Vulnerabilities of fuzzy vault schemes using biometric data with traces

Maryam Lafkih, Patrick Lacharme, Christophe Rosenberger, Mounia Mikram, Sanaa Ghouzali, Mohammed El Haziti, Driss Aboutajdine

Vulnerabilities of fuzzy vault schemes using biometric data with traces

Maryam Lafkih*, Patrick Lacharme†, Cristophe Rosenberger†, Mounia Mikram‡, Sanaa Ghouzali§
Mohammed El Haziti¶, Driss Aboutajdine*
*LRIT (Associated unit with CNRST, URAC 29), Faculty of Sciences, Mohammed V University, Rabat, Morocco
† ENSICAEN, GREYC, F-14032 Caen, France
‡The School of Information Sciences, Rabat, Morocco
§Information Technology Department, College of Computer and Information Sciences, King Saud University, Riyadh, Kingdom of Saudi Arabia
¶Higher School of Technology, Sale, Morocco

***Abstract*—Biometric cryptosystems represent emerging techniques for biometric template protection. These cryptosystems are vulnerable to different types of attacks, as brute force attacks or correlation attacks if several templates are compromised. Another biometric security issue comes from certain biometric data (as fingerprint or face image) that can leave traces, but are, in the same time, the most commonly biometric modalities used in mobile security. In this paper, fuzzy vault biometric cryptosystems are investigated in the case of an attacker possessing altered version of biometric data of real users. Experimental results carried out using fingerprint a1nd face modalities show that this assumption has serious impact on the security of these type of biometric cryptosystems.**

I. Introduction

Biometric systems are considered as alternative solution to the traditional authentication such as password and personal identification number that can be stolen or forgotten. Mobile biometric solution is becoming an increasingly part of the biometric applications and the ubiquitous properties of mobile phones require an accurate investigation of the security of these systems. Authentication biometric systems are based on two stages: Enrollment and authentication. During enrollment, biometric feature is extracted from captured trait of the user to construct the reference template. During authentication, biometric feature of the request are also extracted and compared to the reference template using a selected threshold. The request is accepted if both features of enrollment and authentication are similar. If biometric systems store directly the template without prior encryption, it gives rise to very important security risks. Two technologies of biometric template protection are proposed: *Features Transformation* and *Biometric Cryptosystems* [11], that are able to handle data with intra-class variations (i.e variations between biometric features extracted from the same biometric trait of the same user) and are standardized in 2011 [1]. Biometric cryptosystems aim to generate helper data using a secret key and user biometric features. This helper data is the only stored data (meaning that the secret key and the biometric feature are not stored). During authentication, the secret key is retrieved using request biometric features and the helper data for a successful authentication. *Fuzzy Commitment* and *Fuzzy Vault* are the two most known approaches of biometric cryptosystems. Fuzzy commitment [13], proposed by Juels and Wattenberg, hides a biometric feature with a random codeword in an helper data. Fuzzy vault is proposed by Juels and Sudan [12] for non-ordered biometric data of variable length such as a set of minutiae (i.e. feature extracted from fingerprint). This scheme uses either a decoding algorithm of error correcting codes or alternatively some polynomial interpolations to recover the secret key during authentication. Even if biometric cryptosystems are designed to secure biometric templates, these systems are vulnerable to several threats as spoofing and falsification. Besides, biometric data are not always secret, introducing vulnerabilities for the protection of the secret key. For example, the biometric data can be recovered by lifting fingerprint traces from objects touched by some peoples (particularly a mobile phone) or from some pictures recuperated from a Facebook account.

Since these compromised images have usually degraded resolution, it is not clear if these data can be used for successful authentication. This problem has been only analysed without protection scheme or in the case of fuzzy commitments in [21]. This paper investigates this attack against fuzzy vault biometric cryptosystems. The resistance of this scheme is evaluated for several degree of alteration of biometric data in the cases of fingerprints and face images. Figure 1 illustrates our supposed scenario and experiments are carried out on fingerprints and face images. It is found that these systems are vulnerable to the proposed attack in particular if the alteration level is minimal.

The organization of this paper is as follows. In Section 2, a description of fuzzy vaults and an overview of existing attacks on this scheme are presented. The *Low-Resolution* attack on fuzzy vault scheme is proposed in Section 3 and experimental applications are discussed in Section 4. Conclusion and future works are given in Section 5.

II. Fuzzy vaults : description and attacks

The original presentation of fuzzy vaults proposed by Juels and Sudan [12] uses a polynomial where a secret key is

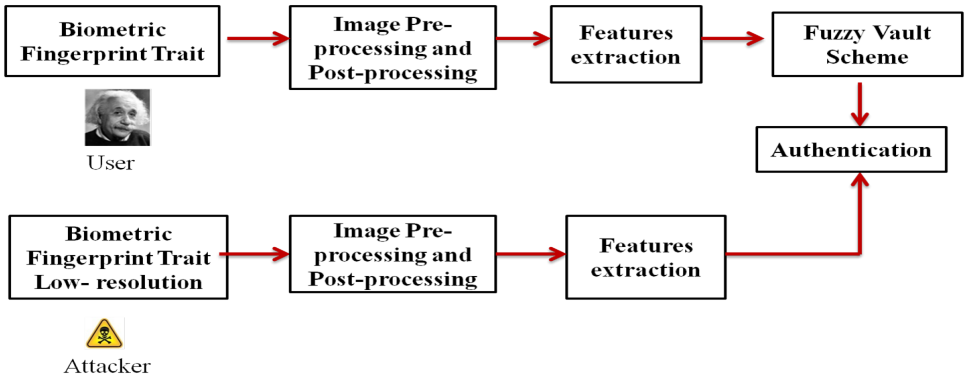

Fig. 1. Scenario of our proposed attack.

encoded in the polynomial coefficients. This polynomial is evaluated on each values derived from the biometric feature and a large series of chaff points (i.e. random points) are added to the polynomial values to form the $Vault$. If request features are approximately close to the abscissas of the vault, the polynomial and the secret key can be recovered using polynomial interpolation or error correcting code such as Reed-Solomon codes.

The enrollment biometric feature b is a set of n values x_i in a finite field $\mathbf{F}_q$ and P is a polynomial of $\mathbf{F}_q[x]$ of degree $k < n$. The vault V is the union of two sets $V_A \cup V_B$, where the set $V_A = \{(x_i, P(x_i)), i = 1, \ldots, n\}$ corresponds to the polynomial evaluation and the set $V_B = \{(x_j, y_j) \mid x_j \neq x_i, \forall i = 1, \ldots, n, y_j \neq P(x_i)\}$ corresponds to chaff points. During the authentication, for a query set of minutiae b', the unlocking set $U = \{(x, y) \in V,\ x \in v'\}$ of size m is computed. The polynomial P is recovered using a decoding algorithm on U as a received vector from a $[m, k]$ Reed Solomon code, or alternatively by some polynomial interpolations. The authentication is considered to be successful if and only if the unlocking set U contains at least k genuine points from enrolled features. The correctness of the resulting polynomial can be verified for example with an helper data such as $H(P)$, where H is a cryptographic hash function. Details and analysis of this construction are provided in [12], [23]. Besides, the applications of fuzzy vaults on fingerprints are numerous [5], [18], [20], [24], particularly using the FVC2002 database, [16]. These schemes introduce generally a data alignment step before the vault construction. Implementation of fuzzy vaults is realized on other biometric modalities such as face biometrics [9], iris images [14], handwritten signature [10] and also performed using a combination of several modalities (i.e multibiometric systems) [19].

There are different attacks applied on fuzzy vaults (and other biometric cryptosystems) if an attacker is able to compromise one or several stored biometric informations from a database. For example these informations can be used by either reverse engineering the original data (brute force attacks, hill climbing attacks) or replaying the stored template. Chang et al. have identified the location of chaff points, this is proved by the observation of non-randomness of fuzzy vaults [4]. The brute force attack is related to the hardness to recover the polynomial from the vault, and the probability that t vault pairs are in the genuine list is $\binom{k}{t}\binom{n}{t}^{-1}$ [5]. Correlation attacks suppose that an attacker which has two vaults of the same user stored in different applications tries to correlate the both data to retrieve the biometric trait of the user. These attacks are particularly investigated on the fuzzy vault context in [3], [22].

III. Attack with altered data

Despite active research in recent years in the evaluation of biometric template protection schemes, very few studies have focused on the impact of alteration on the security and the robustness of these systems. In [8], alteration of fingerprints is used on biometric systems (without any protection) to hide the identity of the attacker. This alteration is classed in three categories: *obliteration*, *distortion* and the *imitation*. The obliteration can be done on friction ridge patterns by abrading, cutting, burning, applying strong chemicals, and transplanting smooth skin. While the distortion can be done by turned the friction ridge patterns into unnatural ridge patterns, the imitation is a surgical process where a large area friction skin can be transplanted from other parts of the body, or cutting and then mosaicking several portions of friction skin. In the case of face authentication, the alteration is applied on face via plastic surgery or prosthetic make-up [7]. Attack using the distribution of minutiae and the orientation field is proposed by Yoon et al [26].

In this paper, we present other type of alteration that can be applied on different biometric cryptosystems with different modalities. Unlike the alterations in [8], consequences of altered image is investigated on biometric cryptosystems. Thus, we consider the attacker has an altered version of fingerprint or face image (several cases of low resolution are analysed) The attacker uses this altered data as request to gain unlawful authentication to the fuzzy vault biometric cryptosystems, for example for the access of the mobile content. The attacker can typically recuperated the low-resolution images from a

Fig. 2. Example of low resolution fingerprint (level 0.3).

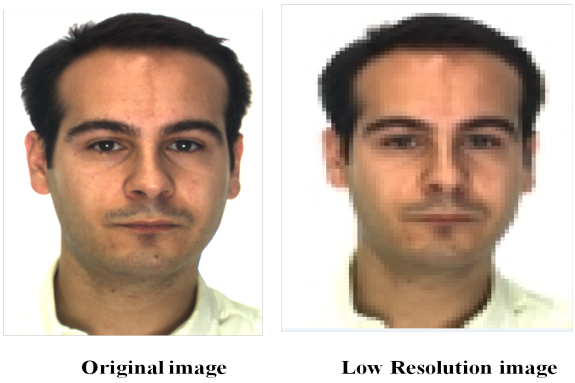

Fig. 3. Example of low resolution face (level 0.3).

fingerprint traces of the real user or user photograph for attacking the face based fuzzy vault.

In order to create several low resolution images, we varied the resolution using the downsampling [25] where we reduce the number of pixels compared to the user image which result degraded images quality. The downsampling is based on different scales inferior to 1 and bicubic interpolation (used in image resizing). Since the attacker can improve the image quality if he has user images with low resolution, the antialiasing process [15] is then applied after the downsampling in order to enhance the quality of altered images. Hence different images that are scale times the size of user image are generated. The appearance of image is altered prior preprocessing and features extraction. Resulting features from the low resolution image are then used to retrieve the unlock set from the stored vault.

IV. Experimental Results

A. Experimental Setup

Fingerprint authentication system is created based on four steps [6]. The first step is the pre-processing where biometric image is enhanced using histogram equalization, Fourier transform, binarization. In order to elicit the important information in the fingerprint image, a segmentation is then applied. Next, minutiae are extracted based on ridge highlighting and minutiae marking. Afterwards, post-processing is realized where H-breaks isolate points and false minutiae are removed. Alignment process is applied to align request set of minutiae with respect to the reference set. The ridge correlation factor is calculated and the similarity between both ridges is then measured. If the similarity score is above to 0.8, then transform each set of minutia with respect to the reference. Finally, minutiae are matched if they have almost identical direction and position. Figure 4 illustrates the different steps of pre-processing, features extraction and post-processing of fingerprint image.

The face authentication system requires the calculation of the number of associations between the reference and request images. At first, local features are detected and extracted using Scale-Invariant Feature Transform (SIFT algorithm) [2]. Matching process is based on comparison of the number of associations between both images (reference and request) and the system threshold. Figure 5 illustrate the created face authentication system. Both created biometric systems are based on verification process where one biometric image is matched to one template (i.e.(1:1)).

Experimental results are carried out using FVC 2002 [16] database for fingerprint system and AR [17] database for face biometric system. The FVC 2002 database is generally used for the performance evaluations of fuzzy vaults implementation of fingerprints in the literature (several evaluation results are given in [23], with a genuine acceptance rate of 92% for the entire database).

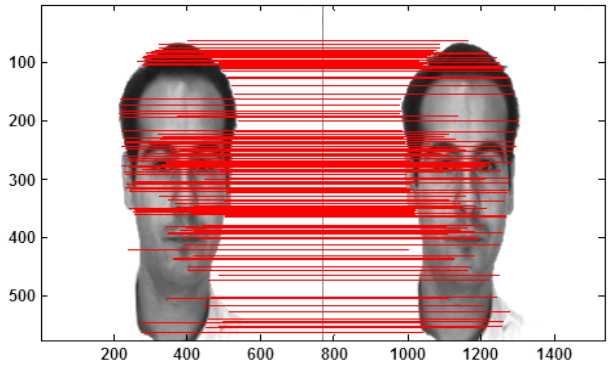

Fig. 5. Face authentication system.

Both fuzzy vaults biometric cryptosystems (fingerprint fuzzy vault and face fuzzy vault) use a secret key K, which is encoded as a polynomial P of degree 13 in the Galois field $GF(2^{16})$ (the secret is coefficients of the polynomial). For fingerprints fuzzy vault, an enrollment set X of extracted features (864 features: 72 minutia and the rest present the ridge associated with each minutia) from user image is evaluated to form the *Lock* set V_A. A set V_B of 8000 random chaff points that do not lie on P are generated in order to envelop the original features. For face fuzzy vault, 194 biometric features

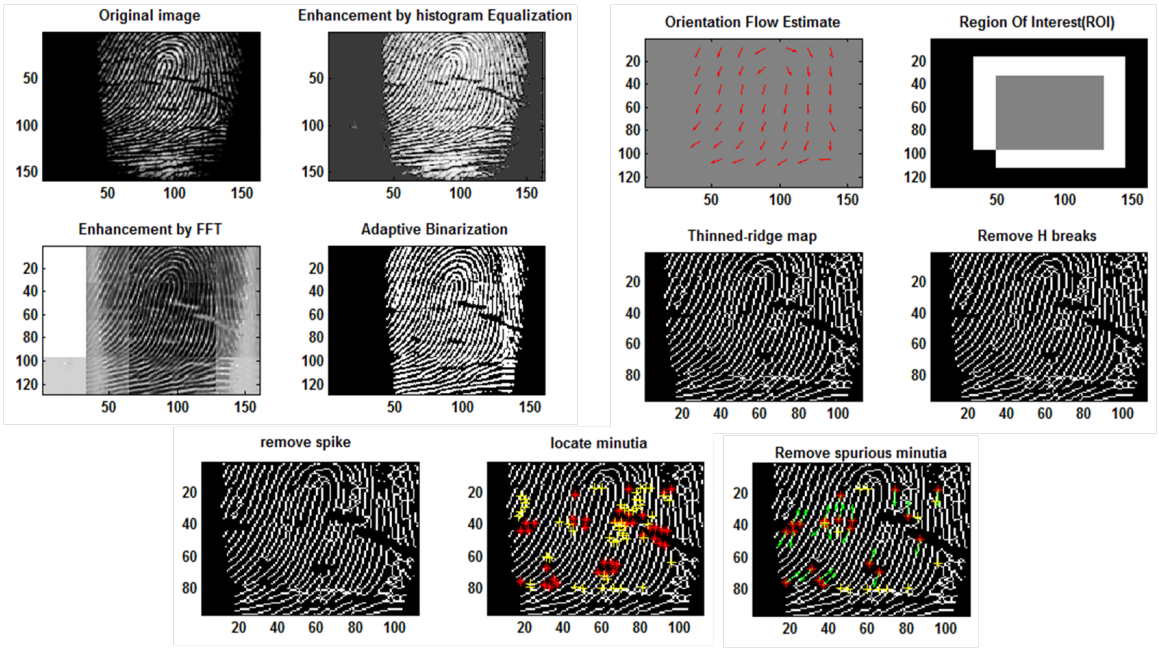

Fig. 4. Example of different steps of pre-processing, features extraction and post-processing of fingerprint altered image.

are extracted from user image and 2000 chaff points are added to construct the vault V.
During authentication, the *Unlock* set (corresponded features between the request presented by the attacker and the vault abscissa) is generated. Thus interpolation is used to retrieve the polynomial P (or the secret K).

After creating the fingerprint and face fuzzy vaults, we generated 112 altered versions (with low resolution) of user image as explained in Section 3, we tested these images as requests for verification process (i.e (1:1)) where all altered images are tested against the reference image of user. The matched features between each altered image and vault abscissa is then derived to create the unlocking set. In order to extract the number of correct matched features, the similarity between the enrolled user features and the unlocking set is then calculated.

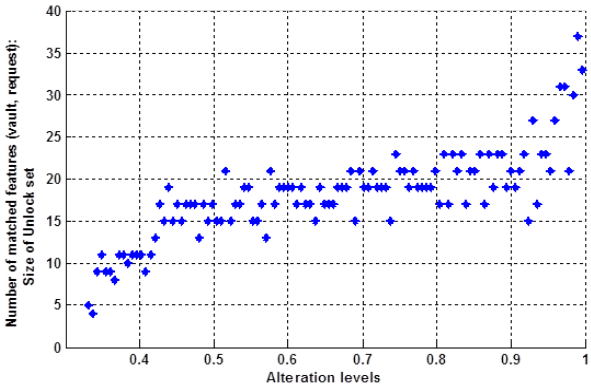

Fig. 6. Number of matched features between the vault and the altered images (i.e. size of unlocking set) according to alteration levels in fingerprints fuzzy vault.

B. Evaluation of Fingerprint Fuzzy Vault

Figure 6 shows the size of unlocking set in the fingerprints fuzzy vault according to alteration levels. We observe some degree of correlation between the size of the unlocking set and the alteration levels. If the level of alteration is goes to 1, we obtain image with resolution almost similar to the user image. Hence, where image quality is not very degraded compared to the original image, the size of unlocking set is increased. Whereas if the level of alteration is higher, the number of corresponded features between the vault and the request is decreased.

In order to determinate if the attacker can gain access to the system using altered images, we compare the unlocking set and the original features extracted from user image (in enrolment stage) to derive the number of correct matched features "*correct match*". Hence, the authentication is considered to be successful if at least k genuine features can be recovered from the unlocking set. The correct match of fingerprint fuzzy vault is presented in Figure 7.

This Figure describes the number of matched features between the unlocking set and the original feature extracted from user image during the enrollment stage. We remark that the number of matched features between the unlocking set and the original features of the user is increased according to the alteration levels. When the alteration level is greater to 0.44, we notice that the number of genuine features is greater to k. Thus, the attacker can gain access to the system even if the

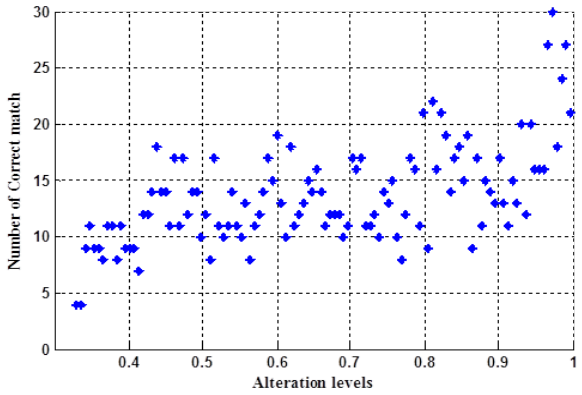

Fig. 7. Correct match of altered images according to alteration levels in fingerprints fuzzy vault.

level of alteration is higher. On the other hand, if the attacker uses image with minimal alteration (alteration level goes to 1), he can gain access with probability 100%.

C. Evaluation of Face Fuzzy Vault

In Figure 8, we show the number of corresponded associations between the vault and the altered images (size of unlocking set) according to the resolution levels in face fuzzy vault system. We remark that the size of the unlocking set is increased in accordance with the alteration levels.

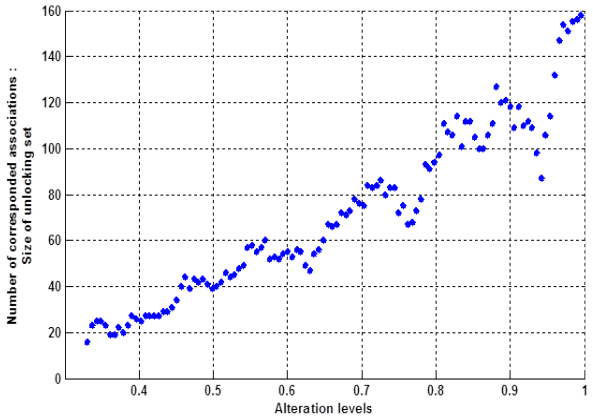

Fig. 8. Number of corresponded associations between the vault and the request (i.e. size of unlocking set) according to level of alteration in face fuzzy vault

In order to derive the number of genuine features that can be extracted from the unlocking set, we calculate the number of corresponded keypoints between the unlocking set and the original keypoints extracted from the user image. We measure then the number of correct match for face fuzzy vault as shown in Figure 9. We remark that the distribution of correct match is increased if the level of alteration is minimal and vis versa. On the other hand, the number of genuine keypoints is always greater to the polynomial degree (the number of genuine features derived from the unlocking set is greater or equal to k) for overall altered images, this means that the attacker can authenticate with 100% for whole altered images even if the level of alteration is higher.

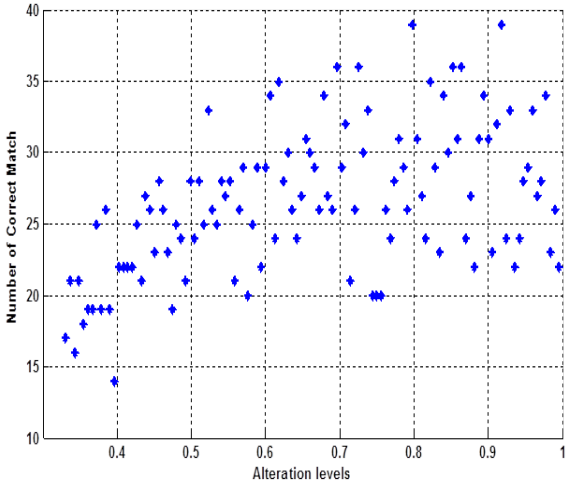

Fig. 9. Correct matching of face fuzzy vault according to the alteration level.

D. Discussion

In order to illustrate the relation between the resolution level and the correct match, Table 1 and Table 2 summarize the relation between, the resolution levels, the number of extracted features from altered images, the number of corresponded features between the request and the vault abscissa (i.e. size of the unlocking set) and the genuine extracted features from the unlocking set. We can see that for most cases, alteration level can affect the number of extracted features. When the resolution of altered image is not very degraded compared to the user image, the system can extract important number of features. Thus, the number of corresponded features between the vault and the request (size of unlocking set) can be increased which increase the number of genuine features derived from the unlocking set (i.e. the correct match).

We empirically quantified the success of the attacker which have biometric image traces of the real user to gain illegitimate access. We conclude that the attacker able to have 100% as probability of successful authentication (more than k genuine features) for whole altered images in face based fuzzy vault and for the majority of altered requests in fingerprint based fuzzy vault supporting the claim that the fuzzy vault based biometric cryptosystems are indeed vulnerable to such attack.

V. Conclusion

Biometric authentication used in mobile technologies is generally based on biometric data with traces. Thus, attackers are possibly able to recover some altered versions of real

Resolution Level	Number of extracted features	Size of unlocking set	Number of genuine features
0.33	38	5	4
0.342	90	11	9
0.69	459	21	12
0.87	750	24	17

TABLE I
FINGERPRINT BASED FUZZY VAULT.

Resolution Level	Number of extracted features	Size of unlocking set	Number of genuine features
0.33	108	17	16
0.342	119	25	21
0.69	186	76	26
0.87	201	120	31

TABLE II
FACE BASED FUZZY VAULT.

biometric data. This paper analysed the security of fuzzy vault schemes under this assumption, where several degree of low resolution are investigated. We practically tested this attack against fuzzy vault biometric cryptosystems with fingerprints and face images. Our results show that this scheme is vulnerable to the proposed attack even if the level of alteration is higher, particularly in the case of face images. In future work, other alteration attacks, as blur and lightness, should be applied, on possibly different biometric modalities, as voice recognition, also used in mobile authentication.

REFERENCES

[1] ISO/IEC 24745:2011 JTC1 SC2 security techniques. information technology - security techniques - biometric information protection, 2011.

[2] M. Bicego, A. Lagorio, E. Grosso, and M. Tistarelli. On the use of SIFT features for face authentication. In *Computer Vision and Pattern Recognition Workshop*, pages 35–35, 2006.

[3] M. Blanton and M. Aliasgari. Analysis of reusability of secure sketches and fuzzy extractors. *IEEE Transactions on Information Forensics and Security*, 2013.

[4] E.-C. Chang, R. Shen, and F. W. Teo. Finding the original point set hidden among chaff. In *ACM ASIACCS*, pages 182–188, 2006.

[5] T. Clancy, D. Lin, and N. Kiyavash. Secure smartcard-based fingerprint authentication. In *ACM SIGMM workshop on Biometric Methods and Applications*, pages 45–52, 2003.

[6] A. El-Sisi. Design and implementation biometric access control system using fingerprint for restricted area based on gabor filter. *Int. Arab J. Inf. Technol.*, 8(4):355–363, 2011.

[7] N. Erdogmus, N. Kose, and J.-L. Dugelay. Impact analysis of nose alterations on 2d and 3d face recognition. In *Multimedia Signal Processing (MMSP)*, pages 354–359, 2012.

[8] J. Feng, A. K. Jain, and A. Ross. Detecting altered fingerprints. In *International Conference on Pattern Recognition (ICPR)*, pages 1622–1625, 2010.

[9] Y. C. Feng and P. C. Yuen. Protecting face biometric data on smartcard with reed-solomon code. In *CVPR Workshop on Biometrics*, 2006.

[10] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia. Cryptographic key generation using handwritten signature. In *SPIE Conference Biometric Technologies for Human Identification*, volume 6202, pages 225–231, 2006.

[11] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP J. Adv. Sig. Proc*, 2008.

[12] A. Juels and M. Sudan. A fuzzy vault scheme. *Designs, Codes and Cryptography*, 38(2):237–257, 2006.

[13] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *ACM CCS*, pages 28–36, 1999.

[14] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim. Biometric key binding: Fuzzy vault based on iris images. In *Int. Conference on Biometrics (ICB)*, pages 800–808, 2007.

[15] R. Lukac and K. N. Plataniotis. *Color image processing: methods and applications*. CRC press, 2006.

[16] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. FVC2002: Second fingerprint verification competition. In *International Conference on Pattern Recognition (ICPR)*, volume 3, pages 811–814. IEEE, 2002.

[17] A. M. Martinez. The AR face database, 1998.

[18] A. Nagar, K. Nandakumar, and A. K. Jain. Securing fingerprint template : Fuzzy vault with minutiae descriptors. In *International Conference on Pattern Recognition (ICPR)*, pages 1–4, 2008.

[19] K. Nandakumar and A. K. Jain. Multibiometric template security using fuzzy vault. In *BTAS*, 2008.

[20] K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint based fuzzy vault : implementation and performance. *IEEE Transactions on Information Forensics ans Security*, pages 744–757, 2007.

[21] C. Rathgeb and A. Uhl. Iris-biometric fuzzy commitment schemes under signal degradation. In *ICISP*, pages 217–225, 2012.

[22] W. J. Scheirer and T. E. Boult. Cracking fuzzy vaults and biometric encryption. In *Biometrics Symp.*, pages 1–6, 2007.

[23] B.-B. Tams. *Cryptanalysis of the Fuzzy Vault for Fingerprints: Vulnerabilities and Countermeasures*. PhD thesis, Georg-August-Universität Göttingen, 2012.

[24] U. Uludag, S. Pankanti, and A. K. Jain. Fuzzy vaults for fingerprints. In *Audio and Video based Biometric Person Authentication*, 2005.

[25] X. Wu, X. Zhang, and X. Wang. Low bit-rate image compression via adaptive down-sampling and constrained least squares upconversion. *IEEE Transactions on Image Processing*, 18(3):552–561, 2009.

[26] S. Yoon, J. Feng, and A. K. Jain. Altered fingerprints: Analysis and detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 34(3):451–464, 2012.