Enhancing the privacy of electronic passports

Rima Belguechi, Patrick Lacharme, Christophe Rosenberger

Enhancing the privacy of electronic passports

R. Belguechi

National School of Computer Science,
ESI, Algeria
Fax: 213021516156
E-mail: r_belguechi@esi.dz

P. Lacharme

GREYC Research lab,
ENSICAEN - Université de Caen Basse Normandie - CNRS,
14000 Caen, France
Fax: +33 231538110
E-mail: patrick.lacharme@ensicaen.fr

C. Rosenberger

GREYC Research lab,
ENSICAEN - Université de Caen Basse Normandie - CNRS,
14000 Caen, France
Fax: +33 231538110
E-mail: christophe.rosenberger@ensicaen.fr

Abstract: We address in this paper the problem of privacy in the current architecture in electronic passports for the storage and transmission of biometric data such as fingerprints. The current architecture provides a good protection of biometric personal data but brute force attack could be used in a near future using cloud computing. We propose a new solution combining cryptographic protocols and cancelable biometrics. The indivdual's biocode in protected by cryptographic keys exchanged by the PACE protocol. We put into obviousness the benefit of the proposed solution in terms of security and privacy.

Keywords: Electronic passport, cancelable biometrics, privacy, cryptographic protocol.

Reference

Biographical notes:
Rima Belguechi is a PhD student at ESI, Algeria. She obtained her Master in 2006 from the national school of computer science at Algiers. She is working under the supervision of Pr. C. Rosenberger in cancelable biometrics to achieve a better privacy for biometric verification systems.

Patrick Lacharme is an assistant professor at ENSICAEN, France. He obtained his Master of Science in 2002 and its Ph.D. degree in 2007 from the University of Toulon. He works at the GREYC laboratory. His reasearch interests concern privacy in electronic transactions.

Christophe Rosenberger is a Full Professor at ENSICAEN, France. He obtained his Master of Science in 1996 and its Ph.D. degree in 1999 from the University of Rennes I. He works at the GREYC laboratory. His research interests include computer security and biometrics. He is particularly interested in authentication methods for e-transactions applications.

1 Introduction

Secure and privacy preserving management of our digital identities in the constantly evolving numerical world is of paramount importance for citizens, industries, social groups, and governments. Numerous applications are emerging related to physical access control (buildings, restricted areas, customs, ...), logical access points (bank accounts, e-commerce, tax payments...) or

identity documents (passport, national identity card. . .).

In order to achieve more secure systems, biometrics technology is employed in an increasing manner in order to verify the identity of an individual (i.e. to perform an authentication) or to determine his identity (i.e.dentification tasks). The major reason for this widespread usage of biometrics is that this technology provides the strongest proof of the physical identity of a person. Indeed, the relationship between the individual and its identity credentials

cannot be more important. Biometric modalities available in the literature can be classified in three broad categories:

- Biological characteristics such as, DNA, cardiac signals as proposed by (3) . . .
- Behavioral characteristics such as, online handwritten signature, voice, keystroke dynamics (1) . . .
- Morphological characteristics (the most widely employed) such as fingerprints, face, iris, hand veins (2) . . .

However, with more and more applications using biometrics, new privacy and security risks arise. For example, personal biometric information could be tracked from one application to another by cross-matching between biometric databases, thus compromising privacy. A crucial issue is the potential misuse of collected biometric data. Questions like "What can I do if my biometric data has been stolen or misused?" require urgent attention not only to reassure users with regards to privacy intrusion but also to prevent misuse and improve accuracy. Moreover, since standard biometric templates are permanently associated with an individual, they could not be used anymore in case they are compromised. Since they cannot be replaced, they are also inherently non revocable. This makes "classical" biometric systems inappropriate for privacy and security critical applications. Therefore, these major issues should be solved urgently.

The idea of of a biometric electronic passport has been done after terrorism attack on September 11th in 2001. Since October 26th in 2006, it is required to enter the US. The number of countries that deliver a biometric passport is near 90. Most of European countries deliver it following the Schengen agreement. The number of biometric passports in the world is estimated to 100 millions. Even if the security of electronic passports is very good, some attacks are possible such as brute force to break a confidential transmission between the chipset and the terminal. Considering the fact a biometric information is not intrinsically revocable, some risks still remain.

Over the last decade, a new innovative multidisciplinary research field has emerged, that combines biometrics and cryptography. It has the capability to guarantee biometric data privacy in an algorithmic way. The resulting innovative hybrid systems have the following important properties: they confer to biometric characteristics the needed capabilities of revocability, privacy, and diversity, and provide cryptographic systems with a strong link to the user through biometrics. We propose to use this technology through the definition scheme for fingerprints privacy preserving for the protection of biometric information in the electronic passport.

In section 2, we present the different mechanisms that exist to guarantee the security of an electronic passport. Section 3 presents the proposed method after showing the state of the art in this domain. Section 4 presents some experimental results and a security analysis showing the benefit of the proposed solution. We finally give some conclusions and perspectives of this work.

2 Electronic passport

The International Civil Aviation Organization (ICAO) presented in 2004 a guideline proposing a set of specifications for Machine Readable Travel Documents (MRTD) (11). This specification is used as standard for a majority of countries for the first generation of electronic passports. It includes several cryptographic protocols to ensure authenticity, security and privacy of personal data. Later, European Union proposed in 2006 a new mecanism called Extended Access Control (EAC), to provide better security on personal data of the document (9). EAC suite concerns the second generation of electronic passports. This suite presents a new PKI infrastructure and new cryptographic protocols.

2.1 Personal data

Electronic passports have an integrated chip, generally embedded in the cover page of the document, that contains personal information and biometrics data on the document owner. Biometrics information are used to have a more secure identification on the document holder than for previous passports. Additionally, a contactless (or RFID) technology has been chosen for the inspection process.

According to ICAO first specification, the choice for biometrics data is the digital facial image of the owner, and other biometrics data are optional as fingerprint data or iris scan. Nevertheless, facial images are not considered by ICAO as sensitive biometrics informations. Moreover, fingerprint data are mandatory for European Union passports since 2009.

In ICAO specification, the memory of the chip is composed of 16 data groups namely DG1,.., DG16, which correspond to the standardized Logical Data Structure (LDS). This data structure is divided in the following way :

- DG1 is a digital copy of the Machine Readable Zone (MRZ) of the electronic passport.
- DG2 is a digital picture of the face of the owner (in jpeg or jpeg2000 format).
- DG3 is composed of fingerprint data.
- DG4 is reserved for iris scan.
- DG14 and DG15 are used for public keys.

Moreover, the hash of all these data groups are stored in the Security Object of the Document(SOD) zone, and all these data are digitally signed by the issuing country. Finally, the chip contains additional information as private keys, stored in a secure section of the memory.

Fusion of RFID and biometrics technology is important in electronics passports, particulary for privacy considerations.

Following ICAO specification, the contactless chip is conform to the ISO 14443 norm, which is the standard for proximity contactless chip and specifies a radio frequency of 13,56 MHz (12). These chips are subject to classical attacks on contactless technology :

- Eavesdropping attacks : an attacker eavesdrops on a legitimate communication between the passport and a reader.
- Scanning attacks : an attacker communicates with the chip without the consent of the passport holder, using a false reader in proximity to the passport.

Other vulnerabilities on electronics passports using contactless technology are numerous (but not described in this paper). For example, a relay attack is developed by Hlavac and Rosa on Czech passport in (10). Chotia and Smirnov presented in 2010 a method for tracking the passport holder (7) and Richter, Mostowski and Poll show how to detect the presence of a passport and to retrieve its nationality, (16).

Eavesdropping attacks and scanning attacks can be used to retrieve data stored in the memory of the tag without the content of the passport owner, even for sensitive data such as biometrics data. Consequently, an access control protocol and a secure communication channel are necessary.

2.2 Secure access

The first ICAO standard specification of 2004 includes three cryptographic protocols, where only the first was mandatory (11) :

1. Passive Authentication is used to verify the authenticity of the data in the memory of the chip, with a control of the signature of all data of the chip.
2. Active Authentication is used for the authenticity of the chip himself, which must prove the knowledge of a private key used in a challenge-response protocol.
3. Basic Access Control (BAC) is used to prevent unauthorised access and scanning attacks. BAC protocol produces also a session key, used to prevent eavesdropping attacks.

Passive and Active Authentication protocols are not described in this paper, because they concern authenticity of the data in the memory of the passport and the passport himself and are out of scope of this paper. A precise description of these protocols can be found in (14).

In the Basic Access Control protocol, the reader proves to the passport that he knows informations of the MRZ zone which are visually printed in the first page of the passport. These informations are read by OCR (Optical Character Recognition) scanner. Then, an acces key K is directly derived from these data by the reader, using the 128 most significant bits of the hash function Sha-1, by

$$K = 128\text{msb}(\text{Sha-1}(\text{MRZ})).$$

Then, two keys of 128 bits K_{enc} et K_{mac} are derived from K (where $||$ means concatenation) :

$$K_{enc} = 128\text{msb}(\text{Sha-1}(K||1)),$$

$$K_{mac} = 128\text{msb}(\text{Sha-1}(K||2)).$$

These two keys are also contained in the memory of the chip and are used in a challenge/response mechanism with a 3-DES encryption (denoted Enc in all this paper) and a ANSI MAC with the following algorithm :

1. The chip generates a challenge C_c of 64 bits and sends it to the reader.
2. The reader generates two words K_r and C_r of 64 bits, and computes with K_{enc} and K_{mac}

   $$\text{MAC}(\text{Enc}(C_r||C_c||K_r))||\text{Enc}(C_r||C_c||K_r),$$

   and sends it to the chip.
3. The chip retrieves the challenge C_c and extracts the key K_r. The chip generates a key K_c of 64 bits and sends to the reader the quantity

   $$\text{MAC}(\text{Enc}(C_c||C_r||K_c))||\text{Enc}(C_c||C_r||K_c).$$

4. The reader retrieves the challenge C_r and extracts the key K_c.

5. The reader and the chip compute the new session keys with $K' = K_r \oplus K_c$ and

$$K'_{enc} = 128\text{msb}(\text{Sha-1}(K'||1)),$$

$$K'_{mac} = 128\text{msb}(\text{Sha-1}(K'||2)).$$

The aim of the BAC protocol is to ensure that only someone who has seen MRZ informations can access to the data of the chip. The reader directly derives the keys K_{enc} and K_{mac} used in the protocol with the knowledge of MRZ data.

The session keys K'_{enc} and K'_{mac} are used to establish a secure communication channel between the passport and the reader to prevent eavesdropping attacks.

The new suite of cryptographic protocols called *Extended Access Control* of European Union proposes to replace Active authentication by a new protocol, called chip authentication (not described here).

A new protocol is also specified for terminal authentication. This protocol means that the reader must be authenticated by the passport as a valid reader before the access of biometrics data. For this purpose, a PKI architecture is used, including country verifying certificate authorities, document verifiers and inspection systems. This infrastructure is hierarchical, which means that each country sign all document verifiers certificates and each document verifiers sign inspection system certificate. At each control, the passport must verify that the reader has a valid certificate. More details on this PKI architecture can be found in (15). Later, Pasupathinathan, Pieprzyk and Wang analyzed in 2008 the Australian electronic passport, and reported several flaws in the EAC suite (15). Authors presented a new protocol, called OSEP, where they propose to execute the terminal authentication protocol before the chip authentication protocol. Finally, Abid and Afifi modified this protocol using elliptic curves (4).

Consequently, the German organism BSI realized a new specification in 2008 for a new version of EAC, called EAC Version 2 (6). This specification proposes to execute the terminal authentication before the chip authentication as in the OSEP protocol. It contained also a new protocol for access control, called PACE protocol (6) to replace BAC protocol.

The PACE protocol works in two independent times in the following way : firstly, the reader reads a specific data on the passport with an OCR scanner. This data is a random number π which is independent to personnal data of the passport owner. This number π must have enough entropy to avoid a brute force attack. In a second time, the reader and the passport realize a key exchange protocol to derive a common secret. This protocol can be the standard Diffie-Hellman protocol, or the elliptic curve key exchange protocol. In both cases, the key exchange protocol is denoted KA and the domain parameters are denoted D_c, as notations of (6). Finally, a session key is derived from this common secret, using the following algorithm :

1. The chip generates a challenge R_c, computes the key $K_\pi = \text{Sha-1}(\pi||3)$, encrypts the challenge R_c with the key K_π in z and sends it to the reader with domain parameters D_c.

2. The reader computes the key $K_\pi = \text{Sha-1}(\pi||3)$ with the knowledge of the number π, decrypts z with the key K_π and retrieves the challenge R_c.

3. The chip and the reader compute the ephemeral domain parameters D' with the challenge R_c and the domain parameters D_c.

4. The chip and the reader compute a common key K using the key exchange protocol KA on the new ephemeral domain parameters D' : in a first time, the chip and the reader generate respectively two public and private key pairs $(PuK_{c,pace}, PrK_{c,pace})$ and $(PuK_{r,pace}, PrK_{r,pace})$, then they obtain a common key K by computing

$$K = \text{KA}(PrK_{c,pace}, PuK_{r,pace}, D')$$

$$= \text{KA}(PrK_{r,pace}, PuK_{c,pace}, D').$$

5. The chip and the reader compute the session key :

$$K_{enc} = 128\text{msb (Sha-1}(K||1)),$$

$$K_{mac} = 128\text{msb (Sha-1}(K||2)).$$

6. The chip and the reader realize a mutual authentication protocol as following. The reader computes and sends its authentication token $T_r = \text{MAC}(K_{mac}, PuK_{c,pace})$ to the chip. The chip computes it and verifies the token T_r.

   The chip computes its authentication token $T_c = \text{MAC}(K_{mac}, PuK_{r,pace})$ and sends it to the reader. The reader computes it and verifies the token T_c.

2.3 Discussion

Many works in the analysis of the BAC mechanism have been reported. One of the first security analysis is presented by Juels, Molnar and Wagner in 2005, where several flaws where identified (13).

Data of MRZ concern precisely the date of birth of the holder, the passport number and the expiry date of the passport. Firstly, informations of MRZ can be directly read on the passport by someone or partially known (for example, the date of birth of the passport

owner is maybe on the web). Moreover, the entropy of MRZ information is very low, especially for country generating passport number in sequence. Possibility of brute force attacks on BAC mechanism was clearly presented on many passport as Belgian, Dutch or German passports (5).

The PACE protocol corrects the main weakness of the BAC protocol. This protocol is *a state-of-the-art passsword-based access control resisting active attacks* (8). More precisely, the security of the mechanism is based on two points : firstly, there are no reasons to use personal data printed on the MRZ zone as a shared secret between the reader and the passport. The entropy of a (true) random number is not overevaluated. Secondly, the generation of the session key uses a public-key crypto-system (and not a symetric crypto-system where the secret key is written in the MRZ of the passport), realized independently to the first phase of access control.

Unfortunately, several flaws have been reported in this new specification by Chaabouni and Vaudenay in (8). The RFID tag has no internal clocks and can not receive revocation list of reader. This means that the electronic passport considers date with the information received from reader the last time the passport is controlled, and compares it with expiration date of reader. As a consequence the terminal authentication of the EAC suite can be realized successfully by a reader with expired certificate.

Authors identify also an other weakness in the specification of (6). According this specification, *if compatibility to ICAO is required, the passport shall grant access to less sensitive data to terminals authenticated by Basic Access Control.* Therefore a false reader can require the passport to use BAC protocol with all its weakness.

More generally, the number π is just printed on the passport and consequently can be retrieved by social engineering or directly read on the passport in the case where the electronic passport is stolen. In this case, an attacker with a fake reader can execute successfully the PACE protocol. Therefore a reader executing successfully the terminal authentication protocol (maybe with an expiree certificate) has access to all sensitive data.

Finally, it will be maybe possible in the future to access physically to data in memory of the chip even if, to our knowledge, nobody has presented a method to do this. However, it is not possible to change raw biometrics data if they are compromise. In this conditions it is important that raw biometrics data are not directly stored in the memory of the chip.

3 Proposed method

We put into obviousness the risk due to the protection of biometric templates with cryptographic keys. The proposed solution to this problem is to embed a cancelable biometric template of an individual in its electronic passport. We describe in the next section the general principle of the proposed solution for both of the enrolment and verification steps.

3.1 Principle

Figure 1 details the general scheme for the enrolment and verification steps. Note that the proposed enrolment scheme can be used for the update of the biocode (cancelable biometric template). Instead of storing a JPEG image of the fingerprint (that could be stolen and used by an attacker), we store in the electronic passport as DG3 information a biocode. This biocode is generated given a random number stored in a tamper resistant secure area of the passport (containing private cryptographic keys). During the verification step, the chipset sends this random number and the associated biocode to the terminal. The terminal computes a biocode given this random number and a biometric capture. The identity of an individual is verified by comparing the stored biocode and the computed one (using the Hamming distance). After a period, the biocode can be regenerated with another random number following the same process as previously explained.

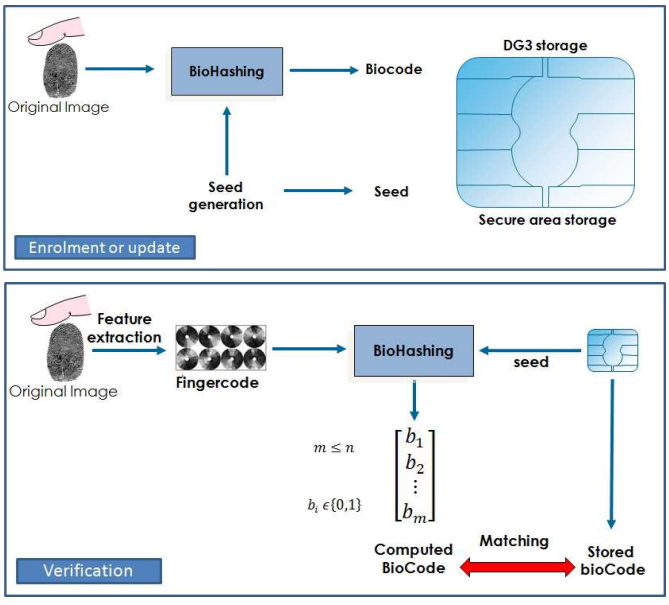

Figure 1 Scheme of the proposed method

In order to define precisely this protocol, we have to implement a cancelable biometric generation method.

We present the state of the art in this domain in the next section.

3.2 Cancelable biometrics: state of the art

The solutions combining biometrics with cryptography can be classified into three categories: (a) protecting biometrics data with cryptographic techniques, (b) obtaining cryptographic keys using biometrics, and (c) cancelable biometrics.

A common solution in order to protect the privacy of users when using a biometric information consists in encrypting it with cryptographic. This solution has many drawbacks. First, it implies some key management issues (Publi Key Infrastructure or exchange of secret keys). Second, the privacy is guaranteed through the cryptographic scheme. Even if a cryptographic algorithm such as 3DES has not been broken yet, with progress in cloud computing, there are many chances it will be in a near future. This is a problem as it is not possible for an user to change its biometric information. To be completely safe, we should be able to guarantee a cryptographic algorithm would not be broken during the life of an individual (say 100 years) and it is difficult to be sure of that. Last, even if biometrics is combined with some other parameters (such as smart card, password, cryptographic key), it cannot improve the verification performance. Indeed, the comparison is always done in the biometric feature domain which can make it easier for an attacker to obtain the raw biometric data. As a conclusion, this first approach does not offer good guarantees on the privacy of users.

Along with revocability and privacy protection, stable cryptographic keys can also be obtained using biometric data. Examples of such systems are (17; 18; 19), etc., which deliver a stable bit-string, denotes as crypto-bio key, using biometric data. There are two possible modes of obtaining such keys it can be obtained directly from the biometric data (key generation) or a randomly generated key can be protected using biometric data and can be retrieved whenever it is required (key regeneration) by presenting fresh biometric data. These systems have the advantage to provide revocability, security, non repudiation, and privacy protection. In addition, these systems output a key which can be used in cryptographic systems. In the context of the electronic passport, we cannot use this approach because it does not fit the PKI used by governments.

In cancelable biometric systems (20; 21; 22), the biometric signal/feature vector is generally converted using an one-way transformation so that the biometric data is not stored in its usual form. The biometric template is transformed such that it does not reveal the original biometric data. The transformation makes it possible to issue different templates of a person for different applications by using different transformation parameters. Thus, the templates cannot be matched across databases providing privacy protection. Moreover, if the template is known to be compromised, it can be canceled. In this case, a new template can be issued using the same biometric information. This ability to change the template and issue a new one is called revocability. (22) 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 one. However, the performances of the proposed systems are worse than the baseline biometric system. Using tokenized random numbers for biometric discretization is another solution proposed by (24). 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. (20) proposed a fingerprint based revocable biotokens scheme in which they use robust matching techniques in encrypted domain. This scheme combines a user assigned token with biometric data, and as expected, improves the performance as compared to the baseline system. (25) propose to shuffle the iris code in order to improve the verification performance of the system and to protect the original biometric data (iris code). Moreover, a novel method of correcting biometric data variabilities using error correcting codes is proposed. When the proposed algorithm is applied on the iris data, the performance (in terms of Equal Error Rate EER) is improved by more than 90% (EER decreases from 1.70 to 0.057%).

3.3 Cancelable biometrics

We propose a cancelable biometric approach for fingerprints based on texture decomposition (23). First, the general process is described. Secondly, the computational details of the biometric template are given. The BioHashing process is presented next.

Figure 2 illustrates the general process to compute the biometric feature based on Gabor filtering (texture analysis) delivering a fingercode of size 384 bits. The main advantage of this solution for feature computation is the resulting number of bits compared to minutiae extraction. For more details on this feature extraction part, please refer to the following article (23).

In order to generate a cancelable biometric information (biocode), we apply the Biohashing process to the previously described fingercode. In general, the process of BioHashing has two stages. In the first stage, some features $(f_1, f_2, ..., f_n)$ are derived from the raw biometric signal. In the second stage, features are mapped to a binary descriptor $b \in \{0,1\}^m$, where m is the length of the bit-string code. Different biometric signals exploit different techniques in the first process,

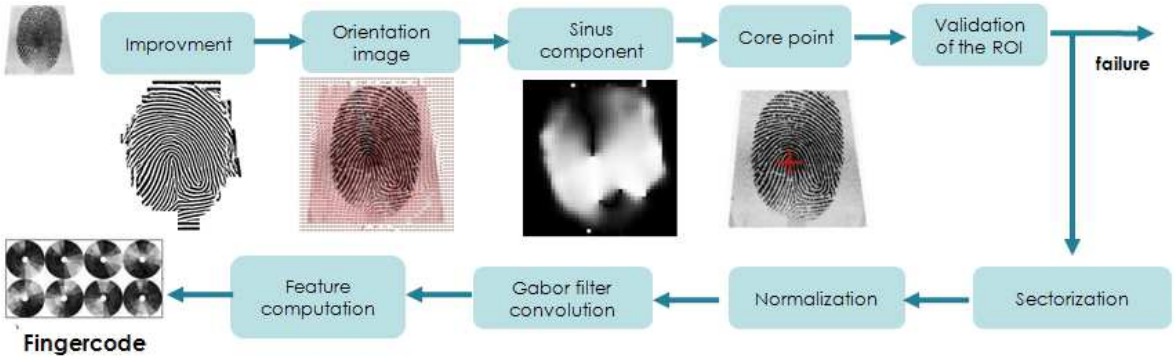

Figure 2 Fingercode generation

but the focus of our analysis is discretization, the process of BioHashing, consisting of four steps:

1. Generate a set of pseudo-random vectors A. In practice, a random number sequence r could be generated from a seed stored on the passport chipset through a random number generator. The seed is different among different users. For testing, random bit/number algorithms are publicly available such as ad hoc scheme.

2. Apply Gram-Schmidt process to transform the basis A into an orthonormal set of matrices $r^i_\perp$, $i = 1..m$

3. Compute the inner product $(< f, r^i_\perp >)$, $i = 1..m$ between the biometric feature f and $r^i_\perp$. This projection results in an error tolerant representation.

4. Compute an m-bit biocode denoted as b ($b \in 2^m$):

$$b_i = \begin{cases} 0 & if(< f, r^i_\perp >) \leq \Gamma \\ 1 & \text{otherwise} \end{cases}$$

where Γ is a preset threshold.

The resulting bitstring b named biocode is compared using Hamming distance. The security of the process is assured if the biocode is non invertible. Note that the user must provide his biometric data (the fingercode) and the seed value to be authenticated.

4 Results and discussion

In this section, we present first a study on the performance on the verification realized with the biocode. A security analysis on the proposed passport architecture is given.

Verification performance

The performance of a biometric system is commonly described by its False Acceptance Rate (FAR) and False Rejection Rate (FRR). The two measurements can be controlled by adjusting a threshold, but it is not possible to exploit this threshold simultaneously reducing FAR and FRR. FAR and FRR must be traded-off, as reducing FAR increases FRR and vice versa. Another index of performance is Equal Error Rate (EER) defined as the point where FAR and FRR are equal. A perfect system would have zero EER.

In the experiment, following ICAO recommendations, we acquire an optical fingerprint scanner that meets the FBI image quality specifications [26] in order to be conform with a real border control scenario. Our constructed database has the following properties :

- The images of the people were taken on two different sessions and no 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.

Figure 3 Fingerprints database

First of all, we present the performance of the fingercode method (without biohashing) on the databases. We simulate the genuine distribution, we obtain an EER value of 4% (see Figure 4). Note that the obtained performance is far from the best algorithm from the state of the art but it is not important for our study. This performance has to be compared in a relative way with the cancelable biometric method.

In order to quantify the robustness of the proposed cancelable biometrics method, we defined different

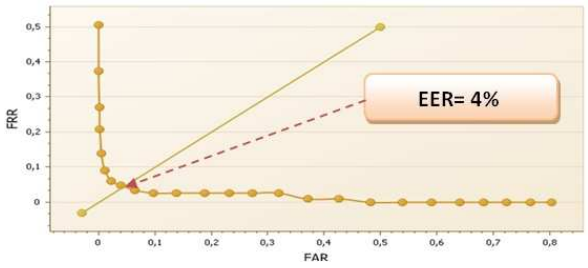

Figure 4 Fingercode verification efficiency

possible scenarios. In all scenarios, we suppose that the impostor presents himself at the terminal.

Scenario 1 (genuine distribution) : to generate genuine distribution, each BioCode of each subject is matched against all other BioCode of the same subject leading to 2240 comparisons ($7 \times 8/2$ attempts for each subject $\times 80$). To plot the ROC curve, we simulate an impostor distribution by comparing the first BioCode of each subject against the first one of all other subjects and the same process done for all the database, leading to $(80 \times 79)/2 \times 8 = 252850$ attempts. We notice that after fixing parameters (quantization thershold 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 (see Figure 5). This result means that the BioCode is able to correctly separate intra-class from inerclass distribution as long as parameters are well tuned. However, in a reality the claim of always having 0% error rate is not realistic. An impostor can steal a genuine passport and tries to masquerade as the authentic user. We explore this issue in the next scenario.

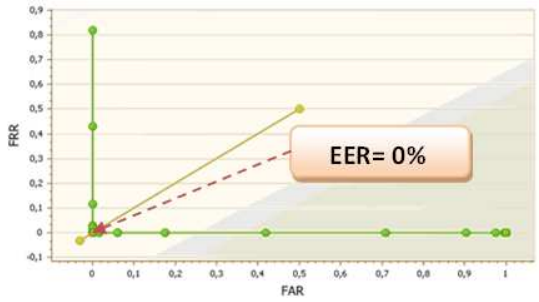

Figure 5 Biocode verification efficiency

Scenario 2 (always-stolen-passport) : here, we consider a very worst scenario when an impostor steals all the passports of the genuine users (not probable in practice) and presents himself to the border control. In term of our database, a passport is the combination of BioCode+user random number; to simulate this it is sufficient to put the same random number for all the subjects. As in scenario 1, we have 2240 genuine attempts and 252850 impostor attempts. We notice in this scenario that the performances are weaker compared to the use of the biometric alone (see Figure 6). By increasing the parameter m, we can improve the results. With $m = 384$ bits (maximal value considering the fingercode size), we obtain en EER of 6.78%

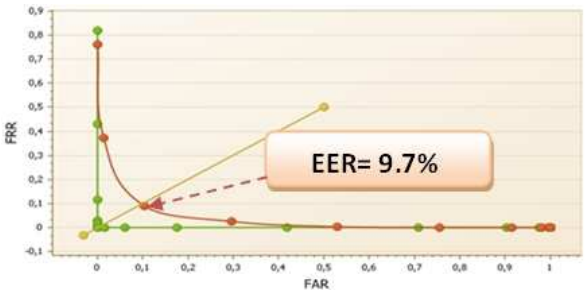

Figure 6 Biocode verification efficiency in the worst case on the first database

4.1 Privacy protection analysis

In this section, we study how the proposed biometric data management scheme is consistent with generally accepted privacy principles. First of all, we consider that our fingerprint representation based on fingerprint texture analysis (i.e. The Fingercode) is personally sensitive information this means that FingerCode can expose enough information about individual and can be used against his or her wishes (e.g. gaining acces to other biometric systems). We analyze privacy in terms of reversibility and linkage attacks.

Reversibility attack : for a feature vector $f(n \times 1)$ and a random matrix $R(m \times n)$. The BioCode B is $B = Q(Rf)$ where Q is a quantizer. The process is invertible if we can derive f from B having R. This may happen when EAC protocol fails and a false reader gain access to B and R simultaneously.

Considering, the process $B = Rf$ without quantization. The problem can be viewed as rectangular linear equation system where we have more unknowns than equations $(n > m)$. If R is a non-full rank matrix, the infinite system solutions underlies the non-irreversibility of the equation $B = Rf$.

If R is a full rank matrix, using the QR factorization it is possible to find a close estimation a of f which minimizes the norm $\| f - a \|$ in term of least squares approximation. Note that,a is never equal to f. Furthermore, the discretisation step enforces the non-invertible property of BioCode even if R and B are known.

In the other hand, we believe that this close estimation possibility is related to the contiguous nature of the vector f. If we make a certain random swapping before projection, the non- reversibility can be guaranteed in all cases.

Linkage attacks : Here we examine the possibility to link BioCode template with other fingerprint databases in order to track individual activities. Always based on the possibility of EAC protocol failure and the access to the biometric information (BioCode) , we try to analyze if a BioCode can be correctly submitted to any other BioCode-based databases. This depends on the strengths of revocability scheme. For testing this, we assign each individual with n different keys and make comparison between templates. We always find that Hamming distances is always above a certain threshold which means that revoked templates are sufficiently distant.

5 Conclusion

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.

References

[1] Giot, R., El-Abed, M., Rosenberger, C., (2009) 'Keystroke Dynamics With Low Constraints SVM Based Passphrase Enrollment', *IEEE Third International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington DC USA*.

[2] Ladoux, P.-O., Rosenberger, C., Dorizzi, B., (2009) 'Hand Vein Verification System based on SIFT matching', *The 3rd IAPR/IEEE International Conference on Biometrics (ICB)*.

[3] Phua, K., Chen, J., Huy Dat, T., Shue, S., (2008) 'Heart sound as a biometric', *Pattern Recognition*, Vol. 41, No. 8, pp.906–919.

[4] Abid, M., and Afifi, H., (2008) 'Secure E-Passsport Protocol Using Elliptic Curve Diffie-Hellman Key Agreement Protocol', *Proceedings of IAS'08, IEEE*, pp.99–102.

[5] Avoine, G.,Kalach ,K. and Quisquater, J.J., (2008) 'ePassport : Securing international contacts with contactless chips', *Proceedings of FC'08, Lecture Notes in Computer Sciences* Vol. 5143, Springer-Verlag, pp.141–155.

[6] Bundesalt fur Sicherheit in der Informationstechnik, Germany, (2008) 'Advanced Security Mechanism for Machine Readable Travel Documents', *Technical Guideline TR-03110*, version 2.02.

[7] Chotia, T. and Smirnov, V., (2010) 'A Traceability attacks against e-passports', *Proceedings of FC'10, Lecture Note in Computer Sciences*, Springer-Verlag.

[8] Chaabouni, R. and Vaudenay, S., (2009) 'The extended Access Control for Machine Readable Travel Documents', *Proceedings of Proceedings of BIOSIG'09*, Vol. 155, pp.93–103.

[9] Justice and Home Affairs, (2006) 'EU standard specifications for security features and biometrics in passports and travel documents', *Technical report, European Union*.

[10] Hlavac, M. and Rosa, T., (2007) 'A note on the relay attacks on e-passport : the case of Czech e-passport', *Technical report*.

[11] International Civil Aviation Organization, 'Doc 9303 : Machine Readable Travel Documents', *Technical report* - Part 1, Vol. 1 (2004) and Vol. 2 (2006).

[12] International Standard Organization ISO/IEC : Iso/iec14443, identification cards - contactless integrated circuit(s) card - proximity card, 2000

[13] Juels, A., Molnar, D., Wagner D., (2005) 'Security and privacy issues in e-passports', *IEEE SecureComm*, pp.74–88.

[14] Nithyanand, R. (2009) 'A survey on the evolution of cryptographic protocols in ePasseports', *Technical report*.

[15] Pasupathinathan, V., Pieprzyk J., Wang H., (2008) 'An On-Line Secure E-Passport Protocol', *Proceedings of ISPEC'08, Lecture Notes in Computer Sciences*, Vol. 4991, pp.14–28, Springer-Verlag.

[16] Richter, H., Mostowski, W., Poll, E., (2008) 'Fingerprinting passports', *NLUUG'08 Spring Conference on Security*.

[17] Uludag, U., Jain, A.K., (2006) 'Securing Fingerprint Template: Fuzzy Vault with Helper Data', *Conference on Computer Vision and Pattern Recognition Workshop*, No. 20, pp.163–170.

[18] Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., Zmor, G., (2007) 'Optimal Iris Fuzzy Sketches', *IEEE Conference on Biometrics: Theory, Applications and Systems*.

[19] Hao, F., Anderson, R., Daugman, J., (2006) 'Combining Crypto with Biometrics Effectively', *IEEE Transactions on Computers*, Vol 55, No 9, pp.1081–1088.

[20] Boult, T.E., Scheirer, W.J., Woodworth, R., (2007) 'Revocable Fingerprint Biotokens: Accuracy and Security Analysis', *IEEE Conference on Computer Vision and Pattern Recognition*, pp.1–8.

[21] Lumini, A., Nanni, L., (2007) 'An improved BioHashing for human authentication', *Pattern Recognition*, Vol. 40, No. 3, pp.1057–1065.

[22] Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M., (2007) 'Generating Cancelable Fingerprint Templates', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, No. 4, pp.561–572.

[23] Belguechi, R., Rosenberger, C., (2009) 'Study on the Convergence of FingerHashing and a Secured Biometric System', *Procceedings of the International conference CIIA*.

[24] Goh, A., Ngo, D.C.L., (2003) 'Computation of cryptographic keys from face biometrics', *International Federation for Information Processing*, pp.1–13.

[25] Kanade, S., Petrovska-Delacrtaz, D., Dorizzi, B., (2009) 'Cancelable Iris Biometrics and Using Error Correcting Codes to Reduce Variability in Biometric Data', *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*.