THE PERSONAL IDENTIFICATION NETWORK: BIOMETRIC SIGNATURE VERIFICATION: PART II

Lee Luan Ling, Miguel G. Lizarraga

DECOM-FEEC-UNICAMP
Campinas, SP, Brasil

ABSTRACT

This paper consists in a description of biometric signature verification algorithm implemented in a biometric system via the Internet, named The Personal Identification Network. The proposed biometric signature verification approach has the following characteristics: (1) based on global/local features; (2) through a sequential, multi-expert and multi-resolution scheme; and (3) using weighted Euclidean distance classifiers, and probably the most important, (4) on-line responses and capable of detecting both random and skilled forgeries. Simulation results show the following system performance: 0.47 % false rejection error and 2.35 % false acceptance error for random forgeries; 12.75% false rejection error and 19.22 % false acceptance error for skilled forgeries. The prototype of the proposed biometric system for handwritten signatures now is implemented, operating and can be accessed via the *Web* site: http://www.lrprc.fee.unicamp.br/id.

1. INTRODUCTION

Automatic and real time personal identification for security purposes has become an important issue and has drawn much attention than ever with the advance in Electronics, computer and communication technology [1,2,3]. Particularly biometrics based personal identification has become an important alternative or complement approach to many classical and non-biometrics based methods. Biometric systems are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics, like a fingerprint or iris pattern or some aspect of behavior, like handwriting or key-stroke patterns. In this paper we describe an automatic real time signature verification method which takes part of in an Internet based biometric system. The prototype of this biometric system now is found implemented, operating and can be accessed via the *Web* site: http://www.lrprc.fee.unicamp.br/id.

The implementation of a fully automatic signature verification system is a challenging task because it is expected that the system is capable of discriminating among genuine signature, random signatures and skilled forgeries [4,5]. Besides this, in terms of signature acquisition, a signature verification system can be classified into two main categories: on-line and off-line systems. In an on-line system, signature samples in general are collected via a special electronic instrument, the so-called graphics tablet, and verification tasks are carried out in real time. An advantage of using a graphics table for capturing signatures is that some dynamic information like writing speed, applied pressure, number of strokes, etc. can be easily registered. Note that this dynamic information in general is highly discriminating and absent in off-line systems.

In off-line systems, signature samples are captured by some optical means like scanners and digital cameras and the verification is based mainly on signature´s static information, that is, relying only on a signature image. As a consequence, much dynamic handwriting information is lost and signature verification is largely based on signature morphological information and/or some derivation of this. More explicitly, some commonly deployed features in off-line systems include: global, statistical, geometric and topological types. Notice that these characteristics are not mutually exclusive. Among some widely used global features we cite transforms, image gradients, and polygonal descriptions. Statistical features in an off line system in general are derived from or related somehow with the image pixels statistical distributions. Features, like binary pressure measurements, proportionality between some statistical measurements among upper, middle, lower and initial signature zones, belong to this category. Geometrical and topological features describe the signature's local and structural properties. Examples of these are: local slope measurements, critical points, distance between successive strokes, etc.

In this paper we present a real time, sequential multi-expert and multi-resolution off-line signature verification method which deploys global/local features. The organization of this paper is as follows. Section 2 describes the signature image preprocessing procedure. Section 3 is dedicated to the signature features extraction. Section 4 defines the similarity measure used in this work. Section 5 shows in detail the implemented multi-decision strategy. Finally in Section 6 we report the performance of the proposed signature verification algorithm obtained experimentally. For a more detailed description of the proposed method, please refer to [11].

2. IMAGE PREPROCESSING

Three main operations are carried out in the pre-processing stage: signature image enclosing, normalization and frame division. The signature enclosing operation searches for the smallest box that covers the all-significant parts of a signature image. The signature size normalization operation consists of finding a suitable spatial resolution for signature representation and scaling the signature image into a standard size. The size-normalized signature image has therefore 256 pixels in width and 64 pixels in height. The signature frame division operation partitions horizontally each size-normalized signature into five partially (50%) overlapped frames. The frame division operation has the goal of isolating some significant local information. Fig. 1 shows how a signature is frame-divided.

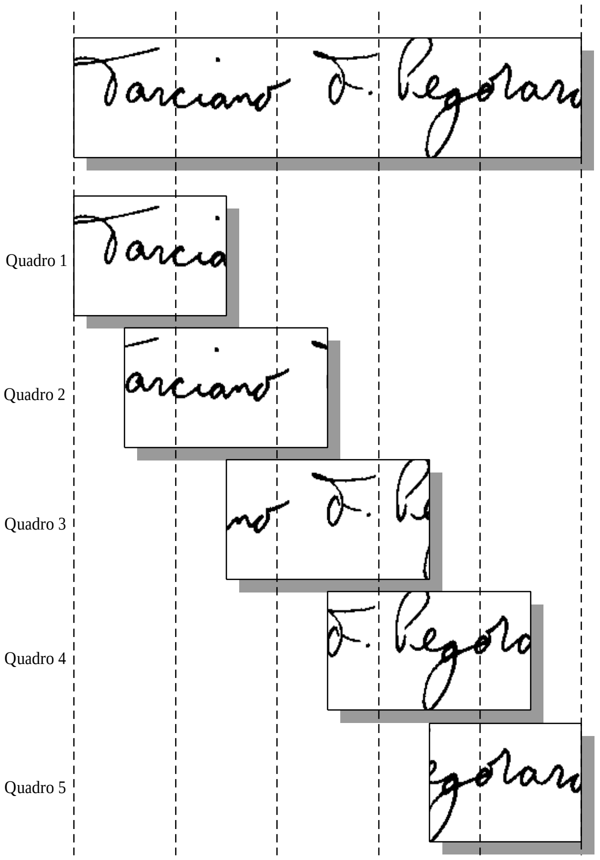

Fig. 1: An example of the frame division operation

3. SIGNATURE FEATURE EXTRACTION

In this work a collection of eight sets of features is used to represent a signature. Most of these feature sets were chosen from the literature, which were extensively employed by other signature verification systems. The first feature set basically is the one proposed by Qi and Hunt in [6], which consists of global geometric and local grid features. The second and third sets were proposed by Bajaj and Chadhury in [7], which deal with the statistical moments extracted from the horizontal and vertical projections of signature images. The fourth and fifth feature sets consist of Hu invariant moments and Tsirikolias-Mertzios moments, respectively [8]. The sixth and seventh feature sets characterize a signature via the orientation of the handwriting strokes and the orientation of the envelope of the dilated signature image [4]. Finally the eighth feature set, which is of our recent contribution, is called the correlation feature set.

Correlation Feature Vector Extraction

The image correlation is a standard approach for determining the degree of match of a sub-image *w(x,y)* of size *J* x *K* within an image *f(x,y)* of size *M* x *N*, assuming *J* ≤ *M* and *K* ≤ *N*. In other words, the correlation between *f(x,y)* and *w(x,y)* is given by

$$C(s,t)=\sum_{x=0}^{J-1}\sum_{y=0}^{K-1} f(x,y)w(x-s,y-t) \qquad (1)$$

where *s* = 0, 1, 2, . . ., *M* -1 and *t* = 0, 1, 2, . . . , *N*-1, and the summation is taken over the image region where *f(x,y)* and *w(x,y)* overlap. For any fixed pair of *(s,t)*, the application of equation (1) yields a unique value *c*. Varying *s* and *t* implies moving image *w(x,y)* around the domain of image *f(x,y)* that results in function *C(s,t)*. The coordinate that grants the maximum value of *C(s,t)* indicates the position where the image *w(x,y)* best matches the image *f(x,y)*.

Once the best match between two images *f(x,y)* and *w(x,y)* is determined; the EXCLUSIVE-OR operation is carried pixel-by-pixel between *f(x,y)* and *w(x-S,y-T)* where *(S,T)* denotes the coordinate where the best match has occurred. The correlation feature vector that measures some correlation characteristics between *f(x,y)*. and *w(x-S,y-T)* has the following entries: (1) the first element indicates the number of matched pixels between these two images, (2) the second element counts the number of pixels that do not match, (3) the third element is the size of the template image in pixels, (4) the fourth element is the size of the candidate image in pixels, (5) the fifth element is the number of black pixels in the candidate image, and finally (6) the sixth element is the ratio between the number of matched pixels and that of non-matched pixels.

4. SIMILARITY MEASURE

The following weighted Euclidean distance measure is used to evaluate the similarity between two feature vectors, that is,

$$D=\sqrt{\sum_{i=i}^{k}\frac{\left(F_{T_i}-F_{I_i}\right)^2}{s^2_i}} \qquad (2)$$

where F_{T_i} and s^2_i are the mean value and variance of the *i*th feature of the training set, respectively, and F_{I_i} is the *i*th feature value of the input candidate signature.

Notice that Equation (2) is a basic form for the measure of similarity, which can be applied directly to the correlation feature vector. When dealing with multiple frames, that includes all other kinds of feature set other than the correlation feature vector, certain adjustment is needed. In other words, the final similarity measure between two signature images is given by the sum of each individual frame-based similarity measure.

5. THE CLASSIFICATION STRATEGY

As mentioned before, the proposed signature verification method is an automatic, real time, and serial multi-expert and multi-resolution system [18]. The decision process is divided into two sequential stages. The first decision stage has the goal of detecting as many random and simple forgeries as possible while the second decision stage is designed to detect most skilled forgeries.

In the first classification stage, feature set 1, 2, 3, 4, 5 and 8 are used. Figure 2 shows how these feature sets are combined to obtain the first-stage final distance measure where *S* and *P* represent, respectively, the addition and multiplication operator. Let D_i denote the distance measure for the *i*th feature, then the first-stage final distance measure d_1 is calculated as

$$d_1 = \left(\sum_{i=1}^{5} D_i \right) \cdot D_5$$

The decision rule in this first stage is the following. If $d_1 > t_1$, then the input signature is regarded as forgery; otherwise, the decision procedure goes into the second stage classification test. Here, t_1 is the chosen decision threshold for the first classification stage.

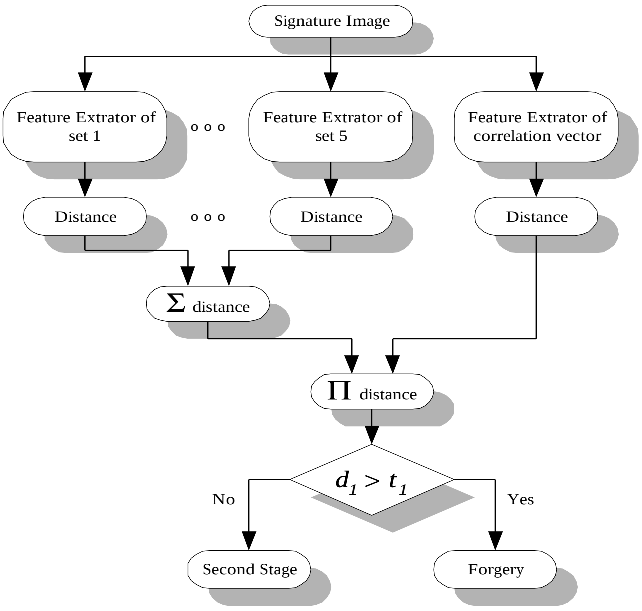

Figure 2: The first classification stage of the multi-expert classification system.

In the second classification stage the similarity measure is calculated in a similar fashion as that in the first classification stage, however using only feature vectors 6, 7 and 8. That is,

$$d_2 = \left(\sum_{i=6}^{7} D_i \right) \cdot D_8$$

In this case if $d_2 > t_2$,, then the input signature is regarded as a skilled forgery; otherwise, the input signature is declared as a genuine one. Here t_2 is the chosen decision threshold for the second classification stage.

6. SYSTEM PERFORMANCE

The signature database used to evaluate the proposed signature verification method is composed of 2500 genuine signatures, 100 random forgeries and 750 skilled forgeries [9]. The genuine signatures were collected from 50 volunteers over a six-month period, each subject contributing with his 50 genuine samples. For random forgery, fifty additional subjects were recruited, each one providing two samples of his true signature used to form the random forgery set. Finally, 750 skilled forgeries were collected based on a population of 25 distinct genuine signatures, that is, 30 forgery samples were produced for each genuine type. Visual inspection reveals that our signature database contains a large variety in signature writing style, including completely incomprehensible line strokes, Chinese and Arabic signatures and clear and neat handwriting. All these paper registered signatures were transformed into binary and 200dpi digital images. Notice that, in this work only 3 true signature samples for each genuine signature were used for the system training. We imposed this requirement of 3-sample training set in order to simulate most practical situations where only 2 or 3 signatures were saved as reference samples.

The evaluation of the system performance is done in terms of FRR_0 (False rejection rate at zero false acceptance), FAR_0 (False acceptance rate ate zero false rejection) and EER (equal error rate). Initially we evaluate each classification stage individually. Table 1 summarizes the result of this evaluation and reveals that two classification stages indeed have good discriminating capabilities for each dedicated forgery work.

Table 1: FFR, FAR and EER obtained by the single experts

Stage	FRR_o(%)	FAR_o(%)	EER_o(%)
First stage, only random forgeries	**3.82**	**2.58**	**0.97**
Second stage, only skilled forgeries	**26.62**	**32.65**	**9.72**

However, in many real situations, hardly are we able to know a priori whether a signature is a random or skilled forgery. Moreover, for most real applications, only small number of genuine samples is collected for the biometric system training. In order to set the system for real application, achieving therefore meaningful results, we impose that only 3 genuine samples be used for the system training. Next, we show how to determine decision thresholds t_1 and t_2 based only on a set of three training samples.

Determination of decision thresholds t_1 and t_2

Our approach for the determination of decision thresholds t_1 and t_2 consists of finding suitable a_1 and a_2 used in these two equations:

$$t_1 = a_1 * (D_8) * \sum_{i=1}^{5} (D_i)$$

and

$$t_2 = a_2 * (D_8) * \sum_{i=6}^{7} (D_i),$$

where D_{ii} is the distance measure for feature set i between the candidate signature and the mean value based on the reference training set. For our case, experimental investigation shows that a_1 = 1000 becomes a suitable choice to a low false rejection rate against random forgeries while a_2 = 100 is able to guarantee low false rejection rate against skilled forgeries. Table 2 shows the performances of the two classification stages using experimentally set values (a = 1000 and a_2 = 100).

Table 2: Real time results

Stage	ERR(%)	FAR(%)
First stage and α = 1000	**0.47**	**2.45**
Second stage and α = 100	**12.75**	**19.22**

7. CONCLUSIONS AND COMMENTS

In this paper we presented a real time automatic signature verification method based on a serial multi-expert and multi-resolution approach. The decision process is subdivided in two classification stages, each one carefully designed and using an adequate collection of features. The first classification stage copes with most random and simple forgeries while the second classification stage is an expert in detecting skilled forgeries. This result was benefited by dividing a signature image into a number of frames (small size images) which explore efficiently signature local characteristics.

We also contributed with a correlation feature, which measures the degree of similarity between a candidate signature and the training signature set. The performance evaluation given by Tables 2 and 3 are considered highly satisfactory once only three signature sample images were used for the signature verification system setup. Notice that the performance of our system is comparable to those systems that use in general more than 10 signature samples for the system training [6, 7, 8, 9]. Another important aspect of the proposed system is that only simple linear weighted Euclidean classifiers are used. Unlike those neural based systems, our approach does not face problems like small training sample sets, real time training and responses, quick system updating, etc. In fact, the proposed system takes only few seconds to be set up for the use. The biometric signature system via the Internet now is implemented and can be accessed via the *Web* site: http://www.lrprc.fee.unicamp.br/id. Figure 3 show the *Web* page of this biometric service.

8. REFERENCES

[1] O. Ureche, R. Plamondon. Document transport, transfer and exchange: security and commercial aspects, Proc. ICDAR 99, Bangalore, India, 1999, 585 – 588.

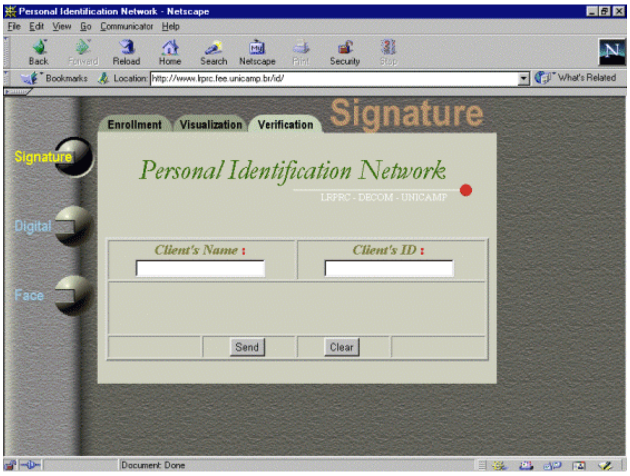
Personal Identification Network - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.lrprc.fee.unicamp.br/id/
What's Related
Enrollment
Visualization
Verification
Signature
Signature
Digital
Face
Personal Identification Network
LRPRC - DECOM - UNICAMP
Client's Name :
Client's ID :
Send
Clear
Document: Done

Figure 3: The verification service is activated by pressing ***Verification*** *tab*

[2] J. Ashbourn, Biometrics – Advanced Identity Verification, Springer, 2000.

[3] D. Zhang, 2000, Automated Biometrics: Technologies & Systems, Kluwer Academic Publishers, USA.

[4] M. G. Lizárraga, An automatic system for static signature consultation and verification, MS. Thesis, State University of Campinas –UNICAMP, 1996. (In Portuguese)

[5] R. Plamondon, S. Srihari, On-line and off-line handwriting recognition: A comprehensive survey", IEEE Trans. on Pattern Analysis and Machine Intelligence, 22, (1) (2000) 63-84.

[6] Y. Qi, B. Hunt, Signature verification using global and grid features, Pattern Recognition 27 (12) (1994) 1621- 1629.

[7] R. Bajaj, S. Chaudhury, Signature verification using multiple neural classifiers, Pattern Recognition 30 (1) (1997) 1-7.

[8] L. Cordella, P. Foggia, C. Sansone, M. Vento, Document validation by signature: a serial multi-expert approach, Proc.ICDAR 99, Bangalore, 1999, pp. 601 – 604.

[9] R. Sabourin, G. Genest, Off-line signature verification by local granulometric size distributions, IEEE Trans. on Pattern Analysis and Machine Intelligence 19, (9) (1977) 976 – 988.

[10] K. Huang, H. Yan, Off-line signature verification based on geometric feature extraction and neural network classification, Pattern Recognition 3, (1) (1997) 9-17.

[11] M. G. Lizárraga, Biometric personal identification via the Internet with emphasis on static signatures, Ph.D. Thesis, State University of Campinas –UNICAMP, August, 2000. (In Portuguese)