A SWARM INTELLIGENCE APPROACH FOR BIOMETRICS VERIFICATION AND IDENTIFICATION

L. Pulina

March 9, 2012

University of Sassari

Computer Vision Laboratory

Technical Report No. CVL -2012-002

UNIVERSITY
of
SASSARI

A SWARM INTELLIGENCE APPROACH FOR BIOMETRICS VERIFICATION AND IDENTIFICATION

L. Pulina

University of Sassari
Computer Vision Laboratory
Porto Conte Ricerche - Loc. Tramariglio
07041 Alghero (SS)
www.uniss.it

March 9, 2012

Technical Report No. CVL -2012-002

Abstract

In this paper we investigate a swarm intelligence classification approach for both biometrics verification and identification problems. We model the problem by representing biometric templates as ants, grouped in colonies representing the clients of a biometrics authentication system. The biometric template classification process is modeled as the aggregation of ants to colonies. When test input data is captured – a new ant in our representation – it will be influenced by the deposited pheromones related to the population of the colonies.

We experiment with the Aggregation Pheromone density based Classifier (APC), and our results show that APC outperforms "traditional" techniques, like 1-nearest-neighbour and Support Vector Machines. We also show that performance of APC are comparable to several state of the art face verification algorithms. The results here presented let us conclude that swarm intelligence approaches represent a very promising direction for further investigations for biometrics verification and identification.

1 Introduction

The biometrics authentication problem [14] consists in recognize in a trustworthy way humans on the basis of their physical traits, e.g., face, fingerprints, and voice. In the last decade, the solutions proposed by the biometrics scientific community have been key enablers for a wide range of personal biometrics authentication systems, e.g, identity access management and access control – see [13] for a survey. Roughly speaking, a personal biometrics authentication system is composed of a set of individual biometric samples, that has been captured and labeled during an *enrollment* stage. The features extracted from the biometric(s), together with their related labels, are collected by the system. In biometrics, such data is usually called *template*. Biometrics authentication systems can be used in two different modes, namely *verification* and *identification*. Concerning the former, the claimed person identity is classified to be genuine or impostor comparing the input biometric with the enrolled template. This mode can be modeled as a binary classification problem. Considering the latter, the captured template of a person is compared with all the enrolled templates. This task can be modeled as a multiple-class classification problem.

Despite several success stories – see e.g. [4] – a fully reliable biometrics authentication system is yet an open issue of paramount importance. As a matter of facts, when captured biometric data are matched against enrolled templates, a perfect matching is hardly obtained. This is mainly due to the fact that enrolled templates are usually captured one time only (for user convenience) and in controlled environmental conditions. In order to cope with this issue, in the last decade several approaches has been proposed, including pattern classification, geometrical approaches, and statistical analysis – see, e.g, [7] for a survey.

In this paper we investigate a swarm intelligence based classification algorithm for both biometrics verification and identification problems. Despite the several success stories reported in scientific literature about the application of swarm intelligence methods in a wide range of applications – e.g., finding optimal routes [6], scheduling [10],

data mining [12] –, to the extend of our knowledge, no swarm intelligence approaches for the biometrics verification or identification problems has been proposed.

In the case of verification, we model the problem by representing biometric templates as ants, grouped into two colonies. The first one is populated by the ants representing the enrolled template related to a given client. The second one is populated by the ants representing the data used as impostor training. In the case of identification, ants are grouped into n colonies, where n is the total amount of clients. The biometric template classification process is modeled as the aggregation of ants to colonies. When test input data is captured – a new ant in our representation – it will be influenced by the deposited pheromones related to the population of the colonies.

In order to highlight the potential advantages of swarm intelligence based classification algorithms on biometrics verification and identification, we focus on the biometric face, and we tested the Aggregation Pheromone density based Classifier (APC) [8] on the BANCA 2D faces dataset [2]. In our experiments we show that APC outperforms "traditional" techniques like 1-nearest-neighbour [1] and Support Vector Machines [5]. Moreover, we show that performance of APC are comparable to several state of the art face verification algorithms. The results here presented let us conclude that swarm intelligence approaches represent a very promising direction for further investigations for biometrics verification and identification.

The paper is structured as follows. In Section 2 we briefly outline how a personal biometrics authentication system operates. In Section 3 we recap the APC algorithm, and we detail its usage in the context of biometrics verification and identification problems. In Section 4 we describe our experiments, and we conclude in Section 5 summarizing our current results and future research directions.

2 Biometrics authentication systems

As stated in [13], a biometrics system is essentially a pattern recognition system that acquires biometric data from an individual, extracts a feature set from the data, compares this feature set against the feature set(s) stored in a database, and executes an action based on the result of the comparison.

We can view a (generic) biometrics system as the composition of four different modules. The first one is devoted to acquire the raw biometric data of a person. In the case of faces, such data could be captured, e.g., by a digital camera. The second module is devoted to features extraction. Still considering the biometric face, in scientific literature has been proposed a wide range of methods. The third module is devoted to decision-making, and it is the one to which we focus this work. Here, the extracted features are tested against the stored templates, and the result of such comparison is used, e.g., to validate a claimed identity. The last module consists of a system database aimed to store the repository of biometric informations. For instance, in face recognition systems, it may store multiple templates of an individual corresponding to different facial poses with respect to the camera.

Depending on the application domain, a biometrics system may operate either in the verification or identification mode. In the verification mode, the system validates

a claimed person identity by comparing the captured biometric data with her own biometric template(s) stored in the system database. In the identification mode, the system computes a one-to-many comparison, in order to establish an individual identity without the client having to claim an identity. In such systems, a failure is reported if the subject is not enrolled in the database. In our experiments, we assume that all the subjects' templates involved in the identification are stored in the database.

3 Algorithm and Implementation

In this section we model the biometrics authentication problem using the APC algorithm. The reader is referred to [8] for a deeper analysis of APC.

Considering biometrics verification, let L be the training data, composed of both enrolled templates related to the genuine user, and other data used for non client training purpose. Let consider $\bar{x}^i_1, \ldots, \bar{x}^i_{|C_i|}$, $i = \{0, 1\}$, as the given training data patterns in the training class C_i, where:

- $\bar{x}^1_j$, $j = 1, \ldots, |C_1|$ denotes the feature vector computed from the enrolled templates related to the genuine user.
- $\bar{x}^0_j$, $j = 1, \ldots, |C_0|$ denotes the feature vector computed from the templates related to the "All World" data used for non client training.

We modeled these patterns as a population of $|C_i|$ ants represented as $a^i_1, a^i_2, \ldots, a^i_{|C_i|}$.

Let U be the set containing the test (unclassified) data patterns, and let $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_{|U|}$ be the test data represented as a set of feature vectors. We modeled them as a set of "unlabeled" ants $a_1, a_2, \ldots, a_{|U|}$, approaching to some colony C_i.

We use the representation described above for each recorded client, and we can summarize the initial state of the system as follows: (i) Enrolled templates are represented as ants belonging the colony C_1; and (ii) data used for non client training are represented as ants belonging the colony C_0.

Considering a batch of $|U|$ new captured data – the approaching ants $a_k, k = \{1, \ldots, |U|\}$ –, APC works as follows.

1. Each $a^i_j \in C_i$ emits pheromones at its neighborhood, and its intensity decreases with the distance. This is modeled – see [8] – by a Gaussian distribution: The effect of pheromone density on a_k, – located at $\bar{x}_k$ – due to $a^i_j \in C_i$ – located at $\bar{x}^i_j$ is given by

$$\Delta\tau(\bar{x}^i_j, \bar{x}_k) = exp(-\frac{d(\bar{x}^i_j, \bar{x}_k)^2}{2\delta^2}) \quad (1)$$

where δ is the spread of a Gaussian function, while d denotes the Euclidean distance. The average effect of the pheromone density on a_k due to C_i is

$$\Delta\hat{\tau}_{ki} = \frac{1}{|C_i|} \sum_{\bar{x}^i_j \in C_i} \Delta\tau(\bar{x}^i_j, \bar{x}_k), \forall k, i \quad (2)$$

2. The ant will join the colony related to the greatest value returned by Eq. 2.

Concerning the modeling related to biometrics identification, the procedure is analogue to the one described above, with the noticeable difference that in this case we consider a colony C_i for each user for which templates are stored in the database. Notice that, in this case, we assume that all the clients approaching to the system have a least one template stored in the database.

In order to compare the performance of APC against some well-established classification algorithms, we will also experiment both biometrics verification and identification involving **1-nearest-neighbor** (1-NN) and **Support Vector Machine** (SVM). 1-NN is a classifier yielding the label of the training instance which is closer to the given test instance, whereby closeness is evaluated using some proximity measure, e.g. Euclidean distance. We involved 1-NN in our analysis in order to have a simple baseline to compare the performance of APC.

SVM is a supervised learning algorithm used for both classification and regression tasks. Roughly speaking, the basic training principle of SVMs is finding an optimal linear hyperplane such that the expected classification error for (unseen) test patterns is minimized. The reader is referred to [5] for further details. We involved SVM in our analysis because it is a well-established machine learning algorithm, used to accomplish several tasks in a wide range of application domains, including face authentication – see, e.g., [9].

4 Experimental Analysis

We experiment APC on the BANCA 2D faces dataset [2]. The dataset is composed of 6240 images divided in two groups, namely $g1$ and $g2$, composed of 3120 images. The images are related to 26 subjects per group, recorded in 12 sessions, and each sessions consists in 10 images, 5 of which are used as client images, while the remaining ones for impostor attack. The 12 session are related to three different scenarios, namely *Controlled* (sessions 1–4), *Degraded* (sessions 5–8), and *Adverse* (sessions 9–12).

Concerning the features, a bank of Gabor filters with 5 scales and 8 orientations is applied to each 110x110 resized images on the 121 nodes of a uniform grid superimposed to the image. As result of the computation, a feature vector composed of 4000 elements has been obtained for each image.

Concerning face verification, we follow the guidelines proposed for the BANCA dataset [2]. In particular, out of the seven configuration proposed, we focused on the following ones: (*i*) Matched Controlled (MC), in order to have a baseline related to the accuracy of the algorithms; (*ii*) Unmatched Degraded (UD), in order to test the performance of APC against low-quality images; (*iii*) Unmatched Adversary (UA), in order to test performance when different conditions occur between training and testing conditions; and (*iv*) Pooled test (P), in order to test performance on varied testing conditions. We built both training and test set according to the BANCA protocol. Finally, group $g1$ has been used as development set – in order to tune δ –, while $g2$ as evaluation set. We also used $g1$ to tune both C and γ of a C-SVC with RBF kernel, implemented on top of LibSVM [3].

Protocol	APC						1-NN		
	R = 0.1		R = 1		R = 10		R = 0.1	R = 1	R = 10
	δ	WER	δ	WER	δ	WER	WER	WER	WER
MC	0.2	3.16	0.05	3.29	0.05	1.23	6.18	4.01	1.17
UD	0.6	4.19	0.4	9.67	0.1	3.45	37.76	20.77	3.77
UA	0.7	3.67	0.1	10.41	0.05	2.39	29.67	16.32	2.97
P	0.6	3.92	0.1	11.27	0.1	4.65	24.69	13.66	2.63

Table 1: Performance of APC and 1-NN on the BANCA dataset. The table is structured as follows. The first column ("Protocol") denotes the protocol of the experiment, and it is followed by two groups of columns. The first one reports the performance of APC related to the different values of R (group "R = 0.1", "R = 1", and "R = 10"), and it is composed of two sub-columns. The first sub-column reports the APC parameter related to the obtained performance (column "δ") while in the second one we report the value of WER (column "WER"). The next group of columns reports the performance of 1-NN, and it is composed of three sub-columns, in which we report the value of WER related to different values of R.

Our first experiment is aimed to test the performance of APC on the four configurations listed above. As performance measure for face verification, we use Weighted Error Rate (WER) [11]. Given the False Rejection Rate (FRR), and the False Acceptance Rate (FAR), we show the results related to three specific operating conditions which – as described in [11] – corresponded to three different values of the Cost Ratio $R = C_{FAR}/C_{FRR}$. Assuming equal a priori probabilities of genuine clients and impostor, the idea is to test the algorithm when FAR is an order of magnitude less harmful than FRR, FAR and FRR are equally harmful, and, finally, when FAR is an order of magnitude more harmful than FRR ($R = \{0.1, 1, 10\}$, respectively).

With a fixed R, and given FRR and FAR, WER is defined as

$$WER(R) = \frac{FRR + R \cdot FAR}{1 + R}$$

We detail the results related to WER(R) in Table 1.

Looking at the table, we first notice that we did not report the performance related to SVM. The motivation is that we found significant results only considering the MC protocol. For $C = 64$ and $\gamma =$ 2e-2, we report that WER(0.1) = 18.68, WER(1) = 10.27, while WER(10) = 1.87.

In Table 1, concerning the results related to MC, we can see that performance of APC are slightly better that the ones reported for 1-NN considering $R = 0.1$ and $R = 1$. If we look at the remaining protocols, we can see that APC outperforms 1-NN in terms of WER.

Considering now the results related to the protocol P, we can obtain an hint about the potential of APC if we compare our results with the ones presented in [11], that we report in Table 2 for convenience. Such results are related to Part I of the competition (pre-registered images), group $g2$. It is the same used in our experiments, in order to obtain an apple-to-apple comparison . Considering $R = 0.1$, we can see that 2 out of 12 systems outperform APC, namely "Tsinghua Univ.", "Univ. Nottingham".

Algorithm	WER(0.1)	WER(1)	WER(10)
IDIAP – HMM	8.15	20.25	6.24
IDIAP – FUSION	7.43	16.88	6.06
QUT	8.53	16.12	4.83
UPV	6.18	14.56	4.96
Univ. Nottingham	1.77	7.11	1.58
National Taiwan Univ.	8.22	27.13	11.33
UniS	7.22	13.66	5.10
UCL – LDA	9.49	16.51	6.45
UCL – Fusion	6.01	13.84	4.10
NeuroInformatik	6.50	10.80	4.30
Tsinghua Univ.	0.73	1.85	0.84
CMU	4.75	11.61	7.45

Table 2: Performance of a pool of algorithms on the $g2$ group of the BANCA dataset under the P protocol. The table is composed of four columns. The first one ("Algorithm") denotes the used algorithm as reported in [11]. Finally, last three column report WER with $R = 0.1$ (column "WER(0.1)"), $R = 1$ (column "WER(1)"), and $R = 10$ (column "WER(10)").

Protocol	APC						1-NN		
	R = 0.1		R = 1		R = 10		R = 0.1	R = 1	R = 10
	δ	WER	δ	WER	δ	WER	WER	WER	WER
MC	0.2	3.01	0.1	5.27	0.05	1.24	11.91	6.65	1.39
UD	0.6	4.77	0.3	9.61	0.1	3.57	38.26	21.04	3.83
UA	0.7	5.94	0.2	11.87	0.2	3.11	33.27	18.30	3.33
P	0.6	4.78	0.2	12.16	0.05	2.67	27.85	15.35	2.85

Table 3: Performance of APC and 1-NN on the BANCA dataset having training sets composed of a single image. The table is organized as Table 1.

Looking now at group "R = 1", we report that the picture does not change substantially, with the noticeable exception of "NeuroInformatik" that returns a slightly better performance with respect to APC. Finally, looking at WER(10), we report that APC performance is comparable with the other systems.

Motivated by the fact that most part of biometrics verification systems store only one template per client, our next experiment aims to test APC on this harder setting. In order to do that, we modified the composition of the training sets related to the BANCA protocols, rebuilding them with only one image per genuine user, i.e., $|C_0| = 1$. In this case, it is reasonable to find a leak of performance on classifiers, and aim of this experiment is to test the effectiveness of APC in this context. Table 3 shows the results of the experiment above.

Looking at Table 3, and comparing the results against the ones reported in Table 1, we do not report noticeable differences between them. On the other hand, we report for 1-NN a two times greater error on MC for $R = 0.1$.

Our last experiment aims to test – in a preliminary way – APC on the face identification problem. Because of the BANCA dataset was designed for identity verification, authors do not provide any suggestion about the face identification protocols. Hence, in order to simulate a working face identification system, we experiment on the following on a set of protocols computed as follows:

Protocol	APC	1-NN	SVM
PC	88.46%	89.23%	86.92%
PC_1	88.06%	87.85%	88.06%
PD	51.15%	46.53%	49.03%
PD_1	49.03%	33.65%	42.50%

Table 4: Performance of APC, 1-NN, and SVM on the BANCA dataset concerning the face identification problem. The table is structured as follows. The first column ("Protocol") denotes the protocol of the experiment, and it is followed by three columns reporting the accuracy (in percentage) for APC, 1-NN, and SVM, respectively.

- **PC**: The training set is composed of the whole set of session 1 controlled images, while the test set is composed of the whole set of session 2–4 controlled images. The rationale is to try a protocol as "close" to MC as possible. Protocol PC_1 is the same one, but involving only one image per client in the training set.
- **PD**: The training set is the same as the PC, while the test set is composed of the whole set of session 5–9 low-quality images. The rationale is to try a protocol as "close" to UD as possible, in order to test if there is a leak of performance in the case of degraded images. Also in this case, PD_1 is the same one, but involving only one image per client in the training set.

Table 4 shows the results of the experiment above. Looking at the table, concerning PC, we report that 1-NN returns the best performance, but we also report that all classifiers accuracies are in the same ballpark. Looking now at PC_1, we can see that the picture does not change in a noticeable way. Finally, in our opinion, the most interesting results is the one that we report for both PD and PD_1. Also if the accuracies are not at all satisfying for a face identification system, we can see that APC seems to be more robust with respect to both 1-NN and SVM.

5 Conclusions and Future Work

Summing up, in this paper we modeled biometrics verification and identification using a Swarm Intelligence approach. We experimented with the BANCA 2D faces dataset using the APC algorithm, and in our experiments we have shown that such approach could be very promising for further developments and investigations. Particularly, we believe that the presented results can be improved by integrating classification algorithms with methodologies automatic parameter configuration. As we showed in our experiments, the parameters optimization for each value of R affects the performance significantly. In order to avoid parameter grid search, our future work will be devoted to investigate automatic parameters optimization in this context. We also plan to test swarm intelligence approaches both to different biometrics – e.g., fingerprints – and to multibiometrics systems, i.e., systems in which templates are composed of features extracted from different captured biometrics.

Acknowledgments The author wish to thank the University of Sassari for its financial support, and the anonymous reviewers for giving me helpful suggestions on how to improve the draft version of the paper. Enrico Grosso and Massimo Tistarelli are to be thanked for helpful discussions about biometrics systems.

References

[1] D. Aha, D. Kibler, and M. Albert. Instance-based learning algorithms. *Machine learning*, 6(1):37–66, 1991.

[2] E. Bailly-Baillire, S. Bengio, F. Bimbot, M. Hamouz, J. Kittler, J. Marithoz, J. Matas, K. Messer, F. Pore, and B. Ruiz. The BANCA database and evaluation protocol. In *In Proc. Int. Conf. on Audio- and Video-Based Biometric Person Authentication (AVBPA03*, pages 625–638. Springer-Verlag, 2003.

[3] C. Chang and C. Lin. LibSVM: a library for support vector machines. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2(3):27, 2011.

[4] G. Chetty, R. Biswas, and J. Goodwin. Identity retrieval in biometric access control systems using multimedia fusion. *Neural Information Processing. Models and Applications*, pages 590–597, 2010.

[5] C. Cortes and V. Vapnik. Support-vector networks. *Machine learning*, 20(3):273–297, 1995.

[6] M. Dorigo and L. Gambardella. Ant colony system: A cooperative learning approach to the traveling salesman problem. *Evolutionary Computation, IEEE Transactions on*, 1(1):53–66, 1997.

[7] P. Flynn, A. Jain, and A. Ross. *Handbook of biometrics*. Springer, 2008.

[8] A. Halder, A. Ghosh, and S. Ghosh. Aggregation pheromone density based pattern classification. *Fundamenta Informaticae*, 92(4):345–362, 2009.

[9] K. Jonsson, J. Kittler, Y. Li, and J. Matas. Support vector machines for face authentication. *Image and Vision Computing*, 20(5-6):369–375, 2002.

[10] D. Merkle, M. Middendorf, and H. Schmeck. Ant colony optimization for resource-constrained project scheduling. *Evolutionary Computation, IEEE Transactions on*, 6(4):333–346, 2002.

[11] K. Messer, J. Kittler, M. Sadeghi, M. Hamouz, A. Kostin, F. Cardinaux, S. Marcel, S. Bengio, C. Sanderson, N. Poh, et al. Face authentication test on the BANCA database. In *ICPR 2004. Proceedings of the 17th International Conference on*, volume 4, pages 523–532. IEEE, 2004.

[12] R. Parpinelli, H. Lopes, and A. Freitas. Data mining with an ant colony optimization algorithm. *Evolutionary Computation, IEEE Transactions on*, 6(4):321–332, 2002.

[13] A. Ross, K. Nandakumar, and A. Jain. *Handbook of multibiometrics*, volume 6. Springer-Verlag New York Inc, 2006.

[14] W. Shen and T. Tan. Automated biometrics-based personal identification. *Proceedings of the National Academy of Sciences*, 96(20):11065, 1999.