Cancelable authentication based on fingerprints texture

Rima Belguechi[1] Christophe Rosenberger[2] Samy Ait Aoudia[1]

[1]Ecole nationale Supérieure d'Informatique ESI, Alger
[2]Laboratoire GREYC, ENSICAEN –Université de Caen– CNRS, France

r_belguechi@esi.dz
christophe.rosenberger@greyc.ensicaen.fr
s ait aoudia@esi.dz

Abstract

The challenges during the deployment of biometric systems are numerous. We have to take into account performance, privacy, security and acceptability issues. In this context, we developed an authentication system using fingerprints whose extraction phase of the representative model breaks up into two stages. In the first stage, a vector characteristic of the fingerprint image is derived by using a Gabor filterbank. A detection process of the area of interest is operated beforehand. During the second stage, the characteristic vector is plunged in a salting scheme by using a secret key K. The model thus generated is a binary vector called BioCode. Only the BioCode will be registered for the recognition which is done in a match-on-card system. The BioCode thus obtained offers an elegant solution to the mentioned problems before as our phase of tests proves it.

Keywords

Security, Fingerprint, crypto-biometrics, smartcard

1. Introduction

The biometric recognition, which consists of checking the identity of a person starting from his anatomical or behavioural attributes, offers a possible solution to the problem of authentication in the identity management systems.
Several studies expect an explosion of the biometric market in relationship to the development of the electronic transfers of data, in particular on Internet (home-bankings, etc.) The interest for biometrics is explained by the fact that it offers an ergonomic manner to authenticate or to identify a person. Moreover, it constitutes an elegant way to address the problem of non-repudiation posed by the traditional elements of authentication such as passwords or tokens. However, to place biometrics in a prospect for industrial deployment
causes several reserves, new privacy and security risks arise. Ratha et al. [1] analyzed these attacks,

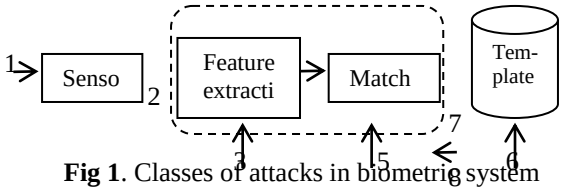


Fig 1. Classes of attacks in biometric system

We can emphasize the Fig 1. with the table bellow:

N°	Description
1	Presenting a fake biometric (e.g. gummy fingerprint [12,13]).
2,4, 7	Submitting an intercepted biometric data (replay), replacing the transmitted one, brute force attack,etc.
3,5, 8	Trojan horse attack
6	Attacking the template database (theft, abuse, etc).

Tab 1. The eight attacks description

Hence, we can see that a biometric system is prone to several threats. To prevent a fake biometric, number of efforts has been made for assuring the liveness detection of the signal [14]. Encrypted communication techniques as time-stamps [15] have been presented to thwart remote attacks. However, one of the most critical attacks remains the hacking of the biometric templates stored in the database which either may be done by the security personnel. In such situation, a potential abuse is privacy violation. For example, personal (biometric) information could be tracked from one application to another by cross-matching between biometric databases, thus compromising privacy (Imagine a case where a fingerprint template stolen from a bank's database may be used to search a criminal fingerprint database or crosslink to person's health records). Moreover, unlike password when the biometric template is compromised, it cannot be cancelled or revoked. So, question like "What can I do if my biometric data has been stolen or misused?" requires urgent attention not only to reassure users with regards to privacy but also to prevent abuses and improve accuracy.

Over the last decade, a new innovative research field has emerged, trying to find in an algorithmic way template protection schemes. The resulting systems must have the following important properties: *i) non-invertibility*, refers to the difficulty in recovering the original biometric given the secure template; *ii) revocability*, refers to the ability of generating a new template from the same biometric trait and iii) *diversity*, which is the difficulty in guessing one secure template given another secure template generated from the same biometric. Until now, the available template protection schemes are not yet mature for large-scale deployment. They don't meet properties mentioned above with keeping a high accuracy performance. In this paper, we are going to give a brief overview of those emerging technologies. For a complete survey see the reference [16]. We then present an example of a verification biometric system implemented in our recent research works.

2. Previous works

The most practical way for addressing the privacy invasion problem is to use a dual factor authentication like combining biometrics and smartcards. In 1998, Davida et al. [17] were among the first to suggest biometric based authentication systems which do not require the incorporation of an online database for the security infrastructure. An off-line biometric system is achieved by incorporating a biometric template on a storage device (such as token or smartcard). Assuming that such tokens are tamper resistant is not always true. In general, there are two main classes of physical attacks against smartcards: non-invasive and invasive attacks [18]. So, concerning the physical access application, an attacker may retrieve the data stored in memory. To provide protection against such an attack, a solution consists to encrypt the contents of memory using encryption keys which involves key management issues. Encrypting the template prior to storage can make template compromise harder. But, due to the intra-user variability over multiple acquisitions on the same biometric trait, one cannot store a biometric template in an encrypted form and then perform matching in the encrypted domain. Presently, there are quite a number of publications reporting the integration of biometrics into smartcard [19]. However, the only effort being applied in this line is to store the user's template inside a smartcard, protected with Administrator's Keys. Some are allowed to verify themselves in the card, but with degraded performance [20]. Among the commercially available biometric technologies suitable for smartcards using Match-On-Card technology, the fingerprint based systems have good performance.

The drawback of these approaches is that even though they combine biometrics with some other parameter (such as smart card, password), they cannot offer the property of revocability wanted for such authentication systems. Moreover, the comparison is always done in the biometric feature domain which makes it easier for an attacker to obtain the raw biometric data.

The concrete idea of cancelable (revocable) biometrics was firstly established by Ratha et al. [1]. This research area is growing rapidly and many new techniques have been proposed since then. These methods generally fall into two categories:

i- Biometric cryptosystems.
ii- Feature transformation functions.

In *biometric cryptosystems*, a helper data as a secret key k is combined with the template to lock the biometric set. Here, error correcting codes were designed as an alternative to deal with the intra-variation problem. Fig 2. illustrates a possible cryptosystem scheme:

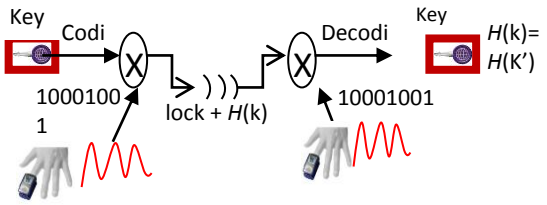


Fig 2. Example of a biometric cryptosystem

Fig. 2 presents a method proposed by Juels and Wattenberg [2], called fuzzy commitment. During the enrolment step, a word associated to a code $c \in \{0,1\}^n$ is computed given the Key **K** belonging of the user U. The biometric template for the user is represented given a sequence x containing n bits. Only the couple $(c \otimes x, H(k))$ will be saved, H being a hashing function. During the verification step, the user U gives its biometric signal x'. To verify the commitment $(c \otimes x, H(k))$, the value $(c \otimes x \otimes x')$ is computed in order to derive the value of the key **K'**. The user U is authenticated if $H(k) = H(k')$. Even if this approach does not necessitate the storage of the biometric template, it is limited to biometric data having binary representation. In 2002, Juels and Sudan [3] modified this approach in order to be used for partial representations with the name of fuzzy vault where the polynomial interpolation principle has been used. A secret (Key **K**) is a polynomial function P of degree d. During the enrolment step, the system computes one fuzzy vault V with P and the reference biometric template. The user is authenticated when it is possible to get back P from V and the fresh biometric data. The shortcoming of the fuzzy vault is the absence of any revocability scenario.

In parallel, in the feature transform approach, a transformation function F is applied to the biometric template T and only the transformed template $F(T)$ is stored in the database.

Ideally, F is a one-way function.

Ratha et al. [4] proposed three different transformations for fingerprints (Cartesian, polar, and functional). These transformations are one-way transformations in a way that it is not possible (or practically feasible) to obtain the original biometric data from the transformed data. However, the performances of the proposed systems are worse than the baseline biometric system.

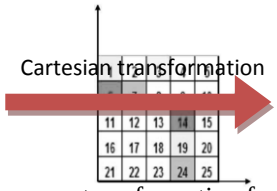
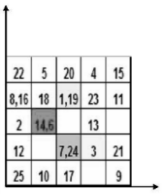


Fig 3. One way transformation function example



Using tokenized random numbers for biometric discretization is another solution proposed by Goh and Ngo [5]. By combining the high uncertainty and low entropy biometric data with user specific random data, the inherent entropy of the resulting template is increased. Another advantage of combining tokenized pseudo-random number is to obtain a cancelable biometric data. To re-issue the user identity, a specific new token needs to be issued. The authors denote this model as BioHashing. For our biometric system, we use this principle for fingerprint modality. Our interest for BioHashing is explained by its revocability property. And the use of fingerprint is related to the supremacy of this modality over the biometric market.

3. Proposal system

We have as the main objective the realization of a biometric authentication system which would join together some requirements of security. We specify these requirements by the following points:

- We need to have **a reliable biometric system** in term of error rate or verification performance.
- The biometric data must be protected from such way that it would be impossible to go back in a polynomial time to the original biometric data starting from the template. This will have an impact on **the principle of privacy.**
- We need to limit **the risks of identity usurpation** (theft, etc.), in particular, by doubling the biometric system with other means of credentials using safe devices, like a smartcard to delimit their transfer outside the secured area.
- We need to have a cancelable biometric. Indeed, it should be simple to revoke a compromised template and to re-emit a new identifier while being based on the same biometric data.

With this intention, we conceived a system whose components are illustrated on the figure bellow:

Fig 4. The strong authentication proposal system

It is a strong authentication system where the smartcard is used like a system match-on-card. The architecture of the system is summarized by the following figure:

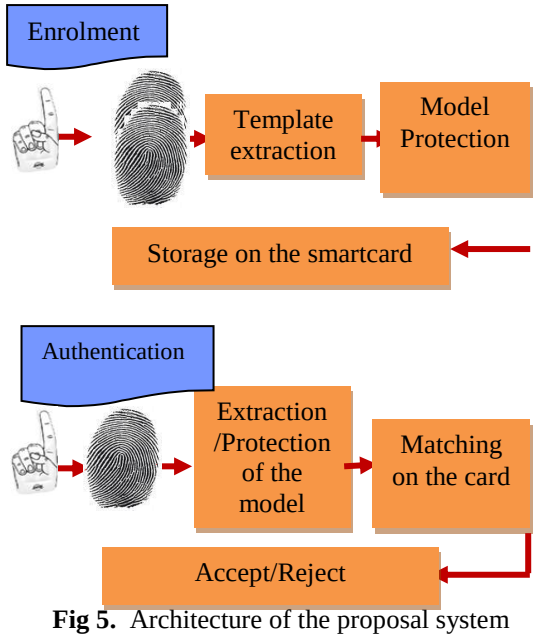


Fig 5. Architecture of the proposal system

Thus, the system breaks up into two phases: a phase of enrolment and a phase of verification or matching.

4. Enrolment phase

During this phase, the considered modality is the fingerprint of the user acquired with a liveness sensor. The 256 levels gray fingerprint image is then available on the server. Relevant characteristics in the form of *template* are therefore

extracted from this image by the extraction module. The security of this template is then reinforced by the protection module using a secret key being on the user- token.

4.1. Extraction module

A fingerprint seems as an alternate surface of ridges and valleys parallel on the majority of local regions. The minutiae details constitute the most popular representation for a fingerprint (Fig 6.). The minutiae represent local discontinuities and mark the positions where the ridges finish or fork as shown in the following figure:

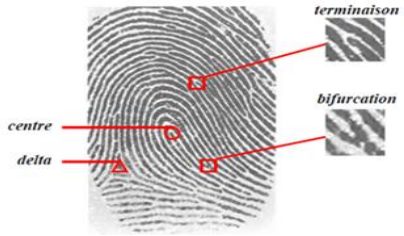


Fig 6. Minutiae representation

Our protection module imposes in entry a characteristic vector ordered and stable in size what oblige us to consider texture descriptors instead minutiae even reputed more robust (i.e. EER=1.6% vs EER=12% on the same database). Thereby, we will use a bank of Gabor filters following the algorithmic stages clarified as follows:

i. Enhancement stage

In practice, a significant amount of image is considered of average or low quality, this is generally due to: *Acquisition conditions* or *epidermal alterations*. These cases of image distortion cause matching process failure if no enhancement is applied on the raw image. Dealing of such line pattern images, noise can be expressed as breaks in the directional flow of ridges. Hence, we have used an enhancement technique based on short Fourier transform.

The algorithm proposed in [6] estimates simultaneously local orientation and space frequency of the ridges. Such contextual information has to make in advance the textured nature of fingerprint images: on a block, the gray levels of the ridges and valleys constitute a sinusoidal form along the normal direction to the orientation field (see Fig 7).

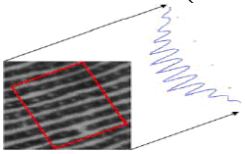


Fig 7. Gray scale projection in an oriented block

The use of contextual filters locally tuned with orientation *O* and frequency *F* is able to clean each non overlapping block. Filtering is then operated as follows:

Image enhancement pseudo-algorithm
For each block B(x,y) of size WxW **do**
1. Compute the angular filter F_a centred on the orientation O(x,y).
2. Compute the radial filter F_r centred on the frequency F(x,y).
3. Filtering the block in FFT domain: F = F x F_a x Fr.
4. Compute the enhanced block B'(x,y) = IFFT(F)
using the inverse Fourier transform.

The figure bellow shows result of this filtering:

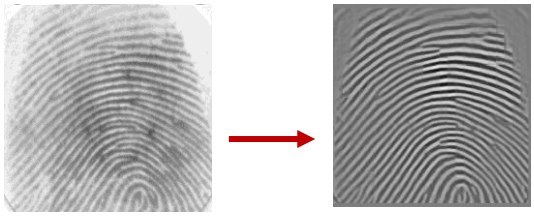
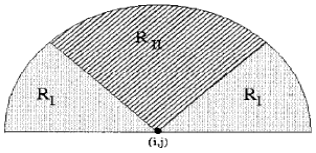


Fig 8. Image enhancement stage

ii. Region of Interest (ROI) localisation

To take into account the non-linear distortion introduced during the image acquisition, we locate on the image the core point. This central point is defined as the point of the maximum curve. The algorithm indice du poincaré defined bellow is used to estimate it:

Core point detection pseudo-algorithm
1. Estimate the orientation field O using the mean square algorithm presented in [9].
2. Smooth this orientation field with a Gaussian filtering 5x5.
3. Compute ξ, the sinus component of the orientation image *O*: $\xi(i,j) = \sin(O(i,j))$.
4. Let *A* be the label matrix initialized to 0.
For each pixel (i,j) in ξ, integrate the intensities of the pixels in the following regions R_I and R_{II} :



In such away that: $A(i,j) = \sum_{R_I} \xi(i,j) - \sum_{R_{II}} \xi(i,j)$

5. The coordinates of the maximum value in A will be those of the core point.

The region of interest (ROI) is determined by a circular tessellation surrounding the core point. This tessellation consists of *B* concentric bands of *b* pixels width. Each band is devised in 16 sectors of the same angle (22,5°) as illustrated in the figure bellow:

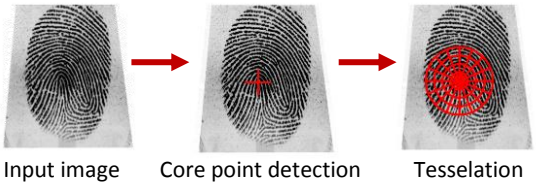


Fig 9. ROI localisation

This ROI is validated if it is in the boundary of the image and each sector *S* represents an alternation of ridges and valleys. We express this alternation by the energy *E* of Fourier spectrum so,

- If $E > T_r$ then the sector is accepted else it is rejected.

T_r is a global Otsu threshold.

iii. Attribute vector extraction

We follow the same method in [7] where the attribute vector is called FingerCode. Firstly, a normalisation step is necessary to eliminate contrast in each sector of the image *I*:

$$I(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{Var_0 (I(i,j) - M)^2}{Var}} & \text{If } I(i,j) > M \\ M_0 - \sqrt{\dfrac{Var_0 (I(i,j) - M)^2}{Var}} & \text{else} \end{cases}$$

M, *Var* are the mean and the variance of each sector *resp*. M_0 and Var_0 are fixed to 100. The FingerCode will be calculated after application of a bank of Gabor filters. It is a bank of filters since 8 directions are used:

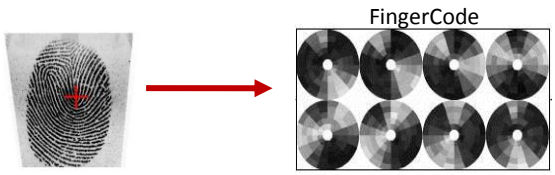


Fig 10. The FingerCode image attribute vector

The extraction is detailed by this pseudo-algorithm:

FingerCode template computation

1. Let FingerCode be an array of size: nb_sectors x nb_directions (i.e. Bx16 x 8).
2. **For** $\theta = 0$ à $7\pi/8$ **Do**

2.1. Construct the convolution matrix by using the following symmetric component of Gabor filter;

$$G(x,y;T,\theta) = \exp\left(-\frac{1}{2}\left[\frac{x_\theta^2}{\delta_x^2} + \frac{y_\theta^2}{\delta_y^2}\right]\right)\cos\left(\frac{2\pi x_\theta}{T}\right)$$

With : $x_\theta = x\cos\theta + y\sin\theta$ et

$y_\theta = -x\sin\theta + y\cos\theta$

T is the period of the sinusoid (Fig. 7), δ_x and δ_y are the standard deviations of the Gaussian envelop (This filter has selective properties in orientation and frequency what is well adapted to texture in a fingerprint).

2.2. Filter each normalised sector.

2.3. Store the value of the variance of each sector filtered in the FingerCode array.

3. Convert the values of FingerCode towards

4.2. Protection module with salting process

The FingerCode will not be stored in clear just as it is; it will be transformed by a salting process. Salting, in cryptography, is the injection of a random secret data called *salt* in a hashing function in order to increase the complexity of an attack. Because of the variations of the biometric signal, we cannot apply the traditional algorithms of salting/hashing as one would have done for a password by using for example the standard method PKCS5. To do this, authors in [5] introduce the BioHashing process. The principle of this cancelable method is to generate a BioCode from a biometric feature and a user-specific salt value (random value in order to change the BioCode after revocation). The salt value (seed) has to be stored in a secure element (USB disk, smartcard, etc.). The generated BioCode is composed f binary elements. Fig.10. illustrates the principle of BioHashing:

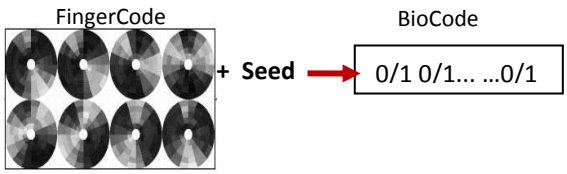


Fig 11. BioHashing for protecting the FingerCode

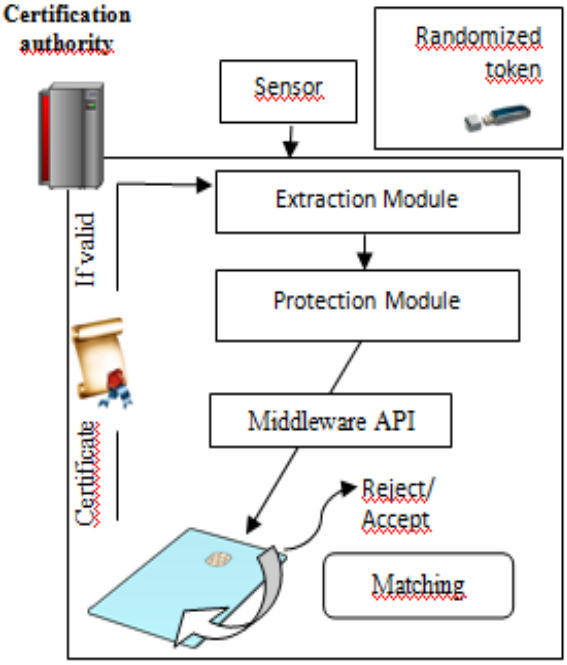
The complete process is detailed as follows:

BioHashing pseudo-algorithm

1. Let FingerCode be the biometric feature of the user *U* of length *n*.
2. Let BioCode be a vector of length *m*.
3. Let seed the salt attributed to the user *U*.
4. Generate from the seed a random matrix of size *n x m* (raw x column).
5. Apply the process of Gram-Schmidt to transform this matrix to an orthonormal set. In this case, we must have: $m \le n$.
6. Make the projection of FingerCode on this matrix:
7. Quantification of BioCode by thresholding:

$$b_i = \begin{cases} 0 \text{ si } b_i \le \tau \\ 1 \quad \text{sinon} \end{cases}$$

τ is a global threshold generally equal to à 0, $\forall\ i = 1..m$.



4.3. Storage module

The BioCode may be stored in a database. However, its compact size (*m* bits i.e. 100 bits) and the facility of comparison between two BioCodes (Hamming distance) incite us to use a match-on-card system in a javacard. We load the applet *Bio* on the card which will be personalized with the following information:

- Personal information + BioCode.
- Reference orientation computed as done in [10] since core point is tolerant to the translation but not to the rotation distortion.
- The codes PIN and PUK.
- The certificate T_u attributed to the user *U* and signed by the private key SK_{CA} of the certification authority in order to verify the issuer of the card thus preventing cloning problem.

The seed will be stored in a token with a pseudo-random generator.

5. Authentication stage (matching)

The following figure summarizes the stage of recognition:

After the code PIN verification, the card returns the certificate. If this one is validated by the certification authority, the customer on the level of the biometric terminal will introduce his fingerprint like his token. The problem of rotation is dealt by carrying out a rotation of the image according to the value: reference orientation in the card – actual reference orientation. Extraction and protection modules compute thereafter the BioCode which will be sent to the card for comparison. This comparison is done by the Hamming distance between two BioCodes, let *D* be this distance. If $D < T_s$ the user is authenticated else it is refused, T_s is a decision threshold.

6. System evaluation

Accurately with our starting objectives, we will assess the system in terms of performance and robustness to the attacks. Only theft and cloning attacks will be considered. We do not take into account the communication attacks which can infiltrate between the sensor, the card, the token and the server; we suppose that any communication is well sealed.

The performance metrics considered are:

- FTE (Fail To Enroll): It corresponds to the proportion of users who could not be enrolled in the system because the area of interest was not validated at the end of the maximum number of acquisitions (Here, fixed to 5).

- FRR (False Rejection Rate): it corresponds to the proportion of genuine access refused.
- FAR (False Acceptance Rate): it corresponds to the proportion of imposters accepted by the system.
- EER (Equal Error Rate): corresponds to the point where FRR=FAR, usually used as the value representative of the system performance.

We have two databases: the FVC2002 [21] which is a standard benchmark and a proprietary database constructed using our optical sensor (Fig 13.). Properties of the last database are:

- Image size is 355 x 390 pixels.
- The images of the people were taken on two different sessions and not efforts were made to ensure a minimum of quality acquisition.

The image contains 80 individuals and 8 acquisitions for the same finger given a total of 640 images.

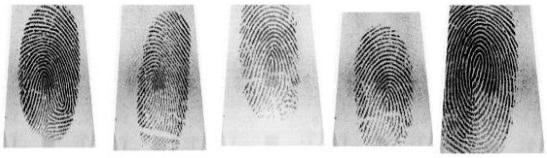


Fig 13. Images of the proprietary database

6.1. Proprietary database

At present, we clarify the results on the second database:

- *FTE*; the best result was obtained with the following parameters:

Parameters	FTE
B (number of bands) : 3 b (band width) : 20 Gabor filter size : 9x 9 Gabor filter size : 10 δ_x and δ_y : 4 R_I, R_{II} radius : 5	0,75%

- *FRR, FAR, EER* ; we use the ROC curve (Receiver Operating Characteristic) which allows to represent the performance of the couple (FRR, FAR) according to different values of the threshold T_S.

The impostor, in the client interface, has several possible scenarios:

- ***Scenario 1***: the impostor presents himself at the interface after having been able to obtain the card of the user (in addition to the PIN code) with his proper token. The ROC curve is as following :

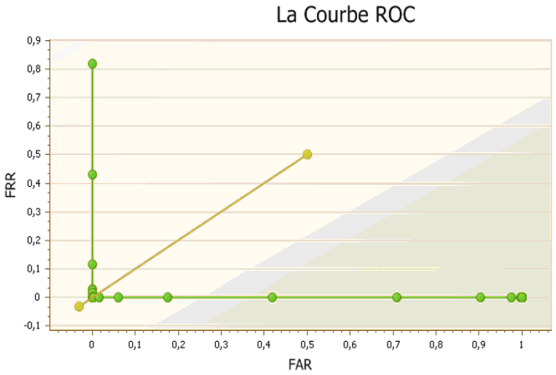


Fig 14. ROC curve of scenario 1 n=384, m=184, τ =0

We notice that after fixing parameters (quantification threshold and BioCode length) the error rate of 0% is obtained which means that a genuine user is always accepted and an imposter is always rejected; of course, this is impossible while using the sole biometric. Indeed, the ROC curve based on FingerCode is given by the following figure:

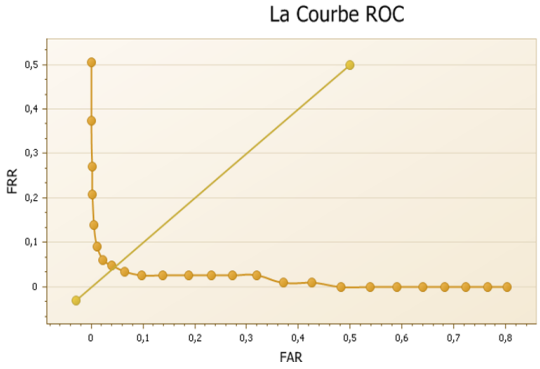


Fig 15. ROC curve of the sole biometric -based verification

- ***Scenario 2:*** the impostor presents himself at the interface by having the good token (good seed) with a not issued card. Thus, the PKI will invalidate this card.

- ***Scenario 3*****:** the impostor presents himself at the interface by having all the user credentials (card, pin and token). In this case, the ROC curve is given as follows:

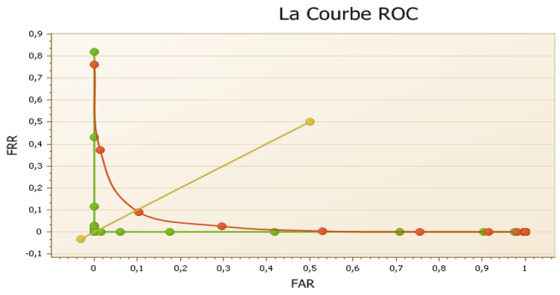


Fig 16. ROC curve of scenario 3

We notice in this scenario that the performances are weaker compared to the use of the biometric alone. By increasing the parameter *m*, we could improve the results:

m	EER(%)
184	9,71
284	8,23
384	6,78

Tab 2. Influence of the BioCode length on the performances in the case of scenario 3

Scenario 3 remains the worst of all these cases. Admittedly, the length of BioCode improves the results but it remains limited by size *n* of the biometric template, in fact the FingerCode. However, the user in the event of theft will have the possibility of revoking his credential starting from the same biometric data; it would be enough to assign a new value of the seed to him. This administrative management of the scenario after theft clearly improves the use of the biometric systems in real security applications.

For privacy protection point, we can claim that the problem is mainly solved by our system. Indeed, having the BioCode without the seed, it is very complex to recover the original FingerCode. Having the seed and the BioCode, it becomes commonplace to get a FingerCode close to the initial one but the protection of BioCode by the system match-on-card never allows its migration out of the card which handicaps largely this type of attack.

6.1. FVC2002

We have also tested our system on database DB2 of the FVC2002 benchmark. This public database contains 800 images (80 individuals with 10 acquisitions for each one).

We compare in Tab 3. our system called S1 with a reference method presented in [11] which we call S2.

	EER(%)	m
S1 sans vol	0%	384
S1 avec vol	**8,44%**	384
S2 sans vol	0%	100
S2 avec vol	**15,5%**	100

Tab 3. Comparaison de notre système S1 avec une méthode de référence S2

We notice that in S1, the size of BioCode *m* is larger than in S2 thing that improves the result. The guarantee of *m* with 384 bits for all the enrolled images in the system, is supported by our method of ROI validation.

7. Conclusion

We developed a biometric authentication system adapted to the requirements of security and privacy in such way that it will benefit of the public acceptability. Most of this work dealt with the extraction of the biometric model. This extraction which relies on the detection of the central point was clearly made reliable by the enhancement process. To protect the extracted model, a transformation function was used based on a salt. The salt is a user specific secret number which in best case involves 0% error rate. Moreover, this system ensures the revocability property. However, the weakness inherent of this system remains palpable when an impostor is in possession of all the user credentials. The salting transformation becomes reversible end the privacy will be threatened. On the other hand, our solution of a match-on-card system will continue to protect this right to privacy. As regards to the performance problem, we are currently working this axis while trying to exploit several tracks: the length of BioCode conditions the performance of the system; it would be necessary to imagine mechanisms to increase it like the fusion of several fingers. Minutiae are more reliable than texture descriptors, in [8] we developed a robust minutiae extraction approach, we expect in future to use this template information.

Reference

[1] N.K. Ratha, J.H. Connelle, R. Bolle. Enhancing Security and Privacy in Biometrics-Based Authentication System, *IBM Systems J.*, vol. 40, pp. 614-634, 2001.

[2] Juels and M. Wattenberg. A fuzzy commitment scheme. *Proceedings of the 6th ACM conference on Computer and communications security*, pp.28–36, 1999.

[3] A. Juels and M. Sudan, A fuzzy vault scheme. *Proc. IEEE Int. Symp. Information Theory*, 2002.

[4] N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle, Generating cancelable fingerprint templates. *IEEE Trans on PAMI*, Vol. 29, pp. 561-572, 2007.

[5] A. Teoh, D. Ngo, A. Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 2004.

[6] S.Chikkerur, N.Cartwright, V. Govindaraju, Fingerprint image enhancement using STFT analysis, *IEEE Proceedings in ICAPR*, pp. 20-29, 2005.

[7] A.K. Jain, S. Prabhakar, L. Hong, S. Pankanti, Filterbank-based fingerprint matching, *IEEE Trans. Image Process*, Vol 5, pp. 846–859, 2000

[8] R. Belguechi, C. Rosenberger. A Minutiae level fusion for AFIS systems. *European Signal Processing Conference (EUSIPCO)*, 2009.

[9] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar. *Handbook of Fingerprint Recognitio.* Springer, New York, 2003.

[10] M. Liu, X. Jiang, A. Kot. Fingerprint reference-point detection. *AURASIP Journal*, 2005.

[11]A. Lumini, L. Nanni. An improved biohashing for human authentication. *pattern recognition journal*, 2006.

[12]T. Matsumoto, H.Matsumoto, K.Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. *Proc. of SPIE*, vol. 4677, pp. 275-289, 2002.

[13]R. Cappelli, A. Lumini, D. Maio, D. Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Trans. PAMI*, 2007.

[14]A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni. Fake finger detection by skin distortion analysis. *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 3, pp. 360–373, 2006.

[15]K. Lam and D. Gollmann. Freshness assurance of authentication protocols. *Proceedings of the European Symposium on Research in Computer Security (ESORICS '92)*, pp. 261–272, 1992.

[16] A.K. Jain, K. Nandakumar, A. Nagar. Biometric template security. *EURASIP journal on advances in signal processing*, 2008

[17] G.I. Davida, Y. Frankel and B. Matt. On Enabling Secure Applications through Off-Line Biometric Identification. *Proc Security and Privacy*, 1998.

[18] M. Kuhn, R. Anderson. Tamper resistance: A cautionary note. *Workshop on Electronic Commerce*, 1996.

[19]Y. Isobe, Y. Seto, M. Kataoka. Development of personal authentication system using fingerprint with digital signature technologies. *Proc. System Sciences*, 2001.

[20] R. Sanchez-Reillo. Including biometric authentication in a smartcard operating system. *AVBPA*, 2001.

A. FVC 2002, http://bias.csr.unibo.it/fvc2002/