POSTER: ADAPTATIVE TEMPLATES IN BIOMETRIC AUTHENTICATION

Ricardo García Noval
University of the Balearic Islands
Son Lledó Building,
Valldemossa Road, km 7.5.
07122, Palma, Balearic Islands, Spain
ricardo.garcia@uib.es

Francisco Perales López
Computer Graphics, Vision, and Artificial Intelligence Group,
University of the Balearic Islands
Anselm Turmeda Building,
Valldemossa Road, km 7.5
07122, Palma, Balearic Islands, Spain
paco.perales@uib.es

ABSTRACT

Biometric authentication systems are usually based on features extraction. Features are a collection of measurable details, obtained from the biometric trait that defines the identity of a certain person. This collection of data is known as template, and it's stored in the database. The acquired biometrics quality must be controlled in order to model the identity of the individual in a unique and distinct way. The creation and update of templates is a critical task for the correct use of a biometric application. In this paper we propose the implementation of a model that, using biometric-independent tools, intends to update, select and improve the templates stored in the database, in what we have called "adaptive biometric templates". It has been tested with a fingerprint biometric database of 60 users. We have obtained an average improvement over traditional templates of 26% for FMR and of 53% for FNMR, we consider these results very successful.

Keywords

Biometric authentication, Template selection, Multi-modal interfaces.

1. INTRODUCTION

A generic biometric system can be defined with a very simple working paradigm that is used in most applications and commercial solutions.

First, when a security system is being installed, the biometric traits of all users with access to the resource must be acquired, thus creating a database that models the identity of the individuals by means of templates.

This step or working mode is known as enrollment. Each time a new genuine user wants to access the resource we must enroll him, acquiring his biometrics. Currently, user's identities stored as templates in the database don't change after enrollment and remain invariable in the database.

Subsequently, users who want to enter the system must show their biometrics for comparison with the stored templates and verify that his identity is found in the database and, thus, grant him access. At this moment biometric security system works in "authentication" mode.

With this working scheme the enrollment process is essential since it's the only moment when templates stored in the database are modified. These templates are the main link between the designed user's model and his real identity, and they remain static as long as we don't acquire another set of biometric traits, process that can be annoying to the user.

But achieving biometric templates that represent the user's identity in an accurate way can be a difficult task as a consequence of several factors: it is not easy to measure the quality of a biometric trait (the only "objective" values are FMR and FNMR [1]), the user's biometrics are not in good condition at the time of acquisition (e.g., dry fingers in a fingerprint system or irritaded eyes in iris detection [2]) and, though it's not a desirable feature, some biometrics, like voice, could change with time.

Moreover, if the number of database users is high, a "manual" control over biometric templates quality that rejects incorrect traits and acquires a new (correct) set of traits could not be possible.

Two problems surge from the limitation explained above: first, the need of updating biometric templates in order to accommodate them to the trait's real evolution in the individuals and second the proper (correct) selection of templates in order to turn down deficiencies or errors in acquisition, therefore reducing error rates associated with authentication.

In the next sections, we propose a new adaptative biometric template system. The proposed system improves the update template process increasing inter-class differences and reducing intra-class differences, using the standard authentication procedure to attain more precise ROC curves. Also our system is designed in an open way, so that future new templates from other biometrics features can also be included and therefore offer a multibiometric approach.

2. ADAPTATIVE BIOMETRIC TEMPLATES

A lot of schemes that bring successful solutions to these problems have been implemented. X. Jiang and W. Ser [3] propose a recursive technique for improving biometric templates that compute average values of minutiae included in each instance of a fingerprint template. Other known methods are biometric independent, like the ones proposed by Jain, Ross and Uludag, [4] that use binary trees between the different instances that form a template (dendograms, DEND method) or average distances of similarity between these instances (MDIST). Scheidat et. al. [5], on the other hand, focus the update problem as if it was a "cache" pages' issue. They propose the use of classics algorithms (FIFO, LRU, clock) for replacing the biometric traits that became obsolete. The paradigm that we will show next (implemented in the structure of a multimodal biometric library [9]) doesn't intend to replace none of the mentioned above techniques, whose efficiency and performance has been proved. The main idea is to provide an automatic tool for supporting adaptative biometric templates that, using the information obtained from the access of the different users, could make the templates stored in the database more different between them and more similar to the real trait of the individual.

The working scheme until now was:

1. *Acquire user's biometrics and store its features in a biometric template in the database.*
2. *When a users tries to access:*
   a. *Verify that the biometric given is similar to the one stored in the template.*

We propose the following:

1. *Acquire user's biometrics and store its features in a biometric template in the database*
2. *When a users tries to access:*
   a. *Verify that the biometric given is similar to the one stored in the template*
   b. *Store the biometric trait used in the access.*
3. *Periodically and for each user:*
   a. *Evaluate the quality of the biometric traits used in the access.*
   b. *If the quality of this traits is better then include them in the template, else reject them.*

In order to implement this system we need to use a second biometric database, parallel to the main database. This second database stores the different "attempts to access" that occur when the security system works in authentication mode, for its later evaluation. The information stored is:

- Date and time of the access.
- Name of the user whose identity was claimed in the access.
- Set of biometric features given in the access.

These entries are stored in different lists. First, for each user we store a list of all the successful accesses that he has made, in order to examine directly the evolution of the biometric trait along the different genuine entries. Second, we store a list of users than haven't achieved the access to the system, representing a database of potential impostors. We want the stored users to be as less similar as we can to these impostors.

Second chance verification

To support adaptative biometric templates we need a method that distinguishes user's access that has produced a false non match and the access of an impostor that tries to pass off as a genuine user. If we keep the two lists described above and include genuine user's features to the stored template we can reject features of potential impostors.

That's why we have to implement what we call second chance verification algorithm. The goal of this algorithm is to give, in the moment of verification, a classification mechanism that could speed up the template selection process and the computing rate of the false non match. This algorithm uses two authentication mechanisms *A* and *B*. Mechanism *A*, which we take as predominant, is the biometric trait that we will make all the improvements over, and *B* would only be used in case of error or rejection in verification using *A*. Mechanism *B* could be a password, an ID card or even another biometric trait (so we would have a multimodal biometric system [6]). The algorithm is so simple:

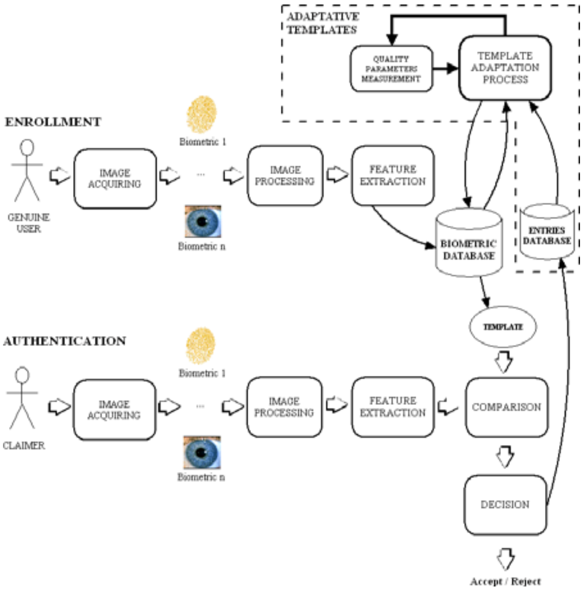

Figure 1. Working scheme of a biometric system with adaptative templates

1. *We use biometric* ***A*** *for verifying the identity of the user:*
   - *a. In case of accept by A =>*
     - *i. The access is* ***granted*** *to the user and the verification is over.*
     - *ii. The access data is stored in the list of genuine access of the user.*
   - *b. In case of reject using A => step 2.*
2. *We use mechanism* ***B*** *for verifying the identity of the user:*
   - *a. In case of accept by B =>*
     - *i. The access is* ***granted*** *to the user and this entry counts as a* ***false non match*** *for biometric A.*
     - *ii.The access data is stored in the list of genuine access of the user.*
   - *b. In case of reject by B =>*
     - *i. The access is* ***denied*** *to the user.*
     - *ii.The access data is stored in the list of access of impostor users.*

If we take a close look to the algorithm we can see the need of a second mechanism that could tell us the difference between an impostor who tries to introduce his traits in the stored templates (in an illegal way) and a genuine user that has suffered a false non match but that can be authenticated using a second mechanism. If a multimodal biometric system is used, the choice of main and secondary biometric must be rational. Logic tells us to use as mechanism *B* a more robust biometric trait, with less loss of quality in the templates but slower than biometric *A* in verification or identification process. *A* doesn't need to have a outstanding initial performance, because adaptative templates would improve error rates. In this way we could avoid the two biometric disadvantages and make the most of them.

Quality parameters measurement

The adaptative templates scheme needs a module that measures parameters and gives an idea of the global quality of the biometric features, in order to select those accesses with a quality potential better than the current stored template. The implemented system uses the following parameters for each template and user's access:

Similarity with the other users *(SO – Similarity Others)*: is the average of the similarity scores obtained in the comparison between the user and the rest of the users stored in the database and the users found in the impostor access list. The smaller the value, the more accurate is the biometric trait. A small value indicates a great distinction with the rest of the users stored in the database and potential impostors. This small similarity score doesn't overcome the threshold. Minimization of this value reduces the false match rate (FMR).

Let s(x,y) be the matching similarity score between users x and y, given N genuine users, $G_1,G_2,\ldots,G_n$, and M impostors $I_1,I_2,\ldots,I_m$, we define $SO(G_i)$ as:

$$SO(G_i)=\frac{\sum_{j=1,j\neq i}^{j=N} s(G_i,G_j)+\sum_{k=1}^{k=M} s(G_i,I_j)}{N+M}$$

Similarity with himself *(SS – Self Similarity)*: is the average of the similarity scores obtained in the comparison between the user and the different access he has made. The greater the value, the more accurate is the biometric trait. A large value indicates similarity between the different stored versions of the user's biometric trait. This large similarity score overcomes the threshold. Maximization of this value reduces the false non match rate (FNMR).

Let s(x,y) be the matching similarity score between users x and y, given N genuine users, $G_1,G_2,\ldots,G_n$, and P(i) successful and genuine access of user i, $A(i)_1, A(i)_2,\ldots, A(i)_{P(i)}$, we define $SS(G_i)$ as:

$$SS(G_i)=\frac{\sum_{j=1}^{j=P(i)} s(G_i,A(i)_j)}{P(i)}$$

Template adaptation process

This process improves stored template's quality by checking the stored biometric features for each user's access.A singularity that we must not forget is that a biometric template could use several instances or a set of features of the biometric traits (such as the 3 biometric user's fingerprints in out test) and generalizes them into a single template, or simply use a single instance and template. This fact, as we will see below, bears upon the way the biometric template is updated in the database.The process work with this algorithm:

```
For each genuine user $G_i$, $i=1,…,N$ in the database:
1. Assign quality parameters  of templates stored in
   biometric database: best_so=SO($G_i$) and
   best_ss=SS($G_i$)
2. For each genuine access $A(i)_j$, $j=1,…,P(i)$ of the $i^{th}$ user
   a. If template only uses one instance of the trait
      i.Compute quality parameters of the biometric
        features used in the access: $SO(A(i)_j)$, $SS(A(i)_j)$
      ii.If $SO(A(i)_j)$<best_SO and $SS(A(i)_j)$<best_SS
         1. Replace template stored in database with
            features in access $A(i)_j$.
         2. Assign best_SO= $SO(A(i)_j)$, best_SS= $SS(A(i)_j)$
   b. If template uses several instances of the trait
      i.Assign replaced_feature=0
      ii.For each instance or set of features $F_k$, $i=1,…,L$ of
         the stored template:
         1. Obtain generalized template $T_{ijk}$ replacing  $F_k$
            instance with features used in access $A(i)_j$
         2. Compute quality parameters of resulting
            template $SO(T_{ijk})$ and $SS(T_{ijk})$
         3. If $SO(T_{ijk})$<best_SO and $SS(T_{ijk})$<best_SS
            a. Assign replaced_feature=k
            b. Assign best_SO= $SO(T_{ijk})$,
               best_SS= $SO(T_{ijk})$
      iii.If replaced_feature>0
         1. Replace template stored in database with
            template $T_{ijreplaced\_feature}$
```

In short, it's basically a maximum algorithm whose goal is to store in the database the combination of features (template) that has given the better value of the quality parameters (low SO and high SS). The computational complexity of this algorithm is polynomial, though that's not a critical factor.

3. VALIDATION & RESULTS

In order to test the adaptative biometric templates system we have emulated a scenario similar to the one found in a small university or research center lab or in an office with confidential information. The system has been tested during a two month period using a database of 60 users, 15 of them with periodical access. The total number of accesses has been of 100, and since we use 3 fingerprints in enrolment for each user, the total number of samples is higher than 250. The alternative method of authentication used (*B*) has been password, due to its simplicity in implementation and testing.

4. CONCLUSIONS

In this paper we propose a solution to a common problem in most biometric systems, the update and selection of biometric templates in a database. The solution developed here offers a new paradigm of biometric authentication that intends to achieve two goals at a time: the evolution of stored templates with the real trait of the individual and the selection of those features that are characteristic of the individual (reducing intra-class differences) and that also differentiates him from other individuals (increasing interclass differences).

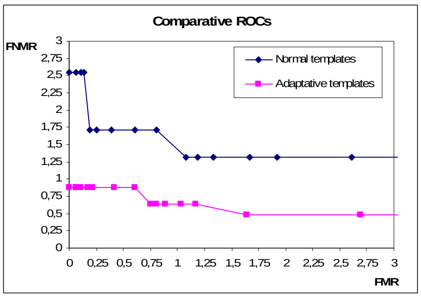

Figure 2. Comparative ROC on performance between normal and adaptative emplates

The system proposed here has been validated with real users in a university environment, obtaining successful and promising results. Furthermore, the results obtained encourages us to study this method in depth, combining it with others such as, multimodal biometric algorithms based on user-specific parameters, in order to make greater improvements, and test its performance in bigger scenarios with a higher level of access. This work has been supported by the Spanish Dirección General de Investigación del Ministerio de Educación, Ciencia y Tecnología through the TIN2004-07926 and TIN2007-67993 projects.

5. BIBLIOGRAPHY AND REFERENCES

[1] A. K. Jain; R. Bolle; S. Pankanti. *"Biometrics: Personal Identification in Networked Society"*, Kluwer Academic Publishers. ISBN 0-7923-8345-1. United States of America, 1999.

[2] R. Bolle; J.H. Cornell; S. Pankanti; N. K. Ratha; A. W. Senior. *"Guide to Biometrics"*, Springer-Verlag. ISBN 0-387-40089-3. United States of America, 2004.

[3] X. Jiang; W. Ser. *"Online Fingerprint Template Improvement"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24. United States of America, 2002.

[4] A.K. Jain; U. Uludag; A. Ross. *"Biometric Template Selection: A Case Study in Fingerprints"*, in Proc. of 4th Int'l Conference on Audio- and Video-Based Person Authentication (AVBPA). Guildford (UK), 2003.

[5] T. Scheidat; A. Makrushin; C. Vielhauer. *"Automatic Template Update Strategies for Biometrics"*, Otto-von-Guericke University of Magdeburg. Germany, 2007.

[6] A.K. Jain; A. Ross. *"Multimodal Biometrics: An Overview"*, in Proc. of 12th European Signal Processing Conference (EUSIPCO). Viena (Austria), 2004.

[7] A.K. Jain; A. Ross. *"Learning user-specific parameters in a multibiometric system"*, in Proc. International Conference on Image Processing (ICIP). Rochester, New York (USA), 2002.