Efficient online signature authentication approach

Saidani Kaouther,[a] Mostefai Messaoud,[a,*] Bouziane Abderraouf,[a,b] and Chahir Youssef[b]
[a]University of Bordj Bou Arreridj, MSE Laboratory, BP 64, El Anasser, 34030, Algeria
[b]University of Caen, GREYC Laboratory, CNRS UMR 6072, 14032, France

Abstract. Signature authentication systems often have to focus their processing on acquired dynamic and/or static signatures descriptors to authenticate persons. This approach gives satisfactory results in ordinary cases but remains vulnerable against skilled forgeries. This is mainly because there is no relation between the signatory and his signature. We will show that the inclusion of the hand shape in the authentication process will considerably reduce the false acceptance rates of skilled forgeries and improve the authentication accuracy performances. A new online hand signature authentication approach based on both signature and hand shape descriptor is proposed. The signature acquisition is completely transparent, which allows a high level of security against fraudulent imitation attempts. Authentication performances are evaluated with extensive experiments. The obtained test results [equal error rate (EER) = 2%, genuine acceptance rate (GAR) = 96%] confirm the efficiency of the proposed approach. *© 2014 SPIE and IS&T* [DOI: 10.1117/1.JEI.23.6.063009]

Keywords: online signature authentication; skilled forgeries; hand geometry; scores matching.

Paper 14148 received Mar. 26, 2014; accepted for publication Oct. 24, 2014; published online Nov. 21, 2014.

1 Introduction

Skilled forgeries pose a real problem to the majority of existing signature authentication systems. This limits the use of this modality in case of applications with high level security requirements (military, banks and sensible areas, and so on). In spite of that, this nonconstraining modality remains very much used by a great number of multimodal biometric authentication systems.[1,2]

Several works based on signature and on another modality have been proposed for the construction of efficient bimodal authentication systems (signature and speech, signature and face, signature and iris, and so on). Humm et al.[3] have developed a bimodal authentication system using both signature and speech modalities. The proposed approach was based on two scenarios: in the first one, a bimodal signature and voice information are acquired. The user was asked to speak the content of his signature. However, in the second scenario, the user was asked to write and read synchronously the content of a given text.

In another study, Elmir et al.[4] have combined signature and face modalities. The proposed system is based on fusion at the score level of the face and signature traits of a user. Used scores were obtained from two verification systems; the first system was based on face verification using a combination of Gabor filter for feature extraction and support vector machine for classification. The second system was based on online signature verification using Nalwa's method.[5] Several strategies have been used to fuse face and online signature scores such as simple sum, minimum, and maximum scores.

Almayyan et al.[6] have presented a multimodal biometric authentication system based on a new feature level fusion scheme of signature and iris features. The last were extracted separately and concatenated to form a fused feature vector. A binary particle swarm optimization approach was used to reduce the dimension of the features' vector while keeping the same level of performance.

Although these combinations enhance security and accuracy, the complexity of the proposed methods increases with the increased number of extracted features and the number of used sensors.

In this work, we describe a bimodal authentication system which simultaneously uses the signature and the hand shape for the authentication of any person. The proposed approach allowed us to obtain the best compromise between efficiency [equal error rate (EER) = 2]and simplicity (only one sensor is required).

This paper is organized as follows: in Sec. 2, we briefly present the developed acquisition system. In Sec. 3, we present the limits of the well-used dynamic time warping (DTW) authentication method against skilled forgeries. In Sec. 4, we show the importance of including the hand shape descriptor to overcome these limitations and to improve authentication accuracy. The performances of the proposed heuristic approach are evaluated with extensive experiments. Finally, Sec. 5 concludes the paper.

2 Acquisition System

A laboratory prototype[7] has been developed for this purpose (Fig. 1). It is composed of a high resolution camera placed in front of a transparent signing glass. Signers perform signatures by moving their pen on the glass. Acquired movements are used to generate the correspondent signature features $[x(t), y(t), (x, y)]$. To reduce the effects of lighting variations, the signing plan is protected by an opaque lid. Examples of acquired successive frames during a signing process are presented in Fig. 2.

Figure 3 presents some reconstructed signatures obtained with our acquisition system. In the case of continuous signatures, offline [Figs. 3(a) and 3(e)] and online [Figs. 3(b) and 3(f)] signatures are identical. However, any pen up in

*Address all correspondence to: Mostefai Messaoud, E-mail: bbamostefai@yahoo.fr

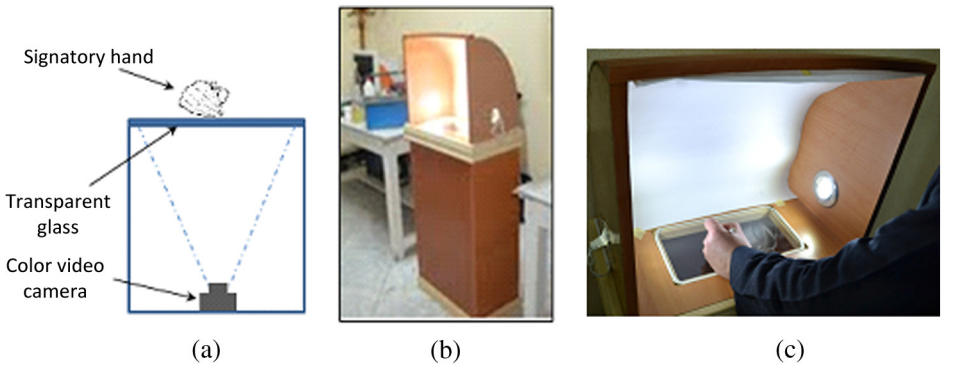

Fig. 1 Used online signature acquisition system: (a) global view, (b) laboratory prototype, and (c) signing operation view.

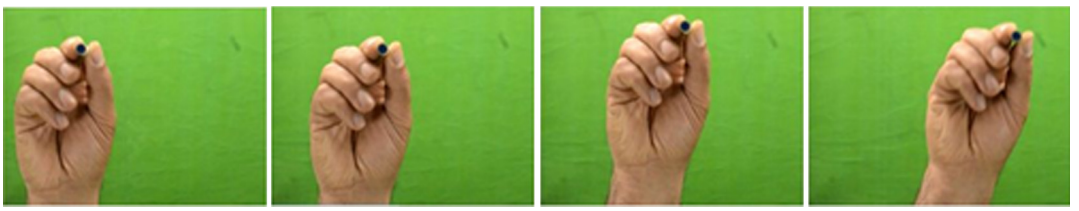

Fig. 2 Acquired successive frames during a signing process.

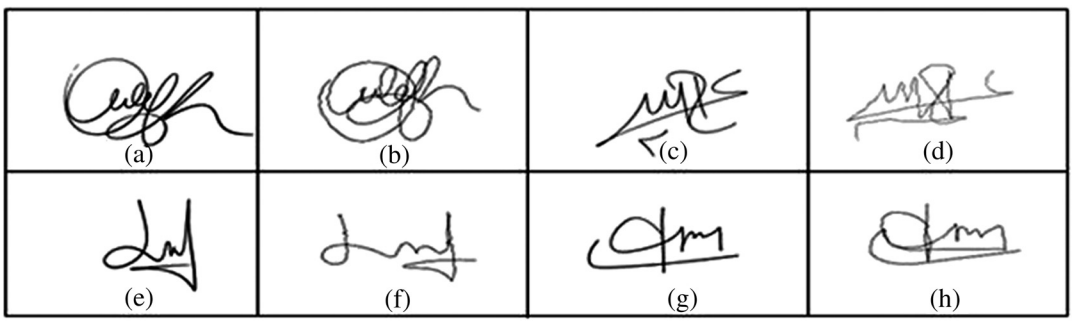

Fig. 3 Comparison between offline [(a), (c), (e), (g)] and online [(b), (d), (f), (h)] signatures.

offline mode [Figs. 3(c) and 3(g)] will be considered as a continuous curve in online mode [Figs. 3(d) and 3(h)]. This complementary dynamic information will allow a precise signature analysis and will make difficult any intentional imitation attempt.

3 Signature Authentication

A wide range of techniques have been developed to perform offline or online signature authentication tasks.[8] All of them seek to find the best representative features in order to perform an efficient similarity measure between enrolled and test signatures. For a first approach, the well-known DTW[9] has been used to perform a signature authentication task. The objective is not to evaluate its performances in ordinary cases but rather to show its limits in the case of skilled forgeries.

3.1 *Test Database Construction*

The test database was filled with the signatures of 100 participants: 60 men and 40 women. Each participant was asked to perform 10 genuine signatures, 3 for the generation of the reference signature and 7 for tests. After a time of training, each contributor agreed to perform 5 random forgeries and 5 skilled ones. A total of 700 genuine signatures with 500 random forgeries and 500 skilled forgeries were collected for authentication test purposes. Users' hand shapes were also recorded at the beginning of the signing process. There are 3 acquisitions for the generation of the reference hand and 7 for tests which were paired with signature data for testing.

3.2 *Preliminary Authentication Tests*

The authentication performance is generally evaluated by drawing the receiver operating characteristic (ROC) curve as well as the evolutions of false acceptance rate (FAR) and false rejection rate (FRR) at different threshold values. The obtained authentication results allowed us to establish the corresponding ROC and FRR–FAR curves as can be seen in Figs. 4 and 5 and Table 1. One can see that the DTW gives acceptable results in the case of genuine signatures. However, the inclusion of forgeries considerably decreases the authentication accuracy.

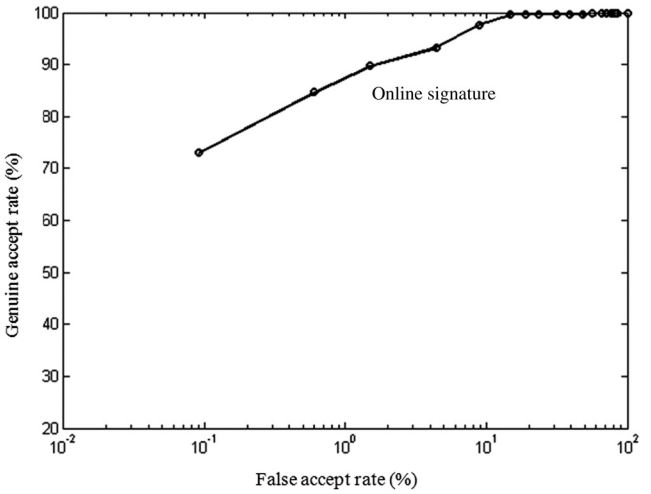

Fig. 4 ROC curve showing the performance of online signature modality.

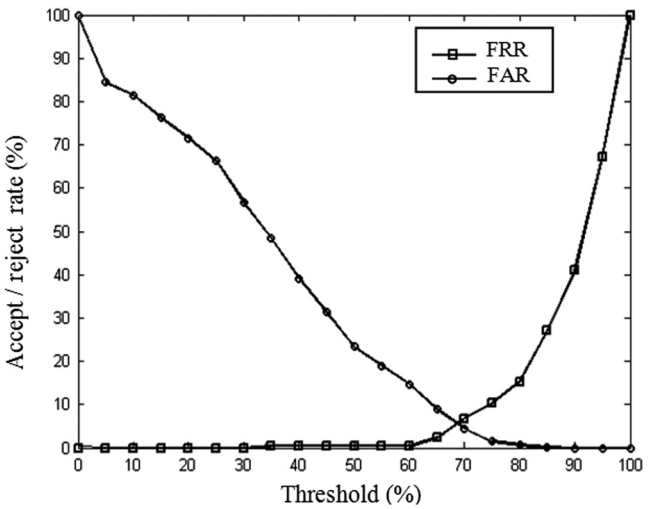

Fig. 5 False rejection and acceptance rates against the threshold of online signature modality.

Table 1 Authentication test results for the signature modality.

Threshold	Genuine acceptance rate (GAR) (%)	False acceptance rate (FAR) (%)
33	100	56.8
40	99.6	39.1
55	99.6	18.9
65	97.7	8.9
80	84.7	0.6
85	73	0.09
88	58.9	0.00

3.3 *General Report*

Usually, authentication systems focus their processing on acquired dynamic and/or static signatures features. This approach gives satisfactory results in ordinary cases but remains vulnerable against skilled forgeries. This is due to the fact that there is no relation between the signatory and his/her signature. In what follows, we will show that the inclusion of the hand shape in the authentication process will considerably reduce skilled forgeries FARs and improve the signature authentication performances.

4 Authentication Accuracy Improvement

4.1 *Signing Hand Shape*

Several interesting works have used hand shape in their authentication schemes.[10,11] The latter exploit captured images of the top view and the side view of the hand to compute the width of the fingers at various locations, width and thickness of the palm, length of the fingers, and so on.

To the best of our knowledge, there is no work which exploited the bottom view of the signing hand shape to improve the performances of any signature authentication scheme. The challenge here is to show that this information could be exploited efficiently to reduce skilled forgeries FARs.

By re-examining the acquired video frames, we noted that it is possible to extract at the beginning of the signing process a discriminative hand shape descriptor able to characterize the signatory hand. Indeed, on the basis of the principle that a person has the same habits regarding his/her initial signing hand pose, one can extract and exploit a dedicated hand shape descriptor in order to verify if the signing hand is similar to that of the enrolled person or not.

4.2 *Hand Shape Descriptor Extraction*

Because of the closed signing hand state, the well-used distance metrics described in Ref. 11 are not suitable for our case. Thus, several tests based on hand surface, perimeter, width, and height have been performed to find the best discriminative hand shape descriptor. Only hand widths gave us good results. An example of two acquired hands with their corresponding hand shape widths is presented in Fig. 6. For each hand, a set of nine distances are extracted and used to compute the hands' similarity. For a better precision, one can take more than nine hand shape widths (for example 17 or 21 values).

Consider two signing hands Hand_X and Hand_Y with their corresponding nine hand widths:

$$\mathrm{Hand}_X(d_{X0}, d_{X1}, d_{X2}, d_{X3}, d_{X4}, d_{X5}, d_{X6}, d_{X7}, d_{X8})$$
$$\mathrm{Hand}_Y(d_{Y0}, d_{Y1}, d_{Y2}, d_{Y3}, d_{Y4}, d_{Y5}, d_{Y6}, d_{Y7}, d_{Y8}).$$

The percentage of similarity $S(X, Y)$ between the two signing hands is obtained as follows:

First, a difference vector composed of the nine differences couples is computed with

$$V_{\mathrm{Diff}(x,y)} = \{|d_{X0} - d_{Y0}|, |d_{X1} - d_{Y1}|, \ldots, |d_{X8} - d_{Y8}|\}. \quad (1)$$

The obtained values are compared with a predefined threshold T and fixed to "zero" if the difference is inferior

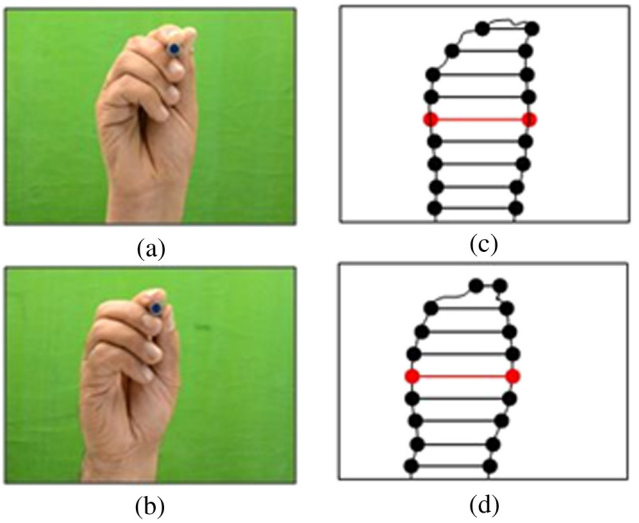

Fig. 6 Signatory hand distances: (a) and (b) two signing hands, (c) and (d) corresponding hand's widths.

to T or "one" if not. The similarity measure is then computed as follows:

$$S(X,Y) = \left(\frac{\text{Nbr of zero values}}{9}\right) \times 100. \quad (2)$$

An example of an obtained quantized difference vector is: $V_{Q\text{Diff}(x,y)} = \{1,1,0,0,0,0,1,0,0\}$

The computed similarity is equal to $(6/9) \times 100 = 67\%$

Note that the value of T is empirically fixed according to the required level of security. In the experiments, the value of

Fig. 7 Volunteers signing hands.

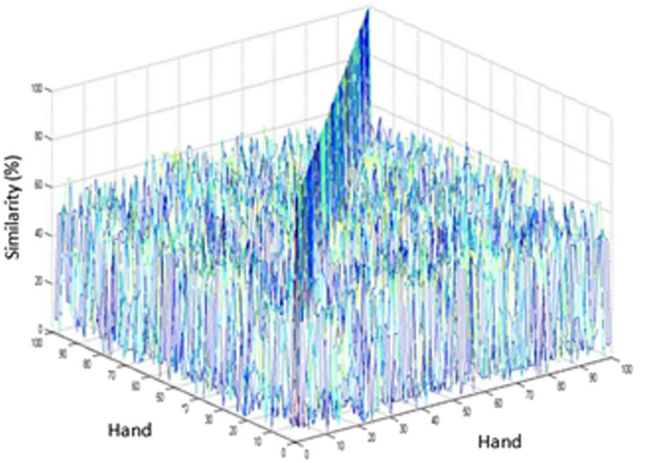

Fig. 8 Computed hand similarity scores.

T is fixed to 10. Figures 7 and 8 present, respectively, examples of some contributors' signing hands as well as their computed hand similarity scores. One can see that the probability of having similar hands is low. Therefore, it is possible to exploit this information to reduce the number of accepted forgeries.

Figures 9 and 10 and Table 2 show the performance of the authentication based on hand shape modality. The obtained results confirm the efficiency of this modality for authentication.

4.3 *Matching Score Level Fusion*

In our case, any enrolled person is automatically identified by his/her reference signature and his/her hand shape vector (Table 3).

The authentication process consists of fusing the signature and hand shape authentication scores. Thus, no good imitation will automatically mislead the signature verification system, unless the imitator's hand is similar to the enlisted person's hand. A decision tree[12] is applied to the obtained scores with signature and hand shape modalities.

The processing is performed in two steps (Fig. 11). In the first step, signature authentication scores are compared to a

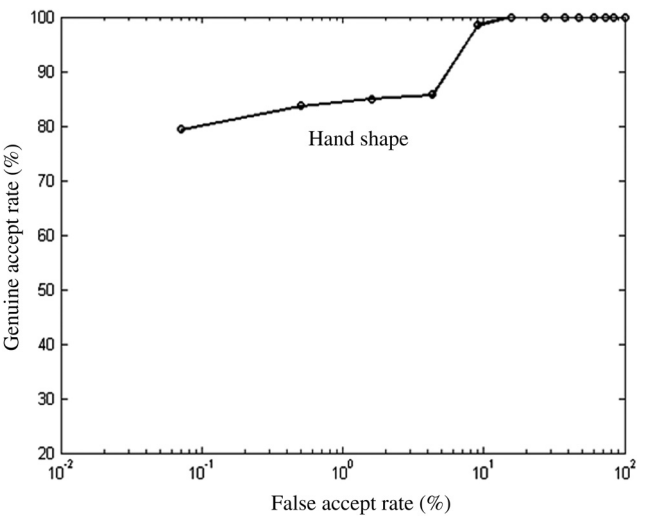

Fig. 9 ROC curve showing the performance of hand shape modality.

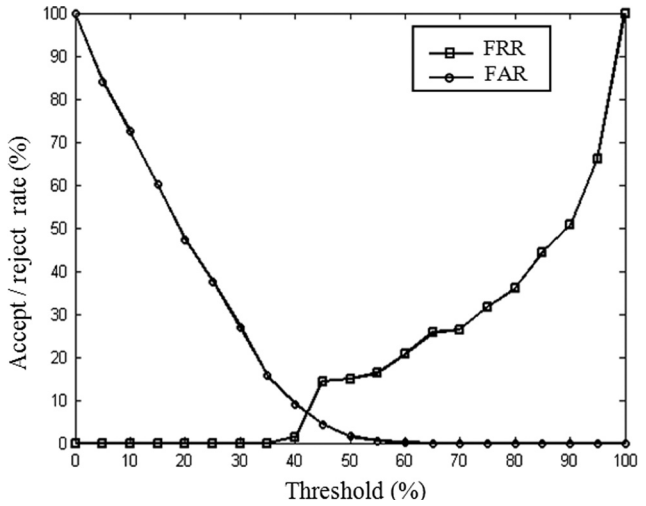

Fig. 10 False rejection and acceptance rates against threshold of hand shape modality.

Table 2 Authentication test results for the hand shape modality.

Threshold	GAR (%)	FAR (%)
35	100	15.6
40	98.6	9.00
45	85.7	4.30
50	85	1.60
56	83.7	0.50
60	79.4	0.07
63	74.3	0.00

Table 3 Associated enrolled person's database structure.

Enrolled person	Reference signature	Hand shape vector
P_0	Ref_0	$\{d_{00}, d_{01}, \ldots, d_{08}\}$
P_1	Ref_1	$\{d_{10}, d_{11}, \ldots, d_{18}\}$
…	…	…
…	…	…
…	…	…
P_n	Ref_n	$\{d_{n0}, d_{n1}, \ldots, d_{n8}\}$

fixed threshold (T_1). Those with scores higher than T_1 are retained for the second-processing step, while the rest are considered as forgeries and are rejected. The second step consists of comparing the corresponding hand scores results of the retained signatures to a fixed threshold (T_2). If any hand score result is higher than T_2, then the corresponding

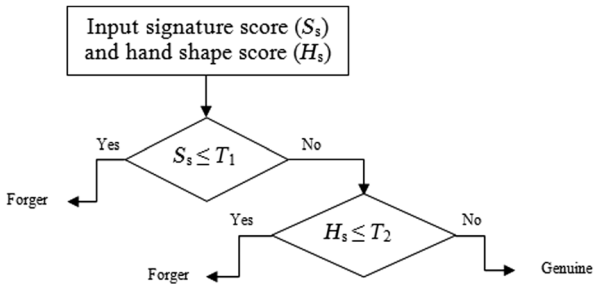

Fig. 11 Adopted decision tree.

signature is declared as a genuine signature, otherwise it is declared as a forgery.

The obtained results presented in Figs. 12 and 13 and Table 4 show that the inclusion of the hand shape descriptor allows a considerable improvement in the authentication performances.

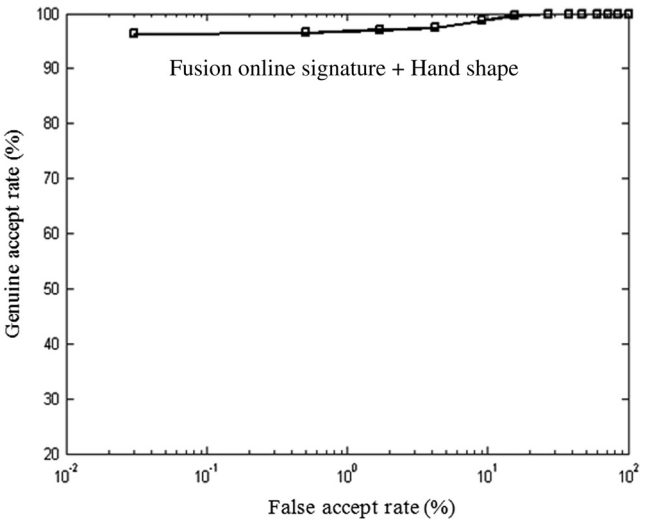

Fig. 12 ROC curve showing an improvement in performance by combining signature and hand shape modalities.

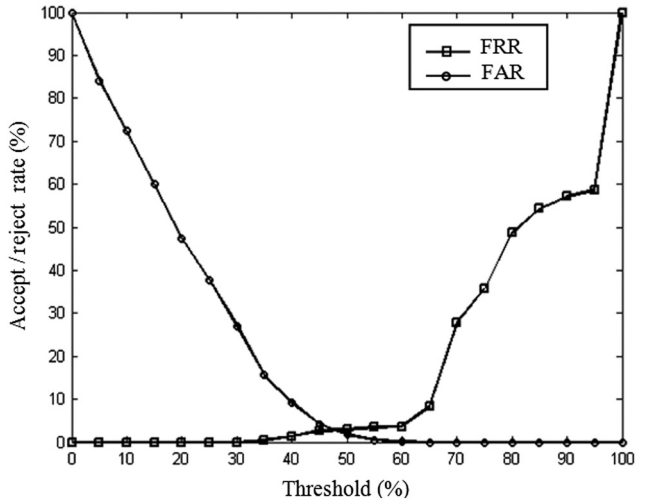

Fig. 13 False rejection and acceptance rates against threshold of combined signature and hand shape modalities.

Table 4 Authentication test results for the combined signature and hand shape modalities.

Threshold	GAR (%)	FAR (%)
30	100	27
35	99.7	15.6
50	97.1	1.70
55	96.6	0.50
60	96.4	0.03
65	91.7	0.00
88	58.9	0.00

4.4 *Advantages of the Proposed Hand Shape Descriptor*

4.4.1 *Detection of signatory habit changes*

The proposed hand shape descriptor allows the system to distinguish between the signatories hands on one hand, and on the other hand, to detect any changes in signatory habits. Indeed, a signatory generally keeps the same disposition of his/her hand and the manner of holding the pen when signing.

Therefore, any change in the signatory habits will automatically decrease the degree of similarity between the tested and enrolled hand. The following example (Fig. 14) shows different hand dispositions of the same person at the beginning of a signing process: Figure 14(a) represents the enrolled hand; Figs. 14(b)–14(d) are the test hands. Reported hand similarity scores (H_S) show that if the signatory hand disposition changes, the degree of similarity decreases.

As a consequence, a declared authentic signature can be thus regarded as false simply because the signatory has changed the manner of signing. This interesting feature is beneficial for the authentication because it adds to the handwriting habits, which are concretized by the produced signature, a complementary and selective hand disposition habit. In other words, any person is declared authentic only if she/he performs the same signing habit with the same hand disposition habit, otherwise she/he is declared as a forger.

4.4.2 *Efficient forgery detection*

Another interesting feature concerns the dissimilarity score obtained by the developed descriptor in the case where the forger and the genuine signer are persons from different sexes. As the latter present generally different hand morphologies, the probability to have a man's hand similar to that of a woman's hand is very weak. In fact, the probability of accepting the imitation, even if perfect, will be also very weak. In order to check that, we gathered the imitations carried out by a group of 20 men on the signatures of 20 women and vice-versa. The full number of imitations is 2000 ($20 \times 10 \times 10$) for each sex.

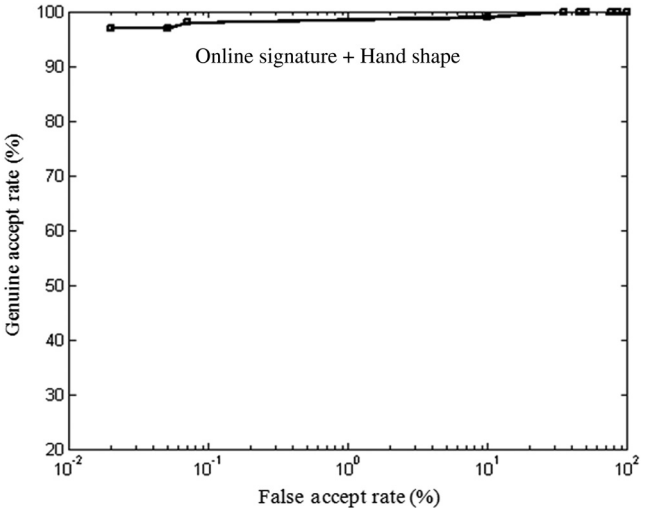

Fig. 15 ROC curve showing an improvement in performance by combining signature and hand shape modalities.

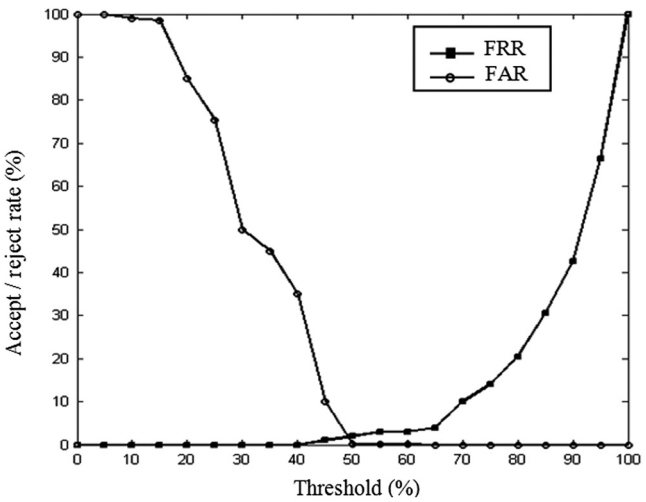

Fig. 16 False rejection and acceptance rates against threshold of combined signature and hand shape modalities.

Fig. 14 Example of hand similarity scores (H_S) between an enrolled hand and a test hand: (a) reference hand, (b) Hs = 100%, (c) Hs = 80%, (d) Hs = 66%.

The experimental results, presented in Figs. 15 and 16 and Table 5, show that the exploitation of such a descriptor in a signature authentication scheme will significantly limit the fraudulent imitation attempts, for example, by breach of trust between couples and also between colleagues or close or remote members of the same family. The best results were obtained with a threshold fixed to 64 [genuine acceptance rate $(\mathrm{GAR}) = 96\%$ and $\mathrm{FAR} = 0$].

4.4.3 *Computation complexity*

The complexity of the proposed method is due to the computation of the difference vector (1) and the percentage of similarity (2). These values are computed by simple mathematical operations. Let us consider the case where the size of the difference vector is equal to nine. The computation of (1) and (2) requires 9 subtractions, one division and one multiplication.

We implemented and tested our hand shape authentication method in MATLAB R2012 on a PC Dual Core 2.10 GHz, 2-GB RAM. The computational complexity is evaluated by measuring the speed of processing for different hand shape descriptor's sizes. The obtained results are summarized in Table 6.

Because of its simplicity, the proposed hand shape descriptor is well suited for hardware implementation. Actually, a hardware module composed of simple hand pixels and lines counters with few registers and a small size memory is under development within an field programmable gate array circuit for a real-time hand shape features' extraction and authentication.

Table 5 Authentication test results for the combined signature and hand shape modalities.

Threshold	GAR (%)	FAR (%)
41	100	35
46	99	10
51	98	0.07
56	97	0.05
60	97	0.02
63	96	0.00

Table 6 The computational timing for processing.

Hand shape descriptor size	Processing time (ms)
9	0.215
17	0.280
21	0.310

5 Comparison of the Proposed Approach with Other Leading Techniques

A comparative study with some existing bimodal authentication methods is presented in Table 7. The comparison concerns: the used features, number of participants (P), number of used sensors, and obtained FAR, FRR, or EER scores.

Even though the first three methods[13–15] have good authentication performances (EER < 1), they exploit physical descriptors and are more vulnerable to attacks than behavioral descriptors.[17,18] Indeed, such approaches can be spoofed by the presentation of a fake hand and/or a recorded face. The rest of the reported methods (including the proposed method) combine both physical and behavioral descriptors into a single-authentication system. As mentioned before, the particularity of the proposed method is that the physical closed hand shape descriptor can be also considered as a behavioral descriptor because it gives additional information about the signatory hand disposition habit.

The information and results collected from the articles[3,4,13–15,16] show that our approach presents the best compromise between efficiency (EER = 2) and simplicity (only one sensor is used). Indeed, unlike the other bimodal systems, the proposed system requires only one sensor to simultaneously capture the required hand shape and signature modalities. Furthermore, simultaneously spoofing the closed hand disposition and the signature will certainly be a hard task for the experimental forgers.

Table 7 Comparison with other leading techniques.

Reference and Year	Used features	Database	Number of sensors	Performances
Ref. 13 and 2013	Vascular and hand geometry	100 P	1	EER = 0.06
Ref. 14 and 2003	Palmprint and hand geometry	100 P	1	FAR = 0, FRR = 1.41
Ref. 15 and 2011	Palmprint and face	130 P	2	EER = 0.79
Ref. 3 and 2006	Signature and speech	70 P	2	Random EER = 3.5 skilled EER = 6.9
Ref. 16 and 2004	Signature and face	100 P	2	EER = 2.2
Ref. 4 and 2012	Signature and face	40 P	2	EER = 3
2014	Our approach	100 P	1	EER = 2

6 Discussion and Conclusion

In this article, we have shown that it is better to consider the signature as a couple of handwriting and hand disposition habits rather than a simple handwriting habit.

An efficient heuristic authentication approach based principally on the exploitation of both the hand signature and hand shape descriptor has been validated. Unlike existing multimodal authentication approaches, the proposed authentication method requires only one sensor since the reconstructed online signature and the hand shape descriptor are extracted from the same video source.

Based on the hypothesis that the same person has the same habits regarding his/her initial signing hand pose, one can extract and use a hand shape descriptor to perform a precise signature authentication. Thus, an authentic signature or a good forgery is declared as a genuine signature only if the signatory hand is similar to that of the enrolled person's hand.

The DTW authentication method has been used for signature authentication, but due to its computational complexity, it will not be chosen to perform real-time online signature authentication. A dedicated authentication method, based on motion vectors computation, is under development to suit real-time constraints. Moreover, the developed hand shape authentication approach presents a low-computational complexity and is, therefore, well suited for a hardware implementation.

Even if it depends entirely on a dedicated acquisition system, the proposed approach allows performing a precise signature authentication, which is required for banking transactions and sensible site control access applications.

Acknowledgments

This work was supported by the national research project (PNR 42/TIC/2011). The authors are thankful to the anonymous reviewers for their valuable comments and suggestions to improve the quality of this paper.

References

1. D. Impedovo and G. Pirlo, "Automatic signature verification: the state of the art," *IEEE Trans. on Syst., Man Cybernet.* **38**(05), 609–635 (2008).
2. A. K. Jain, F. D. Griess, and S. D. Connell, "Online signature verification," *Pattern Recognit.* **35**(12), 2963–2972 (2002).
3. A. Humm, J. Hennebert, and R. Ingold, "Scenario and survey of combined handwriting and speech modalities for user authentication," in *Proc. of the 6th Int. Conf. on Recent Advances in Soft Computing (RASC 2006)*, K. Sirlantzis, Ed., pp. 496–501 (2006).
4. Y. Elmir et al., "A multi-modal face and signature biometric authentication system using a max-of-scores based fusion," *Lect. Notes Comput. Sci.* **7667**, 576–583 (2012).
5. V. Nalwa, "Automatic on-line Signature Verification," *Proc. IEEE* **85**(2), 215–239 (1997).
6. W. Almayyan et al., "A multimodal biometric approach based on binary particle optimization," *Research and Development in Intelligent Systems*, pp. 139–152, Springer, London (2011).
7. A. Oulefki et al., "New online signature acquisition system," *J. Electron. Imaging* **22**(1), 010501 (2013).
8. G. K. Gupta, "The state of the art in the on-line handwritten signature verification," Clayton School of Information Technology, Monash University, Melbourne, Technical Report 200 (2006).
9. M. Zoghi and V. Abolghasemi, "Persian signature verification using improved dynamic time warping-based segmentation and multivariate autoregressive modeling," *Proc. IEEE 15th workshop of Statistical Signal Processing (SSP'09)*, Cardiff, pp. 329–332 (2009).
10. C. C. Han, "A hand-based personal authentication using a coarse-to fine strategy," *Image and Vision Computing* **22**, 909–918 (2004).
11. A. K. Jain, A. Ross, and S. Pankanti, "A prototype hand geometry-based verification system," in *2nd Int. Conf. on Audio- and Video-based Biometric Person Authentication (AVBPA)*, pp. 166–171, AVBPA, Washington (1999).
12. C.C. Lip and D.A. Ramli, "Comparative study on feature, score and decision level fusion schemes for robust multi biometric systems," in *Frontiers in Computer Education*, Vol. **133**, pp. 941–948, Springer, Berlin Heidelberg (2012).
13. G. Park and S. Kim, "Hand biometric recognition based on fused hand geometry and vascular patterns," *Sensors* **13**, 2895–2910 (2013).
14. A. Kumar et al., "Personal verification using palmprint and hand geometry biometric," *Lect. Notes Comput. Sci.* **2688**, 668–678 (2003).
15. A. Poinsot, F. Yang, and V. Brost, "Palmprint and face score level fusion: hardware implementation of a contactless small sample biometric system," *Opt. Eng.* **50**(2), 027002 (2011).
16. A. M. Namboodiri et al., "Skilled forgery detection in on-line signatures: a multimodal approach," *Lect. Notes Comput. Sci.* **3072**, 505–511 (2004).
17. I. Buhan and P. Hartel, "The state of the art in abuse of biometrics," Technical Report TR-CTIT-05-41 Centre for Telematics and Information Technology, University of Twente (2005).
18. G. Hogben, "Behavioural biometrics," Technical Report, ENISA (European Network and Information Security Agency) (2010).

Saidani Kaouther received her master's degree in computer science in 2011 from the University of Bordj Bou Arreridj. She is currently pursuing her PhD degree in informatics at MSE Laboratory, University of Bordj Bou Arreridj (Algeria). Her current research involves multimodal biometric authentication systems, digital image processing, and compression.

Mostefai Messaoud is a professor in the Computer Science Department, Bordj Bou Arreridj University (Algeria). He supervises several PhD theses in computer science fields. He is currently responsible for the information theory group at MSE Laboratory. His research interests include flexible and real-time embedded systems, signal, and image processing algorithms.

Bouziane Abderraouf is an associate professor at the Computer Science Department at Bordj Bou Arreridj University (Algeria). He is a member of the MSE laboratory. His research interest fields include spectral analysis, organization, and indexing of high-dimensional multimedia data.

Chahir Youssef is a professor in the Computer Science Department, Caen University (France). He is a member of the Image Team at the GREYC laboratory. His research interest fields include image and video processing and analysis, multimedia data-mining, spectral analysis, and restitution and animation in virtual environment.