Evaluation of Biometric Template Protection Schemes based on a Transformation

Christophe Rosenberger
Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France

Keywords: Biometric Template Protection, Security Analysis, Performance Evaluation.

Abstract: With more and more applications using biometrics, new privacy and security risks arise. New biometric schemes have been proposed in the last decade following a privacy by design approach: biometric template protection systems. Their quantitative evaluation is still an open research issue. The objective of this paper is to propose a new evaluation methodology for template protection systems based on a transformation by proposing some metrics for testing their performance and robustness to face attacks. These metrics enable us to estimate the probability of successful attacks considering different scenarios. We illustrate this evaluation methodology on two transformation based template protection schemes in order to show how some security and privacy properties can be checked by simulating attacks.

1 INTRODUCTION

Biometrics is an emerging technology for authentication applications. Many biometric modalities are well known and used (such as fingerprints), the design of intelligent sensors is advanced (liveness detection) and algorithms provide very good results. Privacy issues concerning this particular personal information still limit its operational use. In many countries, as for example, the central storage of biometric data is forbidden or limited to a small amount of users. In order to solve this problem, new biometric systems have been proposed in the last decade based on the ”privacy by design” paradigm. These biometric template protection schemes have for objective to guarantee the security and privacy of users to face attacks such as identity theft (e-government applications, border control, *etc.*) (Jain et al., 2008a).

Three main approaches can be distinguished dealing with template protection in biometrics. First, biometric crypto-systems or secure sketches, such as those presented in (Juels and Wattenberg, 1999; Chabanne et al., 2007), resort to cryptography. Second, secure computing methods aim at computing the comparison of two biometric templates by an untrusted party (Bringer et al., 2014; Chatterjee et al., 2016). Last, we find feature transformations approaches for template protection. The BioHashing algorithm is one of the most popular technique and is based on biometric data salting. It has been developed for different biometric modalities such as those presented in (Teoh et al., 2004; Belguechi et al., 2010; Saini and Sinha, 2011).

These last systems are called cancelable since the BioCode generated from a biometric template, can be revoked in case of interception or loss. This BioCode cannot be used as a cryptographic key as the generated BioCode is not exactly the same for each biometric capture. These particular biometric systems must of course address classical issues such as a high level of performance (*i.e.*, minimizing the Equal Error Rate (EER) or Area Under the Curve (AUC) value of the system) but also new constraints concerning privacy. In the literature, many papers have been published dealing with the definition of new schemes for the protection of biometric templates (such as those presented in (Ratha et al., 2007; Belguechi et al., 2010)). In order to validate their proposition, authors generally provide some experimental results based on performance evaluation (EER value, DET curves, *etc.*) and a security analysis by considering different scenarios. None standard methodology has been defined in order to qualify these schemes even if some previous research works have been proposed (Nagar et al., 2010; Nandakumar and Jain, 2015). These works do not provide any generic and computable quantitative metrics. This is the major contribution of this paper. We clearly list the properties that are requested for cancelable biometric systems, and we propose a quantitative-based evaluation framework to assess

Rosenberger, C.
Evaluation of Biometric Template Protection Schemes based on a Transformation.
DOI: 10.5220/0006550502160224
In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, pages 216-224
ISBN: 978-989-758-282-0

how the targeted system fulfills these properties. The quantitative approach easily allows the comparison of new cancelable biometric systems. The second contribution of the paper is the comparative study of two cancelable biometric systems namely the BioHashing and BioPhasor algorithms on fingerprints.

The plan of the paper is the following. Section 2 gives the background on template protection schemes based on a transformation. We also define the properties these biometric systems should follow. Section 3 is dedicated to a literature review on the evaluation of template protection schemes based on a transformation. We present the proposed methodology in Section 4. Some criteria that permit to assess the privacy compliance of a cancelable biometric system are proposed. Section 5 illustrates the proposed methodology on two cancelable biometric systems. We conclude and give some perspectives of this study in section 6.

2 BACKGROUND

In the sequel, we focus on template protection schemes using a transformation (see Figure 1) since some weaknesses have been reported in the former approach in (Simoens et al., 2009). A feature transformation is a function f using a key K (that is typically a random seed or a password), applied to a biometric template b. The transformed template $f(b,K)$ is stored in a database or in a personal device. During the authentication step, the same transformation is applied to the query template b' with the same key K and a comparison is realized between $f(b,K)$ and $f(b',K)$. It is generally considered that, given the transformed template $f(b,K)$ and the key K, it is possible to recover the original template b (or a close approximation) as presented in (Nagar et al., 2010). Thus, it is preferable to store securely this key, even if the reconstruction of the original template depends strongly to the used biometric modality. We suppose having a biometric modality where the template is represented by a vector of real values (it can be generalized to any representation like a map of interested points). We use the following notations like in the paper (Nagar et al., 2010). The decision result of cancelable biometric system is given by the following equation:

$$R_z = 1_{\{D_T(f(b_z,K_z),f(\acute{b_z},K_z))\leq\varepsilon\}} \tag{1}$$

Where:

- R_z: decision result for the verification of user z using the cancelable system,
- D_T: distance function in the transformed domain,
- f: the feature transformation function,
- b_z, $\acute{b_z}$ represent the template and query biometric features of user z,
- K_z: set of transformation parameters associated to user z,
- ε: decision threshold.

Cancelable systems must fulfill several properties, some of them are mentioned in (Maltoni et al., 2003):

- *Revocability/Renewability:* It should be possible to revoke a biometric template and to generate a new one from the original data. Given the biometric template of user z, through a transformation based cancelable biometric system, it should be possible to compute one BioCode $f(b_z,{K_z}^1)$ given parameters ${K_z}^1$ and to revoke it by computing $f(b_z,{K_z}^2)$ with other parameters ${K_z}^2$. As only the reference BioCode is stored, the revocability can be achieved easily.
- *Performance:* The template protection shall not deteriorate the performance of the original biometric system. As the performance is related to the security of the authentication process (*e.g.*, minimizing the number of false acceptance), a cancelable biometric system must be as efficient as possible. For transformation based cancelable biometric systems, the seed (contained in K_z for user z) can be seen as an *a priori* information (or a secret key). For this reason, a gain of performance is expected. To assess the efficiency of a biometric system (without any transformation), we generally consider two error metrics:

$$FRR_O(\varepsilon) = P(D_O(b_z,\acute{b_z}) > \varepsilon) \tag{2}$$

$$FAR_O(\varepsilon) = P(D_O(b_z,\acute{b_z}) \leq \varepsilon) \tag{3}$$

Where D_O is the distance between biometric templates, FRR_O is the false rejection rate and FAR_O is the false acceptance rate of the original biometric system (without any template protection). For a transformation based cancelable biometric system, we consider the two following metrics:

$$FRR_T(\varepsilon) = P(D_T(f(b_z,K_z),f(\acute{b_z},K_z)) > \varepsilon) \tag{4}$$

$$FAR_T(\varepsilon) = P(D_T(f(b_z,K_z),f(\acute{b_z},K_z)) \leq \varepsilon) \tag{5}$$

Where FRR_T is the false rejection rate and FAR_T is the false acceptance rate of the cancelable biometric system (with template protection).

- *Non-invertibility or Irreversibility:* From the transformed data, it should not be possible to obtain enough information on the original biometric data, to prevent any attack consisting in forging

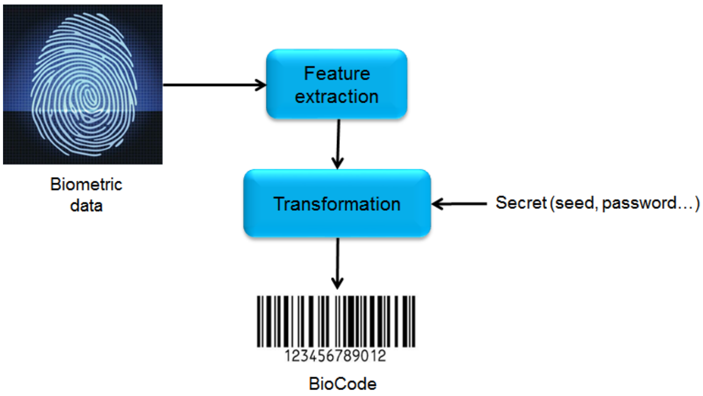

Figure 1: General principle of fingerprint template protection using a transformation.

a stolen biometric template (as for example, it is possible to generate an eligible fingerprint given minutiae (R. Cappelli and Maltoni, 2007)). This property is essential for security purposes. For any attack, an impostor provides an information in order to be authenticated as the legitimate user. The success of the attack is given by:

$$FAR_A(\varepsilon) = P(D_T(f(b_z, K_z), A_z) \leq \varepsilon) \qquad (6)$$

Where FAR_A is the probability of a successful attack by the impostor for a decision threshold set to ε. The A_z BioCode is computed by the impostor by taking into account as much information as possible within different contexts.

- *Diversity or Unlinkability:* It should be possible to generate different BioCodes for multiple applications, and no information should be deduced from the comparison or the correlation of different realizations. This is an important property for privacy issues as it avoids the possibility to trace an individual based on the authentication information. Let be $B_z = \{f(b_z, K_z{}^1), .., f(b_z, K_z{}^Q)\}$ a set of Q generated BioCodes for user z and $K_z{}^i$ the set of parameters for user z for the ith revocation, it shall constitute a random sub-sampling of $\{0,1\}^Q$. This property prevents also the linkage attack consisting in using different BioCodes of an user to predict an admissible one. This is related to an attack consisting in for an impostor to listen different realizations of BioCodes for the same user.

3 RELATED WORKS

The evaluation of template protection schemes is not the most studied area in biometrics. Few works focus on the proposal of a quantitative and objective evaluation of template protection schemes. We believe it is an important topic nowadays in biometrics. In order to illustrate the benefits of a template protection scheme, authors use a classical evaluation methodology (Wang and Hu, 2014). DET curves are used to estimate the performance of the biometric system (with template protection) describing False acceptance rate versus Genuine Acceptance Rate (Isobe et al., 2013). The security of the template protection scheme is usually estimated by considering the stolen token attack (secret known by the impostor) by looking at the degradation of performance (Jain et al., 2008b). A more recent work listed different criteria or requirements a template protection scheme must fulfill (Simoens et al., 2012) but no quantitative and objective measure is proposed. A recent work by Jain et al. (Nandakumar and Jain, 2015) proposed many ways to compute non-invertibility of template protection schemes. This is interesting but limited for this requirement. Even the work done by Nagar et al. (Nagar et al., 2010) is older, it is clearly more interesting as the main security and privacy requirements are considered. Some quantitative measures are proposed mainly based of DET curves to estimate the robustness of the template protection schemes. These measures are not easy to understand as all measures depend on the decision threshold value of the biometric system. We believe a small amount of measures should be more interesting in order to compare template protection schemes. We propose in this paper to improve this analysis by computing some metrics measuring the performance and security efficiency of such template protection schemes.

4 EVALUATION METHODOLOGY

This section is devoted to the definition of a framework to verify if the properties defined in section 2 are fulfilled by a cancelable biometric system. Based on some of the early works (Ratha et al., 2001), (Bolle et al., 2002) which identified weak links in each subsystem of a generic authentication system, some papers considered the possible attacks in cancelable biometric systems (such as those presented in (Teoh et al., 2008; Jain et al., 2008a; Nagar et al., 2010; Saini and Sinha, 2011)). We go further in this paper: given a cancelable biometric system, how can we verify if these properties are fulfilled ? Is it possible to quantify the risk associated to the feasibility of an attack limiting one of these properties ? We propose in the next section some measures and attacks to answer these two questions.

4.1 Evaluation Metrics

We follow the Shannon's maxim ("The enemy knows the system"), we so assume that the impostor has all necessary information on the process used to generate the BioCode (feature generation method, BioCode size...). Note that the following study requires that the decision threshold ε to be set. In this paper, we set the decision threshold ε_{EER_T} to the EER value of the cancelable biometric system (after template protection). Even if this functioning point of the biometric system has no operational meaning, it is often used and can always be estimated. Different other values can be used for ε depending on the security requirements of the application. In order to quantify the robustness of the studied cancelable biometric system, we suppose having a biometric database with multiple biometric samples for each user. Some samples permit to generate the biometric template of each user while the others are used for the tests.

We detail below how we quantify if the properties previously mentioned are fulfilled: nine criteria are described below. For each criterion, a value $A_i \in [0,1]$, $i = 1,\dots,9$ is computed on the template protection scheme (there is at least one criterion for one required property). The security and privacy analysis can be done for the two classical steps in biometrics *authentication* (proof of identity) or *identification* (determination of the identity). In this paper, we focus on the *authentication* problem (one against one matching): we develop different attack scenarios that an impostor would manage to impersonate a particular legitimate user.

1. Performance (A_1): To verify if the efficiency of the biometric system is not decreased by using the template protection scheme, we propose to compute the following measure:

$$A_1 = 1 - \frac{\mathrm{AUC}(\mathrm{FAR_T},\mathrm{FRR_T})}{\mathrm{AUC}(\mathrm{FAR_O},\mathrm{FRR_O})} \qquad (7)$$

where *AUC* denotes the area under the ROC curve (to be as low as possible) for both systems (original and after transformation). The AUC value is computed considering the False Acceptance Rate (FAR) and False Rejection Rate (FRR) for different thresholds values. Many cases are interesting to consider. First, it may happen that $A_1 = 1$ meaning that the cancelable biometric system provides a perfect performance (without any error or $AUC(FAR_T, FRR_T) = 0\%$). Second, if the value A_1 is negative, it means that the efficiency of the biometric system is deteriorated by the template protection scheme. Otherwise, the scheme improves performance.

2. Non-invertibility or Irreversibility (A_2 to A_6): This important property can be evaluated through different attacks. For all these attacks, we use one or multiple biometric samples to generate an admissible query $\acute{b}_z$ of the user z. Based on the scenario of each attack, we generate many fake attempts A_z of the genuine user (as described in equation 6):
   - *Zero effort attack* (A_2):
     an impostor user x provides its own biometric feature $\acute{b}_x$ and parameter K_x to impersonate user z : $A_z = f(\acute{b}_x, K_x)$
   - *Brute force attack* (A_3):
     An impostor tries to be authenticated by trying different random values of A: $A_z = A$
   - *Stolen token attack* (A_4):
     An impostor has obtained K_z of the genuine user z and tries different random values b to generate: $A_z = f(b, K_z)$
   - *Stolen biometric data attack* (A_5):
     An impostor knows $\acute{b}_z$ (directly or after computation of the feature on a biometric raw data) and tries different random numbers K to generate: $A_z = f(\acute{b}_z, K)$
   - *Worst case attack* (A_6):
     An impostor user x provides its own biometric feature $\acute{b}_x$ and parameter K_x to be authenticated as the user z (zero effort attack) and has also obtained the token K_z of the genuine user z to generate: $A_z = f(b_x, K_z)$

To evaluate the efficiency of these five attacks, we propose to compute for each of them, the following criteria while computing A_z differently for each scenario:

$$A_i = P(D_T(f(b_z,K_z),A_z) \leq \varepsilon_{EER_T})\ i = 2:6 \quad (8)$$

These metrics correspond to the probability of successful attack by an impostor for each scenario when the template protection systems sets ε_{EER_T} as decision threshold. Indeed, from the impostor point of view, the FAR is the relevant value: the intruder has to generate $f(\acute{b_z},K_z)$ using different available data (K_z, $\acute{b_z}\ldots$). Recall that the threshold has been set to the value ε_{EER_T} (obtained by computation of the EER of the cancelable biometric system without any attack). From the impostor's point of view, the values A_i, $i = 2,\ldots,6$ must be as high as possible. These values allow us a ranking of the different attacks and directly gives the risk for the system that an impostor can be authenticated as a genuine user.

3. Diversity or Unlinkability (A_7 to A_9) :
   A prominent feature of a cancelable biometric system is its ability to produce different BioCodes for the same individual and for different applications. The first criterion we want to assess concerns the unlinkability property for privacy issues.

   - *Mutual information of BioCodes:* In order to measure the diversity property in this case, we propose to compute the mutual information provided by several BioCodes issued from the same biometric data as defined in equation (9):

     $$I(X,Y) = \sum_x \sum_y P(x,y) \log(\frac{P(x,y)}{P(x)P(y)}) \quad (9)$$

     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 individual. The value A_7 is then computed using the average value for all users of the highest value of mutual information, according to equation 10:

     $$A_7 = \frac{1}{N} \sum_z \sum_{j=1}^{M} \max(I(f(b_z,K_z), f(b_z^j,K_z))) \quad (10)$$

     Where:

     - b_z: denotes the biometric template of the individual z in the database,
     - b_z^j: denotes the j^{th} biometric query of the individual z in the database,
     - N: the number of individuals in the database,
     - M: the number of generated BioCodes for each individual,
     - P: the estimation of the probability.

     The A_7 permits to compute the correlation of BioCodes generated from the same biometric template with different keys. A low value of A_7 is expected.

   - *Listening attacks:* An impostor must not be able to extract any information from different BioCodes issued from the same user. Since BioCodes can be revoked, an impostor can intercept Q of them and issue a new BioCode by predicting an admissible value (as for example by setting each bit to the most probable value). These attacks are tested given by the following process:

     - Generation of Q BioCodes for user z: $B_z = \{f(b_z,{K_z}^1),..,f(b_z,{K_z}^Q)\}$
     - Prediction of a possible BioCode by setting the most probable value of each bit given B_z,
     - Computation of equation (8).
       ⇒ A_8 value for $Q = 3$ and A_9 for $Q = 11$

     We considered two values of Q: $Q = 3$ corresponds to a realistic attack (getting three keys) and $Q = 11$ can be considered as the worst one. Of course, more complex prediction methods of the BioCode given B_z could be proposed. This is one perspective of this work. An evolution of the efficiency of this attack (depending on the evolution of Q) may be used to predict how many interceptions are necessary for the intruder to achieve an authentication.

These criteria allow us to quantify the robustness of cancelable biometric systems based on feature transformation.

5 ILLUSTRATIONS

We apply the proposed methodology on two popular template protection schemes: BioHashing (Teoh et al., 2004) and BioPhasor (Teoh and Ngo, 2006). We detail briefly each algorithm.

The Biohashing algorithm is applied to biometric templates, represented by real-valued vector of fixed length (the metric used to evaluate the similarity between two biometric features is the Euclidean distance) and generates binary templates of length lower or equal to the original length (the metric used to evaluate the similarity between two transformed templates is the Hamming distance). This algorithm has been originally proposed for face and fingerprints by Teoh *et al.* in (Teoh et al., 2004), where the fingerprint features are, in a first time, transformed in a real-values vector of fixed length to generate the biometric

Algorithm 1: BioHashing.

```
Inputs
$b = (b^1, \dots, b^n)$: biometric template
$K$: seed value
Output $B = (B^1, \dots, B^m)$: BioCode
Generation with $K$ of $m$ pseudo-random vectors $V_1, \dots, V_m$ of length $n$,
Orthogonalize vectors with the Gram Schmidt algorithm,
for $i = 1, \dots, m$ do compute $x_i =< b, V_i >$.
end for
Compute BioCode:
    $$B^i = \begin{cases} 0 & \text{if} \quad x_i < \tau \\ 1 & \text{if} \quad x_i \geq \tau, \end{cases}$$
    where $\tau$ is a given threshold, generally equal to 0.
```

template (this step is not useful and not described in this paper).The Biohashing algorithm is applied, in a second time, on the biometric template and generates a binary BioCode. At the end of the enrollment phase, the biometric template is discarded and only the BioCode is stored. The biohashing algorithm can be applied on any biometric modalities, that can be represented by a real values vector of fixed length. The Biohashing algorithm transforms the biometric template $b = (b^1, \dots b^n)$ in a binary template $B = (B^1, \dots B^m)$, with $m \leq n$, as described in Algorithm 1. The performance of this algorithm is ensured by the scalar products with the orthonormal vectors. The quantization process of the last step ensures the non-invertibility of the data (even if $n = m$, because each coordinate of the input b is a real value, whereas the coordinates of the output B is a single bit). Finally, the random seed guarantees the diversity and revocability properties.

The BioPhasor algorithm (Teoh and Ngo, 2006) is supposed to be an improvement of the BioHashing one. It is described in Algorithm 2.

Algorithm 2: BioPhasor.

```
Inputs
$b = (b^1, \dots, b^n)$: biometric template
$K$: seed value
Output $B = (B^1, \dots, B^m)$: BioCode
Generation with $K$ of $m$ pseudorandom vectors $V_1, \dots, V_m$ of length $n$,
Orthogonalize vectors with the Gram Schmidt algorithm,
for $i = 1, \dots, m$ do compute $h_i = 1/n \sum_j^n arctan(b^{j^2}/V_i^j)$.
end for
```

5.1 Experimental Protocol

We detail the protocol we followed in this comparative study. We used three fingerprint databases, each one is composed of 800 images from 100 individuals with 8 samples from each user. These databases have been used for competitions (Fingerprint Verification competition) in 2002 and 2004 (FVC2002 DB2, FVC2004 DB1 and FVC2004 DB3). We used Gabor features (GABOR) (Manjunath and Ma, 1996) of size n=512 (16 scales and 16 orientations) as biometric template. These features are very well known and permit a good texture analysis of a fingerprint (Belguechi et al., 2016). For each user in a dataset, we used the first sample as reference template. Others are used for testing the proposed scheme. We compute BioCodes with the BioHashing and BioPhasor algorithms of different sizes (32 to 512 bits). Concerning performance assessment, we compute legitimate scores by comparing all samples belonging to one individual with the associated reference template. For each dataset, we obtain $7 \times 100 = 700$ legitimate scores. Impostor scores are obtained by comparing each sample belonging to another individual with the reference template of the considered user. For each dataset, we obtain $7 \times 100 \times 99 = 69300$ impostor scores. These scores allow us to compute the AUC performance metric to compute A_1 and the threshold associated to the EER value. Considering attacks, we replace each test sample by the sample A_z generated by the impostor following the different scenarios A_2 to A_6, A_8 and A_9.

5.2 Experimental Results

We first present the value of the nine metrics $A_i, i = 1:9$ for the BioHashing and BioPhasor algorithms in Tables 1 and 2. We start by commenting metrics A_1 and A_7 that are not related to an attack. If we consider A_1, we see clearly that these two algorithms obtain a value near 1 meaning the obtained performance after applying the transformation is defined by EER=0%. That also illustrates the fact that considering the ε_{EER_T} value as threshold for attacks is not a bad idea (as the performance is optimal in an operational mode for this configuration). For the BioHashing algorithm, if the size of the BioCode is low (64 or 32 bits), the ERR is not exactly 0% that is why A_1 is not equal to 1. The A_7 metric related to the mutual information is the same for the two algorithms and is more related to the complexity of the datasets (see Table 1).

Now, if we consider attacks, we see clearly that most of attacks obtain a low probability except A_6.

Table 1: Biohashing analysis for the three datasets and for different sizes of the BioCode.

Size	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9
512	1	0	0	0	0	1	0.36	0	0
256	1	0	0	0	0	1	0.36	0	0
128	1	0	0	0	0	0.99	0.36	0	0
64	0.99	0	0	0.02	0	0.99	0.36	0	0
32	0.98	0.03	0	0.19	0.03	0.94	0.36	0.03	0.07
512	1	0	0	0	0	1	0.46	0	0
256	1	0	0	0	0	0.99	0.46	0	0
128	0.99	0	0	0	0	0.99	0.46	0	0
64	0.99	0.01	0	0.09	0	0.99	0.46	0.01	0.02
32	0.92	0.07	0	0.4	0.06	0.93	0.46	0.12	0.12
512	1	0	0	0	0	0.99	0.62	0	0
256	1	0	0	0	0	0.99	0.62	0	0
128	0.99	0	0	0	0	1	0.62	0	0
64	0.99	0	0	0.01	0	1	0.62	0	0
32	0.84	0.02	0	0.18	0.02	0.95	0.62	0.05	0.05

Table 2: BioPhasor analysis for the three datasets and for different sizes of the BioCode.

Size	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9
512	1	0	0	0	0	0.99	0.36	0	0
256	1	0	0	0	0	1	0.36	0	0
128	1	0	0	0	0	1	0.36	0	0
64	1	0	0	0.28	0	0.99	0.36	0	0
32	0.99	0	0	0.84	0	0.99	0.36	0	0
512	1	0	0	0	0	0.99	0.46	0	0
256	1	0	0	0	0	1	0.46	0	0
128	1	0	0	0	0	1	0.46	0	0
64	1	0	0	0	0	0.99	0.46	0	0
32	1	0	0	0	0	0.99	0.46	0	0
512	1	0	0	0	0	1	0.62	0	0
256	1	0	0	0	0	1	0.62	0	0
128	1	0	0	0	0	0.99	0.62	0	0
64	1	0	0	0	0	0.99	0.62	0	0
32	1	0	0	0	0	0.99	0.62	0	0

When the BioCode size is low, the BioHashing can be attacked with different scenarios. That is not the case for the the BioPhasor algorithm that is much more robust. The big problem is related to the A_6 metric for the worst case scenario. In this context, the impostor has obtained the K_z (transformation parameters) for user z to impersonate and used his/her own biometric data (zero effort attack). These two algorithms are not robust to this attack (it is known but the proposed methodology permits to valuate it). When the BioCode size is low and for the BioHashing algorithm, this probability is not exactly 1. This can be explained by the fact the performance as mentioned earlier is not perfect. The main benefit of these metrics is to have quantitative and objective measures to assess and compare template protection schemes based on a transformation. If we want a more detail on attacks, we can consider some curves describing the evolution of the probability of successful attack for each scenario related to the decision threshold value. Figures 2 and 3 present these curves for the two considered algorithms for two BioCodes sizes (32 and 512 bits) for the first dataset (others are similar). These curves allow us to compare the efficiency of attacks from the most efficient (worst case) to the less one (brute force). We show the value of the ε_{EER_T} by a black dot line. The value of the metrics corresponds to the probability of successful attack for this point. This evaluation methodology has been implemented in Matlab in order to automatically compute these metrics and curves. The computation time to generate these 9 metrics depends on the BioCode size. For 32 bits, it takes less one minute but for 512 bits, computations take approximatively 3 hours using Matlab on a computer (I7 with 2.4GHz).

6 CONCLUSION AND PERSPECTIVES

The protection of biometric data is a crucial trend in computer security as it becomes a classical tool for authentication. We proposed in this paper an evaluation methodology to estimate the performance and robustness of template protection schemes based on the transformation of biometric raw data. The benefit of this solution is to measure with quantitative metrics the efficiency of well known attacks on these protection schemes. With this methodology, we are able to compare objectively different transformations. The proposed solution is also very important for the designing of such protection schemes. Perspectives of this study is first a comparative study of the main protection schemes based on biometric transformation. Many such transformations have been proposed in the last decade, as it represents an efficient way to protect biometric raw data (even in embedded devices). Second, we intend to design our own transformation minimizing the proposed metrics.

REFERENCES

Belguechi, R., Hafiane, A., Cherrier, E., and Rosenberger, C. (2016). Comparative study on texture features for fingerprint recognition: application to the biohashing template protection scheme. *Journal of Electronic Imaging*, 25(1):013033–013033.

Belguechi, R., Rosenberger, C., and Aoudia, S. (2010). Biohashing for securing minutiae template. In *Proceedings of the 20th International Conference on Pattern Recognition*, pages 1168–1171, Washington, DC, USA.

Bolle, R., Connell, J., and Ratha, N. (2002). Biometric perils and patches. *Pattern Recognition*, 35(12):2727–2738.

Bringer, J., Chabanne, H., Favre, M., Patey, A., Schneider, T., and Zohner, M. (2014). Gshade: faster privacy-preserving distance computation and biometric identification. In *Proceedings of the 2nd ACM workshop on Information hiding and multimedia security*, pages 187–198. ACM.

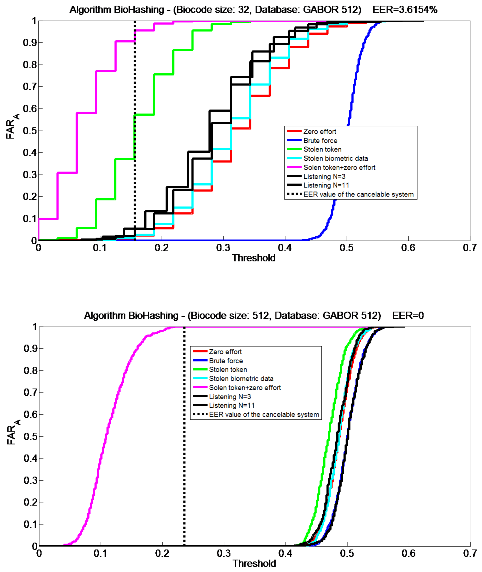

Figure 2: Probability of successful attack for the BioHashing algorithm with the BioCode size 32 (up) and 512 (down).

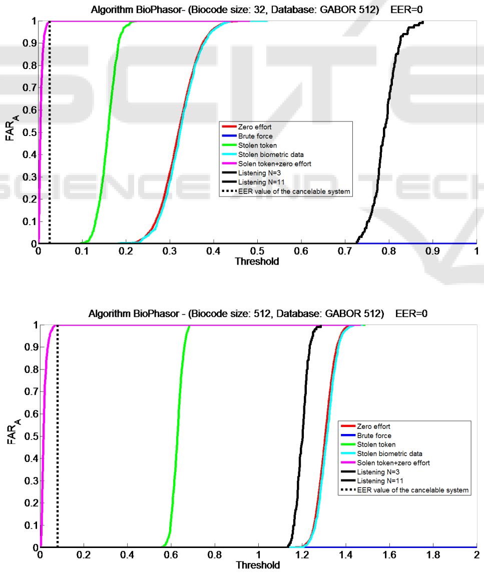

Figure 3: Probability of successful attack for the BioPhasor algorithm with the BioCode size 32 (up) and 512 (down).

Chabanne, H., Bringer, J., Cohen, G., Kindarji, B., and Zemor, G. (2007). Optimal iris fuzzy sketches. In *IEEE first conference on biometrics BTAS*.

Chatterjee, S., Roy, S., Das, A. K., Chattopadhyay, S., Kumar, N., and Vasilakos, A. V. (2016). Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment. *IEEE Transactions on Dependable and Secure Computing*.

Daugman, J. (2004). Iris recognition and anti-spoofing countermeasures. In *7-th International Biometrics conference*.

Isobe, Y., Ohki, T., and Komatsu, N. (2013). Security performance evaluation for biometric template protection techniques. *International Journal of Biometrics*, 5(1):53–72.

Jain, A., Nandakumar, K., and Nagar, A. (2008a). Biometric template security. In *EURASIP Journal on Advances in Signal Processing*.

Jain, A. K., Nandakumar, K., and Nagar, A. (2008b). Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008:113.

Juels, A. and Wattenberg, M. (1999). A fuzzy commitment scheme. In *ACM conference on Computer and communication security*, pages 28–36.

Lee, C. and Kim, J. (2010). Cancelable fingerprint templates using minutiae-based bit-strings. *J. Netw. Comput. Appl.*, 33:236–246.

Maltoni, D., Maio, D., Jain, A., and Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*. Springer.

Manjunath, B. S. and Ma, W. (1996). Texture features for browsing and retrieval of image data. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18:37–42.

Nagar, A., Nandakumar, K., and Jain, A. K. (2010). Biometric template transformation: A security analysis. *Proceedings of SPIE, Electronic Imaging, Media Forensics and Security XII*.

Nandakumar, K. and Jain, A. K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine*, 32(5):88–100.

R. Cappelli, A. Lumini, D. M. and Maltoni, D. (2007). Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis Machine Intelligence*, 29:1489–1503.

Ratha, N., Chikkerur, S., Connell, J., and Bolle, R. (2007). Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4):561–572.

Ratha, N., Connelle, J., and Bolle, R. (2001). Enhancing security and privacy in biometrics-based authentication system. *IBM Systems J.*, 37(11):2245–2255.

Saini, N. and Sinha, A. (2011). Soft biometrics in conjunction with optics based biohashing. *Optics Communications*, 284(3):756 – 763.

Simoens, K., Chang, C., and Preneel, B. (2009). Privacy weaknesses in biometric sketches. In *30th IEEE Symposium on Security and Privacy*.

Simoens, K., Yang, B., Zhou, X., Beato, F., Busch, C., Newton, E. M., and Preneel, B. (2012). Criteria towards metrics for benchmarking template protection algorithms. In *Biometrics (ICB), 2012 5th IAPR International Conference on*, pages 498–505. IEEE.

Teoh, A., Kuanb, Y., and Leea, S. (2008). Cancellable biometrics and annotations on biohash. *Pattern recognition*, 41:2034–2044.

Teoh, A. and Ngo, D. (2006). Cancellable biometrics realization through biophasoring. In *Proceedings of 9th*

IEEE International Conference on Control, Automation, Robotics and Vision (ICARCV'06).

Teoh, A., Ngo, D., and Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 40.

Tyagi, H. and Watanabe, S. (2014). A bound for multiparty secret key agreement and implications for a problem of secure computing. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 369–386. Springer.

Wang, S. and Hu, J. (2014). Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. *Pattern Recognition*, 47(3):1321–1329.