الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohamed Khider – Biskra

Faculté des Sciences et de la technologie

Département : **Génie Electrique**

Ref :……

جامعة محمد خيضر بسكرة
كلية العلوم و التكنولوجيا
قسم: الهندسة الكهربائية
المرجع:.....

Thèse présentée en vue de l'obtention
du diplôme de

Doctorat en sciences en automatique

Combinaisons de données d'espaces couleurs et de méthodes de vérification d'identité pour l'authentification de visages

Présentée par :

Fedias Meriem

Soutenue publiquement le ……

Devant le jury composé de :

Dr. Okba Kazar	**Professeur**	**Président**	**Université de Biskra**
Dr. Djamel Saigaa	**Maitre de Conférences 'A'**	**Rapporteur**	**Université de M'Sila**
Dr. Redha Benzid	**Maitre de Conférences 'A'**	**Examinateur**	**Université de Batna**
Dr. Nabil Benoudjit	**Professeur**	**Examinateur**	**Université de Batna**
Dr. M.S Mimoune	**Professeur**	**Examinateur**	**Université de Biskra**
Dr. Mohamed Boumahraz	**Maitre de Conférences 'A'**	**Examinateur**	**Université de Biskra**

Remerciement

*Je remercie tout d'abord « **Allah** » le tout puissant, de m'avoir donnée le courage et la patience afin de mener à bien mon projet de doctorat.*
Je remercie chaleureusement ma mère qui est toujours à coté de moi dans les moments difficiles.
Je remercie considérablement mon encadreur Dr : Djamel Saigaa, pour son investissement à mon étude, la liberté qu'il m'a laissée dans mon travail et ces encouragement.
Je remercie vivement Dr. Bahri Mbarek, pour m'avoir accueilli au sein du laboratoire de modélisation des systèmes énergétiques «LMSE» dont il est le directeur, et pour ces encouragements, et son gentillesse pendant ces années de mes projets de magistère et doctorat. Je remercie également tous les membres de LMSE pour leur soutien au cours de ces années de travail.
Je remercie personnellement le Dr. M. Boumehrez pour ces conseils ces encouragements et son aide illimité et je remercie le professeur M.S. Mimoune et le Dr. A. Titaouine pour leur soutien moral et l'ambiance qui m'ont aidé beaucoup de terminer mon travail dans un environnement accueillant. Et je remercie aussi le Dr. A.K Allag et Mme R.Boumaaraf pour ces encouragements.
Je voudrais transmettre aux membres du jury ma sincère considération.
Je remercie chaleureusement Mme Betka Faiza pour son aide sa gentillesse et son soutient moral dés le premier jour que je la connaître.
Enfin, J'aimerais également souligner le support de mon frère et mes sœurs et tous les membres de ma famille. Grandes remerciements à mes meilleures amies Bacha Nadjet et Medaouakh Saadia et à tout ceux qui m'aiment et à tout ceux qui m'aident dans les moments difficiles.

Je dédie ce travail à mon père Mostefa… et mes grandes mères…

Fedias Meriem

Résumé

Ce travail de recherche s'inscrit dans le contexte de la biométrie dont l'objectif est de l'authentification d'une personne à partir de l'image de son visage. Les systèmes d'authentification de visage utilisent généralement la représentation en niveaux de gris de l'image de visage comme caractéristique d'entrée de ces systèmes. Mais nous proposons l'utilisation de la représentation en couleurs qui améliore les performances de ces systèmes. Nous avons testé Plusieurs espaces de couleur pour la transformation des composantes colorimétriques RGB des images originales. Les résultats obtenus dans les différentes espaces/ou composantes colorimétriques sont combinés par l'utilisation d'une fusion logique et non linéaire pour la classification avec un réseaux de neurones simple de type MLP (Multi Layer Perceptron). Concernant les techniques utilisé pour l'extraction des caractéristiques de l'image de visage nous avons appliqué la méthode d'analyse linéaire discriminante (LDA), le modèle amélioré de ficher (EFM), la transformé en cosinus discrète (DCT), la transformé de radon, la méthode appelé 'Local Binary Pattern' (LBP) et les statistiques d'ordre deux de la matrice de cooccurrence. Enfin nous avons proposé une nouvelle méthode basée sur les statistiques d'ordre un de l'image de visage qu'on l'appelle (MS) l'abréviation en anglais de *'Mean and Standard déviation'*. Les résultats présentés montrent l'intérêt du développement de la nouvelle approche (MS) qui permettent de diminuer le temps de calcule grâce à sa simplicité et la robustesse lorsqu'on travail avec une grande base de données. Pour valider ce travail nous avons testé ces approches sur des images frontales de la base de données XM2VTS selon son protocole associé (protocole de Lausanne).

Mots-clés : Biométrie, Couleur, authentification de visage, fusion des experts, extraction de caractéristiques.

ملخص:

هذا البحث هو في سياق المقاييس الحيوية بهدف التحقق من شخص من خلال صورة وجهه. نظمة التحقق من الوجه عادة ما تستخدم الصور بالأبيض و الأسود . ولكن نحن نقترح استخدام الصورباالألوان لتحسين أداء هذه الأنظمة. لقد اختبرنا عدة تمثيلات للألوان لايجاد المناسب منها لنظامنا .يتم الجمع بين مختلف تمثيلات الألوان باستخدام الدمج المنطقي و الدمج الغير خطي لتحسين أداء أنظمة التحقق من الوجه. لاستخراج خصائص صور الوجه طبقنا عدة تقنيات نذكر منها

(LDA, EFM, DCT, Radon, LBP, matrice Cooccurrence).

و أخيرا اقترحنا تقنية جديدة تعتمد على المتوسط والانحراف المعياري للصورة. و النتائج المتحصل عليها تثبت فعاليتها و سرعتها خاصة عند التعامل مع قاعدة بيانات كبيرة. قاعدة البيانات المستخدمة هي XM2VTS و البروتوكول المرتبط بها (بروتوكول لوزان).

Table des matières

Chapitre 5 Mise en œuvre et Résultats

Liste des Tableaux

Listes des Figures

Contributions originales

Les contributions originales de cette thèse sont les suivantes:

[1] **M. Fedias**, D. Saigaa " **A New approach based in mean and standard deviation for authentication system of face** ", International Review on computers and software (IRECOS), pp. 309-314, Vol. 5 n°3 May 2010, Italy.

[2] **M. Fedias**, D. Saigaa "**Non linear fusion of colors to face authentication using EFM method** ", Journal of Applied Computer Science & Mathematics (JACSM), n°9 (4) Nov 2010, pp. 42-50, Romania.

[3] **M. Fedias**, D. Saigaa " **A New Fast method of face Authentication based on First order Statistical Feature** ", International Journal of Computer Applications (IJCA), Vol. 14 n°8 February 2011, pp. 32-37, New York USA.

[4] **M. Fedias**, D. Saigaa, M. Boumehrez "**Logic Fusion of Color based on new Fast Feature extraction for face authentication**", International Journal of Computer Science Issues (IJCSI), Vol.8 n°3 May 2011.pp.36- 44.

[5] **M. Fedias**, D. Saigaa " **Nonlinear fusion of colors to face authentication** ", *Proc. Conf. ICEEDT'08*, International conference on electrical engineering design and technologies, Hammamet, Tunisia, Nov. 2008.

[6] **M. Fedias**, D. Saigaa " **Linear Discriminant Analysis LDA and logic fusion of Colors decisions to face authentication** ", *Proc. Conf. ICEEDT'08*, International conference on electrical engineering design and technologies, Hammamet, Tunisia, Nov. 2008.

[7] **M. Fedias**, D. Saigaa "**Comparison between LDA and PCA with the use of the color to face authentication** ", *Proc. Conf. STA'2008*, the 9th international conference on sciences and techniques of automatic control and computer engineering, Sousse, Tunisia, 2008.

[8] **M. Fedias**, D. Saigaa "**Linear Discriminant Analysis LDA and the nonlinear fusion of colors to face authentication**", *Proc. Conf. STA'2008*, the 9th international conference on sciences and techniques of automatic control and computer engineering, Sousse, Tunisia 2008.

[9] **M. Fedias**, D. Saigaa " **Non linear fusion of colors to face authentication using EFM method** ", the International Workshop on Systems Communication and Engineering in Computer Science CECS' 2010, 3 to 5 Oct 2010 Batna Algeria (Collaboration with TU-Berlin German University and University of Batna, to appear in Springer).

[10] D. Saigaa, **M. Fedias**, A.Harrag, A.Bouchelaghem, D.Drif " C**olor space MS based feature extraction method for face verification** ", the 11th International conference on hybrid intelligent systems HIS' 2011, 5 to 8 Dec 2011 Melaka, Malaysia. (IEEE proceeding).

INTRODUCTION GENERALE

La croissance internationale des communications, tant en volume qu'en diversité (déplacements physiques, transactions financières, accès aux services...), implique le besoin de s'assurer de l'identité des individus. En effet, l'importance des enjeux peut motiver les fraudeurs à mettre en échec les systèmes de sécurité existants. Il existe donc un intérêt grandissant pour les systèmes électroniques d'identification et de reconnaissance. Leur dénominateur commun est le besoin d'un moyen simple, pratique, fiable et peu onéreu de vérifier l'identité d'une personne sans l'assistance d'un tiers. Le marché du contrôle d'accès s'est ouvert avec la prolifération de systèmes, mais aucun ne se révèle efficace contre la fraude, car tous utilisent un identifiant externe tel que : badge/carte, clé, code. Il est fréquent d'oublier un code d'accès. Il existe d'ailleurs de nombreux bureaux où les mots de passe sont notés dans des listes, ce qui représente une dangereuse faille dans la sécurité informatique de l'entreprise puisque toute confidentialité est alors perdue .De même, un badge ou une clé peuvent être, volés ou copiés par des personnes mal intentionnées. Le défaut commun à tous les systèmes d'authentification est que l'on identifie un objet (code, carte...) et non la personne elle-même. Face à la contrainte de l'authentification par « objets », la biométrie apporte une simplicité et un confort aux utilisateurs. Cette discipline s'intéresse en effet, à l'analyse du comportement ainsi qu'à l'analyse de la morphologie humaine et étudie, par des méthodes mathématiques (statistiques, probabilités,…), les variations biologiques des personnes. Ce thème se situe dans la problématique générale de la biométrie qui est une science qui propose d'identifier les personnes à partir de la mesure de leurs indices biologiques. La biométrie recouvre deux approches principales : analyse comportementale (vitesse de signature, marche,…) ou analyse de la morphologie humaine (empreintes digitales, iris, rétine, voix, main, visage, …). Un des objectifs de la biométrie est de sécuriser des accès à des locaux ou à des matériels. Ceci peut se faire aujourd'hui par un contrôle de pièce d'identité ou par la saisie d'un mot de passe, mais les deux modes de contrôle sont contraignants et peuvent donner lieu à des falsification. L'utilisation de techniques biométriques doit permettre d'identifier une personne à travers la consultation d'une base de données, ou de vérifier l'identité affirmée d'un individu. Nous avons retenu la modalité « visage » car c'est un indice biologique très fort contenant de nombreuses indications sur l'identité de la personne et dont l'image peut être acquise de manière non invasive. La reconnaissance de la forme du visage est la technique la plus commune et populaire. Elle est la plus acceptable parce qu'on peut l'utiliser à distance sans contact avec

l'objet. Utiliser une caméra permet d'acquérir la forme du visage d'un individu et puis retirer certaines caractéristiques. Les caractéristiques essentielles pour la reconnaissance du visage sont: les yeux, la bouche, le tour du visage, le bout du nez,… etc. Selon le système utilisé, l'individu doit être positionné devant la caméra où peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont comparées au fichier référence. Le logiciel doit être capable d'identifier un individu malgré différents artifices physiques (moustache, barbe, lunettes, etc..). Le visage est une biométrie relativement peu sûre. En effet, le signal acquis est un sujet à des variations beaucoup plus élevées que d'autres caractéristiques. Celles-ci peuvent être causées, entre autres, par le maquillage, la présence ou l'absence de lunettes, le vieillissement et l'expression d'une émotion. La méthode de la reconnaissance du visage est sensible à la variation de l'éclairage et le changement de la position du visage lors de l'acquisition de l'image.

Cette thèse traite de l'authentification du visage. Un système d'authentification a pour but de vérifier l'identité d'un individu après que celui-ci se soit identifié. Il ne s'agit donc pas d'un système d'identification qui lui se charge de découvrir l'identité a priori inconnue d'un individu. Dans ce contexte, nous développerons un algorithme pour l'authentification du visage vu de face.

Plusieurs méthodes ont été développées dans la littérature pour la reconnaissance de visage [15][16]. Dans ce travail les techniques utilisées pour l'extraction des caractéristiques de l'image de visage sont : la méthode d'analyse linéaire discriminante (LDA) [24], le modèle amélioré de ficher (EFM)[10], la transformée en cosinus discrète (DCT) [38], la transformée de radon [40], la méthode appelée 'Local Binary Pattern' (LBP) [22] et les statistiques d'ordre deux de la matrice de cooccurrence[43][44]. Enfin, nous avons proposé une nouvelle méthode basée sur les statistiques d'ordre un de l'image de visage qu'on l'appelle (MS) l'abréviation en anglais de '*Mean and Standard déviation*'. Pour valider ce travail nous avons testé ces approches sur des images frontales de la base de données XM2VTS selon son protocole associé (protocole de Lausanne). Cette base de donnée a été choisie grâce à sa popularité puisqu'elle est devenue une norme dans la communauté biométrique audio et visuelle de vérification d'identité afin de comparer les résultats obtenus des différentes techniques utilisées dans cette thèse et parce que les images sont en couleur et c'est l'information de couleur qui nous intéresse dans ce travail afin de prouver l'importance de la couleur à l'authentification de visage.

Récemment, très peu de travaux où l'information couleur est utilisée dans les applications de la reconnaissance faciale pourrait être trouvées dans la littérature, parce que la croyance commune et que la couleur n'est pas nécessaire à la reconnaissance faciale [55]. Heureusement, ce sujet a attiré l'attention de plusieurs chercheurs et le nombre de publications sur ce thème a augmenté d'une manière significative au cours des dernières années. Cependant, la plupart des travaux qui ont été faits jusqu'à présent appartiennent essentiellement au moins à un des deux groupes. Le premier groupe n'utilise pas pleinement l'information couleur, tandis que le second groupe l'utilise pour augmenter la performance de système de reconnaissance de visage. Une approche suggère d'utiliser des images gris échelle, avec un ajout de la couleur de la peau comme une nouvelle fonctionnalité proposée par Marcal et Bengio en 2002 [56]. Cette approche améliore la précision de la reconnaissance faciale avec un coût bas de transformation supplémentaire. Une image 30x40 en échelle de gris est utilisée, ce qui nous donne une entrée vectorielle de dimension 1200. Le vecteur supplémentaire que représente la fonction de la couleur de peau est de dimension 96. Ainsi, le vecteur d'entrée est d'une dimension totale de 1296. Cette approche est bonne, du point de vue des coûts de traitement et nous donne une meilleure performance au cours similaires des approches qui utilisent uniquement des images en niveaux de gris, mais ce n'est pas faire un plein usage de la couleur sur les images. Marcal et Bengio ont aussi mentionné dans leur article que leur méthode a un point faible en raison de la similitude de couleur des pixels cheveux et la peau, ce qui amène à une incertitude sur le vecteur de caractéristique extrait. Une autre approche suggère d'utiliser un codage de canal de couleur avec les matrices normalisés non négatives (NMF) proposée par Rajapakse, et al. en 2004 [57] où les canaux de couleur comme le rouge, vert et bleu (RGB) agissent en tant que des vecteurs distincts des données indexées représentant chaque image. NMF est ensuite utilisée pour la couleur de codage. Bien que cette méthode permet une meilleure utilisation des informations de couleur, elle a un coût de traitement grand et inhérent en raison de l'encodage et l'excessive itérative des opérations qui comprend l'inversion de la matrice. Ainsi, dans ce cas, l'amélioration des performances est au prix de l'efficacité du traitement. Les réseaux de neurones se sont révélés être parmi les meilleurs outils dans les applications de reconnaissance faciale et sont largement utilisés dans des approches basées sur des images en niveaux de gris. Mais L'approche de Youssef et Woo en 2007 [58] est initialement proposé pour l'utilisation de Réseau de neurone avec des images colorées d'une

manière qui rend l'utilisation optimale des informations de couleur, sans frais de traitement supplémentaire par rapport aux mêmes approches qui utilisent des images en niveaux de gris.
Des approches utilisent la couleur sur ACP [61][67][62]. Une autre approche proposée par Zhiming Liu, Jian Yang et Chengjun Liu en 2010 [59] est la production d'un nouveau espace couleur (CID) appliqué principalement à la reconnaissance faciale où chaque composante couleur est dérivée par l'utilisation d'un algorithme itérative. L'article de Jian Yang, Chengjun Liu et Lei Zhang en 2010 [60] propose une technique appelée CSN pour la normalisation est qui peut augmenter la discrimination faible des espaces couleurs et qui augmente ainsi la performance de la système de reconnaissance faciale. Ces dernières années l'importance de la couleur dirige les chercheurs d'utiliser l'information de la couleur pour la reconnaissance faciale comme d'autres domaines de traitement d'images comme la compression, la segmentation, la reconnaissance des formes et suivi d'objet…etc.
Le but essentiel de ce travail est de prouver que l'information couleur augmente la performance de système d'authentification. Pour cela nous avons testé Plusieurs espaces de couleur pour la transformation des composantes colorimétriques RGB des images originales. Les résultats obtenus dans les différents espaces/ou composantes colorimétriques sont combinés par l'utilisation d'une fusion logique et non linéaire pour la classification avec un réseau de neurone simple de type MLP (Multi Layer Perceptron). Les résultats présentés montrent que la couleur augmente la performance de système d'authentification par la majorité des techniques.
Aussi les résultats trouvés présentent l'intérêt du développement de la nouvelle approche (MS) qui permettent de diminuer le temps de calcule grâce à sa simplicité et sa robustesse lorsqu'on travaille avec une grande base de données.

Plan de la thèse

Le chapitre 1 présentera quelques techniques biométriques qui existent dans la littérature, ses applications et les détails sur la technique biométrique basée sur le visage.
Dans le chapitre 2, nous allons mettre en évidence les différents avantages et inconvénients de la reconnaissance faciale, le processus de la reconnaissance de visage, les techniques utilisées et enfin nous avons proposé une technique basée sur les statistiques d'ordre un.

En chapitre 3, nous allons présenter la base de données des visages qui a été choisie pour nos expériences. Ainsi le protocole expérimental qui a été soigneusement conçu pour cette base de données.

En suite nous allons exposer les espaces couleur utilisées dans notre travail en chapitre 4.

Le chapitre 5 présentera les améliorations possibles en utilisant l'information couleur pour améliorer les résultats obtenus par les algorithmes décrits en chapitre 2.

Nous terminons enfin par une conclusion générale et perspective.

1.1 Introduction

Le piratage, la fraude, les virus informatiques posent un grand problème pour les personnes les entreprises et les gouvernements dans leur quête de protection de données contre le vol. Une solution qui parait logique est d'exploiter des caractéristiques humaines physiques ou comportementales telles que l'empreinte digitale, la signature, l'iris, la voix, le visage, la démarche, et un geste de main pour différencier des personnes, toutes ces dernières s'appelle les caractéristiques biométriques. Ces caractéristiques sont traitées par certain ordre de processus automatisés à l'aide des dispositifs comme des modules de balayage ou des appareils photo. À la différence des mots de passe ou des PINs (numéros d'identification personnelle) qui sont facilement oubliés ou exposés à l'utilisation frauduleuse, ou des clefs ou des cartes magnétiques qui doivent être portées par l'individu et qui sont faciles à êtres copiées ou perdues.
Dans ce chapitre, nous allons expliquer quelques techniques biométriques qui existent dans la littérature, ses applications et les détails sur la technique biométrique basés sur le visage.

1.2 Les principales techniques biométriques

Une des définitions de la biométrie est donnée par Roethenbaugh [1] : « La biométrie s'applique à des particularités ou des caractères humains uniques en leur genre et mesurables, permettant de reconnaître ou de vérifier automatiquement l'identité ». Mais Aucune modalité biométrique n'est en elle-même fiable à 100 %. Il existe des problèmes, liées aux dispositifs de capture des données, à l'utilisateur lui-même ou au condition lors de la capture, dans lesquelles une modalité quelconque peut s'avérer défaillante. Parmi les principales modalités biométriques physiologiques (empreintes digitales, forme de la main, traits du visage,...) et comportementales (dynamique du tracé de la signature, frappe sur un clavier d'ordinateur,...) les traces biologiques (odeur, salive, ADN,...) on note [1][2][3][4][5] :

- **La voix**

Basée sur l'analyse des caractéristiques comme la fréquences, les harmoniques, la puissance sonore, etc.

- **Les empreintes digitales**

Analyse des caractéristiques des sillons cutanés, terminaison des sillons, croisements, bifurcations, etc.

- **L'oeil**

Basée sur l'étude de la disposition des muscles circulaires et radiaux qui ouvrent et ferment la pupille.

- **La main**

Mesure de la longueur, largeur, forme des phalanges, des articulations, des lignes de la main, etc…

- **Le visage**

Cherche la géométrie du visage de face et profil, Le visage est sujet à une variabilité tant naturelle (vieillissement, par exemple) que volontaire (maquillage, chirurgie esthétique, grimaces, etc.). Son traitement est donc difficile (forme des yeux, de la bouche, du nez, position des pommettes, etc.) à partir d'une photographie numérique ou d'une caméra infrarouge (thermographie pour utilisation dans le noir).

- **L'oreille**

Analyse de la forme de l'oreille.

- **La signature** (reconnaissance statique ou dynamique)

Analyse de la forme (statique) et/ou de la vitesse et de la trajectoire de la signature (dynamique).

- **L'ADN**

La méthode la plus fiable pour identifier une personne, mais actuellement pas adaptée à la reconnaissance en temps réel.

- **Muli-modalité**

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

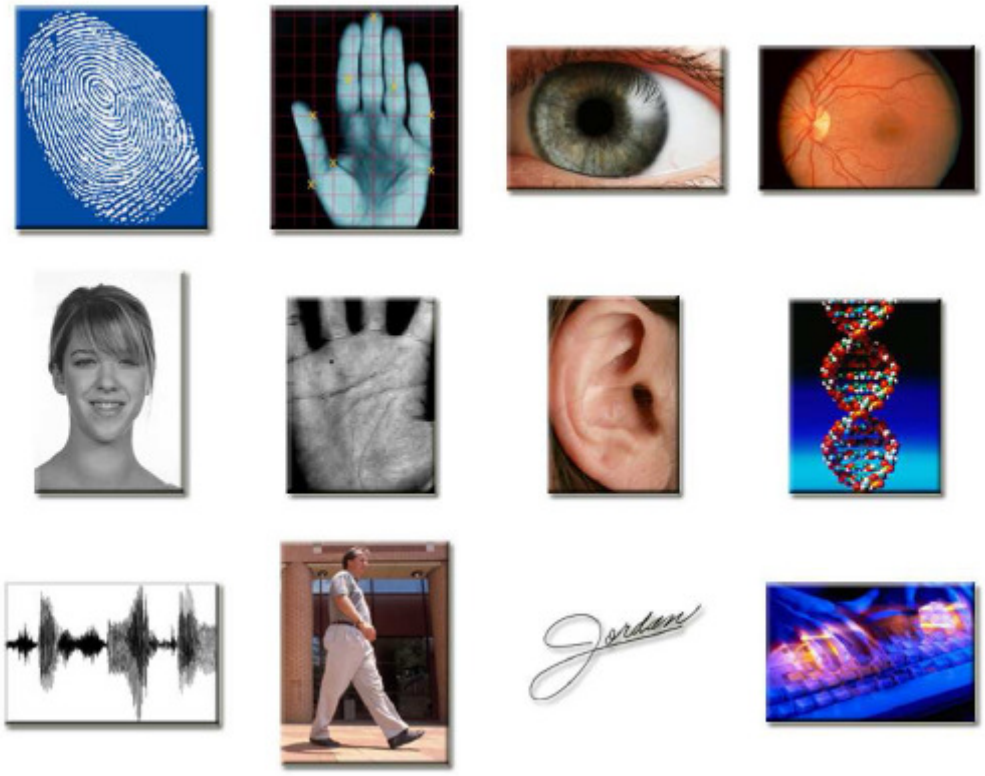


Figure 1.1 les différentes caractéristiques biométriques [2].

1.3 Les propriétés d'une modalité biométrique

L'identification et l'authentification par la biométrie sont plus précises que celle utilisant les moyens classiques d'identification tels que les cartes, clés ou mots de passe car elle constitue un lien fort et permanent entre une personne physique et son identité. Les propriétés principales d'une modalité biométrique sont :

- l'universalité : toute la population doit posséder cette modalité.
- l'unicité : deux personnes différentes doivent avoir des représentations de leur biométrie différentes.
- la stabilité : une stabilité dans le temps et une stabilité pour chaque personne.
- l'acceptabilité et la facilité d'usage : se rapportent aux contraintes liées à l'acquisition et l'utilisation d'une modalité biométrique.
- la non reproductibilité : concerne la facilité ou non à falsifier une modalité biométrique.

En effet aucune biométrie n'est parfaite mais du moins avec des degrés différents. Le compromis entre présence ou absence de certaines de ces propriétés se fait selon les besoins de chaque application [4].

1.4 Les domaines d'applications de la biométrie

Les technologies biométriques se retrouvent désormais à la base d'une vaste gamme de solutions de vérification personnelle et d'identification hautement fiables. De nombreux dispositifs et systèmes technologiques mettent désormais en oeuvre des solutions biométriques, notamment pour le contrôle d'accès aux locaux, aux postes de travail, aux réseaux et à certaines applications logicielles. Utilisée seule ou intégrée à d'autres technologies telles que les cartes intelligentes, les clés de cryptage et les signatures numériques, la technologie biométrique devrait s'imposer de plus en plus dans bon nombre de secteurs de l'économie ainsi que dans notre vie quotidienne. De plus en plus de produits électroniques grand public intègrent la technologie d'identification biométrique comme, par exemple certains ordinateurs portables, certains assistants numériques personnels, certains téléphones cellulaires ou lecteurs MP3 [6][7].

Les solutions biométriques sont-elles vraiment nécessaires ? Le recours aux caractéristiques biologiques comme alternative aux systèmes d'identification par mot de passe rencontre de moins en moins de réticences. Compte tenu du nombre de mots de passe à retenir au quotidien (carte de crédit, porte d'accès, anti-démarrage codé des véhicules, etc.), il apparaît en effet plus simple et plus rapide de passer le doigt devant un écran plutôt que de mémoriser et de saisir un nouveau mot de passe. Dans le cadre de l'authentification personnelle, la biométrie semble mieux adaptée que les autres techniques actuelles (telles que mots de passe ou cartes intelligentes). La tendance est à la centralisation de la gestion des identités – par le biais d'une combinaison de paramètres d'accès tant physiques que logiques à différents types de ressources. C'est une solution à laquelle tendent de plus en plus d'entreprises, et qui implique le recours à la biométrie. Compte tenu de l'augmentation des brèches de sécurité et des transactions frauduleuses, les technologies de vérification personnelle et d'identification hautement fiables trouvent toute leur utilité. Donc la biométrie à des avantages sur divers domaines, où la sécurité biométrique a déjà prouvé son importance.

On peut distinguer huit grands types d'applications biométriques [8] :

- Accès physique: ici, l'avantage est l'application de l'identification biométrique pour contrôler l'accès des employés aux zones sensibles des organisations d'entreprises, banques, aéroports et autres lieux. L'accès physique aux maisons et les garages peut aussi être contrôlées par cette technologie.
- PC et l'accès au réseau: les applications biométriques pour contrôler l'accès non autorisé aux ordinateurs et réseaux dans une organisation ou à la maison. La grande importance, si on parle d'une organisation avec des ordinateurs et des ressources réseau en tant que ses composants vitaux.
- Temps et Présence: L'importance des données biométriques dans le maintien de temps des employés et la participation à une organisation a augmenté collecteurs dans les dernières années.
- Accès logique: La sécurité biométrique joue un rôle important dans le contrôle d'accès logique aux ordinateurs, facilitée par des mots de passe et autres outils d'identification.
- Sécurité financière: opérations de commerce électronique, de souscrire une assurance en ligne et autres activités similaires à des procédures d'avancées telles que l'identification biométrique.
- Secteur de la santé: ces dispositifs biométriques sont largement utilisés pour protéger l'identité des utilisateurs. En outre, assurer la sécurité dans les locaux de l'hôpital.
- Application de la loi: les services de police et d'autres organes répressifs utilisent de l'identification biométrique pour la capture de criminels et d'enquêter.
- L'immigration et les aéroports : les applications biométriques sont aussi prospère dans le domaine de l'industrie et l'immigration dans les aéroports pour assurer la sécurité contre le terrorisme.
- Autres- Ordinateurs portables, téléphone portable, Verrouillage.

La figure suivante présentes quelques domaines d'application de la biométrie dans la vie quotidienne.

Figure 1.2 les applications de la biométrie dans notre vie [8].

1.5 Comparaison des technologies biométriques

Il n'y a pas de système biométrique parfait. L'International Biometric Group a procédé à une comparaison des différentes technologies sur base de 4 critères :

- 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).

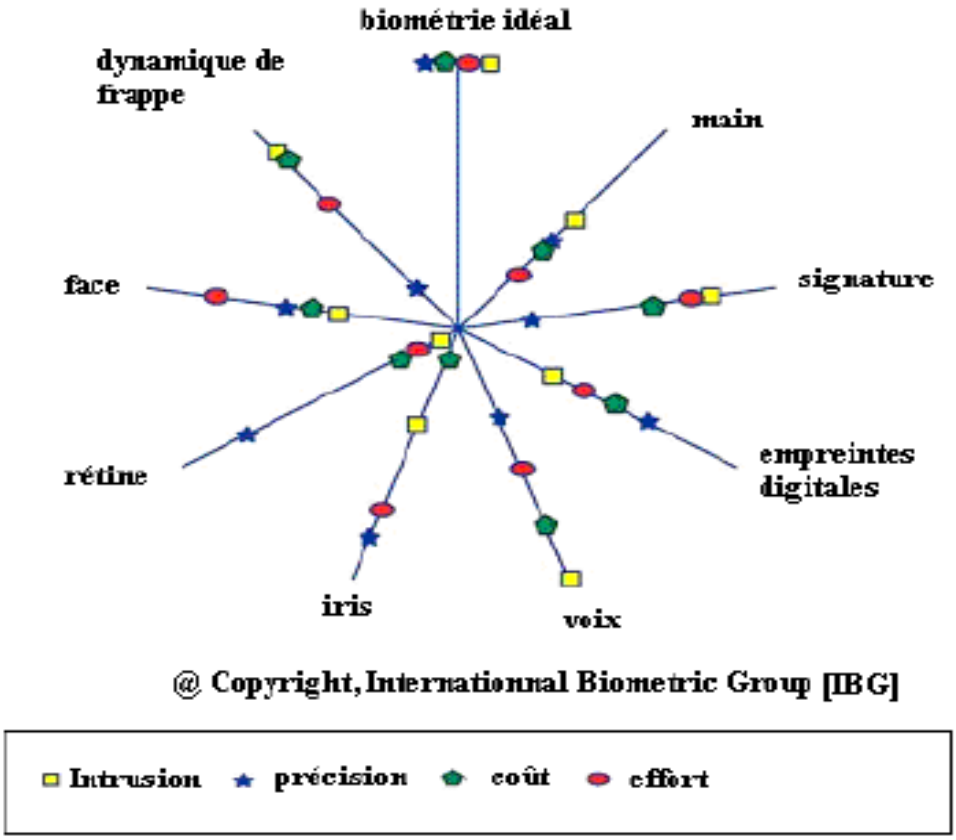


Figure 1.3 Analyse Zephyr [9]

Cette comparaison permet de choisir une technologie en fonction des contraintes liées à l'application. La Figure 1.3 montre qu'il n'existe pas de méthode idéale. Les méthodes se divisent en deux grands groupes. Le premier groupe englobe les méthodes conviviales pour les utilisateurs (effort à fournir faible, méthode peu intrusive, prix modéré) mais assez peu performantes. Ce groupe qui correspond aux méthodes basées sur la biométrie comportementale (reconnaissance de la voix, de la signature…). L'autre groupe contient les méthodes plus sûres (méthodes intrusives et prix élevés, performances très bonnes). Il est donc nécessaire de déterminer, au cas par cas, pour chaque problème, la méthode qui conviendra le mieux à la situation. Pour cela, il faut étudier attentivement le niveau d'exigence en sécurité, le budget pouvant être investi dans le système et la façon dont risque de réagir les utilisateurs. Actuellement, pour la mise en place des grands projets de passeports biométriques, les systèmes retenus par l'Europe semble être un stockage de la photo d'identité, des empreintes digitales et de l'iris sous forme numérique. A noter que le choix du

ou des dispositifs biométriques peut aussi dépendre de la culture locale. Ainsi en Asie, les méthodes nécessitant un contact physique comme les empreintes digitales, sont rejetées pour des raisons d'hygiène alors que les méthodes basées sur l'iris sont très bien acceptées. La dynamique de frappe fait partie des méthodes biométriques les moins performantes mais très intéressantes au niveau du coût, de l'effort à fournir et du niveau d'intrusion perçu. Elle est donc adaptée aux applications de sécurisation des zones peu sensibles et pour lesquelles il n'y a pas la volonté ou la possibilité de débloquer des budgets très élevés.

En France, le CLUSIF a également proposé une comparaison (avantages / inconvénients) des principales technologies biométriques. Comme le montre le tableau suivant :

Techniques	**Avantages**	**Inconvénients**
Empreintes digitales	Coût, ergonomie moyenne, facilité de mise en place, taille du capteur	Qualité optimale des appareils de mesure (fiabilité), acceptabilité moyenne, possibilité d'attaques (rémanence de l'empreinte,...)
Forme de la main	Très ergonomique, bonne acceptabilité	Système encombrant, coût, perturbation possible par des blessures et l'authentification des membres d'une même famille
Visage	Coût, peu encombrant, bonne acceptabilité	Jumeaux, psychologie, religion, déguisement, vulnérabilité aux attaques
Rétine	Fiabilité, pérennité	Coût, acceptabilité faible, installation difficile
Iris	Fiabilité	Acceptabilité très faible, contrainte d'éclairage
Voix	Facilité	Vulnérable aux attaques
Signature	Ergonomie	Dépendant de l'état émotionnel de la personne, fiabilité
Frappe au clavier	Ergonomie	Dépendant de l'état physique de la personne

Table 1.1 Avantages et inconvénients des différentes technologies biométriques.

Pour la reconnaissance de visage c'est une technique commune, populaire, simple et qui a beaucoup d'avantage à savoir l'utilisation des visages qui sont des données publiques, la possibilité de s'intégrer aux systèmes de surveillance existants et elle ne nécessite pas des équipements chers. Pour cela la reconnaissance de visage est la technologie biométrique

qu'on utilisera dans notre système de reconnaissance. Dans le chapitre suivant nous voyons brièvement les algorithmes principaux qui ont été développés pendant les deux dernières décennies pour aborder le problème provocant de l'identification ou de la vérification de visages. Nous décrivons alors en détails les algorithmes que nous avons utilisés dans cette thèse.

1.6 Principaux modules du système biométrique

Que ce soit pour une application d'authentification ou d'identification, le processus d'un système biométrique est toujours la même et comprend deux phases distinctes : l'apprentissage et la reconnaissance (authentification ou identification). Le processus d'apprentissage a pour but d'assembler des informations biométriques sur les personnes à identifier. Plusieurs campagnes d'acquisitions de données peuvent être réalisées afin d'assurer une certaine robustesse au système de reconnaissance aux variations temporelles des données. Pendant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numérique (signatures), et enfin stockées dans la base de données.

On parle de vérification (authentification) d'identité lorsqu'une personne clame être déjà enrôlée dans le système biométrique (et posséderait donc une ID-card ou un login name). Dans ce cas, les données biométriques obtenues de cette personne sont comparées avec sa signature d'utilisateur qui est enregistré dans la base de données. En résumé, un système biométrique opérant en mode vérification répond à la question "*Suis-je réellement la personne que suis-je entrain de proclamer?*".

On parle d'identification quand l'identité de l'utilisateur est à priori inconnue. Dans ce cas, les données biométriques de l'utilisateur sont comparées aux signatures de tous les utilisateurs enregistrés dans la base de données du système biométrique, car l'utilisateur pourrait être n'importe lequel (sinon aucun) d'entre eux. 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 ?*".

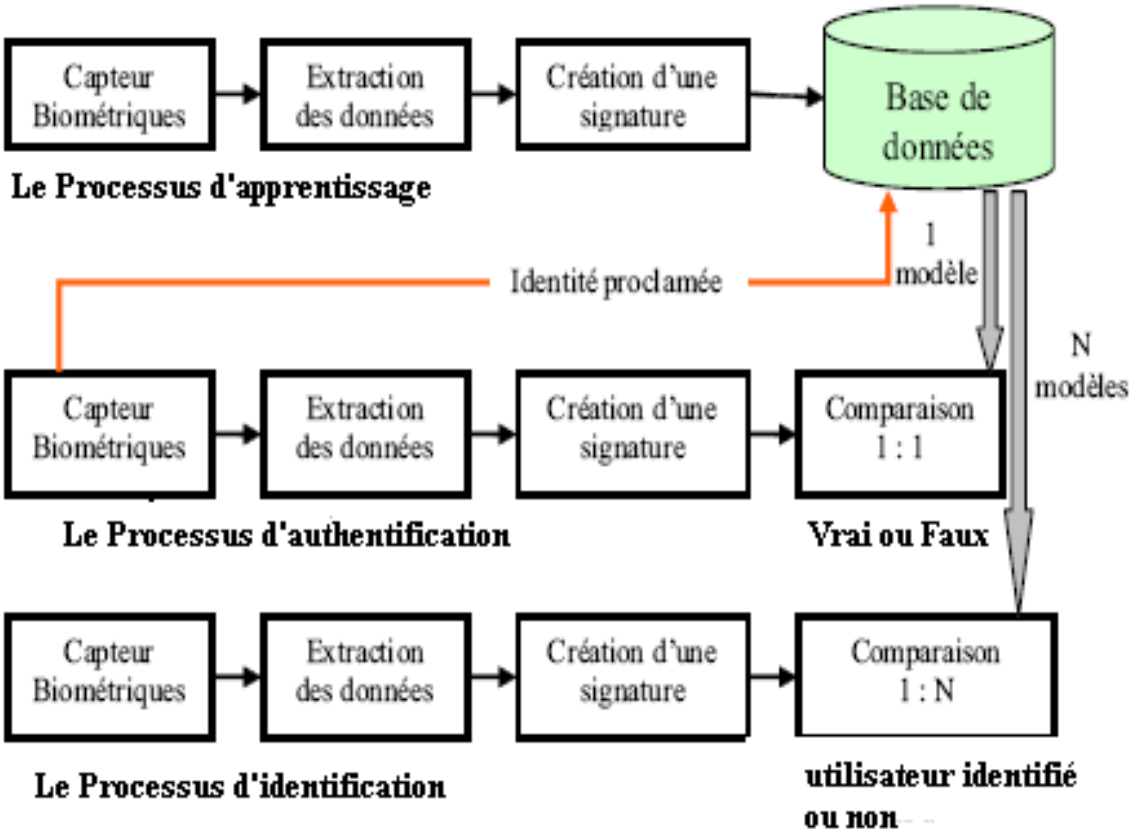


Figure 1.4 Principaux modules d'un système biométrique [3].

1.7 Evaluation de la performance d'un système biométrique

Tout d'abord, afin de comprendre comment déterminer la performance d'un système biométrique, il nous faut définir clairement deux types d'erreurs :

- Une erreur de faux rejet, qui survient lorsqu'un utilisateur légitime est faussement rejeté, parce que le système trouve que ses données biométriques ne sont pas suffisamment similaires à celles du profil maître de la base de données.
- Une erreur de fausse acceptation, qui survient quand un imposteur est malencontreusement accepté en tant qu'utilisateur légitime, parce que le système trouve que ses données biométriques sont suffisamment similaires à celles du profil maître de la base de données.

Dans un système idéal, il n'y a pas de faux rejet et de fausse acceptation. Dans un système réel cependant, leur nombre n'est pas nul et peut prendre des valeurs non négligeables lorsque les modalités et conditions d'utilisation augmentent la variabilité des données. Les taux de faux rejet et de fausse acceptation dépendent du seuil de sécurité. Plus la valeur du seuil sera

grande, plus il y aura de faux rejets et moins de fausses acceptations, et inversement, plus la valeur du seuil sera petite, moins il y aura de faux rejets et plus de fausses acceptations. Le nombre de faux rejets et celui de fausses acceptations sont inversement proportionnels. Le choix de la valeur de seuil à utiliser dépend principalement de la finalité du système biométrique. Cette valeur est choisie de manière à faire un compromis adéquat entre la sécurité et l'utilisabilité du système. Par exemple, un système biométrique aux portes d'un parc d'attraction comme Disneyland appliquera typiquement un seuil beaucoup plus petit qu'un système biométrique aux portes des quartiers généraux.

Le nombre de faux rejets et de fausses acceptations est habituellement exprimé en un pourcentage par rapport au nombre total de tentatives d'accès autorisés (resp. non autorisés). Ces taux sont appelés taux de faux rejet (TFR) et taux de fausse acceptation (TFA) et sont donc liés à une certaine valeur de seuil. Ces taux d'erreur sont définis comme suit:

$$TFR = \frac{nombre\ des\ clients\ rejetés(FR)}{nombre\ total\ d'accès\ clients} \tag{1.1}$$

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

Certains appareils biométriques (ou les logiciels les accompagnant) prennent le seuil de sécurité désiré comme paramètre du processus de décision. Les autres appareils biométriques retournent un score (borné) sur la base duquel la décision d'accepter ou de rejeter l'utilisateur va être prise par l'application elle-même. En général, si le score est plus grand ou égal au seuil, l'utilisateur va être accepté et, si le score est plus petit, il sera rejeté [10]. Dans le cas où le dispositif biométrique retourne un score, on peut générer un graphe indiquant la dépendance des taux de fausse acceptation (TFA) et de faux rejets (TFR) au seuil. La figure 1.5 montre un exemple d'un tel graphe.

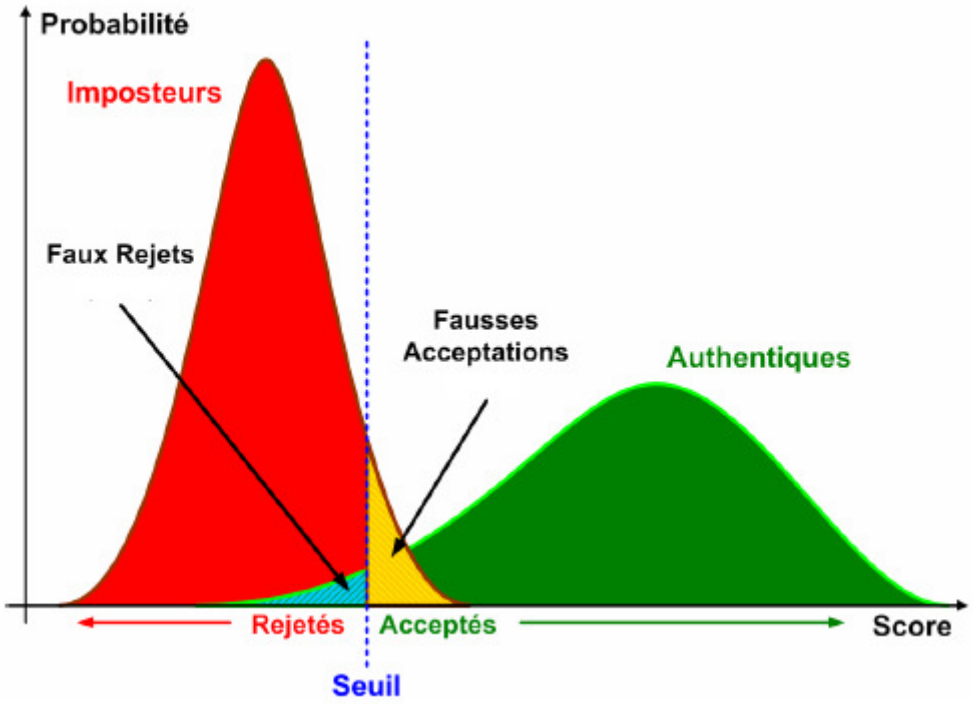


Figure 1.5 Illustration du TFR et du TFA [2].

Les courbes des TFA et TFR se coupent en un point où les taux de fausse acceptation et de faux rejet sont égaux ; la valeur en ce point est appelée taux d'égale erreur (TEE). Cette valeur n'a presque pas d'utilité pratique car on ne souhaite généralement pas que le TFA et le TFR soient les mêmes, mais elle constitue un bon indicateur de la précision du dispositif biométrique. Par exemple, si l'on a deux appareils avec des taux d'égale erreur de 1% et 10%, on sait alors que le premier est plus précis (i.e. qu'il fait moins d'erreurs) que le second. Pourtant, de telles comparaisons ne sont pas aussi simples en réalité. D'une part, les valeurs fournies par les fabricants sont incomparables parce que ces derniers ne publient habituellement pas les conditions exactes de leurs tests, et d'autre part, même s'ils le font, les tests dépendent vraiment du comportement des utilisateurs et d'autres influences extérieures, telles que la qualité des senseurs ou l'utilisation de ceux-ci. Dans une banque par exemple, un dispositif de reconnaissance vocal sur le système téléphonique induira un TFR élevé et un TFA petit, car si les personnes qui veulent téléphoner se font sans cesse rejeter, elles vont être frustrées et risquent de rompre leur relation avec la banque, ce qui va coûter beaucoup plus cher à cette dernière que si quelques personnes non autorisées se font un peu trop facilement accepter. Au contraire, un système biométrique sur un coffre fort induira un TFR petit et un TFA élevé, car si une personne autorisée veut accéder au coffre (ce qu'elle ne fait en général qu'à de rares occasions) et qu'elle se fait rejeter, ce ne sera pas grave. Elle va recommencer le

processus de vérification peut-être une fois ou deux jusqu'à ce qu'elle soit acceptée. Elle sera même ravie de la réticence du système à accepter toute personne et finira par avoir accès à ses biens, ce qui ne va pas coûter grande chose à la banque. Par contre, si un imposteur se fait malencontreusement accepter, il pourra avoir accès au contenu du coffre et le voler, ce qui va coûter cher à la banque qui va devoir dédommager son client [11].

En effet, une vérification parfaite d'identité (FAR=0 et FRR=0) est non réalisable dans la pratique. Mais n'importe lequel de ces deux taux (TFA, TFR) peut être réduit à une petite valeur arbitraire en changeant le seuil de décision, avec l'inconvénient d'augmenter l'autre. Une seule mesure peut être obtenue en combinant ces deux taux d'erreurs dans le taux erreur totale (*TET*) ou son complément, le taux de succès total (*TS*):

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

$$TS = 1 - TET \tag{1.4}$$

Cependant, un soin devrait être pris en utilisant une seule mesure. En effet, cette seule mesure (*TET* ou *TS*) pourrait être fortement pondérée par l'un ou l'autre type d'erreurs (*TFA* ou *TFR*), dépendant seulement du nombre d'accès qui ont été utilisés en obtenant ce type d'erreur. Le *TET* sera toujours plus près de l'erreur (*TFA* ou *TFR*) qui a été obtenue en utilisant le plus grand nombre d'accès dans son type. Selon la nature (authentification ou identification) du système biométrique, il existe deux façons d'en mesurer la performance :

1. Lorsque le système opère en *mode authentification*, on utilise ce que l'on appelle une courbe ROC (pour "Receiver Operating Characteristic" en anglais). La courbe ROC (Figure 1.6) trace le taux de faux rejet en fonction du taux de fausse acceptation. Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé.

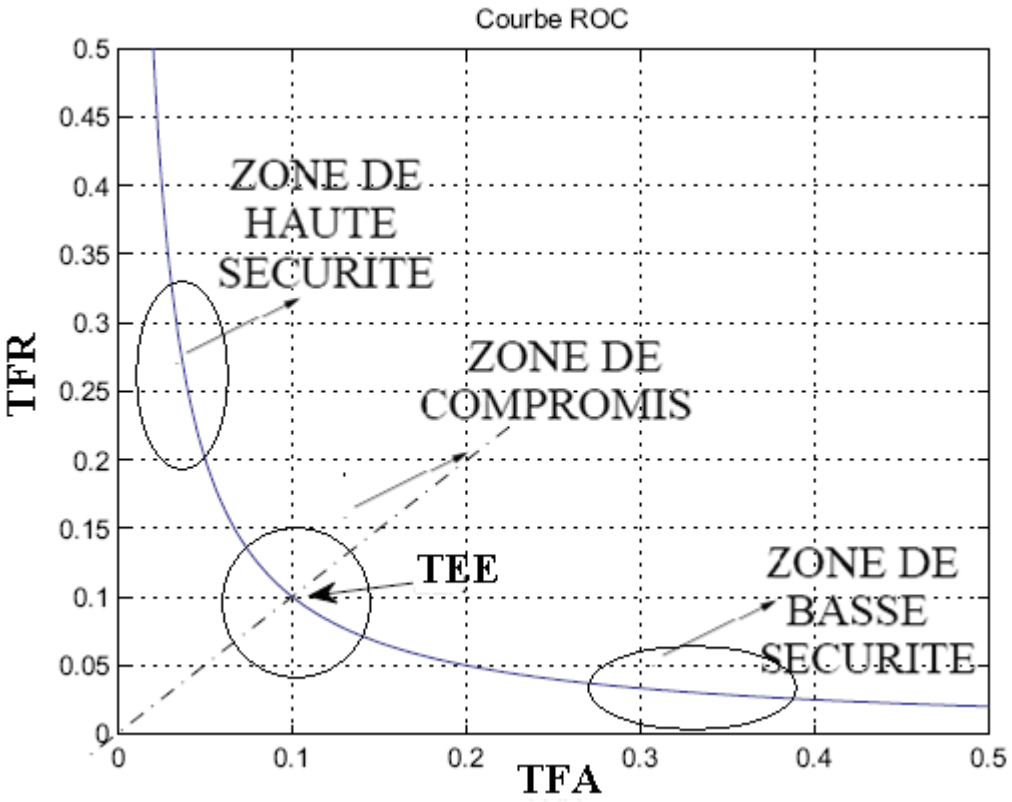


Figure 1.6 Courbe ROC [11].

Le domaine d'application de la biométrie impose la nature de l'erreur tolérable. Pour une application hautement sécuritaire, la fausse acceptation est intolérable. On fixe le seuil pour avoir le moins de TFA au détriment du TFR. Alors que pour les applications personnelles, on privilégie un TFR bas. Dans tout les cas un TEE faible est demandé par les utilisateurs, pour s'approcher le plus des systèmes de mot de passe traditionnels. De là, on peut fixer un autre point de fonctionnement plus adéquat. Le taux de vérification à 0.1% de TFA donne une autre idée sur le comportement du système à faible taux de TFA. Dans ce cas on ne veut pas d'imposteurs. Ce point de fonctionnement est généralement utilisé avec des modalités tels que l'iris ou l'empreinte. Très souvent, on utilise le TEE pour comparer entre les performances de différents systèmes biométriques [12].

2. En revanche, dans le cas d'un système utilisé en *mode identification*, on utilise ce que l'on appelle une courbe CMC (pour "Cumulative Match **C**haracteristic" en anglais). La courbe CMC (Figure 1.7) donne le pourcentage de personnes reconnues en fonction d'une variable qui s'appelle le rang [13]. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit, parmi deux images, celle qui

correspond le mieux à l'image d'entrée, etc. On peut donc dire que plus le rang augmente, plus le taux de reconnaissance Correspondant est lié à un niveau de sécurité faible.

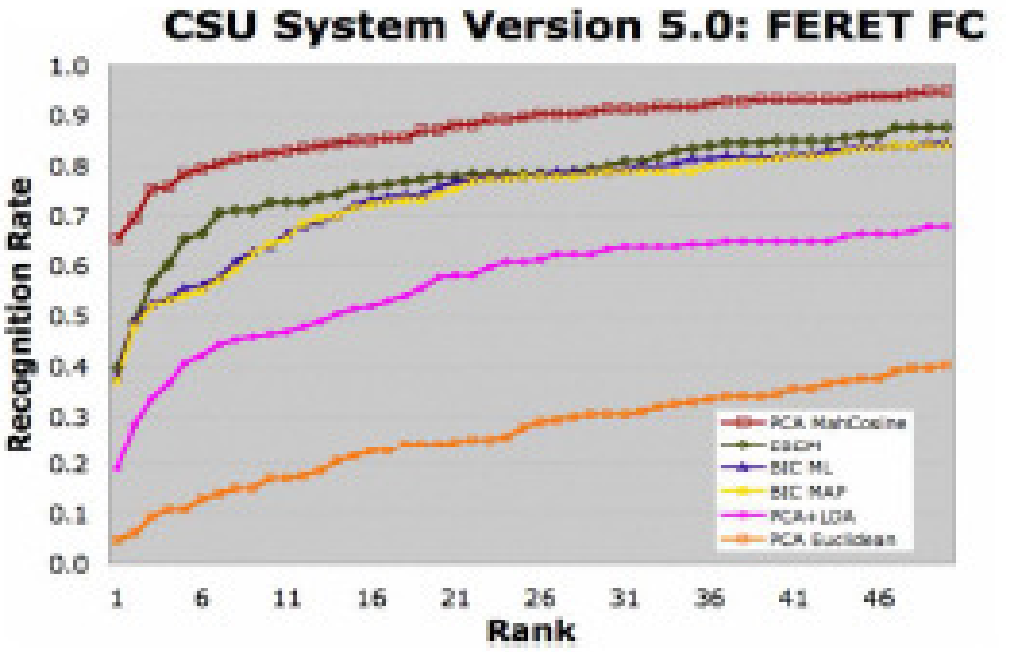


Figure 1.7 Courbes CMC du CSU System 5.0 pour le "FERET Probe Set FC" et pour différents algorithmes de reconnaissance faciale [2].

1.8 Conclusion

Dans ce chapitre nous avons mis en relief quelques notions et définitions de base liées à la biométrie et ses diverses technologie, les principales modules des systèmes biométriques et comment mesurer leurs performance ainsi que les domaines d'applications. Après une comparaison des technologies biométriques on a choisit la reconnaissance de visage pour sa popularité et sa simplicité ainsi le coût faible de réaliser ce système parce qu'il suffit un caméra pour capter les images de visages et un micro-ordinateur pour faire les calcules. Dans le chapitre suivant nous décrivons en détaille les différents techniques utilisées.

2.1 Introduction

La reconnaissance faciale, en tant qu'une des technologies biométriques de base, a pris une part de plus en plus importante dans le domaine de la recherche, ceci étant dû aux avances rapides dans des technologies telles que les appareils photo numériques, Internet et les dispositifs mobiles, le tout associé à des besoins en sécurité sans cesse en augmentation. Selon IBG (International Biometric Group) [9], la modalité la plus utilisée après l'empreinte est le visage.

2.2 Les avantages et les inconvénients de la reconnaissance de visage

Plusieurs facteurs rendent la modalité visage attractive pour une utilisation à grande échelle :

- acceptable : les personne sont moins résistantes pour la capture de visage, vu que c'est une partie apparente du corps. Et aussi que nous avons nos photos de visage sur toutes nos pièces d'identité.
- vérifiable : n'importe quel opérateur peut facilement vérifier la décision d'un système biométrique a base de visage. La modalité visage peut dans certains cas, comme le cas de contrôle des frontières, conforter la décision de l'agent pour la vérification d'identité et constituer un système d'aide à la décision et non de remplacement de l'agent ce qui rend cette modalité plus acceptable.
- Sans contact (intrusive) : la capture du visage est assez facile sans contact si on compare avec d'autres modalités tel que l'iris qui sont difficiles à capter. La vérification peut être faite sans trop déranger l'utilisateur : l'utilisateur doit seulement se présenter devant une caméra.
- Coût bas du capteur : De plus les capteurs d'images sont moins chers sur le marché. Ce qui facilite une commercialisation d'un système à base de reconnaissance de visage.
- Cette technologie nous aide à éviter qu'une personne puisse avoir deux cartes d'identité ou usurpe l'identité d'une autre personne.

La différence d'apparence d'un même visage capturé dans deux conditions d'acquisition distincte pose un énorme problème dans le domaine de la reconnaissance faciale. Cette différence est dû, généralement, à des facteurs d'environnement comme les conditions d'éclairage, les caractéristiques des capteurs et aussi leur positionnement par rapport au visage

lors de l'acquisition. Cette variation peut aussi être dus aux modifications du visage liées aux expressions ou aux changements de poids ainsi qu'à l'âge.

La modalité de visage présente des inconvénients qui influent sur la qualité de la reconnaissance. On peut cité les aspects suivants [3][10][12] :

- Changement d'illumination : 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.
- Variation de pose : Le taux de reconnaissance de visage baisse considérablement quand des variations de pose sont présentes dans les images.
- Expressions faciales : 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.
- 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.
- Les vrais jumeaux qui ont le même indicatif d'ADN, peuvent tromper les personnes qui ne les connaissent pas (les personnes familiers avec les jumeaux ont reçu une grande quantité d'information sur ces derniers et sont donc beaucoup plus qualifiés à distinguer les jumeaux.). Il est peu probable que la vérification automatique de visage, ne pourra jamais détecter les différences très subtiles qui existent entre les jumeaux.

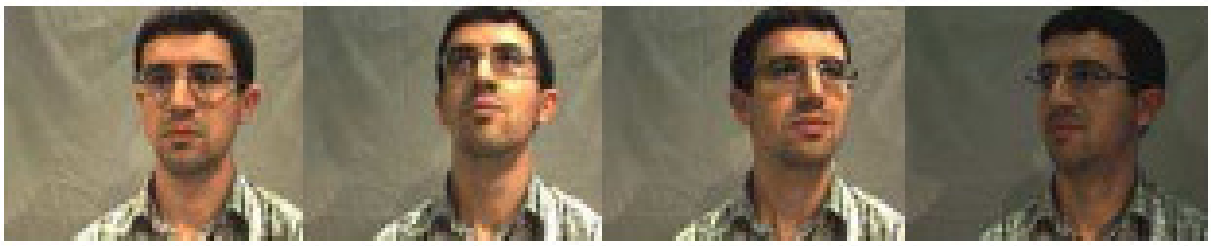


Figure 2.1 variation de pose, changement d'illumination et présence des lunettes [3].

2.3 Processus de la reconnaissance faciale

De nos jours, le visage peut être utilisé pour identifier une personne dans une base mais il est plus communément utilisé pour vérifier l'identité. Il s'agit alors de déterminer si une identité réclamée est correcte ou fausse. Pour la vérification des visages, ce processus est effectué en comparant un modèle du demandeur (une ou plusieurs images de test), avec un modèle stocké (une ou plusieurs images de référence).

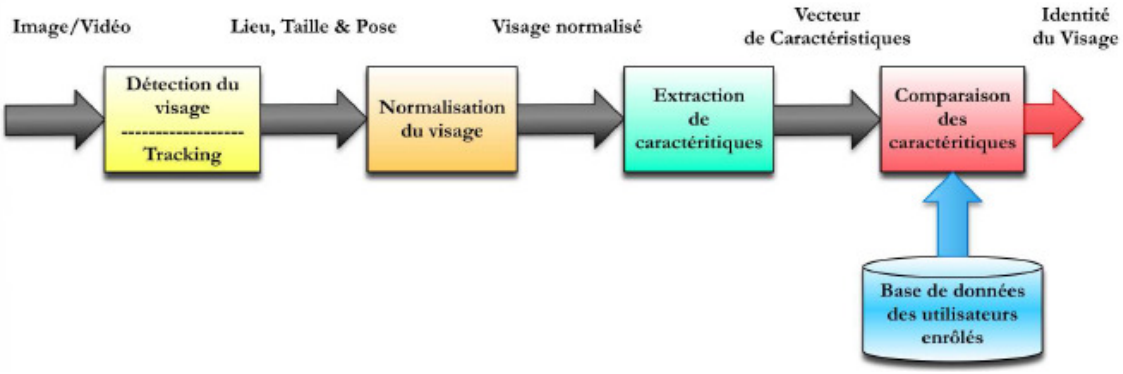


Figure 2.2 architecture générale d'un système de reconnaissance faciale [2].

Le processus complet de vérification des visages est décrit ci-dessous [3][12][10] :

- Capture du visage : En effet, avoir des images de bonne qualité en référence améliore les performances de reconnaissance. Il faut réussir à capter l'information pertinente sans bruit. Il existe plusieurs types de capteurs pour l'acquisition du visage qui se classent selon leur mode de fonctionnement, leur domaine de sensibilité spectrale et leur mode d'acquisition. On trouve sur le marché les capteurs classiques d'image à 2D tels que : les CCD (Couple charged device) ou CMOS pour capturer des images dans le spectre visible et/ou proche infrarouge, ou les capteurs thermiques qui permettent une acquisition dans l'infrarouge. Des informations spécifiques à la capture peuvent être déterminées aussi lors de l'acquisition de l'image, comme la pose de la personne par rapport à la caméra, l'expression ou aussi les conditions d'illumination de la capture de l'image.
- Détection : L'image 2D acquise peut contenir à la fois le visage de la personne et éventuellement, un arrière-plan. Dans le processus de détection, le visage est localisé dans l'image. Cette étape est dépendante de la qualité des images acquise.

- Normalisation : Le rôle de la normalisation est, d'une part d'éviter les influences des facteurs d'échelle quand les données varient dans des intervalles différents. D'autre part La normalisation tente d'éliminer ou de réduire les effets de l'illumination de l'image. Il existe un grand nombre d'opérateurs de normalisations classiquement utilisés et présentés notamment dans [14]. Pour normaliser une donnée, il est nécessaire de posséder des informations sur sa distribution. Les informations utilisables sont le maximum , le minimum, la moyenne, l'écart type de la variable à partir desquelles une transformation mathématique est appliquée à la donnée afin d'obtenir la donnée normalisée.
- Extraction des caractéristiques : le but est d'extraire les caractéristiques du visage qui peuvent le rendre à la fois différent de celui des autres personnes et robuste aux variations de la personne elle-même. C'est l'information nécessaire pour que le visage d'une personne ne ressemble pas à celui d'une autre personne et en même temps qu'il ressemble à lui-même dans d'autres conditions d'acquisition. Plusieurs techniques existent pour cette étape par exemple les techniques qui utilisent LDA, EFM…etc.
- Comparaison des caractéristiques : selon les caractéristiques extraites précédemment, les algorithmes de comparaison diffèrent. On trouve dans la littérature plusieurs approches : calcul de distance, calcul de similarité…etc. Cette comparaison produit un score, représentant la similarité ou la distance de l'image test par rapport à l'image ou au modèle référence.
- Décision : Le score est comparé à un seuil qui détermine si l'image est acceptée ou rejetée en tant que représentant de l'identité proclamée.

Nous voyons maintenant brièvement l'état de l'art sur les algorithmes principaux qui ont été développés pendant les deux dernières décennies pour aborder le problème provocant de l'identification ou de la vérification de visages. Et puis nous décrivons en détails les approches que nous avons utilisés ainsi que notre approche proposée dans cette thèse.

2.4 État de l'art sur la reconnaissance de visage

De nombreux algorithmes ont été proposés dans la littérature pour la reconnaissance faciale [15][16], elles peuvent être classées en trois catégories :

- **Les approches Géométriques:** On les appelle aussi les méthodes à traits, à caractéristiques locales, ou analytiques qui extraient des caractéristiques faciales, puis les combinent au sein d'un modèle plus global pour ensuite effectuer une

Classification. Ce modèle correspond à la manière avec laquelle l'être humain perçoit le visage, c'est à dire, à nos notions de traits de visage et de parties comme les yeux, le nez, la bouche, etc. La tâche de reconnaissance proprement dite est ensuite réalisée en effectuant certaines mesures (comme la distance entre les yeux) sur ces caractéristiques. Un certain nombre de stratégies ont modélisé et classé les visages sur la base de distances normalisées et angles entres points caractéristiques. Cette phase d'extraction des traits caractéristiques du visage constitue l'étape clé du processus, car la performance du système entier en dépend. L'avantage de ces méthodes est qu'elles prennent en compte la particularité du visage en temps que forme naturelle à reconnaître, et un nombre réduit de paramètres (de 9 à14 distances au maximum a considérer) La difficulté éprouvée quand il s'agit de prendre en considération plusieurs vues du visages ainsi que le manque de précision dans la phase "extraction" des points constituent leur inconvénient majeur. L'approche locale la plus populaire est l'*ElasticGraphMatching* (EGM) où un ensemble de point d'intérêts est extrait du visage, à partir duquel un graphe est créé. Brunelli et Poggio [17] utilisent des modèles géométriques comme la distance entre des paires de points caractéristiques pour réaliser la reconnaissance faciale.Wiskott *et al.*[18] utilisent des filtres de Gabor sur le voisinage de ces points pour calculer un ensemble de *jets* pour créer la méthode dite de l'*Elastic BunchGraphMatching* (EBGM). Les méthodes locales, basées sur des modèles, utilisent des connaissances a priori que l'on possède sur la morphologie du visage et s'appuient en général sur des points caractéristiques en détectant certains points ou traits caractéristiques d'un visage puis en les comparant avec des paramètres extraits d'autres visages. Ces méthodes constituent une autre approche pour prendre en compte la non-linéarité en construisant un espace de caractéristiques local et en utilisant des filtres d'images appropriés, de manière à ce que les distributions des visages soient moins affectés par divers changements. Les approches Bayesiennes (comme la méthode BIC [19], les machines à vecteurs de support (SVM) [20], la méthode des modèles actifs d'apparence (AAM) [21] ou encore la méthode "local binary pattern" (LBP) [22] ont été utilisées dans ce but. Toutes ces méthodes ont l'avantage de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression par rapport aux méthodes globales.

- **Les approches Globales** : qui réalisent souvent une forme de projection linéaire de l'espace de grande dimension dans un espace de dimension plus faible. La méthode la plus populaire appelée *Eigenfaces* (introduite par Turk et Pentland [23]) est basée

sur l'Analyse en Composantes Principales (ACP) des visages. L'Approche ACP (ou Les Visages Propres), son but est de capturer la variation dans une collection d'images de visages et d'utiliser cette information pour coder et comparer les visages (en termes mathématiques : trouver les vecteurs propres de la matrice de covariance de l'ensemble des images de visages). Le nombre possible de visages propres peut être approximé en utilisant seulement les meilleurs visages propres qui correspondent aux plus grandes valeurs propres. Cette approche rencontre le problème du coût des calculs élevé et celui de la détermination du nombre de visages propres utiles. Une autre technique populaire appelée *FisherFaces* est basée sur une Analyse Discriminante Linéaire (LDA) [24], [25], [26], qui divise les visages en classes selon le critère de Fisher. Une comparaison de ces méthodes est effectuée par Socolinsky et Selinger dans [27], et par Wu *et al.* dans [28] qui testent également l'utilisation des Transformées en Cosinus Discrets (DCT). Le principal inconvénient des approches globales est leur sensibilité aux changements de luminosité. En effet, lorsque la luminosité d'un visage change, son apparence subit une transformation non–linéaire, et étant donné l'aspect linéaire des approches globales, la classification peut échouer. Des extensions de ces approches linéaires ont été proposées comme l'Analyse en Composantes Principales à Noyaux (Kernel–PCA) [29], ou l'Analyse Discriminante Linéaire à Noyaux (Kernel–LDA) [30] pour la reconnaissance faciale. L'inconvénient de ces extensions est qu'il n'y a pas d'invariance à certaines transformations à moins que celles–ci ne soient prises en compte lors de la création du noyau, et donc encore une fois manuellement. C'est également le défaut d'autres techniques d'apprentissage comme les Machines à Vecteurs de Support (SVM) [31], et la méthode de la ligne caractéristique [32]. La méthode de Laplacianfaces [33] qui dépendent largement du nombre d'exemples d'apprentissage par personne. Dans le cas d'un exemple par personne, ces méthodes se ramènent encore à la méthode « eigenface ». L'Approche connexionniste [34] L'inconvénient de cette approche est que l'apprentissage est long. A ce jour, il n'est pas claire comment de tels systèmes vont s'étendre à des problèmes plus larges, il faut prendre en compte un grand nombre d'individus. Pour l'approche Stochastique les images frontales sont balayées de haut en bas il y a un ordre naturel dans lequel les caractéristiques apparaissent, et de ce fait peut être modélisé d'une manière pratique en utilisant un modèle caché de Markov (HMM : Hidden Markov Model) [35]. Ce modèle rencontre les problèmes de prises de vue des images en entrée. L'approche statistique et l'approche probabiliste: cette approche repose essentiellement sur la

théorie de décision pour résoudre les problèmes de classement et de classification, et pour cela en utilise généralement la classification fondée sur le théorème de Bayes.

- **Les approches Hybrides :** Les méthodes hybrides sont des approches qui combinent les caractéristiques holistiques et locales afin d'améliorer les performances de la reconnaissance de visages. En effet, les caractéristiques locales et les caractéristiques globales ont des propriétés tout à fait différentes. Plusieurs techniques peuvent parfois être combinées où fusionnées afin de résoudre un problème de reconnaissance des formes. Chacune d'entre elles possède évidemment ses forces et ses faiblesses qui, dans la majorité des cas, dépendent des situations (pose, éclairage, expressions faciales, etc.). 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. Cette approche n'est cependant pas triviale, ni miraculeuse et certaines erreurs de classification peuvent parfois survenir même lorsqu'un des classificateurs est correct [3].

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

Maintenant et après ce rapide survol sur les différentes méthodes existantes dans le domaine d'authentification de visage, on peut donner, en détail, les techniques qui ont été utilisées dans ce travail avec la proposition d'une nouvelle méthode. Et pour l'augmentation de la performance de notre système d'authentification de visage on a ajouté l'information couleur et on a appliqué la fusion entre les composantes colorimétriques pour chaque technique.

2.5 Les techniques utilisé

Parmi toutes les méthodes présentées dans l'état de l'art, certaines demeurent plus avantageuses que d'autres. On a choisi quelques techniques de reconnaissance pour la réalisation de notre application. Les critères utilisés pour cette sélection reposent notamment sur les temps d'exécution et les taux de reconnaissance. Une des techniques les plus utilisées dans la reconnaissance de visage est l'Analyse en Composantes Principales (ACP). Une méthode très populaire, basée sur la technique ACP, est la méthode « eigenface » introduite

en 1991 par Turk et Pentland [23]. 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. La technique Eigenface globale est une méthode très utilisée pour la reconnaissance de visage. Sa popularité est due à sa nature relativement simple, son fondement mathématique fort et ses résultats bons. Il faut noter que plusieurs méthodes globales comme LDA et EFM repose sur cette méthode de base. Mais le problème avec l'ACP est qu'elle ne prend pas en compte la discrimination des classes. Pour augmenter la séparabilité des classes dans le sous-espace de composantes principales on utilise l'analyse discriminante linéaire de Fischer bien connue en anglais (Fischer Linear Discriminant Analysis : FLD ou LDA) décrite en détail ci-dessous.

2.5.1 Analyse Linéaire Discriminante de Fischer (LDA)

Les étapes à suivre pour extraire les discriminants pour un ensemble d'images sont [24][25][26] :

a) Pour la ième classe, une matrice de dispersion (Si) est calculé comme la somme des matrices de covariance des images centrées dans cette classe.

$$S_i = \sum_{x \in x_i} (x - m_i)(x - m_i)^T \tag{2.1}$$

Où chaque x est un vecteur visage et m_i est la moyenne des images dans la classe. La dispersion de la matrice (S_W) est la somme de toutes les matrices de dispersion.

$$S_w = \sum_{i=1}^{c} S_i \tag{2.2}$$

C est le nombre des classes.

b) La dispersion entre la classe (S_B) mesure la quantité de dispersion entre les classes.

$$S_B = \sum_{i=1}^{c} n_i (m_i - m)(m_i - m)^T \tag{2.3}$$

n_i est le nombre d'images dans la classe, m est la moyenne de toutes les images.

c) Résoudre le problème généralisé eigenvalue :

Résoudre la généralisation des vecteurs propres (V) et valeurs propres Λ au sein de la classe et la dispersion entre les classes.

$$S_B V = \Lambda S_W . V \tag{2.4}$$

d) Trier les vecteurs propres associés par leurs valeurs propres du plus haut au plus bas vecteurs propres. Ces vecteurs propres forment la base.

e) Projeter de toutes les images originales sur base des vecteurs en calculant le point de produits de l'image avec chacun des vecteurs de base.

LDA est une technique qui cherche les directions qui sont efficaces pour la discrimination entre les données.

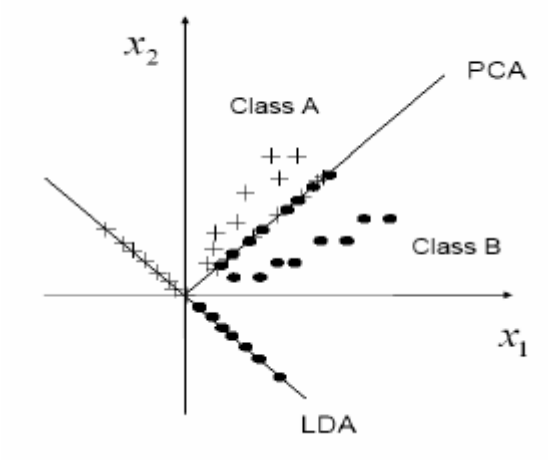


Figure 2.3 les projections ACP et LDA d'un ensemble de données.

Comme l'ACP ne prend pas en compte la discrimination des classes mais LDA résoudre ce problème, et que les méthodes basées sur LDA standard telles que Fisherfaces, appliquent en premier lieu l'ACP pour la réduction de dimension et puis l'analyse discriminante. Des questions appropriées au sujet de l'ACP sont habituellement liées au nombre des composantes principales (CP) utilisées et comment elles affectent la performance. Concernant l'analyse discriminante on doit comprendre les raisons de sur-ajustage de précision et comment l'éviter. Les réponses à ces deux questions sont étroitement liées. On peut réellement montrer qu'employer plus de CP peut mener à la diminution de la performance de l'authentification. L'explication de ce comportement est que les CP correspondantes aux vecteurs qui ont des petites valeurs propres correspondent aux composantes de hautes fréquences codent habituellement le bruit. En résulte, si les vecteurs propres correspondant aux petites valeurs propres sont employés pour définir le sous-espace réduit de PCA, le procédé FLD s'accompagne aussi bien par le bruit et par conséquence le sur-ajustage de précision a lieu. Pour cette raison le modèle amélioré du FLD (Enhanced FLD Model : EFM) est employé pour surmonter ces problèmes liés au sur-ajustage de précision, montrée en détail ci-dessous.

2.5.2 Le Model Discriminant linéaire amélioré de Fisher (EFM)

Le modèle discriminant linéaire amélioré de Fisher (EFM) améliore les possibilités de généralisation de LDA en décomposant le procédé LDA en diagonalisation simultanée des deux matrices de dispersion intra-classe et inter-classe [36]. La diagonalisation simultanée est une étape sagement équivalente à deux opérations comme précisé par Fukunaga [37]: blanchissant la matrice de dispersion intra-classe et application du l'ACP sur la matrice de dispersion inter-classe en utilisant les données transformées. Durant l'opération de blanchissement de la matrice de dispersion intra-classe apparaisse dans le dénominateur de la séparabilité des petites valeurs propres qui tendent à capturer du bruit [36][37]. Pour réaliser des performances améliorées l'EFM préserve un équilibre approprié entre le choix des valeurs propres (correspondant aux composantes principales de l'espace d'image original) qui tiennent compte la majeure partie de l'énergie spectrale des données brutes, c.-à-d., une représentation adéquate, et la condition que les valeurs propres de la matrice de dispersion intra-classe (de l'espace ACP réduit) ne sont pas trop petites, c.-à-d., une meilleure généralisation [10].
On doit alors calculer les valeurs propres de la matrice de dispersion intra-classe dans l'espace ACP réduit pour faciliter le choix du rang des composantes principales de sorte que l'ordre de grandeur soit satisfait. Vers cette fin, on effectue le LDA par des étapes comme décrit ci-dessous. En particulier, ces étapes de LDA permettent de trouver les valeurs propres et les vecteurs propres de $S_w^{-1}S_b$ comme résultat de la diagonalisation simultanée de S_w et S_b. Blanchissons d'abord la matrice de dispersion intra-classe :

$$S_W \mathrm{E} = \mathrm{E}\Upsilon \quad and \quad \mathrm{E}^T\mathrm{E} = I \tag{2.5}$$

$$\Upsilon^{-1/2}\mathrm{E}^T S_W \mathrm{E}\Upsilon^{-1/2} = I \tag{2.6}$$

où $\mathrm{E}, \Upsilon \in \Box^{mxm}$ sont la matrice des vecteurs propres et la matrice diagonale des valeurs propres de S_W respectivement. et m est le rang des composantes principales pour la réduction de dimension.
EFM diagonalise en premier lieu la matrice de dispersion de intra-classe S_W en utilisant les équations (2.11) et (2.12). Notez que E et Υ sont maintenant les matrices des vecteurs

propres et des valeurs propres correspondants aux vecteurs caractéristiques. En second lieu EFM procède à calculer la matrice de dispersion inter-classe comme suit [36]:

$$\Upsilon^{-1/2}\mathrm{E}^{T} S_b \mathrm{E}\Upsilon^{-1/2} = K_b \tag{2.7}$$

Diagonalisons maintenant la nouvelle matrice de dispersion inter-classe K_b:

$$K_b \mathrm{H} = \mathrm{H}\Theta \quad et \quad \mathrm{H}^{T}\mathrm{H} = I, \tag{2.8}$$

où $H, \Theta \in \square^{mxm}$ sont respectivement, la matrice des vecteurs propres et la matrice diagonale des valeurs propres de K_b. La matrice de transformation globale du procédé EFM est définie maintenant comme suit [36] [37] :

$$D = \mathrm{E}\Upsilon^{-1/2} H \tag{2.9}$$

La prochaine technique de reconnaissance de visage retenue utilise l'espace fréquentiel à l'aide de la transformée de cosinus discrète (DCT). Plus de détail dans la section suivante.

2.5.3 Transformée de cosinus discrète (DCT)

Généralement la transformée DCT est plus utilisable dans le domaine de compression multimédia. Et l'utilisation de la transformée de cosinus discréte (Discrete Cosine Transform ou DCT) [38] à la reconnaissance de visage est assez récente [39]. Mais si on le compare avec l'ACP la méthode DCT est beaucoup plus rapide concernant l'extraction de vecteur caractéristique. La méthode est simple chaque image de visage est représentée par un vecteur composé des premiers coefficients de la transformée DCT. Et lorsqu'un visage est présenté sa transformée est calculée et un certain nombre de coefficients est retenu pour comparaison avec ceux de la base de données. Et pour chacune des images de la base de donnée on calcul sa transforme en cosinus discrete de l'image normalisée et on extraire les premiers coefficients de la DCT afin de former un vecteur unifié, puis on sauvegarde des représentations. Donc le processus d'apprentissage est réalisé sur chaque image indépendamment contrairement aux techniques ACP LDA et EFM. On remarque que l'un des avantages de cette méthode repose sur sa grande flexibilité en cas d'ajouts d'images ou de personnes. En effet, cette opération n'implique donc aucun ré-apprentissage complet, contrairement aux méthodes comme l'ACP, LDA et EFM. Une autre avantage c'est que les

ressources requises par cette méthode ne concernent que la liste des représentations vectorielles, ce qui résulte en une très faible consommation de mémoire.

Premièrement l'image de visage est décomposée en blocs de taille (8x8) puis on applique la transformée en deux dimension de la DCT sur chaque bloc individuellement. Les 64 coefficients de chaque bloc sont regroupés en parcourant les éléments dans l'ordre imposé par une séquence particulière appelée séquence zigzag. On lit les valeurs en zigzags inclinés à 45° en commençant par le coin supérieur gauche et finissant en bas à droite. Cette séquence à la propriété de parcourir les éléments en commençant par les basses fréquences et de traiter les fréquences de plus en plus hautes. Puisque la matrice DCT contient beaucoup de composantes de hautes fréquences nulles, l'ordre de la séquence zigzag va engendrer de longues suites de 0 consécutives. Le résultat est donc une suite monodimensionnelle des coefficients quantifiés numérotés de 1 à 64 pour chaque bloc. Et pour tous les blocs on génèrent le vecteur caractéristique pour le processus de reconnaissance de visage.

Pour une image de taille (*NxN*) la transformé DCT en deux dimension est définit par :

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\frac{\pi(2x+1)u}{2N}\cos\frac{\pi(2y+1)}{2N} \qquad (2.10)$$

Où $v = 0,1,2,...N-1$ $\alpha(u),\alpha(v)$ est définit par $\alpha(u) = \sqrt{\frac{2}{N}}$ pour $v = 0$ et $\alpha(v) = \sqrt{\frac{2}{N}}$ pour $v \neq 0$.

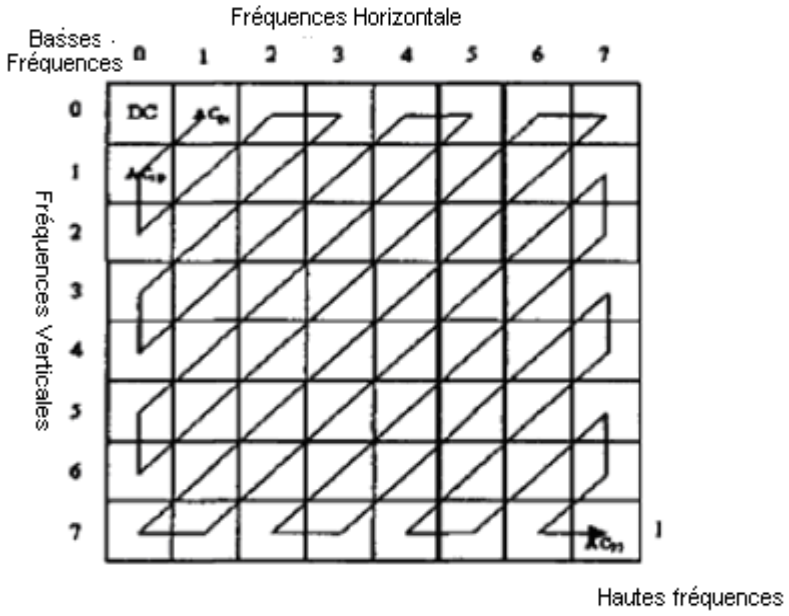


Figure 2.4 séquence zigzag de lecture d'un bloc de (8x8).

2.5.4 La transformation de radon

La transformation par radon et son inverse a été introduite premièrement par le mathématicien australien « Johann Radon » en 1917. C'est une transformation intégrale qui calcule les intégrales de ligne à partir de plusieurs sources le long des chemins parallèles. Mais ces dernières années, la transformée de Radon a reçu beaucoup d'attention surtout dans le domaine de traitement d'images. La transformation de Radon est un outil fondamental qui est utilisé dans diverses applications Telles que l'imagerie radar, imagerie géophysique, imagerie médicale et des tests. Son principe est de calculer les projections d'une image où matrice selon des directions spécifié. Une projection d'une fonction bidimensionnelle f (x, y) est un ensemble d'intégrales en ligne. Dans cette thèse nous allons appliqué la transformé de radon sur l'authentification de visage. Les résultats vont montrer l'efficacité, la rapidité et la simplicité de cette transformation [40][41].

Pour représenter une image, la fonction de radon prendre plusieurs projections parallèles de l'image sous différents angles en tournant la source autour du centre de l'image. La figure 2.5 montre une projection unique à un angle de rotation spécifié [40].

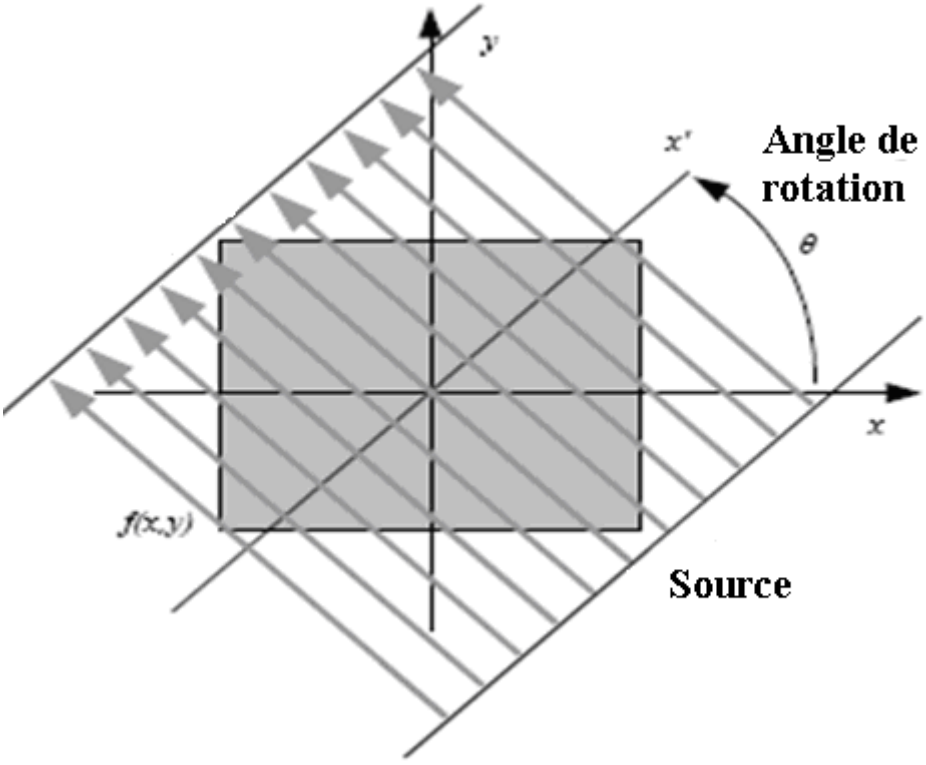


Figure 2.5 Projection unique à un angle de rotation spécifié.

La transformée de Radon est la projection de l'intensité de l'image le long d'une ligne radiale orientée à un angle spécifique. Les coordonnées de la ligne radiale sont les valeurs le long de l'axe x', qui est orientée au θ degrés dans le sens de l'axe des abscisses x. L'origine des deux axes est le centre de l'image. Par exemple, l'intégrale de f (x, y) dans le sens vertical est la projection de f (x, y) sur l'axe des x. et l'intégrale dans le sens horizontal est la projection de f (x, y) sur l'axe des y. La figure 2.6 montre les projections horizontale et verticale pour une simple fonction en deux dimensions.

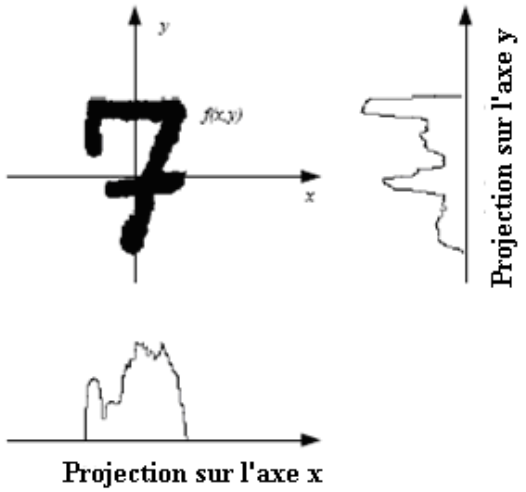


Figure 2.6 Les projections horizontale et verticale d'une simple fonction *f(x,y)*.

Les projections peuvent être calculées tout au long de n'importe quel angle θ, par l'utilisation de l'équation générale de la transformée de radon suivante :

$$R_\theta(x') = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} f(x,y)\delta(x\cos\theta + y\sin\theta - x')dydy \qquad (2.11)$$

où δ (·) est la fonction de l'impulsion de dirac et qui est définit par une valeur non égale à zéro et égal à 0 ailleurs. Et :

$$x' = x\cos\theta + y\sin\theta \qquad (2.12)$$

x ' est la distance perpendiculaire au rayon de l'origine et θ est l'angle d'incidence des rayons. La figure 2.7 illustre la géométrie de la transformée de radon.

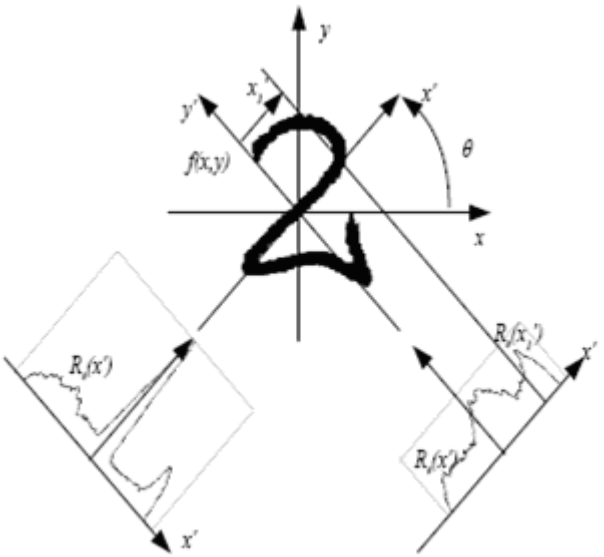


Figure 2.7 La géométrie de la transformée de Radon.

La propriété très forte de la transformée de Radon est la capacité d'extraire les lignes (courbes en général) à partir d'images très bruitées. La transformée de Radon possède des propriétés intéressantes relatives à l'application de transformations affines. On peut calculer la transformée de Radon de tout transition, rotation ou changement l'échelle d'image, sachant la transformée de Radon de l'image originale et les paramètres de la transformation affine appliquée. C'est une propriété très intéressante pour la représentation des symboles parce qu'elle permet de distinguer entre les objets transformées, mais on peut aussi savoir si deux objets sont liés par une transformation affine en analysant leur transformé de Radon. La figure suivante illustre quelques images binaires et leurs transformées de radon (dans le désordre).

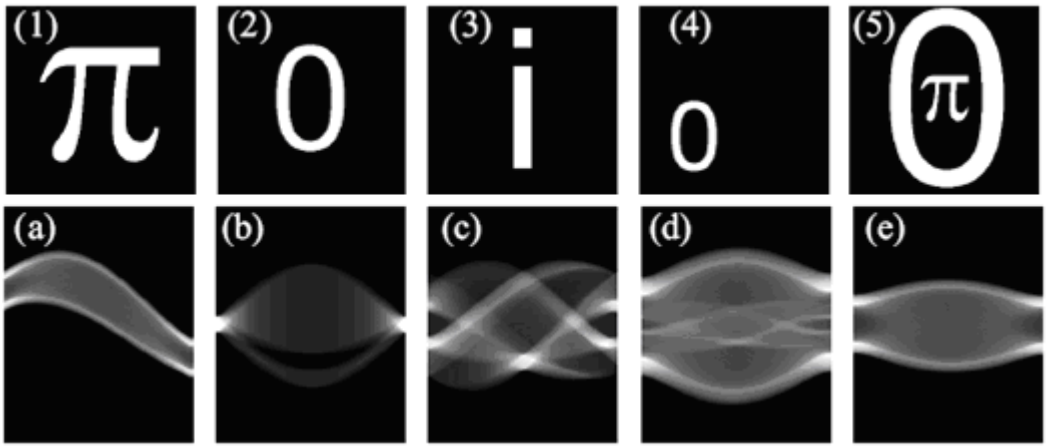


Figure 2.8 illustration qualitative de la transformée de radon.

2.5.5 La méthode LBP (Local Binary Pattern)

2.5.6 Les statistiques d'ordre deux de la matrice de co-occurrence

En 1973, Haralick [42] a proposé 14 caractéristiques statistiques (appelés aussi les attributs texturaux) extraites à partir de la matrice de co-occurrence de niveaux de gris. Ces attributs texturaux sont des attributs très importants pour la description de l'image et la reconnaissance des objets. L'étude de la texture des objets d'une image peut avoir des objectifs très divers : obtenir des informations sur la nature d'un l'objet, segmenter l'image en régions homogènes, identifier la texture afin de la réduire à un ensemble de paramètres (compression d'images), recherche d'image par contenu…etc. Actuellement, seulement les quatre caractéristiques les plus appropriées sont largement utilisées : l'énergie, l'entropie, le contraste et le moment inverse de différence pour la majorité d'application. La texture d'une image peut être interprétée comme la régularité d'apparition de couples de niveaux de gris selon une distance donnée dans l'image. La matrice de co-occurrences contient les fréquences spatiales relatives d'apparition des niveaux de gris selon les quatre directions suivantes : $\theta = 0, \theta = 45°, \theta = 90°, \theta = 135°$. Les relations de voisinage entre pixels, nécessaires au calcul des matrices, sont illustrées en figure 2.10 ; par exemple, les plus proches voisins de 'x' selon la direction □135° sont les pixels 4 et 8.

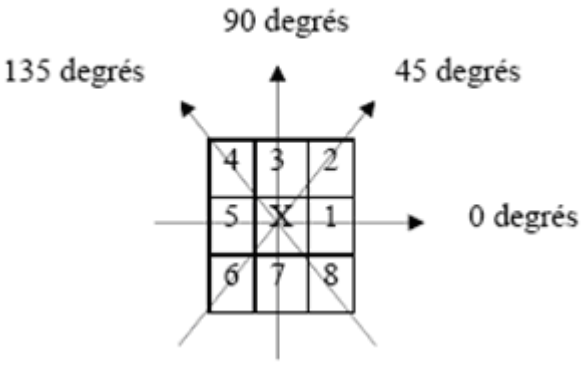


Figure 2.10 plus proches voisins du pixel x selon 4 directions

La figure 2.11 montre un exemple de calcul des matrices de co-occurrence $P_{d,\theta}(i, j)$ à partir d'une petite image 4× 4 composée de quatre niveaux de gris (0, 1, 2,3). Cet exemple se limite au cas *d* □= 1 et $\theta = 0$. L'élément (2,3) de la matrice *P*(1, 0) est égal à 4, cela signifie qu'il existe 4 configurations dans l'image ou un pixel de niveau de gris 2 est séparé horizontalement d'un autre pixel de niveau de gris 3 par une distance 1. Ces configurations sont représentées en trait gris sur l'image.

La plupart des images sont codées sur 256 niveaux de gris, par conséquent, la taille des matrices de cooccurrence est de 256 × 256. On s'aperçoit ainsi que ces matrices comptabilisent une très grosse quantité d'informations difficile à exploiter directement. Mais c'est Haralick et al [42] qui ont proposé les premiers 14 paramètres, caractérisant les textures, issus de ces matrices.

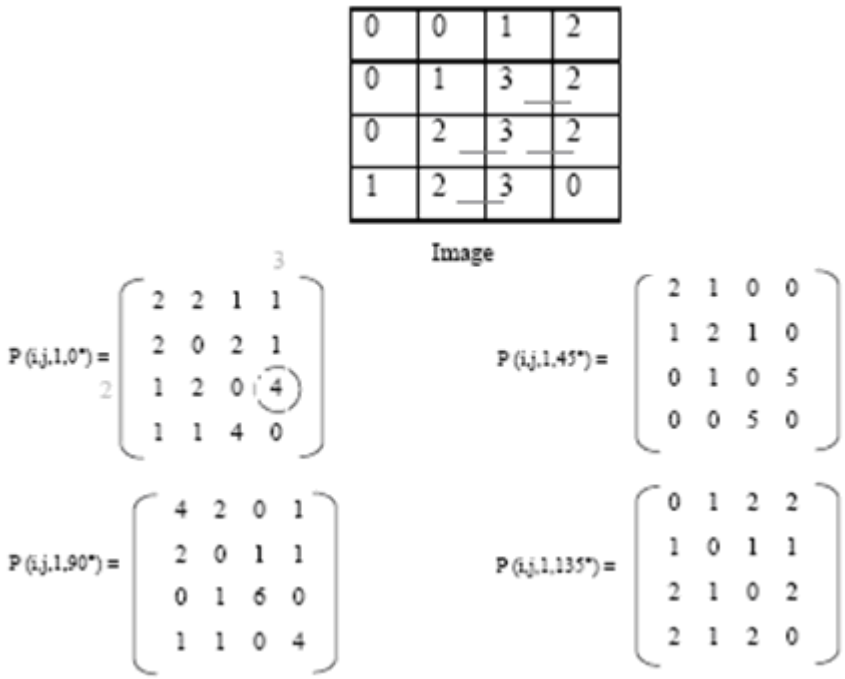


Figure 2.11 Exemple de matrices de co-occurrence construites à partir d'une image 4x4 composée de 4 niveaux de gris.

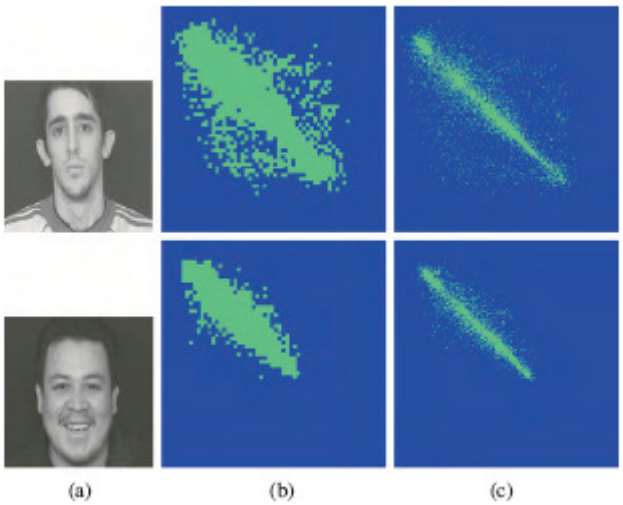


Figure 2.12 (a) exemple sur deux images de visages (b) matrice de cooccurrence avec 64 niveaux de gris (c) avec 256 niveaux de gris [44].

Notations :

La matrice de co-occurrences $P_{d,\theta}(i,j)$ représente le nombre de fois où un couple de points séparés par la distance *d* dans la direction θ a présenté les niveaux de gris de l'image *I(i,j)*. La matrice de co-occurrences $P(i,j)$ est carrée et de dimension (N_gxN_g), où N_g est le nombre de niveaux de gris présents dans l'image. Les indices de la matrice de co-occurrences sont donc les niveaux de gris de la texture étudiée.

$P_x(i)$ et $P_y(j)$ sont les probabilités marginales.

$$P_X(i) = \sum_{j=1}^{N_g} p(i,j) \tag{2.13}$$

$$P_y(j) = \sum_{i=1}^{N_g} p(i,j) \tag{2.14}$$

μ_x et μ_y sont les moyennes de $P_x(i)$ et $P_y(j)$ définit par :

$$\mu_X = \sum_{i=1}^{N_g} i p_x(i) \tag{2.15}$$

$$\mu_y = \sum_{i=1}^{N_g} i p_y(i) \tag{2.16}$$

σ_x et σ_y sont les écart types de $P_x(i)$ et $P_y(j)$:

$$\sigma_x = (\sum_{i=1}^{N_g} p_x(i)(i-\mu_x)^2)^{1/2} \tag{2.17}$$

$$\sigma_y = (\sum_{i=1}^{N_g} p_y(i)(i-\mu_y)^2)^{1/2} \tag{2.18}$$

$$p_{x+y}(k) = \sum_{i=1}^{N_g}\sum_{j=1}^{N_g} p_{i+j=k}(i,j); k = 2,3,...,2N \tag{2.19}$$

$$p_{x-y}(k) = \sum_{i=1}^{N_g}\sum_{j=1}^{N_g} p_{i-j=k}(i,j); k = 0,1,...,N-1 \tag{2.20}$$

$$HXY1 = -\sum_{i=1}^{N_g}\sum_{j=1}^{N_g} p(i,j)\log\{p_x(i)p_y(j)\} \tag{2.21}$$

$$HXY2 = -\sum_{i=1}^{N_g}\sum_{j=1}^{N_g} p_x(i)p_y(j)\log\{p_x(i)p_y(j)\} \tag{2.22}$$

$$Q(i,j)=\sum_{k=1}^{N_g}\frac{p(i,k)p(j,k)}{p_x(i)p_y(j)} \tag{2.23}$$

HX et HY sont les entropies de $P_x(i)$ et $P_y(j)$ respectivement :

$$HX=-\sum_{i=1}^{N_g}p_x(i)\log\{p_x(i)\}\ HY=-\sum_{j=1}^{N_g}p_y(j)\log\{p_y(j)\} \tag{2.24}$$

Haralick a proposé 14 caractéristiques statistiques extraites à partir de la matrice de co-occurrences, Afin d'estimer la similarité entre ces matrices. Les 14 Descripteurs de textures basés sur les co-occurrences sont :

1. **Homogénéité**

$$f_1=\sum_{i=1}^{N_g}\sum_{j=1}^{N_g}p(i,j)^2 \tag{2.25}$$

2. **Contraste**

$$f_2=\sum_{n=0}^{N_g-1}n^2\left\{\sum_{i=1}^{N_g}\sum_{j=1}^{N_g}p_{|i-j|=n}(i,j)\right\} \tag{2.26}$$

3. **Corrélation**

$$f_3=\sum_{i=1}^{N_g}\sum_{j=1}^{N_g}\frac{(i-\mu_x)\ (i-\mu_y)p(i,j)}{\sigma_x\sigma_y} \tag{2.27}$$

4. **Variance**

$$f_4=\sum_{i=1}^{N_g}\sum_{j=1}^{N_g}(i-\mu\ )^2\,p(i,j) \tag{2.28}$$

5. **Moment des différences inverses**

$$f_5 = \sum_{i=1}^{N_g}\sum_{j=1}^{N_g}\frac{p(i,j)}{1+(i-j)^2} \tag{2.29}$$

6. Moyenne des sommes

$$f_6 = \sum_{k=2}^{2N_g} k p_{x+y}(k) \tag{2.30}$$

7. Variance des sommes

$$f_7 = \sum_{k=2}^{2N_g} (k - f_6)^2 \, p_{x+y}(k) \tag{2.31}$$

8. Entropie

$$f_8 = -\sum_{k=2}^{2N_g} p_{x+y}(k) \log\{p_{x+y}(k)\} \tag{2.32}$$

9. Entropie des sources

$$f_9 = -\sum_{i=1}^{N_g}\sum_{j=1}^{N_g} p(i,j) \log\{p(i,j)\} \tag{2.33}$$

10. Variance des différences

$$f_{10} = \sum_{k=0}^{N_g-1}\Big[k - \sum_{l=0}^{N_g-1} l \, p_{x-y}(l)\Big]^2 p_{x-y}(k) \tag{2.34}$$

11. Entropie des différences

$$f_{11} = -\sum_{k=0}^{N_g-1} p_{x-y}(k) \log\{p_{x-y}(k)\} \tag{2.35}$$

12. Autres mesures de corrélation

$$f_{12} = \frac{f_9 - HXY1}{\max(HX, HY)} \tag{2.36}$$

$$f_{13} = (1 - \exp[-2(HXY2 - f_9)])^{1/2} \tag{2.37}$$

13. Coefficient de corrélation maximale

$$f_{14} = (Seconde \quad plus \quad grandes \quad valeur \quad de \quad Q)^{1/2} \tag{2.38}$$

Plusieurs recherches utilisent la matrice de cooccurrence pour la classification des textures. Mais récemment la matrice de cooccurrence et ces caractéristiques de second ordre, ont été utilisée dans la reconnaissance faciale par l'article de Mohan et al[43] en 2010 et Alaa ELEYAN, Hasan DEMIREL [44] en 2011. Pour cette raison on a choisit cette méthode récente pour notre application et pour comparer ces résultats avec notre approche proposée qui se base seulement sur les caractéristiques de premier ordre.

2.5.7 Algorithme proposé (les statistiques d'ordre un)

Dans la littérature on trouve une autre famille de méthodes qui est basée sur l'utilisation de données statistiques comme la moyenne et la variance, couplées à l'utilisation de tests ou de mesures statistiques. Différentes mesures et test ont été utilisées :

- Pour le test de Gaines et al. En 1980 ; la comparaison de deux moyennes elles permet de comparer deux échantillons d'une population ont une même moyenne. Ce test nécessite que les variances des deux échantillons soient identiques ce qui est souvent difficile à prouver. De plus la qualité du test est également très fortement dégradée par la taille des deux échantillons. Ce test n'est pas utilisé dans les applications mais il peut être utilisé dans des travaux préliminaires pour savoir s'il est possible de différencier deux individus.
- Pour le test de Wilcoxon-Mann-Whitney en 1947 ; elles permettent de vérifier que deux échantillons d'une population suivent une même distribution. Il est un peu plus fiable que le test précèdent, mais avec les mêmes inconvénients.

En effet, il existe de nombreux autres tests statistiques dont les conditions d'application et les hypothèses varient. L'avantage de ces tests est de permettre de décider (facilement et avec un faible coût de calcul) si une observation est émise par le même utilisateur que le profil, ces tests ne nécessitent que peu de données d'apprentissage. Néanmoins, on ne peut pas être sûr que l'hypothèse testée est celle qui permet de distinguer les imposteurs.

Mais dans cette thèse on a prouvée qu'on peut utiliser seulement les statistiques d'ordre un (la moyenne, l'écart type, le skewness et kurtosis) pour la reconnaissance de visage. Les résultats obtenus sont satisfaisants en terme de taux de réussite avec un faible coût de calcul.

Nous avons l'habitude de ne pas intéressée aux nombres individuelle mais aux certaines quantités descriptives comme la moyenne et la variance. En générale, la même chose est appliquée 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.

La méthode proposée se déroule comme suit :

Soit $A = (x_1 x_2 ... x_i ... x_N)$ représente une matrice de donnée de dimension $(n \times N)$ où chaque x_i 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 x_i 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 $(r \times c)$ est réduit à un vecteur caractéristique de dimension $n = (q \times (r + c))$. 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 [45][46][47] :

a. La Moyenne

La moyenne arithmétique est définit par :

$$\mu = \frac{\sum_{i=1}^{n} x_i}{n} \tag{2.39}$$

b. La Variance

La variance est une quantité importante définit par :

$$Var = \frac{\sum_{i=1}^{n} (x_i - \mu)^2}{n} \tag{2.40}$$

c. L'écart type

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

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \mu)^2}{n}} \tag{2.41}$$

d. Moment d'ordre 3 (Skewness)

$$S = \frac{\sum_{i=1}^{n}(x_i - \mu)^3}{n} \tag{2.42}$$

e. Kurtosis

$$K = \frac{\sum_{i=1}^{n}(x_i - \mu)^4}{n} \tag{2.43}$$

Puis nous faisons la photonormalisation. 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 photonormalisation 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 toutes les vecteurs caractéristiques et on divise par la déviation standard). La photonormalisation est définit par :

$$phot(x) = \frac{x - \mu_x}{\sigma_x} \tag{2.44}$$

Les figures 2.13 et 2.14 représentent la moyenne et l'écart type d'un image de visage.

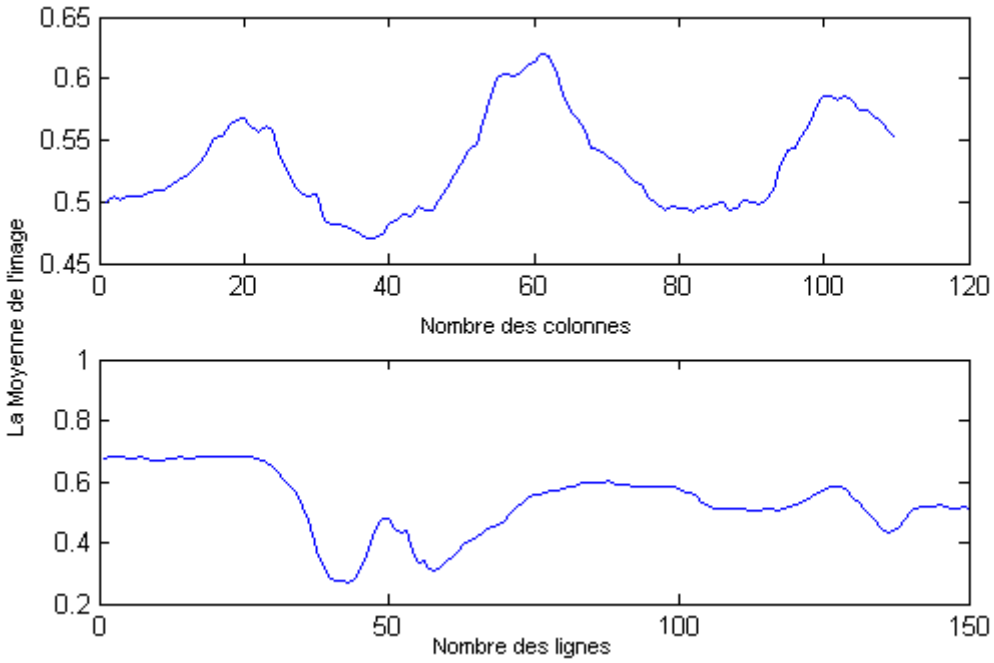


Figure 2.13 Moyenne de l'image de visage.

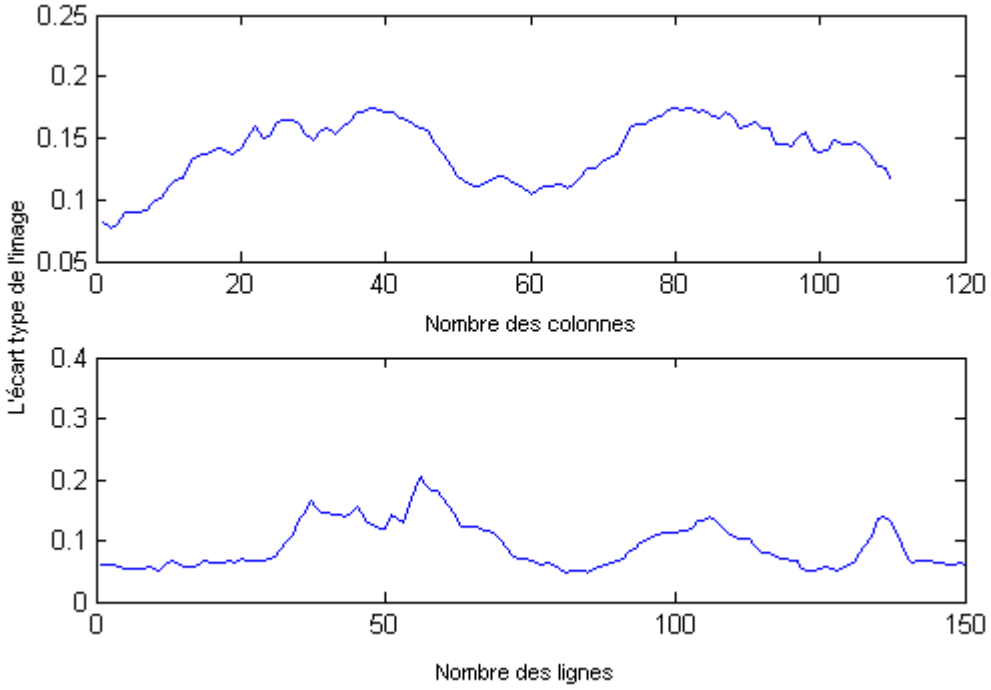


Figure 2.14 L'écart type de l'image de visage.

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 contiens 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. Un autre avantage si on compare cette méthode à la DCT est que la taille de vecteur caractéristique et très court par rapport à celle de la méthode de DCT. 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.

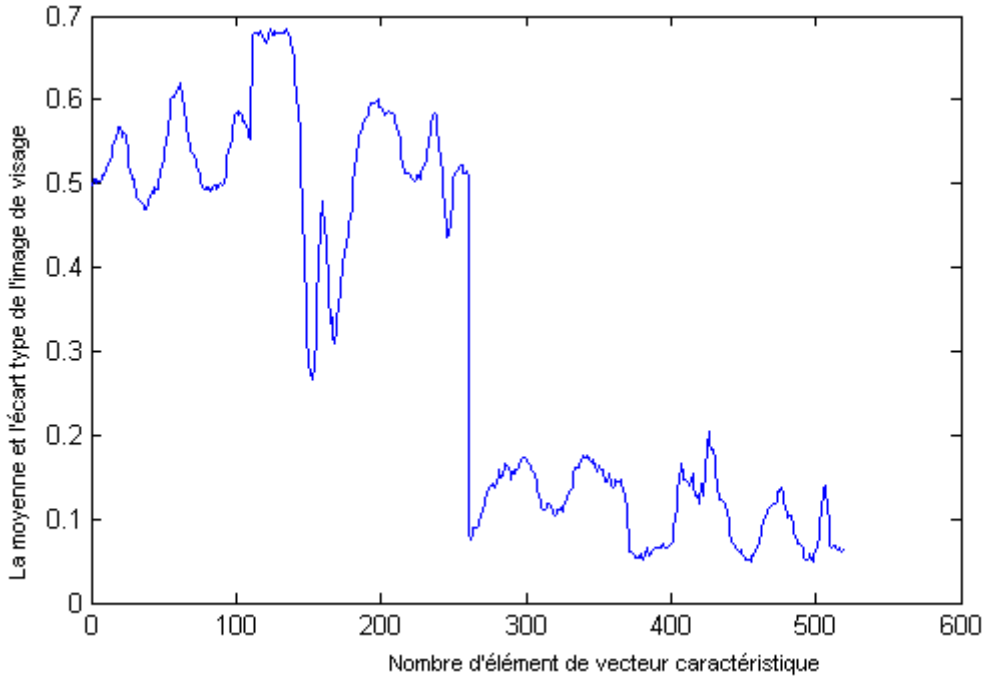


Figure 2.15 le vecteur caractéristique en combinant la moyenne et l'écart type.

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.

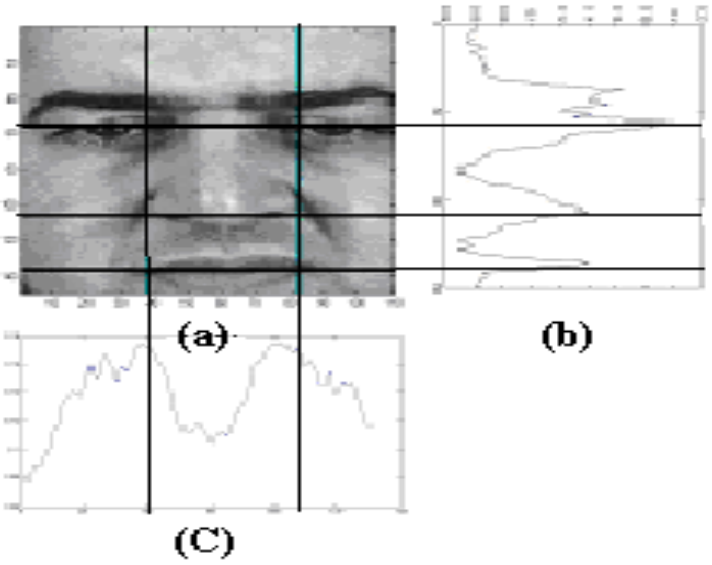


Figure 2.16 (a) image de visage (b) l'écart type verticale (c) l'écart type horizontale.

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

2.6 Conclusion

Dans ce chapitre nous avons mis en évidence les différentes avantages et inconvénients de la reconnaissance faciale, le processus de la reconnaissance de visage, les techniques utilisées sont détaillées et enfin nous avons proposé un technique basé sur les statistiques d'ordre un et dans le chapitre de résultats nous allons prouvé son efficacité et sa rapidité.

3.1 Introduction

Le but pratique de la reconnaissance Biométrique est d'avoir un système performant et applicable dans la réalité ; malgré tous les problèmes existant dans la réalité et qui perturbe la qualité de ces systèmes. On cite comme exemple les problèmes de bruit des systèmes électronique utilisé pendant le processus d'acquisition et de stockage des données. Les protocoles de test doivent être conçus soigneusement pour éviter les défauts méthodologiques, qui se produisent si l'algorithme de vérification est examiné en utilisant les mêmes données qui ont été employées pour la conception. Et comme notre objectif repose sur une modalité spécifique qui est la reconnaissance de visage, plusieurs banques d'images ont été créées afin de comparer les différentes méthodes entre elles selon diverses conditions (éclairage, pose, occultations, etc.). Parmi celles-ci, il y a notamment la FERET , AR-face, AT&T (appelée auparavant Olivetti), X2MVTS [48], Yale, MIT, Achermann ainsi que plusieurs autres. Chacune d'entre elles possède évidemment ses particularités spécifiques ainsi que ses qualités et Défauts. Nous allons présenter dans ce chapitre**,** la base de données des visages qui a été choisie pour nos expériences. Ainsi le protocole expérimental qui a été soigneusement conçu pour cette base de données. La base de données que nous avons travaillée sur laquelle est une base multimodale développée au sein du projet européen ACTS, elle contient des images fixes, des séquences vidéo et des images faciales de 295 personnes. Elle est utilisée pour la vérification d'identité. La base de données XM2VTS a été réalisée sur une longue période ce qui a permis d'obtenir plusieurs images d'une même personnes et donc une grande variabilité d'apparence (changement de coiffure, présence et/ou absence de lunettes, …etc.). Par contre, seules les expressions neutres ont été considérées. La motivation pour le choix de cette base de données est principalement sa taille tout à fait grande, et sa popularité. On a choisis la base de données prolongée XM2VTS puisqu'elle est devenue une norme dans la communauté biométrique audio et visuelle de vérification d'identité

3.2 Présentation de la base de données XM2VTS

XM2VTS est une base de données multimodale publiquement disponible, elle est enregistrée spécifiquement pour évaluer l'exécution des approches biométriques à la vérification d'identité. Elle contient les enregistrements synchronisés des visages et des paroles de 295 personnes. Les sujets ont été enregistrés en quatre sessions séparées uniformément distribuées pendant 5 mois. En effet, C'est le centre CVSSP (Centre for Vision, Speech and Signal Processing), de l'université de Surrey, en grande Bretagne, qui a conçu la base de données

XM2VTS, pour permettre la comparaison de différents méthodes de vérification d'identité. Elle succède à la base de données M2VTS (Multi Modal Verification for Teleservices and Security applications). Sa construction s'inscrit dans le cadre du projet européen ACTS qui a pour but d'étudier le contrôle d'accès par une vérification multimodale d'identité.

La session se compose de deux enregistrements. Un enregistrement pour les séquences de la parole et un enregistrement pour les séquences vidéo de la tête. Pour chaque personne huit prises ont été effectuées en quatre sessions distribuées pendant cinq mois afin de prendre en compte les changement d'apparence des personnes selon plusieurs facteurs (lunettes, barbe, coupe de cheveux, pose…). Les vidéos et photos sont en couleur de haute résolution (format ppm) , la taille est de 256 x 256 pixels pour les images et de très bonne qualité codé sur 24 bits dans l'espace RGB. Cela permet de travailler en niveaux de gris ou en couleur. Le choix principal de XM2VTS est sa taille grande, avec 295 personnes et 2360 images en total et sa popularité puisqu'elle est devenue une norme dans la communauté biométrique audio et visuelle de vérification multimodale d'identité.

Nous ne nous intéresserons évidemment, dans le cadre de ce projet, qu'aux photographies prises de face pour le processus de l'authentification de visage. L'éclairage des faces de ces deux ensembles est contrôlé. La figure 3.1 présente des images de face typiques de la base de données XM2VTS [48].

Figure 3.1 Images typiques de la base de données XM2VTS.

3.3 Le protocole de Lausanne

Si on parle d'une base de donnée pour la vérification d'identité cela veut dire la nécessiter d'un protocole performant qui permet la comparaison entre les algorithmes de vérification.

Pour la base de donnée XM2VTS le protocol associé s'appelle le protocole de lausanne [49] Sont principe est de partager la base de données en deux classes, 200 personnes pour les clients, et 95 pour les imposteurs.

La base de données est divisée en trois ensembles : apprentissage, évaluation et test. L'ensemble apprentissage permet de construire les modèles de clients. L'ensemble test est utilisé pour calculer les scores des clients et des imposteurs. En fonction de ces scores, un seuil est choisi afin de déterminer si une personne est acceptée ou non.

- L'ensemble **d'apprentissage :** il contient l'information concernant les personnes connues du système (seulement les clients).
- L'ensemble de **évaluation :** permet d'établir les paramètres du système de reconnaissance de visage.
- L'ensemble de **test :** permet de tester le système en lui présentant des images de personnes lui étant totalement inconnues.

Il existe Deux configurations différentes, la configuration I et la configuration II [49].

Nous utiliserons la configuration I dans le cadre de cette thèse puisqu'elle est la plus dure.

Dans la configuration I, pour la formation de l'ensemble d'apprentissage trois images par client sont employées afin de créer les caractéristiques ou modèles clients. L'ensemble d'évaluation est constitué de trois autres images par client, ils sont utilisés essentiellement pour fixer les paramètres de l'algorithme de reconnaissance ou de vérification des visages. L'ensemble de test est formé par les deux autres images restantes.

Pour la classe des imposteurs, les 95 imposteurs sont réparties dans deux ensembles : 25 pour L'ensemble d'évaluation et 75 pour l'ensemble de test.

La répartition des images selon la configuration I est représentée par la figure 3.2.

<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</td><td rowspan="2">Test</td></tr>
<tr><td>2</td></tr>
</table>

Figure 3.2 Répartition des images de la base de données selon la configuration I

Dans la configuration II, pour la catégorie clients, quatre images par clients des deux premières sessions sont employées pour former l'ensemble d'apprentissage et les deux images de la troisième session constituent l'ensemble d'évaluation, alors que les deux images restantes de la quatrième session constituent l'ensemble de test. Pour la catégorie imposteurs la répartition est identique à la répartition de la configuration I.

La répartition des l'images selon la configuration II est représentée par la figure 3.3.

<table>
<tr><th>Session</th><th>Pause</th><th>Clients</th><th colspan="2">Imposteurs</th></tr>
<tr><td>1</td><td>1
2</td><td rowspan="3">Apprentissage</td><td rowspan="5">Evaluation</td><td rowspan="5">Test</td></tr>
<tr><td>2</td><td>1
2</td></tr>
<tr><td>3</td><td>1
2</td><td>Evaluation</td></tr>
<tr><td>4</td><td>1
2</td><td>Test</td></tr>
</table>

Figure 3.3 Répartition des images de la base de données selon la configuration II

Les tailles des différents ensembles de la base de données selon les deux configurations cités précédemment sont reprises dans le tableau 3.1.

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)

Tableau 3.1 Répartition des photos dans les différents ensembles.

3.4 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 des différents techniques utilisé dans cette thèse et avec les techniques des autres chercheurs. Aussi parce que les images sont en couleur et c'est l'information couleur que nous s'intéresse dans ce travail afin de prouver l'importance de la couleur à l'authentification de visage. Le chapitre suivant décrit les espaces couleurs utilisées.

4.1 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. On nomme couleur la perception par l'oeil d'une ou plusieurs fréquences d'ondes lumineuses, avec des amplitudes donnée.

L'ensemble des couleurs est défini par ses trois caractéristiques de teinte, valeur et saturation. L'ensemble des fréquences des ondes lumineuses forme le spectre des Couleurs allant des infrarouges aux ultraviolets. La teinte c'est les fréquences qui engendrant la couleur. La valeur est l'amplitude lumineuse définissant la couleur. Plus elle est proche du noir, plus la valeur est basse. Et la saturation c'est la pureté d'une couleur. Et on appelle le gris les couleurs intermédiaires entre le blanc et le noir. Le noir est un gris de valeur nulle et correspond à l'absence de toute lumière. Le blanc est un gris de valeur maximale et peut être considéré comme une plénitude de couleurs.

Nous présentons ici les espaces les plus couramment utilisés. La majorité de connaissances suivants sont extrait de [50], [51] [52] et [53][54].

4.2 Image numérique couleur

Dans un système de vision industrielle, différent éléments, représentés sur la figure 4.1, interviennent pour restituer l'information couleur. Ce sont d'abord l'éclairage et les matériaux dont sont constitués les objets de la scène observée qui vont déterminer les propriétés physiques de la couleur.

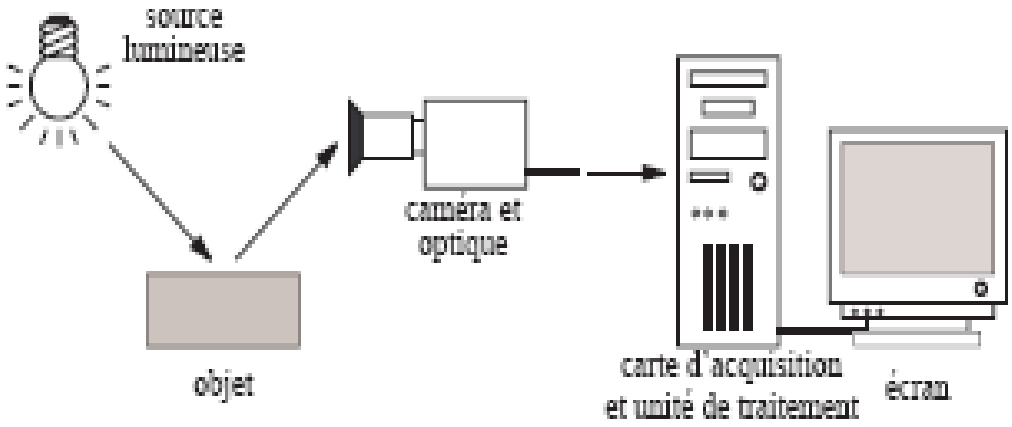


Figure 4.1 Vision artificielle.

Les images couleur sont ensuite acquises généralement par une caméra vidéo couleur associée à un dispositif optique puis numérisées par un ordinateur via une carte 'acquisition La visualisation de ces images couleur est généralement réalisée sur un écran à tube cathodique via la carte vidéo de l'ordinateur. C'est donc l'ordinateur qui assure la liaison entre les entrées et les sorties associées aux périphériques ainsi que les traitements à appliquer sur les images.

4.3 Les espaces couleurs utilisé

L'espace couleur RGB est le plus connu des espaces de couleur et à partir de trois couleurs primaires dont les trois plus usités sont le rouge, le vert et le bleu on peut produire toutes les couleurs possibles. Il existe cependant d'autres méthodes de représentation des couleurs qui ont été développés et d'autres qui sont en cours de développement pour diverses raisons : certains espaces sont liés à des équipements spécifiques (télévision, imprimantes, caméras), d'autres ont été développés pour des traitements numériques liés à l'imagerie couleur. Parmi les espaces couleurs qui existent dans la littérature, nous avons travaillé avec les espaces couleurs ci-dessous ; afin de répondre à la question 'quelle est l'espace adéquat à notre problème'.

4.3.1 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.

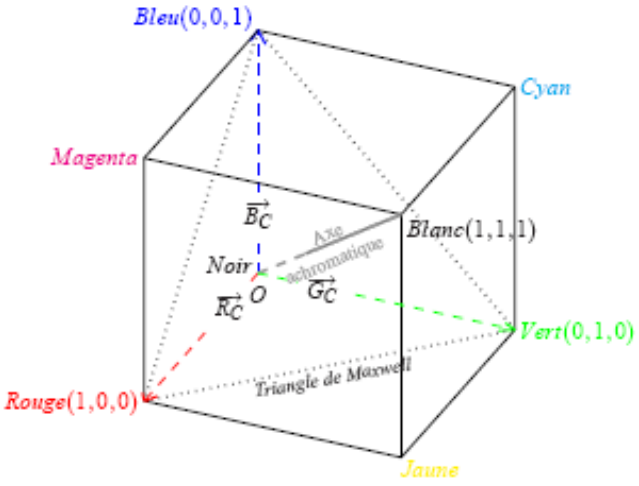


Figure 4.2 Cube des Couleurs.

Mais on trouve que l'espace RGB défini par la CIE présente quelques inconvénients comme l'existence d'une partie négative (figure 4.3) 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.).

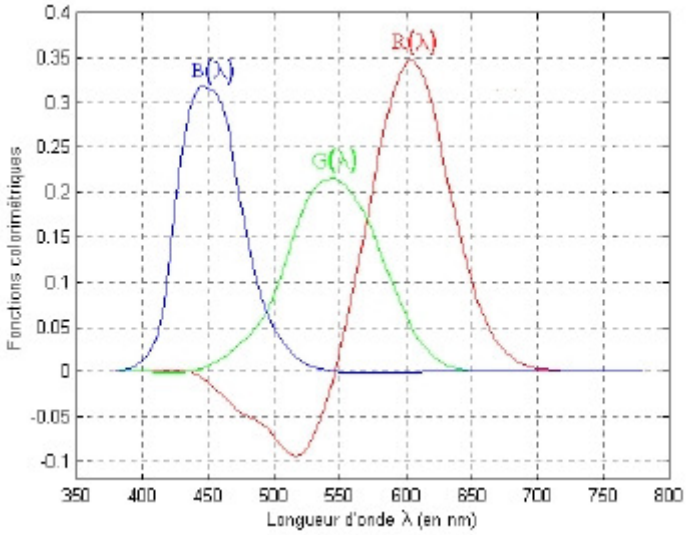


Figure 4.3 Les courbes d'appariement R(λ), G(λ) et B(λ) correspondant aux Expériences d'égalisation avec standardisées par la CIE en 1931.

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.

4.3.2 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 (figure 4.4) 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.

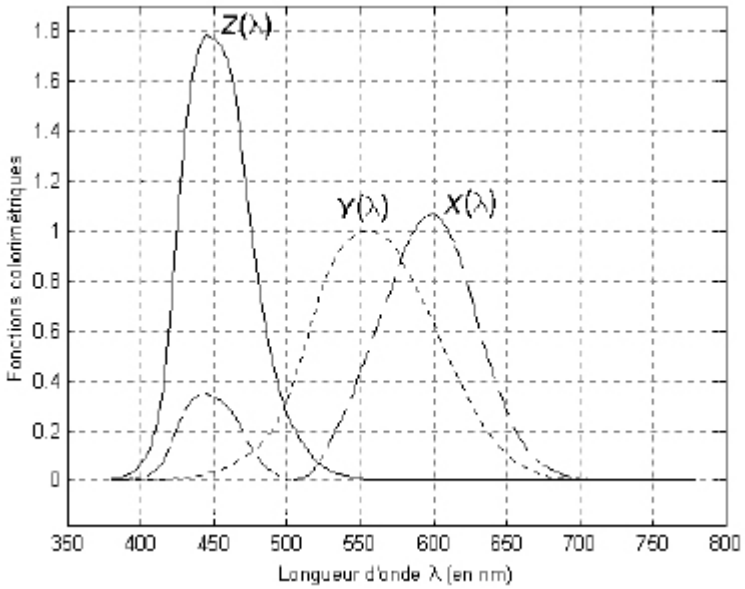


Figure 4.4 Les fonctions colorimétriques X(λ), Y(λ) et Z(λ).

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 :

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} 2.7690 & 1.7518 & 1.1300 \\ 1.0000 & 4.5907 & 0.0601 \\ 0.0000 & 0.0565 & 5.5943 \end{pmatrix} \begin{pmatrix} R \\ V \\ B \end{pmatrix} \tag{4.1}$$

4.3.3 L'espace de couleur LAB

Il est Défini en 1976 par la CIE, ce modèle est basé sur la façon dont l'oeil humain perçoit les couleurs, C'est un espace plus uniforme dans lequel Deux couleurs proches en distance le sont aussi pour l'oeil. Une représentation 3D de l'espace CIELab est donnée à la figure 4.5. Le point achromatique est au centre du repère. Les valeurs 0 et 100 du L représentent un noir et un blanc de référence respectivement. Les valeurs a* et b* représentent les attributs rouge-vert et jaune-bleu respectivement et elles sont non cohérentes.

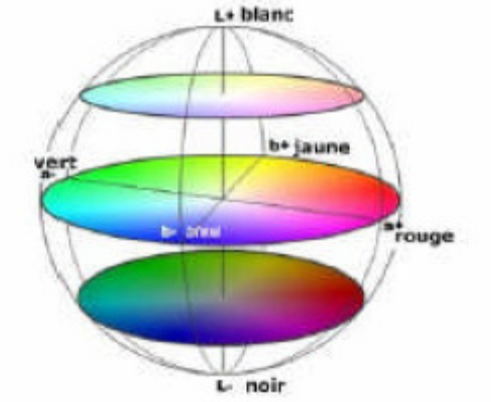


Figure 4.5 Espace chromatique CIE LAB.

Le modèle Lab est basé sur la transformation non linéaire de modèle XYZ. Ce modèle est représenté en fonction du blanc de référence dont voici les valeurs dans l'espace XYZ:

$$\text{Si } \frac{Y}{Y_W} > 0.008856 \ : \ L = 25\left(100\frac{Y}{Y_W}\right)^{\frac{1}{3}} - 16 \approx 116\left(\frac{Y}{Y_W}\right)^{\frac{1}{3}} - 16 \tag{4.2}$$

$$\text{Sinon : } L = 903.3\frac{Y}{Y_W} \tag{4.3}$$

$$\begin{cases} a^* = 500\left(f\left(\frac{X}{X_W}\right) - f\left(\frac{Y}{Y_W}\right)\right) \\ b^* = 200\left(f\left(\frac{Y}{Y_W}\right) - f\left(\frac{Z}{Z_W}\right)\right) \end{cases} \tag{4.4}$$

$$\text{Avec : } \quad f(x) = x^{\frac{1}{3}} \quad \text{si } x>0.008856 \tag{4.5}$$

$$f(x) = 7.787x + 16/116 \quad \text{sinon} \tag{4.6}$$

Où X_W, Y_W et Z_W sont les composantes XYZ d'un blanc de référence.

4.3.4 L'espace de couleur HSV

Nous choisissons le modèle « HSV » car c'est le plus couramment employé dans les logiciels de référence dans le traitement numérique en terme de retouches couleurs. HSV pour Hue Saturation Value (nuance, saturation et luminosité), L'intérêt de cet espace est que ces composantes sont très proches de la perception humaine des couleurs. La composante Nuance dans cet espace est composée de mesures angulaires, analogues à la position autour du disque

de couleurs. Une nuance égale à zéro indique la couleur rouge, 120 pour le vert et 240 pour le bleu. La composante saturation dans donne l'intensité de la couleur. Une saturation égale à zéro indique que l'image est en niveaux de gris. Pour la composante Luminosité Une valeur égale à zéro représente la couleur noire et une valeur maximale donne une couleur la plus lumineuse possible. Les espaces RGB et HSV sont des transformations non linéaire l'un de l'autre donc plus discriminantes.

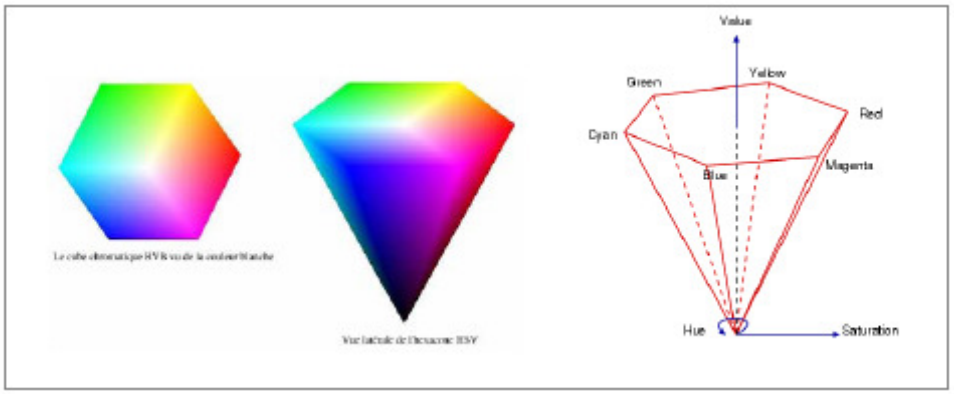


Figure 4.6 Représentation du modèle HSV.

Le passage d'un système RGB au système HSV est donné par les équations non linéaires suivantes :

$$V = \frac{R+G+B}{3} \tag{4.7}$$

$$S = 1 - \frac{3\min(R,G,B)}{R+G+B} \tag{4.8}$$

$$H = \cos^{-1}\left(\frac{0.5((R-G)+(R-B))}{\sqrt{((R-G)^2+(R-B)(G-B))}}\right) \text{ si } B<G, \text{ sinon } H=2\pi-H \tag{4.9}$$

L'intensité varie donc de 0 (noir) à 1 (blanc). La saturation n'est pas définie pour le noir (0,0,0). Elle varie de 0 (niveaux de gris) à 1 (couleurs du contour). La teinte n'est pas définie pour les niveaux de gris. La teinte varie de 0 (rouge) à 2π (rouge) en passant par 2π/3 (vert) et 4π/3 (bleu).

4.3.5 L'espace de couleur I1I2I3

Cet espace a été introduit en 1980 par Ohta, Kanade et Sakai. Il est inspiré de la transformation de Karhunen_Loeve afin de déterminer les trois axes de plus grande variance de l'ensemble des couleurs. Cet espace est une transformation linéaire à partir de l'espace RGB où I_1 correspond à la composante de luminance. I_2 et I_3 représentent respectivement les oppositions bleu-rouge et magenta-vert.
Il a définie par les formules suivantes :

$$I1 = \frac{R + G + B}{3} \tag{4.10}$$

$$I2 = \frac{R - B}{2} \tag{4.11}$$

$$I3 = \frac{2G - R - B}{4} \tag{4.12}$$

4.3.6 L'espace de couleur YCrCb

Cet espace fait partie d'un ensemble défini en 1976 par la CIE, Dans ce modèle, Y représente la luminance (monochrome) et Cr et Cb sont les composantes de couleur. En vidéo, YCrCb est un modèle de représentation de chaque pixel d'une image par sa luminosité, et ses composantes rouge et bleue. A l'aide de ces trois informations, il est possible de reconstituer les composantes RGB. L'avantage de passer de RGB à Y-Cr-Cb est que l'information est dissociée en luminance, qui est la partie la plus porteuse d'informations pour notre cerveau, et en chrominances.
La vision colorée est caractérisée par trois sensations distinctes, traduites par des grandeurs subjectives qui sont la luminance, la teinte et la saturation. Le but pour un espace de couleur est d'être le plus proche de la vision humaine, afin de ne transmettre que les informations qui seront pertinentes pour le cerveau.

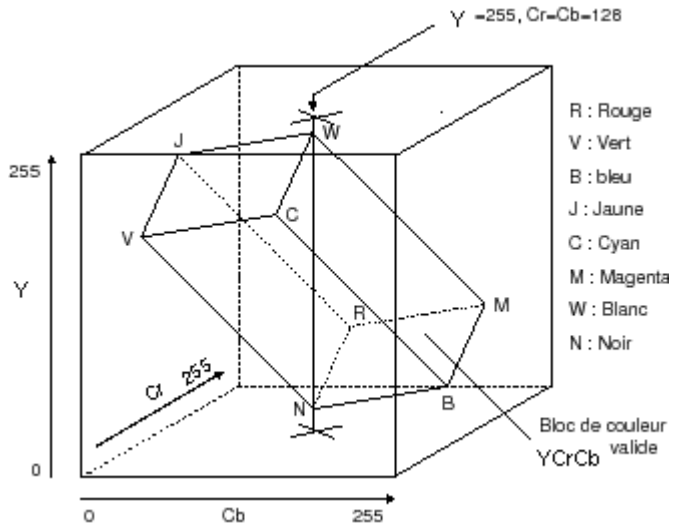


Figure 4.7 Représentation de l'espace YCrCb

Plusieurs mots permettent de définir une partie de la couleur :

- La luminance : elle qualifie l'impression d'intensité ou de vivacité d'une lumière ; elle est liée à la puissance du rayonnement reçue par l'œil, et bien sûr, à la sensibilité de celui-ci en fonction de la longueur d'onde.
- La teinte est la sensation colorée que nous interprétons en fonction de la longueur d'onde dominante de la radiation.
- La saturation est liée à la pureté ou la saturation de la radiation.

Nous allons maintenant expliquer comment nous passons de l'espace RGB à l'espace YCrCb. Pour ce changement d'espace, on passe par une valeur temporaire de manière à simplifier les Calculs :

Temp = R - (G + B) / 2. Ensuite, nous calculons la valeur des trois composantes :

$$\begin{aligned} Y &= B + G + Temp / 2 \\ Cr &= G - (Y / 2 + Temp / 16) \\ Cb &= Temp + (3 * Cr / 4) \end{aligned} \qquad (4.13)$$

Pour la réciproque, nous avons de nouveau recours à une variable temporaire pour aboutir à la matrice suivante :

$$\begin{aligned} Temp &= Cb - (3 * Cr) / 4 \\ G &= Cr + (Y / 2 + Temp / 16) \\ B &= Y - G - Temp / 2 \\ R &= Temp + (G + B) / 2 \end{aligned} \qquad (4.14)$$

4.3.7 L'espace de couleur YUV

En 1976, la CIE propose un nouveau système tridimensionnel perceptuellement uniforme, le système CIEYUV. Le système de représentation YUV est un codage vidéo basé sur les composantes de luminance (Y) et de chrominance (UV). L'information de luminance correspond ici à la clarté qui, dans le vocabulaire de la CIE, représente la réponse de l'oeil à un niveau de luminance. les composantes de chrominance respectives de U et V correspondant au blanc de référence.

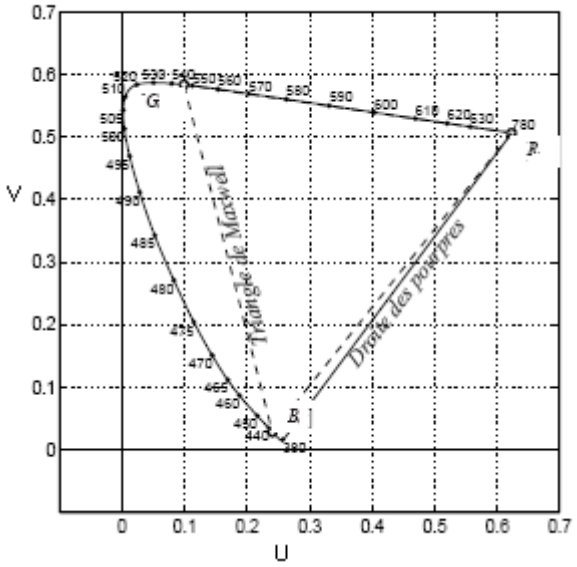


Figure 4.8 Diagramme de chromaticité (U,V).

Cet espaces est utilisée en télévision pour transmettre les images vidéos, les téléviseurs noirs et blancs reproduisent sur l'écran le Y, alors que les les téléviseurs modernes reconstruisent le signal RGB à partir des trois composantes YUV.

La transformation de cet espace est rapide puisqu'elle s'effectue par simple changement linéaire matriciel.

$$\begin{bmatrix} Y \\ U \\ V \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{4.15}$$

selon une approche physiologique corrigée par les données de la psychométrie : on a alors recours à des espaces comme le CIE LAB (1976) et le PAL YUV mais L'espace CIE YUV présente de nombreux avantages sur beaucoup de points. Il semble en effet être approprié au traitement informatique que nous souhaitons réaliser. Par exemple pour la détermination des

grandeurs LAB est complexe et fait intervenir des équations présentant une puissance 1/3. Or, cette puissance utilisée dans les algorithmes de traitement d'images animées allonge énormément les temps de calculs. Au contraire, le calcul est simplifié pour passer des valeurs RGB aux valeurs YUV, car les formules sont cette fois linéaires. Cette propriété est à l'avantage des processeurs informatiques, en terme de temps de calculs de rendus. Aussi, Les espaces CIE LAB et PAL YUV, ont été jugés de mérites équivalents. Aucun n'est plus uniforme que l'autre. Cependant, les valeurs numériques obtenues par les deux formules de différence couleurs sont la plupart du temps différentes, surtout pour les couleurs saturées. Pour des simplifications d'opérations et de représentation, l'espace PAL YUV est adéquat comme espace de traitements des couleurs.

4.3.8 L'espace de couleur YIQ

Le système de télévision en couleur NTSC utilise une base de couleurs YIQ. Dans ce système le Y est le même que la fonction de luminance Y de CIE XYZ et sert pour la transmission en noir et blanc. La chrominance est encodée dans les champs I (in phase) et Q (quadrature) où I représente l'axe des couleurs de la peau (orange-cyan) et Q l'axe des vert-pourpre.
La conversion de RGB à YIQ est définie par la matrice linéaire suivante :

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.275 & -0.321 \\ 0.212 & -0.528 & 0.311 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{4.16}$$

4.4 Conclusion

Dans ce chapitre nous avons exposé les espaces couleur utilisée dans notre travail. Après les résultats obtenus avec ces espaces couleur on peut répondre à la question de notre problème c'est à dire l'espace adéquat à la l'authentification de visage. 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 et le chapitre suivant montre l'efficacité d'un espace couleur par rapport aux différentes espaces de couleurs utilisé.

5.1 Introduction

Après une présentation des différentes techniques de reconnaissance de visage dans le chapitre précèdent ; maintenant il faut appliquer ces techniques pratiquement et voir ainsi les avantages et les inconvénients de chaque 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 de ces algorithmes dépend beaucoup de la qualité des résultats de détection et de normalisation des visages. Les expériences ont été développées sur les visages de la base XM2VTS dont les images sont prises dans des conditions favorables (une vue frontale de toutes les images, l'éclairage des visages ne change pas et une distance fixe entre le visage et la caméra). Le choix principal de cette base de données est sa grande taille, avec 295 personnes et 2360 images en total et sa popularité, puisqu'elle est devenue une norme dans la communauté biométrique audio et visuelle de vérification multimodale d'identité [48]. Pour chaque personne huit prises ont été effectuées en quatre sessions distribuées pendant cinq mois. Le protocole lié à XM2VTS divise la base en deux catégories 200 clients et 95 imposteurs, les personnes sont des deux sexes et de différents ages. Les photos sont en couleur de haute qualité et de taille (256x256).

La figure 5.1 représente quelques exemples d'images de visages de la base de données XM2VTS.

Figure 5.1 quelques exemples d'images de visages de la base de données XM2VTS.

Le système de reconnaissance de visage peut être composé de trois étapes à savoir : la détection et prétraitement de visage, extraction de caractéristiques et reconnaissance de visages.

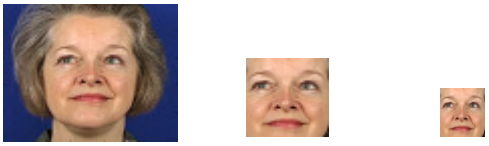
5.2 Prétraitement

Le prétraitement est une phase importante dans le processus d'authentification ; c'est une méthode simple qui augmente en général les performances du système. Elle permet souvent une première réduction des données et elle atténue les effets de différentes conditions lors des prises de vues. En regardant les images on aperçoit directement qu'apparaissent au niveau du cou des particularités non souhaitées comme les cols de chemise,….etc. par ailleurs les cheveux sont également une caractéristique changeante au cours temps. C'est pourquoi nous

avons décidé de couper les images dont l'opération est d'extraire seulement les paramètres essentiels pour l'identificateur et qui changent très peu avec le temps. On utilise filtrage uniforme passe- bas pour la décimation (seulement lorsqu'on appliquent les méthodes : LDA et EFM). Quand les images sont filtrées par un filtre passe–bas, on peut réduire bien étendu la résolution des images. Ainsi les images de dimension (NxM) après découpage se transforment en une dimension (N/2xM/2) après décimation (voir figure 5.2 puis nous faisons la photonormalisation aux images. Lla photonormalisation a un double effet : d'une part elle supprime pour tout vecteur un éventuel décalage par rapport à l'origine et ensuite elle supprime tout effet d'amplification (multiplication par un scalaire). Pour chaque image on effectue l'opération suivante :

$$photonormalisation(x) = \frac{x - mean(x)}{std(x)} \tag{5.1}$$

Finalement on applique la normalisation qui s'agit sur un groupe d'image (pour chaque composante, on retire la moyenne de cette composante pour toutes les images et on divise par la déviation standard) .



(a) (b) (c)

Figure 5.2 a) image d'entrée, b) image après découpage et c) image après décimation.

5.3 Extraction des caractéristiques

L'extraction des caractéristiques se fait par les méthodes expliquées déjà dans le chapitre 02.

5.4 Classification

Dans le problème de vérification d'identités, nous cherchons à définir, pour chaque personne, ou de manière globale, un seuil. Ce dernier va déterminer le minimum de ressemblance entre deux images pour admettre qu'il s'agit de la même personne .Ce minimum de ressemblance va s'exprimer comme une distance maximale entre les caractéristiques des deux images. Le problème qui nous occupe il contient deux classes, à savoir d'une part les clients et d'autres part les imposteurs .Un système d'authentification impitoyable et extrêmement strict indique un TFA (Taux de Fausse Acceptation) faible et un TFR (Taux de Faux Rejet) élevé. Par

contre un système laxiste sera caractérisé par un TFA élevé et un TFR plutôt bas. Le juste milieu situe quelque part entre les deux, et si les taux d'erreurs sont égaux, il se trouvera au taux d'égale erreur ou TEE.

Tous ces taux d'erreurs ont été calculés dans deux ensembles d'abord dans un ensemble d'évaluation, qui va permettre de fixer plus ou moins le TEE en faisant varier les paramètres d'acceptation et de rejet du système. Ensuite, dans un ensemble de test en utilisant les paramètres fixés précédemment. Ainsi, on peut vérifier la robustesse du système d'authentification de visage.

5.5 Mesure de similitude

Une fois que les caractéristiques des images sont extraites, il reste à déterminer quelles sont les images semblables. Il y a beaucoup de mesures possibles de distance et de similitude, mais ici on a choisi la corrélation puisque nous donne les meilleurs résultats par rapport aux d'autre mesure de similitude et parce que la corrélation est mieux adaptée à des données du grande dimension. Elle mesure le taux de changement entre les composantes de deux vecteurs *A* et *B*. Elle est donnée par la relation :

$$Corr(A,B) = \sum_{i=1}^{N} \frac{(A_i - \mu_A)(B_i - \mu_B)}{\sigma_A \sigma_B} \tag{5.2}$$

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

5.6 Fusion des experts

Dans le but d'améliorer les performances du système d'authentification nous avons essayé d'utiliser la fusion logique de décisions pour les composantes couleurs et la fusion non linéaire par réseau de neurone. Avant de donner les résultats de chaque technique nous allons expliquer la fusion logique et la fusion non linéaire.

5.6.1 La fusion logique

Pour améliorer les performances du système d'authentification, nous avons utilisé la fusion logique des décisions trouvées pour chaque composante d'un même espace couleur. La fusion des décisions se fait alors par des opérateurs logiques comme le OR ou le AND ou de prendre deux décisions parmi trois (2 AND). Le tableau 5.1 explique les différentes opérations de fusion logique des décisions :

Espace couleur	Résultat de la composant	Résultat de la fusion		
		OR	2 AND	AND
1er composante	Client	Client	Client	Imposteur
2ème composante	Imposteur			
3ème composante	Client			

Tableau 5.1 la fusion logique des résultats

Si le système d'authentification de visage répond par oui c'est un client avec la première composante couleur et non par la deuxième composante couleur alors la décision sera oui c'est un Client avec l'opérateur OR et non c'est un imposteur avec l'opérateur AND. Et dans le cas de l'opérateur (2 AND) c'est la troisième composante couleur qui décide, si c'est un client alors nous avons deux qui décident que c'est un client parmi les trois donc c'est une décision de vote des trois, et dans le cas contraire c'est un imposteur.

5.6.2 La Fusion non linéaire

Pour l'amélioration de la performance de ce système, nous avons l'idée de fusionner les résultats de chaque composants d'un espace couleur, pour cela nous avons appliquer la fusion non linéaire pour la classification avec un réseau de neurone simple de type MLP (Multi layer perceptron). Ce réseau est constitué de trois couches : couche d'entrée, couche cachée et couche de sortie. Chaque couche contient un nombre fini des unités qu'on appelle les neurones qui reçoivent les signaux d'activation des autres neurones, en traitant puis transmettant le signal de sortie à toutes les unités de la couche suivante. Chaque neurone de la couche (i-1) est connecté à tous neurone de couche (i). Il n'existe aucune connexion entre les unités d'une même couche.

La figure 5.3 montre le schéma synoptique d'un réseau de neurone MLP à une couche cachée. Dans notre travail nous avons utilisé le réseau MLP comme un classifieur binaire (client où imposteur).

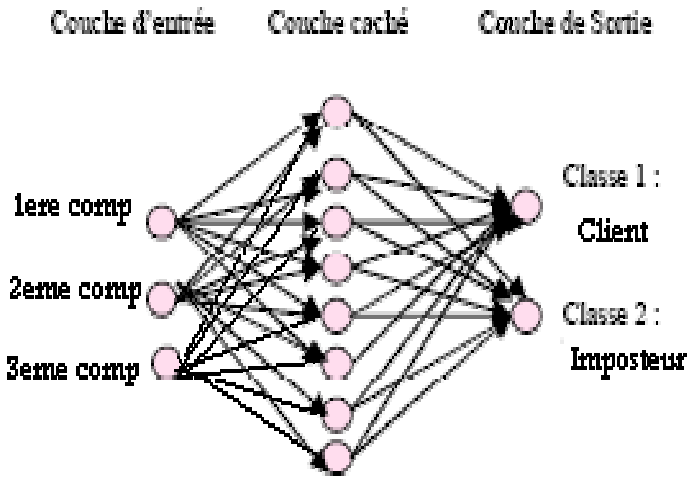


Figure 5.3 Un réseau MLP à une couche cachée.

Nous avons entraîné le MLP avec des paires éléments (distances intra des Clients, distances extra des imposteurs) de l'ensemble d'évaluation pour fixer les paramètres du réseau MLP. Pour évaluer les performances du système d'authentification en utilisant un classifieur MLP. On calcule les taux de succès de ce classifieur dans l'ensemble de test.

Les paramètres choisis pour notre MLP sont :

- Une couche cachée avec neuf neurones
- Trois neurones dans la couche d'entrée
- Deux neurones dans la couche de sortie

Les paramètres d'entrée du réseau MLP sont :

- La distance en utilisant la première composante couleur.
- La distance en utilisant la deuxième composante couleur.
- La distance en utilisant la troisième composante couleur.

5.7 Présentation des résultats de chaque technique utilisée

Le but essentiel de notre système d'authentification de visage est de donnée une décision binaire avec le minimum taux d'égale erreur, c'est-à-dire que ce système d'authentification répondre par oui si c'est un client où non si c'est un imposteur avec bien sur le minimum taux d'exécution possible. Pour plus de performance nous avons effectué nos expériences sur plusieurs espaces de couleurs et nous avons fusionné les différentes espaces de couleur de chaque technique.

5.7.1 Authentification de visage par LDA

Nous avons trouvé que l'utilisation de la représentation en niveaux de Gris donne un taux de succès TS de l'ordre de **93.30%** avec la méthode d'analyse linéaire discriminante LDA. Nous avons testé l'information couleur sur LDA afin d'améliorer la performance de ce système. Pour cela nous avons choisi les paramètres de la méthode LDA suivants :

- Prétraitement avec photonormalisation
- Composante couleur : RGB, XYZ, LAB, HSV, I1I2I3, YUV, YCrCb, YIQ.
- Coefficients : 100 coefficients de projection triés suivants les valeurs propres décroissantes.
- Mesure de similarité: corrélation.
- Seuillage : Globale.

Les résultats obtenus avec ces paramètres sont présentés dans le tableau 5.2. Nous remarquons dans ce tableau une propriété très importante c'est que les différents taux d'erreurs sont très stables dans les différents ensemble (évaluation et test). La méthode LDA donne assez bons de résultats. Avec seulement 100 caractéristiques on peut atteindre un taux de succès de l'ordre de **96.10**% en utilisant la composante couleur Cr seule de l'espace couleur YCrCb et un taux d'égale erreur TEE de l'ordre de **1.65**%. Cela veut dire que le TS présente une amélioration de **2.8**% par rapport à l'utilisation des images en niveaux de gris.

Couleur	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE (%)	TFR	TFA	TS (%)
X	0,030	0,030	3,01	0,030	0,031	93,91
Y	0,032	0,033	3,22	0,025	0,035	93,97
Z	0,027	0,027	2,69	0,018	0,030	95,23
Y	0,030	0,030	2,99	0,033	0,031	93,62
Cr	**0,017**	**0,016**	**1,65**	**0,023**	**0,017**	**96,10**
Cb	0,032	0,032	3,20	0,025	0,029	94,62
R	0,037	0,036	3,65	0,048	0,033	91,94
G	0,030	0,031	3,04	0,023	0,032	94,56
B	0,027	0,026	2,65	0,015	0,030	95,53
Y	0,032	0,033	3,22	0,030	0,032	93,78
I	0,028	0,028	2,83	0,028	0,022	95,03
Q	0,020	0,020	1,99	0,030	0,020	94,99
Y	0,032	0,033	3,22	0,030	0,032	93,78
U	0,030	0,031	3,05	0,020	0,027	95,33
V	0,022	0,021	2,13	0,025	0,022	95,27
H	0,067	0,066	6,65	0,055	0,083	86,22
S	0,023	0,024	2,38	0,030	0,026	94,38
V	0,033	0,034	3,35	0,040	0,031	92,89
I1	0,030	0,031	3,03	0,030	0,033	93,73
I2	0,033	0,032	3,21	0,038	0,032	93,06
I3	0,017	0,017	1,67	0,030	0,015	95,50

Tableau 5.2 les résultats par la méthode LDA avec l'utilisation des images en couleur.

- **Fusion logique sur LDA**

Le tableau suivant montre les résultats de la fusion logique par l'opérateur OR de la méthode LDA.

Couleur	L'ensemble de test		
	TFA	TFR	**TS (%)**
I1I2I3	0,0517	0,0125	93,58%
HSV	0,1231	0,0075	86,94%
RGB	0,0701	0,0075	92,24%
XYZ	0,04829	0,0100	**94,17**%
YCrCb	0,0662	0,0075	92,63%
YIQ	0,0642	0,01500	92,08%
YUV	0,0664	0,0125	92,11%

Tableau 5.3 taux d'erreur de la fusion logique OR de la méthode LDA.

Le système d'authentification par l'utilisation de la fusion logique de décision par l'opérateur OR donne un taux de faux rejet (TFR) très faible et un taux de fausse acceptance (TFA) grand. Ce genre de système laxiste accepte facilement un imposteur et ne peut pas être employé dans le cas où une haute sécurité est demandée.

Avec la fusion logique par l'opérateur AND de la méthode LDA on trouve les résultats du tableau suivant :

Couleur	L'ensemble de test		
	TFA	TFR	**TS (%)**
I1I2I3	0,00245	0,0525	94,51%
HSV	0,00207	0,0875	91,04%
RGB	0,01527	0,0475	93,72%
XYZ	0,01790	0,0375	94,46%
YCrCb	0,0010	0,0500	94,90%
YIQ	0,0011	0,055	94,39%
YUV	0,0023	0,0375	**96,01**%

Tableau 5.4 taux d'erreur de la fusion logique AND de la méthode LDA.

Alors que Le système d'authentification par l'utilisation de la fusion logique de décisions par L'opérateur AND donne un taux de faux rejet (TFR) grand et un taux de fausse acceptance (TFA) très faible. Donc ce type de système strict peut être employé dans le cas où une haute Sécurité est demandée. Et même le taux de succès est bon de l'ordre de 96.01% avec l'espace couleur YUV.

Avec la fusion logique par l'opérateur (2 AND) nous obtenons des résultats stables comme le montre le tableau 5.5.

Couleur	2AND in teste set			
	TFA	TFR	TEE	**TS (%)**
I1I2I3	0,026	0,033	0,029	94,16%
HSV	0,015	0,030	0,022	95,51%
RGB	0,034	0,020	0,027	94,59%
XYZ	0,030	0,025	0,028	94,49%
YCrCb	0,009	0,023	0,016	**96,81**%
YIQ	0,009	0,018	0,013	**97,34%**
YUV	0,012	0,025	0,019	96,26%

Tableau 5.5 taux d'erreur de la fusion logique (2 AND) de la méthode LDA.

A partir de l'ensemble de ces résultats nous remarquons que le taux de fausse acceptance de la fusion logique de décisions (2 AND) et le taux de faux rejet pour le même espace couleur sont faibles et presque égaux. Cela veut dire que le système d'authentification se situe dans le juste milieu (un taux d'erreur égale TEE faible de l'ordre de 1.3% avec l'espace couleur YIQ) donc le système est stable et c'est une propriétée importante. Et nous avons trouvé un taux de succès de l'ordre de 97.34% avec l'espace couleur YIQ. Donc cette fusion logique par l'opérateur AND améliore la performance de système par rapport à l'utilisation des images en niveaux de gris où bien une seule composante couleur. Par contre la différence entre le TFA et TFR en utilisant les opérateurs logiques OR et AND sont grands.

- **Fusion non linéaire sur LDA**

Les différents taux d'erreur et de succès dans l'ensemble de test on utilise un classifieur MLP sont montrés dans le tableau 5.6. On observe que la fusion non linéaire des résultats des trois composantes couleurs de chaque espace couleur donne des résultats satisfaisants et le meilleur c'est avec l'espace couleur YCrCb qui donne un taux de réussite TS de l'ordre de **97.45%**.

Cela veut dire une amélioration de l'ordre de **1.35%** par rapport à l'utilisation d'une seule composante colorimétrique comme caractéristique d'entrée au système d'authentification de visage. Aussi d'après les résultats du tableau 5.6, nous observons que le TFR et grand par rapport au TFA qui est très faible donc le système n'accepte pas facilement un imposteur cela veut dire qu'on peut employer ce genre des systèmes stricts dans le cas où la haute sécurité est demandée.

espace couleur	Taux d'erreur dans l'ensemble de test		
	TFR	TFA	TS(%)
YCrCb	**0,0175**	**0,0080**	**97,45**
RGB	0,0175	0,0271	95,54
YIQ	0,0200	0,0058	97,42
YUV	0,0175	0,0132	96,93
HSV	0,0100	0,0272	96,28
I1I2I3	0,0200	0,0089	97,11
XYZ	0,0175	0,0329	94,96

Tableau 5.6 les taux d'erreurs par la fusion non linéaire de LDA

Nous avons trouvé un taux de réussite TS de **93.30%** avec l'utilisation des images en niveaux de gris. Cela veut dire que l'utilisation de l'information couleur surtout l'espace couleur YCrCb, comme caractéristique d'entrée avec la méthode d'analyse linéaire discriminante LDA et la fusion non linéaire par réseau de neurone de type MLP au système d'authentification de visage apporte une amélioration dans le taux de réussite de l'ordre de **4.15%** par rapport à l'utilisation des images représentées en niveau de gris.

5.7.2 Authentification de visage par EFM

Concernant la méthode EFM nous avons obtenu un taux de succès TS de l'ordre de **94.68%** avec l'utilisation de la représentation en niveaux de Gris. Donc la méthode EFM nous donnent un résultat meilleur que la méthode LDA lorsqu'on utilise des images en niveaux de gris et cette résultat prouve ce qu'on a dire théoriquement sur la méthode EFM. Pour l'augmentation de la performance de ce système, nous avons testé l'information couleur sur la méthode EFM. Nous avons choisi les paramètres de la méthode EFM suivants :

- Prétraitement avec photonormalisation

- Composante couleur : RGB, XYZ, LAB, HSV, I1I2I3, YUV, YCrCb, YIQ.
- Coefficients : 100 coefficients de projection triés suivants les valeurs propres décroissantes pour l'ACP et 60 cœfficients pour EFM.
- Mesure de similarité: corrélation.
- Seuillage : Globale.

Les résultats obtenus avec ces paramètres sont présentés dans le tableau 5.7. Nous remarquons dans ce tableau la même remarque que le système qui utilise LDA. On parle de la stabilité ; les différents taux d'erreurs sont très stables dans les différents ensemble (évaluation et test). Les résultats avec la méthode EFM sont assez bons. Avec seulement 60 caractéristiques on peut atteindre un taux de succès de l'ordre de **96.16**% en utilisant la composante de luminance Y de l'espace couleur YCrCb et un taux d'égale erreur TEE dans l'ensemble d'évaluation de l'ordre de **2.62**%. Le taux de succès TS présente une amélioration de **1.48**% par rapport à l'utilisation des images en niveaux de gris. Mais si on compare cette résultat avec LDA on peut dire qu'on a trouvé presque des résultats semblables, que ce soit LDA ou EFM le taux de succès et de l'ordre de 96% avec l'utilisation d'une seule composante couleur à l'entrée de système d'authentification de visage.

Couleur	Ensemble d'évaluation			Ensemble de test		
	TFR	TFA	TEE (%)	TFR	TFA	TS (%)
X	0.0300	0.0296	2.98	0.0150	0.0297	95.53
Y	0.0283	0.0276	2.80	0.0175	0.0277	95.48
Z	0.0283	0.0274	2.79	0.0150	0.0238	96.12
Y	**0.0267**	**0.0257**	**2.62**	**0.0175**	**0.0209**	**96.16**
Cr	0.0167	0.0166	1.67	0.0325	0.0156	95.19
Cb	0.0267	0.0272	2.70	0.0325	0.0228	94.47
R	0.0333	0.0332	3.33	0.0175	0.0340	94.85
G	0.0267	0.0275	2.71	0.0200	0.0276	95.24
B	0.0267	0.0271	2.69	0.0150	0.0275	95.75
Y	0.0300	0.0296	2.98	0.0150	0.0302	95.48
I	0.0283	0.0269	2.76	0.0250	0.0227	95.23
Q	0.0200	0.0207	2.04	0.0325	0.0213	94.62
Y	0.0267	0.0257	2.62	0.0175	0.0255	95.70
U	0.0317	0.0323	3.20	0.0200	0.0299	95.01
V	0.0217	0.0221	2.19	0.0300	0.0186	95.14
H	0.0583	0.0580	5.82	0.0625	0.0672	87.03
S	0.0233	0.0233	2.33	0.0225	0.0235	95.40
V	0.0333	0.0326	3.30	0.0175	0.0330	94.95
I1	0.0267	0.0268	2.68	0.0150	0.0272	95.78
I2	0.0283	0.0284	2.84	0.0150	0.0283	95.67
I3	0.0150	0.0144	1.47	0.0425	0.0127	94.48
L	0.0333	0.0328	3.31	0.0150	0.0346	95.04
A	0.0217	0.0221	2.19	0.0325	0.0234	94.41
B	0.0317	0.0323	3.20	0.0175	0.0319	95.06

Tableau 5.7 les résultats par la méthode EFM avec l'utilisation des images en couleur.

Les taux d'égales erreur et succès obtenus sur l'ensemble d'évaluation et test de système d'authentification de visage de la méthode EFM pour différentes espaces de couleur sont présentés dans la figure 5.4 et 5.5.

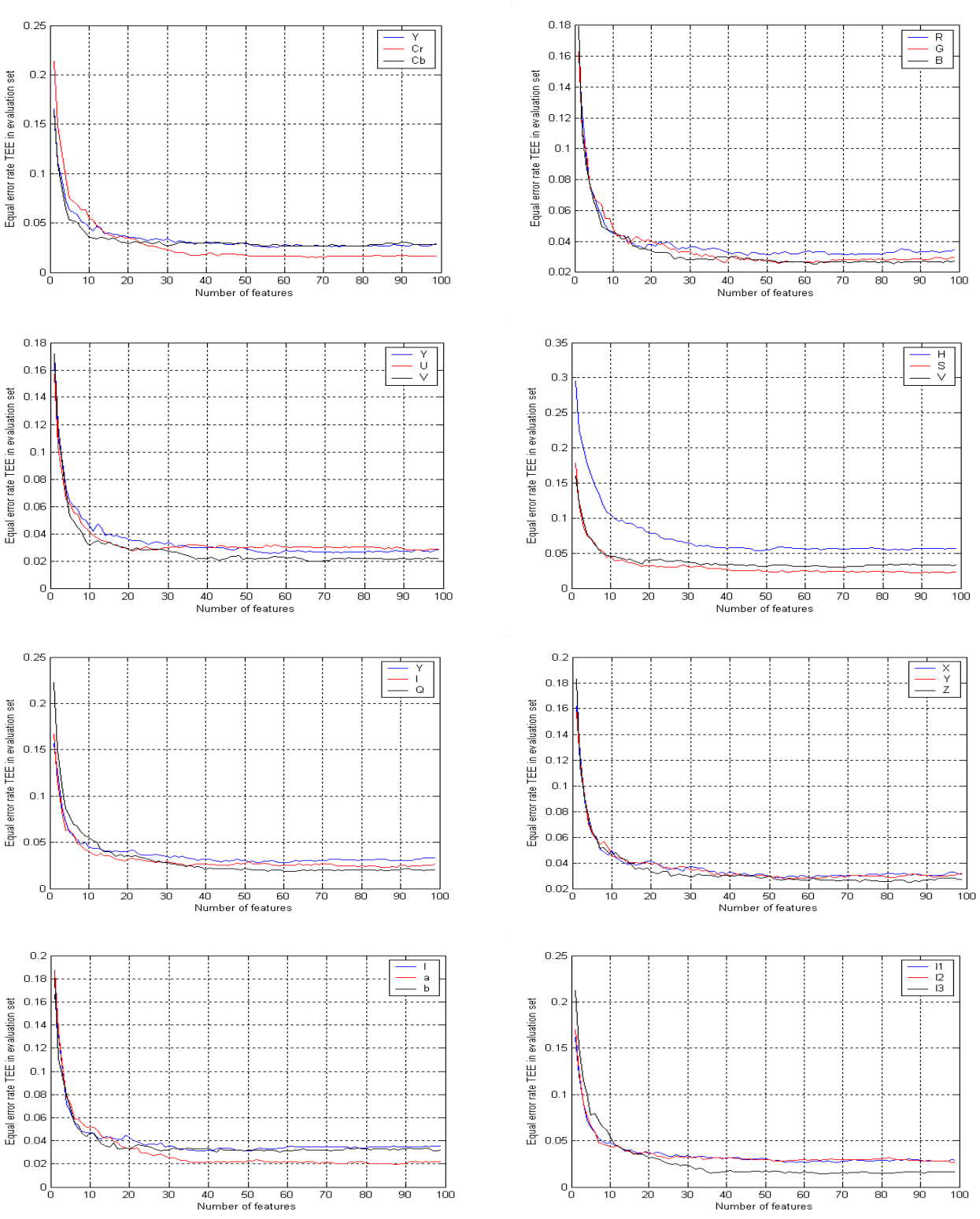


Figure 5.4 Taux d'égale erreur TEE de la méthode EFM en utilisant différentes espaces de couleur.

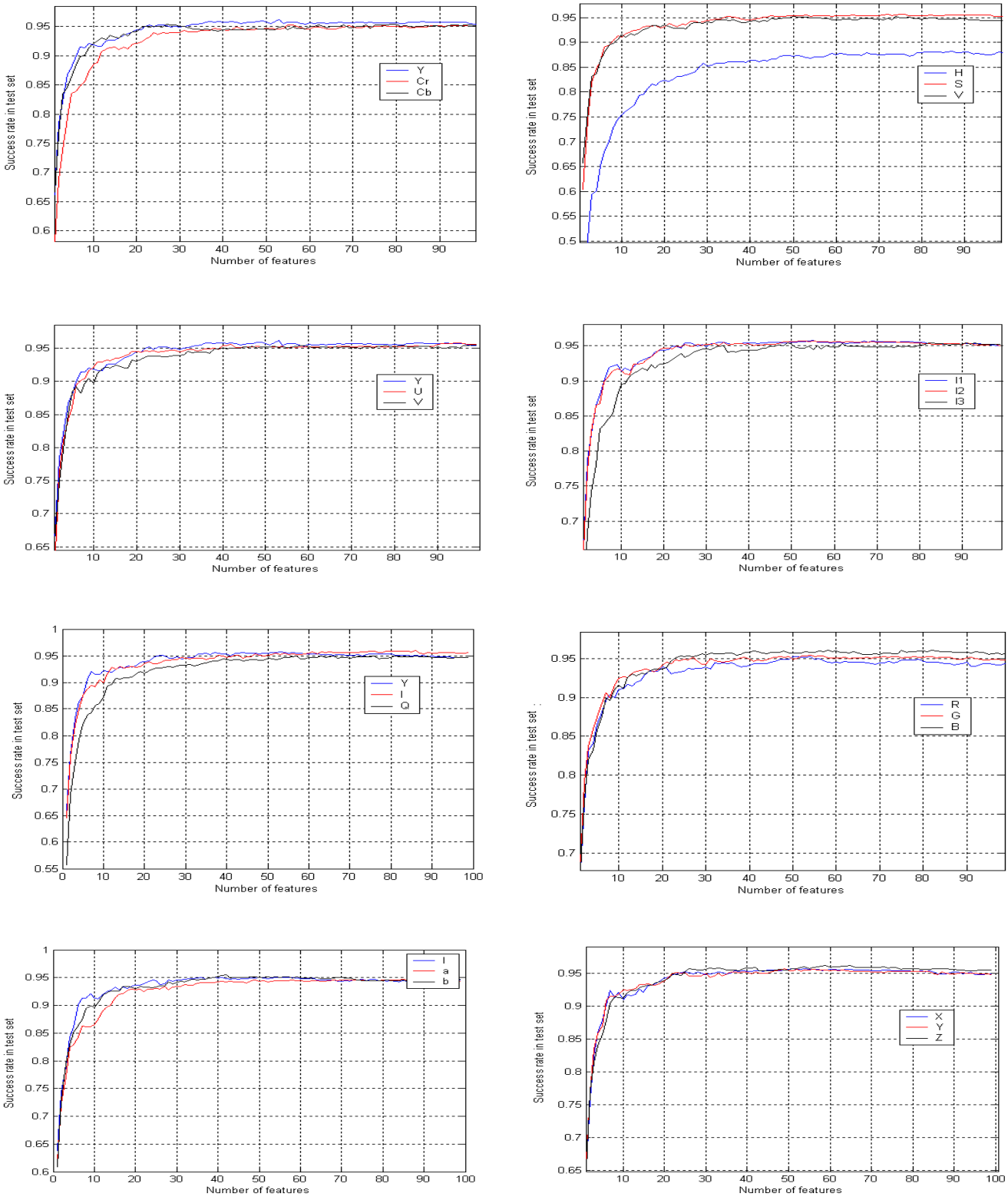


Figure 5.5 Taux de succès TS de la méthode EFM en utilisant différentes espaces de couleur.

- **Fusion logique sur EFM**

Le tableau suivant montre les résultats de la fusion logique par l'opérateur OR de la méthode EFM.

Couleur	L'ensemble de test		
	TFA	TFR	**TS (%)**
I1I2I3	0.0444	0.0125	94.31
HSV	0.1046	0.0075	88.79
RGB	0.0493	0.0125	93.82
XYZ	0.0395	0.015	94.55
YCrCb	0.057	0.0100	93.30
YIQ	0.0613	0.0075	93.12
YUV	0.056	0.0100	93.40

Tableau 5.8 taux d'erreur de la fusion logique OR de la méthode EFM.

Avec la fusion logique par l'opérateur AND de la méthode EFM, on trouve les résultats du tableau suivant :

Couleur	L'ensemble de test		
	TFA	TFR	**TS (%)**
I1I2I3	0.0032	0.0475	94.93
HSV	0.0023	0.0750	92.27
RGB	0.0155	0.0225	96.20
XYZ	0.0202	0.0225	95.73
YCrCb	0.0014	0.045	95.36
YIQ	0.0018	0.0525	94.57
YUV	0.0034	0.0400	95.66

Tableau 5.9 taux d'erreur de la fusion logique AND de la méthode EFM.

Avec l'opérateur OR le système est dans la zone de basse sécurité TFR<<TFA. Par contre le système est dans la zone de haute sécurité avec l'opérateur AND le TFA<<TFR avec un TS de l'ordre de 96.20% avec l'espace couleur RGB.

Avec la fusion logique par l'opérateur (2 AND), nous obtenons des résultats stables comme le montre le tableau 5.10.

Couleur	2AND in teste set			
	TFA	TFR	TEE	**TS (%)**
I1I2I3	0.0269	0.0200	0.0234	95.31
HSV	0.0150	0.025	0.0200	96.00
RGB	0.0267	0.0255	0.0261	95.08
XYZ	0.0302	0.0175	0.0238	95.23
YCrCb	0.0097	0.0150	0.0123	97.53
YIQ	0.0112	0.0150	0.0131	97.38
YUV	0.0136	0.0100	0.0118	97.64

Tableau 5.10 taux d'erreur de la fusion logique (2 AND) de la méthode EFM.

D'après les résultats de ces tableaux on observe que les taux d'erreur TFR et TFA avec l'opérateur 2AND sont plus proches que les erreurs des autres opérateurs comme le OR et le AND. Cela veut dire que le système est stable et la meilleur taux de succès, on le trouve par l'espace de couleur YUV avec un TS de l'ordre de 97.64%. et on remarque qu'avec l'espace de couleur YCrCb le TFA de l'ordre de 0.0097et qui est très faible par rapport au TFR qui est de l'ordre de 0.015 cela veut dire que le système est strict et fonctionne dans la zone de haute sécurité avec un taux de succès très satisfaisant TS de l'ordre de 97.53%.

- **Fusion non linéaire sur EFM**

Les résultats de la fusion non linéaire de la méthode EFM en utilisant un classifieur MLP sont présentés dans le tableau 5.11. D'après le tableau on remarque que la fusion non linéaire des résultats des trois composantes couleurs de chaque espace couleur donne des résultats intéressantes et la valeur supérieur c'est avec l'espace couleur YCrCb qui donne un taux de succès TS de l'ordre de **97.68%**. Donc c'est une amélioration de l'ordre de **1.52%** par rapport à l'utilisation d'une seule composante colorimétrique comme caractéristique d'entrée au système d'authentification de visage. Aussi, nous observons que le TFR et grand par rapport au TFA qui est très faible donc le système n'accepte pas facilement un imposteur cela veut dire qu'on peut employer ce genre de système strict dans le cas où la haute sécurité est demandée.

espace couleur	Taux d'erreur dans l'ensemble de test		
	TFR	TFA	TS (%)
YCrCb	**0,0175**	**0,0057**	**97,68**
RGB	0,0575	0,0069	93.56
YIQ	0,0300	0,0071	96.29
YUV	0,0100	0,0189	97.11
HSV	0,0225	0,0093	96,82
I1I2I3	0,0200	0,0062	97,38
XYZ	0,0175	0,0217	96,08

Tableau 5.11 les taux d'erreur par la fusion non linéaire de EFM

Nous avons trouvé un taux de réussite TS de **94.68%** avec l'utilisation des images en niveaux de gris. Et avec l'utilisation de l'information couleur surtout l'espace couleur YCrCb, comme caractéristique d'entrée avec la méthode EFM et la fusion non linéaire par réseaux de neurone de type MLP au système d'authentification de visage apporte une amélioration dans le taux de succès de l'ordre de **3%** par rapport à l'utilisation des images représentées en niveau de gris.

5.7.3 Authentification de visage par DCT

Pour la transformée en DCT en se basant sur l'information des basses fréquences et on prend seulement la composante DC de chaque bloc pour construire le vecteur caractéristique et on atteint un taux de succès TS de l'ordre de 76.09% sur des images en niveaux de gris. Ce taux de succès est faible par rapport à l'utilisation de la méthode ACP, LDA où EFM. Mais la méthode DCT reste plus rapide que ces derniers pour la phase d'extraction de caractéristiques. Et avec l'application de ces méthodes sur les données DCT et pas sur les images originales directement, on trouve une amélioration dans le taux de succès avec l'ACP dont le TS de l'ordre de 89.78% mais avec LDA et EFM les taux de succès n'augmentent pas par rapport à l'application de ces derniers sur des images originales sans DCT mais les taux de succès restent acceptables. Donc on a réduit la mémoire pour le stockage de vecteur image de taille (64x64) vers un vecteur après DCT à (64). Aussi nous avons appliqué la DCT sur chaque ligne et colonne de l'image originale et on atteint un TS de 86.64% qui est augmenté jusqu'a 10% par rapport à l'application de la DCT sur des blocs (8x8). Avec une taille de vecteur caractéristique de (150+110) donc une très faible consommation de mémoire.

Niveaux de gris	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE	TFR	TFA	TS (%)
DCT (8x8)	0.126	0.128	0.127	0.112	0.126	76.09
DCT avec ACP	0.0633	0.0633	0.0633	0.040	0.0622	89.78
DCT avec LDA	0.055	0.055	0.055	0.041	0.056	90.32
DCT avec EFM	0.035	0.034	0.034	0.030	0.0329	93.71
DCT (ligne colonne)	0.0667	0.0675	0.066	0.0625	0.0711	86.64

Tableau 5.12 les résultats par la méthode DCT en combinaison avec ACP LDA et EFM.

La méthode DCT ne nécessite pas un réapprentissage complet lorsqu'on veut ajouter une personne à la base de données contrairement aux méthodes comme ACP, LDA et EFM.

5.7.4 Authentification de visage par la transformée de radon

Nous avons appliqué la transformation de radon par un angle égale à 40° pour l'authentification de visage sur des images représentées en niveaux de gris. Les résultats obtenus sont acceptables par rapport aux approches utilisées dans cette thèse. Les avantages cités pour la méthode MS, on les trouves ici pour cette transformation mais la méthode MS reste plus performant que la transformée de radon en terme de taux de succès comme nous voyons dans le tableau ci dessous.

Taille de vecteur caractéristique	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE (%)	TFR	TFA	TS (%)
191	0.051	0.052	5.17	0.117	0.0981	82.44

Tableau 5.13 les résultats par la transformée de radon des images en niveaux de gris.

Pour l'utilisation des images en couleur les résultats ne sont pas encouragés puisque la performance de ce système n'est pas améliorée. Pour cela on ne va pas appliquer les deux fusions logique et non linéaire qui ne nous donnent pas une grande chose. Le tableau suivant donne quelques taux d'erreur de la transformée de radon en couleur.

Ensemble d'évaluation		
Couleur	TFR (%)	TFA (%)
Grey	0.0517	0.0518
R	0.0517	0.0526
G	0.045	0.0452
B	0.0517	0.0516
H	0.1033	0.1026
S	0.0717	0.0709
V	0.0517	0.0522
Y	0.0517	0.0525
U	0.0733	0.0738
V	0.075	0.0759
Y	0.0517	0.0525
I	0.0717	0.0707
Q	0.0896	0.0900
Y	0.05	0.0496
Cb	0.0717	0.0712
Cr	0.0683	0.0691

Tableau 5.14 les résultats par la transformé de radon des images en couleur.

Le choix de l'angle de la transformée de radon influent sur la performance de notre système d'authentification de visage. Par exemple si l'angle égale à 90° le TEE est de l'ordre de 25%. Et avec un angle égale à 20° le TEE est de l'ordre de 8.31%. Parmi toutes les angles on a choisi 40° parce que nous donnent la meilleure taux de succès.

5.7.5 Authentification de visage par LBP

Le système d'authentification de visage basé sur la méthode LBP pour l'extraction de vecteur caractéristiques de l'image de visage est stable d'après les valeurs de TFR et TFA qui sont très proches pour les trois composantes couleurs de l'espace de couleur YCrCb et on atteint un TS de 59.60% par la composante Y.

LBP Taille vecteur 256	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE	TFR	TFA	TS (%)
LBP Y	0.1583	0.1583	0.158	0.226	0.178	59.60
LBP Cb	0.2283	0.2286	0.228	0.235	0.241	52.40
LBP Cr	0.2067	0.2081	0.207	0.2075	0.2339	55.86

Tableau 5.15 les résultats par LBP avec l'espace couleur YCbCr.

La taille de vecteur caractéristique de la méthode LBP égale à 256 puisque chaque composante couleur varie de (0 à 255) donc la taille de l'image est réduit de (NxN) vers un vecteur caractéristique de taille 256 fixe et qui indépendant de la taille de l'image, donc une faible consommation du mémoire de stockage des données. Ainsi la rapidité d'extraire ce vecteur grâce à la simplicité de la méthode LBP. Pour augmenter la performance de ce système on a appliqué la fusion logique et on trouve un TS de 64.87% par l'opérateur 2 AND.

LBP fusion logique YCrCb	Ensemble de Test		
	TFR	TFA	TS (%)
OR	0.0275	0.4399	53.26
AND	0.4625	0.0394	49.81
2 AND	0.1775	0.1738	64.87

Tableau 5.16 les résultats de la fusion logique de l'espace couleur YCbCr par la méthode LBP.

Avec l'application de l'ACP LDA et EFM sur les données après LBP, on trouve une amélioration avec EFM qui donne un TS de 62.72%.

La composante Y de ycbcr Avec 100 valeurs propres	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE	TFR	TFA	TS (%)
LBP	0.1583	0.1583	0.158	0.226	0.178	59.60
LBP avec ACP	0.1667	0.1660	0.166	0.225	0.1868	58.82
LBP avec LDA	0.2083	0.2081	0.208	0.2325	0.2156	55.19
LBP avec EFM	0.1617	0.1620	0.162	0.2025	0.1703	62.72

Tableau 5.17 les résultats par la méthode LBP de la composante Y de l'espace couleur YCbCr en combinaison avec ACP LDA et EFM.

5.7.6 Authentification de visage par les caractéristiques de la matrice de cooccurrence

Nous extrayons la matrice de cooccurrence pour chaque image de visage après l'enchaînement ligne par ligne de la matrice de cooccurrence on obtient un vecteur caractéristique de taille (NgxNg) où Ng est le nombre des niveaux de gris contient sur l'image on a choisit Ng=8, 16 et 32. Les paramètres choisissent sont : la distance d=1, l'angle θ=0°. Les résultats de l'authentification de visage utilisant le vecteur de cooccurrence sont présentés dans les trois tableaux ci dessous. Et pour minimiser la taille de vecteur caractéristique on a appliqué la méthode MS décrit en chapitre 02 sur la matrice de cooccurrence.

Les bons résultats sont trouvé avec Ng=16. Le taux de succès TS est de l'ordre de 63.59% avec un vecteur caractéristiques de taille 256. Et même avec un taille réduit de 64 à l'aide de la méthode MS le taux de succès est égale à 63.02% et qui est intéressant malgré la réduction de la taille de vecteur caractéristiques et c'est une propriété très importante de la nouvelle méthode qu'on a proposé pour la réduction des grandes donnée.

Ng=8 (θ=0°, d=1)	Taille de vecteur caractéristique	Ensemble d'évaluation			Ensemble de Test		
		TFR	TFA	TEE	TFR	TFA	TS (%)
Vecteur co_occurence	64	0.228	0.227	0.227	0.207	0.183	60.92
Vecteur MS de co_occurence	32	0.226	0.227	0.226	0.192	0.206	60.11

Tableau 5.18 les résultats par cooccurrence avec 8 niveaux de gris et un angle de 0°.

Ng=16 (θ=0°, d=1)	Taille de vecteur caractéristique	Ensemble d'évaluation			Ensemble de Test		
		TFR	TFA	TEE	TFR	TFA	TS (%)
Vecteur co_occurence	256	0.203	0.203	0.203	0.205	0.159	63.59
Vecteur MS de co_occurence	64	0.210	0.209	0.209	0.175	0.194	63.02

Tableau 5.19 les résultats par cooccurrence avec 16 niveaux de gris et un angle de 0°.

Ng=32 (θ=0°, d=1)	Taille de vecteur caractéristique	Ensemble d'évaluation			Ensemble de Test		
		TFR	TFA	TEE	TFR	TFA	TS (%)
Vecteur co_occurence	1024	0.227	0.227	0.227	0.242	0.184	57.27
Vecteur MS de co_occurence	128	0.206	0.207	0.206	0.175	0.194	63.09

Tableau 5.20 les résultats par cooccurrence avec 32 niveaux de gris et un angle de 0°.

La taille de vecteur caractéristique des caractéristiques de Haralick de la matrice de concurrence est égale à 13. Cela veut dire une faible consommation du mémoire de stockage

des données. Et cette taille de vecteur est indépendante de la taille de l'image. Les résultats de l'authentification de visage par ces 13 paramètres de Haralick de chaque image sont montrés dans le tableau ci dessous. Avec un angle égale à 45° on trouve le maximum taux de succès de l'ordre de 66.09%.

Niveaux de gris Ng=16 d=1	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE	TFR	TFA	TS (%)
Vecteur de Haralick_13 0°	0.1483	0.1484	0.148	0.2150	0.1479	63.71
Vecteur de Haralick_13 45°	0.1517	0.1525	0.152	0.1900	0.1491	66.09
Vecteur de Haralick_13 90°	0.1550	0.1557	0.155	0.1950	0.1536	65.14
Vecteur de Haralick_13 135°	0.1467	0.1472	0.147	0.1975	0.1439	65.86
Les 4 vecteurs de Haralick successive 52	0.1483	0.1492	0.148	0.2050	0.1509	64.41
La moyenne des vecteurs Harlick dans tous les angles 13	0.1467	0.1457	0.146	0.2050	0.1433	65.17

Tableau 5.21 les résultats de 13 paramètres de Haralick avec 16 niveaux de gris et différentes angles : 0°,45°,90°,135°.

Avec l'application de l'ACP LDA et EFM sur les données après le vecteur Haralick on ne trouve pas une amélioration avec ACP, LDA où EFM.

Méthode	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE	TFR	TFA	TS (%)
Vecteur de Haralick_13	0.1483	0.1484	0.148	0.2150	0.1479	63.71
Vecteur de Haralick_13 avec ACP	0.1867	0.1864	0.186	0.2300	0.1777	59.23
Vecteur de Haralick_13 avec LDA	0.3283	0.3297	0.329	0.3900	0.3852	22.48
Vecteur de Haralick_13 avec EFM	0.1717	0.1725	0.172	0.2075	0.1872	60.53

Tableau 5.22 les résultats par cooccurrence avec 16 niveaux de gris et un angle de 0° en combinaison par ACP LDA et EFM.

5.7.7 Authentification de visage par l'approche proposée (Statistiques d'ordre un)

Notre approche est basée sur l'extraction des statistiques d'ordre un de l'image de visage comme la moyenne, la variance, les moments d'ordre 3 (skewness) et les moments d'ordre 4 (kurtosis). Nous avons combiné ces statistiques afin d'augmenter la performance de systeme d'authentification de visage. Nous avons détaillé le principe de cette méthode dans le chapitre 2 et ici on va simplement présenter les résultats obtenus pour l'authentification de visage. Le tableau 5.23 illustre les résultats des différentes statistiques ainsi ces combinaisons appliquées sur des images en niveaux de gris. Nous avons choisi les paramètres suivants :

- Prétraitement avec photonormalisation.
- Mesure de similarité: corrélation.
- Seuillage : Globale.

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 Varience	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, varience, Skewness et Kurtosis	12.69	13.90	15.75	70.35	1040

Tableau 5.23 les résultats par les statistiques d'ordre un en niveaux de gris.

D'après les résultats du tableau 5.23, on remarque que l'utilisation de la moyenne ou bien l'écart type seule donne les taux de succès suivants 85.66 et 84.06 respectivement. Et nous avons obtenu une amélioration dans le taux de succès si nous faisons les combinaisons des différentes valeurs statistiques suivantes : (moyenne et écart type) ; (moyenne et varience) ; (moyenne et skewness) ; (moyenne et kurtosis), ou bien toutes ces combinaisons ensemble et qui donnent respectivement : 89.45%, 78.38%,86.96%,85.50% et 70.35%.

Plus particulièrement, la combinaison (moyenne et écart type) donne la meilleur taux de succès TS de l'ordre de **89.45**% par rapport aux autres combinaisons. Nous préférons d'appeler cette méthode (**MS**) et c'est l'abréviation de (**M**ean and **S**tandard deviation in english).

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 propriétée très importante.

En effet, la méthode MS a des avantages très intéressants si on l'a comparée avec l'ACP, LDA et EFM. Ces avantages se résument en ces points suivants :

- La rapidité : les méthodes comme l'ACP, LDA et EFM 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 base de données : dans l'approche proposée 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 les méthodes ACP, LDA et EFM 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, LDA et EFM. 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	88.70	47.84	0.120
LDA	93.03	119.10	0.100
EFM	94.68	56.64	0.110

Tableau 5.24 Comparaison des performances de MS, PCA, LDA et EFM 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 mais LDA et EFM sont mieux que les méthodes ACP et MS. Mais en effet la méthode MS nécessite un peu du temps de calcul que les autres donc c'est la plus rapide et la plus simple entre elles. Pour réduire la dimension de vecteur caratéristique de la méthode MS, nous avons appliqué un filtre appelé (wavelet 9/7) sur chaque image de visage avons l'extraction de vecteur caractéristique comme le montre la prochaine figure qui explique bien les trios stages de la transformation de (wavelet 9/7).

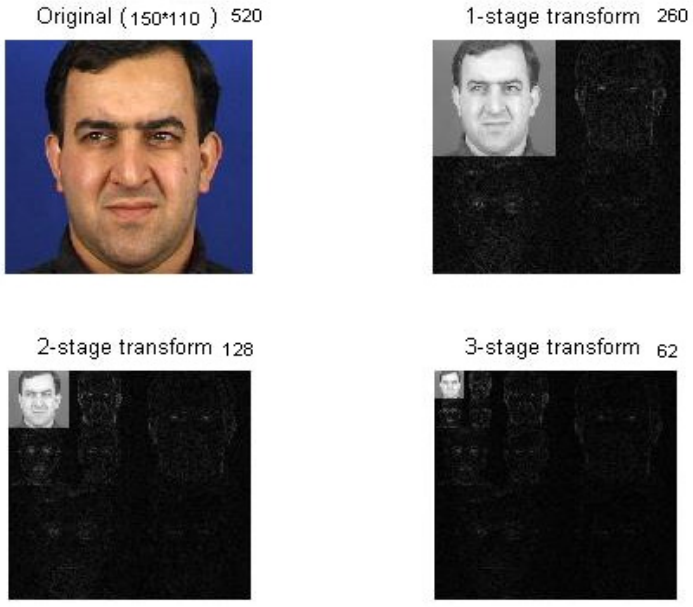


Figure 5.6 les trios stages de la transformation de (wavelet 9/7) pour une image de visage de la base de données XM2VTS..

Les résultats trouvés après cette réduction sont montrés dans le tableau ci-dessous.

Taille de vecteur caractéristique	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE (%)	TFR	TFA	TS (%)
520	0.054	0.055	5.47	0.047	0.057	89.48
260	0.055	0.056	5.55	0.055	0.058	88.63
128	0.058	0.059	5.80	0.060	0.062	87.83
62	0.063	0.064	6.30	0.077	0.064	85.80
30	0.090	0.0891	8.95	0.112	0.091	79.58

Tableau 5.25 Les résultats de la méthode MS en appliquent le filtre (wavelet9/7).

D'après les résultats du tableau 5.25, on remarque que les taux d'erreur TFA et TFR sont très proche cela prouve la stabilité de système même avec la compression de l'image jusqu'à un taille de (18x13) dons le vecteur caractéristique de la méthode MS est de l'ordre de 62. Même avec un vecteur de taille 30 le taux de succé est de l'ordre de 79.58% et c'est un résultat intéressant par rapport à la petite taille de vecteur caractéristique.

La figure suivante présente une courbe des taux de succès de la méthode MS avec les différentes tailles de vecteur caractéristique obtenus de la compression par (wavelet9/7).

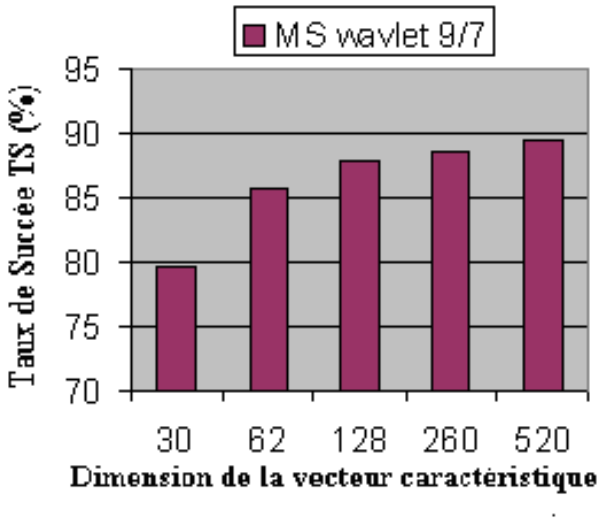


Figure 5.7 les résultats de la méthode MS en appliquant le filtre (wavelet9/7).

Nous avons trouvé une propriété importante c'est que le vecteur caractéristique a été réduit jusqu'à 62 avec la 3éme stage de transformation par le filtre wavelet 9/7, et le taux de succès est de l'ordre de 85.80% qui reste assez bien comparable avec le taux de succès de la taille

originale de l'image de l'ordre de 520 et comparable aussi aux taux de succès de l'ACP avec la même taille 62 de vecteur caractéristique. La figure suivante présente les différentes distances intra pour les clients et extra pour les imposteurs dans les deux ensembles d'évaluation et de test de la méthode MS.

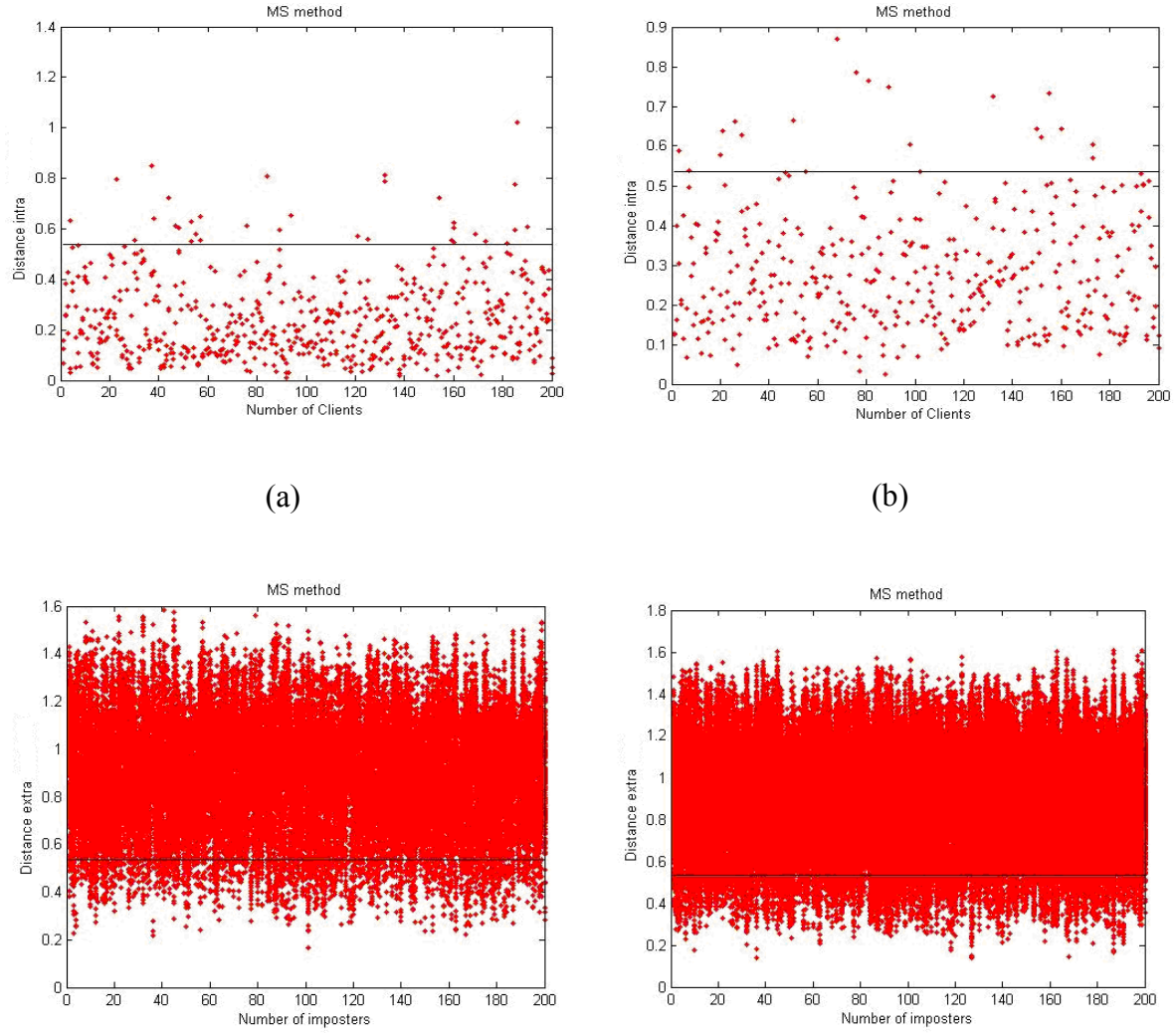


Figure 5.8 les différentes distances de la méthode MS. (a) Distance intra de l'ensemble d'évaluation (b) distance intra de l'ensemble de test (c) Distance extra l'ensemble d'évaluation (d) distance extra de l'ensemble de test.

Le tableau 5.26 illustre les différents taux d'erreur de la méthode MS pour différentes espaces de couleur.

Statistiques	Ensemble d'évaluation	Ensemble de test			Couleur
	TEE (%)	TFA (%)	TFR (%)	TS (%)	
MS	**5.47**	**5.77**	**4.75**	**89.48**	**Grey**
MS RGB	6.13	6.41	6.50	87.09	R
	5.13	**5.42**	**5.00**	**89.58**	**G**
	4.35	4.44	6.75	88.81	B
MS HSV	28.16	29.45	29.25	41.30	H
	4.13	**4.81**	**4.75**	**90.44**	**S**
	5.80	6.12	6.75	87.13	V
MS XYZ	5.64	5.93	5.75	88.32	X
	5.51	**5.78**	**4.50**	**89.72**	**Y**
	4.46	4.54	6.75	88.71	Z
MS I1I2I3	**5.49**	**5.76**	**4.75**	**89.49**	**I1**
	5.54	5.77	6.25	87.98	I2
	8.81	8.06	9.75	82.19	I3
MS YUV	**5.47**	**5.76**	**4.75**	**89.49**	**Y**
	5.03	4.96	6.50	88.54	U
	5.16	5.07	6.00	88.93	V
MS YIQ	**5.47**	**5.76**	**4.75**	**89.49**	**Y**
	5.47	5.27	5.50	89.23	I
	13.46	14.55	19.50	65.95	Q
MS YCbCr	**5.47**	**5.76**	**4.75**	**89.49**	**Y**
	5.04	4.97	6.50	88.53	Cb
	5.14	5.04	6.00	88.96	Cr

Tableau 5.26 taux d'erreur de la méthode MS pour différentes espaces de couleur.

D'après ce tableau, nous avons trouvé que le résultat de la méthode MS obtenu par la composante couleur S de l'espace couleur HSV est la meilleure avec un taux de succès de l'ordre de **90.44**% suivi par la composante de luminance Y de l'espace couleur XYZ avec un taux de succès de l'ordre de 89.72%, ensuite la composante G de l'espace couleur RGB avec un taux de succès de l'ordre de 89.58% et finalement la luminance des espaces couleurs I1I2I3, YUV, YIQ et YCrCb avec un taux de succès de l'ordre de 89.49% qui est semblable avec le taux de succès de système en niveaux de gris. Aussi on remarque que la stabilité existe avec toutes les espaces couleurs.

- **Fusion logique sur MS**

Nous avons introduire la fusion logique des trios composantes couleurs de chaque espace couleur afin d'améliorer la performance de notre système d'authentification de visage.
Le tableau suivant montre les résultats de la fusion logique par l'opérateur OR de la méthode MS.

Couleur	L'ensemble de test		
	TFA(%)	TFR(%)	**TS (%)**
I1I2I3	13.23	1.50	85.27
HSV	35.47	1.00	63.53
RGB	8.07	4.25	87.68
XYZ	**6.74**	**4.25**	**89.01**
YCrCb	11.84	1.50	86.66
YIQ	22.16	1.25	76.59
YUV	11.85	1.50	86.65

Tableau 5.27 taux d'erreurs de la fusion logique OR de la méthode MS.

Avec la fusion logique OR le système peut être employé dans les applications de basse sécurité parceque le TFR<<TFA avec un taux de succès de l'ordre de 89.01% de l'espace couleur XYZ.
Mais avec la fusion logique AND le système fonctionne dans la zone de haute sécurité parce que le TFA<<TFR le système rejet des clients facilement donc c'est un système strict, le taux de succès est de l'ordre de 88.12% avec l'utilisation de l'espace couleur XYZ ou bien RGB.

Avec la fusion logique par l'opérateur AND de la méthode MS, on trouve les résultats du tableau 5.28 suivant :

Couleur	L'ensemble de test		
	TFA(%)	TFR(%)	**TS (%)**
I1I2I3	0.81	14.50	84.69
HSV	0.65	35.75	63.60
RGB	**3.13**	**8.75**	**88.12**
XYZ	**3.88**	**8.00**	**88.12**
YCrCb	0.73	11.50	87.77
YIQ	0.35	23.25	76.40
YUV	0.73	11.50	87.77

Tableau 5.28 taux d'erreur de la fusion logique AND de la méthode MS.

Avec la fusion logique par l'opérateur (2 AND), nous obtenons des résultats stables comme le montre le tableau 5.29.

Couleur	2AND in teste set			
	TFA(%)	TFR(%)	TEE(%)	**TS (%)**
I1I2I3	5.54	4.75	5.14	89.71
HSV	4.27	4.00	4.13	91.73
RGB	5.07	5.25	5.16	89.68
XYZ	5.64	4.75	5.19	89.61
YCrCb	**3.21**	**4.25**	**3.73**	**92.54**
YIQ	3.07	5.25	4.16	91.68
YUV	**3.21**	**4.25**	**3.73**	**92.54**

Tableau 5.29 taux d'erreur de la fusion logique (2 AND) de la méthode MS.

Le système est plus stable avec la fusion 2 AND, le TFR très proche de TFA, le meilleur taux de succès est de l'ordre de 92.54% avec les deux espaces de couleurs YUV et YCrCb.
Finalement, on peut dire que la fusion logique des composantes couleurs avec la méthode MS augmente la performance de système d'authentification de visage spécialement avec les deux

espaces de couleurs YUV et YCrCb. Et elle nous donne une augmentation dans le taux de succès de l'ordre de 03% par rapport à l'utilisation des images en niveaux de gris.

- **Fusion non linéaire sur MS**

Les différents résultats de la fusion non linéaire de la méthode MS en utilisant un classifieur MLP sont présentés dans le tableau 5.30.

espace couleur	Taux d'erreur dans l'ensemble de test		
	TFR(%)	TFA(%)	TS (%)
YCrCb	**3.75**	**2.42**	**93.83**
RGB	12.00	2.20	85.80
YIQ	5.00	2.54	92.46
YUV	**3.75**	**2.43**	**93.82**
HSV	4.25	4.15	91.60
I1I2I3	4.50	2.38	93.12
XYZ	13.00	2.06	84.94

Tableau 5.30 les taux d'erreurs par la fusion non linéaire de MS

Nous observons qu'avec l'utilisation de la fusion non linéaire par réseau de neurone de type MLP des trois composantes couleur de l'espace couleur YUV et YCrCb de la méthode MS que nous propose donne le meilleur taux de succès de l'ordre de **93.83**%. Donc le système d'authentification de visage apporte une amélioration dans le taux de succès de l'ordre de **4.35%** par rapport à l'utilisation des images représentés en niveau de gris.

Les tableaux suivants présentent les taux d'erreur des méthodes ACP, LDA et EFM appliquées aux vecteurs qui contiennent les moyennes et l'écart type de chaque ligne et colonne de l'image. On a choisi la composante couleur S de l'espace couleur HSV puisque nous donnent le meilleur résultat par rapport aux autres espaces de couleurs.

D'après ce qu'on trouve sur ce tableau on peut dire que le système reste stable puisque les TFA et TFR sont très proches.

La composante S de HSV Avec 100 valeurs proprs	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE	TFR	TFA	TS (%)
MS	0.0412	0.0414	0.0413	0.0475	0.0481	90.44
MS avec ACP	0.040	0.041	0.040	0.0475	0.0476	90.49
MS avec LDA	0.046	0.047	0.047	0.0350	0.0502	91.48
MS avec EFM	0.0417	0.0407	0.041	0.0375	0.0384	92.41

Tableau 5.31 les résultats par la méthode MS en combinaison avec ACP LDA et EFM de la composante S de l'espace couleur HSV.

D'après le tableau ci dessous, les résultats restent acceptable malgré la réduction de la dimension des images originales de taille *(150x110)* aux images (après l'application de la méthode MS) de taille *(2x(150+110))*. Et ça c'est une propriétée très importante de la méthode MS en combinaison avec d'autres méthodes puisqu'elle permis d'avoir une faible consommation de mémoire (surtout lorsqu'on travail avec des grandes bases de données) sans trop toucher la performance de ce système et surtout avec la rapidité d'extraire les caractéristiques de l'image par la méthode MS.

La composante S de HSV	TS (%)	
	Image originale (150x110)	l'image après MS [(150+110)x2]
ACP	91.09	90.49
LDA	94.38	91.48
EFM	95.40	92.41

Tableau 5.32 comparaison des résultats de ACP LDA et EFM sur l'image originale et après l'application de la méthode MS de la composante S de l'espace couleur HSV.

5.8 Comparaison des techniques utilisées

D'après le tableau 5.33 on observe bien que la nouvelle méthode proposée (MS) est la meilleure parmi les méthodes récentes comme : LBP, DCT, Radon et la matrice de cooccurrence. Et on remarque que la taille de vecteur caractéristique est réduit jusqu'à 62 et le taux de succès reste le meilleur de l'ordre de 85.80%. Et avec la taille originale de l'image (520) le taux de succès est égale à 89.48% qui reste mieux que l'approche ACP qui donne 88.70% mais la méthode (MS) est plus rapide et simple et nécessite une faible mémoire pour le stockage des données.

La méthode	Taille de vecteur caractéristique	Taux de succès TS (%)
MS	62	85.80
MS	520	89.48
radon	191	82.44
DCT	64	76.09
paramètres de Haralick	13	66.09
Cooc-Vecteur	256	63.59
LBP	256	59.60

Tableau 5.33 comparaison des techniques utilisées en terme de taux de succès et taille de vecteur caractéristique.

5.9 Combinaison des techniques et des espaces de couleur

Maintenant on parle de la fusion logique entre les méthodes et les espace couleur qui donnent les meilleur taux de succès: EFM pour la composante couleur Y de YCrCb, LDA sur la composante Cr de YCrCb et MS de la composante S de HSV. La fusion donne le meilleur taux de succès TS de l'ordre de 97.14% avec l'opérateur 2AND et le systéme reste stable. Mais ce taux TS est bas par rapport aux taux de succès de la fusion logique des composantes colorimétriques de l'espace couleur YCrCb de la méthode EFM seule et qui donne un TS de 97.53 % et 97.64% pour l'espace couleur YUV.

EFM LDA MS (Y,Cr,S)	Ensemble de Test		
	TFR	TFA	TS (%)
OR	0.0025	0.0788	91.87
AND	0.0700	0.0013	92.87
2 AND	0.0150	0.0136	97.14

Tableau 5.34 Fusion logique entre : EFM pour la composante couleur Y de YCrCb, LDA sur la composante Cr de YCrCb et MS de la composante S de HSV.

5.10 Conclusion

Dans ce chapitre nous avons implémenté les algorithmes décrits dans le chapitre 02 et les résultats obtenus sont satisfaisants et le système est stable par les différentes techniques utilisées. Chaque méthode a des avantages et des inconvénients que ce soit en terme de taux de succès, la rapidité la simplicité des calcule et la taille de vecteur caractéristiques qui est différent d'une méthode à l'autre. On a introduit l'information couleur pour la majorité des techniques utilisées et on a prouvé l'efficacité de la couleur pour l'augmentation de la performance de système d'authentification de visage. Le meilleur taux de succès est trouvé par la fusion non linéaire des composantes colorimétriques de l'espace couleur YCrCb de la méthode EFM et qui donne un TS de 97.68 %. On a proposé une nouvelle technique qu'on appelle MS et qui donne un taux de succès TS de 93.83% avec la fusion non linéaire des composantes colorimétriques de l'espace couleur YCrCb. Et 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 GENERALE

Ce travail est destiné à l'authentification de visage à partir des images bidimensionnelle. Employé dans beaucoup d'application comme le contrôle d'accès, l'authentification des transactions, la répression et la personnalisation. On a choisit la reconnaissance faciale puisqu'elle offre plusieurs avantages : le système de capture (caméra) est facile à installer, il est accepté dans les lieux publics ce qui nous permet d'avoir des bases de données de plus en plus grandes et ainsi améliorer les performances de la reconnaissance. Ces dernières années, la reconnaissance faciale suscite un intérêt croissant auprès de la communauté scientifique. Le but essentiel de ce travail est de prouver l'importance de la couleur à l'authentification de visage en combinaison avec plusieurs techniques d'extraction de caractéristiques. En effet on a utilisé la fusion logique et la fusion non linéaire pour les trois composantes couleurs de chaque espace couleur des techniques utilisées pour augmenter encore la performance de système d'authentification de visage.

Les résultats obtenus montre l'efficacité de la couleur sur la majorité des techniques utilisées. La meilleur résultat est celle de la méthode EFM avec la fusion non linéaire de l'espace couleur YCrCb et le taux de succée TS est de l'ordre de **97.68**%.

Aussi nous avons proposé une méthode de vérification d'individus basée sur la reconnaissance du visage que l'on appelle **MS** (*Mean and Standard déviation*). L'approche MS est plus rapide et simple à implémenter et ces résultats obtenus sont meilleurs que d'autres méthodes comme l'ACP, DCT, Radon, LBP et les paramètres de Haralick de la matrice de cooccurrence. Aussi une propriété très importante de la nouvelle méthode qu'on a proposé c'est la réduction des grandes données avant l'application des méthodes comme ACP LDA et EFM et même la réduction des donnée après des méthodes comme la matrice de cooccurrence sans trop diminué la performance de système d'authentification de visage. Le taux de succée TS est de l'ordre de **89.48%** avec l'utilisation des images en niveaux de gris et un taux de succée TS de **90.44%** avec l'utilisation de la composante S de l'espace couleur HSV. Et avec la fusion logique et non linéaire de l'espace couleur YCrCb on trouve un TS de **92.54**% et **93.83**% respectivement. Nous avons appliquée la DCT sur chaque ligne et colonne de l'image et nous avons obtenus un TS égale à **86.64%** et la performance de système d'authentification de visage est augmentée jusqu'à **10%** que l'utilisation des bloc (8x8).

Comme perspectives nous proposons la fusion entre plusieurs modalités biométriques comme le visage avec l'iris et l'empreinte digitale. Et l'utilisation de la programmation parallèle afin de minimiser le temps de calcule.

REFERENCES

[1] G. Roethenbaugh. “An Introduction to Biometrics and General History”, Biometrics Explained, Section 1, 1998.

[2] Nicolas MORIZET, Reconnaissance Biométrique par Fusion Multimodale du Visage et de l’Iris Thèse de Doctorat, École Doctorale d’Informatique, Télécommunications et Électronique de Paris,2009.

[3] SOUHILA GUERFI ABABSA, Authentification d’individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D, thèse Doctorat de l'Université Evry Val d'Essonne,2008.

[4] Lorène ALLANO, La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles, Thèse de doctorat de l’ UNIVERSITE D’EVRY-VAL D’ESSONNE,2009.

[5] Djamila.Mahmoudi, Biométrie et Authentification , département Corporate Information and Technology de Swisscom AG. http://ditwww.epfl.ch/SIC/SA/publications/FI00/fi-sp-00/sp-00- page25.html.

[6] http://www.biometrics.org/html/introduction.html

[7] http://csrc.nist.gov/cryptval/des/tripledesval.html

[8] Davide Maltoni, Dario Maio , Anil K. Salil Prabhakar , 2003, Fingerprint Handbook.

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

[10] Djamel Saigaa, Contribution à l'authentification d'individus par reconnaissance de visages, thèse de Doctorat d'état en automatique, Université Mohamed khider Biskra Algérie, Novembre 2006.

[11] Christophe Gisler, Développement Java d’un outil de visualisation de courbes de performance biométriques, Rapport de Travail de Bachelor, Département d’Informatique Université de Fribourg Suisse 2006.

[12] Walid Hizem, Capteur Intelligent pour la Reconnaissance deVisage, Thèse de doctorat de l’institut National des Télécommunications et l’Université Pierre et Marie Curie – Paris, 2009.

[13] R. Beveridge and M. Kirby. “Biometrics and Face Recognition”. IS&T Colloquium, p. 25, 2005.

[14] S. Shan and Al., “Illumination normalization for robust face recognition against varying lighting conditions,”IEEE International Workshop on Analysis and Modeling of Faces and Gestures , pp. 157–164, 2003.

[15] D. Petrovska-DelaCrétaz,G.Chollet, and B.Dorizzi, editors. Biometric Reference Systems and Performance Evaluation.Springer, 2009.

[16] X. Tana, C. Songcan. Face recognition from a single image per person: A survey. Pattern Recognition, 2006.

[17] R. Brunelli et T. Poggio. Face recognition : Features versus templates. PAMI, 15(10) :1042–1052, 1993.

[18] L.Wiskott et J. M. Fellous et N. Kruger et C. von der Malsburg. Face recognition by elastic bunch graph matching. PAMI, 19(7) :775–779, July 1997.

[19] C. Liu and H. Wechsler. “A Unified Bayesian Framework for Face Recognition”. In : Proceedings of the IEEE International Conference on Image Processing, pp. 151–155, 1998.

[20] G. Guo, S. Li, and K. Chan. “Face Recognition by Support Vector Machines”. In : Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition, pp. 196–201, 2000.

[21] T. Cootes, G. Edwards, and C. Taylor. “Active Appearance Models”. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 23, No. 6, pp. 681–685, June 2001.

[22] T. Ahonen, A. Hadid, and M. Pietikainen. Face Recognition with Local Binary Patterns. 2004.

[23] M. A. Turk and A. P. Pentland. Face recognition using eigenfaces. In CVPR, pages 586–590, Hawai, June 1992.P.

[24] Belhumeur, J. Hespanha, D. Kriegman, Eigenfaces vs. fisherfaces: recognition using class specific linear projection, IEEE Trans. Pattern Anal. Mach. Intell. 19 (7) 711–720, 1997.

[25] W. Zhao, R. Chellappa, P.J. Phillips, Subspace linear discriminant analysis for face recognition, Technical Report CAR-TR-914, Center for Automation Research, University of Maryland, 1999.

[26] J. Lu, K.N. Plataniotis, A.N. Venetsanopoulos, Face recognition using kernel direct discriminant analysis algorithms, IEEE Trans. Neural Networks 14 (1) 117–126, 2003.

[27] D.A. Socolinsky and A. Selinger. Thermal face recognition in an operational scenario. In CVPR, pages 1012–1019, 2004.

[28] Shi-Qian Wu, Li-Zhen Wei, Zhi-Jun Fang, Run-Wu Li, and Xiao-QinYe. Infrared face recognition based on blood perfusion and sub–block dct in wavelet domain. In International Conference on Wavelet Analysis and Pattern Recognition, 2007.

[29] H. Sahbi. Kernel PCA for similarity invariant shape recognition. Neurocomputing, 70(16-18) :3034–3045, 2007.

[30] H. Schwenk. The diabolo classifier. Neural Computation, 10(8) :2175–2200, 1998.

[31] P.J. Phillips, Support vector machines applied to face recognition, Adv. Neural Inform. Process. Syst. 11 (03) 809, 1998.

[32] S.Z. Li, J. Lu. Face recognition using the nearest feature line method, IEEE Trans. Neural Networks 10 (2) 439–443, 1999.

[33] X. He, X. Yan, Y. Hu, p. Niyogi, H. Zhang. Face recognition using Laplacianfaces, IEEE Trans. Pattern Anal. Mach. Intell. 27 (3) 328–340, 2005.

[34] S. Duffner, C. Garcia, “A Connexionist Approach for Robust and Precise Facial Feature Detection in Complex Scenes” , Fourth International Symposium on Image and Signal Processing and Analysis (ISPA 2005), Zagreb, Croatie, Septembre 2005.

[35] H.S. Le, H. Li. Recognizing frontal face images using hidden Markov models with one training image per person, Proceedings of the 17th International Conference on Pattern Recognition (ICPR04), vol. 1, pp. 318–321, 2004.

[36] C. Liu and H.Wechsler, “Robust coding schemes for indexing and retrieval from large face databases,” IEEE Trans. on Image Processing, vol. 9, no. 1, pp. 132–137, 2000.

[37] Chengjun Liu and Harry Wechsler “Gabor Feature Based Classification Using the Enhanced Fisher Linear Discriminant Model for Face Recognition”, IEEE Trans. Image Processing, vol. 11, no. 4, pp. 467- 476, 2002.

[38] Ziad M. Hafed et Martin D. Levine : Face recognition using discrete cosine transform. International Journal of Computer Vision, 43(3):167–188, July – August 2001.

[39] K. Rao et P. Yip : Discrete Cosine Transform : Algorithms, Advantages, Applications. Academic Press, 1990.

[40] Mirosław Miciak, Character Recognition Using Radon Transformation and Principal Component Analysis in Postal Applications, Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 495 – 500.

[41] Radon transform - Wikipedia, the free encyclopedia.

[42] R.M. Haralick, K. Shanmugam, I. Dinstein, Textural Features for Image Classification, IEEE Transactions on Systems, Man, and Cybernetics, vol. 3, no. 6, pp. 610–621, 1973.

[43] Mohan et al. , A New Method of Face Recognition Based on Texture Feature extraction on individual components of face / pp. 69-74 International Journal of Signal and Image Processing (Vol.1-2010/Iss.2).

[44] Alaa ELEYAN, Hasan DEM˙IREL , Co-occurrence matrix and its statistical features as a new approach for face recognition, Turk J Elec Eng & Comp Sci, Vol.19, No.1, 2011.

[45] W.J. DeCoursey , Statistics and Probability for Engineering Applications With Microsoft Excel, College of Engineering,University of Saskatchewan,Saskatoon ,Copyright 2003, Elsevier Science (USA).

[46] Fukunaga, K.,(1990). Introduction to Statistical Pattern Recognition, second ed., Academic Press Springer, New York.

[47] L.F Chen et Al. Why recognition in a statistics based face recognition system should be based on the pure face purtion : a probabilistic decision based proof. Pattern recognition. Vol 34,No 7. 2001.

[48] K. Messer, J. Matas, J. Kittler et K. Jonsson : Xm2vtsdb : The extended m2vts database. Audio- and Video-based Biometric Person Authentication (AVBPA), pages 72–77, Mars 1999.

[49] J. Luettin and G. Maitre. “Evaluation protocol for the extended M2VTS database”. IDIAP,available at http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/face-avbpa2001/protocol.ps,1998.

[50] Vincent Lozano, Contribution de l'analyse d'image couleur au traitement des images textile,thèse de doctorat de l'Université Jean Monnet Saint-Etienne spécialité Informatique :Image,1998.

[51] Nicolas VANDENBROUCKE, Segmentation d’images couleur par classification de pixels dans des espaces d’attributs colorimétriques adaptés. Application à l’analyse d’images de football. Thèse de doctorat de l'Université de lille,France,Discipline : automatique et InformatiqueIndustrielle,2000.

[52] Jon Yngve Hardeberg , Acquisition et reproduction d'images couleur : approches colorimétrique et multispectrale ,thèse de doctorat de l’Ecole Nationale Supérieure des Télécommunications Specialité : Signal et Images 1999.

[53] Laurent FUCHS, rapport: Influence des espaces de représentation de la couleur et Influence des espaces de représentation de la couleur et du système de codage dans le cadre du développement du système de codage dans le cadre du développement de JPEG2000. Département Informatique Université de Poitiers Année 2000-2001.

[54] Commission Internationale de l’ Eclairage. Colorimetry.Rapport technique 15.2, Bureau central de la CIE, Vienna, 1986.

[55] Yip, A. & Sinha, P. (2001). Role of Color in Face Recognition, MIT AI Memos, AIM-2001-035, (Dec 2001).

[56] Marcel, S. & Bengio, S. (2002). Improving Face Verification Using Skin Color Information,Proceedings of the International Conference on Pattern Recognition, pp 378-381, August 2002.

[57] Rajapakse, M.; Tan, J. & Rajapakse, J. (2004). Color Channel Encoding with NMF for Face Recognition, Proceedings of the International Conference on Image Processing, pp 2007-2010, October 2004.

[58] Youssef, K. & Woo, P.-Y. (2007). A New Method for Face Recognition Based on Color Information and a Neural Network, Proceedings of the International Conference on Natural Computation, pp. 585-589, 9780769528755, China, Aug 2007, IEEE, Haikou.

[59] Zhiming Liu; Jian Yang; Chengjun Liu; Extracting Multiple Features in the CID Color Space for Face Recognition, image processing IEEE volume 19 issue 9. Sept. 2010.

[60] Jian Yang, Chengjun Liu, Lei Zhang, Color space normalization: Enhancing the discriminating power of color spaces for face recognition, Pattern Recognition, Volume 43, Issue 4, April 2010.

[61] Meriem Fedias, L'apport de la couleur à la verification d'identité à l'aide des images de visages. Université de Biskra, Algérie.2007.

[62] A. Gasteratos, M. Vincze, and J.K. Tsotsos (Eds.):Face Recognition Using a Color PCA Framework ICVS 2008, LNCS 5008, pp. 373–382, 2008.Springer-Verlag Berlin Heidelberg 2008.

[63] M. Fedias, D. Saigaa " A New approach based in mean and standard deviation for authentication system of face ", International Review on computers and software (IRECOS), pp. 309-314, Vol. 5 n°3 May 2010, Italy.

[64] M. Fedias, D. Saigaa "Non linear fusion of colors to face authentication using EFM method ", Journal of Applied Computer Science & Mathematics (JACSM), n°9 (4) Nov 2010, pp. 42-50, Romania.

[65] M. Fedias, D. Saigaa " A New Fast method of face Authentication based on First order Statistical Feature ", International Journal of Computer Applications (IJCA), Vol. 14 n°8 February 2011, pp. 32-37, New York USA.

[66] M. Fedias, D. Saigaa, M. Boumehrez "Logic Fusion of Color based on new Fast Feature extraction for face authentication", International Journal of Computer Science Issues (IJCSI), Vol.8 n°3 May 2011.

[67] M. Fedias, D. Saigaa " Nonlinear fusion of colors to face authentication ", Proc. Conf. ICEEDT'08, International conference on electrical engineering design and technologies, Hammamet, Tunisia, Nov. 2008.

[68] M. Fedias, D. Saigaa " Linear Discriminant Analysis LDA and logic fusion of Colors decisions to face authentication ", Proc. Conf. ICEEDT'08, International conference on electrical engineering design and technologies, Hammamet, Tunisia, Nov. 2008.

[69] M. Fedias, D. Saigaa "Comparison between LDA and PCA with the use of the color to face authentication ", Proc. Conf. STA'2008, the 9th international conference on

sciences and techniques of automatic control and computer engineering, Sousse, Tunisia, 2008.

[70] M. Fedias, D. Saigaa “Linear Discriminant Analysis LDA and the nonlinear fusion of colors to face authentication”, Proc. Conf. STA'2008, the 9th international conference on sciences and techniques of automatic control and computer engineering, Sousse, Tunisia 2008.

[71] M. Fedias, D. Saigaa “ Non linear fusion of colors to face authentication using EFM method ”, the International Workshop on Systems Communication and Engineering in Computer Science CECS’ 2010, le 3-5 Oct 2010 in Batna (Collaboration with TU-Berlin German University and University of Batna; Springer Publishing of CECS 2010 proceedings).