Vérification de Signatures Manuscrites : cas des Faux par Imitation

Imen Abroug Ben Abdelghani [1], Lilia Elouaer [2], Najoua Essoukri Ben Amara[3]

[1] Faculté des Sciences de Bizerte, Tunisie

abrougimen@yahoo.fr

[2] Institut Supérieur d'Informatique et de Mathématique de Monastir

L-elouaer@yahoo.fr

[3] Ecole Nationale d'Ingénieurs de Sousse, Tunisie

Najoua.Benamara@eniso.rnu.tn

Résumé – Dans ce papier nous nous intéressons au problème des faux par imitation dans un contexte de vérification hors ligne de la signature manuscrite. Ce type de faux constitue le cas le plus problématique lié à la vérification de la signature manuscrite hors-ligne. Notre étude a montré l'importance de la prise en compte aussi bien des caractéristiques globales que des détails de la forme de la signature. Nous proposons pour cela une approche de caractérisation efficace qui a conduit des résultats encouragents.

Abstract – In this paper we focuses on the problem of the skilled forgeries within the framework of the handwritten signature verification. This type of forgery still the most problematic case related to the signature verification systems. Our study showed the importance of the consideration as well global characteristics as details of the shape of the signature. We propose for it an approach of effective characterization which led encouragents results.

1. Introduction

Durant ces deux dernières décennies, il y a eu plusieurs développements dans le domaine de vérification des signatures manuscrites [3, 6, 7]. Toutefois, le problème des imitations reste toujours ouvert. En effet, afin de décider de l'authenticité d'une signature, les services judiciaires, ainsi que les banques font toujours appel à l'expertise humaine, d'où le besoin de développer un système objectif capable d'identifier les signatures falsifiées [5, 8]. C'est dans ce cadre que s'insère notre travail. En effet, le contrôle des falsifications par un système hors ligne possède un rôle important dans différents domaines d'applications tels que la médecine (les prescriptions, les rapports médicaux...), le commerce (chèques bancaires, contrats...), les domaines politique et juridique…

La littérature montre que pour l'être humain, la différentiation entre les signatures authentiques et leurs faux simples ou aléatoires est une tâche relativement aisée. En effet, un simple coup d'œil permet de juger de l'authenticité d'un faux aléatoire ou encore d'un faux simple puisque ce type de faux présente une nette dissemblance morphologique par rapport à la signature authentique. Cependant, la tâche n'est pas triviale dans le cas des faux par imitation notamment après une phase préalable d'apprentissage [4].

Dans ce travail, nous proposons une approche de caractérisation et de vérification appropriée aux faux par imitation.

2. Etude des faux par imitation

Nous avons mené une étude morphologique d'un grand nombre de faux par imitation. Cette étude a relevé l'existence d'une très forte corrélation entre les faux par imitation et la signature authentique correspondante. Cependant, nous avons également noté quelques différences qui ne sont pas facilement perceptibles à l'œil nu.

Dans la figure 1, sur l'exemple d'une signature authentique et trois imitations provenant de trois faussaires différents, nous remarquons les différenciations suivantes :

- La négligence des détails : le nombre de zones closes, l'intersection entre les traits (b)
- La négligence de l'aspect global : la taille, la forme convexe et l'orientation globale (c)

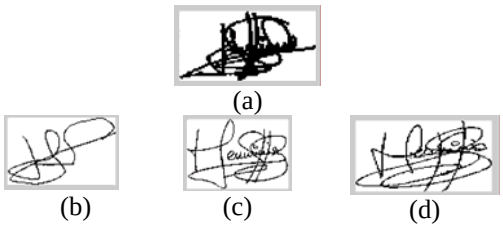

FIG. 1 : Une signature authentique (a) avec des échantillons imités (b, c et d) extraits à partir de la base de test.

La figure 2 présente quatre échantillons authentiques et leur signature imitée.

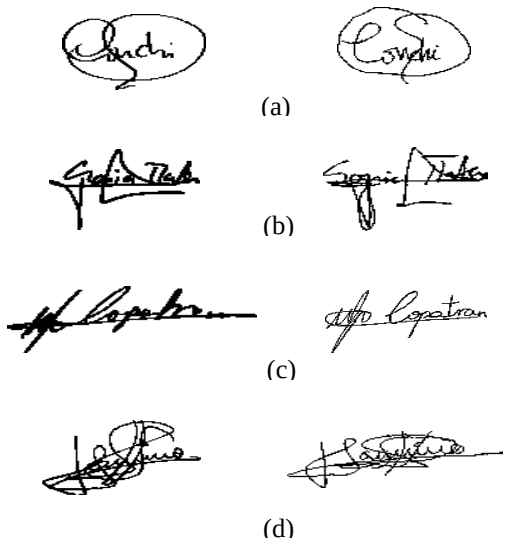

FIG. 2 : Quatre échantillons de signatures authentiques (à gauche) avec leurs imitations (à droite).

L'étude des échantillons de la figure 2 montre des variations aux niveaux de :

-La présence de l'hésitation à travers les lignes sinueuses (a)

- L'ajout des retouches (b)
- La pression est différente (c)
- L'exagération des arrondissements (d)

La figure 3 présente deux exemples de superposition d'une signature imitée (image de premier plan) sur une signature authentique (image de fond).

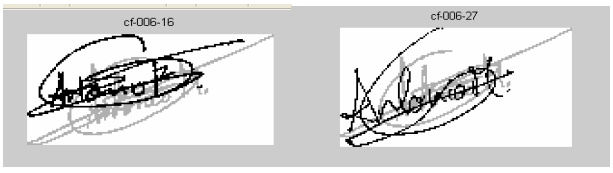

FIG. 3 : Différences en forme ou en sémantique entre signatures imitées et authentiques.

Il est clair d'après cet exemple que nous distinguons entre deux styles d'imitations : la reproduction de la forme en dépit de la sémantique (a) et la reproduction de la sémantique en dépit de la forme (b).

3. Approche développée

Comme dans tout système de reconnaissance de formes, nous passons principalement par trois étapes : les prétraitements, la caractérisation et la classification. Dans ce qui suit nous détaillons chacune de ces étapes.

3.1 Prétraitements

Etant donné que la base utilisée est déjà traitée de point de vue qualité de l'image et réduction de bruit (cf § 4.1), les phases de réduction de bruit et lissage se sont avérées inutiles. Seule la question de la normalisation reste posée. Nous avons fait le choix d'opérer uniquement une normalisation de la taille. Dans ce but, nous avons établi une taille fixe de 53x115 pixels pour tous les échantillons de la base. La figure 4 donne quelques résultats de la normalisation de la taille.

FIG. 4 : Deux échantillons de signatures avant (à gauche) et après (à droite) normalisation de la taille.

3.2 Caractérisation des faux par imitation

Tenant compte des résultats de notre étude, nous avons retenu le jeu des caractéristiques suivant :

- Les deux dimensions de la signature
- Les enveloppes supérieures et inférieures : le nombre de pics ainsi que la valeur et la position du plus grand pic.
- Le nombre de pics ainsi que la valeur et la position du plus grand pic aussi bien de l'histogramme horizontal que vertical.
- La surface convexe
- La rectangularité de la forme de la signature
- L'arrondissement de la forme de la signature

Le choix de ces caractéristiques permet de tenir compte de l'aspect global de la signature, pour les détails, nous avons retenu les deux caractéristiques suivantes :

- Le nombre des points d'intersection entre les traits de la signature
- Le nombre de zones closes (figure 5).

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 :

$$ZCL = 1 + \frac{DL - FL}{2} \quad (1)$$

où FL dénote le nombre de points de fin de ligne, DL le nombre des départs supplémentaires calculé à l'aide de l'équation (2), d'après [3] :

$$DL = \sum_{point\ d'intersections} \left[\left(Nbre\ de\ 8\ voisins \right) - 2 \right] \quad (2)$$

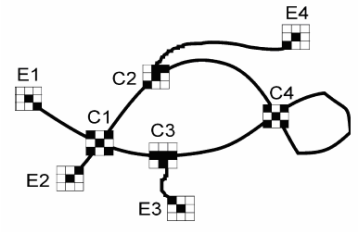

FIG. 5 : Echantillons de points caractéristiques,
E : les points de fin de ligne, C: les points d'intersection,
d'après [3].

3.3 Classification

Dans cette étape nous avons appliqué les réseaux de neurones de type perceptrons multicouches (PMC). D'après nos travaux précédents [1,2], le choix d'une architecture neuronale modulaire (par signataire) a montré des performances meilleures qu'une architecture globale. Un réseau PMC pour chaque signataire a été alors défini.

L'apprentissage des différents réseaux a été effectué moyennant un algorithme avec rétro propagation de l'erreur. Chaque réseau de neurones apprend les primitives du signataire considéré et des autres signataires, le nombre d'échantillons d'apprentissage (vrais et faux) a été choisi de façon équitable. Les échantillons utilisés pour la phase de test des réseaux de neurones sont autres que ceux utilisés pendant l'apprentissage (cf § 4.1).

L'architecture de chacun des réseaux est formée par trois couches : la première couche correspond au vecteur d'entrée, la couche de sortie contient un seul neurone désignant la décision. Plusieurs expériences ont été effectuées pour déterminer le nombre de couches cachées et le nombre de neurones par couche cachée. Ce nombre varie selon le signataire.

Pour la décision, nous avons opté pour l'utilisation d'une approche particulière permettant de raffiner la phase de classification pour chaque classe de signatures. Pour cela, deux étages de classifieurs distincts ont été utilisés. Chaque étage comporte un classifieur qui diffère de l'autre des points de vue primitives d'entrées et but.

Le premier classifieur rend compte de la forme globale des signatures, il est donc alimenté par les caractéristiques globales extraites des différentes signatures. De ce fait, son rôle est d'identifier autant que possible les faux aléatoires. A ce niveau, notre objectif est de minimiser le taux correspondant.

Le deuxième classifieur considère les caractéristiques relatives aux détails. Une précision accrue est alors exigée dans la classification particulièrement des signatures imitées (Figure 6).

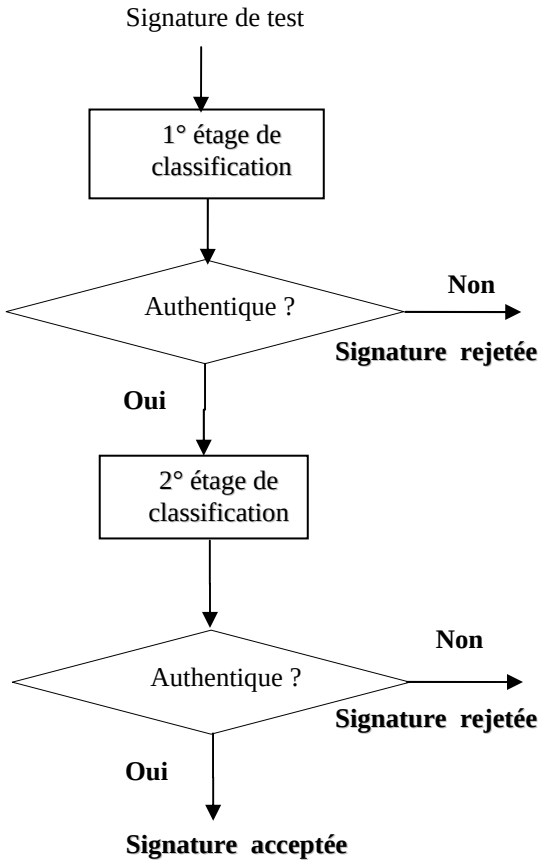

FIG. 6 : Organigramme de la phase de classification.

4. Expérimentations et résultats

Dans cette section, nous définissons d'abord notre base de données ensuite nous donnons les principaux résultats enregistrés.

4.1 Base de données

Dans notre cas, nous avons testé notre système sur les deux bases de l'Université de Las Palmas de Gran Canaria en Espagne [7]. La première base (Base-1) a été collectée avec la collaboration de 39 individus (classes) alors que la deuxième (Base-2) correspond à 160 individus. Chaque individu a donné 24 échantillons authentiques auxquels se sont ajoutés 30 faux par imitation (Tableau 1). Les

imitations en question ont été produites à partir de l'image statique des signatures originales. Chaque faussaire a eu la possibilité de prendre le temps nécessaire pour produire la signature falsifiée. Ainsi, à chaque individu correspondent 30 signatures imitées faites par 10 faussaires différents.

TAB. 1 : Composition des deux bases de données utilisées.

	Nombre de classes	Signatures authentiques par classe	Signatures imitées par classe	Total
Base-1	39	24	30	2106
Base-2	160	24	30	8640

Etant donné les besoins de notre application, en apprentissage puis en test, nous avons réparti notre base de la manière suivante : la phase d'apprentissage est effectuée à l'aide de 15 échantillons authentiques de la classe concernée et de 15 échantillons authentiques choisis aléatoirement du reste de la base (les autres classes de signatures). Quand à la phase de test, nous avons utilisé les 30 faux imités de la classe concernée et 9 faux aléatoires de chaque classe de la base autre que la classe concernée. Le tableau 2 présente la répartition des données en apprentissage et test pour une classe de signatures donnée.

TAB. 2 : Répartition des données en apprentissage et test pour une classe de signatures donnée.

	Apprentissage		Test	
	Authentiques	Aléatoires	Imitées	Aléatoires
Base-1	15	15	30	9 x 38
Base-2	15	15	30	9 x 159

4.2 Résultats enregistrés

Pour évaluer l'approche développée nous avons utilisé comme taux d'erreur le taux de faux acceptés (TFA) qui représente le pourcentage de faux échantillons qui ont étés acceptés (classés comme authentiques).

Le niveau de sécurité de l'application peut être ajusté selon le seuil de décision utilisé. Ce dernier varie entre 0 et 1. Pour une valeur proche de 1, on parle d'un haut niveau de sécurité, une valeur autour de 0.5 correspond à un niveau moyen de sécurité et une valeur proche de 0 correspond à une faible sécurité.

Le tableau 3 résume les résultats que nous avons enregistrés.

TAB. 3 : Les résultats enregistrés, seuil de décision = 0.9.

	TFA %	
	Aléatoires	Imitées
Base-1	0.44	0.94
Base-2	2.30	17.40

5. Conclusion

Dans ce travail, nous avons présenté une approche de vérification de signatures manuscrites hors ligne. Nous avons traité en particulier le cas des faux par imitation qui reste toujours un problème ouvert. Dans ce but, nous avons effectué une étude morphologique d'un grand nombre de signatures ainsi que leurs imitations. Cette étude nous a permis d'extraire un ensemble de caractéristiques mettant en relief à la fois l'aspect global et les détails de la signature. Nous avons utilisé une architecture de classification à deux étages basée sur les réseaux de neurones de type PMC pour chaque classe de signatures. L'approche proposée a été expérimentée sur deux bases de tailles différentes. Les résultats que nous avons enregistrés sont encourageants.

Références

[1] I. Abroug Ben Abdelghani, N. Essoukri Ben Amara, « Deux Approches Neuronales pour la Vérification Hors-ligne de la Signature Manuscrite », A paraître dans les actes du 15ème Congrès Francophone Reconnaissance des Formes et Intelligence Artificielle,(RFIA'06), Tours,France, 25-27 Janvier 2006. Imen : Vérifies l'intitulé du congrès.

[2] I.Abroug, « Vérification Hors Ligne de la Signature Manuscrite », Mémoire de Mastère, Ecole Nationale d'Ingénieurs de Tunis, Tunise-Juillet 2004.

[3] H. Baltzakis, N. Papamarkos, «A new signature verification technique based on a two-stage neural network classifier», Engineering Applications of Artificial Intelligence 14, pp. 95-103, 2001.

[4] M. El Yassa, D. Mammass, A. Chalifour & F. Nouboud, «Etat de l'art sur la vérification Off-line de signatures manuscrites», Conf. Inter. :Sciences, Electroniques, Technologie de l'Information et des Télécommunications, Sousse (Tunisie) 17_21 Mars 2003.

[5] M.C. Fairhurst, «Document Identity, Authentication and Ownership: The Future of Biometric Verification», Proceeding of the Seventh International Conference on Document Analysis and Recognition, (ICDAR 03), 2003.

[6] J. Fierrez-Aguilar, N. Alonso-Hermire, G. Mereno-Marquez and J.Ortega-Garcia, «An Off-Line Signature Verification System based on fusion of local and global information», BioAW 2004, LNCS 3087, Berlin Heidelberg, pp.295-306, 2004.

[7] L. Martinez, C.M. Travieso, J.B Alonso, M.A. Ferrer, «Parameterization of a forgery handwritten signature verification system using SVM», Proceedings of the IEEE 38th annual 2004 International Carnahan Conference on Security Technology, Albuquerque, New Mexico, p. 193-196, October 2004.

[8] R. Plamondon and S.N. Srihari « On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey», IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 22, no. 1, January 2000.