Efficient multimodal biometric database construction and protection schemes.

Asmaa Kebbeb, Messaoud Mostafai, Fateh Benmerzoug, Youssef Chahir

Efficient Multimodal Biometric Database Construction and Protection Schemes

Asma Kebbeb[1], Messaoud Mostefai[1], Fateh Benmerzoug[1], and Chahir Youssef[2]
[1]MSE Laboratory, University of Bordj Bou Arreridj, Algeria
[2]GREYC Laboratory, University of Caen, France

Abstract: *This work proposes an efficient approach for the construction and the protection of a dynamic and evolutionary multimodal biometric database. The last is dedicated to a biometric authentication system operating on a set of connected sites. For a better protection of acquired data, a topological watermarking module is developed to dissimulate the related enrolled person's files links.*

Keywords: *Biometric databases, multimodal authentication, digital watermarking, cross-section topology.*

1. Introduction

Currently and for safety reasons, the majority of the governments and institutions bet on biometrics to reinforce the means to check the identity of persons. Thus, one currently attends the progressive substitution of the classical authentication systems by more powerful biometric systems. In general, the latter carry out a search for similarity between multimodal descriptors relating to the person to be identified with those recorded in advance in a multimodal database [7, 15].

The construction of the latter is often a tiresome process which requires the mobilization of a staff for the database filling with the descriptors of all the persons authorized to reach the controlled site (enrollment). These constraints in the implementation of such systems as well as related data security requirements encouraged us to propose a dynamic and evolutionary approach for the construction and the protection of a multimodal biometric database.

Inspired by the complex human discovery, memorization and authentication process [3, 13] an original approach for the construction of a self-organized multimodal biometric database is proposed. For a better protection of the acquired biometric data, a topological watermarking module is developed to dissimulate the related enrolled person's files links.

After a brief presentation of the classical biometric authentication system as well as their implementation constraints, we will detail our approach which aims at giving more autonomy to the latter by enabling them to acquire and update automatically the required authentication data. Thereafter, the adopted watermarking scheme for the protection of acquired data will be described and validated by test results. Finally, we conclude with perspectives.

2. Existing Multimodal Biometric Authentication Systems

In general, supervised sites have several distant access points which require the installation of powerful surveillance networks able to manage efficiently the whole dedicated surveillance equipment. The first systems adopted for this type of architecture were based on smart control access cards [8]. Although, they ensured efficient authentication and provided continuous historical access, the latter could not in any case guarantee that the holder of the required card was truly the owner and even if these last could integrate the photograph of the owner, the checking must be done only by a dedicated person, which is constraining and expensive.

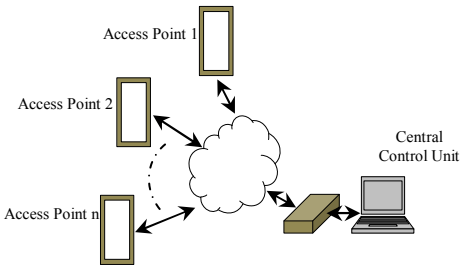


Figure 1. Working environment.

This pushed the designers of these kinds of systems to adopt an online approach which consists in performing an in-situ biometric descriptors extracting and comparison with pre-acquired (enrolled) biometric data stored initially in a dedicated database [14].

Both the type and the number of used descriptors are directly related to the chosen modalities. For performance sake, the mono-modal authentication systems were quickly replaced by multimodal authentication systems that are able to carry out a strong authentication based on the exploitation of

several modalities such as: Face, voice, iris, fingerprint, signature etc., [12].

Although, they are powerful, these systems frequently exploit and in a non-optimal way static databases (dedicated to the storage of the required descriptors). Things become more complicated if the latter is shared in network between several remote sites (our case). Indeed, besides the slowness of the access to the database, emerge the problem of the confidentiality and the security of the biometric data that are recorded and diffused via the network.

In what follows we will present our approach which aim at proposing on one hand a model of dynamic database construction allowing carrying out fast and targeted research and on the other hand, a robust watermarking scheme able to ensure efficient protection of acquired and shared data.

3. Biometric Databases Construction

Generally, the adopted process for the construction of biometric databases is based on an off-line First Come First Served principle (FCFS). Once, the database filled, it becomes operational for use in an authentication system. Often and in order to improve the research performances on such bases, one proceeds to an off-line reorganization of acquired data [12]. This constraining approach goes against the real time systems requirements which must be able to collect and to reorganize in a fluid and transparent way the data as they arrive.

If one wishes to make the authentication systems less constraining, more autonomous and able to interact in a natural way with humans, it is necessary to provide them with data collection and reorganization mechanisms inspired by those of the human ones.

The mechanism adopted for the construction of our multimodal database is based on the following findings:

- The audio-visual human memory fills progressively with time and the events with which the person is confronted to during his/her life.
- Birds of a feather flock together.

On the basis of these reports, one can consider the construction of biometric authentication systems which at the beginning of their startup do not have any enrolled person in the database. Hence, there is neither distinct enrolment phase nor authentication phase (as it is the case for the whole of the classical authentication systems), but rather of online enrollment or authentication operations. Thus, the result will be:

```
if detected person then
  if authorized to be recorded then
     Enrolment
  else
    Authentication
```

In addition, in order to have online organization of the multimodal database, the multidimensional structure (where each modality is assigned to a dimension) is adopted. For a first approach, we start with a 2D biometric database dedicated to the storage of the image and voice modalities.

Any enrolled person will have four associated files indexed according to a generated person position within a 2D memory position matrix. This last can progressively change with the arrival of new peoples. The following example (presented in next section) shows the procedure of indexing of nine enrolled persons $\{P_0$ to $P_8\}$ according to their degree of inter-similarity with the enrolled group. The adopted similarity criterion between candidates is based on hausdorff metric [5] for face modality and HMM with MFCC for voice modality [6]. The obtained inter-similarity results allow us to order the persons from the most similar (with the high score) to the least similar (with the low score). Finally, a coded index is generated to each enrolled person according to his/her 2D position.

4. Data Base Protection

Although, the relation between the affiliated person files are dissimulated, these last can be easily replaced or renamed intentionally or not, putting thus in failure the authentication process. In order to, overcome this problem it is essential to place indicators able to detect and prevent such changes.

By exploiting the advances in the field of data security, we will present in what follows the development of a multimodal database protection module founded on digital watermarking techniques. This last will allow a robust dissimulation of an embedded mark within the enrolled person face. A simple checking of this mark will permit to know if any associated person file has undergone a change or not.

Table 1. Enrolled persons faces inter-similarities results.

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
P_0	100	74	68	52	71	68	59	63	57
P_1	74	100	77	76	66	85	78	68	72
P_2	65	77	100	78	74	72	80	77	68
P_3	57	76	78	100	69	84	87	65	72
P_4	71	66	74	69	100	60	71	76	54
P_5	68	85	72	84	60	100	84	66	66
P_6	59	78	80	87	71	84	100	71	78
P_7	63	68	77	65	76	66	71	100	59
P_8	55	72	68	72	64	66	78	62	100

Table 2. Enrolled persons voices inter-similarity results.

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
P_0	78	42	34	23	36	28	25	8	20
P_1	43	88	24	13	11	27	15	23	22
P_2	17	11	74	12	24	10	19	36	29
P_3	29	12	18	80	34	32	27	26	21
P_4	28	6	12	11	86	23	16	5	21
P_5	13	36	18	17	11	76	22	11	18
P_6	16	33	23	20	33	17	83	18	21
P_7	39	39	12	22	14	33	13	88	33
P_8	26	27	27	18	23	10	33	16	72

Table 3. Enrolled persons faces ordering.

Face index	0	1	2	3	4	5	6	7	8
Score	52	62	65	57	54	56	59	59	55
New Order	P_2	P_1	P_6	P_7	P_3	P_5	P_8	P_4	P_0

Table 4. Enrolled persons voices ordering.

Voice index	0	1	2	3	4	5	6	7	8
Score	8	11	10	12	4	11	16	12	10
New Order	P_6	P_3	P_7	P_1	P_5	P_2	P_8	P_0	P_4

Table 5. New enrolled persons positions.

Voice/ Face	0	1	2	3	4	5	6	7	8
0			P_6						
1				P_1	P_3				
2									
3			P_7						
4						P_5			
5	P_2								
6							P_8		
7									P_4
8								P_0	

4.1. Proposed Method

According to the chosen modalities, any enrolled person will be represented with a group of template files necessary for any authentication operation as shown in Figure 2. These files have a common special position with which their indexes were calculated. If a change occurs on one of these files, the new position will be automatically different from the initial position. In order to detect such changes, we propose to mark the face template of the enrolled person with his/her initial 2D position. Thus, a simple mark lecture and a simple comparison with the position produced by the existing files will indicate if one of these last underwent a change or not.

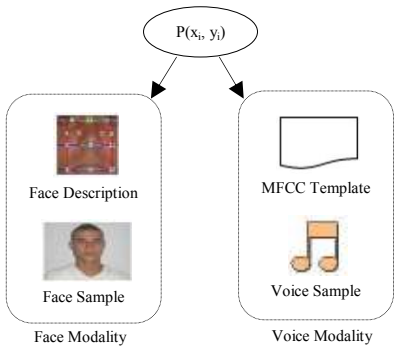


Figure 2. Enrolled person's associated files.

Figure 3. Enrolled persons sample.

4.2. Existing Watermarking Schemes

The general principle of the different watermarking techniques consist in marking work to be protected with an imperceptible signature which allows an easy authentication of the owner while being robust to attacks (malicious or not) [11]. The various watermarking systems suggested in the literature [4] can be classified in one of the following categories: Those that act directly in the space domain and those that act in the frequency domain [10]. In spite of their simplicity of implementation and computation, spatial methods are generally vulnerable to geometrical attacks. Indeed, these methods are based on the image coordinates to insert and extract the embedded mark. A simple line and/or column crop will make impossible the extraction of the mark. This is why the major people choose frequency methods to embed the mark. These last are invariant vis-à-vis the geometrical attacks. This did not slow down the interest carried to the spatial techniques, which remain by far the fastest and the simplest in comparison with frequency techniques.

5. Topological Watermarking Scheme

In our case, the chosen watermarking scheme is spatial, additive and with a secret key. It is based on the topology of the image, and allows the embedding of one or more marks in one or more parts of the image located by a topological map containing the related components of a selected cut [1].

The adopted topological watermarking scheme (presented in Figure 4) is as follow:

1. Conversion of the color image into a gray level image and selection of the required cross section.
2. Extraction of the related components and generation of the marking map (used to locate the insertion points in the original image).
3. Generation of a key with the adopted parameters of insertion.
4. Original image watermarking by following the marking map.

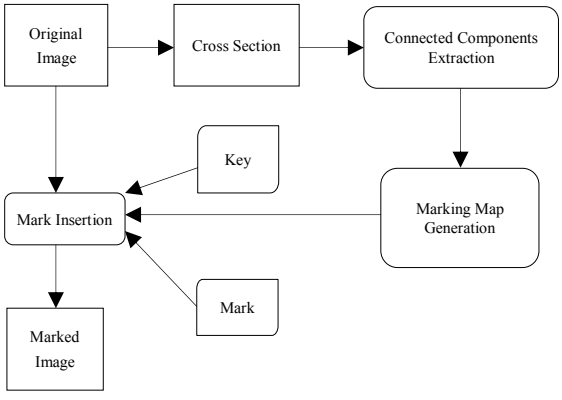


Figure 4. Topological Watermarking Scheme.

5.1. Cross Sections Extraction and Selection

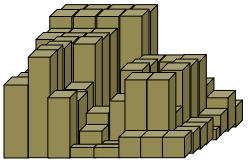
A gray level image can be considered as a stacking of several binary plans called cross sections "cuts". Each cross section is a threshold of the image on a given gray level (K). The binary values of a selected cross section are obtained in the following way:

$$\begin{aligned} &If\ P(x, y) \geq K \\ &\quad then\ P_K(x, y)=0 \\ &else\ P_K(x, y)=1 \end{aligned} \quad (1)$$

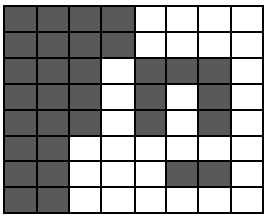
Where, $P(x, y)$ represents a pixel of the image with coordinates x and y and $P_K(x, y)$ a binary pixel of the cross section K. Figure 5 shows an example of a cross section extraction from a gray level image. Figure 5-a represents the gray level value of each point. Figure 5-b is a representation in topographic relief. Figures 5-c and d represent two cross sections of the image.

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

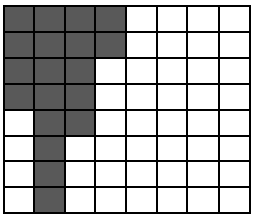
a) Portion of image.



b) Topological representation.



c) Cross section 6.



d) Cross section 8.

Figure 5. Example of cross sections.

5.2. Mark Insertion Space

Once the cut chosen, a topological treatment is applied to the image in order to extract connected components [2]. Their number and size will determine the quantity of information that could be inserted. This task is performed by a statistical module which allows the extraction and the classification of related connected components according to their center and the number of points to be used. Obtained topological map will be used with a secret key to locate insertion points on the original image.

The generation of the key depends on the following elements:

- 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.

Once the key generated, the mark is inserted following the generated topological map. In order to, improve the robustness of the watermarking against the geometrical attacks, (crop and rotation), the insertion points are sorted according to their distance from the center of the related component Figure 6. These values remain unchanged in case of geometrical attacks. A header code is added to the embedded message to indicate the reading direction during the extraction of the mark.

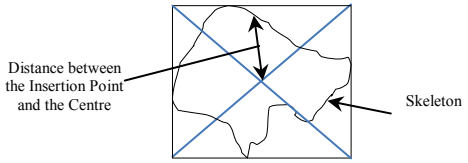


Figure 6. Connected component parameters.

5.3. Insertion of the Mark

Watermarking process consists in forming couples of blocks of fixed size using a sorted list of the insertion points. The insertion of a bit of the mark is made by modifying the difference of averages between two close blocks without deteriorating them. Obtained difference must be equal to one of the two specific values d_0 and d_1. The first value indicates the insertion of one "0" and the second the insertion of one "1".

d_0 is a pseudo-random number generated by the secret key K, whereas d_1 is the sum of d_0 and $R/2$, where, R is the degree of resistance against high frequency attacks Figure 7.

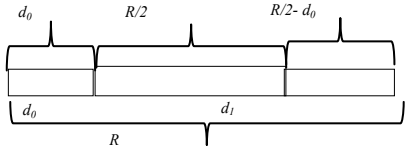


Figure 7. Relation between d_0, $d1$ and R.

Considering that M_A is the average of the block A, and M_B the average of the block B, then:

$$M_{diff}=(M_A-M_B+R\times 256)\ mod\ R \quad (2)$$

The term $R\times 256$ ensures a positive M_{diff} value. In order to, be in conformity with the marking rules a fixed value μ is added to each pixel of the block A and subtracted from each pixel of the block B. In case of a non-entire value, an error diffusion procedure is applied to the couple of blocks [9]. The computation rules of μ are as follows:

- In the case of insertion of "1", the rule is:

$$\begin{aligned} &If\ M_{diff} < d_0 \\ &\quad then\ M_{diff}=M_{diff}+R \\ &\quad and\ \mu=(d_1-M_{diff})/2 \end{aligned} \quad (3)$$

- In the case of insertion of "0", the rule is:

$$\begin{aligned} &If\ M_{diff} > d_1 \\ &\quad then\ M_{diff}=M_{diff} - R \\ &\quad and\ \mu=(d_0 - M_{diff})/2 \end{aligned} \quad (4)$$

The selected component is finally labelled to avoid marking it again.

5.4. Example of Image Watermarking

The following example Figure 8, illustrates our approach: First, we proceed to the extraction of interesting cross sections which allows the insertion of

desired mark. The cross section selection is done manually or automatically. In the first case, the user fixes the cross section to be used for watermarking; in the second case, an automatic research process is lunched to find the best suited cross section for the watermarking requirements in terms of quantity of information to be inserted. In this example, marking required the use of the cross section 102 (with K=102) which has been selected according to the size of the embedded mark which is initially of 16 bits (a coded 2 D position).

Figure 8. Example of watermarking (R=40, d_0=11).

The value of R has an impact on the robustness of the watermarking and the quality of the marked image. More this value is important more the watermarking is robust and more degradation is perceptible.

5.5. Extraction of the Mark

Figure 9 shows the mark extraction process. If the key is right, it contains all required information about the environment of insertion. After the extraction of the used cross section, 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. Knowing the statistical parameters (d_0 and R), the mark can be then regenerated. For the extraction of the embedded bit the difference of the averages between two adjacent rebuilt blocks is computed. If this difference is close to d_0, then the value "0" is extracted; in the contrary case one "1" is extracted.

The following rules are used for the extraction of the embarked bit:

If $|M_{diff} - d_1| < R/4$
then «1» is extracted
else «0» is extracted

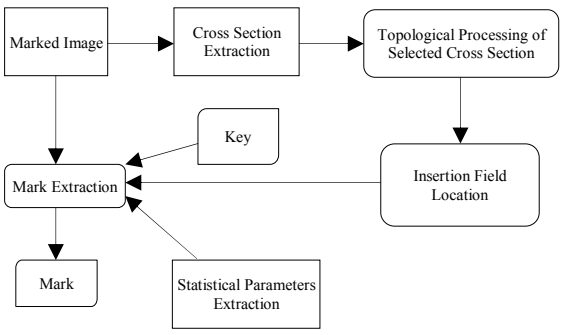


Figure 9. Extraction of the mark.

6. Tests of Robustness

In this part tests are carried out to study the robustness of the watermarking against the various signal processing attacks: Compression, filtering, noise addition and geometrical transformation (see Table 6). For compression attacks, the Mark was successfully extracted with JPEG attacks of about 50%.

Another type of attacks consists on filtering successively the marked image with a low pass filter or on adding a white Gaussian noise with a null average and a variable deviation σ. We succeeded in decoding the mark at the second iteration (for low pass filtering) and for values of σ going up to 60 (for Gaussian filtering); beyond, the mark is lost.

Traditional geometrical attacks (rotation, the mirror effects and fenestration) have also been tested. For each one of these attacks, the mark has been successfully extracted.

These experiments showed that the length of d_0 must be close to $R/4$. More precisely, d_0 Must be between $R/2$ and $R/4$, ($R/4 < d_0 > R/2$).

Table 6. Tests of robustness.

Algorithm Attacks		R=25, d_0=10	R=40, d_0=11	R=70, d_0=17
JPEG-20%		0%	0%	0%
JPEG-40%		4.17%	0%	0%
JPEG-60%		20.94%	8.44%	0%
Low Pass Filter N Iterations	N=1	16.31%	3.16%	2.34%
	N=2	Mark lost	28.17	15.76%
	N=3	Mark lost	Mark lost	Mark lost
Gaussian Filter	σ = 20	6.34%	17.25%	2%
	σ = 40	39.16%	29.12%	5.63%
	σ = 60	Mark lost	35.17	11%
Geometric Attacks	Cropping	0%	0%	0%
	Rotation			
	Mirror			

7. Conclusions and Perspectives

This article presents an efficient biometric database construction and protection scheme. The use of a 2D 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 related components of one or more cross sections, allowing thus efficient watermarking on several parts of the image.

Two improvements remain necessary in this work: The optimization of the database content update and the automation of the watermarking process. These improvements are the subject of our current work.

Acknowledgements

This work was supported by the Algerian research ministry through the PNR project (Ref: 42/TIC/2011). The used hardware and Software tools are supported by the MSE Laboratory.

References

[1] Bertrand G., Everat J., and Couprie M., "Image Segmentation through Operators Based Upon

Topology," *the Journal of Electronic Imaging*, vol. 6, no. 4, pp. 395-405, 1997.
[2] Couprie M., Bezerra F., and Bertrand G., "Topological Operators For Grayscale Image Processing," *Journal of Electronic Imaging*, vol. 10, no. 4, pp. 1003-1015, 2001.
[3] Fàbregas J. and Faundez M., "Biometric Recognition Performing in a Bio-Inspired System," *Cognitive Computation*, *Springer*, vol. 1, no. 3, pp. 257-267, 2009.
[4] Halder R., Pal S., and Cortesi A., "Watermarking Techniques for Relational Databases: Survey, Classification and Comparison," *the Journal of Universal Computer Science*, vol. 16, no. 21, pp. 3164-3190, 2010.
[5] Huttenlocher D., Klandemian G., and Rucklidge W., "Comparing Images using the Hausdorff Distance," *the IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 9, pp. 850-863, 1993.
[6] Iqbal S., Mahboob T., and Khiyal M., "Voice Recognition using HMM with MFCC for Secure ATM," *the International Journal of Computer Science Issues*, vol. 8, no. 3, pp. 297-303, 2011.
[7] Jain A., Ross A., and Nandakumar K., *Introduction to Biometrics*, Springer Publisher, USA, 2011.
[8] Li C. and Hwang M., "An Efficient Biometrics-Based Remote User Authentication Scheme using Smartcards," *the Journal of Network and Computer Applications*, vol. 3, no. 1, pp. 1-5, 2010.
[9] Liu J. and Chen S., "Fast Two-Layer Image Watermarking without Referring to the Original Image and Watermark," available at: http:// www.cis.rit.edu/ ~cnspci/ references/ liu200.pdf, last visited 2001.
[10] Mahmoud K., Datta S., and Flint J., "Frequency Domain Watermarking: An Overview," *the International Arab Journal of Information Technology*, vol. 2, no. 1, pp. 33-47, 2005.
[11] Nasereddin H., "Digital Watermarking a Technology Overview," *the International Journal of Research and Reviews in Applied Sciences*, vol. 6, no. 1, pp. 89-93, 2011.
[12] Ross A., Nandakumar K., and Jain A., *Handbook Multibiometrics*, Springer publisher, USA, 2006.
[13] Sinha P., Balas B., Ostrovsky Y., and Russell R., "Face Recognition by Humans: Nineteen Results All Computer Vision Researchers Should Know about," available at: http:// web.mit.edu/ bcs/ sinha/ papers/ 19results_sinha_etal .pdf, last visited 2006.
[14] Snelick R., Uludag U., Mink A., Indovina M., and Jain A., "Large-Scale Evaluation of Multimodal Biometric Authentication using State-of-the-art Systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 3, pp. 450-455, 2005.
[15] Yu W. and Zaiwen L., "A Survey on Multimodal Biometrics," *the Advances in Automation and Robotics*, vol. 2, no. 123, pp. 387-396, 2011.

Asma Kebbeb received her MS degree in computer science in 2009 from the University of Annaba. Currently, she is pursuing her PhD in image processing at MSE Laboratory, University of BBA, ALGERIA. Her current research involves biometric databases construction and protection, genetic and bio inspired algorithms.

Messaoud Mostefai received his PhD degree in automatic and digital signal processing from the University of Reims, France in 1995. He supervises several PhD theses in electronics and computer science fields. He is currently responsible of information theory group at MSE Laboratory. His research interests include flexible and real time embedded systems, signal and image processing algorithms.

Benmerzoug Fateh received his MS degree in network and multimedia in 2012 from the University of Bordj Bou Arreridj. He is currently the Head of Research and Development at Condor Electronics Company, His research interests include real-time 3D rendering, embedded systems (Linux, Android) and image processing.

Youssef Chahir Professor at the computer science department, Caen University, France. He is a member of the Image team at the GREYC laboratory. His research interest fields include image and video processing and analysis, multimedia data-mining, spectral analysis and restitution and animation in virtual environment.