Preimage Attack on BioHashing

Patrick Lacharme, Estelle Cherrier, Christophe Rosenberger

Preimage attack on BioHashing

Patrick Lacharme, Estelle Cherrier and Christophe Rosenberger
Normandie Univ, France ; UNICAEN, GREYC, F-14032 Caen, France; ENSICAEN, GREYC, F-14032 Caen, France; CNRS, UMR 6072, F-14032 Caen, France
{*patrick.lacharme, estelle.cherrier, christophe.rosenberger*}*@ensicaen.fr*

Keywords: Biometrics, Security, Privacy, Data Protection, Cancelable Biometrics, BioHashing, Spoofing Attacks, Genetic Algorithms

Abstract: Biometric recognition is more and more employed in authentication and access control of various applications. Biometric data are strongly linked with the user and do not allow revocability nor diversity, without an adapted post-processing. Cancelable biometrics, including the very popular algorithm BioHashing, is used to cope with the underlying privacy and security issues. The principle is to transform a biometric template in a BioCode, in order to enhance user privacy and application security. These schemes are used for template protection of several biometric modalities, as fingerprints or face and the robustness is generally related to the hardness to recover the original biometric template by an impostor. In this paper, we propose to use genetic algorithms to approximate the original biometric feature and spoof the authentication system. We show through experimental results on fingerprints the efficiency of the proposed attack on the BioHashing algorithm, by approximating the original FingerCode, given the seed and the corresponding BioCode.

1 INTRODUCTION

Biometrics is a major concern for privacy as it has a direct link with the user and is generally non revocable, without an adapted post-processing. Indeed, if a biometric data is stolen or compromised, it is difficult (if not impossible) to revoke it, contrary to a classical password. Moreover, the same biometric data may be used for several applications, resulting in important threats for the security, in the absence of a strong diversification process. In the same time, biometrics is more and more deployed in various applications, as in electronic passport, access control, electronic payment or forensics applications. Common vulnerabilities of biometric schemes include spoofing and replay attacks or collection of biometric data without the consent of people. As a consequence, biometrics development provides an important technological challenge for data security and user privacy (Cavoukian and Stoianov, 2009).

Biometric template protection schemes are a group of technologies, included in privacy enhancing technologies, used to enhance both privacy and security of biometric data. Therefore, any template protection approach should allow the possibility to revoke a biometric data in case of interception, and should be carefully designed, with a strong security analysis. Among the different solutions in the literature, template protection can be achieved using biometric cryptosystems or by cancelable biometrics (Rathgeb and Uhl, 2011). These biometric template protection schemes strongly depend on the biometric modalities. For example an Iriscode, encoded as a binary vector of 256 bytes could not be protected in the same way than a set of minutiae of varying lengths. Some of these schemes have been recently normalized in the standard ISO 24745 (ISO, 2011).

The concept of cancelable biometrics relies on a transformation of the raw biometric data, enabling the transformed data to address security and privacy protection issues. The general principle consists in the generation of a new biometric template, from the biometric feature vector (such as texture parameters) and a random number. Therefore, it can be seen as a two-factor authentication scheme. At the enrolment stage, once transformed, the new template (or transformed template) is stored in the database, while the original raw biometric vector is discarded and never kept. At the verification stage a comparison is performed between two transformed templates: between the one the user pretends to correspond and between the one he/she presents to the system. Hence, to be authenticated, a user must present the same biometric data (more precisely a similar biometric data) and the same random number. However this random number is generally not considered as secret, in the sense that it is

generally stored with the transformed template for the verification step. Cancelable biometric systems must meet the following four criteria, (Maltoni et al., 2003; Jain et al., 2008; Nagar et al., 2010):

- *Performance*
  The template transformation should not significantly decrease the technical performance of the original biometric system (accuracy).
- *Revocability*
  It should be possible to revoke a biometric template in case of compromission, and to generate a new one from the original data.
- *Irreversibility*
  From the transformed data, it should not be possible to obtain enough information about the original biometric data.
- *Unlinkability*
  It should be possible to generate different transformed data for multiple applications, and no information should be deduced from the comparison or the correlation of different realizations.

The advantage of cancelable biometrics lies in the ease of revoking the transformed template, by simply changing the associated random number. Another interest lies in the possibility to generate different templates to authenticate oneself to different services from the same biometric raw data, with distinct random numbers (one for each service). Thus, the random number should only be used for diversification and revocability purposes and not for the security, without a secure storage. More precisely, the security of any cancelable biometric process requires the associated transformation to be non invertible: it means that it should be hard for an intruder to recover the original raw biometric vector from the transformed template and the random number. Notice that with this commonly admitted definition of the non-invertibility property, the possibility to approximate the original biometric feature vector, given the transformed template and the associated random number, is not considered. Nevertheless, the reconstruction of such sufficiently similar biometric templates, called preimage attack, is a major flaw for cancelable biometric schemes, because in this case, the authentication system could be spoofed. Different definition for irreversibility are detailed in (Simoens et al., 2012) with several criteria: *full-leakage irreversibility*, *authorized-leakage irreversibility* and *pseudo-authorized leakage irreversibility*. For example, it is possible to generate an eligible fingerprint given minutiae (Cappelli et al., 2007).

The BioHashing algorithm is one of the most popular cancelable biometric scheme, proposed for face biometrics in (Goh and Ngo, 2003) and later for fingerprints in (Teoh et al., 2004), which will be detailed hereafter. The invertibility of the Biohashing algorithm has been firstly investigated in (Cheung et al., 2005; Lee et al., 2009). Recently, Nagar et al. presented a method based on optimization problems, to recover a close approximation of face images, generated by the Biohashing algorithm (Nagar et al., 2010).

The main contribution of this paper is to analyze this vulnerability of cancelable biometrics. We propose a new method to generate a biometric feature vector approximating the original biometric feature, based on genetic algorithms. Experiments are carried out on fingerprint modality, with the BioHashing algorithm, using the FVC2002 benchmark.

This paper is organized as follows. Section 2 provides a presentation of cancelable biometric schemes, with a description of the BioHashing algorithm. Section 3 then introduces genetic algorithms and their application to template approximation. Finally, Section 4 proposes experimental results on the FVC2002 database with the BioHashing algorithm.

2 BIOMETRIC DATA PROTECTION

Biometric systems are used for identification or authentication purpose. Identification process generally involves a large database of biometric templates and the verification phase consists in recovering the corresponding template in the database. The centralized storage of non-protected biometric data is a major threat for user privacy. Biometric authentication does not necessarily use a centralized database and many applications require an additional secure element as a smart card for biometric data storage. However, the centralized storage of protected biometric data is a possible alternative, if this centralized approach is not a privacy nor a security threat for the system.

2.1 Biometric cryptosystems

Biometric cryptosystems associate a secret key with a biometric template in order to protect the latter. It includes *fuzzy commitment*, (Juels and Wattenberg, 1999) and *fuzzy vaults*, (Juels and Sudan, 2002). Fuzzy commitments are based on error correcting codes and do not require the storage of the biometric template. They have numerous applications on iris data (Hao et al., 2005) or multimodal systems (Cimato et al., 2008). Fuzzy vaults are especially suitable for partial biometric representations, as for a minutiae representation of fingerprints (Nandakumar

et al., 2007; Örencik et al., 2008). These schemes have been formalized in fuzzy sketches and fuzzy extractors in order to derive cryptographic keys from noisy biometric data (Dodis et al., 2004; Boyen, 2004). Fuzzy commitments are suitable for biometric data having a binary representation, like the Iriscode (Daugman, 2004; Daugman, 2007). However, several weaknesses are presented in (Simoens et al., 2009; Blanton and Aliasgari, 2011; Zhou et al., 2012). In the same way, collusion attacks on the fuzzy vault scheme are proposed in (Schreier and Boult, 2007; Poon and Miri, 2009). Finally biometric cryptosystems combined with private information retrieval (PIR) protocols (Bringer et al., 2007) or homomorphic encryption have recently given interesting solutions for face biometrics (Osadchy et al., 2010), iris and fingerprints (Barni et al., 2010; Blanton and Gasti, 2011).

2.2 Cancelable biometrics and BioHashing

Cancelable biometric systems have been designed to ensure the privacy of the use of biometric data. The feature transformations were first proposed in (Ratha et al., 2001; Bolle et al., 2002) and many cancelable biometric schemes have been proposed later. In addition to the BioHashing algorithm, we can mention the approach proposed in (Ratha et al., 2007), where the authors use three geometric transformations to be applied to minutiae: Cartesian, Polar and Functional transformations. The centralized storage of Biocodes is not a security problem if data are revokable and if the transformation is non-invertible. In this case, the storage of the additional random number must be carefully handled. This data could be stored in a secure element for each service provider, but an alternative solution seems possible, where the identity provider stores for any user identifier (i) a BioCode and (ii) the seed value for each associated service provider. Figure 1 describes this alternative.

In biometric feature transformation schemes, the biometric feature vector is generally represented by a real-valued vector and the metric used to evaluate the similarity between two biometric features is the Euclidean distance. Technical performance of the system (accuracy and accuracy degradation caused by the template protection scheme) is generally measured with FMR/FNMR or FAR/FRR rates (respectively False match rate, false non-match rate, false acceptation rate and false reject rate). Feature transformations should clearly preserve the performance of the biometric system, according to the aforementioned properties. Among the papers dealing with cancelable biometrics, most of them rely on the BioHashing scheme, since the algorithm is easy to analyse and can be used on several biometric modalities. Moreover, the multiplication with the orthogonal matrix preserves the scalar product (more details are given in Section 2.3) and consequently the technical performance of the system.

At the enrolment step, the original biometric feature vector, called FingerCode (on account of the chosen fingerprint modality), is transformed using a random number (called the *seed*), into a new template, called the reference BioCode. Once the transformation is achieved, the original FingerCode is discarded and the reference BioCode is stored, with the associated seed. At the verification step, a new BioCode is computed using the same algorithm, with a second biometric vector and the corresponding random seed. The verification result is obtained from the computation of a simple Hamming distance between the reference BioCode and the one issued from the new capture. Figure 2 illustrates the overall process, with the BioHashing scheme applied to fingerprints.

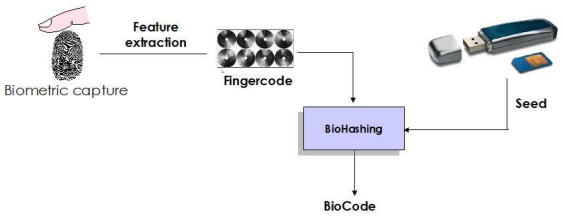

Figure 2: General principle of BioHashing on fingerprints

It is known that the Biohashing algorithm is easy to invert if the random number used as the seed is known. But, the reconstructed biometric feature (called the preimage) is not necessary close to the original template. In this paper, we wonder whether it may be sufficient for an intruder to retrieve, from the knowledge of an intercepted BioCode and the corresponding random number, an approximated FingerCode. We recall that the FingerCode is the vector containing features extracted from the original raw fingerprint data of the user, and not the original data itself.

Nagar et al. have recently presented the first detailed method to recover a close approximation of the original face image given the BioCode and the random seed (Nagar et al., 2010). Nevertheless, the aim for the intruder is to be accepted by the system thanks to the approximate FingerCode and not necessary to retrieve an approximate fingerprint. More precisely, with the knowledge of a BioCode and the associated seed, we investigate the possibility to approximate the

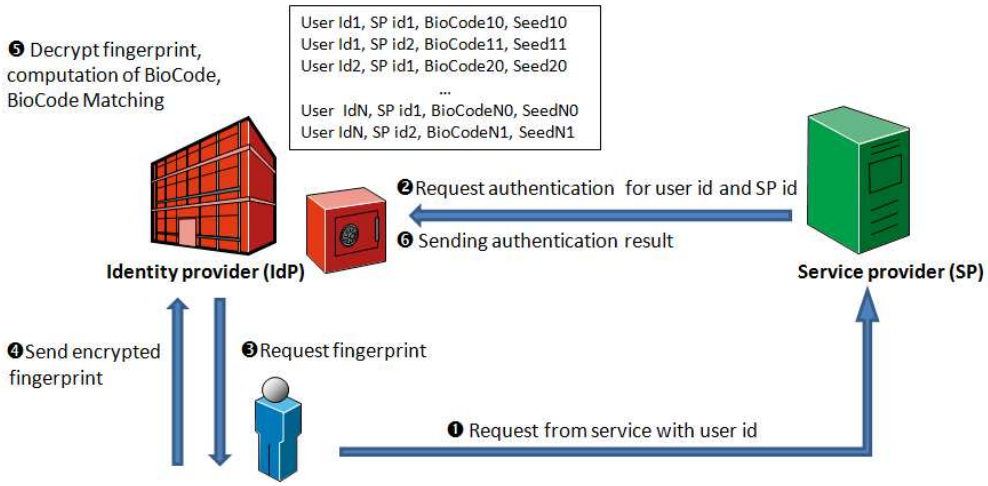

Figure 1: Architecture for identity management using cancelable biometrics

corresponding FingerCode and the possibility to generate other BioCodes with this approximated FingerCode.

2.3 The BioHashing algorithm

In this section, we give some details about the BioHashing algorithm. This algorithm transforms a real-valued vector of length n (i.e. the FingerCode, resulting from a feature extraction method) into a binary vector of length n (i.e. the BioCode), as first defined by Teoh *et al.* in (Teoh et al., 2004). The BioHashing algorithm is mainly used for fingerprints and face modalities. Its principle consists in projecting the FingerCode on an orthogonal basis defined by the random seed, to generate the BioCode. The template transformation uses the following algorithm, where the inputs are the random seed and the FingerCode F and the output is the BioCode B:

1. For $i = 1,\ldots,n$, n pseudorandom vectors v_i of length n are generated (from the random seed) and are gathered in a pseudorandom matrix.
2. The Gram-Schmidt algorithm is applied on the n vectors v_i of the matrix, for the generation of n orthonormal vectors $V_1,\ldots,V_n$.
3. For $i = 1,\ldots,n$, n scalar products $p_i =< F,V_i >$ are computed using the FingerCode F and the n orthonormal vectors V_i .
4. The n-bit biocode $B = (B_0,\ldots,B_n)$ is finally obtained, using the following quantization process:

$$B_i = \begin{cases} 0 & \text{if} \quad p_i < t \\ 1 & \text{if} \quad p_i \geq t, \end{cases}$$

where t is a given threshold, generally equal to 0.

Note that the distance between two FingerCodes is computed with the Euclidean distance, while between two BioCodes, the Hamming distance is used.

The Gram-Schmidt algorithm transforms an arbitrary basis into an orthogonal basis. Roughly speaking, the first part of the algorithm, including the scalar products with the orthonormal vectors, is used for the performance requirements and the last step of the algorithm is used for the non-invertibility requirements of the BioHashing algorithm. As mentioned before, the random seed guarantees the diversity and revocability properties.

3 FINGERCODE APPROXIMATION WITH GENETIC ALGORITHMS

In this section, we present how to obtain an approximate FingerCode, from an intercepted BioCode and the corresponding random seed, resorting to genetic algorithms.

3.1 Introduction to genetic algorithms

A genetic algorithm is *any population-based model that uses selection and recombination operators to generate new sample points in a search space* (Whitley, 1994). A genetic algorithm simulates computational models inspired from evolutionary theory, using the following principle: a random initial population is generated. A criterion is defined, typically a fitness function, in the sense that this criterion is evaluated for each individual, to enable a comparison and a selection between the different individuals. The

individuals obtaining the best score with respect to the criterion are kept, while the others are discarded. Then, inspired from the evolutionary theories, some process of cross-over and mutation are applied, to obtain a new generation of individuals from the previous one. The processes of cross-over and mutation avoid the algorithm to fall into local extrema.

More precisely, genetic algorithms (or GA) determine the optimal value of a criterion by simulating the evolution of a population and survival of best fitted individuals (Wall, 1996). The survivors are individuals obtained by crossing-over, mutation and selection of individuals from the previous generation. GA is an optimization method that does not necessitate to differentiate the fitness function but only to evaluate it. If the population is important enough considering the size of the search space, the fitness criterion is guaranteed to reach its optimal value.

3.2 Application to cancelable biometrics

We use the following notations, introduced in (Nagar et al., 2010). Let b_z and $\acute{b_z}$ represent the template and query biometric features (or FingerCodes) of user z, respectively. Let f be the feature transformation function (i.e. the orthonormal projection followed by the quantization) and K_z be the random seed (or transformation parameters) corresponding to the user z. The resulting enroled BioCode is denoted $B_z = f(b_z, K_z)$ and n is the dimension of the BioCode. In this section, we use a genetic algorithm to approximate b_z, knowing B_z and the secret data K_z. We use the terminology of the Biohashing algorithm (FingerCode and BioCode), but all this section is directly applicable to any feature transformation f. Our approach uses genetic algorithms and -to our knowledge- it is the first time that such algorithms are used in biometrics for this purpose.

A genetic algorithm is defined by considering five essential data, applied here to our FingerCode approximation problem :

1. *Genotype*: a candidate FingerCode denoted $\widetilde{b_z}$ is considered as an individual described by a vector of dimension m,
2. *Population*: a set composed of 10.000 individuals characterized by their genotypes (i.e. a set of 10.000 candidates for the approximation of the FingerCode),
3. *Fitness function*: this function enables to quantify the fitness of an individual to the environment by considering its genotype. Considering the problem of FingerCode approximation, we propose to use the following fitness function:

$$F(\widetilde{b_z}) = \left\| f(\widetilde{b_z}, K_z) - B_z \right\| \tag{1}$$

It means that the intruder wants to retrieve a new FingerCode $\widetilde{b_z}$ which is an approximation of the original one b_z, from the knowledge of the Biocode $B_z = f(b_z, K_z)$ and the associated random seed K_z.

4. *Operators on genotypes*: they define alterations on genotypes in order to make the population evolve during generations. Three types of operators are used:

- Mutation step: individual's genes are modified in order to be better adapted to the environment. We use the non-uniform mutation process which randomly selects one chromosome x_i, and sets it as equal to a non-uniform random number:

$$x_i' = \begin{cases} x_i + (b_i - x_i)h(G) & if\ r_1 < 0.5 \\ x_i - (x_i + a_i)h(G) & if\ r_1 \geq 0.5 \end{cases} \tag{2}$$

where

$$\begin{array}{l} h(G) = (r_2(1 - \frac{G}{G_{max}}))^b \\ r_1, r_2 : numbers\ belonging\ to\ the\ interval\ [0,1] \\ a_i, b_i : lower\ and\ upper\ bound\ of\ chromosome\ x_i \\ G : the\ current\ generation \\ G_{max} : the\ maximum\ number\ of\ generations \\ b : a\ shape\ parameter \end{array} \tag{3}$$

- Selection step: individuals that are not adapted to the environment do not survive to the next generation. We used the normalized geometric ranking selection method which defines a probability P_i for each individual i to be selected as following:

$$P_i = \frac{q(1-q)^{r-1}}{1-(1-q)^n} \tag{4}$$

where

$$\begin{array}{l} q : the\ probability\ of\ selecting\ the\ best \\ \quad individual \\ r : the\ rank\ of\ individual,\ where\ 1\ is\ the\ best \\ n : the\ size\ of\ the\ population \end{array} \tag{5}$$

- Crossing-over step: two individuals can reproduce by combining their genes. We use the arithmetic crossover which produces two complementary linear combinations of the parents:

$$\begin{array}{l} X' = aX + (1-a)Y \\ Y' = (1-a)X + aY \end{array} \tag{6}$$

where

X, Y : *genotype of parents*
a : *a number in the interval* $[0,1]$
X', Y' : *genotype of the linear combinations of the parents*

(7)

5. *Stopping criterion* : this criterion allows to stop the evolution of the population. We can consider the stability of the standard deviation of the evaluation criterion of the population or set a maximal number of iterations (we used the second one with the number of iterations equal to 2000).

The implementation of this algorithm is presented in the next section with the BioHashing algorithm on a fingerprints database.

4 EXPERIMENTAL RESULTS

We generated a FingerCode for each fingerprint in the FVC2002 database (Maio et al., 2002) dB3, composed of 8 fingerprints by individual (resolution 355 x 390 pixels) for 100 individuals. The FingerCode of each user is generated following two feature computation methods (providing different dimensions of the vector):

- Method 1 : Gabor features (Manjunath and Ma, 1996) with 256 parameters. They are based on a Gaussian kernel function modulated by a sinusoidal plane wave, with several different orientations and scales, and are used for texture representation.
- Method 2 : Rotation invariant local binary pattern (LBPFT) with 152 parameters. This is a rotation invariant texture classification method, presented in the reference (Guo et al., 2010).

For each FingerCode, we computed one BioCode with a random seed, using the BioHashing algorithm. We apply the algorithm described in section 3.2 to approximate the value of the FingerCode, given the associated BioCode and seed. Figure 3 explains in an intuitive way the BioHashing process, it consists in projecting the FingerCode on a unit sphere.

In the validation process, we intend to show how the proposed method is able to approximate the FingerCode considering the fitness function (distance between the real BioCode and the predicted one). Second, we have to verify that the predicted FingerCode can be reused. To do that, given one FingerCode in the database, we generate two BioCodes (with differents values of K_z). The first BioCode and the associated parameter K_z are used to approximate the FingerCode. The second BioCode is used to verify if the predicted FingerCode provides a similar BioCode (i.e. if $\left\| f(b_z, K'_z) - f(\widetilde{b_z}, K'_z) \right\|$ is small).

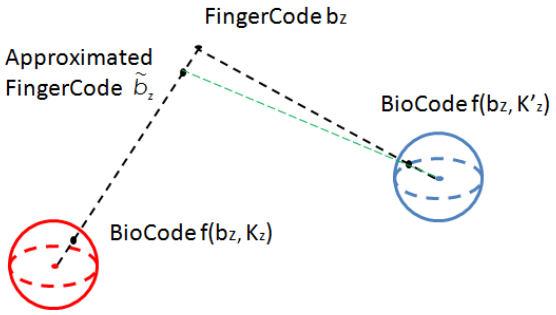

Figure 3: BioCode computation and FingerCode approximation

4.1 FingerCode approximation

We applied the general process described in section 3.2 on FingerCodes generated with method 1 and method 2. The evolution of the fitness function for the the LBPFT (dimension 152) and Gabor (dimension 256) features is presented in figure 4. The average optimal value of the fitness function (1) equals 5.5 for the LBPFT feature extraction method and 9.2 for the Gabor one. This means that the generated BioCode, given the approximated FingerCode, is very similar to the intercepted one. The resulting average difference between the real FingerCode and the approximated one was 6.4 for the LBPFT feature (dimension 152) and 203.2 for the Gabor one (dimension 256). It shows the efficiency of the proposed approach for the LBPFT feature. For the Gabor one, the distance between the real and approximated FingerCode is quite high (but computed on dimension 256).

4.2 Reusability of the approximated FingerCode

In order to verify if the approximated FingerCode is really useful for an attacker, we undertook another experiment. The hypotheses are: the attacker has stolen the random seed and has generated an approximate FingerCode. Therefore, we generated two BioCodes with a new random seed (i) with the original FingerCode and (ii) with the approximated one. From the attacker's viewpoint, we expect to obtain two BioCodes that are similar enough (sufficiently to be accepted by the cancelable biometric system). We obtained an average distance between the BioCodes equal to 8.6 for the LBPFT method and 11.0 for the Gabor method.

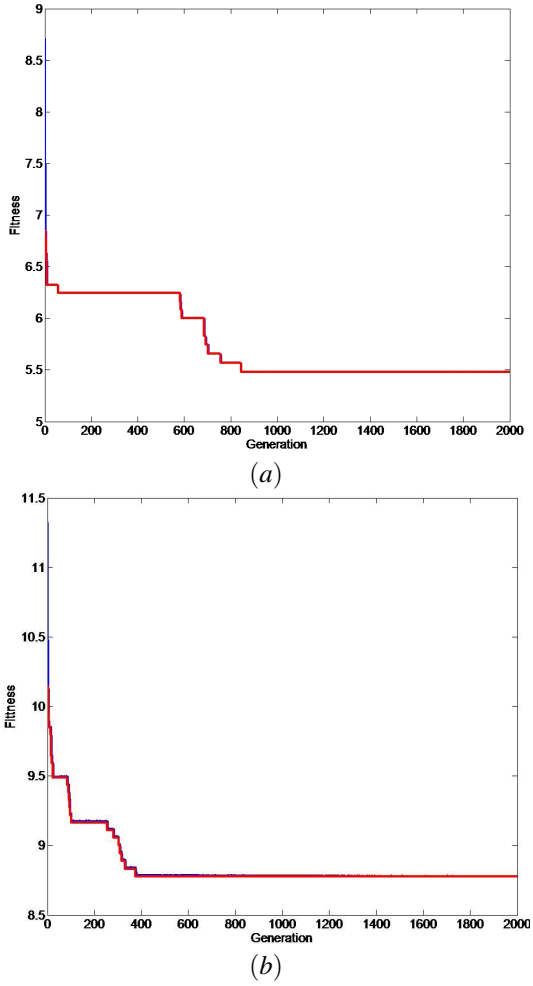

Figure 4: Evolution of the fitness function for each generation: (a) LBPFT, (b) Gabor

The conclusion of this experiment is that the proposed attack reveals a real problem of security if the BioCode and random seed are stored in the same database. It is also a privacy issue since an intruder would be able to generate other BioCodes to impersonate a genuine user.

5 CONCLUSION AND PERSPECTIVES

This paper proposes a new way to approximate the original biometric feature from the transformed template in a cancelable biometric scheme. Our approach uses genetic algorithms and reveals security and privacy problems concerning the associated cancelable biometric system. This attack enables an intruder to recover a biometric template, similar to the original template, under realistic assumptions. Experimentations with the BioHashing algorithm clearly show the importance of storing the additional random data in a secure element, apart from the Biocode. Perspectives of this paper are to study the robustness of different feature transformations to be used in the context of a cancelable biometric system.

REFERENCES

Barni, M., Bianchi, T., Catalano, D., Raimondo, M. D., Labati, R. D., Failla, P., Fiore, D., Lazzeretti, R., Piuri, V., Piva, A., and Scotti, F. (2010). A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates. In *IEEE Fourth International Conference On Biometrics: Theory, Applications And Systems (BTAS 2010)*.

Blanton, M. and Aliasgari, M. (2011). On the (non) reusability of fuzzy scketches and extractors and security in the computational setting. In *SECRYPT*, pages 68–77.

Blanton, M. and Gasti, P. (2011). Secure and efficient protocols for iris and fingerprint identification. In *ESORICS*, pages 190–209.

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

Boyen, X. (2004). Reusable cryptographic fuzzy extractors. In *ACM CCS*, pages 82–91.

Bringer, J., Chabanne, H., Pointcheval, D., and Tang, Q. (2007). Extended private information retrieval and its application in biometrics authentications. In *CANS*, pages 175–193.

Cappelli, R., Lumini, A., Maio, D., and Maltoni, D. (2007). Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(9):1489–1503.

Cavoukian, A. and Stoianov, A. (2009). Biometric encryption.

Cheung, K. H., Kong, A. W., You, J., and Zhang, D. (2005). An analysis on invertibility of cancelable biometrics based on biohashing. In *CISST'05*, pages 40–45.

Cimato, S., Gamassi, M., Piuri, V., Sassi, R., and Scotti, F. (2008). Privacy-aware biometrics: Design and implementation of a multimodal verification system. In *Proceedings of ACSAC'08*, pages 130–139.

Daugman, J. (2004). How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):21–30.

Daugman, J. (2007). New methods in iris recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 37(5):1167–1175.

Dodis, Y., Reyzin, L., and Smith, A. (2004). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *EUROCRYPT'04*, pages 523–540. Springer-Verlag.

Goh, A. and Ngo, D. (2003). Computation of cryptographic keys from face biometrics. In *Communications and Multimedia Security*, pages 1–13. LNCS 2828.

Guo, Z., Zhang, L., Zhang, D., and Zhang, S. (2010). Rotation invariant texture classification using adaptive lbp with directional statistical features. In *IEEE International Conference on Image Processing (ICIP)*.

Hao, F., Anderson, R., and Daugman, J. (2005). Combining cryptography with biometrics effectively. *University of Cambridge Computer Laboratory, Tech. Rep*.

ISO (2011). ISO/IEC 24745 information technology - security techniques -biometric information protection.

Jain, A. K., Nandakumar, K., and Nagar, A. (2008). Biometric template security. *EURASIP J. Advances in Signal Processing*, 8(2):1–17.

Juels, A. and Sudan, M. (2002). A fuzzy vault scheme. In *ISIT*, page 408.

Juels, A. and Wattenberg, M. (1999). A fuzzy commitment scheme. In *ACM Conference on Computer and Communications Security*, pages 28–36.

Lee, Y., Chung, Y., and Moon, K. (2009). Inverse operation and preimage attack on biohashing. In *Workshop on Computational Intelligence in Biometrics*.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., and Jain, A. K. (2002). FVC2002: Second fingerprint verification competition. In *ICPR*, pages 811 – 814.

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., Jain, A., and Pankanti, S. (2007). Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security*.

Örencik, C., Pedersen, T. B., Savas, E., and Keskinoz, M. (2008). Improved fuzzy vault scheme for fingerprint verification. In *SECRYPT*, pages 37–43.

Osadchy, M., Pinkas, B., Jarrous, A., and Moskovich, B. (2010). Scifi - a system for secure face identification. In *IEEE Symposium on Security and Privacy*.

Poon, H. and Miri, A. (2009). A collusion attack on the fuzzy vault scheme. *ISC International Journal of Information Security*, 1(1):27–34.

Ratha, N., Chikkerur, S., Connell, J., and Bolle, R. (2007). Generating cancelable fingerprint templates. *IEEE Transactions on PAMI*, 29(4):561–572.

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

Rathgeb, C. and Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. on Information Security*, 3.

Schreier, W. and Boult, T. (2007). Cracking fuzzy vaults and biometric encryption. In *Biometrics Symposium*.

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 *ICB'12*, pages 498–505.

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

Wall, P. (1996). *A Genetic Algorithm for Resource-Constrained Scheduling*. PhD thesis, MIT.

Whitley, D. (1994). A genetic algorithm tutorial. *Statistics and Computing*, pages 65–85.

Zhou, X., Kuijper, A., and Busch, C. (2012). Cracking iris fuzzy commitment. In *ICB'12*.