Evaluation of Cancelable Biometric Systems: Application to Finger-Knuckle-Prints

Rima Belguechi, Estelle Cherrier, Mohamad El-Abed, Christophe Rosenberger

Evaluation of Cancelable Biometric Systems: Application to Finger-Knuckle-Prints

Rima Belguechi, Estelle Cherrier, Mohamad El Abed and Christophe Rosenberger
GREYC Research lab
ENSICAEN - UCBN - CNRS
Caen, France
Email: christophe.rosenberger@ensicaen.fr

***Abstract*—With more and more applications using biometrics, new privacy and security risks arise. Some new biometric systems have been proposed in the last decade following a privacy by design approach: cancelable biometric systems. Their evaluation is still an open issue in research. The objective of this paper is first to define an evaluation methodology for these particular biometric systems by proposing some metrics for testing their robustness. Second, we show through the example of a cancelable biometric system using finger-knuckle-prints how some privacy properties can be checked by simulating attacks.**

I. Introduction

Biometrics is an emerging technology for authentication applications. Even if many biometric modalities are well known (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, the central storage of biometric data is forbidden or limited to a small amount of users. In order to solve this problem, many new biometric systems have been proposed in the last decade based on a new paradigm: privacy by design. These biometric template protection schemes have for objective to guarantee the privacy of users face to different attacks for identity theft (e-government applications, border control, *etc.*).

These systems are called cancelable since the biocode generated from a biometric information, can be modified in case of interception or loss. This biocode can sometimes be used as a cryptographic key. In this case, the generated biocode must be exactly the same for each biometric capture. These particular biometric systems must of course address classical issues like a maximal level of performance (*i.e.*, minimizing the EER or 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 [14], [2], [9]). In order to validate their proposition, authors generally provide some experimental results based on performance evaluation (EER value, ROC curves, *etc.*) and a security analysis by considering different scenarios. None standard methodology has been defined in order to qualify these biometrics systems even if some previous research works have been proposed recently [13]. This is a major contribution of this paper. We clearly define the properties that are requested for cancelable biometric systems, and we propose a quantitative-based evaluation framework to assess 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 to study and quantify the robustness of a cancelable biometric system based on finger knuckle prints. To our knowledge, very few papers have studied the robustness of this biometric modality.

The plan of the paper is the following. Section 2 gives an overview of the state of the art in the evaluation of cancelable biometric systems. We present the proposed methodology in section 3. We first define the properties these biometric systems should follow. Second, we propose some criteria that permit to assess the privacy compliance of a cancelable biometric system. Section 4 illustrates the proposed methodology on a cancelable biometric system based on the use of finger knuckle prints within the Ratha's approach [15]. We conclude and give some perspectives of this study in section 5.

II. Previous works

The concept of *cancelable biometrics* has been defined for the first time in the pioneering article [15]. It is aimed at enhancing privacy protection and template security, as detailed in the recent reference [7]. Two main approaches can be distinguished dealing with cancelable biometrics. On the one hand, biometric cryptosystems or secure sketches, such as those presented in [8], [5], [4], resort to cryptography. On the other hand, we find feature transformations approaches. 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 [19], [2], [16]. In the sequel, we focus on BioHashing since some weaknesses have been reported in the former approach in [17]. 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 [13]. Let b_z and $b_z^{'}$ represent the template and query biometric features

of user z, respectively. Let f be the feature transformation function and f^{-1} be its inverse. We denote n the dimension of the $f(b_z)$ biocode for user z. Let K_z be a set of transformation parameters corresponding to user z. Let D_O denote a distance function between the biometric features in the untransformed (original) domain and D_T be a distance function in the transformed domain. The biometric system outputs a verification decision if the distance between the template and query biometric features is less than a threshold denoted as ϵ.

Very few works have been dedicated to the evaluation of such biometric systems in the literature [13]. Cancelable systems must fulfill several properties as mentioned in [12]:

- *Efficiency or usability*: 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. To assess the efficiency of a biometric system (without any transformation), we generally consider two error metrics:

$$FRR_O(\epsilon) = P(D_O(b_z, b_z^{'}) \leq \epsilon) \quad (1)$$
$$FAR_O(\epsilon) = P(D_O(b_z, b_z^{'}) > \epsilon) \quad (2)$$

  Where FRR_O is the false reject rate and FAR_O is the false accept rate of the original biometric system (without any template protection). For a cancelable biometric system, we consider the two following metrics:

$$FRR_T(\epsilon) = P(D_T(f(b_z, K_z), f(b_z^{'}, K_z)) \leq \epsilon) \quad (3)$$
$$FAR_T(\epsilon) = P(D_T(f(b_z, K_z), f(b_z^{'}, K_z)) > \epsilon) \quad (4)$$

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

- *Non-invertibility*: 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 a stolen biometric template (as for example, it is possible to generate an eligible fingerprint given minutiae). 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:

$$FAR_A(\epsilon) = P(D_T(f(b_z, K_z), A_z) > \epsilon) \quad (5)$$

  Where FAR_A is the probability of a successful attack by the impostor. The A_z biocode is computed by the impostor by taking into account as much information as possible within different contexts.

- *Diversity*: 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.

We propose in this paper an evaluation framework of cancelable biometric systems using the previously mentioned properties. These properties are well known and often cited in papers from the state of the art. 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 a methodology to answer these two questions.

III. Proposed methodology

This section is devoted to the definition of a framework to verify if the previous properties are fulfilled by a cancelable biometric system. Based on some of the early works [15], [3] which identified weak links in each subsystem of a generic authentication system, some papers consider the possible attacks in cancelable biometric systems (such as those presented in [18], [7], [13], [16]). In this paper, we strengthen this study with the proposition of an evaluation methodology, by taking into account each of the required properties.

A. BioHashing principle

All BioHashing methods share the common principle when generating a unitary biocode from two data: the biometric one (for example face, palmprint, fingerprint modalities) and a random number which needs to be stored (for example on a USB key, or more generally on a token), called tokenized random number. This principle is illustrated in figure 1. First, a biometric template (called FKPCode for the finger print knuckle modality) is extracted from the raw image. The tokenized random number is generally mixed with the biometric template to obtain the binary output called biocode.

B. Evaluation framework

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 first focus on an *authentication* problem (one against one matching): we develop some criteria to estimate the risk (for different attack scenarios) that an intruder would manage to impersonate a particular genuine user. In a second step, the *identification* (one against many

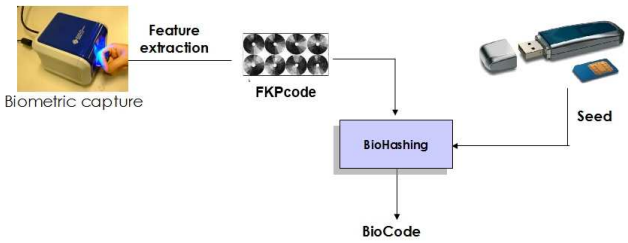

Fig. 1. General principle of the BioHashing algorithm

matchings) problem is considered.

We detail below how we quantify if the properties previously mentioned are fulfilled: eight attacks are described below. For each attack, a value $A_i \in [0,1]$, $i = 1,\ldots,8$ is computed on the chosen FKP BioHashing scheme (there is at least one attack for one required property). These risk values will be gathered in an eight-dimensional vector to characterize the evaluation of the studied cancelable biometric scheme. Notice that the following attack study requires that the decision threshold ϵ to be fixed. In this paper, we set the decision threshold ϵ_{EER_O} to the EER value of the original biometric system (without any template protection). Different other values can be used for ϵ depending on the security requirements of the application.

1) Efficiency or usability (A_1):
To verify if the efficiency is not decreased by using the template protection scheme, we propose to compute the following measure:

$$A_1 = 1 - \frac{\mathrm{AUC}(\mathrm{FAR_T}, \mathrm{FRR_T})}{\mathrm{AUC}(\mathrm{FAR_O}, \mathrm{FRR_O})} \quad (6)$$

where AUC denotes the area under the ROC curve for both systems. Two cases are interesting. First, it may happen that $A_1 = 1$ meaning that the cancelable biometric system provides a perfect performance (without any error, or $EER = 0\%$). Second, if the value A_1 is negative, it means that the efficiency of the biometric system is deteriorated by the template protection scheme.

2) Non-invertibility (A_2 to A_5):
This essential property can be evaluated through four kinds of attacks. For all these attacks, we use one biometric sample to generate the template b_z of the user z (*single enrolment process*). Based on the principle of each attack, we generate many fake attempts $f(\acute{b_z})$ of the genuine user:
   - *Zero effort attack* (A_2):
     an impostor user provides one of its biometric sample $f(\acute{b_x}, K_x)$ to be authenticated as the user z,
   - *Brute force attack* (A_3):
     an impostor tries multiple random values of $f(\acute{b_z})$ for each authentication attempt,
   - *Stolen token attack* (A_4):
     an impostor has obtained the token of the genuine user (K_z) and generates $f(\acute{b_z}, K_z)$ by trying different random values of $\acute{b_z}$,
   - *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 different $f(\acute{b_z}, K)$ of the genuine user.

To evaluate the efficiency of these four attacks, we propose to compute for each of them, the following criterion:

$$A_i = \mathrm{FAR}(\epsilon_{\mathrm{EER_O}}),\ i = 2,\ldots,5 \quad (7)$$

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 fixed to a value ϵ_{EER_O} (obtained by the computation of the EER of the original biometric system without any template protection). From the impostor's point of view, the values A_i, $i = 2,\ldots,5$ must be as high as possible.The obtained value for each attack A_i, $i = 2,\ldots,5$ allows 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 (A_6 to A_8) :
A prominent feature of a cancelable biometric system is its ability to produce different biocodes for the same individual and for different applications. But, an impostor must not be able to extract any information from different biocodes issued from the same user. In order to measure the diversity property, we propose to compute the mutual information provided by several biocodes issued from same biometric data as defined in (8):

$$I(X,Y) = \sum_x \sum_y P(x,y) \log\left(\frac{P(x,y)}{P(x)P(y)}\right) \quad (8)$$

where X and Y are two biocodes 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_6 is then computed using the mean of the highest value of mutual information, according to equation 9.

$$A_6 = \frac{1}{N} \sum_{i=1}^{N} \sum_{j=1}^{M} \max(I\ (f(b_i^0), f(\acute{b_i^j}))) \quad (9)$$

where the subscript i denotes the i^{th} individual in the database, N is the number of individuals in the database and M is the number of generated biocodes for each individual.

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). For each template of the genuine user, we simulate Q biocodes $B_z = \{f(b_z, {K_z}^1), .., f(b_z, {K_z}^Q)\}$ for user z. Given these Q realizations, we predict a possible biocode value by setting the most probable value of each bit. We propose to compute the A_7 value for $Q = 3$ and A_8 for $Q = 11$ according to formula (7). 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 authentication systems. For identification ones, the properties are the same but the criteria are slightly different. For the non-invertibility and cancelability properties, instead of computing the value $A_i = 1 - \mathrm{FAR}(\epsilon_{\mathrm{EER_O}})$, $i = 2, \ldots, 5, 7, 8$, we use the formula $A_i = 2 * EER$ for the different attacks scenarios. Indeed, in the identification case, the impostor tries to impersonate all individuals in the database. The more the value A_i is close to 100%, the less robust the biometric system is. The other values A_i, $i = 1, 6$ are the same in the authentication and identification contexts.

As a conclusion of the proposed methodology, the security and robustness of a cancelable biometric system are characterized by an eight-dimensional vector (A_i, $i = 1, \ldots, 8$). The key benefit of this quantitative presentation is to allow easlity the comparison of cancelable biometric systems. More generally speaking, a comparison between two cancelable systems is considered as a comparison of two continious random variables belonging to *[0,1]*. A statistical hypothesis test (such as the Kruskal-Wallis test [6]) could then be used in order to prove if there is a significant difference of robustness against attacks between the tested systems. We present in the next section an illustration of this methodology on the example of FKP based BioHashing scheme. This is another original contribution of the paper.

IV. Illustration

A. Experimental protocol

We use the PolyU FKP Database presented in [1], [10]. The acquisition device used to create the database can be seen in figure 2. The database has been acquired on 4 fingers of 165 volunteers, leading to 660 different classes. There is no other database containing as many users. Each class contains 12 images acquired during 2 sessions. We use the first image as reference and the remaining eleven are used for testing.

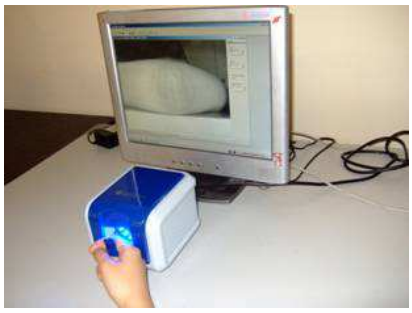

Fig. 2. FKP acquisition device [1]

The database provides two sets of images. The first one corresponds to the whole acquired image. The second one corresponds to region of interest (ROI) images extracted from the first set of images. The ROI extraction, detailed in [10], [20], [21], [11] leads to gray level images of 110*220 pixels. Examples of acquired images are presented in Figure 3. We use this last type of image as raw data to compute Gabor features of size 128 parameters as template.

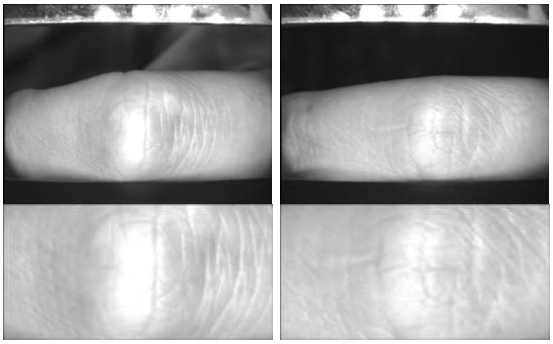

Fig. 3. FKP acquired images and corresponding ROI

B. Experimental results

First, the performance of biometric systems based on the use of the FKPCode and the biocode respectively are studied through an analysis of their ROC curves. In the first case, the biometric system is not cancelable since it uses Gabor features computed on the raw finger knuckle print data. We compute a simple distance (measured with the Minkowski's one) between the reference template b_z and $b_z^{'}$ for each user z. The obtained EER is equal to 30.5% (see figure 4). This performance is obviously far from being the best compared to results in the literature, but this value allows us to set a baseline performance of the system.

In the second case, the performance of a cancelable biometric system is evaluated. In this case, the EER equals to 25.9%, as illustrated in3 figure 4, which corresponds to the percentage of successful attacks when another user in the database tries to be authenticated as a particular genuine user. This scenario is known as a *zero-effort attack*. The

corresponding threshold ϵ_{EER_O} is equal to 0.45. Compared to the FKPCode performance, this improvement looks very interesting: it is mainly due to the smoothing of the intrinsic intra-class disparity by the random projection (the random value is kept fixed for each user). More precisely, it means a reduction of the intra-class variability, leading to better performances. In the sequel, we suppose that the threshold ϵ of the BioHashing system remains at the value ϵ_{EER_O}. This hypothesis allows us to test the robustness of the cancelable biometric system for an operational setting.

For all attacks, we generate 23 fake biocodes (the same number of testing samples in the benchmark database). In order to guarantee the reproductibility of the computations (due to many random draws), we iterate 100 times these attacks. That means we generate $23 * 100 = 2300$ fake biocodes for each attack for each user (660 in our case).

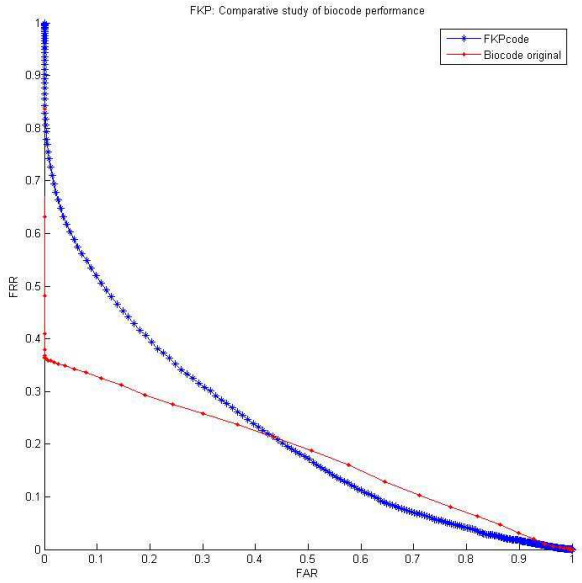

Fig. 4. ROC curves for the biometric systems using FKPCode: EER=30.5% and BioCode: EER=25.9%

C. Discussion

Table I presents the values of the different criteria A_i, $i = 1..8$ describing the robustness of the studied cancelable biometric system. Remark that the percentage values have been normalized as values belonging to $[0, 1]$.

As $A_1 = 0.18$, we can see that the template protection with the Biohashing improves the initial performance of the biometric system. For others attacks, A_i, $i = 2, \ldots, 5, 7, 8$, we obtain quite high values of their risks especially for identification applications where attacks are always successful. The *zero effort attack* is the most dangerous one in the authentication case. This means that all users in the database have a great chance to succeed to be authenticated as a genuine user. The low performance of the cancelable biometric system ($EER = 25.9\%$) explains this problem.

Concerning the diversity property, the average of the highest mutual information of each individual between the reference BioCodes and the test ones is equal to $A_6 = 0.17$. This measure shows the robustness of the cancelable biometric system in generating none correlated biocodes (using different seeds on the same biometric data) with the reference ones. This property is considered as a major concern when dealing with cancelable systems, since it prevents from tracing users in the system.

Considering the cancelability property in the authentication case, we can see that the benefit of intercepting 11 biocodes face to 3 does not increase so much the risk of generating an eligible biocode. Indeed, $A_7 = 0.25$ is not far from $A_8 = 0.31$ while having intercepted nearly four times more biocodes. In the identification case, the attack is always successful. This table provides a powerful and precise characterization of a cancelable biometric system.

V. Conclusion and Perspectives

We define in this paper a new methodology to quantify the quality of a cancelable biometric system. Eight criteria are proposed to quantitatively measure the robustness properties detailed in this paper. They allow a rigorous comparison of cancelable biometric systems. The key benefit of the retained quantitative-based approach is to easily allow the comparison of new cancelable biometric systems. A BioHashing scheme based on the use of Finger-Knuckle-Prints is used to show the utility of the proposed evaluation framework. To our knowledge, very few works have concerned the study of a cancelable biometric system using this modality. The experimental results show some problems on this (simple) implementation based on the Ratha's approach.

The perspectives of this work are to compare the obtained results with the assessment of expert in biometrics for the privacy analysis of different cancelable biometric systems. We think also on new attacks and on more sophisticated approaches to generate a fake biocode given all the known information.

References

[1] "Polyu fkp database," http://www.comp.polyu.edu.hk/ biometrics/FKP.htm.
[2] R. Belguechi, C. Rosenberger, and S. Aoudia, "Biohashing for securing minutiae template," in *Proceedings of the 20th International Conference on Pattern Recognition*, Washington, DC, USA, 2010, pp. 1168–1171.
[3] R. Bolle, J. Connell, and N. Ratha, "Biometric perils and patches," *Pattern Recognition*, vol. 35, no. 12, pp. 2727–2738, 2002.
[4] H. Chabanne, J. Bringer, G. Cohen, B. Kindarji, and G. Zemor, "Optimal iris fuzzy sketches," in *IEEE first conference on biometrics BTAS*, 2007.
[5] J. Daugman, "Iris recognition and anti-spoofing countermeasures," in *7-th International Biometrics conference*, 2004.

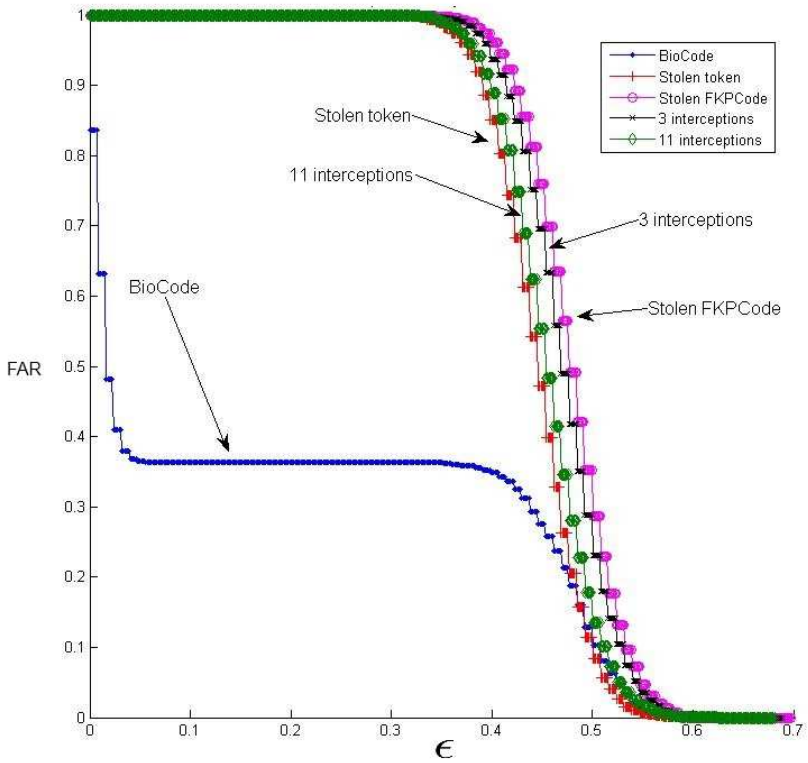

Fig. 5. FRR curves of attacks 2,3,4,5,7,8

Context	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
Authentication	0.18	0.72	0.19	0.32	0.24	0.17	0.25	0.31
Identification	0.18	0.52	0.99	0.97	1	0.17	0.99	0.99

TABLE I
EVALUATION RESULTS OF THE CANCELABLE BIOMETRIC SYSTEM WITHIN THE DIFFERENT CONTEXTS (AUTHENTICATION AND IDENTIFICATION).

[6] J. J. Higgins, "An introduction to modern nonparametric statistics," *The American Statistician*, 2003.

[7] A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," in *EURASIP J. Adv. Signal Process 2008*, 2008.

[8] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *ACM conference on Computer and communication security*, 1999, pp. 28–36.

[9] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *J. Netw. Comput. Appl.*, vol. 33, pp. 236–246, May 2010.

[10] D. Z. Lin Zhang, Lei Zhang, "Finger-knuckle-print verification based on band-limited phase-only correlation," *Proceedings of the International Conference on Computer Analysis of Images and Patterns*, pp. 141–148, 2009.

[11] D. Z. H. Z. Lin Zhang, Lei Zhang, "Ensemble of local and global information for finger-knuckle-print recognition," *Pattern Recognition*, vol. 44, pp. 1990–1998, 2011.

[12] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer, 2003.

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

[14] N. Ratha, S. Chikkerur, J. Connell, and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, 2007.

[15] N. Ratha, J. Connelle, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication system," *IBM Systems J.*, vol. 37, no. 11, pp. 2245–2255, 2001.

[16] N. Saini and A. Sinha, "Soft biometrics in conjunction with optics based biohashing," *Optics Communications*, vol. 284, no. 3, pp. 756 – 763, 2011.

[17] K. Simoens, C. Chang, and B. Preneel, "Privacy weaknesses in biometric sketches," in *30th IEEE Symposium on Security and Privacy*, 2009.

[18] A. Teoh, Y. Kuanb, and S. Leea, "Cancellable biometrics and annotations on biohash," *Pattern recognition*, vol. 41, pp. 2034–2044, 2008.

[19] A. Teoh, D. Ngo, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 40, 2004.

[20] L. Zhang, L. Zhang, and D. Zhang, "Finger-knuckle-print: a new biometric identifier," in *Proceedings of the IEEE International Conference on Image Processing*, 2009.

[21] L. Zhang, L. Zhang, D. Zhang, and H. Zhu, "Online finger-knuckle-print verification for personal authentication," *Pattern recognition*, vol. 43, pp. pp. 2560–2571, July 2010.