Low Cost and Usable Multimodal Biometric System Based on Keystroke Dynamicsand 2D Face Recognition

Romain Giot, Baptiste Hemery, Christophe Rosenberger

Low Cost and Usable Multimodal Biometric System Based on Keystroke Dynamics and 2D Face Recognition

Romain Giot Baptiste Hemery Christophe Rosenberger
GREYC Laboratory, ENSICAEN - University of CAEN - CNRS
{*romain.giot,baptiste.hemery,christophe.rosenberger*}*@greyc.ensicaen.fr*

Abstract

We propose in this paper a low cost multimodal biometric system combining keystroke dynamics and 2D face recognition. The objective of the proposed system is to be used while keeping in mind: good performances, acceptability, and respect of privacy. Different fusion methods have been used (min, max, mul, svm, weighted sum configured with genetic algorithms, and, genetic programming) on the scores of three keystroke dynamics algorithms and two 2D face recognition ones. This multimodal biometric system improves the recognition rate in comparison with each individual method. On a chimeric database composed of 100 individuals, the best keystroke dynamics method obtains an EER of 8.77%, the best face recognition one has an EER of 6.38%, while the best proposed fusion system provides an EER of 2.22%.

1. Introduction

The aim of biometrics is to enable user authentication using different characteristics (physiological, biological or behavioural). In this paper, we are interested in systems that are highly accepted by users and that exploit low cost biometric modalities (they are are not intrusive and do not need any specific material that are not present in classical computers): keystroke dynamics (keyboard) and face recognition (webcam). We also argue that these two biometric modalities are usable because they do not need specific interactions with the user (face and keystroke captures can be done easily without any extra interaction), and these two biometrics are not known to have privacy concerns (in opposition to fingerprint or DNA). Our contribution is the proposition of a multimodal system combining two biometric modalities (and multiple algorithms for each modality), with not so good performance when used alone.

2. Previous Works

We focus in this state of the art on multimodal systems involving biometric modalities usable for all computers (keystroke, face, voice...). The fusion process is the most important process in multimodal systems. It can be operated on the scores provided by algorithms or in the templates themselves [1]. In the first case, it is necessary to normalize the different scores as they do not evolve in the same range. Different methods can be used for doing this, and the more efficient methods are *zscore*, *tanh* and *minmax* [2].

Different kinds of fusion methods have been applied on multibiometric systems. The fusion can be done with multiple algorithms of the same modality. For example, in [3], three different keystroke dynamics implementations are fused with an improvement of the EER (Error Equal Rate), even if less than 40 users are involved in the database. In [4], two keystroke dynamics systems are fused together by using weighted sums for 50 users. No information on the weight computing is provided. The fusion can also be done within different modalities in order to improve the authentication process. In [5], authors use both face and fingerprint recognition. The impact of error rate reduction is used to reduce the error when adapting the user's model. There is only one paper (to our knowledge) on keystroke dynamics fusion with another kind of biometric modality (voice recognition): it is presented in [6], but only 10 users are involved in the experiment. In [7], multi-modality is done on fingerprints, speech, and face images on 50 individuals. Fusion has been done with SVM [8] with good improvements, especially, when using user specific classifiers.

As we can see in this state of the art, very few multimodal systems have been proposed for classical computers and the published ones have been validated on small databases.

3. Proposed Method

In this section, we present the proposed method: the first part presents the biometric recognition methods, while the second part presents the biometric fusion process.

3.1. Biometric Methods

3.1.1. 2D Face Recognition. Two different algorithms have been used for the 2D face recognition. The first is the classical eigenface algorithm [9] (noted *EIG*). The second one is a double association between keypoints (noted *ASSO*) published in [10]. Keypoints are detected on face images with the local descriptor SIFT [11]. The similarity between two face images corresponds to the number of associated keypoints.

3.1.2. Keystroke Dynamics. Three algorithms have been used in this study for the keystroke dynamics modality. We have used a first method based on a two class SVM (noted *SVM* in this paper), where enrolled templates from users are labeled 1 and enrolled templates from impostors are labeled -1. This method can be used in a passphrase environment. Impostor's information are not needed for the two other methods. The second tested method (noted *RHY*) is based on typing rhythm of the users: typing times are discretized in an alphabet of five characters and an hamming distance is computed. The last method is a statistical one (noted *STAT*) and is based on the use of mean, median and standard deviation of typing time. More information on these methods is available in [12], [13]. We have chosen these different methods because of their totally different ways of solving the problem of biometric authentication.

3.2. Fusion Methods

Several fusion configurations have been tested:

(i) fusion between all the methods from each modality (we want to improve performance for each modality), (ii) fusion between all the methods from both modalities (we want to improve the performance by using different modalities), (iii) these two kinds of fusion, without using the *SVM* scores (we want to keep in a classical password scheme different for all users: no need of impostors' data to create the model), (iv) fusion of the best methods of each modality. Figure 1 illustrates the different fusion strategies. Different fusion methods have been tested. Before applying the fusion process, it is necessary to normalize the score, because they are not distributed in the same range. The *tanh* normalization has been used, because in [2], authors argue on the fact that it is robust and efficient.

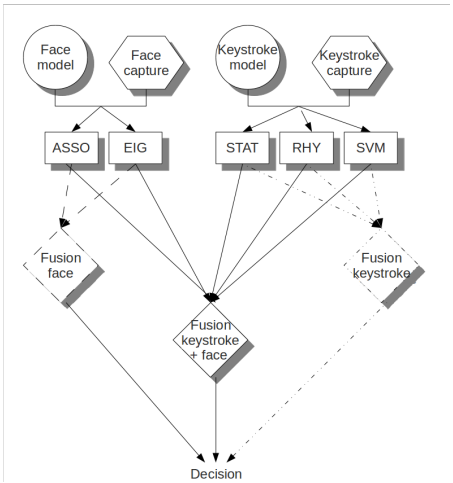

Figure 1. Principles of the different fusion strategies.

3.2.1. Methods From The State of the Art. The first fusion operators used are the following well known ones: *sum* (summing the scores), *mul* (multiplying the scores) and *min* (minimal value of the scores). They have been often used in the literature. We also tried the fusion mechanism by using an SVM, where the data of vector v against user u are the scores for each method between v and the model of u. The intra vectors are labelled 1 and the inter vectors are labelled -1. In order to avoid the skew due to the fact of using the same data for learning and validation, we have operated a 20 folds cross-validation, 100 times with shuffling the data each time in order to have different partitions and averaging the results.

3.2.2. Proposed Methods. Our contribution is on the definition of new fusion functions parametrized with genetic algorithm and fusion function built with genetic programming. We have also used weighted sum configured with genetic algorithms. Formulas are $ga1 = \sum_{i=0}^{n} w_i * s_i$ (weighted sum), $ga2 = \prod_{i=0}^{n} s_i^{x_i}$ (contribution 1) and $ga3 = \sum_{i=0}^{n} w_i * w_i^{x_i}$ (contribution 2), with n the number of available scores, w_i the weight of multiplication of score i, s_i the score i and x_i the weight of exponent of score i. Computation is done with a population of 5000 individuals, 500 generations and a mutation probability of 0.9. The coefficient evolve in the interval [-5;5] and the fitness function is the EER computing.

For the first time, genetic programing [14] has been used in order to evolve fusion programs. Half

of the scores are used to realize some evolution of the fusion function, while the left scores are used for validation. The fitness evaluation function is $fitness = \frac{2*FAR+FRR}{3}$ as we want to have less false recognition than false acceptance, and the functions set is $\{-, +, *, /, \&, |, <, max, min, avg\}$, with a population of 1000 individuals, 20 generations and a mutation probability of 0.45.

4. Validation

4.1. Experimental Protocol

As no public database includes keystroke dynamics and face, we have created a chimerical one [15] based on th AR face database [16] and the greyc keystroke one [17].

The AR face database contains frontal images of 120 individuals, 65 males and 55 females. Images were realized in two different sessions two weeks appart. During each session, 13 pictures were taken with different facial expressions, illumination variations and occlusions. The size of images in the database are $768 * 576$ pixels, and each pixels is a 24bits RGB color values. These images were converted to grayscale and cropped so as final images were $256 * 256$ pixels. The greyc keystroke database contains more than 100 users providing more than 60 captures. The captures were done during several sessions spaced by a week (in most of the cases), where users were asked to type 6 times the password "greyc laboratory" on a laptop and 6 times on an USB keyboard (by alternating the source of typing). So, a session consists of 12 captures on 2 different keyboards. To match with the AR database, we have used the data of 100 individuals and their 26 last captures (by this way, captures are extracted from 3 sessions).

The first ten captures are used to create the model, while the 16 others are used for the verification. So, we have respectively $100 * 16 = 1600$ and $100 * 16 * 99 = 158400$ scores to compute for intraclass and interclass for each implemented method.

4.2. Experimental Results

Table 1 presents the results for the different fusion configurations. The "*" represents the fusion providing much better results than the initial systems' performance, "-" represents results that are not better than the best method used in fusion, "=" represents results approximately equal, and "+" results slightly better. No symbol, means it is not comparable (only one functional point, versus a set of points allowing to compute EER). FAR, FRR, EER respectively stands for False Acceptance Rate, False Rejection Rate, and Error Equal Rate.

For keystroke dynamics, the *SVM* method outperforms the two others (EER=8.77%), and the *RHY* one is the worst (EER=15.46%) . For face recognition, the method based on SIFT (*ASSO*, EER=6.38%) totally outperforms the eigenface one (*EIG*, EER=29.55%).

When only merging the three keystroke dynamics scores, we obtain a performance almost equivalent (or worst) than the *SVM* one. When merging the keystroke dynamics scores without the *SVM* ones, obtained results improve quite a lot and are similar than the *SVM* one. So, in a passphrase environment, the *SVM* methods is required and gives the same result than the fusion of the two other methods in a classical password environment. The fusion of face recognition algorithms gives always worst results than the *ASSO* one. The gap of performance of its two methods is too important to be improved by fusion.

Weighted algorithms (and especially our contributed formulas) give the best results, while genetic programming seems to be an interesting method when we want to privilege one kind of error among FAR and FRR. For a lack of place, the ROC curves and generated trees are not illustrated. We can see that the best methods need a set of learning scores in order to be correctly configured. In a scenario where it is not possible to obtain such a database, the best method is the sum which gives good results in all the cases.

5. Conclusion

For the first time, a low cost and usable multimodal system based on keystroke dynamics and 2D face recognition has been presented. It's interests resides on the facts that these information can be easily get on most computers. Different fusion methods have been tested on a chimerical database containing two kinds of biometric templates for 100 users (keystroke dynamics and face). We have proposed two new fusion functions parameterized thanks to genetic algorithm and one build with genetic programming. By fusing biometric systems of the same modality, we have obtained better performances in the case of keystroke dynamics, but not with face recognition where the performance of the combined methods were too different. Using the fusion with the whole set of methods really improves the results by obtaining an EER of 2.22% in our best scheme. Genetic programming seems to be a good candidate as defining complex and adaptive fusion functions considering the specificity of combined biometric systems. We can also put into obviousness that our proposition outperforms

Table 1. Results of the different fusion configurations. The normalization is done with the *tanh* operator.

Method	FAR	FRR
	Keystroke Dynamics, no fusion	
SVM	8.77%	
STAT	11.57%	
RHY	15.46%	
	Face Recognition, no fusion	
ASSO	6.38%	
EIG	29.55%	
	Keystroke Dynamics, fusion	
sum(SVM,STAT,RHY)	8.99% =	
mul(SVM,STAT,RHY)	9% =	
min(SVM,STAT,RHY)	10.19% -	
	Keystroke Dynamics (no SVM), fusion	
sum(STAT,RHY)	9.92% *	
mul(STAT,RHY)	9.89%*	
min(STAT,RHY)	11.66% *	
	Face recognition, fusion	
sum(EIG,ASSO)	7.75% -	
mul(EIG,ASSO)	7.83% -	
min(EIG,ASSO)	19.7% -	
	All methods, fusion	
sum(SVM,STAT,RHY,ASSO,EIG)	2.59% *	
mul(SVM,STAT,RHY,ASSO,EIG)	2.60% *	
min(SVM,STAT,RHY,ASSO,EIG)	13.01% -	
	All methods (except SVM), fusion	
sum(STAT,RHY,ASSO,EIG)	2.83% *	
mul(STAT,RHY,ASSO,EIG)	2.85% *	
min(STAT,RHY,ASSO,EIG)	14.54% -	
	Best method of each modality, fusion	
sum(SVM,ASSO)	5.02% *	
mul(SVM,ASSO)	5.02% *	
min(SVM,ASSO)	3.62% *	
	All modalities, GA, fusion	
ga1	2.31% *	
ga2	**2.22% ***	
ga3	2.26% *	
	Genetic programming, fusion	
gp(SVM,STAT,RHY,ASSO,EIG)	0.25%	20.25%
gp(SVM,ASSO)	1.94%	10.37%
	Machine learning, fusion	
svm(SVM,STAT,RHY,ASSO,EIG)	4.9%±1.4	14.5%±4.9
svm(SVM,ASSO)	9.91%±0.55	9.70±9.91

the other ones. Our future experiments will be based on using different normalization mechanisms, the creation of user's specific threshold configurations, or pattern fusion.

References

[1] R. Raghavendra, B. Dorizzi, A. Rao, and G. K. Hemantha, "Pso versus adaboost for feature selection in multimodal biometrics," in *Biometrics: Theory, Applications, and Systems, 2009. BTAS '09. IEEE 3rd International Conference on*, Sept. 2009, pp. 1–7.

[2] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270–2285, 2005.

[3] S. Hocquet, J.-Y. Ramel, and H. Cardot, "User classification for keystroke dynamics authentication," in *The Sixth International Conference on Biometrics (ICB2007)*, 2007, pp. 531–539.

[4] P. Teh, A. Teoh, T. Ong, and H. Neo, "Statistical Fusion Approach on Keystroke Dynamics," in *Proceedings of the 2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System-Volume 00*. IEEE Computer Society, 2007, pp. 918–923.

[5] F. Roli, L. Didaci, and G. Marcialis, "Adaptive biometric systems that can improve with use," *Advances in Biometrics. Springer London*, pp. 447–471, 2008.

[6] J. Montalvao Filho and E. Freire, "Multimodal biometric fusionjoint typist (keystroke) and speaker verification," in *Telecommunications Symposium, 2006 International*, 2006, pp. 609–614.

[7] J. Fierrez-Aguilar, J. Ortega-Garcia, D. Garcia-Romero, and J. Gonzalez-Rodriguez, "A comparative evaluation of fusion strategies for multimodal biometric verification," *Lecture notes in computer science*, pp. 830–837, 2003.

[8] V. Vapnik *et al.*, "Theory of support vector machines," *Department of Computer Science, Royal Holloway, University of London*, pp. 1677–1681, 1996.

[9] M. Turk and A. Pentland, "Face recognition using eigenfaces," in *Proc. IEEE Conf. on Computer Vision and Pattern Recognition*, vol. 591, 1991.

[10] C. Rosenberger and L. Brun, "Similarity-based matching for face authentication," in *International Conference on Pattern Recognition (ICPR)*, 2008.

[11] D. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110, 2004.

[12] R. Giot, M. El-Abed, and R. Christophe, "Keystroke dynamics with low constraints svm based passphrase enrollment," in *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2009)*, 2009.

[13] P. Magalhães, K. Revett, and H. Santos, "Keystroke dynamics: stepping forward in authentication," 2006.

[14] J. Koza and J. Rice, *Genetic programming*. Springer, 1992.

[15] L. Allano, S. Garcia-Salicetti, and B. Dorizzi, "On the validity of virtual subjects for multibiometric systems evaluation." in *RASC 2006*, Kent, UK, 2006.

[16] A. Martinez and R. Benavente, "The ar face database," CVC Technical report, Tech. Rep., 1998.

[17] R. Giot, M. El-Abed, and R. Christophe, "Greyc keystroke: a benchmark for keystroke dynamics biometric systems," in *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2009)*, 2009.