BIOMAC, A VERSATILE BIOMETRIC VERIFICATION MACHINE FOR ACCESS CONTROL

Renaud REITTER,Catherine ANDRE,Marie Josèphe REVILLET,Mohamed ACHEMLAL

Centre National d'Etudes des Télécommunications (C.N.E.T.)
Service d'Etudes Communes des Postes et Télécommunications (S.E.P.T.)
42, rue des coutures - BP 6243 - 14066 CAEN Cedex - FRANCE
tél: +33 31 75 92 70

ABSTRACT

The topic of this paper is a low-cost and self contained biometric verification device, devoted to physical or data access control. Because of its modularity, various means of biometric verification, as fingerprint, voice, handwritten signature, may be combined by simply plugging in special-purpose cards and sensors.

By combination, it is possible to increase the degree of security for access control, and apply it to any customer adaptations in the field of biometric verification.

INTRODUCTION

In the whole document, we have used the expression "access control" to mean physical access control, as well as data access control.

Generally, biometric access control takes place in the following way:

The user gives a biometric feature by means of an appropriate sensor. This feature can be voice, fingerprints, handwritten signature, eye retina, hand shape, etc ... Information is then digitized to be treated and compared to a pre-registered reference, which can be stored either on a smart card owned by the user, or in a data base connected to the system. If the reference and the data match, access is authorized.

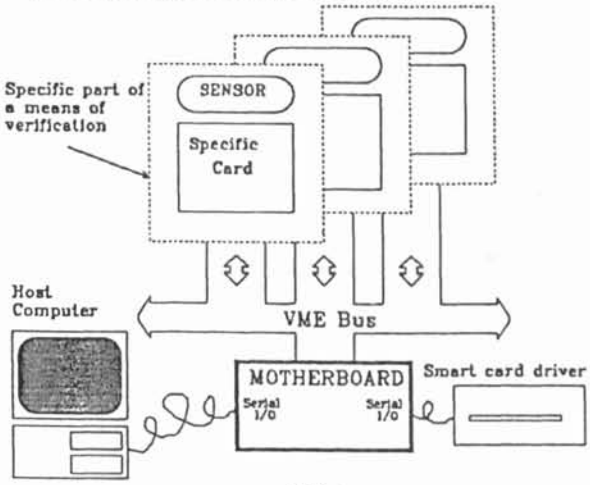
At this moment, numerous biometric verification systems already exist (ref.1). Very frequently, they use only one biometric feature, associated to a personnal identification number to improve reliability. However, not only it is a strain to have to remember a code, but occasionally the user may be not in a good condition to pass the test (loss of voice, momentary damage of a fingerprint, ocular infection, wrist wound, etc ...). In addition, the more reliable and comfortable a system must be, the more sophisticated sensors and software become, involving a fatal increase in cost and computational time.

To avoid these drawbacks, we propose a low-cost, self-contained and versatile machine which would easily combine various means of biometric verification. A first prototype has already been developed at S.E.P.T. to ensure feasibility.

This paper describes successively the basic architecture, some examples of a single mode utilization such as fingerprint, voice, handwritten signature verification, and finally basic examples of multi-mode utilizations.

1. BASIC ARCHITECTURE

The system (fig 1) is built around a motherboard based on a 68000 microprocessor. It controls the processes which are executed on specific cards. These cards have been developed to support sophisticated operations (or special-purpose devices such as sensors, digital signal processors, correlators, ...) that are required for each means of biometric verification.



- FIG 1 -

Furthermore, a video-card may be included to control fingerprint acquisition on a TV monitor. Interface between the user and the machine is reduced to an LCD screen and some function-keys. Serial ports are provided on the motherboard to interface a host computer and a smart card driver. Thus, the various references can be stored on smart cards or in a data base in the host computer.

Other specific cards can be plugged on the VME bus. For example, it is possible to include vectorial processor or transputer cards to improve computational times.

2. DESCRIPTION OF THE SPECIFIC CARDS

For each type of verification, data provided by a sensor are processed on a specific card. The process is supervised by the mother card. The architecture of the card is optimized to reduce computational time.

The three examples quoted in the following paragraphs are based on practical developments achieved at S.E.P.T.

2.1 Fingerprint Verification

2.1.1 Pattern recognition software

The software is divided in two steps: a global analysis and a detail analysis.

During the global analysis, the binarized image is divided in small squares, including at least two ridges of the fingerprint. In each square, the global direction of the lines is detected according to the following algorithm, based on some principles of mathematical morphology (ref.2).

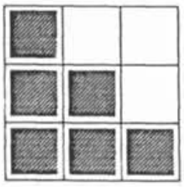
Any configuration provided by each pixel and its eight immediate neighbours can be associated to an address given by the formula:

$$A = \sum_{i=0}^{i=8} 2^i a_i$$

where a_i is the binary value of the pixel number i (fig 2).

$A = \sum_{i=0}^{i=8} 2^i \times Pi$ with P0 = 0 or 1

for the pixel P0, A = 497

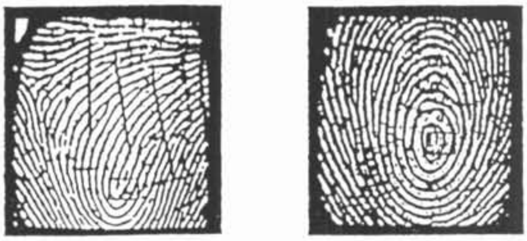


P4	P3	P2
P5	P0	P1
P6	P7	P8

- FIG 2 -

In particular, four directions, corresponding to 0°, 45°, 90° and 135° are looked for. During the scanning of the square, everytime one of the four directions is encountered, the corresponding counter is incremented, so that it is possible to build a rose-window from which a resultant vector is extracted. The direction of the vector illustrates the main orientation of the lines inside the square. Figure 3 gives an example of the tables of the coded values extracted from two different images.

The directions belonging to the 0° - 90° quadrant are coded as positive value and those belonging to 90° - 180° quadrant are coded as negative ones. In a given square the higher the value is, the more the direction of the lines is found to be vertical.



7	-1	-3	3	5	5	5	7	-7	3	-3	-3
3	-3	3	5	5	5	5	7	-7	-3	-3	-3
-3	3	3	5	7	5	5	7	7	-3	3	5
-3	3	5	5	5	5	7	7	5	3	3	5
-3	3	5	7	5	7	7	7	3	3	5	5
-5	5	5	7	7	7	7	5	5	5	5	7
7	7	7	7	7	7	7	7	7	5	5	7
9	7	7	7	7	7	7	7	7	7	7	7
-9	9	9	9	7	9	7	7	7	7	7	7
-9	9	9	9	9	9	7	7	7	7	5	7
-9	-9	9	9	9	9	9	7	7	7	7	7
-9	-9	9	9	9	9	9	7	7	7	7	7
-9	-9	-9	9	9	9	9	9	7	9	9	7
-7	-9	-9	-9	-9	9	-9	9	9	9	9	7
-7	-9	-9	-9	-9	-9	9	9	9	9	9	9
-7	-9	-9	-9	-9	-9	9	9	9	9	9	9
-7	-9	-9	-9	-9	9	-7	7	9	9	9	9
-7	-9	-9	-9	-9	-7	-5	7	9	9	9	7
-7	-9	-9	-9	-7	-5	3	7	9	9	9	7

7	9	7	7	7	5	5	3	-7	-7	-7	-9
9	9	9	9	7	5	5	-5	-7	-7	-9	-9
9	9	9	9	7	7	5	-5	-7	-9	9	-9
9	9	9	9	9	7	5	-7	-7	-9	-9	-9
-9	9	9	9	9	7	7	-7	-9	-9	-9	9
9	9	9	9	9	7	7	-7	9	-9	-9	9
-9	-9	9	9	9	9	7	-7	-9	-9	9	9
-9	-9	9	9	9	7	7	7	-7	-9	-9	9
-9	-9	9	9	9	7	7	-5	-7	-9	9	9
-9	-9	-9	-9	9	9	7	-7	-9	-9	9	9
-9	-9	-9	-9	-9	9	-7	-9	-9	9	9	9
-9	-9	-9	-9	-9	9	9	9	9	9	9	9
-9	-9	-9	-9	-9	-9	9	-7	9	9	9	7
-9	-9	-9	-9	-9	-9	-7	7	7	7	7	7
-9	-9	-9	-9	-9	-7	-5	5	7	7	7	7
-9	-9	-9	-9	-7	-5	-5	5	5	7	7	7
-9	-9	-7	-7	-7	-5	-3	3	5	5	5	7
-7	-7	-7	-7	-5	-5	-3	3	5	5	5	5
-7	-7	-7	-5	-5	-3	-1	3	3	5	5	5

- Fig3 -

From the values of the table we extract two types of information:

- firstly, the table is a good reproduction of the image highly reduced to one line per square. To give an idea, the size of the image is 168000 bytes, that of the table is 228 bytes. From the table, a series of 12 parameters is extracted and kept as the first part of the reference, which illustrates the global form of the fingerprint.
- secondly, it is possible to deduce the localization of the core in the image of the fingerprint following a very simple rule: all the fingerprints end by a series of rounded ridges which cover their core, forming a reversed "U".Locating this zone in the image is equivalent to finding, in the table, the region which represents the curve of the "U". Numerous tests on various images of fingerprints have shown that this method is invariant to translation and, to a certain extent, to rotation, seeing that the core is always entirely included in the image.

By this method, we select a window including the core in the binary image. This window is the second part of the reference, and will be used for correlation during verification.

For each verification, the global analysis process remains the same. After the twelve parameters have been extracted, a comparison is made between these parameters and those of the reference, by computing twelves distances. If one of these values is greater than a previously adjusted threshold, it means that both forms of fingerprints (the image one and the reference one) are unlike. Thus carrying the analysis into further detail is useless, since the fingerprint can be rejected at this level. If not, an area of the image is selected by the same way as above, and is compared to the detail stored in reference by successive correlations. If one of the successive results is greater than a threshold, it means that the reference detail has fit one part of the area, and the fingerprint is accepted definitively. If not, the fingerprint is rejected.

2.1.2 Specific Hardware

Specific hardware can be divided into three main parts: an optical sensor, an acquisition card and a correlation card.

The image of a fingerprint is formed by an optical sensor based on total internal reflection on a right-angle glass prism. When a finger is placed on the hypotenuse face, rays in contact with the relief of the skin (the ridges) are absorbed, creating a dark latent image of the fingerprint. The image, formed by an objective lens upon a CCD matrix sensor, is then digitized to be treated.

Special attention has been paid to the design of the optical system in order to optimize the quality of the image and the size of the sensor (nearly the size of a fist) as well. The sensor has been patented in France.

For the moment the whole process of the global analysis is implemented on the 68000.

As for the detail analysis, the correlation between the reference (64x64 bits) and the image is processed by a special-purpose device developed at S.E.P.T. allowing fast correlation. One correlation is executed in less than 0.3 ms.

2.2 Voice Verification

For speaker verification only one extension card is required. The user utters a sentence he has chosen himself. The system computes the parameters which characterize the best his voice. The result of their comparison to the reference authenticates the voice.

The vocal signal delivered by a microphone is first enhanced, filtered in a 300 - 3400 hz bandpass filter (in order to fit the frequency band of the telephonic lines) and then sampled. The digitized signal is divided into 20 ms segments. The data of each segment is treated by a digital signal processor (DSP 56000 from Motorola) which extracts time and frequency dependent parameters (i.e autocorrelation and cepstral coefficients).

The evolutions of these parameters for the whole sentence are compared to those of the corresponding ones in the reference. A distance is computed by using a dynamic programming algorithm.

At any moment the user is allowed to change his sentence. The threshold, which depends on the speaker and his sentence, is thus reevaluated.

Only about 400 bytes are required for the reference to be stored.

2.3 Signature Verification

Handwritten signature is taken from a digitizing tablet connected to a serial input on the motherboard. For this application, no specific card is required. The whole computation is executed by the 68000. To create the reference, the system needs ten genuine signatures and ten forgeries. For each signature, the system computes forty parameters which depend on the reflexes of the subject (duration of signature, writing duration, maximum writing velocity, ...). An automatic method is carried out to select about fifteen personalized parameters which can be considered as the most characteristic and distinctive ones (ref.3). This system requires only thirty bytes per user for the reference to be stored.

During the verification phase the same parameters are computed and the closeness between the signature to be verified and the reference is estimated by the distance d:

$$d = \frac{1}{n} \sum_{i=1}^{i=n} \left| \frac{p_i - p_{ri}}{p_{ri}} \right|$$

with:

n = number of parameters

p_i = value of the ith parameter for the signature to be verified

p_{ri} = value of the ith parameter for the reference.

3. MULTI-MODE USE

There is no hierachical structure between the different cards that constitute the system. The position of the specific cards on the bus is indifferent. The choice of such an architecture backs the system up in its modularity, and makes its adaptation to any future development possible (new means of verification, use of more powerful processors or algorithms, etc ...).

We can mention here some basic examples in which the system uses several biometric verification processes.

3.1. Adaptative Biometric Verification

It happens that some people are unable to use one means properly, simply because they either have bad fingerprints (skin disease), or never sign in the same way, for example. By the plurality of biometric features, it is possible to temporarily or definitively choose the means of verification that suits the user best.

3.2 Random drawing verification

Given an access with only one degree of security, the system can choose the means of verification at random. If the procedure fails, the system can either give another chance to the user, or choose a different means.

If we consider that all the false rejection rates (FRR_i) and false acceptance rate (FAR_i) associated to each means of verification i are independant, the global rates are given by the following formulae :

$$FRR_G = (1/N) \sum_{i=1}^{i=N} FFR_i$$

$$FAR_G = (1/N) \sum_{i=1}^{i=N} FAR_i$$

where N represents the number of means of verification available.

3.3 Multi-level access verification

Given an access with several degrees of security (i.e. an information system in which one part is accessible to any user and the other is reserved to those in charge of the system), it is possible to create a hierarchy among the corresponding accesses:

- access to the first level: one biometric feature is tested
- access to the second level: one more is tested, and so on.

If he wants to have access to the highest level of security, the user will have passed the previous levels.

It is also possible to associate the lowest level of security to the least powerful means of verification.

The global probability P_G for the user to pass M levels given by the formula :

$$P_G = \frac{1}{C_N^M} \sum_{\substack{i_1<i_2<..<i_M \\ 1<i_j<M}} P_{i_1}.P_{12}...P_{i_M} \quad \text{and } M \leq N$$

where P_i is the probability for the user to pass the test corresponding to the means i, N is the number of means available and M the number of levels.

In particular, if N = M the previous formula becomes :

$$P_G = P_1.P_2. .P_N$$

CONCLUSION

In this paper, we have described a first prototype of the BIOMAC system. For the moment, it combines three means of biometric verification, each of which being the result of previous research at S.E.P.T.

Verifications are carried out in a few seconds and first results are very promising.

We intend to develop a second generation system, in which the specific computation will be supported by transputers.

ACKNOWLEDGEMENT

The authors wish to thank all the people at S.E.P.T. who made a fruitful contribution to that work.

REFERENCES

1. B.L. MILLER, G.H. WARFEL, 1987 Biometric Industry Directory, Personal Identification News.
2. J. SERRA, Image Analysis and Mathematical Morphology, Academic Press 1982
3. M. ACHEMLAL, M. MOURIER, G. LORETTE, J.P. BONNEFOY, Dynamic Signature Verification, Proceedings of 4th IFIP/Sec'86, Monte Carlo.