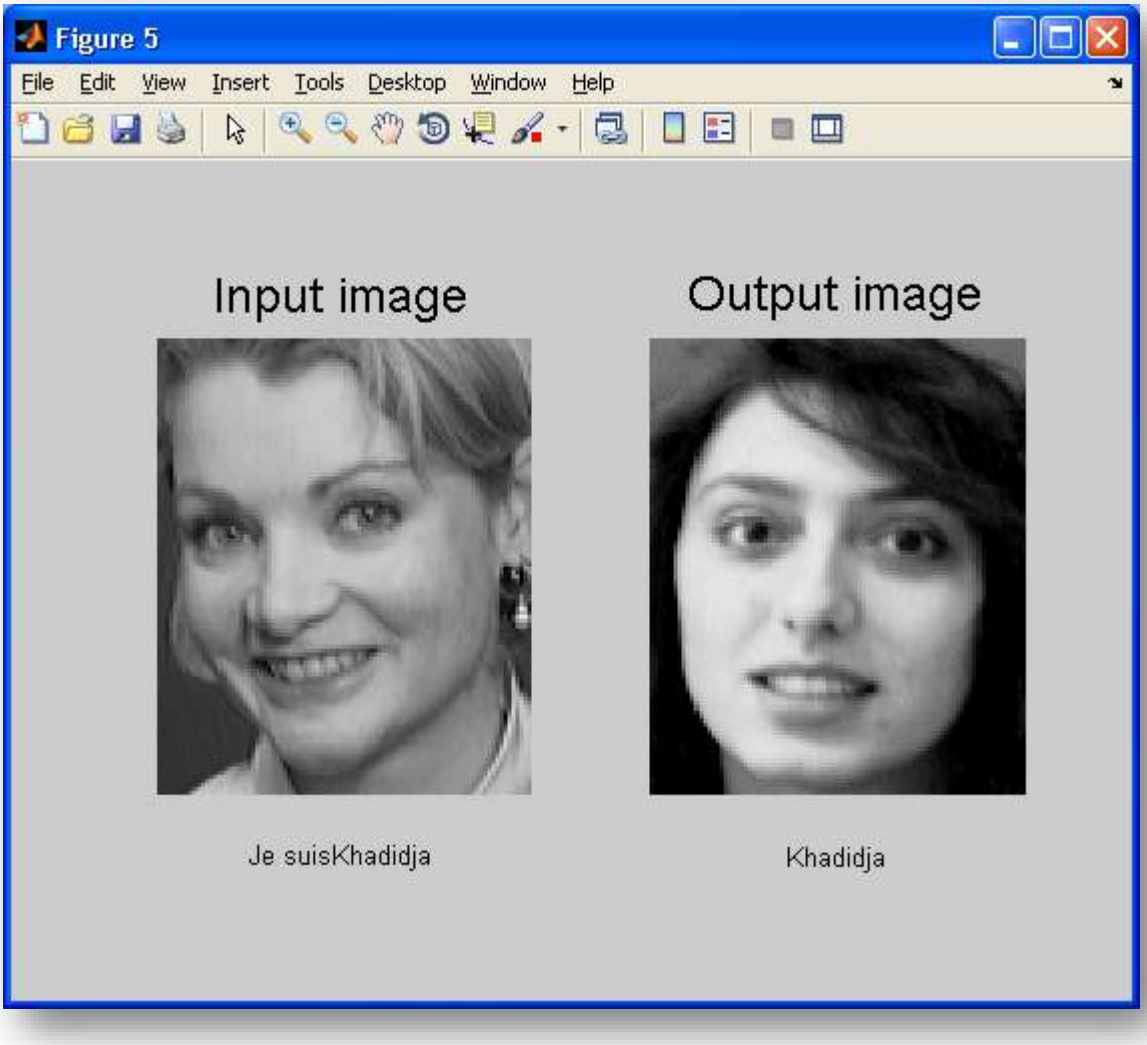


Figure 4.16 : Comparaison entre le visage d'entré et le visage de la base de donné.

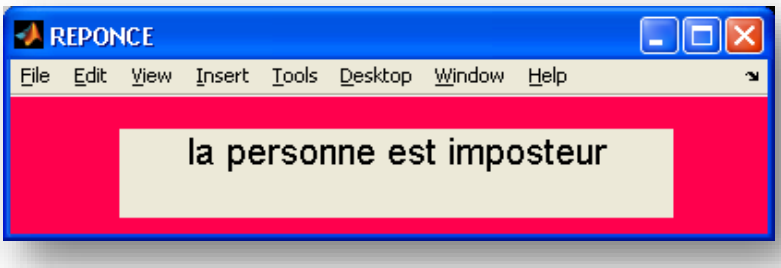


Figure4.17: Résultat du système de vérification.

4.10. Performance du système:

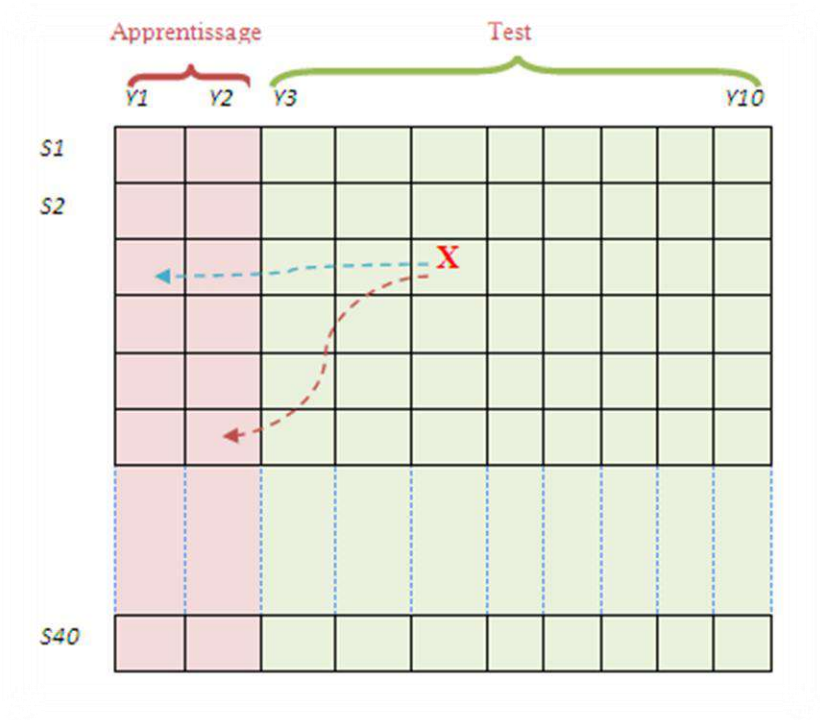
Pour notre application on utilise 40 personnes nommé s1…s40 et 10 visages nommé y1…y10 pour chaque personne. 80 visages pour l'apprentissage et 320 visages pour le test .pour reconnaitre les performances de ce système de reconnaissance (trace le courbe ROC) on va faire 25600 test de vérification.

Par exemple l'image X doit être testé avec tous les 80 images de la base de données, si le test avec l'image de la même colonne d'image X donc personne accepté (FA=FA+1) sinon le personne rejeté (FR=FR+1), dans le cas idéal on a le nombre des personnes accepté authentiques FA= [(10-2)*2*40]=640 et le nombre des personnes rejeté imposteurs FR= [(80-2)*(10-2)*40]=24960, le taux de fausse acceptation FAR et le taux de fausse rejeté FRR sont calculé par les formules suivant.

$$FAR = {}^{nb\ de\ FA}/_{nb\ des\ imposteurs}$$

$$FRR = {}^{nb\ de\ FR}/_{nb\ des\ authentiques}$$

Table4.1 : Matrice de la base donnée.



4.10.1. Expérience 1 :

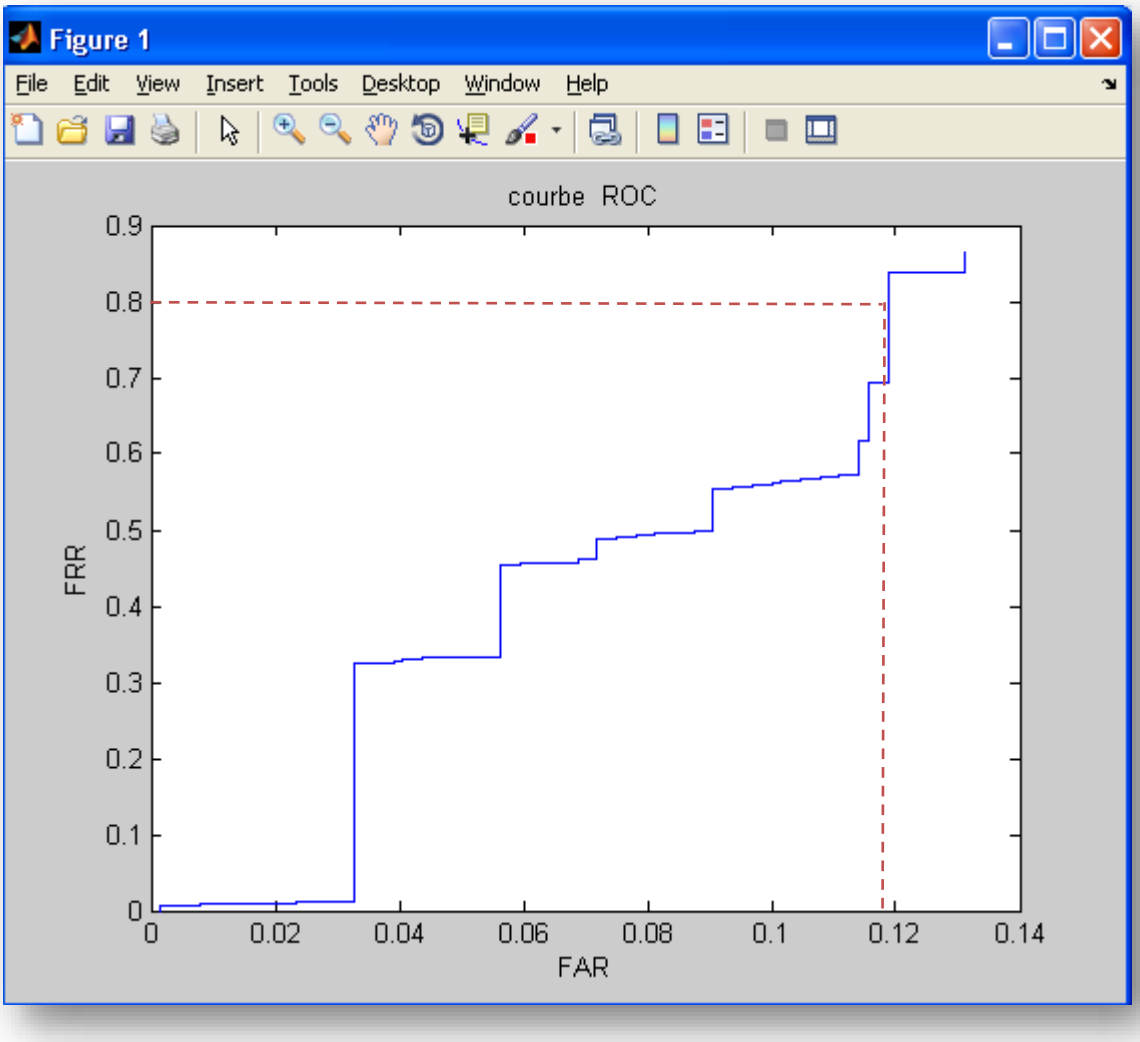


Figure 4.18 : le courbe ROC : seuil=0.29.

La figure 4.18 définie la courbes ROC avec une seuil égale à 0.29,on remarque que si FAR=0.118 FRR=0.8 donc FRR>FAR donc le nombre des personnes rejetés supérieur que le nombres des personnes acceptés donc avec la seuil 0.29 on a un système de grand sécurité.

4.10.2. Experience2 :

h

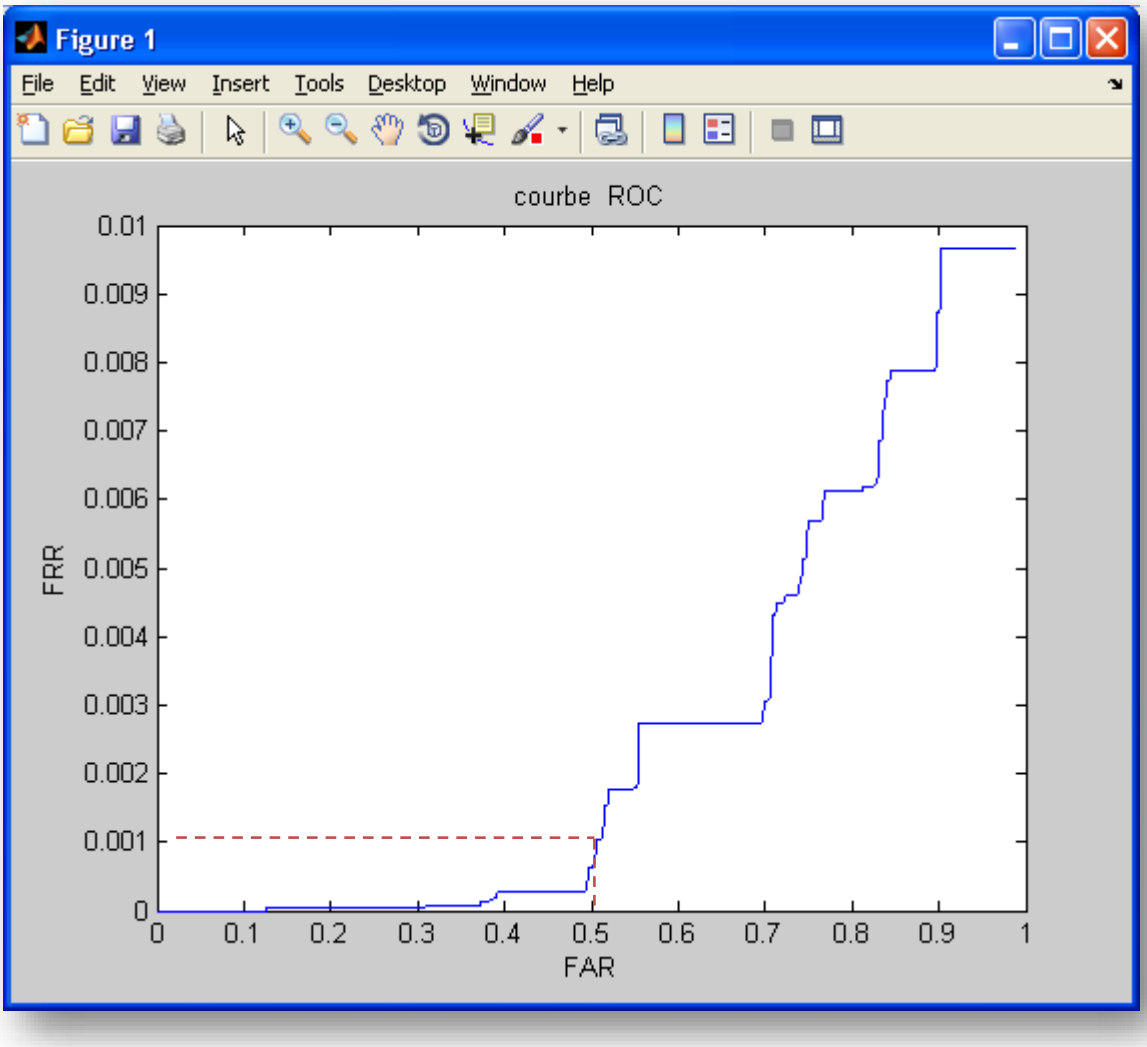


Figure 4.19 : le courbe ROC2 : seuil=0.08.

La figure 4.19 définie la courbes ROC avec une seuil égale à 0.08,On remarque que si FAR=0.5 FRR=0.002 donc FRR<FAR donc le nombre des personnes acceptés supérieur que le nombres des personnes rejetés donc avec la seuil 0.08 on a un système de faible sécurité.

4.10.3. Expérience 3 :

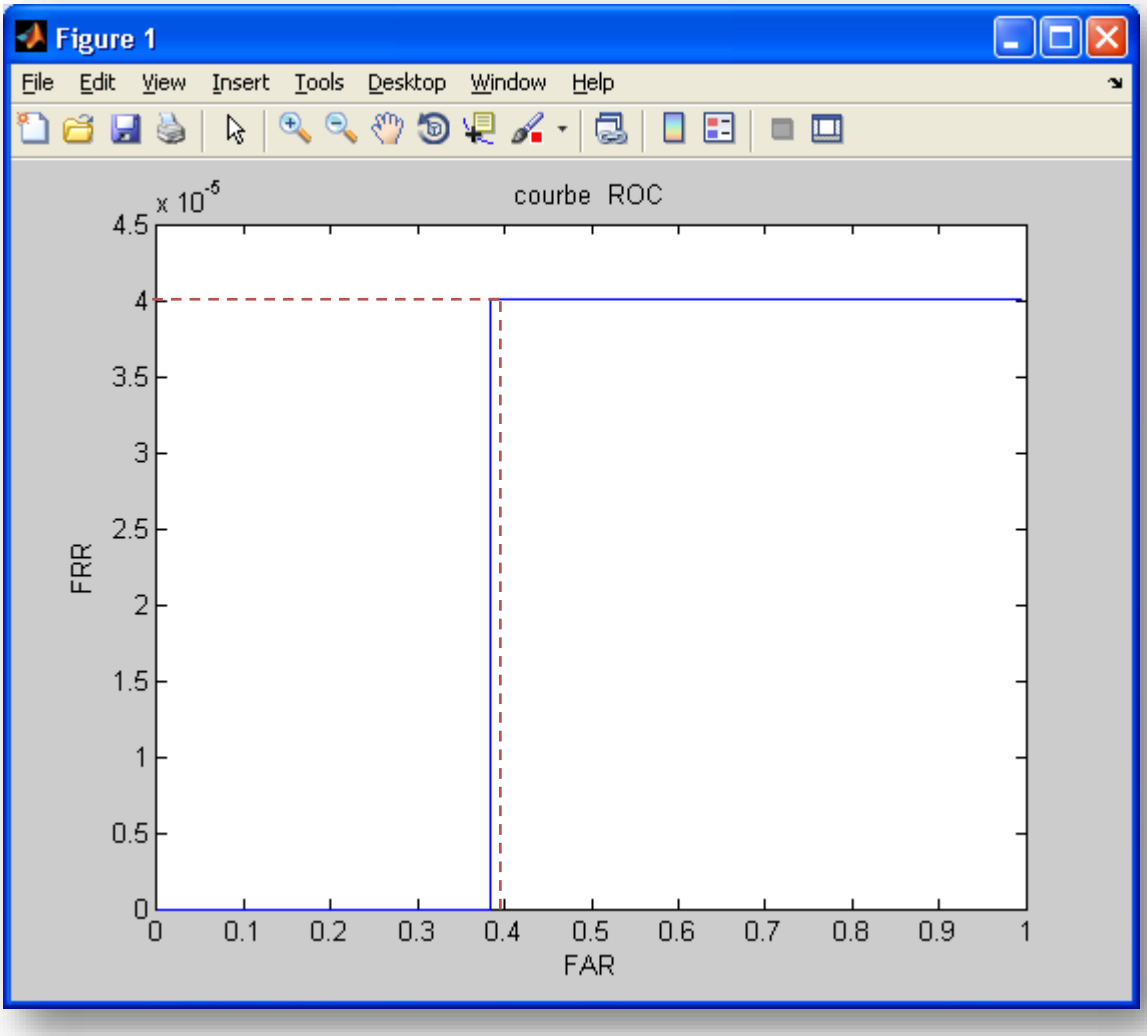


Figure 4.20 : le courbe ROC : Seuil=0.03.

La figure 4.20 définie la courbes ROC avec une seuil égale à 0.03,On remarque que si FAR=0.4 FRR=4*10^-5 donc FRR<<FAR donc le nombre des personnes acceptés plus grand que le nombres des personnes rejetés donc avec la seuil 0.08 on a un système de très faible sécurité.

4.11. Conclusion:

Nous avons implanté l'algorithme ACP à la biométrie de visage quant utilise la base de donnée ORL et voir des exemples sur la phase d'identification et de vérification, et que le seuil influencer largement sur le résultat de la reconnaissance.

Conclusion Générale

La sécurité n'est pas appliquée en se concentrant sur un seul paramètre. Au lieu de résoudre un problème à une dimension, un environnement sécurisé requiert de multiples dimensions de points de contrôle critiques. L'authentification sécurisée est assurée par plusieurs paramètres. Un paramètre est un jeton de sécurité d'un individu possède de façon unique, tel qu'une clé physique ou une carte à puce. Un autre paramètre est un élément unique d'une personne sait, tel qu'un code PIN. Un paramètre supplémentaire est les caractéristiques biologiques uniques d'un individu, par exemple l'ADN ou bien un code d'iris.

La technologie biométrique pourrait avoir un impact positif considérable dans la société, si elle est correctement utilisée pour augmenter la robustesse des systèmes de sécurité à travers le monde. Cela aiderait à réduire les niveaux croissants de fraude, la criminalité et le terrorisme. Toutefois, la biométrie a le potentiel de nuire à la société en permettant aux gouvernements une quantité massive d'informations personnelles concernant les particularités. Pour intégrer un système d'identification biométriques complet sera un long processus, mais la technologie a le potentiel de changer la façon dont le monde fonctionne, aucun mot de passe et plus des cartes à puce à utiliser, simplement en utilisant votre corps comme votre clé. Toutefois, la biométrie a été utilement appliquée pour les questions de moindre importance, par exemple « time monitoring systems and industry authentication systems ». Comme les progrès de la technologie augmentent, il est assuré que la biométrie peut être effectivement appliquée à des systèmes importants.

Il ne fait aucun doute que la biométrie est la prochaine étape de la technologie de sécurité omniprésents dans notre plus en plus paranoïaque, la société autoritaire. Cependant, il reste encore beaucoup à faire: les clients sont effrayés par l'échec à s'inscrire élevé et les taux de non match ainsi que les incompatibilités. En outre, la sécurité du système dans son ensemble a besoin de plus de soins à être enlevé. Les améliorations futures de la technologie d'acquisition et d'algorithmes, ainsi que la disponibilité de normes industrielle va certainement assurer un avenir prometteur pour la biométrie. Sera-ce la fin de mot de passe classique ou d'un jeton à base de

systèmes? Certainement pas la biométrie n'est pas la solution idéale soit, c'est juste un bon compromis entre la sécurité et la facilité d'utilisation.

De nombreuses recherches se poursuivent dans le domaine de la biométrie. La mise à jour dynamique des modèles de reconnaissance est l'un de ces axes de recherche.

Autre axe, implémentation par autre méthodes de reconnaissance et voire les résultats, la multi modalité, qui consiste à combiner des reconnaissais (voix et visages par exemple) pour améliorer la fiabilité globale d'un système et la cryptographie biométrique.