L'apport de la couleur à l'authentification de visage

M. Fedias[1]

[1] Departement d'électronique,
Laboratoire de modélisation des systèmes énergétiques LMSE,
Université Mohamed khider,
B.P 145 RP Biskra (07000),
Algerie,
Email : meriem_fedias@yahoo.fr

D. Saigaa[2]

[2] Departement d'automatique,
Laboratoire de modélisation des systèmes énergétiques LMSE Université Mohamed khider,
B.P 145 RP Biskra (07000), Algerie,
Email : saigaa_dj@yahoo.fr

Résumé

Les systèmes d'authentification de visage utilisent souvent la représentation de l'image du visage en niveaux de gris comme caractéristique d'entrée. Mais lorsque les images sont représentées en couleur, il est avantageux d'utiliser cette information supplémentaire pour améliorer les performances du système d'authentification. Dans cet article, Nous avons proposé d'introduire l'information de couleur au système d'authentification. Plusieurs espaces de couleur ont été testés sur la base de données XM2VTS selon son protocole associé «protocole de Lausanne ». Pour l'extraction du vecteur de caractéristiques du visage nous avons utilisé la méthode d'analyse en composantes principales (ACP) ou (EigenFaces). Les résultats trouvés montrent que l'information couleur de certains espaces couleurs améliore les performances du système d'authentification.

Mots clé : L'analyse en composantes principales (ACP), authentification de visage, les espaces de couleur, Eigenfaces.

1. INTRODUCTION

La vérification d'identité a gagné une attention considérable ces dernières années, par le besoin croissant de systèmes de contrôle d'accès en utilisant plusieurs modalités biométriques. Les premières études théoriques de la reconnaissance faciale remontent au début des années 1970 [2]. En 1991, Turk et Pentland [1] ont introduit le concept d'EigenFaces à des fins de reconnaissance. En se basant sur une analyse en composantes principales (ACP) ; la méthode d'Eigenfaces repose sur une utilisation des premiers vecteurs propres de la matrice de covariance des données d'apprentissage comme visages propres, d'où le terme EigenFaces.

La tache est simple ; l'image du visage est captée par une caméra. Le sujet peut se présenter devant celle-ci et selon la technique utilisée, le système extrait les caractéristiques du visage pour faire la comparaison avec les caractéristiques de la personne réclamée qui est conservées dans une base de données.
L'article est organisé comme suit: la section 2 présente le problème d'authentification de visage, la section 3 explique l'algorithme de l'ACP utilisé pour l'extraction de caractéristiques, dans la section 4 nous présentons les résultats expérimentaux obtenues , et enfin dans la section 5 nous donnons les conclusions et les perspectives.

2. AUTHENTIFICATION DE VISAGE

Un système d'authentification sait a priori l'identité de l'utilisateur (par exemple par un mot de passe) et doit vérifier cette identité pour plus de sécurité, si c'est vraiment l'utilisateur ou bien un imposteur.
Le principe du système d'authentification de visage d'un individu est l'extraction d'un vecteur X de caractéristiques de ce dernier, afin de le comparer avec un vecteur Y_i qui contiens les caractéristiques de ce même individu extrait à partir de ses images qui sont stockés dans une base de données ($1 \le i \le p$, où p est le nombre d'images de visage de cette personne dans l'ensemble d'apprentissage). Pour estimer la différence entre deux vecteurs, il faut introduire une mesure de similarité. Plusieurs métriques peuvent être utilisées comme par exemple les distances euclidiennes L1 et L2, la distance de Mahalanobis la corrélation, … etc.
Par exemple, si la distance euclidienne entres les vecteurs X et Y_i est inférieure à un seuil, on constate que l'image du visage correspond à la personne réclamée. Donc le choix d'un meilleur seuil de décision est très important. Un seuil trop petit donne un taux élevé de faux rejet (*TFR*) des clients (utilisateurs

légitimes du système), alors q'un seuil trop grand donne un taux élevé de fausse acceptance (*TFA*) des imposteurs. Donc il faut ajuster le seuil de décision pour atteindre une valeur désirée et prédéfinie de *TFR* ou de *TFA*.

3. EXTRACTION DE CARACTERISTIQUE PAR L'ACP

La prise des décisions sur des images approximatives s'est avérée nettement sensible aux conditions d'illumination, aux points de vue, à l'expression et aux différences de jour en jour dans un visage de la même personne, au point que deux images très semblables (à l'œil humain) pourraient être extrêmement différentes si elles sont comparées pixel par pixel. Il est donc nécessaire d'extraire les caractéristiques appropriées et discriminantes à partir des images [10].

L'analyse en composantes principales (ACP) est une méthode mathématique linéaire d'analyse de données , son principe est de rechercher les directions de l'espace (les axes) qui maximise la variance des données et minimise l'écart au carré par rapport aux axes [8][9].

Dans le cas de la reconnaissance de visage nous considérons l'ensemble des images de visages d'un ensemble d'apprentissage comme un ensemble de vecteurs aléatoires (matrice de vecteurs visages), où chaque vecteur visage est constitué par l'enchaînement des lignes ou des colonnes d'une image de visage. L'ACP est appliquée à cette matrice des vecteurs visages. Elle consiste essentiellement à effectuer une réduction de dimensionnalité en codant les visages dans une nouvelle base formée par les premiers vecteurs propres (EigenFaces) provenant du calcul de l'ACP.

La méthode d'EigenFaces se déroule comme suit :

Soit $A=(X_1,X_2,...,X_i,....,X_N)$ représente une matrice de donnée de dimension nxl , où chaque X_i est un vecteur visage de dimension n . Ici n représente le nombre de Pixel dans l'image de visage et l est le nombre d'images de visages dans l'ensemble d'apprentissage.

1. Un vecteur visage moyen $\overline{X}$ est calculé à partir des *l* vecteurs images de visages de l'ensemble d'apprentissage.

$$\overline{X} = \frac{1}{l}\sum_{1}^{l} X_i \qquad (1)$$

2. Le vecteur visage moyen est soustrait des images d'apprentissage (on élimine donc les ressemblances pour se concentrer sur les différences), ce qui génère les vecteurs de différences $\overline{X}_i$ associés à chacune des images :

$$\overline{X}_i = X_i - \overline{X} \qquad (2)$$

3. Les vecteurs $\overline{X_i}$ sont combinés, côte à côte, pour créer une matrice de données d'apprentissages $\widetilde{X}$ de taille (*nxl)*.

$$\widetilde{X} = \left[\overline{X_1}\,\overline{X_2}..... \overline{X_l}\right] \qquad (3)$$

La matrice de données $\widetilde{X}$ est multipliée par sa transposé pour trouver la matrice de covariance Ω , donnée par [3] :

$$\Omega = \widetilde{X}.\widetilde{X}^T \qquad (4)$$

4. La transformation linéaire d'un vecteur visage est donnée par:

$$Y_i = W^T \overline{X_i} \qquad (5)$$

où Y_i est un vecteur caractéristique de dimension $mx1$ et qui contient les coefficients de projection du vecteur visage $\overline{X_i}$ dans le nouveau espace de transformation et W est une matrice formée par les *m* premiers vecteurs propres de la matrice de covariance correspondant aux *m* plus grandes valeurs propres . Noter bien que *m* est très inférieur à n ($m << n$).

Donc par l'application de l'ACP, un vecteur visage d'entrée de dimension *n* est réduit à un vecteur caractéristique dans un sous espace de dimension *m*.

4. RESULTATS EXPERIMENTAUX

4.1. BASE DE DONNEE

La comparaison de techniques ou d'algorithmes, permettant ainsi une évaluation relative des performances du système d'authentification, nécessite l'utilisation d'un ensemble de données volumineux, représentatif et standardisé. Nos expériences ont été exécutées sur des images frontales de visage de la base de données XM2VTS. 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 [4].

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).

Le protocole de Lausanne partage la base de données en trois ensembles [5]:

1. L'ensemble **d'apprentissage** (training): il contient l'information concernant les personnes connues du système (seulement les clients)

2. L'ensemble d'**évaluation** (validation): permet de fixer les paramètres du système d'authentification de visages.
3. L'ensemble de **test** : permet de tester le système en lui présentant des images de personnes lui étant totalement inconnues.

Pour la classe des imposteurs, les 95 imposteurs sont répartis dans deux ensembles : 25 pour l'ensemble d'évaluation et 75 pour l'ensemble de test. La figure1 illustre la répartition des images dans les différents ensembles [5].

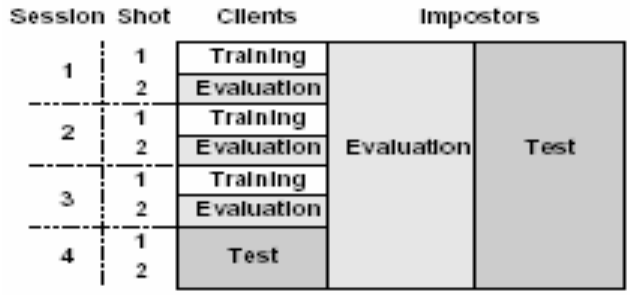


Figure 1. Configuration I de la base de données XM2VTS

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

ensemble	clients	imposteurs
apprentissage	600 (3par personnes)	0
Evaluation	600 (3par personnes)	200 (8par personnes)
Test	400 (2par personnes)	560 (8par personnes)

TABLEAU I. Répartition des photos dans les différents ensembles

La figure 2 représente quelques exemples d'images de visages de la base de données XM2VTS.

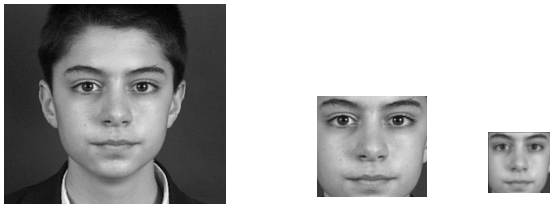
Figure 2. Exemples de photos de la base XM2VTS

4.2. PRETRAITEMENT

Chaque image est constituée de plusieurs informations comme : l'arrière plan, les cheveux, les cols de chemise, les oreilles…etc.

En effet, toutes ces informations ne servent à rien, mais gonfle inutilement la taille des données. Donc une réduction d'image est nécessaire dont l'opération est d'extraire seulement les paramètres essentiels pour l'identificateur et qui changent très peu avec le temps.

Pour cela, on découpe l'image par une fenêtre rectangulaire de taille 132x120 centrée autour des caractéristiques les plus stables liées aux yeux, aux sourcils, au nez et à la bouche. Ensuite on filtre les images par un filtre passe bas uniforme (2x2) afin d'effectuer une décimation de facteur 2(voir figure 3) puis nous faisons la photonormalisation aux images càd : que pour chaque image, nous soustrayons à chaque pixel la valeur moyenne de ceux-ci sur l'image, 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 un groupe d'images (pour chaque composante, on retire la moyenne de cette composante pour toutes les images et on divise par la déviation standard) [6].



(a) (b) (c)

Figure 3. a) image d'entrée, b) image après découpage et c) image après décimation.

4.3. EXTRACTION DE CARACTERISTIQUE

L'extraction des caractéristiques se fait par la méthode d'EigenFaces basée sur l'analyse en composante principale ACP. La méthode se déroule comme nous l'avons déjà détaillé à la section 3.

4.4. CLASSIFICATION

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 faible et un TFR 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 sont calculés dans deux ensembles : d'abord dans un ensemble d'évaluation, qui va permettre de fixer plus ou moins le TEE en faisons

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.

4.5. MESURE DE SIMILTITUDE

Une fois que les images sont projetées dans un sous-espace, il reste à déterminer quelles sont les images semblables..

Il y a beaucoup de mesures possibles de distance et de similitude, parmi lesquelles on cite :

A. La norme L2

Connue aussi sous le nom norme euclidienne, c'est la somme du différence carré entre les composantes des deux vecteurs A et B. Elle est donnée par l'équation suivante :

$$L2 = \sum_{i=1}^{N} \left(A_i - B_i\right)^2 \qquad (6)$$

B. Corrélation

Elle mesure le taux de changement entre les composantes de deux vecteurs *A* et *B*. Elle est donnée par la relation :

$$Corr(A,B) = \sum_{i=1}^{N} \frac{(A_i - \mu_A)(B_i - \mu_B)}{\sigma_A \sigma_B} \qquad (7)$$

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

4.6. COMPARAISON

En effet, il existe différents espaces de couleurs On peut légitiment se poser la question : quel espace de couleur choisir ?. Pour répondre à cette question nous avons effectué nos expériences sur plusieurs espaces couleurs. Pour faire une comparaison de résultats , nous avons présenté ces derniers avec une méthode basique l'EigenFaces, qui a pour paramètres :

_ Prétraitement avec photonormalisation

_Coefficients : les coefficients de projection triée suivants les valeurs propres décroissantes.

_ Mesure de score (similarité): corrélation.

_Seuillage : Globale.

A partir de la figure4, nous pouvons dire que avec l'utilisation des images présentées dans l'espace couleur YIQ sont les meilleurs avec un taux d'égale erreur TEE=0.0412 en utilisant un nombre de caractéristique égale à 98 ,suivis de ceux de l'espace de couleur RGB ,puis de ceux de l'espace de couleur Lab, et enfin les résultats obtenus en utilisant les composantes couleur de l'espace de couleur HSV, qui est loin avec un taux d'égale erreur TEE=0.1436 en utilisant un nombre de caractéristique égale à 82(voir figure5.b) .

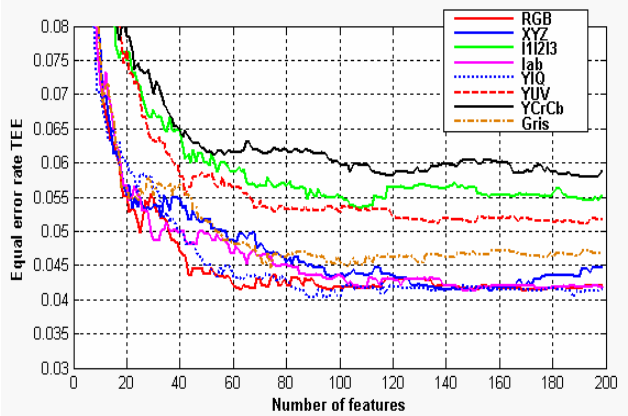


Figure 4. Taux d'erreurs dans l'ensemble d'évaluation des différentes espaces couleur.

A partir de l'ensemble des figures (de la figure5.a jusqu'à la figure5.k), nous remarquons aussi que quelques composantes couleurs individuellement donnent des résultats meilleurs que ceux en utilisant simultanément les trois composantes couleurs de même espace. Sauf dans le cas de l'espace RGB qui donne des résultats meilleurs que celles de ses composantes R,G ou B individuellement .

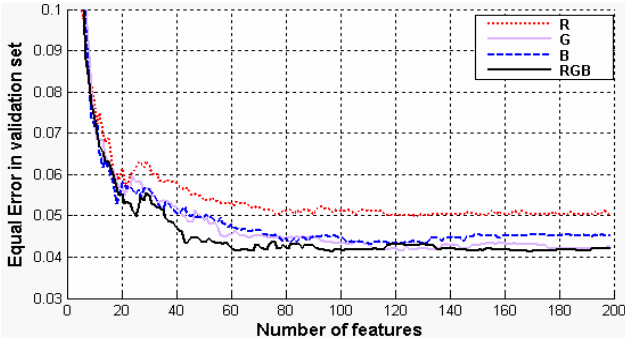


Fig 5.a

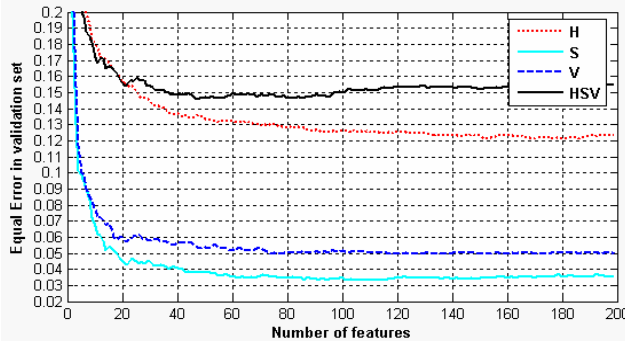


Fig 5.b

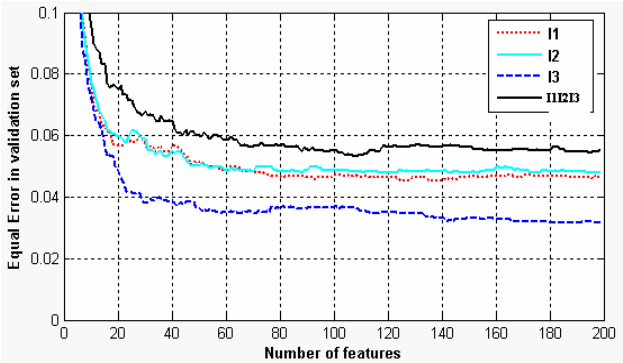


Fig 5.c

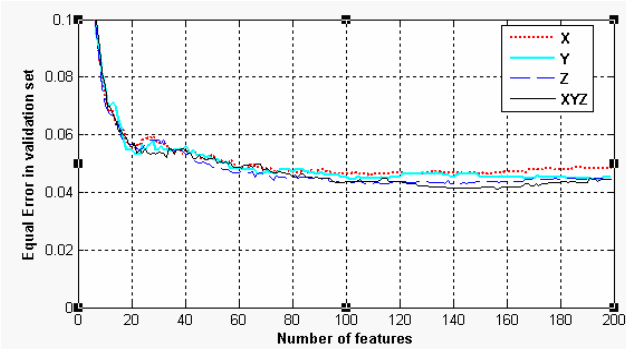


Fig 5.d

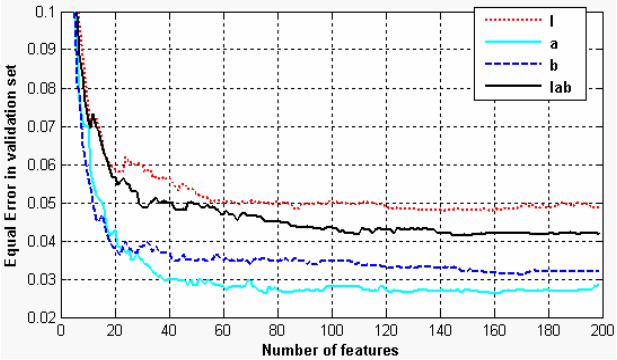


Fig 5.e

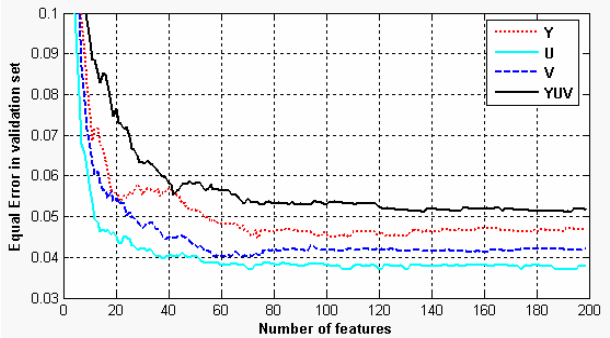


Fig 5.f

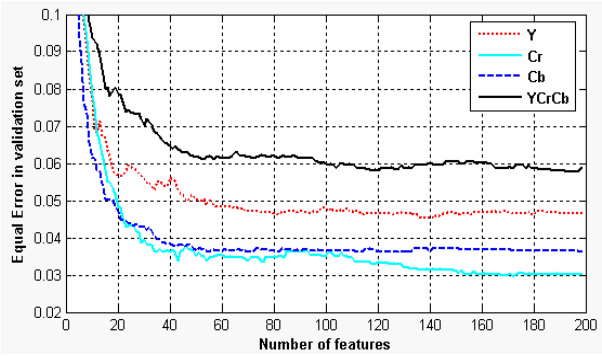


Fig 5.g

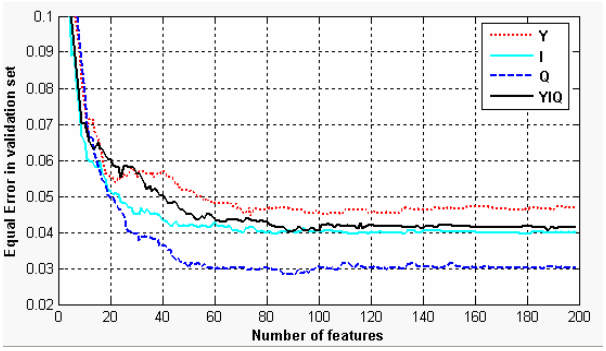


Fig 5.k

Figure5. résultats des différentes espaces couleur avec ses composantes couleur .

La dernière courbe figure6 présente les résultats obtenus de plusieurs composantes couleur de différentes espaces couleurs. Nous pouvons voir que les résultats obtenus avec la composante couleur {a}de l'espace Lab est la meilleur avec un TEE de l'ordre de 0.02642 en utilisant 83 composantes principales du vecteur visage d'entrée, suivi du résultats obtenu avec la composante couleur{Q}de l'espace YIQ avec un TEE de l'ordre de 0.0283 en utilisant 88 composantes principales du vecteur visage d'entrée .

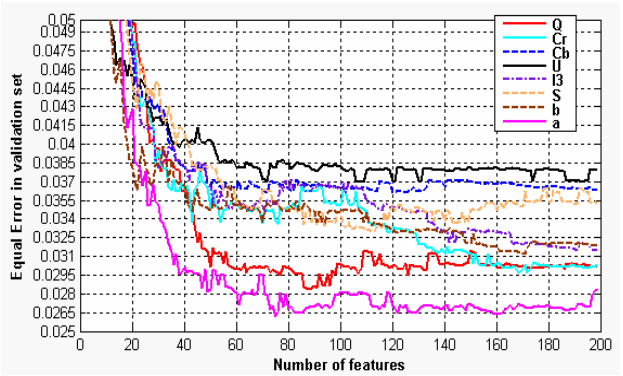


Figure 6. Taux d'erreurs dans l'ensemble d'évaluation des différentes Composantes couleur

Lorsque nous avons essayé d'appliquer la mesure de similitude par la distance euclidienne à la composante {a} de l'espace couleur Lab . Nous avons remarqué que les résultats sont moins meilleurs que celle avec l'utilisation de la corrélation qui est mieux adaptée à des données en grande dimension que la norme euclidienne

C'est pour cette raison nous choisissons l'utilisation de la corrélation comme mesure de similitude.

Le tableau II présente le minimum du taux d'égale erreur TEE dans l'ensemble d'évaluation ainsi que le TFA et le TFR dans l'ensemble de test des différentes espaces couleurs et de quelques composantes colorimétriques, avec l'utilisation de la corrélation comme mesure de similitude.

La caractéristique de l'espace couleur Lab est qu'il a été crée afin de fournir une expression quantitative de classification des couleurs dans le système de Munsell, d'où la non cohérence et l'orthogonalité de ses composantes [7][12][11].

Pour cela nous avons obtenu une meilleur résultat avec la composante{a} qui s'appelle la dominante vert-rouge de l'espace couleur Lab

Composante/ où espace Couleur	**Nombre de caracté-ristique**	**L'ensemble d'evaluation**	**L'ensemble de test**	
		TEE	**TFA**	**TFR**
Niveaux de gris	98	0.0452	0.0584	0.05
YIQ	**98**	**0.0412**	**0.0412**	**0.05**
RGB	68	0.0415	0.0529	0.0525
Lab	109	0.0417	0.0406	0.0525
XYZ	97	0.0434	0.0565	0.045
YUV	127	0.0516	0.0442	0.05
I1I2I3	116	0.0548	0.050	0.052
HSV	82	0.1463	0.116	0.17
{a}lab	**83**	**0.026421**	**0.0298**	**0.0475**
{Q}YIQ	88	0.0283	0.0298	0.0525
{Cr}YCrCb	168	0.0297	0.0311	0.05
{b}lab	160	0.0317	0.0414	0.04
{I3}I1I2I3	189	0.0315	0.0329	0.0475
{S}HSV	102	0.03323	0.0455	0.0425
{Cb}YCrCb	120	0.0361	0.0284	0.0475
{U}YUV	108	0.0369	0.0356	0.03

TABLEAU II. Les résultats avec l'information couleur.

Les différences entre les erreurs des deux ensemble évaluation et test , sont faibles Ceci est une propriété très importante donc on peut dire que le système d'authentification est stable .

CONCLUSION

Nous avons étudié l'apport de la couleur à l'authentification de visage des différentes espaces couleurs les plus utilisable. Pour l'extraction de caractéristique nous avons utilisé la méthode d'Eigenface basée sur l'analyse en composantes principales (ACP).

Lorsqu'on utilise les trois composantes associes au même espace couleur , les meilleurs résultats sont obtenu par l'utilisation de l'espace couleur YIQ avec un taux d'égale erreur dans l'ensemble d'évaluation TEE=0.0412. en utilisant un nombre de caractéristiques égale à 98 .

L'utilisation d'une seule composante couleur donne des meilleurs résultats avec la composante {a} de l'espace couleur Lab avec un taux d'égale erreur dans l'ensemble d'évaluation TEE=0.02642. en utilisant un nombre de caractéristiques égale à 83 .

Nous avons vu aussi, que l'utilisation de la corrélation pour la mesure de similarité, améliore sensiblement les résultats et augmente les performances du système d'authentification**.**

Dans les travaux futurs nous proposons la fusion des différentes composantes ou espaces couleur avec l'ACP où bien d'autre méthodes comme: L'analyse linéaire discriminante (LDA), L'analyse en composantes indépendantes (ICA).

BIBLIOGRAPHIE

[1] TURK M. A. et PENTLAND A. P.: *Face recognition using eigenfaces*. IEEE Comput. Sco.
Press, p. 586-591, June 1991.

[2]CHELLAPPA R., WILSON C. L., and SIROHEY S.: *Human and machine recognition of faces*: A survey. Proceedings of the IEEE, p. 705-740, 1995.

[3] Matthew Turk et Alex Pentland : Eigenfaces for recognition. Journal of cognitive
neuroscience, 3(1):71–86, 1991

[4] 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.

[5] 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.

[6]:D.Saigaa, N.Benoudjit, K.Benmahamed, S.Leland-ais: Authentification d'individus par reconnaissance de visage, courier de savoir-N°6, juin 2005, Biskra, Algerie.

[7] Jon Yngve Hardenberg, 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.

[8] C. Havran, L. Hupet, J. Czyz, J. Lee, L. Vandendorpe, M. Verleysen "Independent Component Analysis for face authentication" KES'2002 proceedings –
Knowledge- Based Intelligent Information and Engineering Systems, Crema (Italy),16- 18 September 2002

[9] Wendy S. Yambor "analysis of PCA and Ficher discriminant-based imag recognition algorithms. Technical rapport, Colorado State University July 2000.

[10] P. Belhumeur, J.P. Hespanha, D.J. Kriegman , Eigenfaces vs. Fisherfaces: recognition using class specific linear projection. IEEE Trans. on Pattern Analysis and Machine Intelligence, 1997, pp. 711-720.

[11] D. Saigaa, S. Lelandais, K. Bemahammed and N. Benoudjit "Color Space for Face Authentication using Enhanced Fisher linear discriminant Model (EFM)", WSEAS International Conference on Applications of Electrical Engineering (AEE'06), Prague, Czech Republic, March 12-14, 2006, pp. 196-201.

[12] D. Saigaa, S. Lelandais, K. Bemahammed and N. Benoudjit " Improvements for face authentication using color information", WSEAS Transactions on Signal Processing, ISSN 1790-5022, Vol. 2, March 2006, pp. 343-350.