An integrated framework combining Bio-Hashed minutiae template and PKCS15 compliant card for a better secure management of fingerprint cancelable templates

Rima Belguechi, Estelle Cherrier, Christophe Rosenberger, Samy Ait-Aoudia

An integrated framework combining Bio-Hashed minutiae template and PKCS15 compliant card for a better secure management of fingerprint cancelable templates

Rima Belguechi [a,b], *Estelle Cherrier* [b,*], *Christophe Rosenberger* [b], *Samy Ait-Aoudia* [a]

[a] *Ecole Nationale Supérieure d'Informatique, ESI, Algiers, Algeria*
[b] *E-payment and Biometrics Research Unit, GREYC Laboratory, Caen, France*

A B S T R A C T

We address in this paper the problem of privacy in fingerprint biometric systems. Today, cancelable techniques have been proposed to deal with this issue. Ideally, such transforms are one-way. However, even if they are with provable security, they remain vulnerable when the user-specific key that achieves cancelability property is stolen. The prominence of the cancelable template confidentiality to maintain the irreversibility property was also demonstrated for many proposed constructions. To prevent possible coming attacks, it becomes important to securely manage this key as well as the transformed template in order to avoid them being leaked simultaneously and thus compromised. To better manage the user credentials of cancelable constructs, we propose a new solution combining a trusted architecture and a cancelable fingerprint template. Therefore, a Bio-Hashed minutiae template based on a chip matching algorithm is proposed. A pkcs15 compliant cancelable biometric system for fingerprint privacy preserving is implemented on a smartcard. This closed system satisfies the safe management of the sensitive templates. The proposed solution is proved to be well resistant to different attacks.

1. Introduction

Biometric-based authentication systems are rapidly superseding traditional authentication schemes. Among of them, fingerprint identifiers are widely implemented. This biometric has several undeniable advantages. Fingerprints are unique for each individual and present a long-term stability. They also have good accuracy of recognition which is a key-factor in biometric systems. Nevertheless, fingerprint is considered as highly risked modality in term of privacy violation. It is demonstrated that a fingerprint template, when compromised, allows the reconstruction of the initial signal that can fool the system (Feng and Jain, 2009; Galbally et al., 2008). Moreover, the uniqueness of fingerprint permits to cross match data subjects between different applications involving tracking and profiling possibilities. Meanwhile, when the fingerprint identifier is compromised, it will be useless forever. Unlike password or token, fingerprint data cannot be revoked and re-issued. Therefore, a fingerprint system must take into account these privacy and security issues during its deployment. With the present risks, handling fingerprint data becomes more important.

In order to solve the problem, some algorithms known as template protection schemes have recently been proposed. On theory, as defined by the ISO/IEC 24745 standard (2011), these algorithms are designed to guarantee the following requirements: *irreversibility* (the biometric data shall be transformed in such a way that the biometric sample cannot be

* *Corresponding author*. Tel.: +33 (0)2 31 53 81 79.
E-mail address: estelle.cherrier@ensicaen.fr (E. Cherrier).

retrieved from the transformed representation); and *unlinkability* (the stored biometric references shall not be linkable across applications or databases).

Basically, two approaches have been developed in the literature: biometric cryptosystems such as fuzzy vault (Juels and Sudan, 2002) and fuzzy commitment (Hao et al., 2006) schemes and cancelable fingerprints. However, we remark that many solutions exist but a real deployment of a compatible solution that maintains recognition performance as well as privacy is still challenging. Furthermore, the absence of a rigorous evaluation process directly impacts the confidence in such systems. According to some research works, we find that a variety of template protection techniques are not well resistant to smart attacks. Scheirer and Boult (2007) present four attacks that questioned the privacy-enhancing properties of the basic fuzzy vault framework. Due to the correlation of biometric features, Zhou et al. (2011) as Simoens et al. (2009) conclude the privacy leakage of the fuzzy commitment scheme. Regarding cancelable fingerprints, a weak point is related to the management of the user-specific key used in the transformation process. If this key is revealed, we observe a performance decrease in term of false acceptance rate. If it is not sufficiently low, an attacker can look for a pre-image (not necessary the exact one) to pass the verification step. Furthermore, this attack can be performed without accessing the server, when both the transformed template and the corresponding key are known. Thus, it is much more serious than online dictionary attacks which can be prevented as mentioned by Takahashi and Hirata (2011). Cancelable constructions are widely concerned by the key management problem. In certain cases, if the confidentiality of the transformed template is not ensured, the reversibility of the protected template may be feasible. As an example, the transformed minutiae of Ratha et al. (2007), Yang and Busch (2009) or Lee and Kim (2010) have been inverted when the transformed template is leaked simultaneously with the algorithm parameters. Template protection schemes can also be attackable by record multiplicity attack or ARM attack. In fact, the recent paper of Li and Hu (2013) show that measuring the diversity property via statistics is not sufficient and practical attacks can be conducted through cryptanalysis. Authors launch successful attacks on each of these recent schemes: Lee et al., 2007, Ahmad et al., 2011 and Wang and Hu, 2012. ARM attack is feasible if several transformed templates are obtained with their algorithm parameters.

In this paper, we investigate security of a fingerprint cancelable scheme by creating a system that includes both a smartcard and a cancelable template. The decision to create such an integrated framework results from a security threat analysis that determines a need to keep the protected template confidential and to not store this template at the same place as the key. The previous presented attacks motivate further this need. It was seen that transformation algorithms may be vulnerable if the transformed template is leaked simultaneously with the user key. To achieve this objective, we rigorously follow different steps: First, we propose a cancelable fingerprint template technique based on a biohashed minutia template. The method extracts the FingerCode (Jain et al., 2000) for every minutia and applies BioHashing (Teoh et al., 2004) at the Fingercode to produce a protected minutia template. This proposed version extends our previous work on (Belguechi et al., 2013) with the improvement in the way to support the alignment problem. The process of aligning fingerprint is quite complex regarding transformation algorithms. The original approach relies on the existence of the core point to correct the displacement between reference and input images. Therefore, it presents limitation in case where this point is missing on the fingerprint. To deal with this drawback, we modify the registration phase. An algorithm that validates the detected point is proposed. If this point is considered as a non reference point, a self-alignment template is subsequently created. The reliability of the algorithm is then enhanced in term of fail to enroll rate which moves from 9% to 1.25%. Second, we study security and privacy risks of the proposed approach. The modeling is based on a general evaluation framework we have proposed in (Belguechi et al., 2012). We intend in this paper to use it for evaluating the proposed cancelable system. This modeling shows that a loss of different revoked transformed templates can be threatening as well as a lost key. Third, we propose a biometric cancelable Match on Card (MoC) system to meet extremely stronger security requirements. The proposition of a chip matching algorithm permits to ensure the confidentiality of the biometric template since it never leaves the card. The proposed matching algorithm lets to make verification between the probe and the pushed cancelable templates in the card without any performance downside. Thereafter, the proposed 3-factor authentication system offers a better resistance to possible attacks. If the key is lost, it will be useless without the corresponding card. Both the lost key and lost card risks may exist (even if it's low), however this will be better managed on account of the cancelability property of the biometric system. Compared to the already existing MoC systems, our proposition add a new value since the biometric template is cancelable which will improve its security if possible external attacks are conducted on the card. In fact, a MoC system that stores a biometric template with cancelability property would have a greater security level than one that uses an unprotected template. To describe how/where to place the biometric template on the card, we propose a full design of a compatible PKCS15 (2000) solution with one major addition concerning the use of the PKCS15 with the revocation property. For a proper security context, we have looked into combining the biometric technology with industry standards. This permits a larger and easier adoption and interoperability.

The rest of this paper is organized as follows. Section 2 discusses the related works on fingerprint template protection. The robustness of the proposed cancelable system is evaluated in Section 3. The match on card system is presented in Section 4. The conclusion is given in Section 5.

2. Previous work on fingerprint template protection schemes

The idea in template protection scheme is to encode the biometric template X to the pseudo-identity $E(X)$ (Breebaart et al., 2008) before storage. A simple solution is to consider

$E(X)$ based on cryptographic mechanisms. For instance, the ANSI X9.84 rules (ANSI X9.84, 2010) were designed to maintain the integrity and confidentiality of biometric information using encryption algorithms. However, cryptography becomes insufficient when applied to biometrics. Due to the intra-user variability over multiple acquisitions of the same biometric trait, one cannot store a biometric template in an encrypted form and then perform matching in the encrypted domain. For this reason, the comparison is always done in the biometric feature domain which can make it easier for an attacker to obtain the raw biometric data.

Since conventional hash functions are not applicable, the stability of a pseudorandom key S has been introduced to deal with the variability of the biometric X and combine them with a function F to obtain the auxiliary data HD. Only HD and a transformation of S (here $H(S)$ with $H(.)$ a 1-way hash function) are stored. For verification, W is combined with the biometric Y in the function F to obtain V. The comparison succeeds if $H(S)=H(V)$. So, if we define the helper data HD as a data guaranteeing that a unique string can be derived from the biometric template X, we can broadly classify methods to protect fingerprint templates into two categories: **(i)** *methods with helper data* mostly known as biometric cryptosystems and **(ii)** *methods without helper data* or cancelable fingerprints.

In *methods with helper data*, to compensate for the signal variability, the pioneering work of Davida et al. (1999) involves the extension of a biometric template into an error-correcting codeword. The helper data HD is taken as check bits in the (N,K,D) error correction code for the given K information bits in X. Only HD and the sealed template $H(X||HD)$ are stored in the database (where $H(.)$ denotes a 1-way hash function and $||$ the concatenation symbol). The system is said to be secured if the helper data HD does not reveal too much about the original template. However, because of the redundancy in the code, check bits may lead to some leakage of information about the user's biometric data. In contrast, Juels and Wattenberg (1999) treat the template itself without any modification as a corrupted codeword. This idea has lead to different constructions such as fuzzy commitment (Hao et al., 2006), fuzzy vault (Juels and Sudan, 2002) and fuzzy extractor (Dodis et al., 2004). Tuyls and Goseling (2004) prove that perfect security of fuzzy commitment is possible if input biometric data is an ideally independent and identically distributed string which is rarely the case in practice. In their analysis, Zhou et al. (2009, 2011) focus on the biometric data distribution in practical systems, and report that security weakness and privacy leakage occur due to the correlation of biometric features, in particular when local descriptors are used in the biometric template. In a recent paper, Simoens et .al (2009) show that an adversary has an advantage close to 1 to easily find related templates in large databases for the fuzzy commitment. The same proof has been done for the bit-permutation construction of Dodis et al. (2004).

Linnartz and Tuyls (2003) propose shielding function as a framework to extract secret from common randomness. Therefore, given a randomly chosen secret $S \in \{0, 1\}^K$ and a biometric data $X \in R^k$, *helper data* $HD \in \{0, 1\}^k$ is computed such that $F(X,HD) = S$ (or the equation $F(X,HD) = S$ is solved for HD). This method is promising but needs to be carefully handled in practice since biometric data have a non-uniform distribution and moreover the authors assume the template is noise-free.

In the syndrome approach (Draper et al., 2007; Nagar et al., 2010a), the biometric template X is encoded into a secure syndrome HD which is considered as the helper data by using low density syndromes rather than algebraic error correction codes. Only HD and $H(X)$ are stored. During authentication, the query biometric Y (a noisy version of X) is used with the stored HD to estimate X. Meanwhile, unlinkability and diversity of this method are not proven.

Boult and Woodworth (2008) try to address this issue by proposing an original approach. Their transformation called Biotope induces a robust distance measurement. The biometric feature data X is first transformed (applied per feature) via scaling and rotation into $X' = (X - t)^*s$ while t and s are randomly generated parameters. The transformed data is then separated into a fraction r (remainder) and a stable integer part q (quotient). q is hidden using encryption while the remainder r remains in clear and supports a robust distance measure. With the Biotope, authors report a better accuracy than the initial biometric system. However, the robust revocable transform is specifically computed for each user and thus the accuracy improvement can again rely on the uniqueness of the transform. In order to enhance the security of the previous schemes, Bringer et al. have proposed a combination of a secure sketch with a probabilistic encryption and a PIR protocol in (Bringer et al., 2007; Bringer and Chabanne, 2008). The biometric authentication protocol nicely illustrates the possibilities proposed by homomorphic encryptions for privacy enhancement in biometric authentication.

In *methods without helper data* also called cancelable transforms, the principle is to perform the verification between the transformed templates. Suppose X will be transformed into the encoded data T during enrollment. For verification, the query biometric Y will be encoded into T' and the authentication will succeed if T is close to T' using a certain similarity distance. A number of approaches that applies a specific transformation to the fingerprint data were proposed. Ratha et al. (2007) propose three different transforms: Cartesian, polar and functional. Quan et al. (2008) show that most of the transformed minutiae will be known to the attacker if the algorithm parameters and the transformed template are leaked simultaneously. Kumar et al. (2010) propose symmetric hash function applied on k-neighboring minutiae. In their analysis, no care taken if both the key and the transformed template are compromised at the same time. Jin et al. (2009) propose a cancelable system based on histogram representation. In case of the lost key, there is a real decrease in the system performance since the system will accept more than 10% of the intruders population. Among the most recent developments, we refer the reader to the following references: Lee and Kim (2010) generate m vectors for m minutiae by mapping each minutia into a 3D array based on the position and the orientation of the reference minutia. But, in case of lost key as well as the reference template, the reversibility is straightforward. Jin et al. (2012) use bit-string minutiae

based representation approach. For cancelability purpose, the resultant bit-string is permuted using a user key. In case the key is lost, the system will accept 6.94% of the intruders population. The test is drawn on the popular FVC2002-DB2 (Maio et al., 2002) database. Ahmad et al. (2011) use the polar transformation proposed earlier by Ratha et al. (2007), where the initial template is based on the polar coordinates from a reference minutia. On a partial set of the FVC2002-DB2 database, the system accepts 6% of the intruders population if the key is lost. Wang and Hu (2012) develop a novel approach where the same template as that used by Ahmad et al. (2011) is transformed according to a model based on densely infinite-to-one mapping. This approach, compared to the previous ones, gives better performance. In the FVC2002-DB2 database, when the key is lost, it falsely accepts 5% of the impostor population. It is satisfactory but still a strict security requirement is not reached.

Another approach is the biometric salting when user-specific random patterns are convolved with biometric data. Some of the popular salting-based approaches are known as BioHashing (Teoh et al., 2004). The approach involves the use of the random multispace quantization. The resulting template is a bit-string called biocode. In zero-knowledge case, BioHashing has significant advantages such as extremely clear separation of the genuine and the imposter population and a difficulty to invert the transform and obtain the fingerprint features as demonstrated in (Teoh et al., 2008). However, if the tokenized random number (TRN) is lost, the performance of BioHashing can be worse than the basic biometric system. The results of some tests on different modalities are given in (Lumini and Nanni, 2006). For fingerprint texture template for example, the authors have demonstrated that the performance of the system in term of EER (Equal Error Rate) moves from 7.3% when no hashing is performed to 10.9% when basic BioHashing is operated under the hypothesis that the token is always stolen, while EER is evaluated to 1.5% in case where no TRN is stolen (FVC2002-DB2).

Note that, in the cited methods, the diversity is given by the randomness of the user key. So, featuring biometric data with user specific randomness like a seed or a password seems to be the easiest way to achieve revocability property via direct replacement with a new seed. However, these methods lose security when the management of the key is not ensured. Today, the challenge in designing a practical implementation may follow one of these three following tracks: finding a mechanism that works with *public key*, offering a more competitive protection scheme or finding a usable protocol in an operational context.

In the following, we present a minutiae matching system where each minutia is defined by a local descriptor. Since this local descriptor is ordered and stable in size, we can use the principle of BioHashing to protect it. While BioHashing is applied on minutiae template, we demonstrate that is it concurrent with recent developments. A general framework is then used to evaluate the robustness of the given biometric system regarding security and privacy. This analysis expounds the importance of keeping the reference transformed template as confidential as possible. Subsequently, a solution based on a cancelable *match-on-card* system is proposed to enhance the security requirements. The resultant system is allowed to verify itself in the card without any performance downside.

3. BioHashed minutiae based cancelable system: attacks and robustness

3.1. *Template creation*

Let $M = \{m_i\}_{i=1}^{\mu}$ a set of minutiae points extracted from a fingerprint image. The template creation process is described in Fig. 1:

As shown on Fig. 1, the minutia descriptor comprises a MinuCode and a k-plet. The Minucode is the descriptor of the texture surrounding the minutia. Around each minutia, we define a circular tessellation as B concentric bands. Each band is divided into 16 sectors of the same angle (22.5°). The texture of the ridge flow in this tessellation is then extracted using the FingerCode descriptor presented in (Jain et al., 2000). It should be noted that the images are preprocessed with the method proposed in (Chikkerur, 2005) before minutiae are extracted. Further, we use small sets of k-neighboring minutiae to represent local structure between them. A k-plet is formed by a reference minutia and its K spatially closest ones. Its role is to add global information to the matching algorithm. Thereafter, only minutiae validated by the selection step are kept in the final template. From the set M, a minutia m_i is selected only if its surrounding ROI (Region Of Interest) 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 the Fourier spectrum so, if $E > T_r$, then the sector is accepted else it is rejected, where T_r is a global Otsu threshold.

The final template is noted: $\{m_i\}_{i=1}^{\upsilon} = \{MinuCode_i + \{a_j\}_{j=1}^{K}\}_{i=1}^{\nu}$ while a_j denotes a minutia label and $\upsilon < \mu$. The size of the template reduces from μ minutiae to υ while υ varies between 10 and 20. Hence, only minutiae containing useful information are retained in the final template. Such compact template will be suitable for memory limited applications.

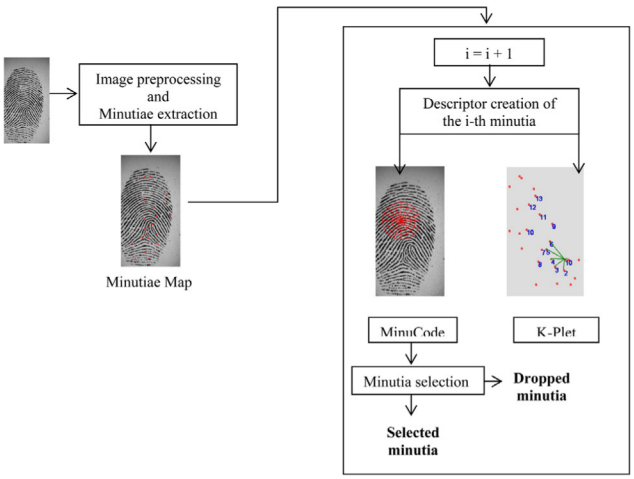


Fig. 1 – Biometric template creation principle.

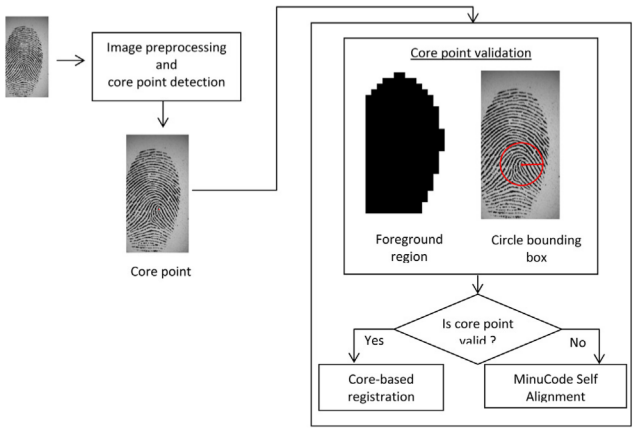


Fig. 2 – Support of the alignment problem.

3.2. *Alignment problem coverage*

A possible displacement in the scanning process can cause a non overlap between the template and the input fingerprints. While the translation factor is implicitly undertaken by using local structure around each minutia, the rotation problem remains since the MinuCode is not invariant with respect to rotation. In our previous work (Belguechi et al., 2013), a core-based registration approach was used. If the core point is reliably detected, the method performs well. However, on fingerprints where the core point is explicitly missing such as arch classed fingerprints, the registration will return a Fail To Enroll (FTE) message. To enhance the treatment, in case of an FTE, we propose to use the minutia direction θ_i as a reference axis to define the region of interest around the minutia. Compared to the original version of the FingerCode, the bank of Gabor filters will start from the direction θ_i instead of 0° (the horizontal axis). Note that θ_i is given in the range [0…360°[. Fig. 2 resumes the overall process:

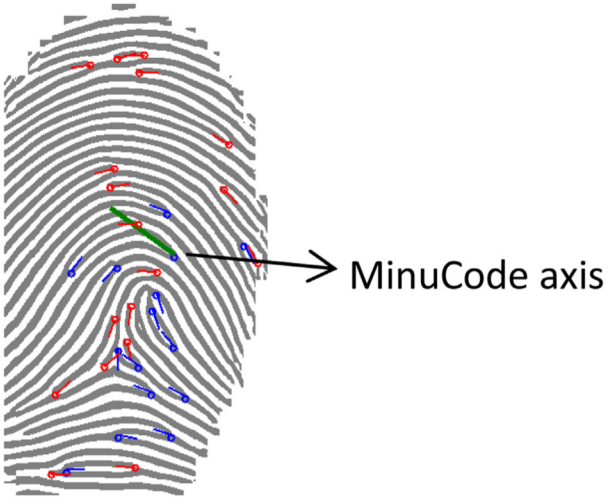


Fig. 3 – The oriented axis for the MinuCode extraction.

In core-based registration, the core position is defined as the location of the maximum curve point. An algorithm similar to (Jain et al., 2000) is used. Since the algorithm will detect in all cases a point even with the minimum of consistency, a validation stage is necessary to eliminate the false positive. As in Fig. 2, the core point is validated if: *(i)* it's in the boundary of the image and *(ii)* the around circle-bounding box represents an alternation of ridges and valleys. As for the MinuCode, this alternation is expressed by the energy E of the Fourier spectrum. The radius r of the bounding box is defined as:

$$r = \min\left(\frac{image\ width}{2}, \frac{image\ height}{2}\right) \quad (1)$$

If the core point is rejected, an oriented MinuCode is extracted based on the direction of each minutia as shown on Fig. 3:

3.3. *Template protection*

Each MinuCode mc_i in the clear template $\{m_i\}_{i=1}^{v} = \{MinuCode_i + \{a_j\}_{j=1}^{K}\}_{i=1}^{v}$ will be protected by BioHashing to obtain the protected template $PT = \{PMinuCode_i + \{a_j\}_{j=1}^{K}\}_{i=1}^{v}$. The process is explained in the algorithm 1:

Algorithm 1. BioHashing process pseudocode

For each MinuCode mc_i do:
1: *Let $(x_1,x_2,\ldots,x_n)$ the MinuCode of length n.*
2: *Normalize the MinuCode vector in the range [−1, 1].*
3: *Let biocode a vector of length m.*
4: *Let K be the seed attributed to the biometric capture subject U.*
5: *Generate from K a uniform random matrix R_{nxm}.*
6: *Control that vectors in R are linearly independents else go to 4.*
7: *Apply the process of Gram-Schmidt to transform R to an orthonormal set. In this case, we must have: $m \leq n$.*
8: *Make the projection of MinuCode on this matrix:*

$$[x_1, x_2, \ldots x_n] \cdot \begin{bmatrix} or_{1,1} & \cdots & or_{m,1} \\ \vdots & \ddots & \vdots \\ or_{n,1} & \ldots & or_{n,m} \end{bmatrix} = [w_1, w_2, \ldots w_m] \quad (2)$$

9: *Binarize W by thresholding to obtain the biocode vector $[b_1,b_2,\ldots b_m]$ such as:*

$$b_i = \begin{cases} 0 & \text{if} \quad w_i < \tau_b \\ 1 & \text{else} \end{cases} \quad (3)$$

τ_b is a binarization threshold generally equal to 0. However, instead of using the value 0, we propose to estimate the median over a training dataset A (the median cuts in two the population and the probability of having positive or negative element will be equal) and to set the threshold to the obtained value.
10: *Delete the MinuCode and store the biocode.*

3.4. *Matching algorithm*

We implement a local minutiae matching by comparing protected MinuCodes. To be consistent at the global level, we use the k-plet as first nodes to explore in the matching process. Hence, the algorithm is explained as following:

Algorithm 2. *Minutiae matching pseudocode*

Let $T=\{t_1,\ldots t_m\}$ and $P=\{p_1,\ldots p_n\}$ be the biocodes extracted from the template and input fingerprints.

- ***Phase1***: it consists of the selection of the best matched pair (root$_1$,root2)/root$_1 \in T$ and root$_2 \in P$ by using the following cost estimation technique:

  min = initial value; root$_1$ = -1; root$_2$=-1;
  for i=1 to m
  for j=i to n
  dist = D(t_i,p_j);
  if (dist < min)
  {min = dist; root$_1$ = i; root$_2$ = j;}

  $D(t_i,p_j)$ is the hamming distance between biocodes of minutia t_i and of minutia p_j.
- ***Phase2***: consider root$_1$ and root$_2$ first nodes to explore in T and I resp.

  push the pair (root$_1$, root$_2$) in a queue and mark it as visited
  While (the queue is not empty)
  pop the pair (node$_1$, node$_2$) from the queue
  match the k-plet of node$_1$ with that of node$_2$ (we can use a greedy matching since the k-plet size is small)
  push each matched pair not yet visited in the queue and mark it as visited
- ***Phase3***: the matching score is computed by the following formula,

$$score=\frac{nb\ matched\ \ pair}{Minimum(m,n)}$$

m,n size of T, P resp

3.5. *Studying security and privacy of the proposed cancelable system*

In order to validate their proposition, authors generally provide some experimental results based on performance evaluation (EER value, ROC curves, etc.) and sometimes through a security analysis by considering different scenarios. None standard methodology has been defined in order to qualify the system. Recently, some research works have been proposed (Nagar et al., 2010b; Zhou et al., 2009) for some known transforms. A more general framework for benchmarking template protection algorithms applicable to all protection methods was proposed by (Simoens et al., 2012) but not yet adopted in practice. In the following, as a result of our work published in (Belguechi et al., 2012), we present an evaluation framework for the proposed cancelable system, that can be seen as a general evaluation framework. The evaluation is based on two important points. The first is the security analysis, performed by measuring the computational complexity of effective known attacks. This point enables an evaluation of the hardness of the problem. The analysis is then completed by the second point, namely the quantification of privacy in term of information theoretical measure. These metrics can prove the feasibility of the given construction. Fig. 4 illustrates the detail of the proposed evaluation model.

Now, we detail the proposed framework. The threat model is decoupled in terms of security and privacy threats which are based on the following protection goals: recognition performance, irreversibility/privacy leakage, unlinkability/diversity.

We use the following notations introduced in the paper (Nagar et al., 2010b). Let x_z and $\dot{x}_z$ represent the template and query biometric features of the user z, respectively. Let f be the feature transformation function. We denote m the dimension of $f(x_z,k_z)$. Let k_z be a set of transformation parameters corresponding to user z. Let D_O denotes a similarity function between the biometric features in the untransformed (original) domain and D_T be a similarity function in the transformed one.

1) System performance

- System usability/intrusion risk

For the usability/intrusion risk of the cancelable system, we consider, respectively, the following metrics:

$$\begin{aligned} FRR_T(\varepsilon) &= P\left(D_T\left(f(x_z;k_z),f\left(\dot{x}_z;k_z\right)\right)\le\varepsilon\right)\\ FAR_T(\varepsilon) &= P\left(D_T\left(f(x_z;k_z),f\left(\dot{x}_z;k_z\right)\right)\ge\varepsilon\right) \end{aligned} \tag{4}$$

Depending on the choice of the decision threshold ε, the FRR (False Rejection Rate) counts the number of rejection when the person at the biometric terminal is legitimate and the FAR (False Acceptance Rate) counts the number of acceptance when the person is an impostor. In practice, it is common to set ε to the value ε_D where $FRR_T(\varepsilon_D) = FAR_T(\varepsilon_D)$. Hence, the system usability is associated to $FRR_T(\varepsilon_D)$ and the intrusion risk is associated to $FAR_T(\varepsilon_D)$.

We note A_1 the couple parameters noted $(FRR_T(\varepsilon_D),FAR_T(\varepsilon_D))$.

2) Irreversibility/Privacy leakage

We analyze this criterion considering the complexity of possible attack scenarios. All these attacks try to recover all or a little biometric information which can successfully pass the verification process.

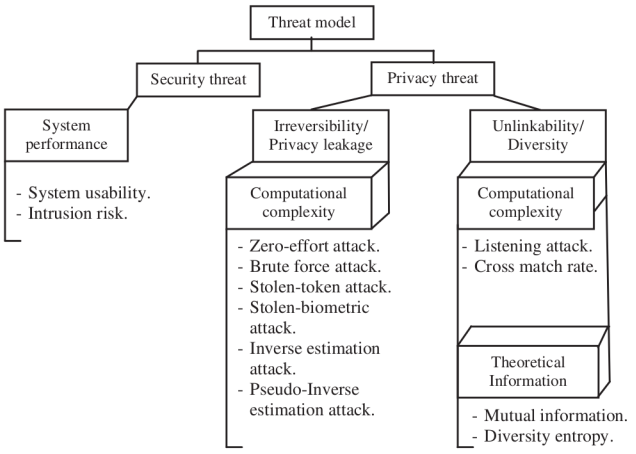


Fig. 4 – Security and privacy framework evaluation.

- Zero effort attack

In this scenario, the impostor y tries to impersonate the genuine user z by presenting its own biometric data $\hat{x}_y$ with unknown key k_y. Let A_2 be the complexity metric for this attack.

- Brute force attack

In this scenario, the impostor y decides to overcome the feature protection component by sending a ready template to the matcher. He will try to estimate an accepted template by an exhaustive search. Let A_3 be the complexity metric for this attack.

- Stolen token attack

In this scenario, the impostor y tries to impersonate the genuine user z with available key k_z but by presenting its own biometric $\hat{x}_y$. Let A_4 be the complexity metric for this attack.

- Stolen biometric attack

For this test, we assume that the impostor y has recovered a fingerprint from the database, and seeks to be recognized by the system as the authorized user z with his own key k_y. Let A_5 be the complexity metric for this attack. This attack can also model the known masquerade or spoofing attacks (Cappelli et al., 2007; Galbally et al., 2008).

For the computation of these metrics, we compute for each of them the following equation:

$$A_i = FAR(\varepsilon_D);\ i = 2\ldots5 \tag{5}$$

- Inverse estimation attack

Here, we measure the possibility on determining either exactly the original template or one that match it in the unprotected domain. This measure depends on the transformation used.

For the proposed cancelable system, Teoh et al. (2006) show that the irreversibility of BioHashing process can be deduced from the fact that there exists an infinity of solutions for a non-full rank linear equation system $w = R \cdot x$ ($m < n$). Therefore, this assumption can be compromised if an attacker knows the linkage among I protected templates with their projection matrix [R1 R2…RI]. When the matrix [R1 R2…RI] becomes full-rank, the projection can be reversible. Although the binarization process makes this attack more difficult, theoretically the reversibility is always possible as mentioned by Zhou et al. (2011). In fact; a feasible region of biometric features x can be calculated with *known biocodes and compromised projection vectors*. The vector direction of x can be isolated in the intersection of the m half-hyperspace regions defined by the m column vectors of the matrix R. This estimate becomes more evident, if more matrices R and their corresponding biocodes are revealed after each revocation. If we note A_6 the complexity of this attack, it will have the value TF which means Theoretically Feasible.

- Pseudo-Inverse estimation attack

In this attack, we measure the possibility on determining a close approximation of the template that match in the protected domain but not necessarily in the unprotected domain. This is also known as pre-image attack.

For the BioHashing transform, Nagar et al. (2010b) has presented a manner for computing an accepted biocode. It is effective, however complex to achieve. This scenario assumes that an attacker has both the key k_z of the user z and the protected biocode $f(x_z,k_z)$ and wants to estimate the inverse x_z. The attacker also needs a set A of t unrelated biometric feature vectors. The set A is chosen such that Hamming distance between biohash features corresponding to the set A and the biocode b is less than a certain threshold. The problem of inversion is then formulated as an optimization problem as follows:

$$\text{argmin}\|x - a\|_2, \text{subject to} \quad \sum_{j=1}^{n} R_{ji}x_j < \tau \quad if\ \ b_i = 0, \text{and}$$
$$\sum_{j=1}^{n} R_{ji}x_j > \tau \quad if\ \ b_i = 1, i = 1\ldots m \tag{6}$$

Let A_7 the complexity of this attack, it will have the value PF which means Practically Feasible.

3) Unlinkability/diversity

We want now to evaluate the diversity (or randomness) of the cancelable system when the template is revoked. We first use complexity measures.

- Cross match rate

A common way to evaluate diversity is to match different transformed templates obtained from the same biometric data after assigning each user t different keys. We call the metric A_8, the cross matching rate which represents the percentage of successful match. A_8 is then computed from the equation (5).

- Listening attack

  An impostor must not be able to extract any information from different templates issued from the same user. Since the template can be revoked, an impostor can intercept N of them and issue a new one by predicting an admissible value (as for example by setting each bit considering the highest probability value). These attacks are tested by the following process:

  - It is sufficient to consider the estimation of one k-plet.
  - Generation of N biocodes for each minutia in the k-plet of the user z by assigning N different keys $k_{Z1}, \ldots, k_{ZN}$.
  - Prediction of a possible biocode value by setting the most probable value of each bit given.
  - Computation of equation (5). A_9 value for $N = 3$ and A_{10} for $N = 11$ (consider $N > 11$ is unrealistic).

  We assess now the diversity property from theoretical information viewpoint.

- Mutual information

In order to measure the diversity property, we propose to compute the mutual information provided by several templates issued from the same biometric data as defined in equation (7):

$$I(x,y) = \sum_{x}\sum_{y} P(x,y)\log\left(\frac{P(x,y)}{P(x)P(y)}\right) \tag{7}$$

where x and y are two random variables and P the estimation of the probability. In order to measure the diversity property, we quantify the highest value of the mutual information among different biocodes for each minutia. The value A_{11} is then computed using the average value for all users of the highest value of mutual information.

- Diversity entropy

To measure diversity in term of entropy, we suppose that an attacker will try to predict an accepted template after eavesdropping N templates of the genuine user. We will explore if a prediction of the $(N+1)th$ template is possible.

Because the biocode is a set of binary strings, we can study the correlation by Hamming distance distribution as done by Daugman (2003). To this purpose, we study the statistical distribution of Hamming distance of N biocodes from the same minutia generated with N different keys (Pseudo-imposter distribution). We repeat the study for several minutiae. Let x be the random variable that represents the number of non matched bits in the biocode. The pseudo-impostor distribution can then be approximated by a binomial distribution where the binary event is the fact that two bits are equal or not and the number of trials is m, the biocode length. The mean will be $m \times P$ with P the probability of the binary event. If we consider $y = x/m$, the random variable of the normalized Hamming then the probability P will be equal to the mean value of the distribution of y. Daugman (2003) shows that the degree of freedom of the fractional binomial distribution can be estimated from the variance σ^2 as $P(1-P)/\sigma^2$.

We call this degree of freedom, the diversification entropy and note it A_{12}.

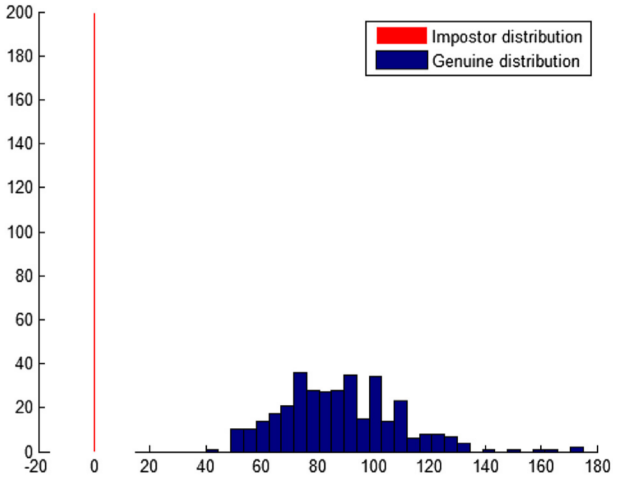


Fig. 5 – Impostor/genuine distributions of the cancelable system.

3.6. *Experimental results*

We present now our experiments on the implemented cancelable biometric system.

All simulations are made on the FVC2002-DB2 (Maio et al., 2002) database. We recall the configuration: 100 users – 8 samples per user using an optical sensor of 569 dpi. The length of a biocode or a protected MinuCode is $m = 180$. The size of a k-plet is $k = 6$.

Fig. 5 illustrates the genuine and impostor population distribution where there is a clear separation between them. So, a decision threshold ε_D for which the system has zero error exists: $FRR_T(\varepsilon_D) = FAR_T(\varepsilon_D) = 0\%$.

We decide to set ε_D at the value of the cancelable system decision threshold having $EER = 0\%$. Table 1 resumes the values of the different evaluation criteria:

From Table 1, we remark that if we tune the threshold to get FAR = FRR = 0% for the cancelable system (see A_1 in the table), the critical attack of the stolen token scenario is possible in 21% of cases (see A_4). It is then more appropriate to set ε_D to the value under stolen token assumption. In Table 2, new values of the evaluation criteria are reported:

Table 1 – Values of the different evaluation criteria where ε_D is chosen from the cancelable system threshold to obtain $EER = 0\%$.

A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}
(0,0)	0	0	20.90%	0	TF	PF	0	0	0	0	202

Table 2 – Values of the different evaluation criteria where ε_D is chosen under the stolen token assumption.

A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}
(5.97%,0)	0	0	7.16%	0	TF	PF	0	0	0	0	202

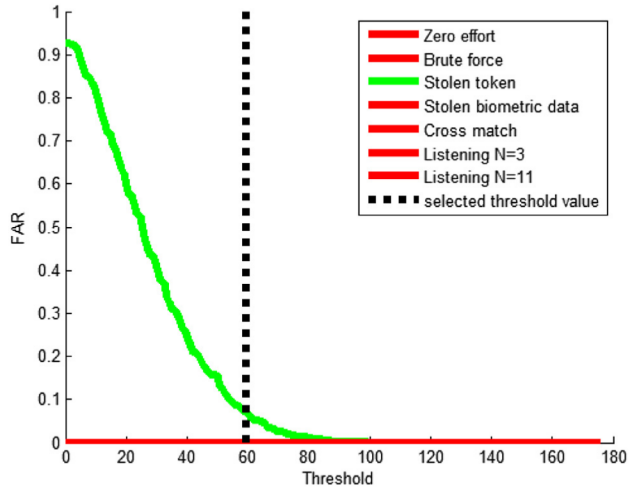


Fig. 6 – Evolution of the FAR for the different attack scenarios.

The evolution of the FAR is expressed in Fig. 6:

The parameter A_{12} of the diversification entropy is calculated from the histogram in Fig. 7. The mean value is 49.58%. This informs that the probability of predicting a correct value by bit is $1 - P = 50.52\%$, which satisfies almost a total ambiguity.

The framework provides a unified way to analyze the robustness of the cancelable BioHashing based transform. From this study, we can draw the following conclusions:

- The choice of the decision threshold is an important task which can affect the robustness of the system with respect to the stolen token attack.
- The cross match rate of 0%, the mutual information of 0 and the diversity entropy equal to the length of the biocode highlights the diversity property of the proposed cancelable system. This is a strength factor.

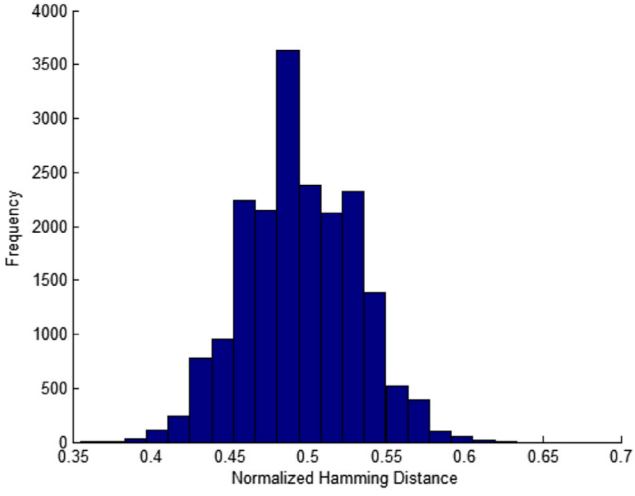


Fig. 7 – Pseudo-impostor distribution histogram.

Table 3 – EER of some recent template protection schemes.

	(Wang et al., 2012)	(Ahmad et al., 2011)	The proposed method
FVC2002-DB1	3.5%	9%	3.78%
FVC2002-DB2	5%	6%	6.68%
FVC2002-DB3	7.5%	27%	10.87%

- The system is vulnerable to the following attacks: (i) Stolen token attack, (ii) Full-rank based inversion from revoked templates, (iii) pseudo-inverse estimation attack.

In attack (i), the a priori information is the key Kz of the user z. In (ii) as in (iii), the a priori information is the key Kz of the user z and a set of related biocodes.

For the attack (i), if the FAR is not sufficiently low, an attacker can look for a pre-image (not necessary the exact one) to pass the verification step. Table 3 shows the EER (Equal Error Rate) of some recent developments of the literature. This informs that the challenge of finding a practical solution is still ongoing.

Further, as said by Takahashi and Hirata (2011): "this attack can be performed offline, i.e. without accessing the server, when both the transformed template and the corresponding parameter are known. Thus, it is much more serious than online dictionary attacks which can be prevented, e.g., by locking the system or alarming after some number of consecutive authentication failures".

As we can see, the threatening attacks are effective when the *key Kz as well as one or a set of related templates are known*. We mean by related templates, the biocodes of the same biometric feature generated by using different keys (for example, for one MinuCode, we can have different biocodes from multiple databases or after a periodicity of diversification from the same database). Even if it seems difficult to link related templates in our cancelable system, it may be possible to capture the reference transformed template from the centralized database itself. So, regarding the biometric information lifecycle (Fig. 8), the use of a central database may pose risks of administration and access to the biocodes of users. For the key management, as it is mentioned in (Wang and Hu, 2012), user-specific keys (whatever the transform used for the cancelable system) must be stored separately from the cancelable templates to prevent them being leaked at the same time.

So, if we ensure the confidentiality of the transformed template, such threats can be prevented. If we also store the key and the transformed template on mobile and disconnected devices, the stolen token attack becomes more difficult and would be better managed. As a solution we propose in the next section a MatchOnCard (MoC) system as a revocable

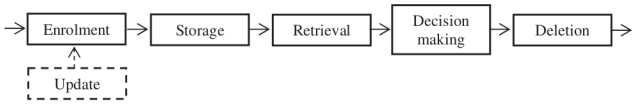


Fig. 8 – Biometric information lifecycle.

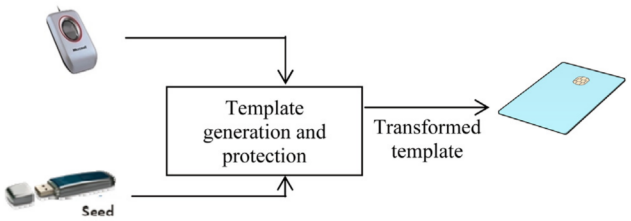


Fig. 9 – Principle of the 3-fector authentication system.

PKCS15 (PKCS15, 2000) applet. This 3-factor cancelable system is more robust to different attacks then the 2-factor traditional cancelable system.

4. MatchOnCard (MoC) PKCS15 revocable applet

4.1. *Basic ideas*

The proposed MoC PKCS15 revocable applet is based on some key ideas which are listed below:

1\ The previous robustness analysis showed the diversity property of the proposed cancelable system. However, if different related templates of the same user are revealed at the same time as the corresponding secret keys, the process may be vulnerable. A solution consists in protecting the confidentiality of the transformed template by a MoC system. Hence, it will never be exposed outside the card. This is further motivated by the easy implementation of biocodes matching process based on the calculation of a Hamming distance. Hence, a reasonably cheap microprocessor card (we choose a JavaCard) is sufficient to perform the matching.

2\ A 3-factor authentication system offers a better management of the stolen key scenario. In fact, if the key is stolen, it will be useless without the corresponding card. Both the stolen key and stolen card risks may exist (even if it's low), however this will be better managed on account of the cancelability property of the biometric system.

3\ The proposal of a PKCS15 (PKCS15, 2000) compatible implementation allows an easy integration of cancelable biometric systems in various applications (biometric identity card, web authentication, etc.) because of the broad industry adoption of PKCS15 specifications. It also helps to have a biometric and revocable PKCS15 card which offers a multiple-factor authentication and then more security.

4\ Considering card loss, the revocation process enables to change the stored reference biometric data to avoid any misuse of these cards.

5\ PKCS15 is an effective method to better manage the biometric information in open cards like javacard. It is secured and compliant with existing standards like PKCS11 (PKCS11, 1999) and ISO7816.

4.2. *The solution design*

The principle of the proposed MoC cancelable system (Fig. 9) is to generate a cancelable template from a biometric feature and a salt value and to store it in the smartcard. The secret seed has also to be stored in a secure element (token). The generated card performs the matching itself and returns the result to the outside world as a Yes/No response.

We now detail the internal management of the card. For this purpose, we propose a PKCS15-compliant management. PKCS15 is a standard defining data structures for storing information relating to cryptographic device security. It allows users to identify themselves to applications regardless of location in the support. PKCS15 design consists in an object oriented approach addressing how the keys, certificates and authentication objects are stored in the card. Fig. 10 shows a hierarchy of objects defined by PKCS15:

An object can be private (i.e. protected against unauthorized access) or public. Any kind of access to private objects is defined by authentication objects (PIN and/or Biometrics), where it is necessary to authenticate the cardholder before any operation.

Having a JavaCard as the target platform, the design of the PKCS15 applet is based on the construction of the following modules:

- Memory management.
- PKCS15 files management.
- PKCS15 objects management.

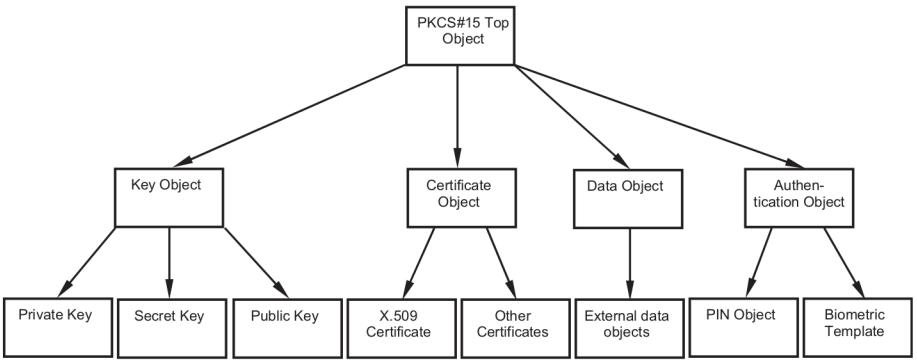


Fig. 10 – PKCS15 objects hierarchy (PKCS15, 2000).

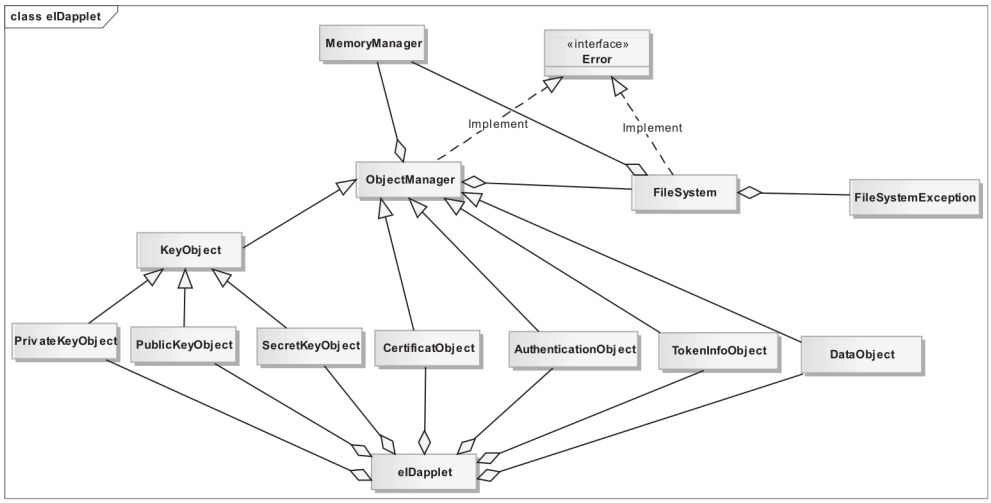


Fig. 11 – Class diagram of the PKCS15 applet.

- Security management.

We propose to manage the security of the applet at three levels:

- The use of ACL (Access Control List) to restrict access permissions to a file or an object.
- The use of authentication object codes such as PINs, biometrics or cryptographic keys.
- The permission to interact outside the world only through a set of commands (APDU) that must be defined.

We can now model the applet PKCS15 by the class diagram given in Fig. 11:

Table 4 contains all the classes included in the package installed on the JavaCard:

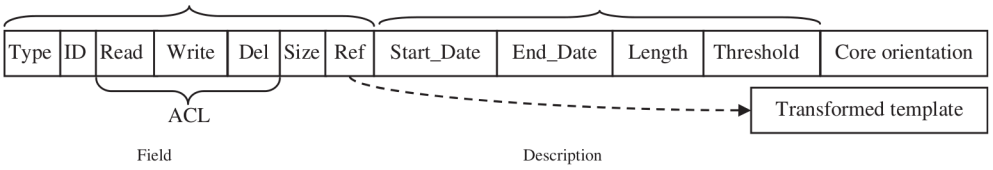
The detailed design of the applet is out of the scope of the present paper. We are only interested in the biometric parts. Our applet allows the use of 16 identities by which it is possible to authenticate the client applications (applications on the host):

- Identity 0 to 3: for PIN code authentication.
- Identity 4 to 12: for cryptographic Challenge/Response protocol based on RSA asymmetric key.
- Identity 13 to 14: for the biometric authentication protocol.
- Identity 15 is reserved.

The transformed template is secured by access restrictions. It is considered as private, so it cannot be read in any case. In case of revocation, it may be deleted or modified only by an administrator. An administrator is associated with

Table 4 – Description of the classes in the PKCS15 applet.

Classes	Descriptions		
MemoryManager	To manage the memory of the applet.		
FileSystem	To manage PKCS15 files.		
ObjectManager	Abstract class. To manage objects in the applet.		
	Subclasses	**Descriptions**	
	CertificatObject	To manage X.509 certificates	
	AuthenticationObjet	To manage authentication objects	
		Specialization	**Description**
		PIN objects	To manage PIN objects
		Biometric objects	To manage biometric objects
	DataObjet	To manage data objects	
	TokenInfo	Contains information about the card and the applet	
	Key	Abstract class. To manage key objects	
		Specialization	**Description**
		PrivateKey	To manage private keys
		PublicKey	To manage public keys
		SecKey	To manage symmetric keys
FileSystemException	To generate an exception in the case of a problem with the file system		
EIDApplet	Class that will retrieve and execute commands sent to the card		



Field	Description
TYPE	Authentication object (PIN, biometric), data object, certificate object, etc.
ID	A unique number that identifies the object.
ACL	Access Control List pour for managing access permissions.
SIZE	The size of the data actually written to the object.
REF	Contains the address of the data contained in the object.
Start_Date-End_Date	The biometric object is associated to an effective and expiration dates to allow the update of the template.
Length	The length of the template.
Threshold	The value of the decision threshold $\varepsilon_{\mathcal{D}}$.
Core orientation	The orientation of the core point if it exists, -1 else

Fig. 12 – The descriptor of the biometric object.

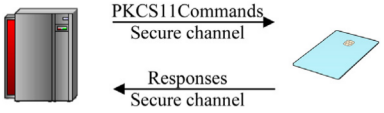


Fig. 13 – Channel exchange between the terminal and the card.

the identity 4 and is authenticated by the card using a challenge/response RSA protocol.

The biometric object is characterized by a descriptor that is located in the corresponding PKCS15 file (i.e. PrKDF for key objects and AODF for authentication objects). As shown on Fig. 12, a descriptor includes a set of common fields to all object types, in addition to type-specific field.

After the presentation of the internal management of the card, we are interested now in its external board. The requirements that must be met by a biometric match-on card solution are namely: increase security during personalization (enrollment)/post-personnalisation (revocation), provide security during user verification. To make our biometric solution trustworthy, we propose to add these requirements as below.e implement the enrollment/revocation/verification protocols by developing a compatible biometric cryptoki (CRYptographic TOKen Interface) application running on the card terminal station. The Cryptoki is an API that inherits the functionalities defined by the PKCS11 (PKCS11, 1999) standard.

The advantage of using PKCS11 standard on the card host is the compliance with standards that allow deployment and easy integration of our solution on different existing platforms. As shown on Fig. 13, a secure channel may be established between the card and the host to protect the exchanged messages when necessary (case of remote authentication). We recommend the reader interested in the establishment of a secure messaging protocol to refer to document (EMV CPS, 2007) initiated by EMV Corporation.

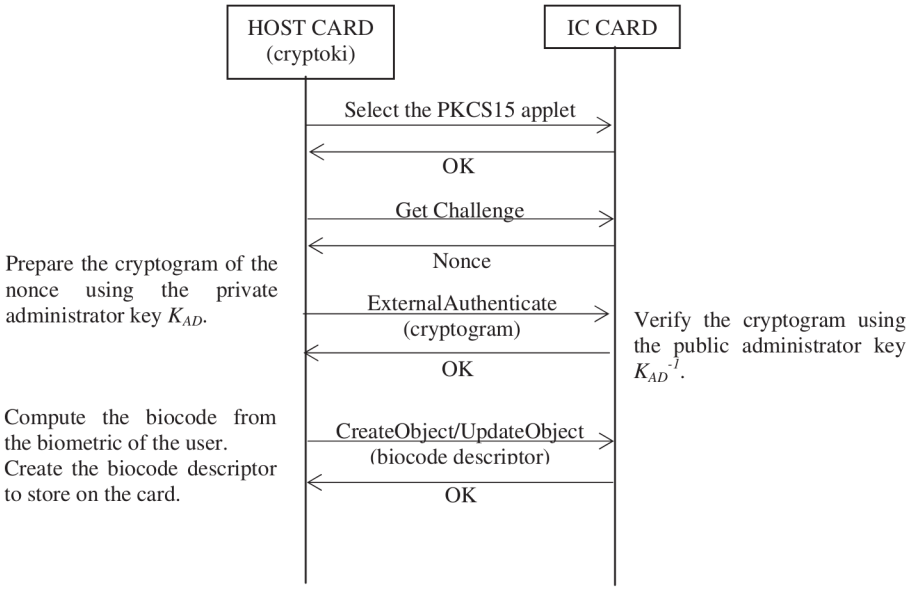


Fig. 14 – Commands exchanged in the Enrollment/Revocation phases.

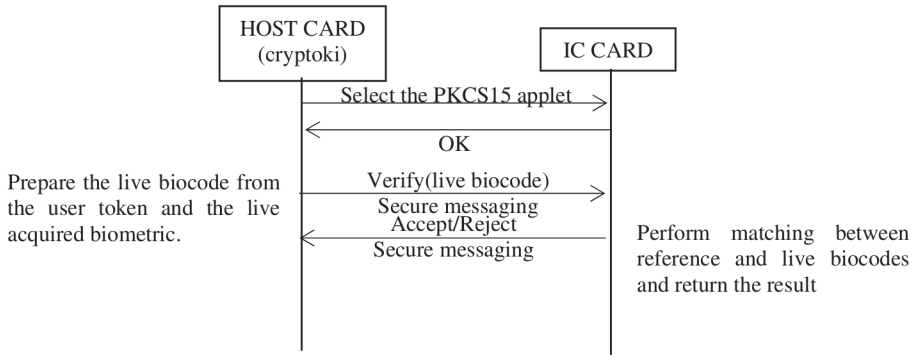


Fig. 15 – Commands exchanged in the verification phase.

Table 5 – Evaluation of the MoC system.

Evaluation criteria	Value	Remarks
A_1	5.97%\0	Unchanged compared to the system without card
A_2	0	Unchanged compared to the system without card
A_3	0	Unchanged compared to the system without card
A_4	0	If the card is not stolen, this attack is not effective
	7.16%	If the card is stolen the same time as the token, A4 keeps the same value as the system without the card but the stolen token attack is better managed. In fact, contrary to the system without the card, the detection whether authenticator, the token or the card, has been stolen is possible, before it is used illicitly. The legitimate user can then revoke its credentials.
A_5	0	Unchanged compared to the system without card
A_6	Impossible	This attack becomes impossible because biocode confidentiality is ensured by the access rights of the PKCS15 applet and the tamper proof factor of the card.
A_7	Impossible	This attack becomes impossible because biocode confidentiality is ensured by the access rights of the PKCS15 applet and the tamper proof factor of the card.
A_8	0	Unchanged compared to the system without card
A_9	0	Unchanged compared to the system without card
A_{10}	0	Unchanged compared to the system without card
A_{11}	0	Unchanged compared to the system without card
A_{12}	202	Unchanged compared to the system without card

We describe now the concerned phases:

- Enrollment/Revocation phases (Fig. 14)
- Verification phase (Fig. 15)

4.3. *Security analysis*

Still using our previously defined evaluation criteria, system analysis of the MoC system gives the results summarized in Table 5:

The analysis in Table 4 shows that the confidentiality of the reference template eliminates A6 and A7 threatening attacks and supports more effectively the stolen token attack while keeping the diversity property. Thus, we can say that with the proposed biometric closed system, we are able to achieve our goal of reaching a revocable biometric system, respecting the privacy and resistant to attack.

5. Conclusion

Cancelable fingerprint is a straightforward way to enhance the privacy of the biometric system. In this paper, we propose a Bio-Hashed minutiae cancelable system. However, because of the not very low FAR in the actual fingerprint cancelable systems, the user key and the reference template when leaked simultaneously may lead to the impersonation attack. Based on a proposed evaluation framework, we point out the relevance of the secure management of both the reference template than the user key. The security analysis shows also the diversity property of the given solution. However, if it happens that several revoked credentials are revealed at the same time, it will be feasible to approach an acceptable template in the protected domain. For this, the secure management primarily means keeping the key separately and ensuring the confidentiality of the cancelable template. Therefore, we propose to store this template in a closed module which also performs the matching with the live template. Hence, a JavaCard endowed with an open system was used as the secure device. The storage of the information in the card is managed by a pkcs15 compliant design. The pkcs15 allows a better card

management and allows an easy integration of our solution in different applications. By evaluating its performance, our proposition gives better resistance to attacks than the system without the card and thus suitable for real life applications.

REFERENCES

Ahmad T, Hu J, Wang S. Pair-polar coordinate-based cancelable fingerprint templates. Pattern Recognition 2011;44:2555–64.

ANSI X9.84. Biometric information management and security for the financial services industry. American National Standards Institute; 2010.

Belguechi R, Cherrier E, Rosenberger C, Ait-Aoudia S. Operational bio-hash to preserve privacy of fingerprint minutiae templates. IET Journal on Biometrics 2013:76–84.

Belguechi R, Cherrier E, Rosenberger C. How to evaluate transformation based cancelable biometric systems?. In: NIST international biometric performance testing conference 2012.

Boult T, Woodworth R. Privacy and security enhancements in biometricsIn Advances in biometrics. London: Springer; 2008.

Breebaart J, Busch C, Grave J, Kindt E. A reference architecture for biometric template protection based on pseudo identities. In: Proceedings of the special interest group on biometrics and electronic signatures (BIOSIG) 2008.

Bringer J, Chabanne H, Izabachène M, Pointcheval D, Tang Q, Zimmer S. An application of the Goldwasser–Micali cryptosystem to biometric authentication. LNCS, Springer 2007;4586:96–100.

Bringer J, Chabanne H. An authentication protocol with encrypted biometric Data. In: First international conference on cryptology in Africa 2008.

Cappelli R, Lumini A, Maio D, Maltoni D. Evaluating minutiae template vulnerability to masquerade attack. In: 5th workshop on automatic identification advances technologies (AutoID) 2007.

Chikkerur S. Online fingerprint verification system. M.S thesis. Univ of New York; 2005.

Davida GI, Frankel Y, Matt BJ. On the relation of error correction and cryptography to an offline biometric based identification scheme. In: Workshop on coding and cryptography 1999.

Daugman J. The importance of being random: statistical principles of iris recognition. Pattern Recognition 2003;36:279–91.

Dodis Y, Reyzin L, Smith A. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. Advance in Cryptology LNCS 2004;3027:523–40.

Draper SC, Khisti A, Martinian A, Vetroa A, Yedidia JS. Using distributed source coding to secure fingerprint biometrics. In: IEEE international conference on acoustics, speech and signal processing 2007.

EMV CPS. EMV card personalization specification – ver 1.1–. EMVCo; 2007.

Feng J, Jain AK. FM model based fingerprint reconstruction from minutiae template. In: International conference on biometrics (ICB) 2009.

Galbally J, Cappelli R, Lumini A, Maltoni D, Fierrez-Aguilar J. Fake fingertip generation from a minutiae template. In: 19th International conference on pattern recognition (ICPR2008), IBM best student award 2008.

Hao F, Anderson R, Daugman J. Combining cryptography with biometrics effectively. IEEE Transactions on Computers 2006;55:1081–8.

ISO/IEC 24745. Information technology – security techniques – biometric information protection; 2011.

Jain AK, Prabhakar S, Hong L, Pankanti S. Filterbank-based fingerprint matching. IEEE Transactions on Image Processing 2000;5:846–59.

Jin Z, Teoh ABJ, Ong TS, Tee C. Secure minutiae-based fingerprint templates using random triangle hashing. In: Proceedings of the 1st international visual informatics conference on visual informatics: bridging research and practice 2009.

Jin Z, Teoh ABJ, Ong TS, Tee C. Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. Expert Systems with Applications 2012;39:6157–67.

Juels A, Wattenberg MA. Fuzzy commitment scheme. In: 6th ACM conference on computer and communications security 1999. p. 28–36.

Juels A, Sudan MA. Fuzzy vault scheme. In: Proceedings of IEEE international symposium on information theory 2002.

Kumar G, Tulyakov S, Govindaraju V. Combination of symmetric hash functions for secure fingerprint matching. In: 20th International conference on pattern recognition 2010.

Lee C, Kim J. Cancelable fingerprint templates using minutiae-based bit-strings. Journal of Network and Computer Applications 2010;33:236–46.

Lee C, Choi JY, Toh KA, Lee S, Kim J. Alignment-free cancelable fingerprint templates based on local minutiae information. IEEE Transactions on Systems, Man and Cybernetics – Part B: Cybernetics 2007;37(4):980–92.

Li C, Hu J. Attacks via record multiplicity on cancelable biometrics templates. Concurrency and Computation:Practice and Experience 2013.

Linnartz JMG, Tuyls P. New shielding functions to enhance privacy and prevent misuse of biometric templates4th International conference on audio- and video-based biometric person authentication. LNCS, Springer 2003;2688:393–402. Heidelberg.

Lumini A, Nanni L. Empirical tests on biohashing. NeuroComputing 2006;69:2390–5.

Maio D, Maltoni D, Cappelli R, Wayman JL, Jain AK. Fvc2002: second fingerprint verification competition 2002. In: International conference on pattern recognition, 3; 2002. p. 811–4.

Nagar A, Rane S, Vetro A. Privacy and security of features extracted from minutiae aggregates. In: International conference on acoustics, speech and signal processing 2010.

Nagar A, Nandakumar K, Jain AK. Biometric template transformation: a security analysis. In: Proceedings of SPIE, electronic imaging, media forensics and security XII 2010.

PKCS11. Cryptographictoken interface standard. RSALaboratories; 1999.

PKCS15. Cryptographic token information syntax standard. RSALaboratories; 2000.

Quan F, Fei S, Anni C, Feifei Z. Cracking cancelable fingerprint template of Ratha. In: ISCSCT 2008.

Ratha NK, Chikkerur S, Connell JH, Bolle RM. Generating cancelable fingerprint templates. IEEE Transactions on Pattern Analysis and Machine Intelligence 2007;29:561–72.

Scheirer W, Boult T. Cracking fuzzy vaults and biometric encryption. In: Proc. of biometrics symposium 2007.

Simoens K, Tuyls P, Preneel B. Privacy weaknesses in biometric sketches. In: 30th IEEE symposium on security and privacy 2009.

Simoens K, Yang B, Zhou X, Beato F, Busch C, Newton EM, et al. Criteria towards metrics for benchmarking template protection algorithms. In: International conference on biometrics 2012.

Takahashi K, Hirata S. Parameter management schemes for cancelable biometrics. Computational Intelligence in Biometrics and Identity Management 2011;145:151.

Teoh ABJ, Ngo D, Goh A. BioHashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition 2004;37:11.
Teoh ABJ, Goh A, Ngo DCL. Random multispace quantisation as an analytic mechanism for BioHashing of biometric and random identity inputs. IEEE Transactions on Pattern Analysis and Machine Intelligence 2006;28:1892–901.
Teoh ABJ, Kuanb Y, Leea S. Cancellable biometrics and annotations on biohash. Pattern Recognition 2008;41:2034–44.
Tuyls P, Goseling J. Capacity and examples of template protection biometric authentication systems. In: Biometric authentication workshop 2004.
Wang S, Hu J. Alignment-free cancellable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach. Pattern Recognition 2012;45(12):4129–37. Elsevier.
Yang B, Busch C. Parameterized geometric alignment for minutiae-based fingerprint template protection. In: 3rd IEEE international conference on biometrics: theory, applications, and systems (BTAS) 2009.
Zhou X, Wolthusen SD, Busch C, Kuijper A. Feature correlation attacks on biometric privacy protection scheme. In: IEEE proc in 5th international conference on intelligent information hiding and multimedia signal processing 2009.
Zhou X, Kuijper A, Veldhuis R, Busch C. Quantifying privacy and security of biometric fuzzy commitment. In: IEEE proc in international joint conference on biometrics (IJCB) 2011.

Rima Belguechi obtained her Master in 2006 from the national school of computer science at Algiers. She is currently a PhD student under the supervision of Pr. Christophe Rosenberger. Her research interests include biometric template protection and security issues.

Estelle Cherrier is an Associate Professor at ENSICAEN, France. She obtained her Ph.D. degree from the Collegium ingénieur de l'Université de Lorraine in 2006. She works at the GREYC Laboratory where she is a permanent member of the research group in E-banking & Biometrics. Her research interests include Biometrics, signal processing and chaos system.

Christophe Rosenberger is a Full Professor at ENSICAEN, France. He obtained his Ph.D. degree from the University of Rennes I in 1999. He works at the GREYC Laboratory where he leads the research group in E-banking & Biometrics. His research interests include biometrics (definition of biometric systems and privacy issues). He is involved in developing authentication solutions for e-transactions applications.

Samy Ait-Aoudia is a Full Professor at national school of computer science at Algiers. He obtained his Ph.D. degree from the Ecole Nationale Supérieure des Mines, France in 1994. He works at the LMCS Laboratory where he leads the research group in image processing. His research interests include graphics, machine learning and pattern recognition.