Université Mohamed Khider de Biskra
Faculté des Sciences et de la Technologie
Département de Génie Electrique

MÉMOIRE DE MASTER

Sciences et Technologies
Filière: Télécommunications
Spécialité: Réseaux et Télécommunications

Réf. : ……..

Présenté et soutenu par :
Nom et Prénoms de l'étudiant

Le : lundi 8 juillet 2019

La couleur et la méthode proposé MS à l'authentification de visage

---

Jury :

M.	Ouamane Abdelmalik	MCA	Université de Biskra	Président
Mme.	Ouarhlent Saloua	MAA	Université de Biskra	Examinateur
Mlle.	Fedais Meraim	MCB	Université de Biskra	Rapporteur

Année universitaire : 2018 – 2019

Université Mohamed Khider de Biskra
Faculté des Sciences et de la Technologie
Département de Génie Electrique

MÉMOIRE DE MASTER

Sciences et Technologies
Filière: Télécommunications
Spécialité: Réseaux et Télécommunications

Présenté et soutenu par :
Mazouzi Hasna

La couleur et la méthode proposé MS à l'authentification de visage

Avis favorable de l'encadreur :

Fedias Meriem *signature*

Avis favorable du Président du Jury

Ouamane Abdeelmalk *Signature*

Cachet et signature

Résumé

La reconnaissance de visages est une technologie biométrique en vogue, elle est très utilisée dans les applications de contrôle d'accès. Dans la littérature, on trouve plusieurs méthodes globales, locales et hybrides de reconnaissance de visage. Le but de ce travail est d'effectuer une vérification de validation faciale basée sur la méthode MS pour augmenter le taux de réussite de l'authentification faciale. Les systèmes de vérification des visages utilisent généralement des images en noir et blanc. Nous vous suggérons toutefois d'utiliser des images couleur pour améliorer les performances de ces systèmes: nous avons testé plusieurs représentations de couleurs afin de trouver celles qui conviennent à notre système. Les tests ont été effectués sur une base de données globale XM2VTS pour valider ce travail.
Mots clés : MS, Biométrie, Couleur, authentification de visage, XM2VTS, extraction de caractéristiques.

ملخص

التعرف على الوجوه هي تقنية بيومترية شائعة وتستخدم على نطاق واسع في تطبيقات التحكم في الوصول. في الأدب ، هناك العديد من الأساليب العالمية والمحلية والهجينة للتعرف على الوجوه. الغرض من هذا العمل هو القيام بعملية التحقق مصادقة على الوجه بالاعتماد على طريقة MS لزيادة معدل النجاح في مصادقة الوجه. عادة ما تستخدم أنظمة التحقق من الوجه الصور بالأبيض و الأسود. و لكن نقترح إستخدام الصور بالألوان لتحسين أداء هذه الأنظمة.لقد إختبرنا عدة تمثيلات للألوان لإيجاد المناسب منها لنظامنا. تم إجراء الاختبارات على قاعدة بيانات XM2VTS عالمية لتحقق من صحة هذا العمل.
الكلمات المفتاحية : MS ، القياسات الحيوية، اللون، مصادقة الوجه، XM2VTS، واستخراج الميزات.

Dédicace

Je dédie ce mémoire:

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

À mes frères Bachar et Mohamed Tahaa

À mes sœurs:Nessrine, saàdo, Salsabil

À Mes chers amis Hiyam et Halima

À Mon fiancé Ayoub

À Mon chéri Derouiche Iyad

À toute mes familles : Mazouzi & Zehani & Cheradid

À tous ceux que j'aime, et tous ceux qui m'aiment

Remerciements

Tout d'abord, je remercie Allah, le tout puissant, qui m'a donne la force, la patience et la volonté pour accomplir ce modeste travail.

Je remercie considérablement mon encadreur Mlle: Fedias Meriem, pour son encadrement, ses directives et sa disponibilité.

Mes remerciements s'adressent également le président et les membres de jury, qui me font m'honneur d'accepter de juger mon travail.

Je tiens à remercier ma famille pour apport affectif et leurs sacrifices.

Je remercie également tous les enseignants de département d'électronique de l'université Mohamed khider Biskra qui ont participé à ma formation pendant tout le cycle universitaire.

Je remercie aussi tous mes amies et mes camarades qui m'ont beaucoup soutenu conseillé et aidé.

Mazouzi Hasna.

sommaire

Sommaire

Chapitre II : la reconnaissance faciale

Chapitre III : L'information couleur

Chapitre IV : Les résultats et discussion

Liste des abréviations

MS: Mean and Standard deviation.

TIC: Taux d'identification Correct**.**

TFA : Taux de Fausse Acceptation.

TFR: Taux de Faux Rejet.

TEE : Taux total.

ACP: Analyse en Composantes Principales.

ICA: Analyse en Composantes Indépendantes.

LDA: Analyse Discriminante Linéaire.

EFM: Enhanced Fisher Model.

SVM: Machine à vecteurs de support.

EBGM: Elastic Bunch Graph Matching.

XM2VTS: Multi Modal Verification for Teleservices and Security application.

Liste des figures

Chapitre I

Chapitre II

Liste des tableaux

Chapitre I

Les Technologies Biométriques

I.1 Introduction

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. D'autre part, comme nous allons le voir, les caractéristiques physiques sont loin d'être si parfaites et si précises, et l'on atteint très vite des limites pour ces techniques. Les techniques basées sur la biométrie jouissent à l'heure actuelle d'un engouement général favorisé par un phénomène de mode, principalement par les films au cinéma et à la télévision. Ainsi, il n'est pas rare de voir des scanners rétiniens avec de superbes lasers rouges, des lecteurs d'empreintes digitales avec de très jolis voyants -clignotants-, etc. tout cela représentant le summum de la technologie du contrôle d'accès. Or, les techniques de biométrie sont belles et bien en train de se répandre dans notre vie quotidienne, et ce tout en gardant une image quelque peu trompeuse. Car le problème est bien de savoir quelles techniques existent réellement, et quelles sont leurs limites. Ce document ne se veut pas exhaustif sur un sujet aussi vaste que la biométrie, mais il a tout de même pour vocation de sensibiliser au maximum les étudiants et de leur donner quelques bases indispensables.

I.2 La biométrie

I.2.1 Définition de la biométrie

La biométrie peut être défini comme étant la reconnaissance automatique d'une personne en utilisant des traits distinctifs, une autre définition de la biométrie est touts caractéristiques physiques ou traits personnels automatiquement mesurables , robustes et distinctive qui peuvent être utilisées pour identifier un individu ou pour vérifier l'identité prétendue d'un individu [3].

I.2.2 Les caractéristiques biométriques

Les caractéristiques biométriques par les quelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. La figure I.1 illustre un exemple de quelques modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories : biométrie biologique, comportementale et morphologique. La biométrie biologique se base sur l'analyse des données biologiques liées à l'individu (salive, ADN, etc.). La biométrie comportementale se base sur l'analyse de comportements d'un individu (manière de marcher, dynamique de frappe au clavier, etc.). La

biométrie morphologique se base sur les traits physiques particuliers qui, pour toutes personnes, sont permanents et uniques (empreinte digitale, visage, etc.). Pratiquement, n'importe quelle caractéristique morphologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes [4]**:**

– **Universalité** : toutes les personnes à identifier doivent la posséder ;

– **Unicité** : l'information doit être aussi dissimilaire que possible entre les différentes personnes.

– **Permanence** : l'information collectée doit ˆêtre présente pendant toute la vie d'un individu.

– **Collectabilité** : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons.

– **Acceptabilité** : le système doit respecter certains critères (facilite d'acquisition, rapidité, etc.) afin d'être employé. Les caractéristiques biométriques ne possèdent pas toutes ces propriétés, ou les possèdent mais à des degrés différents. Le tableau 1, extrait de [5], compare les principales modalités biométriques selon les propriétés suivantes : universalité, unicité, permanence, Collectabilité, acceptabilité et performance. Ce tableau montre qu'aucune caractéristique n'est donc idéale et qu'elles peuvent être plus ou moins adaptées à des applications particulières. Par exemple, l'analyse basée sur l'ADN est une des techniques les plus efficaces pour vérifier l'identité d'un individu ou l'identifier [6]. Néanmoins, elle ne peut pas être utilisée pour le contrôle d'accès logique ou physique pour des raisons de temps de calcul, mais aussi, parce que personne ne serait prêt à donner un peu de sang pour faire la vérification. Le choix de la modalité est ainsi effectue selon un compromis entre la présence ou l'absence de certaines de ces propriétés selon les besoins de chaque application. A noter que le choix de la modalité biométrique peut aussi dépendre de la culture locale des usagers. En Asie, les méthodes nécessitant un contact physique comme les empreintes digitales sont rejetées pour des raisons d'hygiène alors que les méthodes sans contact sont plus répandues et acceptées.

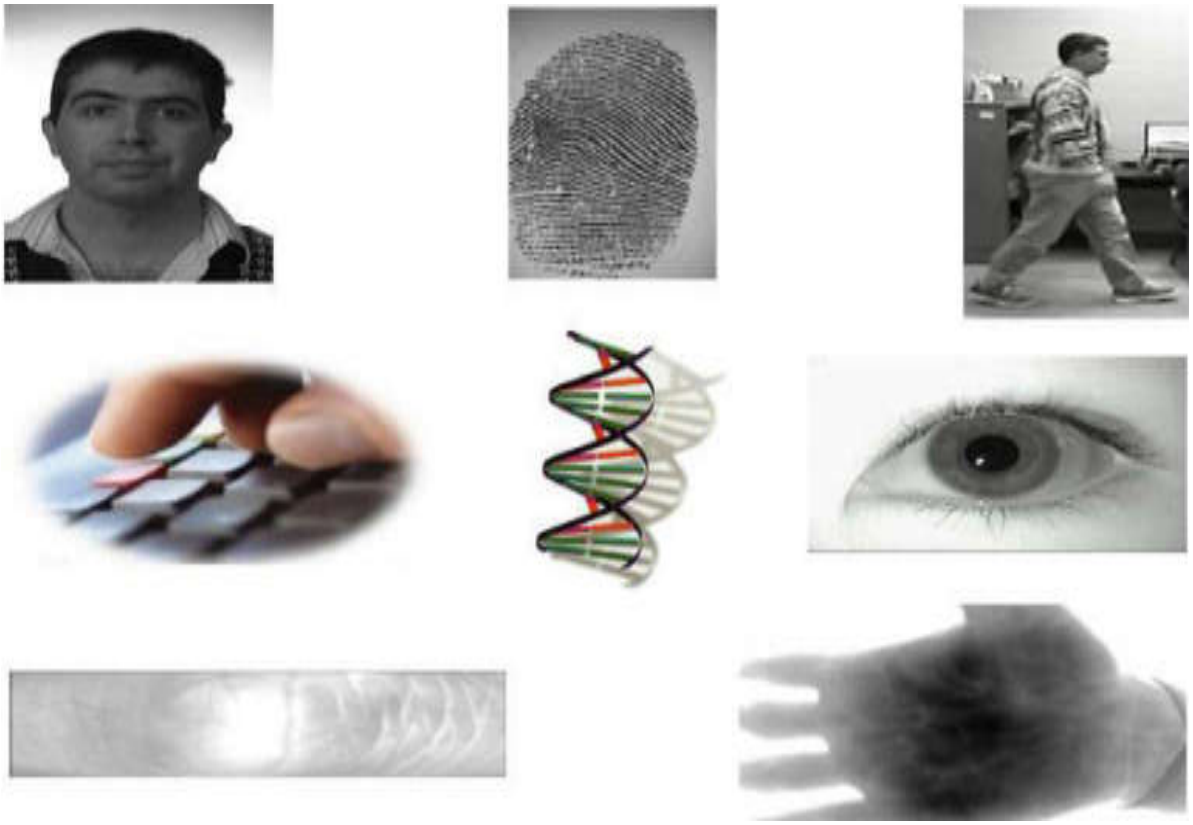

Fig. I.1 : Quelques modalités biométriques.

Biométrie	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptabilité	Circonvention
DNA	Haute	Haute	Haute	Faible	Haute	Faible	Faible
Oreille	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Haute	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Haute
Thermo Visage	Haute	Haute	Faible	Haute	Moyenne	Haute	Haute
Empreinte	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Moyenne
Démarche	Moyenne	Faible	Faible	Haute	Faible	Haute	Moyenne
Géométrie Main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Veines Main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Faible
Iris	Haute	Haute	Haute	Moyenne	Haute	Faible	Faible
Frappe Clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Moyenne
Odeur	Haute	Haute	Haute	Faible	Faible	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute

Tab. I .1: Comparaison entre les modalités biométriques.

I.2.3.Les modèles biométriques

Un modèle biométrique (appelé aussi gabarit ou Template) est l'ensemble des données utilisées pour représenter un utilisateur. Les caractéristiques biométriques acquises ne sont pas enregistrées et utilisées telles quelles. Une phase de traitement est effectuée pour réduire les données biométriques brutes et produire ainsi le modèle biométrique. La figure 2 illustre quelques exemples de modèles biométriques. Pour le stockage de ces modèles, il existe quatre emplacements principaux que sont le l'EUSB, la base centralisée, la machine individuelle de travail et le capteur biométrique. Chacun de ces emplacements présente des avantages et faiblesses en termes de temps de traitement, confidentialité et respect de la vie privée. En France, l'utilisation de la base centralisée est proscrite pour un nombre d'individus élevé par la Commission Nationale Informatique et Libertés (CNIL) [7].

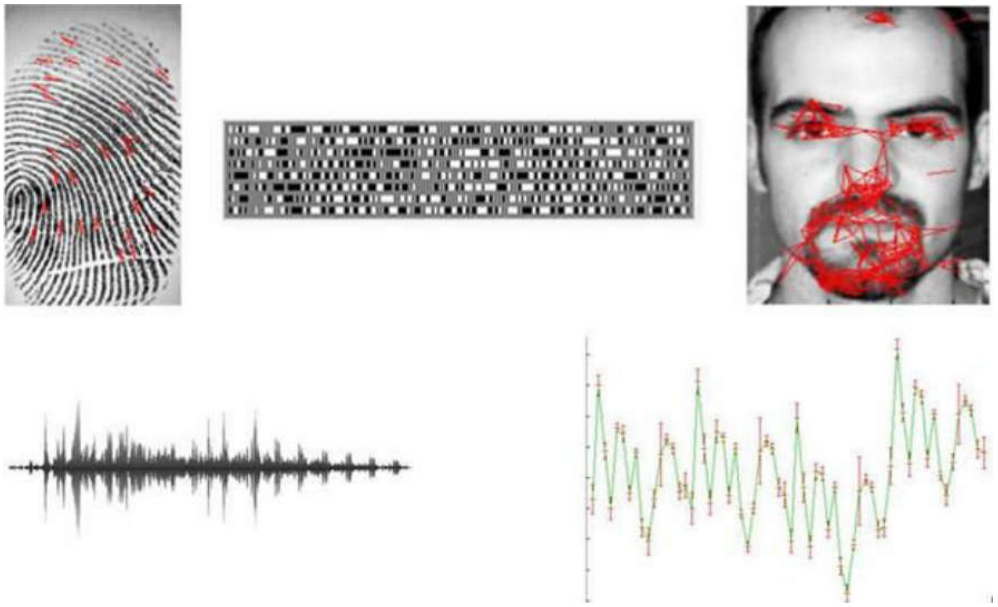

Fig. I.2 : Quelques exemples de modèles biométriques. De gauche à droite, de haut en bas : minuties extraites d'une empreinte, Iris code, graphe d'un visage utilisant les points d'intérêt, signal vocal et signal de dynamique de frappe au clavier.

I.2.4.Les modalités biométriques:

I .2.4.1 L'empreinte digitale : l'empreinte digitale est le modèle de relief cutané des doigts. L'identification par cette caractéristique est la technique la plus anciennement utilisée. En fait, c'était toujours le choix biométrique évident pour les services de police depuis plus de 100 ans, c'est pour cela qu'elle est généralement mal acceptée par les utilisateurs en raison de l'alignement fort avec la criminologie. Il existe plusieurs types de système de capture d'empreinte digitale : optique, thermique, électromagnétique et ultrasons [8].

I .2.4.2 Le visage : le visage est le moyen le plus naturel pour identifier les personnes, ce qui explique pourquoi cette caractéristique est bien acceptée par les utilisateurs. L'image de visage peut être captée par une caméra numérique, ou un appareil photo. Plusieurs recherches sont effectuées, pendant 25 ans [9], [10] pour améliorer la performance de ce genre de système cependant de nombreux problèmes se posent.

I .2.4.3 La géométrie de la main : cette modalité consiste à analyser la forme de la main sa longueur, sa largeur, son hauteur, la courbure des doigts etc. Cette technique est récente, simple, et bien acceptée par les utilisateurs qui suivent des guides des capteurs (LEDs infrarouge, des appareils photos numériques) pour qu'ils bien positionner leurs doigts, ce qui rende ainsi la détection / la segmentation plus aisée, cependant ce genre de système peut être trompé par de vrais jumeau ou même par des personnes ayant des formes de la main proches.

I .2.4.4 L'iris : l'iris est la région annulaire située entre la pupille et le blanc de l'œil. La biométrie par ce trait est la plus récente, et la plus fiable, selon les estimations de Daugmann1 La probabilité de trouver 2 iris suffisamment identiques est 1 sur 10^72 environ. L'image de l'iris est capturée par une caméra standard contraignantes (exemple la distance entre la camera et l'iris ne dépasse pas un mètre), ce qui limite l'utilisation de cette modalité.
I .2.4.5 La rétine : la rétine est la couche sensorielle de l'œil qui permet la vision, cette zone est parcouru par des vaisseaux sanguins dont leurs positions est inchangeable durant toute la vie de la personne. L'identification de la rétine n'est pas récente, elle remonte aux années 30. Cette technologie est la plus fiable toutefois elle est mal acceptée par les utilisateurs à cause des contraintes de l'acquisition.

I .2.4.6 La voix : la reconnaissance de la voix est une biométrie comportementale n'exige aucun contact physique avec le lecteur de système. En 1962 Lawrence Kersta [11] a prouvé que la voix de chaque personne est unique et qu'il est possible de la présenter graphiquement. Il existe deux principales méthodes de traitements de ce trait biométrique, la première dépend de texte prononcé, et la deuxième (la plus difficile) est indépendante de texte. Bien que cette modalité ne nécessite pas de matériel cher (microphone par exemple), cependant le bruit ambiant et les propriétés acoustiques telles que la réflexivité et l'absorption influencent la vérification de la voix en réduisant ainsi son utilisation.

I .2.4.7 La démarche : la démarche est l'une des biométries comportementale. Elle consiste à identifier les individus par leurs manières de marché, qui est supposée (presque) unique pour chaque individu. Deux types de techniques d'identification de ce trait peuvent être distingués,

l'approche "Model-based" qui dépend de quelques paramètres comme la longueur des parties du corps, la longueur de pas, la jointure d'angle etc. et l'approche "appearance-based" qui analyse directement l'image en extrayant les caractéristiques. L'avantage de cette biométrie consiste dans le fait qu'on peut identifier la personne à distance, cependant l'exécution d'un tel système est particulièrement difficile.

I .2.4.8 La signature : la vérification par la signature est l'une des premières méthodes utilisées dans le domaine de la biométrie. Les systèmes de reconnaissance de l'écriture analysent soit la géométrie de la signature (mode statique), soit ses caractéristiques spécifiques comme la vitesse, la pression sur le crayon, ce mode qui s'appelle le mode dynamique est le plus discriminant. La capture se fait à l'aide d'une tablette graphique. bien que la signature soit bien acceptée par les utilisateurs, sa variabilité (à cause de l'état de santé ou l'état émotionnel de l'individu) pose un grand problème.

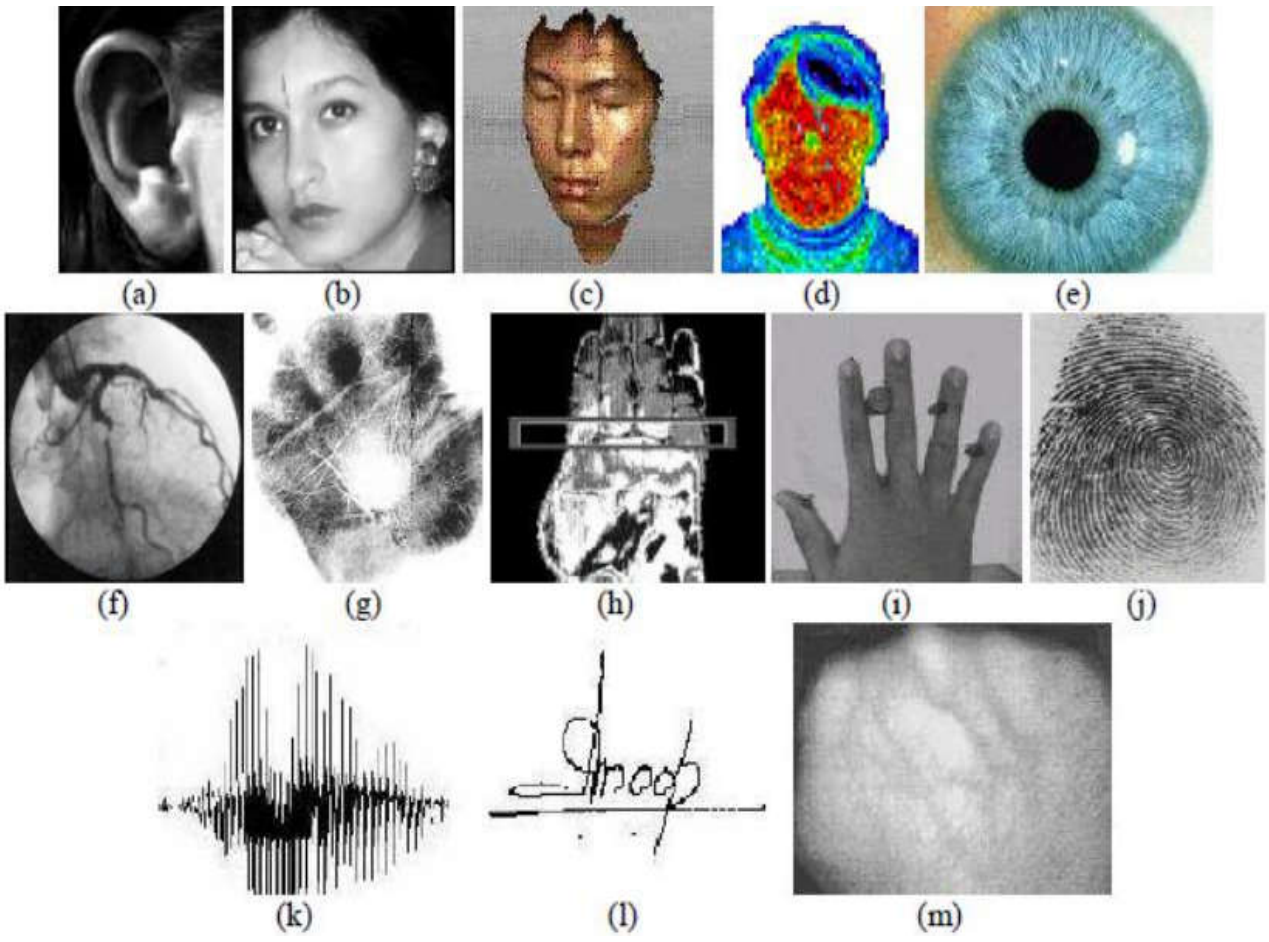

Fig. I.3: Les principales caractéristiques biométriques: a) forme de l'oreille, b) visage 2D, c) visage 3D, d) visage infrarouge, e) iris, f) rétine, g) empreinte de la main, h) thermo gramme de la main, i) forme de la main, j) empreinte digitale, k) voix, l) signature et m) réseau veineux de la main.

I.2.5.Utilisation de la biométrie

Le champ d'application de la biométrie est t'es vaste. En effet, tous les domaines qui nécessitent de vérifier ou d´déterminer l'identité de personnes sont concernés. On retrouve ainsi des applications de la biométrie pour gérer l'accès à des ressources physiques (comme l'accès à des lieux sécurisés) et logiques (comme le commerce elle-tronique).La biométrie intéresse aussi plusieurs pays (l'Europe, les Etats-Unis, etc.) afin de produire des titres d'identité plus sûres, telle que la carte nationale d'identité ou le passeport biométrique. A noter qu'en France, le passeport biométrique est désormais d´employé. Il intègre une puce RFID qui contient au moins deux informations biométriques : une empreinte digitale et une image du visage numérisée. Enfin, la biométrie n'a pas que des applications à vocation sécuritaire, mais également des applications qui facilitent le quotidien des usagers. Ainsi, la biométrie est utilisée dans certains aéroports permettant aux clients réguliers de ne pas perdre de temps lors de l'embarquement. La figure I. 4, réalisée d'après les chiffres d'International Biométrique Group [12], montre les parts de marché des principales méthodes biométriques en 2009. Les empreintes digitales sont toujours les plus utilisées, suivies par la reconnaissance faciale. Ces deux modalités représentent les trois quarts du marché de la biométrie.

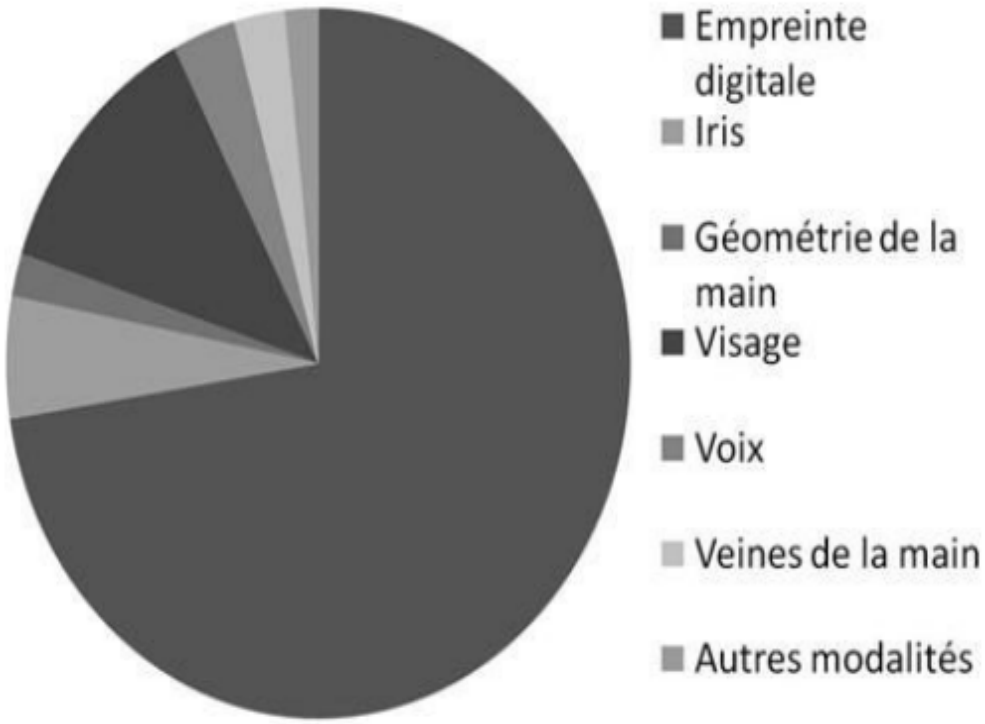

Fig. I.4 : Parts de marché des techniques biométriques en 2009.

I.2.6 Les applications de la biométrie :

Aujourd'hui, les principales applications sont la production de titres d'identité, le contrôle d'accès à des sites sécurisés, le contrôle des frontières, l'accès aux réseaux, systèmes d'information et stations de travail, le paiement électronique, la signature électronique et même le chiffrement de données. Cette liste n'est pas exhaustive, et de nouvelles applications vont très certainement voir rapidement le jour. Les techniques biométriques sont appliquées dans plusieurs domaines et leur champ d'application couvre potentiellement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes. Les applications peuvent être divisées en trois groupes principaux [13] :

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

- Applications de gouvernement : telles que la carte nationale d'identifications, le permis de conduite, la sécurité sociale, le contrôle de passeport, etc.…

- **Applications juridiques :** telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc..

Fig. I.5 : les applications de la biométrie dans notre vie.

I.2.7 Quelle est la meilleure technique biométrique ?

La comparaison des différentes biométries est généralement effectuée en fonction de quatre critères à savoir l'effort, l'intrusion, le coût, et la précision. (Il y'a d'autres critères de comparaison des techniques biométriques (Tab. I .1)).

*Effort : effort fourni par l'utilisateur lors de l'authentification.

* Intrusion : information sur l'acceptation du système par les usagers.

* Coût : coût de la technologie (lecteurs, capteurs, etc.).

*Précision : efficacité de la méthode (liée au taux d'erreur).

L'analyse Zéphyr (Fig. I.6) montre qu'il n'existe pas une méthode biométrique idéale, en effet chaque technique à ses forces et ses faiblesses. Le choix dépend essentiellement de la nature de l'application par exemple la voix et la signature sont des méthodes qui n'exigent pas un grand effort de l'utilisateur, sont peu intrusives, de coût modéré, cependant ils ne sont pas assez performantes. L'iris et la rétine sont fiables toutefois elles sont coûteuses et mal acceptées par le grand public. A noter que le choix de la modalité biométrique dépend aussi de la culture locale des utilisateurs, en Asie les méthodes nécessitant un contact physique comme l'empreinte digitale, sont rejetées pour des raisons d'hygiène alors que les méthodes qui n'exigent pas un contact sont bien acceptées.

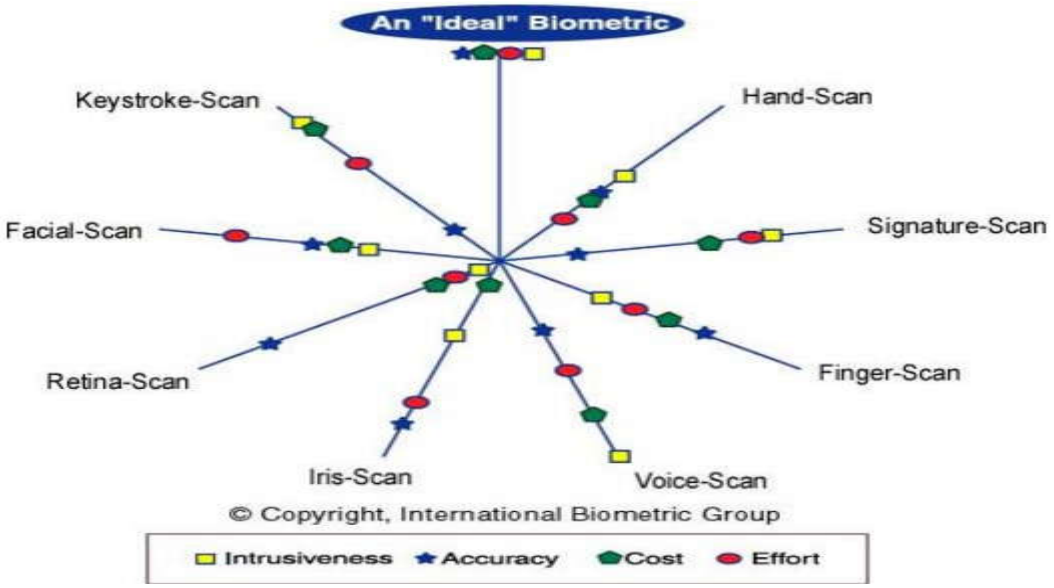

Fig. I.6: Analyse Zéphyr : comparaison de différentes modalités selon quatre critères principaux : l'intrus vite, la précision, le coût et l'effort [14].

I. 3 Systèmes biométriques

I.3.1 Modes de fonctionnement:

Les systèmes biométriques peuvent fournir trois modes de fonctionnement, à savoir, l'enrôlement, l'authentification (ou vérification) et l'identification. Dans ce qui suit, les figures illustreront l'exemple d'un système biométrique utilisant l'empreinte digitale comme modalité [15].

I.3.1.1 Le mode enrôlement: C'est la première phase de tout système biométrique (voir Fig. I. 7), il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données.

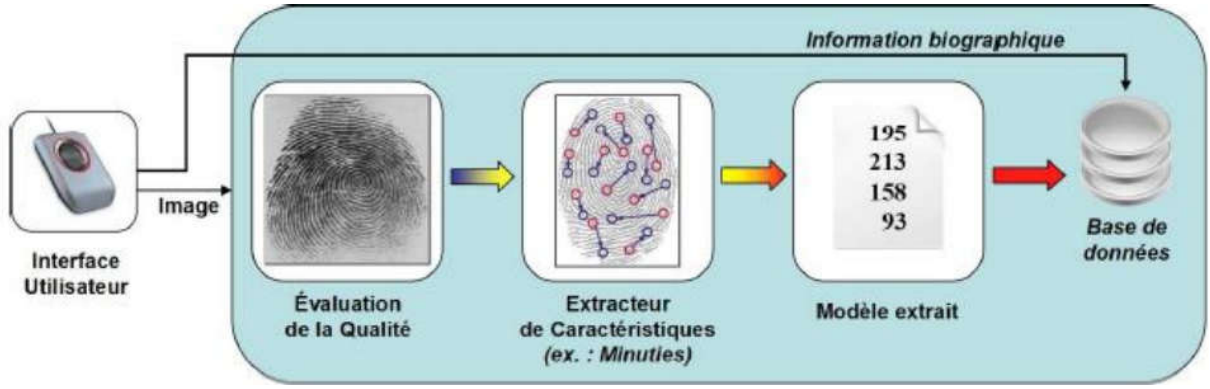

Fig. I.7 : Enrôlement d'une personne dans un système biométrique.

I .3.1.2 Le mode authentification: L'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non (voir Fig. I. 8).

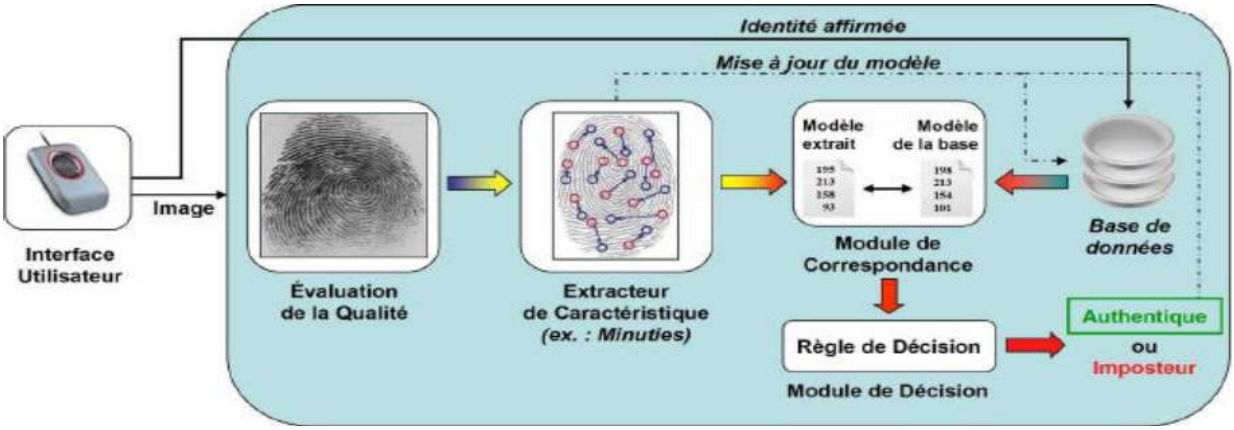

Fig. I.8 : Authentification d'un individu dans un système biométrique.

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?".

I.3.1.3 Le mode identification: L'utilisateur ne dévoile pas explicitement son identité (voir Fig. I. 9). 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.**

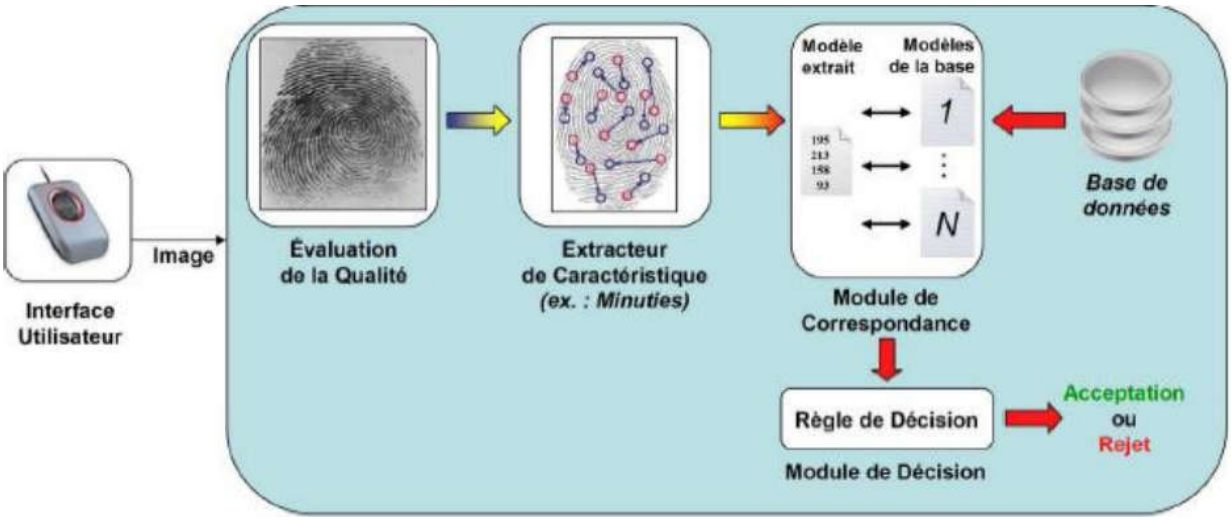

Fig. I.9: Identification d'un individu dans un système biométrique.

Un exemple de système opérant en mode identification serait l'accès à un bâtiment sécurisé : tous les utilisateurs qui sont autorisés à entrer dans le bâtiment sont enrôlés par le système;

lorsqu'un individu essaye de pénétrer dans le bâtiment, il doit d'abord présenter ses données biométriques au système et, selon la détermination de l'identité de l'utilisateur, le système lui accorde le droit d'entrée ou non. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ?".

I.3.2 Architecture d'un système biométrique

Il existe toujours au moins deux modules dans un système biométrique : le module d'apprentissage et celui de reconnaissance [16], [17]. Le troisième module (facultatif) est le module d'adaptation. Pendant l'apprentissage, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un modèle de l'individu. Ce modèle de référence servira de point de comparaison lors de la reconnaissance. Le modèle pourra être réévalué après chaque utilisation grâce au module d'adaptation.

I.3 .2.1 Module d'apprentissage:

Au cours de l'apprentissage, la caractéristique biométrique est tout d'abord mesurée grâce à un capteur ; on parle d'acquisition ou de capture. En général, cette capture n'est pas directement stockée et des transformations lui sont appliquées. En effet, le signal contient de l'information inutile à la reconnaissance et seuls les paramètres pertinents sont extraits. Le modèle est une représentation compacte du signal qui permet de faciliter la phase de reconnaissance, mais aussi de diminuer la quantité de données à stocker. Il est à noter que la qualité du capteur peut grandement influencer les performances du système. Meilleure est la qualité du système d'acquisition, moins il y aura de prétraitements à effectuer pour extraire les paramètres du signal.

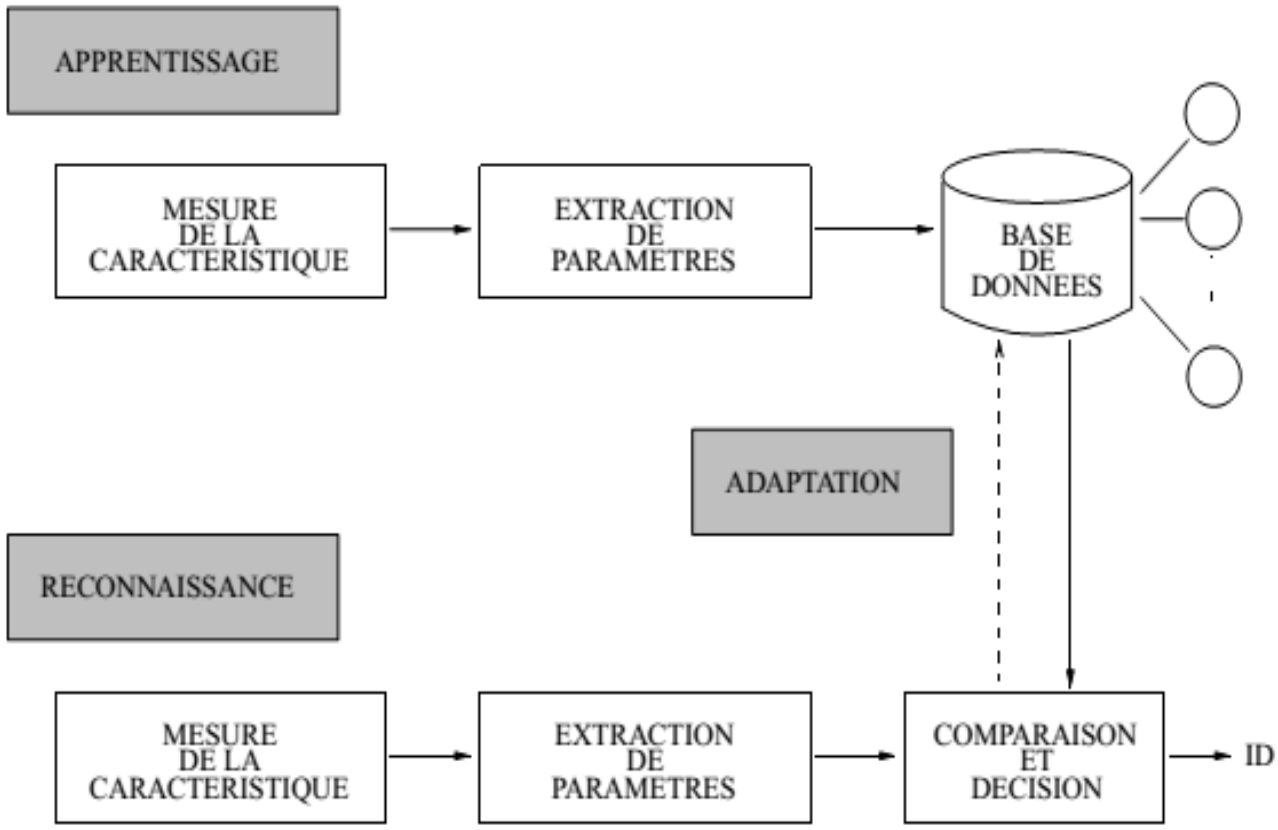

Fig. I. 10: Architecture d'un système de reconnaissance biométrique.

Cependant, les capteurs de qualité sont en général coûteux et leur utilisation est donc limitée à des applications de haute sécurité pour un public restreint.

Le modèle peut être stocké dans une base de données comme représenté sur la Fig. I.10 ou sur une carte de type carte à puce.

I.3. 2.2 Module de reconnaissance:

Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de pré-traitements supplémentaires pour limiter la dégradation des performances. La suite de la reconnaissance sera différente suivant le mode opératoire du système : identification ou vérification.

En mode identification, le système doit deviner l'identité de la personne. Il répond donc à une question de type : « Qui suis-je ? ». Dans ce mode, le système compare le signal mesuré avec

les différents modèles contenus dans la base de données (problème de type 1 : n). En général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base de données.

En mode vérification, le système doit répondre à une question de type : « Suis-je bien la personne que je prétends être ? ».

L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données.

En mode vérification, on parle de problème ouvert puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (imposteur) peut chercher à être reconnu. Identification et vérification sont donc deux problèmes différents. L'identification peut-être une tâche redoutable lorsque la base de données contient des milliers, voire des millions d'identités, tout particulièrement lorsqu'il existe des contraintes de type « temps réel » sur le système. Ces difficultés sont analogues à celles que connaissent par exemple les systèmes d'indexation de documents multimédia.

I.3 .2.3 Module d'adaptation:

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire amélioré la performance d'un système utilisation après utilisation. L'adaptation peut se faire en mode supervisé ou non-supervisé mais le second mode est de loin le plus utile en pratique. Si un utilisateur est identifié par le module de reconnaissance, les paramètres extraits du signal serviront alors à ré-estimer son modèle. En général, le taux d'adaptation dépend du degré de confiance du module de reconnaissance dans l'identité de l'utilisateur. Bien entendu, l'adaptation non-supervisée peut poser problème en cas d'erreurs du module de reconnaissance.

L'adaptation est quasi indispensable pour les caractéristiques non permanentes comme la voix [18], [19].

I .3.3 Principe de fonctionnement d'un système biométrique

a. Capture de l'information à analyser (image ou son).

b. Traitement de l'information et création d'un fichier " signature/gabarit " (éléments caractéristiques de l'image), puis mise en mémoire de ce fichier de référence sur un support (disque dur, carte à puce, code barre).

c. Dans la phase de vérification, l'on procède comme pour la création du fichier " signature/gabarit " de référence, ensuite on compare les deux fichiers pour déterminer leur taux de similitude et prendre la décision qui s'impose.

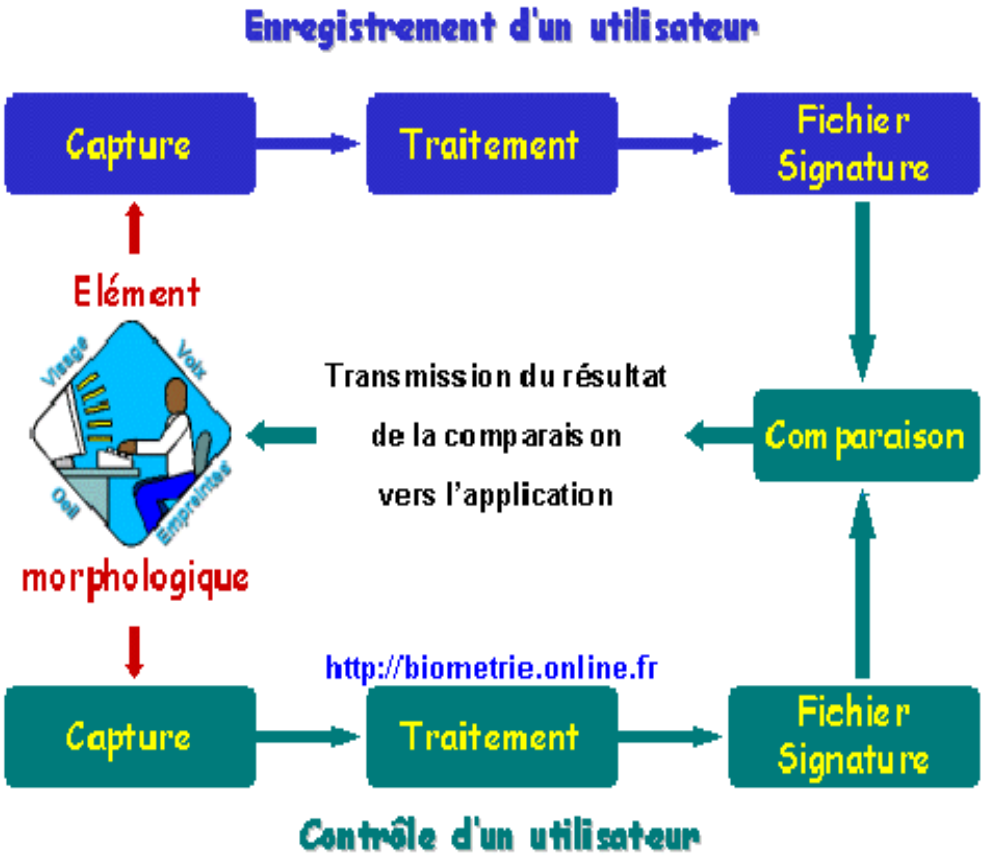

Fig. I. 11: Principe de fonctionnement d'un système biométrique.

Les informations stockées ne sont en jamais les images d'origine, mais un modèle mathématique des éléments qui distinguent l'échantillon biométrique d'un autre. Ce modèle est appelé un " gabarit " ou " signature ". De cette manière, on obtient alors des fichiers de très petite taille. Par exemple, l'image d'origine d'une empreinte digitale à une taille de l'ordre de 100 000 octets, et son gabarit une taille de l'ordre de 500 octets [20].

I .3.4 Evaluations des systèmes biométrique

Typologie d'erreurs et mesures de performances :

Dans un système de reconnaissance de visages, chaque tâche possède ses propres erreurs [21]. Dans cette section nous rappelons la typologie d'erreurs des deux tâches les plus utilisées, à savoir l'identification et la vérification du visage. • Identification : On peut parler de deux types d'erreurs : * Mauvaise identification : c'est le cas où le système propose une identité qui ne correspond pas à celle du locuteur présenté.

* Non détection : cette erreur est caractéristique des systèmes d'identification du visage dans un ensemble ouvert. Elle correspond au cas où le système n'a pas pu identifier le visage de la personne présentée alors que ce dernier a son modèle dans la base de référence.
La mesure des performances des systèmes d'identification du locuteur se base sur le Taux d'identification Correct (TIC) obtenu en phase de test :

$$\text{TIC} = \frac{\text{tests ayant une identification correct}}{\text{tests total}}$$

Équation 1. Taux d'identification Correct

Tests total désigne l'ensemble des tests effectués (Vrai ou Fausse identification).

• Vérification : Il existe deux types d'erreurs:

* Fausse acceptation (FA) : Elle correspond au cas où le système accepte une personne qui a proclamée une identité qui n'est pas la sienne. Une fausse acceptation est une erreur où le système accepte un imposteur.

* Faux rejet (FR) : C'est le cas où le système rejette une personne qui a proclamé sa vraie identité. Autrement dit, c'est quand le système rejette un client. Les mesures de performances d'un système de reconnaissance de visages se basent principalement sur le Taux des Fausses Acceptations (FA) et le Taux des Faux Rejets (FR) obtenu en phase de test :

$$\text{FA} = \frac{\text{tests ayant amené à une fausses acceptation}}{\text{tests total}}$$

Équation 2. Taux des Fausses Acceptations**.**

$$\text{FR} = \frac{\text{tests ayant amené à une faux rejet}}{\text{tests total}}$$

Équation 3. Taux des Faux Rejets

Les performances d'un système de reconnaissance de visages peuvent être présentées sous forme d'une seule courbe appelée courbe DET (Détection Error Trade-of) ou encore courbe ROC (Receiver Operating Characteristic) sur laquelle les FA sont données en fonction des FR. Pour construire cette courbe, on calcule un couple (FA, FR) pour chaque valeur de seuil de décision variant de la plus petite valeur des scores obtenus en phase de test à la plus grande valeur. Les performances des systèmes de reconnaissance de visages sont souvent comparées selon un point particulier de ces courbes qui est le Taux d'Égale Erreur (EER) et qui correspond au point de la courbe où FA = FR. Une autre mesure permet d'évaluer les performances d'un système de vérification est HTER (Half Total Error rate). Cette mesure est utilisée quand le seuil de décision est fixé à priori. Le HTER représente la moyenne de FA et FR.

Idéalement, un système de reconnaissance de visage devrait avoir des FA et FR égaux à zéro. Malheureusement, dans des conditions réelles, ceci n'est pas possible ; car plus le seuil de décision est bas; plus le système acceptera des utilisateurs clients mais aussi des imposteurs. Inversement, plus le seuil de décision est élevé, plus le système rejettera des imposteurs mais aussi des utilisateurs clients. Il est donc impossible en faisant varier le seuil de décision de faire diminuer les deux types d'erreurs en même temps. La Fig. I. 12 explique ce phénomène. Le seuil peut donc être ajusté en fonction de l'application ciblée : Haute sécurité (S2), basse sécurité (S0) ou un compromis entre les deux (S1). La Fig. I. 13 représentant la courbe ROC explique ceci

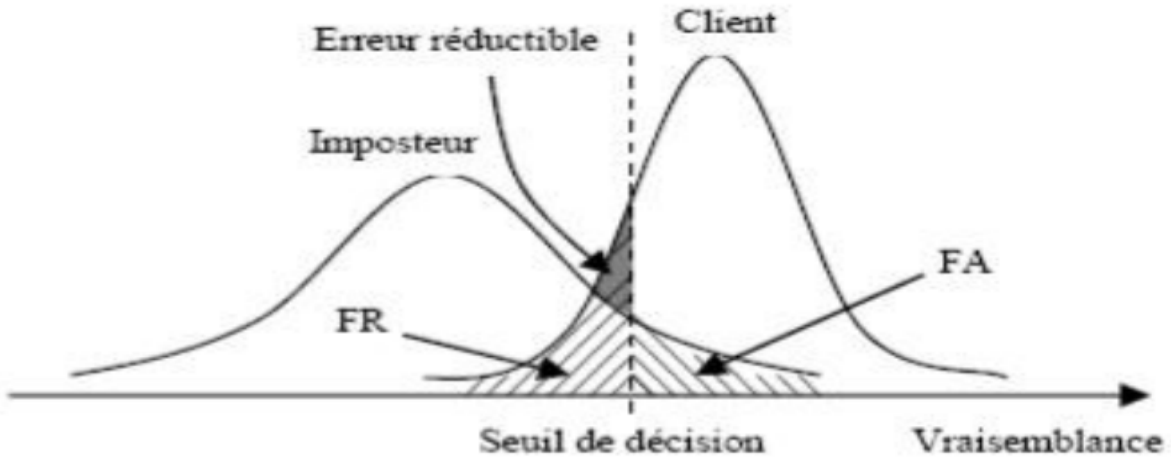

Fig. I. 12 : Seuil de décision et taux d'erreurs**.**

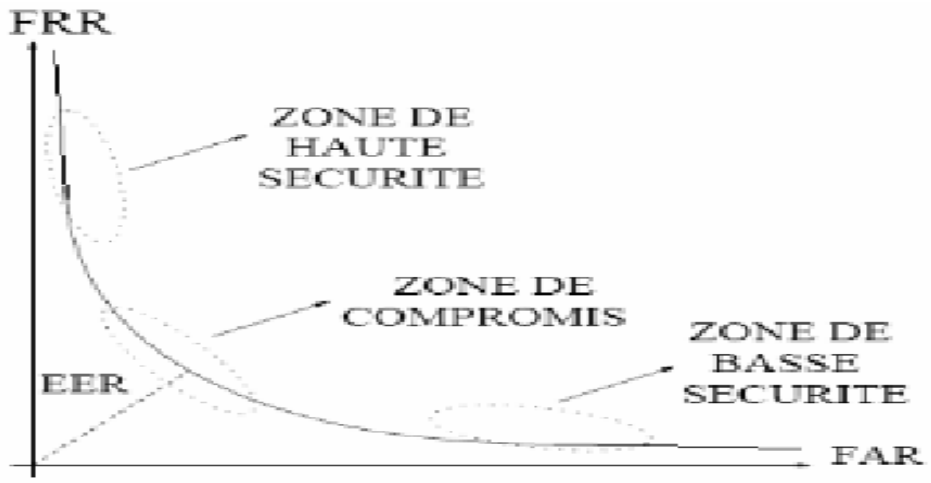

Fig. I. 13: Courbet ROC curve.

Techniques de calcul du seuil: Plusieurs contraintes rendent le seuil de décision impossible à calculer en pratique. Parmi ces contraintes nous citons : l'indétermination de l'estimation réelle des coûts des erreurs ni des connaissances à priori p (x) et p ($\bar{x}$), de plus les fonctions de vraisemblance ne sont qu'une estimation des densités de probabilité exactes. Pour ces raisons nous avons eu recours à l'estimation de seuil de décision par calculs empiriques, et cela suivant deux méthodes : la méthode analytique et la méthode non analytique.

• **Méthode analytique :**

On utilise dans cette méthode des tests sur des personnes clientes et des imposteurs pour calculer les moments d'ordre 1 et d'ordre 2 de leurs scores respectifs. Notons par M_x et σ_x les paramètres statistiques du score des clients et par $\overline{M_x}$et $\overline{\sigma_x}$ceux des imposteurs. Le seuil de décision est calculé par une combinaison linéaire des paramètres statistiques x décrits ci-dessus.

$$seuil = \frac{\overline{M_x}\sigma x + Mx\,\overline{\sigma_x}}{\sigma x + \overline{\sigma_x}}$$

Équation 4. Le seuil de décision

• **Méthode non analytique :**

Dans cette méthode, nous faisons varier le seuil de décision, pour chaque valeur du seuil nous calculons le FA et FR issue d'une série de tests pour les vrais clients et les imposteurs. A l'issue de cette étape, nous pouvons tracer la courbe représentant l'évolution des couples (FA, FR) lorsque le seuil varie. La Fig. I. 14 montre un exemple de cette courbe.

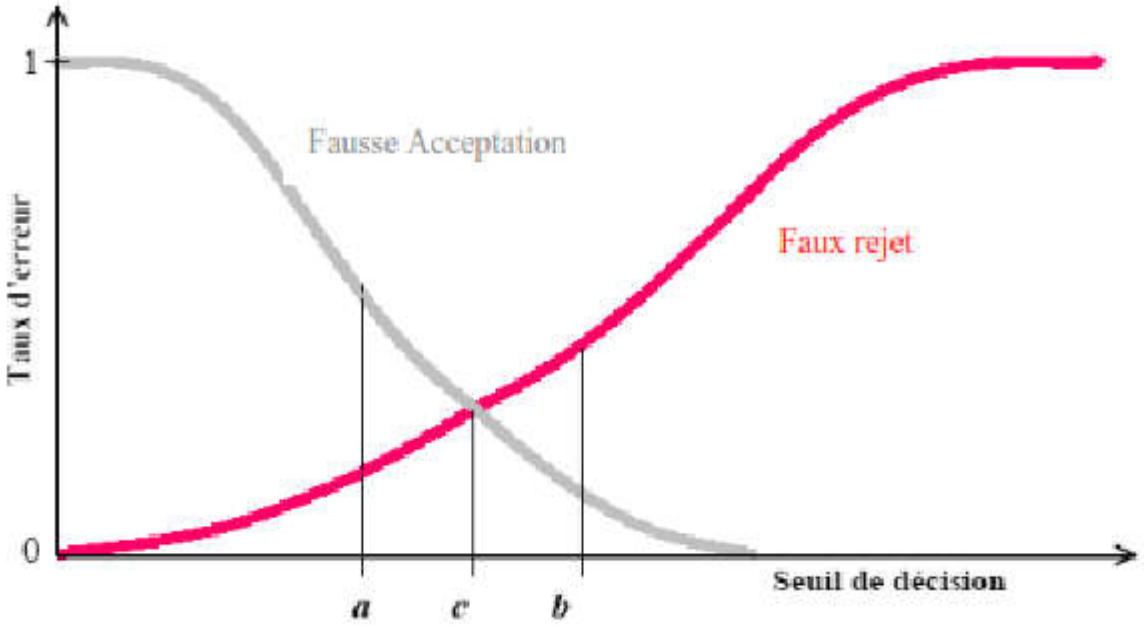

Fig. I. 14 : Distribution des taux d'erreurs par rapport au seuil de décision, « c » représente le seuil de décision optimale.

I. 4. Les avantages et les limites de la biométrie:

I.4.1. Les avantages de la biométrie:

La biométrie est une technologie récente et commence à être adoptée par de grands constructeurs de matériel informatique [22]. L'usage de la biométrie est un complément de l'utilisation des méthodes d'authentification comme des mots de passe, des badges, des cartes à puce.

- Suppression des mots de passe, Suppressions des clés : Au lieu de retaper son mot de passe dès que le PC se met en veille, une simple pression de l'empreinte digitale sur le capteur suffit et permet facilement de changer la session d'utilisateur.

- Utilisation d'une signature biométrique: Grande sécurité, intransmissible à une autre personne. Une identité vérifiée (Le destinataire est bien la personne autorisée à visualiser ou à utiliser les données). Lors de transactions financières, il est capital de savoir quel moyen de paiement du consommateur est le plus sûr. La biométrie offre le chaînon manquant dans la triade du problème de sécurité: - Diminution de la fraude. - Rehaussement de l'intégrité des informations et la sécurité. - Réduction des attaques à l'égard des programmes gouvernementaux. - Croissance de la confiance envers les systèmes de sécurité. - Diminution des frais administratifs. - Accélération des services.

I .4.2. Les limites de la biométrie:

La biométrie présente malheureusement un certain nombre d'inconvénients parmi eux : le problème de la qualité de l'authentification. Ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche des utilisateurs de bonne foi d'accéder à leur système. Car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant: on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent [23]. Prenons le cas le plus simple, celui des empreintes digitales (mais la même chose s'applique à toute donnée physique). Suivant les cas, nous présentons plus ou moins de transpiration, la température des doigts n'est pas régulière. Il suffit de se couper pour présenter une anomalie dans le dessin de ses empreintes. Dans la majorité des cas, les mesures du capteur et du logiciel associé retourneront un résultat différent de la mesure initiale de référence. Or, il faut pourtant bien réussir à se faire reconnaître. En pratique, cela sera réalisé dans la plupart des cas car le système est amené à autoriser une marge d'erreur entre la mesure et la référence.

De manière générale, les faiblesses de ces systèmes ne se situent pas au niveau de la particularité physique sur laquelle ils reposent, mais bien sur la façon avec laquelle ils la mesurent, et la marge d'erreur qu'ils autorisent. Là encore, il convient de ne pas se laisser impressionner par une image illusoire de haute technologie - produit miracle. De plus, les experts techniques mettent au passif de cette technologie, d'une part, son coût, d'autre part, la question de sa révocation. En effet, confronté à une personne qui a subtilisé un mot de passe ou une signature manuscrite, le titulaire du mot de passe ou de la signature peut facilement les remplacer ou les révoquer. La chose semble plus complexe pour une empreinte digitale ou rétinienne. Si un tiers s'approprie une identité biométrique du type empreintes digitales ou identité visuelle, il peut au moyen de ces identités biométriques passer tout type d'actes au nom de la victime. Comment la victime pourrait-elle alors révoquer sa propre empreinte digitale ou identité visuelle ? Les experts en sécurité sont partagés sur la question, même si, en majorité, ils semblent considérer que cette révocation est possible. Tous reconnaissent cependant la difficulté à mettre au passif cette protection technique. Les données biométriques sont comparables à tout autre système de contrôle d'accès comme des mots de passe, …etc. Car du point de vue du système informatique, ce ne sont rien d'autres que des séries de bits comme toute donnée. Autrement dit, la difficulté réside dans la contrefaçon de la caractéristique physique et biologique que l'on mesure. Si la biométrie se généralise dans notre environnement, il est dangereux de penser qu'il s'agit de la réponse à tous les problèmes de sécurité. La

biométrie, de par ses limites fonctionnelles, techniques et juridiques n'est en aucun cas synonyme de technologie miracle et de sécurité absolue.

- Les limites fonctionnelles: Les systèmes d'authentification biométrique représentent une grande partie des limites fonctionnelles. En effet, les systèmes biométriques laissent la place à un certain nombre de faux rejets et de fausses acceptations. Ils ne peuvent à eux seuls garantir à 100% que seules les personnes autorisées pourront passer le contrôle. Ils ne peuvent même pas garantir qu'une personne autorisée ne sera pas rejetée par le système. Il y aura toujours une marge d'erreur à prendre en compte, ce qui n'est pas forcément très rassurant.
- Les limites techniques : Bien que cela représente un travail assez conséquent, les données biométriques peuvent être imitées, notamment celles qui laissent des traces sur le passage de l'individu telles que les empreintes digitales. Un individu mal intentionné peut récupérer les empreintes digitales sur un objet tenu par la victime, les imiter et tenter de passer le contrôle biométrique à l'aide de ces empreintes. De plus, les données biométriques sont dans la majeure partie des cas numérisées sur un support, de préférence individuel. Si ce support n'est pas protégé contre les intrusions et le piratage, tout le système biométrique tombe à l'eau.

I .5 Conclusion

Dans ce chapitre, nous avons présenté la définition de la biométrie et les technologies utilisées dans les systèmes biométriques pour l'identification de personnes. Nous avons aussi donné un aperçu sur les techniques de mesure de leurs performances. Cette étude nous a permis de constater que la reconnaissance de visage suscite de plus en plus l'intérêt de la communauté scientifique, car elle présente plusieurs challenges et verrous technologiques.

Chapitre II

La Reconnaissance Faciale

II.1. Introduction

Par la fréquence à laquelle on le rencontre dans l'environnement et par son contenu riche en information sociale de premier ordre, le visage humain constitue un stimulus visuel de classe à part. En effet, il suffit d'un clin d'œil porté sur le visage d'un individu pour en distinguer le sexe, l'état émotionnel ou l'identité. Non seulement le traitement d'une telle information s'avère fort efficace, mais aussi très rapide – une exposition de 20 ms suffit (p.ex. Rizzolatti & Buchtel, 1977). Cette performance est d'autant plus surprenante que chaque visage est composé des mêmes attributs (yeux, nez, bouche) disposés selon une organisation similaire, créant ainsi un groupe de stimuli d'une homogénéité supérieure à celle retrouvée dans la majorité des catégories d'objets. Pourtant, tout observateur humain se montre capable d'identifier un nombre apparemment infini de visages, alors que seules de fines discriminations visuelles permettent de les identifier. Cette grande capacité à identifier les visages (99%) à pousser les chercheurs à tenter de rapprocher le cerveau humain dans sa rapidité, son exactitude et sa fiabilité par des systèmes de reconnaissance basés sur des approches statistiques ou non statistiques.

II.2. Pourquoi choisir le visage?

La reconnaissance de visages est la technique la plus commune et populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle ; et par rapport aux autres méthodes, la reconnaissance du visage s'avère plus avantageuse, d'une part c'est une méthode non intrusive, c'est-à-dire elle n'exige pas la coopération du sujet (en observant les individus à distance), et d'une autre part les capteurs utilisés sont peu coûteux **[**24**].**

Avantages	**Inconvénients**
Bien accepté par le public. **Aucune action de l'usager** (peu intrusive). **Pas de contact physique.** **Technique peu coûteuse.**	**Technologie sensible à l'environnement** (éclairage, position, expression du visage…) **Difficultés de différencier de vrais jumeaux.** **Sensible aux changements.** (barbe, moustache, lunettes, piercing, chirurgie…)

Tab. II 1: Avantages et inconvénients de la Reconnaissance de Visage.

II.3. Processus d'un système de reconnaissance du visage:

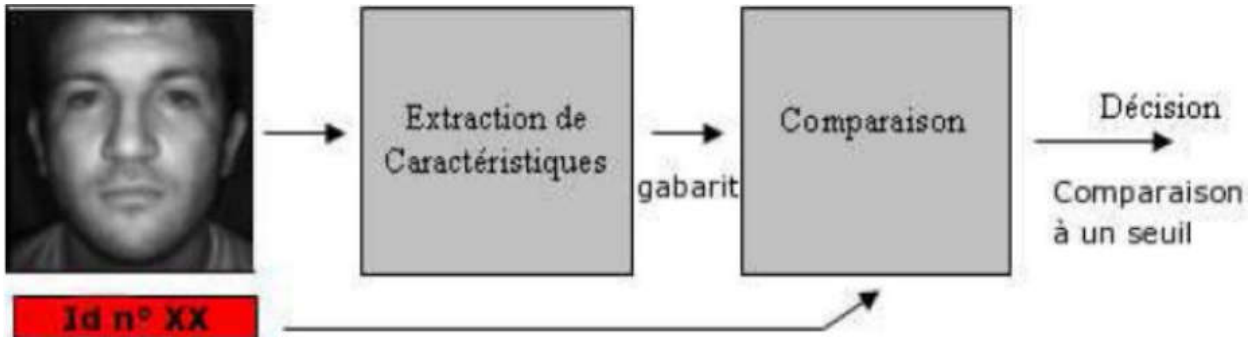

Fig. II.1 : Schéma de vérification d'un visage**.**

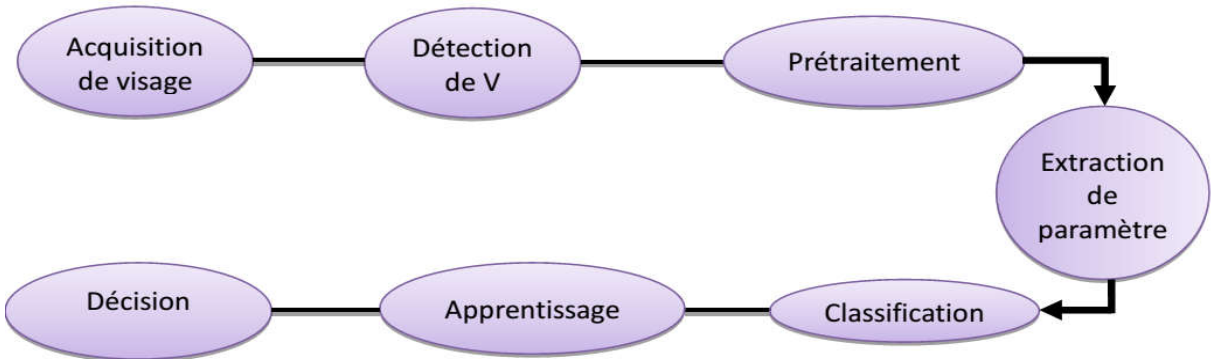

Fig. II.2 : Système de reconnaissance de visage**.**

II.3.1 Acquisition

Un système d'acquisition équipé d'un capteur est utilisé pour acquérir une caractéristique spécifique de l'utilisateur, par exemple: un microphone dans le cas de la voix **[**25**]**.

C'est l'opération qui permet d'extraire du monde réel une représentation bidimensionnelle pour des objets en 3D, cette opération peut être statique (Appareil photo, Scanner, etc.) ou dynamique (Caméra, Web Cam), dans ce cas on aura une séquence vidéo .A ce niveau on aura une image brute **[**2**] [**26**]**.

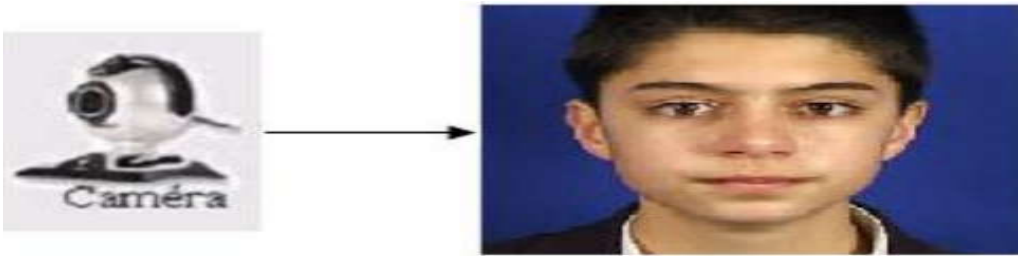

Fig. II.3 : Exemple d'acquisition d'une image.

II.3.2.Détection de visage:

L'efficacité des systèmes biométriques basés sur l'authentification de visage dépend essentiellement de la méthode utilisée pour localiser le visage dans l'image. Dans la littérature scientifique, le problème de localisation de visages est aussi désigné par la terminologie "détection de visages". Plusieurs travaux de recherches ont été effectués dans ce domaine. Ils ont donné lieu au développement d'une multitude de techniques allant de la simple détection du visage, à la localisation précise des régions caractéristiques du visage, tels que les yeux, le nez, les narines, les sourcils, la bouche, les lèvres, les oreilles, etc **[**27**]** [28] [29**]**.

Fig. II.4 : Détection de visage**.**

II.3.3 Le prétraitement:

Où les données biométriques sont traitées pour enlever le bruit lié à l'environnement ou au dispositif de capture **[**30**]**. Il faut éliminer le bruit par des techniques de traitement et de restauration d'images et procéder à une détection de visages, cette opération est très complexe, surtout dans le cas où l'image contient plusieurs visages ou le cas où l'arrière plan n'est pas neutre **[**26**]**.

Les performances globales de tout système automatique de reconnaissance dépendent amplement des performances de la détection de visages **[**27**]**. On peut diviser les approches de détection en quatre catégories : les méthodes basées sur la connaissance où on code la connaissance humaine du visage, les méthodes de correspondance de masques, les méthodes à caractéristiques invariables où on utilise la couleur, les textures et les contours, et finalement les méthodes les plus répandues et qui sont ceux basées sur l'apprentissage ou les statistiques comme **PCA, SVM** et Graph matching **[**31**] [**26**]**.

II.3.4 .Extraction

Appelée aussi indexation, représentation, modélisation [32]. Ayant une image ou une voix en entrée, une étape de segmentation permet d'extraire la caractéristique dont le processus d'authentification a besoin. Par exemple: extraire le visage du fond d'une image dans le cas de l'identification de visage [25]. Pour extraire l'information utile contenue dans le signal capturé [33]. Le choix de ces informations utiles revient à établir un modèle pour le visage, elles doivent être discriminantes et non redondantes [26].

II.3.5.Classification

En examinant les modèles stockés dans la base de données, le système collecte un certain nombre de modèles qui ressemblent le plus à celui de la personne à identifier, et constitue une liste limitée de candidats. Cette classification intervient uniquement dans le cas d'identification car l'authentification ne retient qu'un seul modèle (celui de la personne proclamée) [34].

II.3.6.Apprentissage:

D'une manière générale, nous posons le problème comme celui de l'apprentissage d'une distance entre visages. Nous supposons disposer d'un ensemble de paires d'images de visages, certaines de ces paires représentant des visages de personnes différentes, d'autres des paires de visages provenant de la même personne mais avec des variations d'expression, de pose ou d'illumination. Pour chacune de ces paires nous connaissons la vérité terrain, c'est-à-dire que nous savons s'il s'agit de la même personne ou non. Notre calcul de similarité s'appuie sur quatre grandes étapes :

1. Chaque visage est représenté par un vecteur d'attributs.

2. Nous effectuons ensuite une transformation linéaire des données de départ en utilisant une méthode inspirée de[35], dont l'intérêt est, en plus de réduire la dimensionnalité, de calculer un espace de représentation qui sépare au mieux les données positives des négatives (paires de visages identiques ou différents).

3. Une phase d'apprentissage semi supervisé, où les données de test (dont les labels ne sont pas connus) sont utilisées pour déterminer avec plus de précision la structure des données

dans l'espace de représentation. Cette phase repose sur la construction d'un graphe où les nœuds représentent les paires de visages et les arêtes les relations entre ces paires.

4. L'apprentissage d'un classifier qui combine les informations extraites à partir des deux méthodes précédentes pour mesurer la similarité de deux visages inconnus **[**36**]**.

Elle consiste à mémoriser les représentations calculées dans la phase analyse pour les individus connus. Généralement les deux étapes d'analyse et d'apprentissage sont confondues et regroupées en une seule étape **[**37**]**.

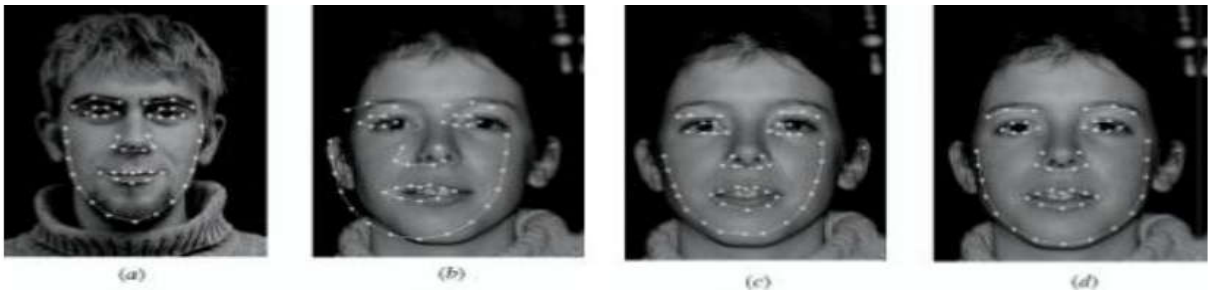

Fig. II.5 : Exemple d'image d'apprentissage

II.3.7.Décision

Dans le cas de l'identification, il s'agit d'examiner les modèles retenus par un agent humain et donc décider. En ce qui concerne l'authentification, la stratégie de décision nous permet de choisir entre les deux alternatives suivantes: l'identité de l'utilisateur correspond à l'identité proclamée ou recherchée ou elle ne correspond pas **[**38**]**. C'est dans ce module que le système donne sa réponse soit dans une identification par la personne de la base la plus proche, soit par une vérification (oui ou non) **[**33**]**. Pour estimer la différence entre deux images, il faut introduire une mesure de similarité. Il est important de noter que le système de vérification automatique de visage se base en sa totalité sur la méthode de localisation **[**39**]**.

II.4. Les classes des techniques de reconnaissance de visages:

Les méthodes de reconnaissance de visages peuvent être classées en deux grandes catégories : les méthodes locales et globales **[**40**]**. Quelques principales d'entre elles seront présentées dans ce qui suit.

II .4.1 Les méthodes globales:

Les méthodes globales basées sur des techniques d'analyse statistique bien connues. Dans ces méthodes, les images de visage (qui peuvent être vues comme des matrices de valeurs de pixels) sont utilisées comme entrée à l'algorithme de reconnaissance et sont généralement transformées en vecteurs, plus faciles à manipuler. L'avantage principal des méthodes globales est qu'elles sont relativement rapides à mettre en Suivre. En revanche, elles sont très sensibles aux variations d'éclairement, de pose et d'expression faciale **[**41**] [**15**]**.

Les principales méthodes existantes sont :

- L'Analyse en Composante principale(ACP) :

L'algorithme ACP appliqué au visage est né des travaux de MA. Türk et AP. Pentland au MIT Media Lab, en 1991**[**41**]**. Il est aussi connu sous le nom de « Eigen faces » car il utilise des vecteurs propres et des valeurs propres. Sa simplicité à mettre en Suvre contraste avec une forte sensibilité aux changements d'éclairement, de pose et d'expression faciale.

- L'Algorithme LDA (Linear Discriminant Analysis):

Appliqué aux images en 1997 par Belhumer et al Yale de la Yale University aux USA, aussi connu sous le nom de Fisherfaces**[**15**]**. Contrairement à l'ACP, il permet d'effectuer une véritable séparation de classes.

- Les réseaux de neurones:

Les réseaux de neurones sont des modèles de calcul qui date des années 40. C'est une technique inspirée des réseaux de neurones biologiques pour exécuter des tâches calculatoires. Elle a la particularité de s'adapter, d'apprendre, de généraliser pour classer les données en entrée [42].

- SVM (Machine à vecteurs de support):

Le principe de cette méthode est de trouver le meilleur hyperplan séparant aux mieux les points dans un espace de grande dimension et qui minimise le taux d'erreur total de classification [43].

II.4.2 Les méthodes locales(Géométrique):

Les méthodes locales consistent à appliquer des transformations en des endroits spécifiques de l'image, le plus souvent autour de points caractéristiques (coins des yeux, de la bouche, le nez,...). Elles nécessitent donc une connaissance à priori sur les images. Ces méthodes sont plus difficiles à mettre en place mais sont plus robustes aux problèmes posés par les variations d'éclairement, de pose et d'expression faciale **[**40**]**. Les principales méthodes existantes sont :

- EBGM (Elastic Bunch Graph Matching):

L'algorithme EBGM est né des travaux de Wiskott et al ,1997**[**44**]**. À partir d'une image de visage, on localise des points caractéristiques (coins des yeux, de la bouche, nez,...etc.). Cette localisation peut se faire manuellement ou automatiquement à l'aide d'un algorithme.

- EingenFace modulaire :

Cette méthode possède le même principe que les EigenFaces, mais appliquée à des parties précises du visage comme les yeux. Mais elle rencontre le problème de non précision lors de la localisation des points caractéristiques du visage avant l'application de la méthode.

- Méthode de Markov caché:

Les HMMs (Hidden Markov Models) sont appliqués à la reconnaissance du visage en considérant l'information du visage comme étant une séquence variable dans le temps [45].

L'avantage des méthodes locales, est qu'elles prennent en compte la particularité du visage en tant que forme naturelle à reconnaître et un nombre réduit de paramètres en exploitant les résultats de la recherche en neuropsychologie et psychologie cognitive sur le système visuel humain. La difficulté éprouvée c'est quand il s'agit de prendre en considération plusieurs vues du visage ainsi que le manque de précision dans la phase « extraction » des points qui constitue leur inconvénient majeur.

II.4.3 Les approches hybrides

Plusieurs techniques peuvent parfois s'appliquer afin de résoudre un problème de reconnaissance des formes. Chacune d'entre elles possède évidemment ses points forts et ses points faibles qui, dans la majorité des cas, dépendent des situations (pose, éclairage,

expressions faciales,….). Il est par ailleurs possible d'utiliser une combinaison de classificateurs basés sur des techniques variées dans le but d'unir les forces de chacun et ainsi pallier à leurs faiblesses [46].

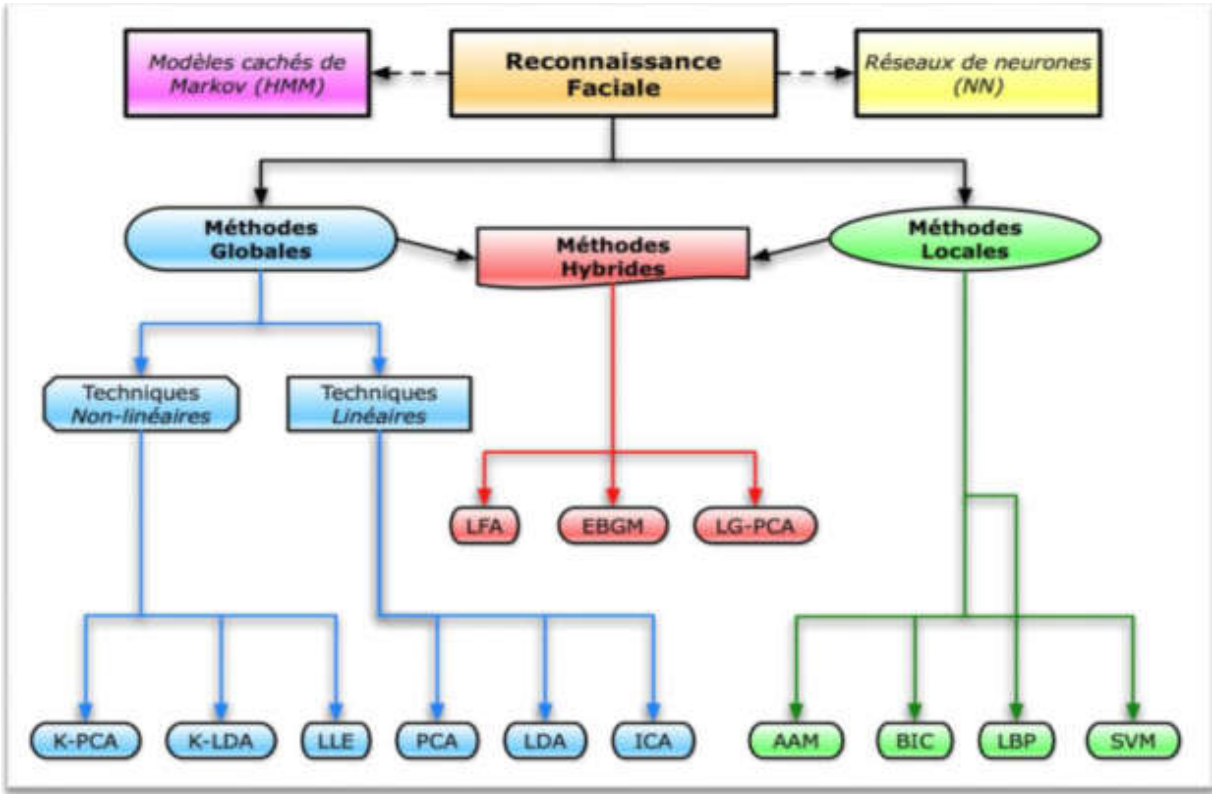

Fig. II.6 : Une classification des algorithmes principaux utilisés en reconnaissance faciale.

II .5 Les techniques utilisées pour la reconnaissance de visages

II .5.1Analyse en Composantes Principales(ACP)

L'algorithme PCA est né des travaux de MA. Turk et AP.Pentland au MIT Media Lab, en 1991[19,20]. L'idée principale consiste à exprimer les M images de départ selon une base de vecteurs orthogonaux particuliers „" les vecteurs propres „" 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. Le but est d'extraire l'information caractéristique d'une image de visage en utilisant la KLT ou la DCT, pour l'encoder aussi efficacement que possible afin de la comparer à une base de données de modèles encodés de manière similaire [47].

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. Donc, la PCA ne

nécessite aucune connaissance à priori sur l'image et se révèle plus efficace lorsqu'elle est couplée à la mesure de distance Mah Cosine, mais sa simplicité à mettre en œuvre contraste avec une forte sensibilité aux changements d'éclairement, de pose et d'expression faciale **[**48**]**.

Il existe plusieurs méthode qui basée sur la technique PCA comme la méthode « eigenface ». Son principe est le suivant : étant donné un ensemble d'images de visages exemples, il s'agit tout d'abord de trouver les composantes principales de ces visages. Ceci revient à déterminer les vecteurs propres de la matrice de covariance formée par l'ensemble des images exemples. Chaque visage exemple peut alors être décrit par une combinaison linéaire de ces vecteurs propres. Pour construire la matrice de covariance, chaque image de visage est transformée en vecteur. Chaque élément du vecteur correspond à l'intensité lumineuse d'un pixel.

Dans **[**49**]**, les auteurs ont démontré que la matrice de covariance C peut s'écrire :

$$C = CI + CE$$

C'est-à-dire qu'elle est égale à la somme de la matrice de dispersion intra-personne CI et la matrice de dispersion inter-personne CE.

Dans le cas d'un seul exemple d'apprentissage par personne, CI = 0, et donc l'équation se réduit à CE. L'Eigen face estimé à partir de la matrice CE seulement n'est pas fiable, parce qu'il ne peut pas différencier de manière efficace l'erreur d'identification des autres erreurs dues à la transformation et au bruit. Pour illustrer l'influence du nombre d'exemples d'apprentissage par personne sur les performances de la reconnaissance, les auteurs ont utilisé la base de données ORL **[**50**]** comme base de test. La base de données ORL contient des images de 40 individus, chacun étant enregistré sous 10 vues différentes. Dans leur expérimentation, les auteurs ont fixé le nombre de visages de test. Par contre, ils ont fait varier le nombre de visages d'apprentissage. Ainsi, pour chaque personne, ils ont utilisé la dernière image (Fig. II .7) pour le test et ont choisi aléatoirement les n premières images (n <= 9) pour l'apprentissage. Cette procédure a été répétée vingt fois.

Fig. II.7: Les dix vues d'une personne dans la base de données ORL.

Dans le cas extrême, si seulement un exemple d'apprentissage par personne est utilisé, le taux d'identification moyen de l'Eigen face tombe en dessous de 65 %. Ce taux atteint 95 % quand on utilise neuf exemples d'apprentissage par personne.

II .5.2 Analyse en Composantes Indépendantes(ACI)

L'analyse en composantes indépendantes peut être assimilée à un problème de séparation de sources comme initialement formulé dans [51] dans le sens où elle permet extraire les structures fondamentales d'une image. Cette méthode, appliquée au problème d'identification de visages, peut également être vue comme une généralisation de la méthode ACP car elle permet non seulement de minimiser les dépendances statistiques de second ordre (covariance) mais également celles d'ordre supérieur. Tout comme l'ACP.

L'ACI permet une projection linéaire des données dans un espace de plus petite dimension, mais cet espace, contrairement à l'espace des visages, n'est pas nécessairement orthogonal et permet une meilleure représentation des données [52]. L'approche consiste donc à considérer une matrice X (les images de visage) comme étant une combinaison linéaire et des sources «s» telle que :

$$Xt = Ast \qquad (2.1)$$

Où A est la matrice de mélange. On peut également définir une matrice de séparation W qui permet à partir des images X (observations) d'estimer les sources s telles que :

$$Ut = Wxt = WAst \qquad (2.2)$$

Où u correspond à l'estimation de la source s. Le but de l'ACI est donc de trouver une estimation de la matrice de mélange A ou de séparation W ainsi qu'une estimation de la matrice des sources S en réduisant au minimum la dépendance de ses composantes.

II .5.3 Analyse Linéaire Discriminante de Fischer (LDA)

La méthode ACP présentée précédemment traite les changements d'apparence du visage dans leur globalité. En effet, l'analyse en composantes principales est effectuée sur des données d'apprentissage non étiquetées et ne permet donc pas de différencier les variations intra individus et les variations extra-individus. L'Analyse Discriminante Linéaire permet, à partir de données d'apprentissage labellisées, de maximiser les variations extra-classe tout en minimisant les variations intra-classe. L'application de l'Analyse Discriminante Linéaire à la reconnaissance de visage a été proposée par Belhumeur et al. [53] en 1997.

Pour cela, l'ensemble des visages d'apprentissage sont annotés pour effectuer un apprentissage supervisé (Chacune de ces images est associée à une classe). Une classe est associée à un individu et contient toutes les images relatives à celui-ci. De plus, les classes ainsi définies doivent être composées d'au moins deux images.

L'image moyenne de chacune des classes c_i, notée$\overline{Ici}$, est définie par :

$$\overline{Ici} = \frac{1}{Nci}\sum_{i=1}^{Nci} Ii \qquad (2.3)$$

Avec N_{ci} le nombre d'images relatifs à la classe *ci*.

De manière similaire au paragraphe précédent, l'image moyenne des N_c classes d'apprentissage est notée $\bar{I}$. Elle est définie par :

$$\bar{I} = \frac{1}{Nc}\sum_{i=1}^{Nc} Nci\ \overline{Ici} \qquad (2.4)$$

Les variations interclasse (between class) Sb et intra-classe (within class) Sw sont alors définies ainsi :

$$\mathrm{Sb} = \sum_{i=1}^{Nc} Nc(\overline{\overline{Ici} - \bar{I}})\ (\overline{\overline{Ici} - \bar{I}})^t \qquad (2.5)$$

$$\mathrm{Sw} = \sum_{i=1}^{Nc}\sum_{1\in ci} \mathrm{Nc}(\mathrm{I} - \overline{Ici})\ (I - \overline{Ici})^t \qquad (2.6)$$

L'analyse discriminante linéaire propose alors de trouver la matrice de projection optimale permettant de maximiser Sb tout en minimisant Sw. Cela revient donc à chercher ζ^m maximisant le critère suivant (appelé critère d'optimisation de Fisher) :

$$\zeta^m = \arg\max_{\zeta}\left(\frac{\zeta^t S_b \zeta}{\zeta^t S_w \zeta}\right) \qquad (2.7)$$

Une fois ce nouvel espace défini, la comparaison entre deux images est faite de manière similaire aux EigenFaces : Le score de similarité entre deux visages est donné par la distance entre leur projection dans ce nouvel espace de représentation des visages.

II .5.4 Le Model Discriminant linéaire amélioré de Fisher (EFM)

Ce modèle discriminant linéaire de Fisher améliore la capacité de généralisation de la FLD en décomposant la procédure FLD en diagonalisation simultanée des deux matrices de dispersion intra-classe et interclasse. La diagonalisation simultanée est une étape sagement équivalente à deux opérations comme l'a souligné Fukunaga .Blanchiment de la matrice de dispersion intra-classe et l'application de l'ACP sur la matrice de dispersion interclasse en utilisant les données

transformées. Durant l'opération du blanchiment de la matrice de dispersion intra-classe apparaisse dans le dénominateur de la séparabilité des petites valeurs propres qui tendent à capturer du bruit. Pour atteindre des performances améliorées l'EFM préserve un équilibre approprié entre la sélection des valeurs propres (correspondant à la composante principale de l'espace de l'image originale) qui tiennent compte de la plupart de l'énergie spectrale des données brutes, c'est à dire, représentation adéquate et l'exigence que les valeurs propres de la matrice de dispersion intra-classe (de l'espace ACP réduit) ne sont pas trop p tites , c'est-à-dire une meilleure généralisation. Le choix de rang des composantes principales (m) pour la réduction de la dimension, prend en compte de l'ordre de grandeur de l'énergie spectrale. Les valeurs propres de la matrice de covariance fournissent un bon indicateur pour répondre au critère de l'énergie. Il faut ensuite calculer les valeurs propres de la matrices de dispersion intra-classe dans l'espace ACP réduit pour faciliter le choix du rang des composantes principales de sorte que l'exigence de grandeur est respectée[54] .

II .5.5 La méthode 'Mean and Standard déviation'(MS)

C'est une technique nouvelle qui a été proposée par notre encadreur m.Fedias elle repose sur les statistiques d'ordre un (la moyenne, l'écart type, le skewness et kurtosis) pour la reconnaissance de visage. On a appliquée cet test à l'image de visage si on considère l'image de visage comme une matrice où chaque ligne et colonne représentent une collection des nombres qui sont caractérisée par une certaine quantité descriptive statistiques d'ordre un comme la moyenne, l'écart type, les moments d'ordre 3 et les moments d'ordre 4…etc. donc le vecteur caractéristique pour chaque image de visage est la combinaison de ces quantités descriptives de chaque ligne et colonne de l'image **[**55**]**.

La méthode MS déroule comme suit :

Soit A = (x1x2...xi ...x N) représente une matrice de donnée de dimension (n× N) où chaque xi est un vecteur visage de dimension n. Ici n représente le nombre d'élément dans le vecteur caractéristique de l'image de visage et N est le nombre d'images de visages dans l'ensemble d'apprentissage. Le vecteur caractéristique xi est la combinaison des quantités descriptives statistiques de chaque ligne et colonne de l'image. Donc par l'application de cette méthode, le vecteur visage d'entrée de dimension (r×c) est réduit à un vecteur caractéristique de dimension n = (q×(r + c)). Ici q représente le nombre des quantités descriptives statistiques, (r,c) sont respectivement le nombre des lignes et colonnes dans l'image de visage. Nous présentant ici certaines quantités descriptives statistiques d'ordre un:

a. La Moyenne

La moyenne arithmétique est définit par :

$$\boldsymbol{\mu} = \frac{\sum_{i=1}^{n} x_i}{n} \qquad (2.8)$$

b. La Variance

La variance est une quantité importante définit par :

$$\mathbf{Var} = \frac{\sum_{i=1}^{n}(x_i-\mu)^2}{n} \qquad (2.9)$$

c. L'écart type

L'écart type est la racine carrée de la variance:

$$\boldsymbol{\sigma} = \sqrt{\frac{\sum_{i=1}^{n}(x_i-\mu)^2}{n}} \qquad (2.10)$$

d. Moment d'ordre 3 (Skewness)

$$\mathbf{S} = \frac{\sum_{i=1}^{n}(x_i-\mu)^3}{n} \qquad (2.11)$$

e. Kurtosis

$$\mathbf{K} = \frac{\sum_{i=1}^{n}(x_i-\mu)^4}{n} \qquad (2.12)$$

Puis nous faisons la photo normalisation. Cela veut dire simplement que pour chaque vecteur caractéristique, nous soustrayons à chaque élément la valeur moyenne de ceux-ci sur le vecteur caractéristique, et que nous divisons ceux-ci par leur déviation standard. La photo normalisation à un double effet : d'une part elle supprime pour tout vecteur un éventuel décalage par rapport à l'origine, et ensuite tout effet d'amplification. Finalement on applique la normalisation qui agit sur l'ensemble d'apprentissage (pour chaque composante, on retire la moyenne de cette composante pour tous les vecteurs caractéristiques et on divise par la déviation standard). La photo normalisation est définit par :

$$\mathbf{phot}\,(\mathbf{x}) = \frac{\mathbf{x}-\boldsymbol{\mu}_{\mathbf{x}}}{\boldsymbol{\sigma}_{\mathbf{x}}} \qquad (2.13)$$

Les figures II.8 et II.9 représentent la moyenne et l'écart type d'une image de visage.

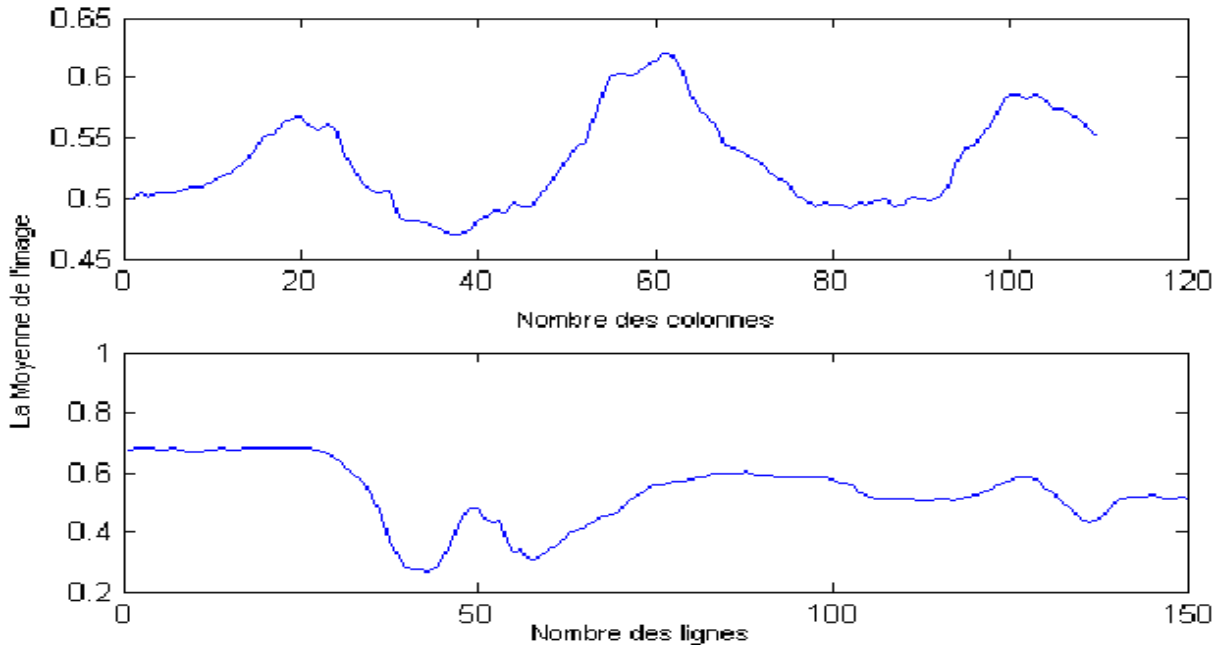

Fig. II.8: Moyenne de l'image de visage.

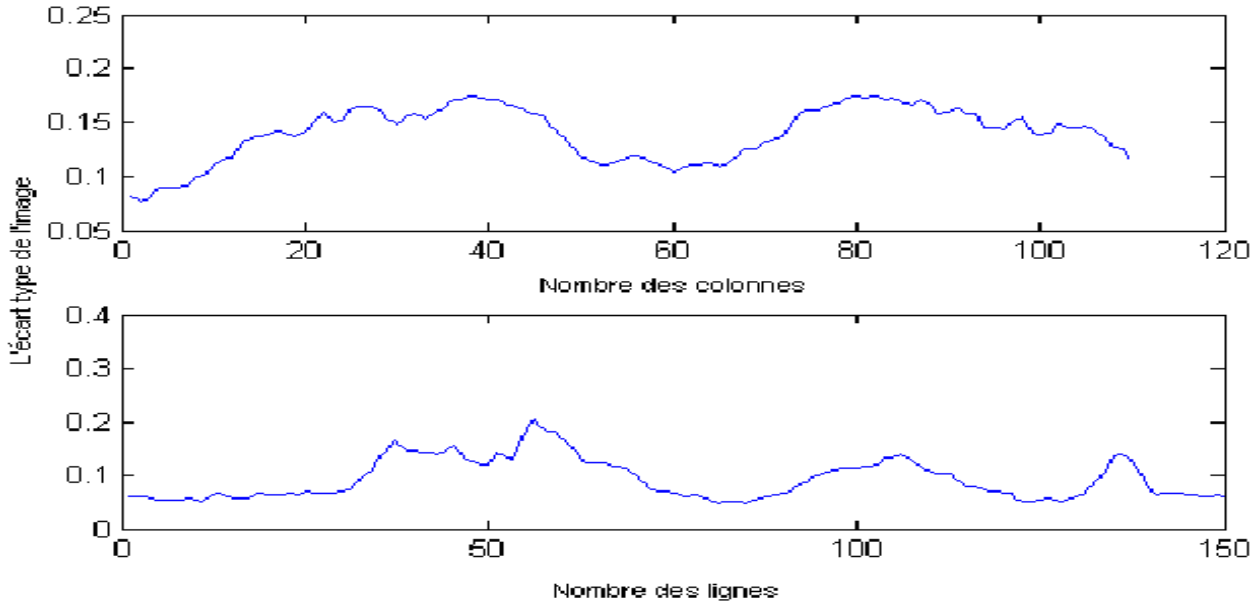

Fig. II.9:L'écart type de l'image de visage.

Le principe de ce système d'authentification de visage est l'extraction d'un vecteur caractéristique d'un individu, afin de le comparer avec un vecteur qui contient les caractéristiques de ce même individu extrait à partir de ses images qui sont stockés dans une base de données. L'intérêt de cette méthode repose sur sa rapidité et sa simplicité et surtout sa souplesse en cas d'ajouts d'images ou de personnes. En effet, cette opération n'implique donc aucun réapprentissage complet, contrairement aux méthodes comme l'ACP, LDA et EFM. Aussi les ressources requises par cette méthode ne concernent que la liste des représentations

vectorielles des quantités statistiques simples, ce qui résulte en une très faible consommation de mémoire.

La figure suivante présente le vecteur caractéristique qui est formé par la combinaison entre la moyenne et l'écart type de chaque ligne et colonne d'une seule image de visage.

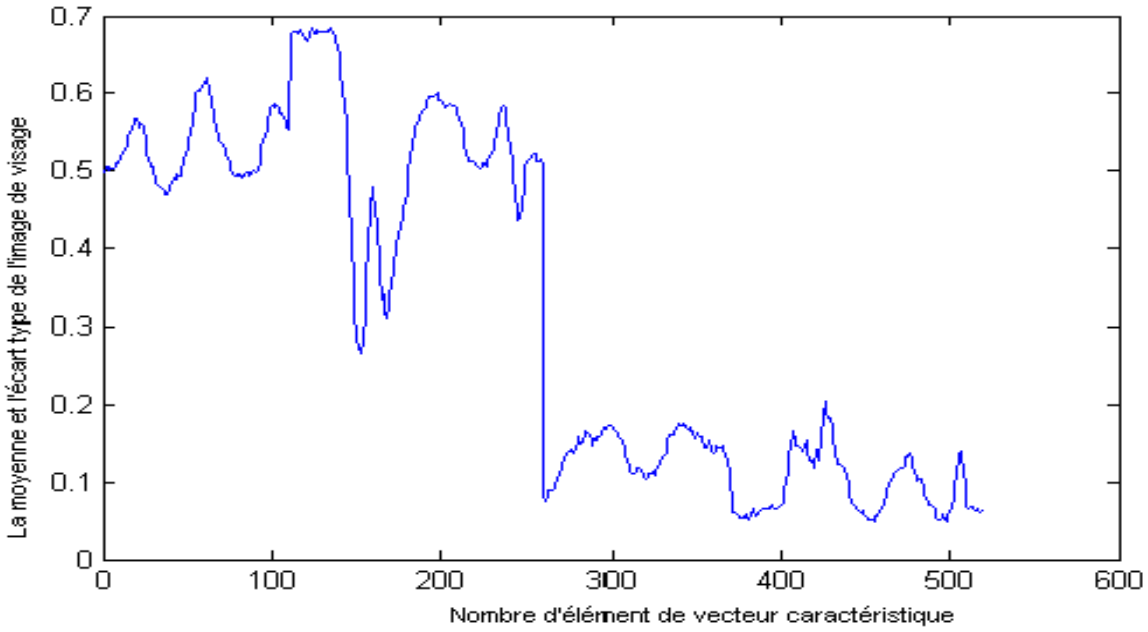

Fig. II.10. Le vecteur caractéristique en combinant la moyenne et l'écart type.

Encore on peut utiliser l'écart type de chaque ligne et colonne de l'image de visage pour la détection des zones de visage humaines comme les yeux la bouche et le nez. Et qui sont localisée aux valeurs maximales de l'écart type. La figure suivante explique sa clairement.

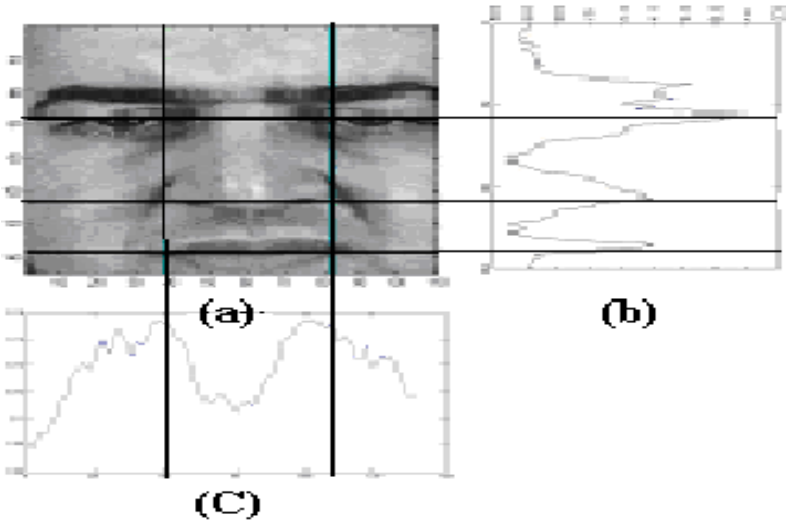

Fig. II.11: (a) image de visage (b) l'écart type verticale (c) l'écart type horizontale.

On remarque que cette méthode de détection est intéressante, simple et rapide pour chercher les positions des différentes parties de visage humain.

II .6 Difficultés de la reconnaissance de visages

Pour le cerveau humain, le processus de la reconnaissance de visages est une tâche visuelle de haut niveau. Bien que les êtres humains puissent détecter et identifier des visages dans une scène sans beaucoup de peine, construire un système automatique qui accomplit de telles tâches représente un sérieux défi. Ce défi est d'autant plus grand lorsque les conditions d'acquisition des images sont très variables. Il existe deux types de variations associées aux images de visages : inter et intra sujet. La variation inter-sujette est limitée à cause de la ressemblance physique entre les individus. Par contre la variation intra sujette est plus vaste. Elle peut être attribuée à plusieurs facteurs que nous analysons ci-dessous.

II.6.1 Changement d'illumination

L'apparence d'un visage dans une image varie énormément en fonction de l'illumination de la scène lors de la prise de vue (voir Fig. II .12). Les variations d'éclairage rendent la tâche de reconnaissance de visage très difficile. En effet, le changement d'apparence d'un visage du à l'illumination, se révèle parfois plus critique que la différence physique entre les individus, et peut entraîner une mauvaise classification des images d'entrée. Ceci a été expérimentalement observé dans Adini et al **[**56**]** où les auteurs ont utilisé une base de données de 25 individus. L'identification de visage dans un environnement non contrôlé reste donc un domaine de recherche ouvert. Les évaluations FRVT **[**57**]** ont révélé que le problème de variation d'illumination constitue un défi majeur pour la reconnaissance faciale.

Fig. II.12 : Exemple de variation d'éclairage.

II.6.2 Variation de pose

Le taux de reconnaissance de visage baisse considérablement quand des variations de pose sont présentes dans les images. Cette difficulté a été démontrée par des tests d'évaluation élaborés sur les bases FERET et FRVT **[**57**]** **[**58**]**. La variation de pose est considérée

comme un problème majeur pour les systèmes de reconnaissance faciale. Quand le visage est de profil dans le plan image (orientation < 30°), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30°, la normalisation géométrique n'est plus possible (voir Fig. II .13).

Fig. II .13: Exemples de variation de poses.

II.6.3 Expressions faciales

Un autre facteur qui affecte l'apparence du visage est l'expression faciale (voir Fig. II .14). La déformation du visage qui est due aux expressions faciales est localisée principalement sur la partie inférieure du visage. L'information faciale se situant dans la partie supérieure du visage reste quasi invariable. Elle est généralement suffisante pour effectuer une identification. Toutefois, étant donné que l'expression faciale modifie l'aspect du visage, elle entraîne forcément une diminution du taux de reconnaissance. L'identification de visage avec expression faciale est un problème difficile qui est toujours d'actualité et qui reste non résolu. L'information temporelle fournit une connaissance additionnelle significative qui peut être utilisée pour résoudre ce problème **[**59**]**.

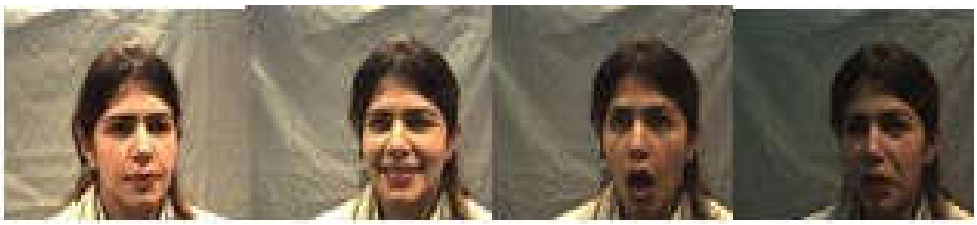

Fig. II .14: Exemples de variation d'expressions.

II.6.4 Présence ou absence des composants structurels

La présence des composants structurels telle que la barbe, la moustache, ou bien les lunettes peut modifier énormément les caractéristiques faciales telles que la forme, la couleur, ou la taille du visage. De plus, ces composants peuvent cacher les caractéristiques faciales de base causant ainsi une défaillance du système de reconnaissance. Par exemple,

des lunettes opaques ne permettent pas de bien distinguer la forme et la couleur des yeux, et une moustache ou une barbe modifie la forme du visage.

Fig. II .15: exemple de présence des Composants structurels

II.6.5 Occultations partielles

Le visage peut être partiellement masqué par des objets dans la scène, ou par le port d'accessoire tels que lunettes, écharpe... Dans le contexte de la biométrie, les systèmes proposés doivent être non intrusifs c'est-à-dire qu'on ne doit pas compter sur une coopération active du sujet. Par conséquent, il est important de savoir reconnaître des visages partiellement occultés. Gross et al **[**59**]** ont étudié l'impact du port de lunettes de soleil, et du cache-nez occultant la partie inférieure du visage sur la reconnaissance faciale. Ils ont utilisé la base de données AR **[**60**]**. Leurs résultats expérimentaux semblent indiquer que, dans ces conditions, les performances des algorithmes de reconnaissance restent faibles.

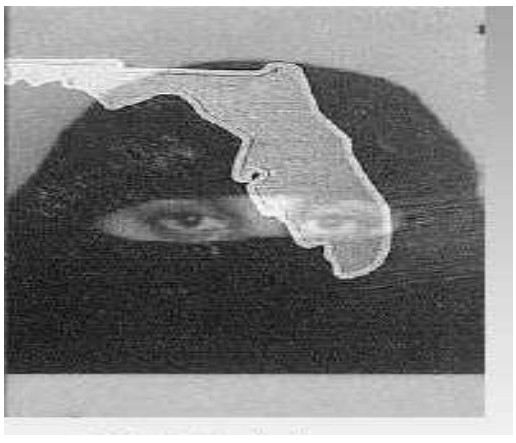

Fig. II .16: exemple d'occultation partielle.

II.7 Conclusion:

Dans ce chapitre, nous avons présenté les technologies utilisées dans les systèmes biométriques pour l'identification de personnes. Nous avons aussi donné un aperçu sur les techniques de mesure de leurs performances. Cette étude nous a permis de constater que la reconnaissance de visage suscite de plus en plus l'intérêt de la communauté scientifique, car elle présente plusieurs challenges et verrous technologiques. Enfin, nous avons mis en évidence les différentes difficultés inhérentes à la reconnaissance automatique de visages, ce qui nous a permis de bien définir les problématiques traitées dans cette mémoire, notamment l'invariance à l'illumination.

Chapitre III

L'information couleur

III.1. Introduction

Les systèmes d'authentification de visage utilisent souvent l'image de visage représentée en niveau de gris comme caractéristique d'entrée. Mais dans ce travail, nous proposons d'utiliser l'information de couleur comme caractéristique pour l'image de visage pour améliorer les performances de ces systèmes d'authentification. En cette partie, nous donnons une définition des espaces couleurs utilisée dans ce travail avec quelques concepts relatifs avec leur RGB, XYZ, HSV, I1I2I3, YCrCb, YUV et YIQ.

III.2 Les espace couleurs

Une couleur est généralement représentée par trois composantes. Ces composantes définissent un espace des couleurs. On peut citer l'espace RGB, l'espace CIE XYZ ou xyz .Selon l'espace de couleurs choisi pour représenter une image couleur, le nuage des couleurs (c'est à dire l'ensemble des couleurs de l'image) n'aura pas la même répartition dans l'espace 3D. Les espaces de couleurs classiques, tels que le RVB, CIE XYZ, etc. ..., sont issus d'une approche purement physique, sans prise en compte de données psychophysiques.

III.2.1 L'espace de couleur RGB

Le système (RC, GC, BC) de la CIE (Commission Internationale pour l'Eclairage), défini en 1931, découle des expériences d'égalisation menées par Wright et Guild qui utilisent les trois primaires, notées respectivement RC, GC et BC, comme les stimuli de couleur monochromatiques rouge, vert et bleu de longueurs d'onde respectives 700,0 nm, 546,1 nm et 435, 8 nm pour reproduire l'ensemble des couleurs du spectre visible [55].

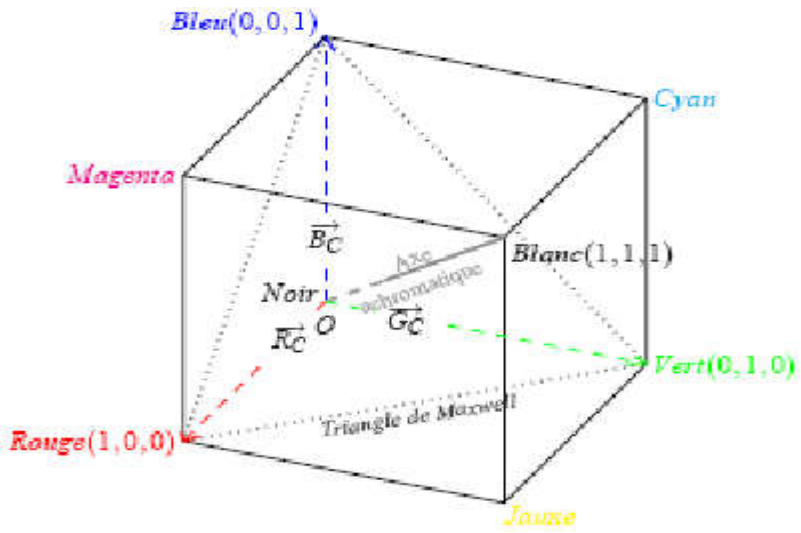

Fig. III.1: Cube des Couleurs.

Mais on trouve que l'espace RGB défini par la CIE présente quelques inconvénients comme l'existence d'une partie négative (Fig. III.2) dans les spectres et par conséquent, l'impossibilité de reproduire un certain nombre de couleurs par superposition des trois spectres. Aussi Les valeurs des composantes trichromatiques sont liées à la luminance qui est une combinaison linéaire des composantes trichromatiques et non une composante elles même. Et l'existence d'une multitude de systèmes [R∗, G∗, B∗] comme (CIE, NTCS, PAL…etc.).

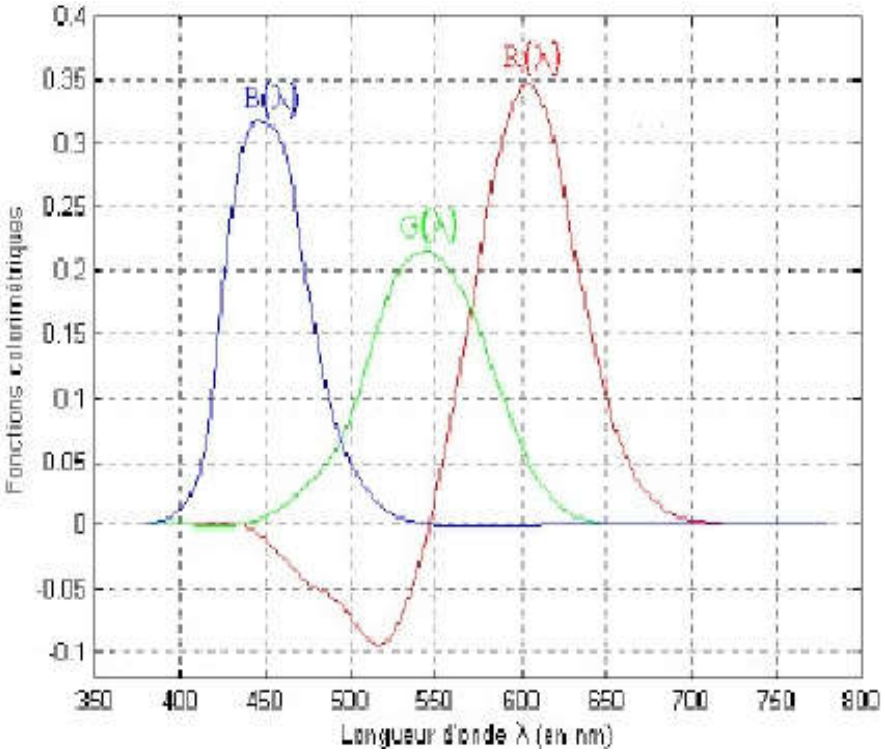

Fig. III.2: Les courbes d'appariement R(λ), G(λ) et B(λ) correspondant aux Expériences d'égalisation avec standardisées par la CIE en 1931.

Afin de pallier ces inconvénients, la CIE a défini un espace de représentation de la couleur basée sur trois primaires non visibles X, Y et Z. Cet espace est traité dans la section suivante.

III.2.2 L'espace de couleur XYZ

En 1931, la CIE établit le système de référence colorimétrique (X, Y, Z) qui a été défini afin de corriger certains défauts de l'espace RGB. Les primaires [X], [Y] et [Z], dites primaires de référence, ont été créées de telle sorte que toutes les couleurs soient exprimées par des composantes trichromatiques positives (Fig. III.3) et de telle sorte que l'une de ces primaires, la primaire [Y], représente une information de luminosité et le X et le Z les deux chrominances, Y étant indépendant de X et Z**[**55**]**.

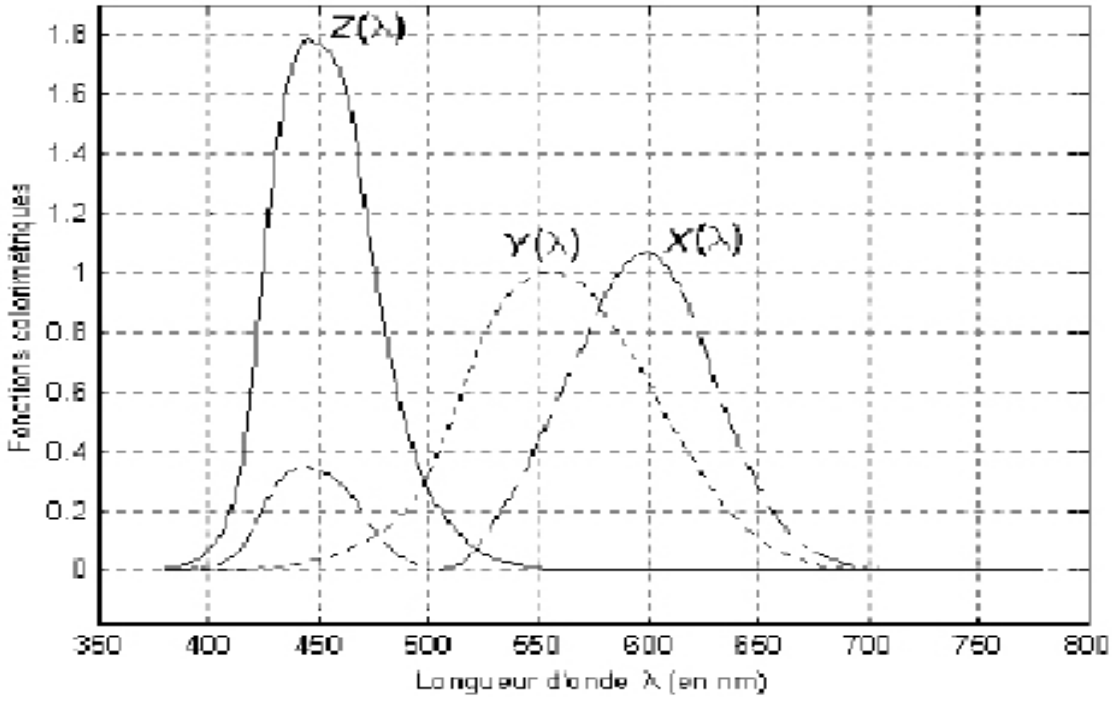

Fig. III.3: Les fonctions colorimétriques X(λ), Y(λ) et Z(λ).

L'espace CIE XYZ dispose d'un grand nombre de propriétés intéressantes:

• deux couleurs de mêmes coordonnées XYZ apparaissent comme identiques

• deux couleurs de coordonnées XYZ différentes apparaissent différentes.

• la couleur XYZ de tout objet peut être mesurée objectivement.

Le système (X, Y, Z) correspond donc à un changement de primaires et s'obtient ainsi à l'aide d'une simple matrice de passage à partir du système (R, G, B) suivante :

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 2.7690 & 1.7518 & 1.1300 \\ 1.0000 & 4.5907 & 0.0601 \\ 0.0000 & 0.0565 & 5.5943 \end{pmatrix} \begin{pmatrix} R \\ V \\ B \end{pmatrix}$$

III.2.3 L'espace de couleur HSV

L'espace HSV est un système de cône hexagonal qui représente la couleur sous la forme d'un triplé : teinte H (Hue), saturation S (Saturation) et luminosité V (Value). Les transformations sont effectuées comme suit [61].

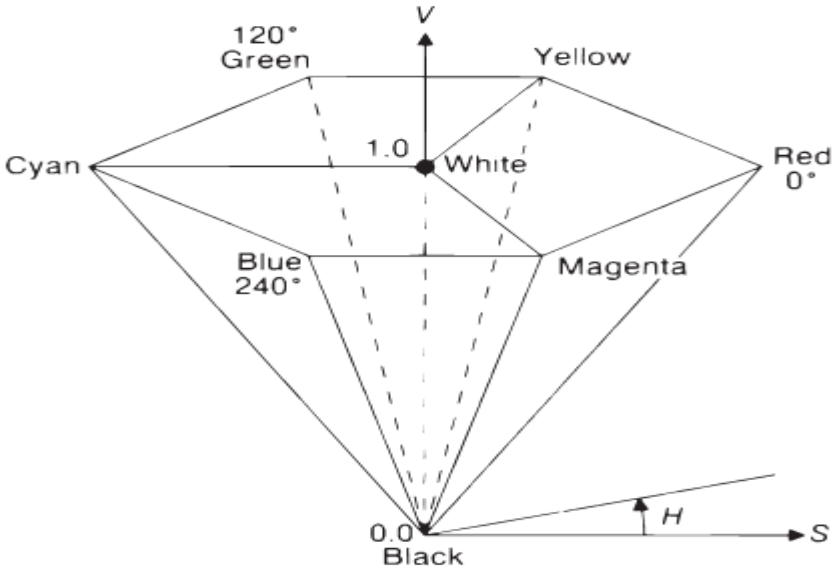

Fig. III.4: Espace de couleur HSV**.**

Conversion RGB → HSV

On suppose que *R, G, B* appartiennent à [0, 1] :

$$H = \frac{\pi}{3}\begin{cases} \frac{G-B}{\max - \min} & \text{si } R = \max \\ 2 + \frac{B-R}{\max - \min} & \text{si } G = \max \\ 4 + \frac{R-G}{\max - \min} & \text{si } B = \max \\ \emptyset & \text{si } \max = 0 \end{cases}$$

$$S = \begin{cases} \frac{\max - \min}{\max} & \text{si } \max = 0 \\ 0 & \text{sinon} \end{cases}$$

$$V = \max (R, G, B)$$

III.2.4 L'espace de couleur I1I2I3

En 1980, OHTA ET AL. [62] ont introduit un nouvel espace nommé I1I2I3 dans le but de produire une segmentation aussi satisfaisante que celle produite par la transformation de KARHUNEN-LOÉVE. A chaque étape de la segmentation, de nouvelles caractéristiques couleurs sont calculées par la transformation de KARHUNENLOÉVE des valeurs RGB. Les trois caractéristiques les plus significatives ont été retenues pour représenter les trois axes de

l'espace I1I2I3. Le passage du système RGB à ce système s'effectue par les équations suivantes**.**

$$\begin{bmatrix} I_1 \\ I_2 \\ I_3 \end{bmatrix} = \begin{bmatrix} 1/3 & 1/3 & 1/3 \\ 1/2 & 0 & -1/2 \\ -1/4 & 1/2 & -1/4 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

Où I1 représente la luminance, I2 et I3 correspondent respectivement une opposition bleu-rouge et magenta-vert.

III.2.5 L'espace de couleur YCrCb

Ce système a été à l'origine développé pour assurer une compatibilité entre les téléviseurs couleurs et les téléviseurs noir et blanc, d'où la séparation des composantes de luminance et de chrominance. Une simple transformation linéaire permet de passer d'un système RGB au système YCrCb, mais cette transformation diffère suivant les standards de télévision (NTSC,

PAL ou SECAM) **[**61**]**.

La forme générale des composantes chromatiques est donnée par :

$$\mathbf{Cb = a1(R - Y) + b1\ (B - Y)}$$

$$\mathbf{Cr = a2(R - Y) + b2\ (B - Y)}$$

Où les coefficients a1, a2, b1 et b2 sont spécifiques au standard considéré et Y est la luminance. Comme déjà souligné, il existe plusieurs systèmes de type YCrCb.

Le système YCbCr est utilisé pour les images JPEG. Ce modèle colorimétrique permet en effet de réduire la taille d'une image. Cette réduction se base sur la constatation suivante : l'œil humain est plus sensible à la luminance qu'à la chrominance.

$$\begin{pmatrix} Y \\ C_b \\ C_r \end{pmatrix} = \begin{pmatrix} 0{,}2220 & 0{,}7067 & 0{,}0713 \\ -0{,}1195 & -0{,}3810 & 0{,}5000 \\ 0{,}5000 & -0{,}4542 & -0{,}0458 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix}$$

III.2.6 L'espace de couleur YUV

Le signal YUV est créé depuis une source RGB (rouge, vert et bleu). Le signal U est obtenu en soustrayant le Y du signal bleu d'origine ; de façon similaire le V est obtenu en soustrayant Y du signal rouge. Ces opérations peuvent facilement être réalisées au moyen d'un circuit analogique **[**63**]**.Les équations suivantes peuvent être utilisées pour dériver Y, U et V à partir des composantes R, G et B : $(R, G, B, Y) \in [0 ; 1]$

$$U \in [-0{,}436 ; 0{,}436]$$

$$V \in [-0{,}615 ; 0{,}615]$$

Cependant, les limites autorisées sur U et V dépendent de Y. De RVB à YUV :

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

III.2.7 L'espace de couleur YIQ

Le modèle Y IQ diffère peu du modèle Y UV et tout comme le précédent, est utilisé dans les travaux d'ULTRÉ, LIANG, CLARAMONT ainsi que dans le standard vidéo NTSC. La transformation de l'espace RGB en l'espace Y IQ est donnée par les relations suivantes **[**64**]** :

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.275 & -0.321 \\ 0.212 & -0.523 & 0.311 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

Où le paramètre Y représente la luminance, I l'interpolation et Q la quadrature. I et Q sont aussi les composantes chromatiques représentant respectivement les oppositions cyan-orange et magenta-bleu.

III.3 Conclusion

Dans ce chapitre nous avons présente les espaces couleur utilisée dans notre travail**.**

En pratique il n'y a pas d'espace couleur idéal pour toutes les applications d'imagerie. L'espace à choisir dépend du traitement à effectuer et ici on parle de la reconnaissance de visage. Dans le prochain chapitre nous discuterons sur la base XM2VTS avec la méthode MS appliquée aux différentes espaces de couleurs utilise.

Chapitre IV

Les Résultats et discussion

IV.1. Introduction

Dans ce chapitre on a testé l'approches sur des images de la base de données XM2VTS selon son protocole associe (protocole de Lausanne). Aussi nous avons prouvé que l'information couleur augmente la performance de système d'authentification. Pour cela nous avons appliqué ce techniques pratiquement et voir ainsi les avantages et les inconvénients de cette algorithme et surtout en termes de taux de réussite et temps de calcul pour le processus de l'authentification de visage. En effet, la performance den ces algorithmes dépend beaucoup de la qualité des résultats de détection et de normalisation des visages.

IV.2.La base de données XM2VTS

XM2VTS est une base de données multimodale publiquement disponible enregistrée spécifiquement pour évaluer les exécutions des approches biométriques à la vérification d'identité. Elle contient 8 images par visage de 295 personnes. Les sujets ont été enregistrés en quatre sessions séparées distribuées pendant 5 mois. Le protocole expérimental standard lié à la base de données divise la base de données en 200 clients et 95 imposteurs. Les sujets sont des deux sexes, proviennent de diverses ethnies et de catégories d'âge différentes. Les photos sont en couleur, de haute résolution (format ppm : 256x256 pixels).

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 le protocole de Lausanne [65] la base de données est scindée en trois ensembles : ensemble d'apprentissage, ensemble de validation et ensemble de test. L'ensemble d'apprentissage est utilisé comme ensemble de référence .Il sert d'ensemble de base, maintenant ainsi l'information concernant les personnes connues du système. L'ensemble d'évaluation permet de fixer les paramètres du système de reconnaissance de visages. Enfin, l'ensemble de test permet de tester le système en lui présentant des images de personnes lui étant totalement inconnues. En fait, la base de données est divisée en deux classes : clients est imposteurs. L'ensemble d'apprentissage ne contient que des clients. Les imposteurs sont répartis dans les deux autres ensembles, à raison de 25 pour l'ensemble d'évaluation et 70 pour l'ensemble de test. La répartition des images dans les différents ensembles est décrite par la Fig. IV.1 [65].

<table>
<tr><th>Session</th><th>Pause</th><th>Clients</th><th colspan="2">Imposteurs</th></tr>
<tr><td rowspan="2">1</td><td>1</td><td>Apprentissage</td><td rowspan="8">Evaluation</td><td rowspan="8">Test</td></tr>
<tr><td>2</td><td>Evaluation</td></tr>
<tr><td rowspan="2">2</td><td>1</td><td>Apprentissage</td></tr>
<tr><td>2</td><td>Evaluation</td></tr>
<tr><td rowspan="2">3</td><td>1</td><td>Apprentissage</td></tr>
<tr><td>2</td><td>Evaluation</td></tr>
<tr><td rowspan="2">4</td><td>1
2</td><td>Test</td></tr>
</table>

Fig. IV.1 : Configuration de la base de données

Les tailles des différents ensembles sont reprises dans le tableau 1.

Ensemble	Clients	Imposteurs
Apprentissage	600 images (3 par personne)	0 images
Evaluation	600 images (3 par personne)	200 images (8 par personne)
Test	200 images (3 par personne)	560 images (8 par personne)

Tab. IV.1 : Répartition des photos dans les différents ensembles

IV.3.Prétraitement

Le prétraitement dans le processus d'authentification est une phase nécessaire et importante pour une meilleure performance du système. Cela permet en première réduction des données et elle atténue les effets de différentes conditions lors des prises de vues. Dans cette phase le procède est comme suit :

Tout d'abord, on fait le découpage des images.

- En suit on utilise le filtrage (passe- bas (pour la décimation)).
- La décimation des images (réduire la résolution de l'image).
- Et en fin, l'application de la photo normalisation aux images, ce qui entraine la

Suppression de tout vecteur un éventuel décalage et supprime tout effet d'amplification.

IV.4.Classification

Le seuil définit la similarité minimale entre deux images pour reconnaître qu'il s'agit de la même personne, et cette ressemblance minimale, un suspect, sera exprimée par la distance maximale entre les propriétés des deux images. Nous avons deux catégories: les clients et les

imposteurs. Un système d'authentification extrêmement strict indique un TFA (Taux de Fausse Acceptation) faible et un TFR (Taux de Faux Rejet) élevé. Pour un système laxiste, le contraire est vrai. Le juste milieu situe quelque part entre les deux est quelque part et si les taux d'erreur sont égaux, ils seront au même taux d'erreur ou TEE. Dans le groupe d'évaluation, tous les taux d'erreur sont calculés, ce qui permet un contrôle plus ou moins TEE en modifiant les paramètres d'acceptation et de rejet du système. Dans un groupe de test, nous faisons la même chose en utilisant des paramètres prédéfinis. Ainsi, on vérifie la force du système d'authentification faciale.

IV.5. Mesure de similitude

Pour mesurer les similitudes, nous avons choisi la corrélation car elle fournit les meilleurs résultats par rapport à d'autres échelles de similarité et est mieux adaptée aux données volumineuses. Elle mesure le taux de changement entre les composantes de deux vecteurs A et B. Elle est donnée par la relation :

$$\mathrm{Corr}(A,B) = \sum_{i=1}^{N} \frac{(A_i - \mu_A)(B_i - \mu_B)}{\sigma_A \sigma_B}$$

Où : σ_A= l'écart type de A, μ_A= la moyenne de A_i

σ_B= l'écart type de B, μ_B= le moyenne de B_i

IV.6.Présentation les résultats de technique utilisée

La méthode MS consiste à extraire des statistiques d'ordre un de l'image faciale, telles que le moyenne, la variance, les moments d'ordre 3 (skewness) et les moments d'ordre 4 (kurtosis). Ces statistiques se combinent pour améliorer les performances du système d'authentification du visage, et nous allons simplement présenter les résultats ici. Le tableau présente les résultats de diverses statistiques obtenues pour la validation faciale et les groupes appliqués aux images en niveaux de gris. Nous avons choisi les paramètres suivants:

• Prétraitement avec photonormalisation.

• Mesure de la similarité: corrélation.

• Le seuil: global.

Statistique	Ensemble d'évaluation	Ensemble de test			
	TEE (%)	TFA (%)	TFR (%)	Taux de Succès TS (%)	Dimension de vecteur caractéristique
Moyenne	6.99	7.59	6.75	85.66	260
Ecart type	7.04	8.94	7.00	84.06	260
Skewness	7.81	8.09	9.75	82.16	260
Kurtosis	10.3	10.32	14.00	75.68	260
Variance	8.14	9.87	8.00	82.14	260
Moyenne et ecart type	5.47	5.77	4.75	89.48	520
Moyenne et Variance	10.03	9.37	12.25	78.38	520
Moyenne et Skewness	5.67	5.05	8.00	86.96	520
Moyenne et Kurtosis	5.51	5.75	8.75	85.50	520
Moyenne, variance, Skewness et Kurtosis	12.69	13.90	15.75	70.35	1040

Tab .IV.2: les résultats par les statistiques d'ordre un en niveaux de gris.

D'après les résultats a présentés dans le tableau IV.2. Nous remarquons l'utilisation de la moyenne seule donne le taux de succès 85.66 et l'écart type seule donne le taux de succès 84.06; Et nous avons obtenu une amélioration dans le taux de succès si nous faisons les combinaisons des différentes valeurs statistiques et qui donnent les résultats suivants : (moyenne et écart type) : 89.45%, (moyenne et varience): 86.96%, (moyenne et skewness): 85.50%et (moyenne et kurtosis): 70.35%.Nous remarque que la combinaison (moyenne et écart type) donne le meilleur taux de succès TS de l'ordre de 89.45% par rapport aux autres combinaisons, , cette méthode appeler (MS) .

- Les avantages de la méthode MS:

En effet, la méthode MS présente des fonctionnalités très intéressantes par rapport à la PCA. Ces avantages sont résumés dans les points suivants:

- Les taux d'erreurs de fausse acceptation et rejet dans l'ensemble d'évaluation et de test sont très proches cela veut dire un système plus stable et c'est une propriété très importante.
- La rapidité : la méthode ACP nécessitent un grand nombre de calcule pour l'extraction des valeurs propre d'une grande matrice de covariance. Par contre avec la méthode MS le nombre d'opérations à effectuer pour calculer le vecteur de caractéristique d'une image de visage est très inférieur.
- La souplesse avec les grandes bases de données : dans la méthode MS, l'opération d'apprentissage n'est pas répétée quand on modifie la base de données en présentant d'autres visages (clients). Par contre dans les autres méthodes, on doit répéter l'opération d'apprentissage chaque fois qu'on présente une personne (client) dans la base de données, parce que l'espace de projection change.
- Mémoire réduit : on n'a pas besoin un grand mémoire avec la méthode MS parce que l'extraction de vecteur caractéristique ce fait directement sur l'image de visage par contre la méthode ACP nécessitent cette grande mémoire pour la préservation de l'espace de projection.

Le tableau ci dessous montre le temps de calcule nécessaire (CPU time en second) pour le calcule de la matrice de projection pour l'ACP. Et le temps nécessaire pour l'extraction de caractéristique de chaque méthode, et le taux de succès de chaque approche sur la base de données XM2VTS

Méthode	Taux de succès TS (%)	Temps CPU pour la Matrice de Projection (s)	Temps CPU Pour extraction de caractéristique d'une image (s)
MS	89.48	/	0.09
ACP	89.16	47.84	0.120

Tab .IV.3: Comparaison des performances de MS et PCA Utilisant la base de données XM2VTS (Pentium 4, 1.6GHZ).

D'après ce tableau on observe que la méthode MS est mieux que ACP en terme de taux de succès et nécessite un peu du temps de calcul donc c'est la plus rapide et la plus simple entre

elles**.** Puisque MS donne un taux de réussite égale à 89.48% en niveaux de gris pour cela on a proposée d'introduire l'information couleur pour augmenter la performance de notre système.

❖ Les tableaux suivants illustrent les différents taux d'erreur de la méthode MS pour différentes espaces de couleur:

- Pour l'espace de couleur RGB:

Couleur		L'ensemble de test			
		TFR	TFA	TS (%)	
MS RGB	R	0.0650	0.0641	87.09	
	G	0.0500	0.0542	89.58	
	B	0.0675	0.0444	88.81	

Tab. IV.4: taux d'erreur de la méthode MS pour de couleur RGB.

- Pour l'espace de couleur HSV:

Couleur		L'ensemble de test			
		TFR	TFA	TS (%)	
MS HSV	H	0.2925	0.2945	41.30	
	S	0.0475	0.0481	90.44	
	V	0.0675	0.0612	87.13	

Tab. IV.5: taux d'erreur de la méthode MS pour de couleur HSV.

- Pour l'espace de couleur I1I2I3:

Couleur		L'ensemble de test		
		TFR	TFA	TS (%)
MS I1I2I3	I1	0.0475	0.0576	89.49
	I2	0.0625	0.0577	87.98
	I3	0.1025	0.0815	81.60

Tab. IV.6: taux d'erreur de la méthode MS pour de couleur I1I2I3.

- Pour l'espace de couleur XYZ:

Couleur		L'ensemble de test		
		TFR	TFA	TS (%)
MS XYZ	X	0.0575	0.0593	88.32
	Y	0.0450	0.0578	89.72
	Z	0.0675	0.0454	88.71

Tab. IV.7: taux d'erreur de la méthode MS pour de couleur XYZ.

- Pour l'espace de couleur YUV:

Couleur		L'ensemble de test		
		TFR	TFA	TS (%)
MS YUV	Y	0.0475	0.0576	89.49
	U	0.0650	0.0496	88.54
	V	0.0600	0.0507	88.93

Tab. IV.8: taux d'erreur de la méthode MS pour de couleur YUV.

- Pour l'espace de couleur YCrCb:

Couleur		L'ensemble de test		
		TFR	TFA	TS (%)
MS YCrCb	Y	0.0475	0.0576	89.49
	Cr	0.0600	0.0506	88.94
	Cb	0.0650	0.0497	88.53

Tab. IV.9: taux d'erreur de la méthode MS pour de couleur YCrCb.

- Pour l'espace de couleur YIQ:

Couleur		L'ensemble de test		
		TFR	TFA	TS (%)
MS YIQ	Y	0.0475	0.0576	89.49
	I	0.0550	0.0526	89.24
	Q	0.1950	0.1463	65.87

Tab. IV.10: taux d'erreur de la méthode MS pour de couleur YIQ.

D'après les tableaux précédents, le résultat de la méthode MS de l'espace colorimétrique HSV donne la composante couleur S la meilleure avec un taux de réussite de 90,44%, suivie de la composante Y de l'espace colorimétrique XYZ avec un succès de 89,72%, la composante G de l'espace colorimétrique RGB à un taux de réussite de 89,58%. Et finalement la luminance des espaces couleurs I1I2I3, YUV, YIQ et YCrCb ont un taux de réussite d'environ 89,49%, est semblable avec le taux de succès de système en niveaux de gris**.**

IV.7 Conclusion:

Dans ce chapitre nous avons présenté la base de données des images des visages XM2VTS qui a été choisie grâce à sa popularité puisqu'elle est devenue une norme dans la communauté biométriques audio et visuelle de vérification d'identité afin de comparer les résultats obtenue de technique utilisé dans cet mémoire .Aussi nous avons implémenté de technique utilisé et les résultats obtenus sont satisfaisants et le système est stable par la technique utilisé. On a introduit l'information couleur pour la technique utilisé et on a prouvé l'efficacité de la couleur pour l'augmentation de la performance de système d'authentification de visage. La technique MS donne un taux de succès TS de 89.48% en niveaux de gris qui est comparables avec le taux de succès de L'ACP mais la méthode MS est plus rapide et simple.

Conclusion Générale

Conclusion générale

Dans ce mémoire, nous avons concentrés sur la biométrie de visage qui présente de nombreux avantages, tels que la facilité d'utilisation, l'acceptation par l'utilisateur et le faible coût. Ainsi, la reconnaissance faciale a déjà été intégrée dans des systèmes de sécurité biométriques utilisant un certain nombre d'algorithmes traditionnels. Malheureusement, ces algorithmes ont des limitations et des restrictions d'utilisation.

L'objectif de notre travail est de prouver l'importance de la couleur pour la validation faciale, car notre travail contribue à la mise au point d'un nouvel algorithme plus puissant, conçu pour identifier une personne à travers le visage.

Nous avons testé les performances de la méthode précédente sur la base de données XM2VTS conformément à son protocole associé au protocole de Lausanne. L'option principale de cette base de données est sa grande taille et sa popularité car elle est devenue un standard dans la communauté des médias audiovisuels pour la vérification de l'identité multimédia.

Les résultats obtenus sur l'efficacité chromatique de la méthode MS montrent que les performances du système d'authentification faciale sont améliorées, car elles sont plus rapides et plus faciles à mettre en œuvre et réduisent les données sans réduire de manière significative les performances du système d'authentification faciale.

Dans ce travail, le taux de réussite est de 89,48% avec une échelle de gris et le taux de réussite TS le plus élevé de 90,44% avec l'utilisation de la composante S de l'espace colorimétrique HSV.

Bibliographies

Bibliographies

[1] : ZITOUNI S.E, SACI A. (2016). Authentification et Identification biométrique des personnes par les empreintes palmaires. Université Kasdi Merbah Ouargla, Département de l'Electronique et de télécommunications.

[2] : Bedoui, L. (2008). Authentification de visages par la méthode d'analyse discriminante linaire de Fischer. Université Mohamed Kheider de Biskra, Ingnieur d'tat en Automatique.

[3]: D. John .Woodward, jr., (2003). Christopher horn Julius gatune, and aryn thomas, "biometrics a look at facial recognition", documented briefing by rand Public Safety and justice for the Virginia state crime commission.

[4]: El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010, October). A study of users' acceptance and satisfaction of biometric systems. In 44th Annual 2010 IEEE International Carnahan Conference on Security Technology (pp. 170-178). IEEE.

[5]: Giot, R., El-Abed, M., & Rosenberger, C. (2010, June). Fast learning for multibiometrics systems using genetic algorithms. In 2010 International Conference on High Performance Computing & Simulation (pp. 266-273). IEEE.

[6]: Giot, R., El-Abed, M., & Rosenberger, C. (2009, May). Keystroke dynamics authentication for collaborative systems. In 2009 International Symposium on Collaborative Technologies and Systems (pp. 172-179). IEEE.

[7] :El-Abed, M.(2011). Évaluation de système biométrique (Doctoral dissertation, Université de Caen).

[8] :Adhami, R., & Meenen, P. (2001). Fingerprinting for security. IEEE Potentials, 20(3), 33-38.

[9]: Chellappa, R., Wilson, C. L., & Sirohey, S. (1995). Human and machine recognition of faces: A survey. Proceedings of the IEEE, 83(5), 705-740.

[10]: Zhao, W., Chellappa, R., & Philips, P. (2000). Face Recognition: A Literature Survey UMD CAR. Technical Report CARTR.

[11]: Koenig, B. E. (1986). Spectrographic voice identification: a forensic survey. The Journal of the Acoustical Society of America, 79(6), 2088-2090.

[12]: International Biometric Group. Http: //www.biometricgroup.com/, 2010. [Cite p. 11, 15, 154].

[13] : BENCHENNANE, I. (2015). Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus (Doctoral dissertation, University of sciences and technology in Oran**.**

[14]: [IBG] International Biometric Group - www.biometricgroup.com/.

[15]: Morizet, N. (2009). Reconnaissance biométrique par fusion multimodale du visage et de l'iris (Doctoral dissertation, Télécom ParisTech).

[16]: Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. IT Professional, 3(1), 27-32.

[17]: Pankanti, S., Jain, A., & Hong, L. (2000). Biometrics: Promising frontiers for emerging identification market. Comm. ACM, 91-98.

[18] : Fredouille, C., Mariéthoz, J., Jaboulet, C., Hennebert, J., Mokbet, J. F., & Bimbot, F. (2000). Behavior of a bayesian adaptation method for incremental enrollment in speaker verification. In 2000 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 00CH37100) (Vol. 2, pp. II1197-II1200). IEEE.

[19]: Heck, L. P., & Mirghafori, N. (2000). On-line unsupervised adaptation in speaker verification. In Sixth International Conference on Spoken Language Processing.

[20]: Wayman, J. L. (2001). Fundamentals of biometric authentication technologies. International Journal of Image and Graphics, 1(01), 93-113.

[21]: Kharroubi, J. (2002). Etude de techniques de classement" Machines à vecteurs supports" pour la vérification automatique du locuteur (Doctoral dissertation, Télécom Paris Tech).

[22]: Soltani, S., & Bendaoud, M. R. (2018). Reconnaissance biométhrique multimodale basée sur la dimension fractale.

[23] : Réda, A. D. J. O. U. D. I. Authentification automatique par identification et reconnaissance dans un système de haute sécurité (Doctoral dissertation, Université de Sidi Bel Abbès-Djillali Liabes).

[24] : Chiheb, A. Reconnaissance de visages par Analyse Discriminante Linéaire (LDA).

[25] : MERIEM, F. (2006). L'apport de la couleur à la vérification d'identité à l'aide d'images de visage (Doctoral dissertation, Université de Biskra-Mohamed Khider).

[26] : Ouamane Abdelmalik et Mehdaoui Abdelghaffar, (2009). «identification et authentification des visages en biométrie», Mémoire de Fin d'Etudes, en vue de la préparation du diplôme: INGENIEUR, Département de Génie Electrique, Université Mohamed Keider Biskra,

[27] : Delalleau, O., & Pré-doctoral, E. (2008). Extraction hiérarchique de caractéristiques pour l'apprentissagea partir de données complexes en haute dimension. Pre-doctoral report, University of Montreal. Spall, James. C. (2005). Introduction to stochastic search and optimization: estimation, simulation, and control (Vol. 65). John Wiley & Sons.

[28] : Achour AbdErrazak et Hachani Samia. (2010) « Reconnaissance biométrique par la méthode ICA », Université Mohamed Kheider de Biskra -Ingénieur d'état en électronique.

[29] : AISSAOUI Azzedine et DJOUAMA Ala Eddine. (2011). «Détection de visage par la méthode SVM», Mémoire de Fin d'Etudes, en vue de la préparation du diplôme: MASTER, Département de Génie Electrique, Université Mohamed Khider Biskra.

[30] : Benatia Mohamed Amine et KHENE Mohamed Walid; (2010) «Reconnaissance de visage en biométrie»; Université Mohamed Khider BISKRA.

[31] : Belahcene Mébarka,(Octobre 1994) «Analyse de texture par ACP»; Magister électricité industrie; Université de Batna.

[32] : «Xièmes rencontres de la Société francophone de classification», (2004). Bordeaux, France.

[33] : Adjout Mohamed et Benaissa Abdelhak, (2007)«Fusion de la DCT-PCA et la DCT-LDA appliquée à la reconnaissance de visages», Institut National de formation en Informatique (I.N.I) Oued-smar Alger.

[34] : Mébarka Belahcene, AbdElMalik Ouamane, Mohamed Boumehrez et AbdElHamid Benakcha, (2011). «Authentification de visages par les transformations de Hough et Gabor associées à EFM et SVM pour la classification», Intelligence artificielle, Université MUNDIAPOLIS Casablanca.

[35]: Torresani, L., & Lee, K. C. (2007). Large margin component analysis. In Advances in neural information processing systems(pp. 1385-1392).

[36]: Mignon, A., & Jurie, F. (2010, January). Reconnaissance de visages: une méthode originale combinant analyse discriminante logistique et distance sur graphe. In Actes de la conférence Reconnaissance de Formes et Intelligence Artificielle (RFIA).

[37] : JOURANI, R. (2006). Reconnaissance de visages. Projet de fin d'études pour ingénieur en informatique.

[38] : Alismail Mohamed Raouf et Ourchani NorElhouda, (2011). «Fuion multimodale des scores pour la reconnaissance des personnes», Mémoire de Fin d'Etudes, en vue de la préparation du diplôme: MASTER, Département de Génie Electrique, Université Mohamed Khider Biskra.

[39] : Bedra Salim et Mansoura Nabil, (2008). « Identification et authentification du visage en biométrie », Université Mohamed Khider BISKRA.

[40] : MORIZET, N., Thomas, E. A., ROSSANT, F., AMIEL, F., & AMARA, A. (2006). Revue des algorithmes PCA LDA et EBGM utilises en reconnaissance 2D du visage pour la biométrie. P1-11. Institut Supérieur d‟ Electronique de Paris (ISEP), département d'électronique.

[41] : Ababsa,S.G. (2008). Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D. Evry-Val d'Essonne.

[42] : W.Hizem (2009). « Capteur intelligent pour la reconnaissance de visage *», thè*se de doctorat a l'Ecole National Supérieur de télécommunication et Université Pierre et Marie Curie- Paris G, France.

[43] : Mellakh, A. (2009). Reconnaissance des visages en conditions dégradées (Doctoral dissertation, Evry, Institut national des télécommunications).

[44] : A. Chirikov, *«* Karhumen- Loeve, for face recognition *»;* Matlab code available à http://mathworks.com/matlabcentral/fileexchange/ loadfile.do.

[45] : Hazim Mohamed Amir et Nabi Rachid, thème reconnaissance de visages, Universités d'Avignon et du pays du Vaucluse IUPGMT 2006 /2007.

[46] : Lemieux, A. (2003). Système d'identification de personnes par vision numérique (p. 153). Université Laval.

[47]: Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. Journal of cognitive neuroscience, 3(1), 71-86.

[48]: Benkiniouar, M., & Benmohamed, M. (2005). Méthodes d'identification et de reconnaissance de visages en temps réel basées sur AdaBoost. Journée d'informatique graphique Biskra.

[49] : Wang, X., & Tang, X. (2003, Octobre). Unified subspace analysis for face recognition. In Proceedings Ninth IEEE International Conference on Computer Vision (pp. 679-686). IEEE.

[50]: Samaria, F. S., & Harter, A. C. (1994, December). Parameterisation of a stochastic model for human face identification. In Proceedings of 1994 IEEE Workshop on Applications of Computer Vision (pp. 138-142). IEEE.

[51]: Jutten, C, & Herault, J. (1991). Blind separation of sources, part I: An adaptive algorithm based on neuromimetic architecture. Signal processing, 24(1), 1-10.

[52]: Bartlett, M. S., Movellan, J. R., & Sejnowski, T. J. (2002). Face recognition by independent component analysis. IEEE Transactions on neural networks, 13(6), 1450-1464.

[53]: Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997). Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. IEEE Transactions on Pattern Analysis & Machine Intelligence, (7), 711-720.

[54] : http://thesis.univbiskra.dz/Mèthodes de Réduction et Classification.

[55] : Fedias, M. (2013). Combinaisons de données d'espaces couleurs et de méthodes de vérification d'identité pour l'authentification de visages (Doctoral dissertation, Université Mohamed Khider-Biskra).

[56]: Y. Adini, Y. Moses, S. Ullman, (1997). Face recognition: The problem of compensating for changes in illumination direction. IEEE Trans. Patt. Anal. Mach. Intell. 19, 721–732.

[57]:D. Blackburn, M. Bone, P. J Phillips.(2001). "Face recognition vendor test 2000". Tech. rep. http://www.frvt.org.

[58]: Phillips, P. J., Grother, P. J., Micheals, R. J., Blackburn, D. M., Tabassi, E., & Bone, M. (2003). Face recognition vendor test 2002: Evaluation report (No. NIST Interagency/Internal Report (NISTIR)-6965).

[59]: Gross, R., Shi, J., & Cohn, J. (2001). Quo vadis Face Recognition: Third Workshop on empirical Evaluation Methods in Computer Vision.

[60]: A.M Martinez, R. Banavente. (1998). The AR face database. Tech. Report 24 CVC Barcelone, Espagne, June.

[61] : Sidibe, D. D. (2007). Une technique de relaxation pour la mise en correspondance d'images: Application à la reconnaissance d'objets et au suivi du visage (Doctoral dissertation, Université Montpellier II-Sciences et Techniques du Languedoc).

[62]: Ohta, Y. I., Kanade,T., & Sakai, T. (1980). Color information for region segmentation. Computer graphics and image processing, 13(3), 222-241.

[63]: http://fr.wikipedia.org/wiki/YUV, MAI 2011.

[64]: Meurie, C. (2005). Segmentation d'images couleur par classification pixellaire et hiérarchie de partitions/par Cyril Meurie (Doctoral dissertation, Caen).

[65]: Luettin, J., & Maître, G. (1998). Evaluation protocol for the extended M2VTS database (XM2VTSDB) (No. REP_WORK). Idiap.