UNE APPROCHE MULTIMODALE POUR LA VERIFICATION BIOMETRIQUE

ISMAHÈNE DEHACHE[(1)] &LABIBA SOUICI-MESLATI[(2)]

[(1)] Laboratoire LRI, Université Badji Mokhtar, BP 12, 23000, Annaba, Algérie
ismaheneinfo@gmail.com
[(2)] Laboratoire LRI, Université Badji Mokhtar, BP 12, 23000, Annaba, Algérie
souici_labiba@yahoo.fr

RÉSUMÉ

Aujourd'hui, la biométrie est un domaine de recherche en pleine expansion, plusieurs systèmes d'identification et de vérification sont à présent développés, cependant leurs performances restent insuffisantes face aux besoins accrus de plus de sécurité. L'utilisation d'une seule modalité biométrique diminue, dans la plupart des cas, la fiabilité de ces systèmes, ce qui nous a incités à combiner plusieurs modalités. Dans cet article, nous prposons une approche de fusion multibiométrique pour la vérification de l'identité. En effet, nous utilisons deux types de biométries : l'empreinte digitale et la signature. Notre approche d'intégration de ces modalités se base sur l'utilisation des séparateurs à vaste marge (SVM), cette fusion est réalisée au niveau des scores générés à partir d'une combinaison de classifieurs neuronaux de type perceptrons multicouches. La décision est prise, par la suite, selon le score émis par le classifieur SVM. Nous avons ainsi conçu et réalisé un système multibiométrique par la fusion des deux modalités, cette fusion a permis d'améliorer significativement les performances de vérification. Les résultats obtenus confirment la supériorité de la multibiométrie par rapport aux systèmes biométriques unimodaux.

MOTS-CLES : Multibiométrie, vérification, signatures, empreintes digitales, fusion de données, classification, SVM, PMC, combinaison.

1 INTRODUCTION

Face à un marché de la sécurité en plein essor, et aux méthodes informatiques traditionnelles employées (accès par codes et/ou mots de passe) dont les limites ont rapidement été démontrées, la biométrie s'impose de manière indéniable comme la technologie d'avenir dans le domaine de la sécurité mais aussi du confort d'utilisation. C'est pour cette raison que beaucoup des travaux de recherches se tournent vers cet horizon.

La biométrie est le domaine technologique traitant de la vérification d'identité et/ou de l'identification de personnes par leurs caractéristiques individuelles, pouvant être morphologiques ou comportementales.

De nombreux travaux ont été réalisés sur l'optimisation séparée de chacune des modalités biométriques, cependant peu d'efforts ont été consentis sur la fusion multimodale relativement à l'unimodalité.

L'objectif de notre travail est de proposer une approche d'intégration de plusieurs modalités biométriques (en l'occurrence deux modalités) afin de pallier aux problèmes de la vérification biométrique unimodale. L'approche proposée est basée sur la fusion de deux modalités biométriques : l'empreinte digitale et la signature, qu'on peut considérer comme les modalités les plus répandues et les plus étroitement liées sur le plan utilisation.

Dans notre proposition, à chaque modalité biométrique correspond à un système unimodal complet de vérification, se basant sur la classification par combinaison de plusieurs réseaux neuronaux de type perceptrons multicouches (PMC). Les deux systèmes génèrent, chacun, un score de vérification, ces deux scores vont être fusionnés par un classifieur SVM (machine à vecteurs de supports), afin de fournir un seule score à partir duquel l'identité de l'individu peut être acceptée ou rejetée.

La suite de cet article est organisée de la manière suivante. La section 2 aborde la fusion des données dans les systèmes multibiométrique sur le plan des sources d'informations et des niveaux de fusion. La section 3 donne un aperçu général sur le système multibiométrique proposé. La section 4 est dédiée à la description du sous-système de vérification basé sur les empreintes alors que la section 5 est consacrée au sous-système basé sur la signature. Les modules de fusion et de décision sont présentés dans les sections 6 et 7. La section 8 contient la présentation et la discussion des résultats obtenus. Nous terminons notre article dans la section 9 par une conclusion et des perspectives d'extensions futures au travail présenté.

2 FUSION DES DONNÉES BIOMÉTRIQUES

Les systèmes multibiométriques sont destinés à reconnaître des personnes à la base d'informations acquises à partir de plusieurs sources biométriques [1] [2]. Sources d'information et taxonomie des systèmes multibiométriques Ross et al. [3] proposent, pour les systèmes multibiométriques, une taxonomie selon les sources d'informations utilisées, en identifiant six classes de systèmes multibiométriques :

2.1 Système multi-capteurs

Correspondant à l'utilisation de plusieurs capteurs pour l'acquisition d'une seule modalité biométrique. Pour la reconnaissance du visage, par exemple, il est possible d'utiliser plusieurs caméras 2D, des capteurs 3D ainsi que des capteurs infra-rouges. L'utilisation de plusieurs capteurs permet d'acquérir des informations complémentaires pour accroître les performances des systèmes unimodaux.

2.2 Système multi-classifieurs ou multi-lgorithmes

Cette classe désigne les systèmes qui utilisent plusieurs classifieurs (de même type ou de types différents) ayant comme entrée les caractéristiques extraites à partir d'une seule modalité biométrique. Les ensembles de caractéristiques présentés à l'entrée des différents classifieurs peuvent être identiques ou différents. Par exemple, il est possible d'utiliser deux classifieurs pour la reconnaissance des empreintes digitales, l'un opérant sur les caractéristiques texturales, l'autre sur les minuties extraites à partir d'un même doigt.

2.3 Système multi-instances ou multi-unités (multi-instance or multi-unit system)

Cette classe désigne les systèmes impliquant l'acquisition de plusieurs unités ou instances de la même modalité biométrique. C'est le cas des systèmes utilisant l'iris droit ainsi que le gauche, l'empreinte de l'index droit ainsi que le gauche.

2.4 Système multi-échantillons

Cette classe désigne les systèmes où un même capteur est utilisé pour obtenir plusieurs variantes ou représentations complémentaires d'une seule modalité biométrique. C'est le cas, lors de la reconnaissance du visage en se basant sur les images du visage de face et selon les profils droit et gauche afin de prendre en compte les variations de la pose faciale.

2.5 Système multimodal

Cette classe correspond aux systèmes impliquant plusieurs modalités biométriques. Le coût de la réalisation de ces systèmes est généralement élevé, ceci est dû principalement à l'utilisation de plusieurs capteurs, et, par conséquent, la mise en place d'interfaces utilisateurs appropriées.

2.6 Système hybride

Le terme hybride est utilisé pour désigner un système multibiométrique qui intègre un sous-ensemble des cinq scénarios décrits précédemment. Par exemple, un système qui comprend deux classifieurs pour la reconnaissance du locuteur et trois autres pour la reconnaissance du visage est à la fois multi-classifieurs car il intègre plusieurs classifieurs pour une même modalité et multimodal puisque plusieurs modalités biomériques sont impliquées.

2.7 Niveau de fusion

La fusion dans les systèmes multibiométriques peut avoir lieu dans quatre niveaux [4]:

2.7.1 Fusion au niveau des capteurs

Les données brutes issues des capteurs sont combinées à ce niveau, ces données représentent des instances d'une même biométrie obtenues, soit par plusieurs capteurs compatibles, ou bien par un unique capteur. Par exemple, les images du visage obtenues par différentes caméras sont combinées pour former un modèle 3D du visage. Les instances des données doivent être compatibles, par exemple, les images du visage ne peuvent pas être combinées ensemble, si elles sont prises avec différentes résolutions.

2.7.2 Fusion au niveau des caractéristiques

Elle désigne la combinaison des vecteurs de caractéristiques obtenus par les différentes sources suivantes : plusieurs capteurs, plusieurs instances ou unités d'une même modalité biométrique, plusieurs modalités biométriques.Lorsque les vecteurs de caractéristiques sont homogènes (plusieurs prises d'une empreinte d'un individu), il résulte un seul vecteur de caractéristiques qui représente la moyenne des poids des vecteurs individuels. Dans le cas contraire (des vecteurs de caractéristiques de différentes biométries telles que : le visage et la signature), une concaténation de ces derniers est possible afin de former un seul vecteur de caractéristiques. La concaténation n'est pas possible dans le cas où les caractéristiques ne sont pas compatibles (c'est le cas pour les minuties des empreintes et les coefficients d'eigen-face, par exemple).

2.7.3 Fusion au niveau du score

Lorsque les classifieurs biométriques génèrent un ensemble de données avec un degré de ressemblance (score de classification), l'intégration peut avoir lieu au niveau du score de classification, appelé aussi fusion au *niveau de mesure* ou bien au *niveau de confiance*. Après les vecteurs de caractéristiques, les scores issus des classifieurs contiennent des informations très riches relatives aux données en entrée, un autre avantage de ce niveau est la possibilité d'accéder et de combiner les différents scores générés par les différents classifieurs, par conséquent, la fusion des données dans ce stade est l'approche la plus commune dans les systèmes multibiométriques [5].

2.7.4 Fusion au niveau de décision

L'intégration de l'information au niveau abstrait ou de décision peut avoir lieu lorsque chaque classifieur décide individuellement sur le résultat en se basant

3 ARCHITECTURE DU SYSTÈME PROPOSÉ

Le système proposé est composé de deux sous systèmes, le premier est basé sur la vérification des empreintes digitale tandis que le second est basé sur la vérification (hors-ligne) de la signature, chacun d'entre eux suit un processus bien déterminé comme le montre la figure 1 afin d'arriver à un score correspondant au score de vérification. La fusion de ces deux scores est réalisée par un classifieur SVM dont la sortie sert de base à la décision du système sur le sort de l'identité proclamée.

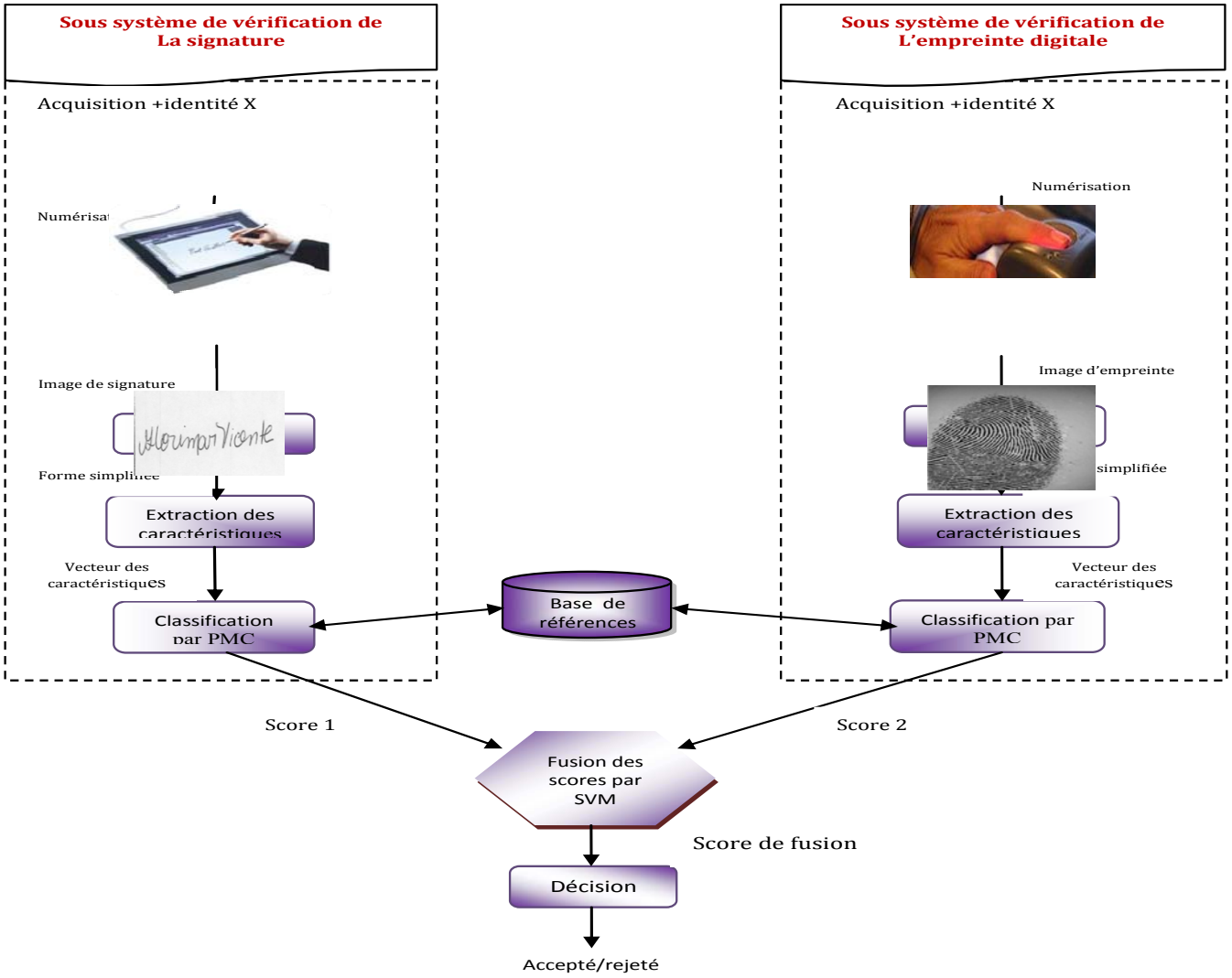

Figure 1 : Architecture du système proposé

4 SOUS SYSTÈME DE VÉRIFICATION DE L'EMPREINTE DIGITALE

4.1 Prétraitement

Le prétraitement des empreintes comprend trois étapes : la binarisation, le filtrage et la squelettisation.

4.1.1 Seuillage ou binarisation

Etant donné que l'image est en 256 niveaux de gris, (variant du noir au blanc), la binarisation donne une image en deux niveaux (binaire). Nous avons utilisé un seuillage simple, le seuil est calculé puis fixé par l'utilisateur (avec une marge prédéfinie), ensuite la valeur de chaque pixel sera comparée à ce dernier, si elle est supérieure au seuil le pixel prend la valeur un (noir) sinon il prend la valeur zéro (blanc).*

4.1.2 Filtrage

Le filtrage utilisé est le filtrage par la moyenne, la nouvelle valeur d'un pixel est calculée par le moyennage des valeurs des huit voisins qui l'entourent.

$$I'(i,j) = \frac{1}{8}\sum I(i,j)$$

Où : $|i-x| \leq 1$; $|i-y| \leq 1$; $(i, j) \neq (x, y)$. x, y représentent les cordonnées du pixel voisin

4.1.3 Squelettisation

L'algorithme de squelettisation opère par suppression de certains points de l'image initiale, jusqu'à obtenir une image ou l'épaisseur de chaque trait est un pixel. La méthode appliquée consiste en l'isolement des lignes principales de l'empreinte binarisée avec des amincissements successifs jusqu'à ce que l'empreinte résultante ne contienne que des lignes d'épaisseur 1 pixel. La méthode nécessite l'emploi successif de 8 masques. Nous effectuons sur l'empreinte une succession de passes ; nous arrêtons lorsque le résultat entre deux passes successives est inchangé.

4.2 Extraction des caractéristiques

Cette étape est l'une des plus importantes car elle va conditionner la suite des traitements. Les caractéristiques liées à l'empreinte digitale appelées aussi des points singuliers sont de deux types : globales (les centres et les deltas) et locales (les minuties).

Notre choix est porté sur les minuties comme étant des caractéristiques uniques pour chaque individu, ces minuties comprennent les points de fin de ligne ainsi que les points de bifurcation, ce choix est avéré beaucoup plus discriminant par rapport à l'utilisation des points singuliers de type global [8].

Nous disposons d'une image binaire squelettisée: un pixel noir prend la valeur 1, un pixel blanc prend la valeur 0 et l'épaisseur des crêtes est égale à 1 pixel. Si on calcule le nombre de transitions de chaque pixel noir qu'on appelle poids, nous obtenons ainsi le nombre de traits partant de ce point, et nous pouvons donc déterminer le type de chaque pixel.

Algorithme de détection des caractéristiques des empreintes digitales :

- Localiser la surface sur laquelle va porter la détection.
- Calculer le poids de chaque pixel noir de l'empreinte squelettisée.
- Si poids=1 alors le pixel correspond à une fin de ligne
- Sinon Si p=3 et 45° <degré (Ai,Aj) ≤ 135 ° alors le pixel est une bifurcation.

4.3 Classification

La classification des empreintes digitale est réalisée à travers la combinaison de classifieurs de type perceptron multicouches (PMC). Afin de faciliter cette étape nous avons choisi de fractionner l'image du centre de l'empreinte, qui contient le plus grand nombre de caractéristiques en quatre parties, chaque partie sera assignée à un classifieur (PMC) comme le montre la figure suivante :

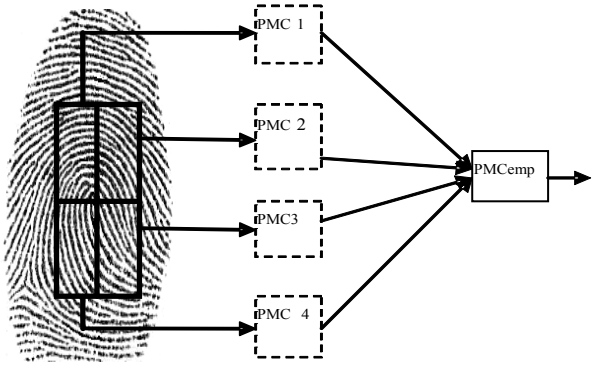

Figure 2 : Classification d'une empreinte digitale.

L'entrée de chaque classifieur PMC sera un vecteur de caractéristiques propre à la partition correspondante, mais comme le nombre de caractéristiques n'est pas connu à l'avance et n'est pas fixe pour chaque empreinte, nous allons le fixer à cinq caractéristiques par partition ce qui donne 20 caractéristiques pour toute l'empreinte. Des chercheurs affirment qu'il faut entre 10 et 20 caractéristiques extraites afin de pouvoir comparer deux empreintes digitales [9]. Chaque caractéristique aura trois attributs :

- Le type (fin de ligne ou bifurcation)
- La position(x,y).

Donc la taille du vecteur de caractéristique de chaque partition est égale à 15.

Les quatre sorties du PMC1, PMC2, PMC3, PMC4 seront combinées ensemble par un autre classifieur de type PMC (PMCemp) afin de fournir la sortie finale de classification de l'empreinte.

Entrée, un vecteur de caractéristiques d'une même taille ce qui justifie l'utilisation d'une architecture identique.

- Le nombre de couches cachées de chaque perceptron est égal à 1.
- Le nombre de neurones de la couche d'entrée correspond au nombre de composants du vecteur de caractéristiques qui est égal à 15.
- Le nombre de neurone de la couche de sortie est égal à 1.
- Le nombre de neurones de la couche cachée est calculé par la relation heuristique suivante :

$$Nbc = 2 \times \sqrt{Nbe + Nbs}$$

Avec :

Nbc est le nombre de neurone de la couche cachée.

Nbe est le nombre de neurone de la couche d'entrée.

Nbs est le nombre de neurone de la couche de sortie. Donc ***Nbc*** = 8 neurones.

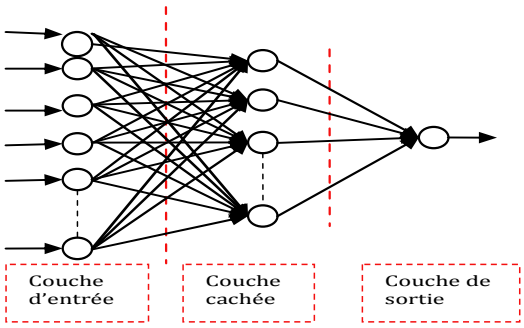

Figure 3 : Architecture du PMC1, PMC2, PMC3, PMC4 pour la vérification d'empreintes.

Pour le PMCemp, il est décrit comme suit (Voir Figure 4) :

- Le nombre de couches cachées est égal à 1.
- Le nombre de neurones de la couche d'entrée est égal au nombre de sorties des quatre PMCs, ce qui donne 4 neurones.
- Le nombre de neurones de la couche de sortie est égal à 1.
- Le nombre de neurones de la couche cachée est égal à 2.

Le processus de classification de l'empreinte est réalisé par les 2 phases : phase d'apprentissage et phase de vérification.

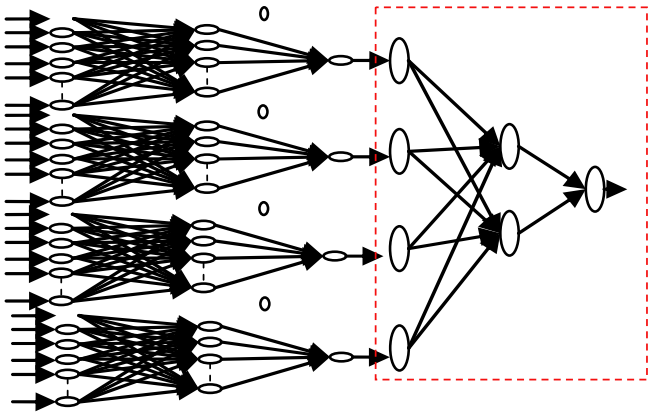

Figure 4 : Architecture du PMCemp pour la vérification d'empreintes.

4.3.1 Phase d'apprentissage des PMCs

Dans la phase d'apprentissage, tous les vecteurs de caractéristiques des l'empreintes d'une personne connue sont introduits aux perceptrons multicouches comme des données d'entrées. Le résultat d'apprentissage fournit les poids et les biais des réseaux correspondants à une image de l'empreinte de cette personne connue. A la fin ce vecteur des paramètres est stocké dans une base de références.

L'apprentissage des PMCs est réalisé à travers l'algorithme de rétropropagation (10).

4.3.2 Phase de vérification

Dans cette phase, une image de l'empreinte est entrée au sous système de vérification de l'empreinte avec l'identité de l'utilisateur. D'abord quatre vecteurs de caractéristiques sont extraits à partir de cette image. Ensuite, chaque vecteur est entré au réseau de neurones qui lui correspond. La classification s'effectue en utilisant la base de référence construite dans la phase d'apprentissage. Une seule classe est choisie.

5 LE SOUS SYSTÈME DE VÉRIFICATION DE LA SIGNATURE

5.1 Prétraitement

Les étapes de prétraitement de la signature sont identiques à celles des empreintes digitales, sauf que la squelettisation n'est pas appliquée pour extraire les caractéristiques globales.

5.2 Les caractéristiques liées à la signature

A la fin de cette étape, la signature ne sera plus représentée par une suite de points mais par deux vecteurs constitués

des valeurs de chacune des caractéristiques choisies. Notre étude des caractéristiques s'est portée sur deux types [11] : globale et locale.

5.2.1 Les caractéristiques globales

- Les deux dimensions de la signature : longueur, largeur.
- La valeur et la position du plus grand pic aussi bien de l'histogramme horizontal que vertical.
- La surface convexe.

5.2.2 Les caractéristiques locales

Pour les caractéristiques locales, nous avons retenu les deux caractéristiques suivantes :

- Le nombre des points d'intersection entre les traits de la signature
- Le nombre de zones closes.

Ce dernier paramètre s'est révélé un trait discriminant pour la signature. L'intérêt d'une telle caractéristique est de décrire la complexité du tracé de la signature. Ce paramètre peut être défini avec la formule suivante :

$$zcl = 1 + \frac{dp - fl}{2}$$

Où : ***zcl*** dénote le nombre de zone close, ***fl*** le nombre de points de fin de ligne, et ***dp*** est le nombre de points de départ supplémentaires calculé à l'aide de l'équation suivante :

$$dp = \sum_{\text{pts d'intersection}} \sum \left[(\text{nombre de 8 voisins}) - 2\right]$$

5.3 La classification

Chaque type de caractéristiques est assigné à un classifieur. Un PMC (PMCsig) pour les caractéristiques globales et, étant donné que le nombre de caractéristiques locales est égal à 2, nous avons utilisé comme classifieur utilisant ces caractéristiques, un perceptron simple avec deux neurones en entrée et un neurone en sortie. La combinaison de ces deux classifieurs est réalisée par un autre perceptron simple.

6 MODULE DE FUSION

Nous disposons, à ce niveau de deux scores, un score pour l'empreinte généré par le sous système propre à l'empreinte digitale, et le second représente le score de la signature, un classifieurs SVM est mis en place afin de fournir un seul score qui représente la fusion de ces deux derniers.

Dans notre cas, l'ensemble des données d'entrée sont représentées par un vecteur qui contient les scores des deux classifieurs.

SVM est un classifieur binaire qui ne traite que des données appartenant à deux classes. Cependant, il existe des versions plus élaborées prenant en compte plus de deux classes simultanément au sein de la même fonction objective. Comme notre système est un système de vérification, le SVM utilisé est un SVM binaire. Nous pouvons formuler notre problème comme suit :

Soit X= (xi) l'ensemble des données d'entrée du classifieur SVM étiquetées suivant Y = (yi) ∈ {-1,1} qui représente la classe de chaque vecteur d'entrée. La fonction de décision f avec :

$$f(x) = \text{sgn}(\sum (y_i \alpha_i \left[K(x)\right]_i, x) - b)$$

Elle indique la classe inférée par le SVM. Le choix de K est très important pour l'efficacité de la solution trouvée, parmi les fonctions noyaux qui existent nous avons opté pour la fonction linéaire K(x, y)=x.y qui, d'après [12] et [13], donne de très bons résultats pour la fusion des données.

7 MODULE DE DÉCISION

Ce module est une suite au module de fusion, selon la sortie du classifieur SVM la décision peut être prise.

Si la sortie est positive alors l'identité proclamée par l'individu est acceptée

Sinon si la sortie est négative **alors** l'identité annoncée est rejetée

8 RÉSULTATS ET DISCUSSION

Notre système a été réalisé sous l'environnement Visual Studio 2008 avec le langage de programmation C#.les expérimentations sont effectuées sur les deux modalités de manière séparée ensuite sur leur fusion, nous avons construit trois types de bases de données : Base 1, Base 2, et Base 3.

8.1 Base 1

La base des signatures, elle est extraite à partir de la base Signature Data Set [14].elle contient 10 signataires, pour chacun, nous utilisons 8 signatures authentiques et 3 fausses signatures, ce qui donne un total de 110 signatures pour la base 1. Cette base est partagée en deux, une base d'apprentissage (SA), et une base de tests(ST).

8.2 Base 2

Cette base est relative aux empreintes digitales. Nous avons utilisé une multi bases créée dans le cadre de FVC2006 (*the Fourth International Fingerprint Verification Competition*) **[**15**]**. Elle est constituée de 4 sous-bases de types différents, chacune d'entre elles a été constituée en utilisant un capteur/technologie différents, chaque sous-base contient 10 individus, chacun est représenté par 8 vraies empreintes

et 3 fausses empreintes. Ce qui donne un total de 110 empreintes pour chaque sous-base. La répartition des tailles de la base d'apprentissage ainsi que la base de tests est semblable à la base 1

8.3 Base 3

Vu l'indisponibilité de bases multimodales, nous avons construit une base fictive ou « chimérique » [13]. A partir des données de signatures et d'empreintes disponibles, nous avons conçu une base d'individus « chimères » en combinant des échantillons de signatures et empreintes d'individus en fait différents (d'où le terme chimères). L'objectif est de fusionner sur cette base de chimères, les deux systèmes unimodaux de vérification de l'identité et de comparer les performances du système multimodal avec celles des systèmes de vérification unimodaux. Nous avons partagé cette base en deux sous bases représentant 10 personnes BAF (base d'apprentissage de fusion) et BTF (base de test de fusion). BAF contient 4 données authentiques bimodales et 2 données imitées bimodales pour chaque personne. BTF contient 4 données authentiques bimodales et 1 donnée imitée bimodales.

Pour évaluer les performances de notre système, nous avons choisi d'utiliser les taux TFA (taux de fausse acceptation) et TFR (taux de faux rejet).

Les résultats de la fusion sont évalués sur la base BTF (base de tests de fusion).

Tableau 1: Comparaison des résultats

Taux / Modèle	TFA	TFR
Système Unimodal Empreinte digitale	10,47%	9,82%
Système Unimodal Signature	6,21%	15,75%
Système Multimodal Fusion par SVM	3,80%	3,55%

Les expérimentations effectuées sur la base d'individus chimères nous a permis de valider notre proposition et de confirmer l'hypothèse de la supériorité de la multibiométrie par rapport à la biométrie unimodale.

Ainsi, la fusion des deux modalités sur un même système par l'intégration des deux scores dans un autre module basé sur la classification par la méthode des SVM, a grandement amélioré la performance du système, les taux TFA et TFR du système basé sur l'empreinte digitale et la signature sont respectivement 10,47, 9,82 et 6,21, 15,75 le système final de fusion a ramené les taux TFA et TFR autour de 3%. Les résultats obtenus confirment que la multibiométrie permet d'obtenir de meilleurs résultats par rapport à l'unimodalité, surtout lorsqu'on utilise des modalités non corrélées comme c'est le cas de la signature et de l'empreinte digitale.

9 CONCLUSION

Dans notre travail, nous avons proposé une approche d'intégration de plusieurs modalités biométriques, tout en montrant l'apport de cette approche multibiomérique par rapport à l'unimodalité, par l'augmentation des performances des systèmes multibiométriques.

Deux types de biométries sont utilisés, la signature et l'empreinte digitale, chacune correspond à un système de reconnaissance à part entière. Des classifieurs neuronaux de type PMC sont utilisés et combinés au niveau des systèmes de reconnaissance dédiés à chacune de ces modalités. Notre approche de fusion se base sur l'utilisation des séparateurs à vastes marges (SVM).

Du point de vue des sources de d'informations en multibiométrie, selon la classification proposée par Ross et al. [3].le système proposé est multimodal puisqu'il intègre plus d'une modalité biométrique. Il peut aussi être qualifié d'hybride puisqu'il est aussi multi-classifieurs pour chaque modalité et multi-capteurs pour l'empreinte digitale.

Nous avons réalisé un système de vérification multibiométrique basé sur les deux modalités citées précédemment, en implémentant toutes les étapes du processus de reconnaissance : l'acquisition, le prétraitement, l'extraction des caractéristiques, la classification et enfin la décision.

Les résultats obtenus sont très satisfaisants, les taux de fausse acceptation (TFA) et de faux rejet (TFR) des systèmes unimodaux basés sur l'empreinte digitale et la signature sont respectivement 10,47, 9,82 et 6,21, 15,75. Le système complet de fusion ramène le TFA et TFR à 3,80 et 3,55. Cette amélioration significative confirme l'intérêt de combiner des modalités biométriques non corrélées.

BIBLIOGRAPHIE

[1] Jain A., Flynn P., Ross A.: «*Handbook of Multibiometrics*», Springer 2006.

[2] Ross A.: «*An introduction to multibiometrics*», Proceeding of 15th European Signal Processing Conference (EUSIPCO), Poland 2007.

[3] Ross A., Poh N.: «*Multibiometric Systems: Overview, Case Studies, and Open Issues*», apparu dans [16], Pages 273-292.

[4] Ross A., Jain A.:« *Information fusion in biometrics* », Pattern Recognition, Volume 24, Pages 2115–2125, 2003.

[5] Jain A., Nandakumar K., Ross A.: « *Score normalization in multimodal biometric systems*», Pattern Recognition, Volume 38, Pages 2270 – 2285, 2005.

[6] http://www.cl.cam.ac.uk/~jgd1000/combine/combine.html

[7] Kuncheva L. « *Combining Pattern Classifiers - Methods and Algorithms* », Wiley 2004.

[8] Maltoni D., Cappelli R. : « *Fingerprint Recognition* », apparu dans [17], Pages 23-42.

[9] Ratha N., Bolle R.: « *Automatic Fingerprint Recognition Systems* », Springer 2004.

[10] Chouinard S. : «*Réseaux de neurones artificiels*», Tutoriel, Université Laval, Colloque GRETSI, Troyes, Canada, 2007.

[11] Abroug Ben Abdelghani I., Elouaer L., Essoukri Ben Amara N. : «*Vérification de Signatures Manuscrites cas des Faux par Imitation*», Tutoriel, Université Laval, Colloque GRETSI, Troyes, Canada, 2007.

[12] Ben Yacoub S.: « *Multi-Modal Data Fusion for Person Authentification using SVM*», IDIAP Research Report 1998.

[13] Fuentes M., Mostefa D., Kharoubi J., Salicetti G., Dorizzi B., Chollet G. : «*Vérification de l'identité par fusion de données biométriques*», Colloque International Francophone sur l'Ecrit et le Document, CIFED 2002, Pages 315-324, Hammamet, Tunisie, 2002.

[14] http://www.cedar.buffalo.edu/NIJ/data/signature.rar

[15] http://bias.csr.unibo.it/fvc2006/

[16] Tistarelli M., Li S., Chellappa R.: «*Handbook of Remote Biometrics: for Surveillance and Security (Advances in Pattern Recognition)* », Springer 2009.

[17] Jain A., Flynn P., Ross A. « *Handbook of biometrics*», Springer 2008.