International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:12, 2013

New Approach for Constructing a Secure Biometric Database

A. Kebbeb, M. Mostefai, F. Benmerzoug, Y. Chahir

***Abstract*—**The multimodal biometric identification is the combination of several biometric systems; the challenge of this combination is to reduce some limitations of systems based on a single modality while significantly improving performance. In this paper, we propose a new approach to the construction and the protection of a multimodal biometric database dedicated to an identification system. We use a topological watermarking to hide the relation between face image and the registered descriptors extracted from other modalities of the same person for more secure user identification.

***Keywords*—**Biometric databases, Multimodal biometrics, security authentication, Digital watermarking.

I. Introduction

DAILY, the individual needs to be identified in a variety of situations: to withdraw money from a distributor, to check his email, to ask for health and social services, to enter his property or access to the workplace, university, library... using multitudes of codes or passwords that can be difficult to remember, simple to guess and share, or ID badges and smart cards which are easy to duplicate, lost or stolen; this still remains inefficient and unsafe for identity verification [1].

In recent years, identification systems were oriented to the peculiar characteristics of each person, called the biometric data: voice, fingerprints, facial features, shape of hand, and signature.... [2]. This orientation introduced a new line of research that generated a lot of interest, although each biometric modality has its own strengths and weaknesses; none effectively meets the requirements of all applications and situations. Thus, the inclusion of various biometric modalities in identification systems can overcome some limitations of uni-modal systems and increase the precision and population coverage.

In this paper, we propose a new method for the construction of a multimodal biometric database and we use a topological watermarking module to hide the related person's files links inside the biometric database for more privacy and to ensure a more secure identification system.

II. Background

In recent years, the need for security has tremendously grown and is now critical for both individuals and governments. For that sake, considerable efforts are provided in the field of biometrics research although each modality has its own disadvantages and advantages like any other classic identification systems, most of those problems can be solved by combining several biometric modalities such as: image, voice, iris, fingerprint, signature etc… [3] to provide a higher level of security and protection. The multimodal biometric databases are one of the main factors in the success of identification systems.

The different types of biometric modalities can be classified into two categories: morphological and behavioral biometrics.

The Morphological biometrics focuses only on biometric part of the human body such as the digital fingerprint or iris while The Behavioral biometrics are those using a personal trait of behavior, as such signature. The Morpho-behavioral biometrics are related to the pattern of behavior of a person, for example the voice that is both related to the morphology the vocal cords, but also the behavior in that the voice can easily be changed by the person depending on his emotional state.

The collection of biometric data and their acquisition into the database are the most time and resource consuming tasks for the multimodal databases construction especially when these are massively including several different modalities (e.g.: MyIdea, BANACA, SDUMLA-HMT …..) [4].

In the remainder, we will explain the different steps of our method to collect the biometrics data and organize the database also the technique used to protect it and simplify the search queries within it, for a light and secure identification system at the same time.

III. Proposed Method

The construction and the protection of the multimodal databases considered as one of the most important task in identification process. In this paper we based on the following findings for the construction of our database:

- The human memory is characterized by the fact that it fills up gradually by time and becomes more and more conscious of the voices and faces to which it was previously confronted during its life. From an empty database, we begin to collect biometrics data according to the following rule:

IF (Detected_person) & (Authorized_person)
THEN Enrolled_person
ELSE Authenticated_person.

A. K., M. M., and F. B. are with the Department of Electronics, Bachir el Ibrahimi University, Bordj Bou Arreridj, Algeria (e-mail: asma.kebbeb@gmail.com, mostefaimess@gmail.com, fatehmtd@gmail.com).

Y. C. is with the computer science department, Caen University, France (e-mail: youssef.chahir@unicaen.fr).

Then, there is no more two phases (enrollment and identification) as is the case for all the classical identification systems.

On the basis of this report, identification system will be less constraining, more autonomous, and able to interact in a natural way with humans.

- Based on animal behavior and organizational patterns that exists in nature, several bio-inspired approaches are applied and have proven their efficiency and robustness to solve complex real world computational problems and in many research areas. In our system we used just the following metaphor to organize the multimodal database: "Birds of a Feather Flock Together".

We adopt a multidimensional database structure where each modality is assigned to one dimension. We are going to work on a three dimensions database to store the descriptors of the following three modalities: image, voice and signature.

Every person recorded in the database will have one specific spatial location identified by the coordinates (x, y, z) calculated in the following way:

$V_F = \{d_{F1}, d_{F2}, d_{F3} \ldots\ldots\ldots\ldots, d_{FM}\}$ for face descriptors;
$V_V = \{d_{V1}, d_{V2}, d_{V3} \ldots\ldots\ldots\ldots, d_{VN}\}$ for voice descriptors;
$V_S = \{d_{S1}, d_{S2}, d_{S3} \ldots\ldots\ldots\ldots, d_{SP}\}$ for signature descriptors.

where: V_F, V_V et V_S three vectors containing the descriptors of each modality

With: M, N and P the number of descriptors used by each modality.

The coordinates (x_i, y_i, z_i) of person i are calculated by:

$x_i = f(d_{F1i}, d_{F2i}, d_{F3i} \ldots\ldots\ldots\ldots\ldots\ldots, d_{FMi})$;
$y_i = g(d_{V1i}, d_{V2i}, d_{V3i} \ldots\ldots\ldots\ldots\ldots\ldots, d_{VNi})$;
$z_i = h(d_{S1i}, d_{S2i}, d_{S3i} \ldots\ldots\ldots\ldots\ldots\ldots, d_{SPi})$.

with $0 \leq x_i \leq X$, $0 \leq y_i \leq Y$, $0 \leq z_i \leq Z$, and X, Y, Z the maximum values of the three dimensional space

In our case (X=Y=Z=255).

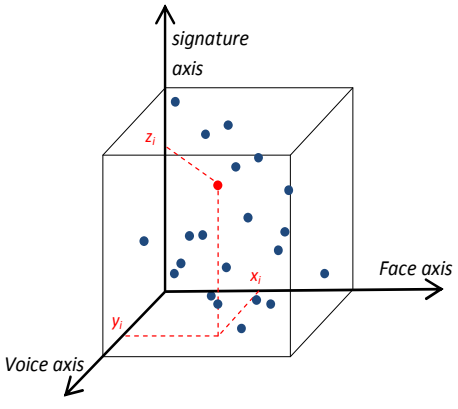


Fig. 1 Position of an individual in the base

Once the biometric data collection is completed, we obtain a group of template files necessary for each enrolled person and we can calculate their indices to specify the common spatial position (see Fig. 1).

Enrolled persons are displayed as a collection of points, where the similar people share a restricted space. This provides a real gain in terms of processing time, simplicity and reliability of similarity search.

In order to protect our multimodal database and increase the authentication accuracy, we propose a method of hiding the more specific and important identification data in our system. The data hiding method is based on digital watermarking technique, it is the process of embedding imperceptible information into the original data; in our case the key idea is to watermark an individual's face image with his 3D initial position. The chosen marking scheme occurs in the spatial domain, by utilizing a verification key. The watermark embedding is achieved by directly modifying the pixel values of the original image in one or more parts located by a topological map containing the related components of a selected cut [5].

In the other hand, we can detect any changes or attacks in our database by a simple and fast operation, we just need to extract the mark and compare it with the initial 3D position calculated using by the coordinates (x, y, z).

The watermarking process is divided in two parts, mark embedding and mark extraction (see Fig. 2).

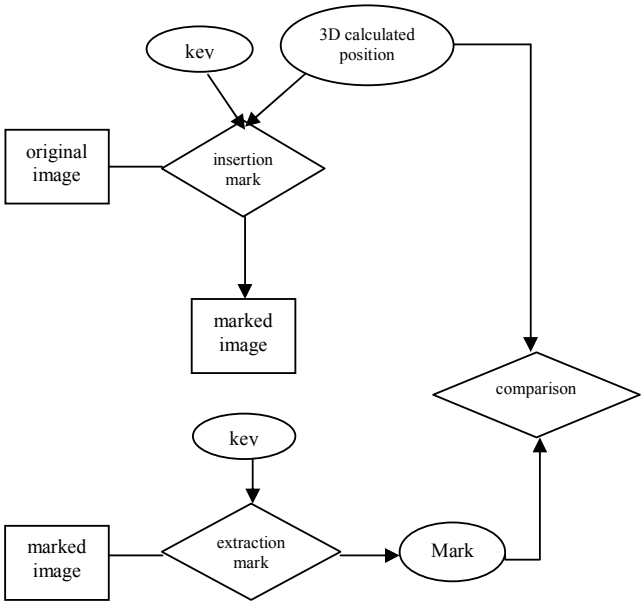


Fig. 2 Watermarking process

A. Watermark Embedding

Also known as watermark insertion, is the process of hiding secret information in the original image, the following steps have been employed in our approach:

Step 1: convert the original color image to grayscale and select the required cross section.

From the grayscale of original image and a given threshold

(K) we obtain a binary plan called cross section "cut" by the following way:

$$\text{If } P(x,y) \geq K \quad \text{then } P_K(x,y)=0$$
$$\text{Else } P_K(x,y)=1.$$

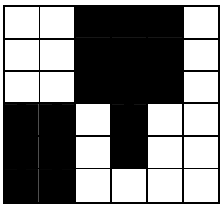
where:
P(x,y) a pixel of the image with coordinates x and y. $P_K(x,y)$ a binary pixel of the cross section K (see Fig. 3).

4	2	6	7	9	3
4	2	6	7	9	3
4	2	6	7	9	3
9	5	3	8	2	4
9	5	3	8	2	4
7	7	1	1	2	4

Portion of grayscale image

0	0	1	1	1	0
0	0	1	1	1	0
0	0	1	1	1	0
1	1	0	1	0	0
1	1	0	1	0	0
1	1	0	0	0	0

Threshold of image k=5



Cross section 5

Fig. 3 Cross Section

A grayscale image can be considered as a stacking of several cross sections and presented in topographic relief (see Fig. 4).

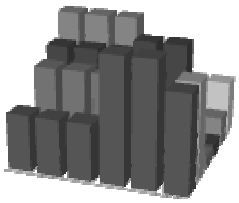


Fig. 4 Topological representation

Step 2: Locate the insertion points in the original image using the related components and the marking map.

A topological treatment is applied to the image in order to extract connected components [6]. According to their distance from the center, the insertion points are sorted (see Fig. 5).

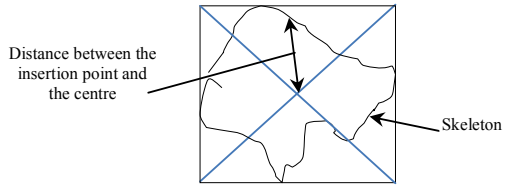


Fig. 5 Connected component parameters

These values remain unaffected by geometrics attacks in order to enhance the robustness of watermarking.

Step 3: The key generation.

According to the following parameters of insertion (Label of the related used component, Size of the mark, Selected field of insertion, Number of the marked cuts, Statistical parameters of selected marked points), the key is generated.

Step 4: Image watermarking.

The size of the embedded mark is initially of 24 bits (a coded 3D position in our biometric database), couples of blocks with this size must be formed using the insertion points. By modifying the difference of averages between two close blocks without deteriorating them, the mark insertion of one bit is made.

Considering that M_A is the average of the block A, M_B the average of the block B, and the term (Rx256) ensures a positive M_{diff} value then:

$$M_{diff} = (M_A - M_B + R\text{x}256) \bmod R.$$

Only one of the two specific values (d_0 and d_1) must be the difference result.

where: d_0 a pseudo-random number generated by the secret key K, d_1 is the sum of d_0 and $R/2$, and R is the degree of resistance against high frequency attacks (this value has an important impact on the robustness of the watermarking).

The d_0 value indicates the insertion of one "0", and d_1 the insertion of one "1".

A fixed value (μ) is added to each pixel of the block A, and subtracted from each pixel of the block B, to be in conformity with the marking rules. In case of a non-entire value, an error diffusion procedure is applied to the couple of blocks [7].

The computation rules of μ are as follows:

In the case of insertion of "1":

IF $M_{diff} < d_0$
then $M_{diff} = M_{diff} + R$
and $\mu = (d_1 - M_{diff})/2$

In the case of insertion of "0":

IF $M_{diff} > d_1$
then $M_{diff} = M_{diff} - R$
and $\mu = (d_0 - M_{diff})/2$

After the mark insertion, the selected component is labeled to indicate its marking and avoid marking it again.

B. Watermark Extraction

The process of extracting the watermark is the opposite of the watermark embedding. From the watermarked image the used cross section is extracted, the topological treatments are

carried out to define the field of insertion of the mark and to reform the blocks used for the insertion of the mark. With the secret key and the statistical parameters (d_0 and R), the mark can be regenerated.

To extract the embarked bit we follow the rule:

IF $/M_{diff}-d_1/<R/4$ ***then*** *extract "1"*
else extract " 0 "

In case the difference of the averages between two adjacent rebuilt blocks is close to d_0, the value "0" is extracted; in the contrary case one "1" is extracted.

VI. Conclusion

In this paper we propose a new efficient biometric database construction and protection scheme. The use of a 3D position matrix allows efficient and rapid localization of enrolled persons as well as a robust protection of their associated files.

The database protection is performed using a spatial watermarking scheme based on cross section topology. The insertion points of the mark are located by a topological map made up of the related components of one or more cross sections, allowing this efficient watermarking on several parts of the image.

The results of this method are the subject of our current work; we have already applied it with two dimensions (face and voice) and the results were presented in another paper, the conducted experiments so far have proved the efficiency and robustness of our method.

References

[1] Li C.T. and Hwang M.S., An efficient biometrics-based remote user authentication scheme using smartcards; *Journal of Network and Computer Applications*, 33(1), 2010, pp. 1-5,

[2] Y .Wang and Z. Liu, A Survey on Multimodal Biometrics; *Advances in Automation and Robotics*, Vol.2, 2011, pp. 387–396.

[3] Ross A., Nandakumar K. and Jain A.K., *Handbook of Multibiometrics*, Springer-Vela edition, 2006.

[4] Fierrez A.J. Ortega g. J. Gonzalez-R.J, Multimodal biometric databases: an overview; *Aerospace and Electronic Systems Magazine, IEEE*, Vol.8, 2006, pp. 29–37.

[5] Bertrand G., Everat J. C. and Couprie M., Image segmentation through operators based upon topology: *Journal of Electronic Imaging*, Vol 6, 1997, pp. 395-405.

[6] M. Couprie, F.N. Bezerra, and G. Bertrand., "Topological operators for grayscale image processing," *Journal of Electronic Imaging*, Vol.10, no. 4, 2010, pp. 1003-1015.

[7] Liu J.C., and Chen S.Y., "Fast two-layer image watermarking without referring to the original image and watermark*", Image and Vision Computing,* vol. 19, 2001, pp. 1083-1097.