ON THE SECURITY OF NON-INVERTIBLE FINGERPRINT TEMPLATE TRANSFORMS

Abhishek Nagar and Anil K. Jain[*]

Department of Computer Science and Engineering
Michigan State University
East Lansing, MI-48824

ABSTRACT

Many transformation functions have been proposed for generating revocable or non-invertible biometric templates. However, their security analysis either ignores the distribution of biometric features or uses inefficient feature matching. This usually leads to unrealistic estimates of security. In this paper we introduce a new measure of non-invertibility, called the Coverage-Effort (CE) curve which measures the number of guesses (Effort) required by an adversary to recover a certain fraction (Coverage) of the original biometric data. In addition to utilizing the feature distribution, the CE curve allows estimation of security against partial recovery of biometric features. We analyze the CE curves obtained using different instances of a mixture of Gaussians based feature transform for fingerprint templates. Our analysis shows that knowledge of the fingerprint minutiae distribution reduces the effort required to obtain a specified coverage.

Index Terms— biometrics, template security, non-invertibility, information measure, fingerprint, minutiae

1. INTRODUCTION

Biometric authentication refers to techniques that utilize human traits e.g. fingerprint, face, and iris as authentication tokens which are matched with the corresponding enrolled tokens, also called template or reference. Biometric systems are being increasingly deployed due to their security advantages over the traditional authentication mechanisms based on credentials (ID cards and passwords) which can be easily lost, guessed or forged. Large scale deployments and the associated template storage have heightened the need to protect the biometric data stored in the system. Theft[1] of biometric data is a compromise of the user's privacy. Further, the stolen biometric data can be used to compromise other biometric systems that have the same trait enrolled for the user. In case of password authentication, loss of password is managed by revoking it and replacing it with a new one. Such a safety mechanism cannot be directly employed in a biometric recognition system due to the small number of human biometric traits.

One way to impart revocability property to biometric traits is to avoid an explicit storage of biometric templates in the system, eliminating any possibility of leakage of the original biometric trait. A number of template protection techniques have been designed for this purpose which can be categorized as i) *feature transformation based techniques*, and ii) *biometric cryptosystems* (cf. [1]). In feature transformation, the template is transformed using a user specific key and only the transformed template is stored in the system. During authentication, the input biometric is similarly transformed and is matched with the stored template [2, 3, 4, 5]. In a biometric cryptosystem, an external key is associated with the template such that neither the template nor the associated key can be obtained from the stored template. The key can only be recovered when a genuine biometric is presented to the system [6, 7, 8, 9].

In order to ensure the security offered by these template protection schemes, a rigorous analysis is needed. While such studies exist for biometric cryptosystems [10, 8, 11, 12, 13], not much attention has been paid to the feature transformation techniques. Security of a feature transformation technique can be evaluated based on two main criteria: i) *non-invertibility*, and ii) *diversity*. Non-invertibility refers to the difficulty in recovering the original biometric given the secure template and diversity refers to the difficulty in guessing one secure template given another secure template generated from the same biometric. Both these criteria may or may not assume knowledge of the password by the adversary. Matching performance, say using the Receiver Operating Characteristic (ROC) curve, is also used as an evaluation measure where again an impostor may or may not have access to the password.

Table 1 lists different evaluation techniques used for abovementioned evaluation criteria. The underlying objective of these evaluations is to measure the amount of information a transformed biometric, say X, can provide about the original biometric (in case of non-invertibility) or another transformed biometric (in case of diversity), say Y. To evaluate diversity, ROC corresponding to the case when the templates generated from the same biometric using different keys are considered as different individuals enrolled in the system is computed (see, e.g., [4, 14]). Non-invertibility, given that the user specific key is not available to the adversary, is usually evaluated by estimating the number of different templates that can be guessed as the original biometric given the transformed biometric (see, e.g., [3, 14]). Both these measures, however, have certain limitations. The False Accept Rate (FAR) in evaluating diversity is usually zero at a reasonable system threshold due to the limited database used in evaluation [4]. Moreover, the biometric matchers are not optimized for such experiments. On the other hand, the measure for non-invertibility does not take the distribution of biometric features into account which can lead to a significant over-estimation of security.

In this paper, we present a measure of non-invertibility for fingerprint minutiae based feature transformation techniques assuming that the user specific key is known to the adversary. The proposed technique measures the relationship between the number of guesses (*effort*) required by an adversary to recover a certain fraction (*coverage*) of the biometric template given the transformed template. The

[*] Anil Jain's research was partially supported by WCU (World Class University) program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology(R31-2008-000-10008-0).

[1] A biometric is considered stolen if an adversary captures the stored biometric trait.

different (coverage-effort)-tuples are plotted to obtain the Coverage-Effort (CE) curve. The computation of a CE curve consists of three main steps:

1. Pre-image Computation: Compute the pre-images of each transformed minutia such that transformation of all the pre-image minutiae would lead to the given transformed minutia.
2. Minutiae Likelihood Computation: Estimate the relative probability of each of the minutiae in the pre-image using kernel density estimation.
3. Non-invertibility Measure Computation: Sort the pre-images according to their likelihoods and compute the coverage i.e. the number of true pre-images guesses given that the adversary checks only a certain portion of the pre-images.

We note that the proposed measure is sufficiently generic to be useful for any feature transformation technique such that the transformation can be evaluated at any given point and is piecewise differentiable.

Evaluation Criteria	Evaluation Technique
Diversity	Match different transformed templates obtained from the same biometric [4, 14]
Non-invertibility	Number of neighboring minutiae that change after the transformation [3]
Non-invertibility with unknown key	Number of different templates that can generate the given transformed template ([3]) and number of impostor biometric templates that can be accepted as corresponding to the given transformed template by a matching algorithm ([14])
Matching performance	ROC [3, 14, 2]

Table 1. Different evaluation criteria and evaluation techniques used for feature transformation of a fingerprint template.

2. MINUTIAE TEMPLATE TRANSFORMS

Minutiae are the most common and distinctive representation of a fingerprint. These are the points on the finger surface where the friction ridges end or bifurcate. Figure 1 shows two prints from the same finger with minutiae overlaid. Note that there is a significant intra-class variation in the fingerprint representations; multiple acquisitions of the same finger lead to different number of minutiae as well as their position (x, y) and orientation (θ). It is this property that makes it difficult to match fingerprints in the encrypted domain. Note that a minutiae based fingerprint template, say T, consists of a collection of n minutiae i.e. $T = \{(x_1, y_1, \theta_1), (x_2, y_2, \theta_2), ..., (x_n, y_n, \theta_n)\}$. The transformation function considered here, $\phi(.)$, takes T to another set of n minutiae i.e. $\phi(T) = \{(x'_1, y'_1, \theta'_1), (x'_2, y'_2, \theta'_2), ..., (x'_n, y'_n, \theta'_n)\}$. Thus a measure of non-invertibility should estimate the difficulty in obtaining T given $\phi(T)$.

A desirable transformation should account for the intra-class variation while at the same time providing a reasonable template security. A number of minutiae based feature transformation techniques have been proposed (see [3, 15, 14]) where the configuration of each minutia is changed according to a user specific key to obtain the transformed template. Ratha et al. [3] proposed three different kinds of transformations i.e. cartesian, polar, and functional as illustrated in Figure 2. The many-to-one nature of these transforms provides non-invertibility even for the case when the adversary knows the user specific key. A cartesian transformation tessellates the image plane into rectangles and then shuffles the rectangles based on the user password such that any two rectangles can map on to a single rectangle. Instead of rectangles, a polar transform tessellates the image plane into sections of annular regions around a center point. A functional transformation, however, transforms the minutiae based on a function evaluated over a minutiae configuration.

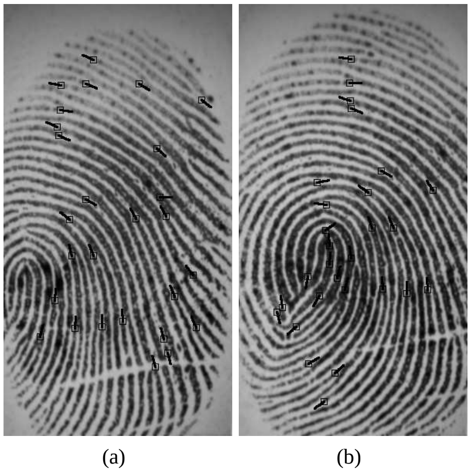


Fig. 1. Two fingerprint images from the same finger with extracted minutiae.

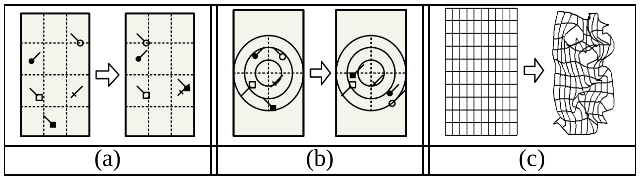


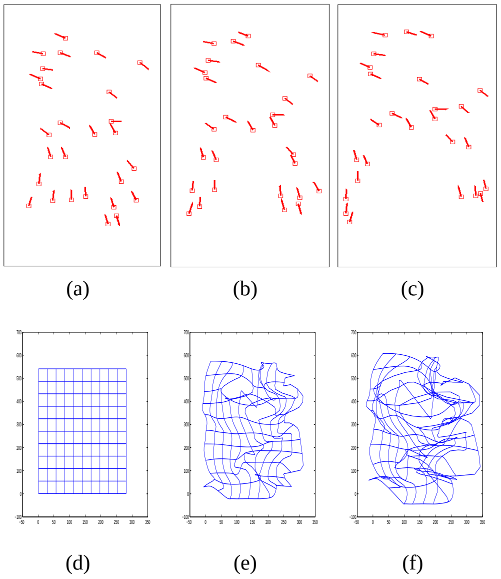
Fig. 2. Feature transformation. (a), (b), and (c) show the cartesian, polar, and Gaussian mixture based transformations [3].

3. NON-INVERTIBILITY MEASURE

The security of the feature transformation based template protection schemes is based on the *non-invertibility* of the transform. Thus it is important to design a measure of the non-invertibility which estimates the likelihood of an adversary being able to guess the original template given the transformed template. For this we propose a three-stage procedure for estimating the non-invertibility: i) pre-image identification, ii) pre-image likelihood evaluation, and iii) non-invertibility measure computation.

3.1. Mixture of Gaussians based Transform

Due to its generic nature and acceptable performance [3], we use the functional transformation technique based on a mixture of Gaussians to compute a measure of non-invertibility. In order to transform a minutia, functions consisting of a mixture of Gaussians and its derivatives are evaluated at the position of minutia and then the minutia is translated according to the values obtained. For the sake


(a) (b) (c)

(d) (e) (f)

Fig. 3. Feature transform based on mixture of Gaussians; (a) minutiae template, (b) and (c) transformed minutiae template with $\beta = 30$ and $\beta = 60$. (d), (e), and (f) depict the transformation functions corresponding to the images shown in (a), (b), and (c), respectively.

of simplicity, we restrict the transformation function to change only the x and y coordinates of a minutia.

The mixture of Gaussians used to obtain the transformation function is given by:

$$f(\vec{x}) = \sum_{i=1}^{K} t_i \pi_i e^{-\frac{1}{2}(\vec{x}-\vec{\mu_i})\Sigma_i^{-1}(\vec{x}-\vec{\mu_i})'} \qquad (1)$$

where K is the number of components, and π_i, t_i, μ_i, and Σ_i correspond to the mixing probabilities, the signs (+ or -), means, and covariance matrices of the different components, respectively. $\vec{x}$ is a vector representation of a minutia consisting of only the x and y coordinates of the minutiae. In our experiments, where the fingerprints are captured at 569 ppi resolution and are 560×296 in size, K is taken to be 24, Σ_i is taken to be a diagonal matrix with each diagonal entry equal to 50^2 for each component. The remaining parameters are determined using the user specific key.

The transformation of each minutia is represented as direction of minutia translation (denoted by ϕ_θ) and magnitude of minutia translation (denoted by ϕ_d). The two components of the transformation can be obtained as:

$$\begin{aligned} \phi_\theta(\vec{x}) = & \quad \arctan\left(\frac{f'_y(\vec{x})}{f'_x(\vec{x})}\right) + \alpha, & (2) \\ \phi_d(\vec{x}) = & \quad \beta\left\{1 + \left[\sum_{i=1}^{K} t_i \pi_i e^{-\frac{1}{2\sigma^2}(\vec{x}-\vec{\mu})(\vec{x}-\vec{\mu})'}\right]\right\}, & (3) \end{aligned}$$

where $f'_y(.)$ and $f'_x(.)$ are the x and y derivatives of f and $\alpha \in [0, 360)$ is a random offset in direction; β is used to manipulate the overall translation of minutiae. Figure 3 shows the fingerprint minutiae transformed according to the functional transformation generated using different values for β (30 and 60).

3.2. Pre-image Computation

In order to compute the pre-image of a minutia, all 4-pixel neighborhoods of the form $(i, j), (i + 1, j), (i, j + 1), (i + 1, j + 1)$ from the original fingerprint image space are transformed and the ones that *cover* a particular transformed minutia are used to obtain candidate pre-images of that minutia. Any one out of the four points in the covering neighborhood is taken as the pre-image minutia. If multiple pre-image points are sufficiently close to each other, only one of them is included in the pre-image set. Complete link clustering [16] is used for this purpose with a splitting criteria depending on the precision required in the guessed pre-image. An extension to incorporate change in θ will involve an 8-point 3D neighborhood including θ instead of a 2D neighborhood. In some cases depending on the transform, if the 4-pixel neighborhood is severely distorted, certain pre-images might not be detected. Such cases will, however, not arise if the pre-image is computed as a closed form solution or a sufficiently fine grid is used.

3.3. Pre-image Likelihood Computation

Let $\vec{v}$ be a transformed minutia and $\vec{u}^1, \vec{u}^2, ..., \vec{u}^m$ be the m pre-images of $\vec{v}$ under the transformation ϕ. Further, let $l_v \in 1, 2, ..., m$ be a random variable indicating which of the pre-images of $\vec{v}$ is the true one. We are interested in computing the probability $P(l_v = r|\vec{v} = \vec{a} = (x_v, y_v, \theta_v))$. Using the Bayes theorem,

$$P(l_v = r|\vec{v} = \vec{a}) = \frac{p(\vec{v}=\vec{a}|l_v=r) * P(l_v=r)}{\sum_{i=1...m} p(\vec{v}=\vec{a}|l_v=i) * P(l_v=i)}. \qquad (4)$$

Taking the prior probability $P(l_v = i) = 1/m, \forall i = 1, 2, ..., m$ (no preference for any particular pre-image) and converting $p(\vec{v} = \vec{a}|l_v = r)$ to $p(\vec{u}^r)$,

$$P(l = r|\vec{v} = \vec{a}) = \frac{p(\vec{u}^r)/J_\phi(\vec{u}^r)}{\sum_{k=0,...,m-1} p(\vec{u}^k)/J_\phi(\vec{u}^k)}, \qquad (5)$$

where $J_\phi(\vec{u}^k)$ is the Jacobian (cf. [17], page 234) of the transformation ϕ which can be computed either numerically or in a functional form depending on the complexity of ϕ.

In order to compute $p(\vec{u}^r)$, we perform a kernel density estimation of minutiae represented as the (x, y, θ)-tuple using a Gaussian kernel with a leave-one-out estimate of the bandwidth[2]. Before estimating the probability density, we align all the fingerprints using their high curvature points based on the Trimmed Iterative Closest Point (ICP) algorithm [9]. Note that an alignment of fingerprints prior to density estimation leads to a more distinctive probability density with a low entropy. Figure 4 shows the estimated probability density.

3.4. Non-invertibility Measure Computation

We compute a measure of non-invertibility as the number of computations required by an adversary to guess the original minutiae set using a specific attack strategy. Let there be n different minutiae in the transformed template whose pre-image needs to be computed. An attack strategy includes the order in which an adversary guesses the various n-tuples corresponding to the selection of a particular pre-image for each of the n minutiae. Note that if there are m_i pre-images of the i^{th} minutia then the number of n-tuples that the adversary needs to prioritize is $\Pi_{i=1,..,n} m_i$ which could be very large.

[2] We use the Kernel Density Estimation Toolbox for Matlab provided by Alexander Ihler (Available at: http://www.ics.uci.edu/ ihler/code/kde.html).

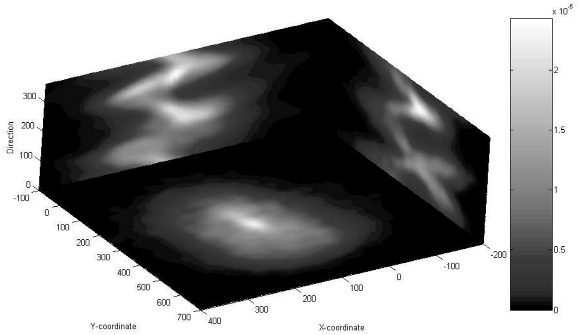


Fig. 4. Marginal densities of minutiae in (x, y), (x, θ), and (y, θ) planes.

In order to make the analysis feasible, we assume that instead of guessing from all the pre-images of a minutia, the adversary guesses only from some of the more probable pre-images of each minutiae. In the limiting case, the adversary will just select the most-probable pre-image for each minutiae.

In our experiments, we consider an adversary that checks only the 2^{H_i} most probable pre-images[3] of the minutia $v_i, i = 1...n$. Here H_i is the entropy or the difficulty in guessing the true pre-image given by

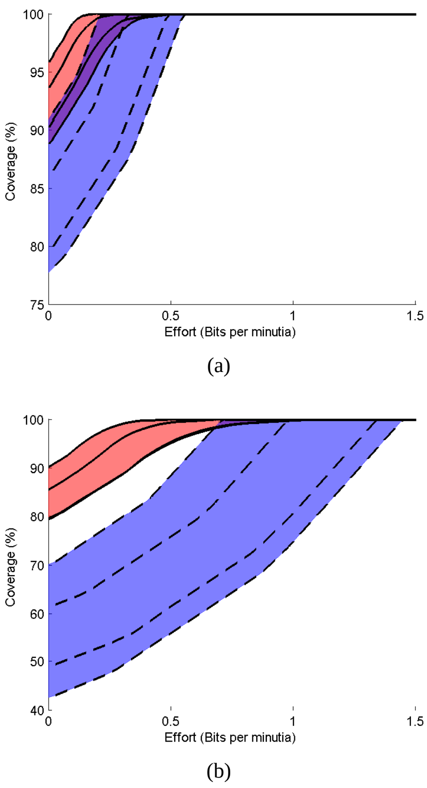
$$H_i = -\sum_{r=1}^{m_i} P(l_{v_i} = r|\vec{v_i}) \log_2(P(l_{v_i} = r|\vec{v_i})), \qquad (6)$$

where m_i is the number of pre-images of v_i. In this scenario, $\Pi_i 2^{H_i}$ different guesses will be made simultaneously for each individual minutia leading to an effort equivalent to $1/n \sum_i H_i$ bits per minutia. The corresponding coverage is computed as the fraction of minutiae whose true pre-images lie among the searched space. Note that these two values, i.e. effort and coverage, provide only a single point on the Coverage-Effort curve. In order to increase or decrease the coverage, we assume that adversary searches for $min(m_i, \lceil 2^{H_i+\eta} \rceil)$ most probable pre-images per minutia, where $\eta \in [-max(H_i), max(H_i)]$. Note that in this case, the adversary is making $\approx 2^{n\eta}$ times more (or less if η is negative) guesses than the previous case. This leads to the complete CE curves as shown in Figure 5.

4. EXPERIMENTS

To demonstrate the effectiveness of the proposed non-invertibility measure, we evaluated it on the publicly available FVC2002 database-2 which contains 800 fingerprint images (100 fingers × 8 impressions/finger) of size 560×296 captured at 569 ppi resolution. There are about 35 minutiae per fingerprint in the database. The experiments are based on mixture of Gaussians based functional transformation technique.

Figure 5 shows the Coverage-Effort curves corresponding to the mixture of Gaussians based transformation with two different parameter settings. For each parameter setting, four different randomly generated transformation instances were used, say corresponding to using four different passwords. We also obtain the CE curves corresponding to the case when the minutiae distribution is uniform. As shown in Figure 5, the curves obtained using the uniform minutiae distribution depict significantly greater security as compared to when the true minutiae distribution is taken into consideration. This is due to the fact that the minutiae with low pre-image entropy have the correct pre-image among the first few highly probable pre-images. Also, it can be observed that different parameter values can lead to significantly different security for a transformed template. Note that the proposed approach can be used to compute the coverage effort curve for individual fingerprints. Figure 6 shows the CE curve and the corresponding minutiae from a fingerprint.



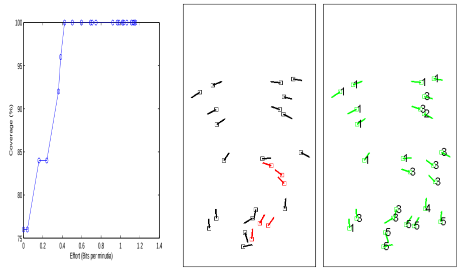
(a)

(b)

Fig. 5. Coverage-Effort curves for the mixture of Gaussians based feature transformation. (a) and (b) CE curves for the case when β equals 30 and 60, respectively keeping the remaining parameters fixed. In each figure four different instances of the transformation are shown with four different solid lines. The dotted lines correspond to random guesses of the true pre-image. The size of the colored regions indicate variance in the security imparted by different instances of the transform.

We used the Neurotechnology Verifinger SDK [18] in order to perform the minutiae matching. The genuine matches were performed by matching each of the eight impressions of a finger with each other impression leading to 2,800 genuine matches and the impostor matches were performed by matching the first impression of each finger with the first impression of the remaining fingers leading to 4,950 impostor matching scores. The matching results reported here are for the case when the impostor knows the true user specific key i.e. all the templates in the database have been transformed using the same user specific key. Figure 7 shows the ROC curves corresponding to the transformed templates based on two different parameter settings of the mixture of Gaussians transform (same as

[3] Note that for a random variable Z with m equally likely pre-images, $m = 2^{H_Z}$ where H_Z is its entropy.



(a) (b) (c)

Fig. 6. CE curve for individual finger. (a) shows the CE curve, (b) the most likely pre-image of each minutia with the correctly guessed minutiae shown in black, and (c) the true pre-images with the total number of pre-images per minutia.

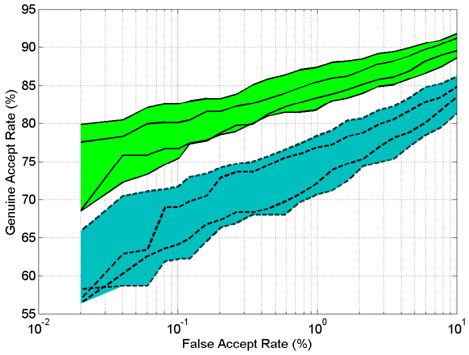


Fig. 7. ROC curves for the mixture of Gaussians based transformation of fingerprint template. Four random instances of the two cases where β (see eq. (3)) equals 30 and 60 are shown as solid and dotted lines, respectively. The size of colored regions indicate variance in performance of different instances of the transform.

those used in computing the CE curves). It can be observed that the parameter setting that leads to lower security has better matching performance verifying the trade-off between security and matching performance as expected.

5. CONCLUSIONS

As noted in [19], proper evaluation is essential to motivate the development and acceptance of good security techniques. In this paper we have identified the shortcomings in the existing measures used to evaluate non-invertibility of a minutiae transformation technique. We propose a new evaluation measure, the CE curve, that takes into account the distribution of biometric features thereby providing a quite realistic estimate of security. Note that a template that can be easily inverted not only compromises the associated system but also some systems that use different features extracted from the same biometric. We have also validated the measure using the Gaussian of mixture based transformation technique on a public database.

6. REFERENCES

[1] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," *EURASIP Journal on Advances in Signal Processing*, January 2008.

[2] Andrew B.J. Teoh, Yip Wai Kuan, and Sangyoun Lee, "Cancellable biometrics and annotations on biohash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034–2044, 2008.

[3] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating Cancelable Fingerprint Templates," *IEEE Trans. PAMI*, vol. 29, no. 4, pp. 561–572, April 2007.

[4] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and Revocable Fingerprint Recognition," in *Proc. Computer Vision and Pattern Recognition*, Minneapolis, June 2007.

[5] Y. Sutcu, H. T. Sencar, and N. Memon, "A Secure Biometric Authentication Scheme Based on Robust Hashing," in *Proc. ACM Multimedia and Security Workshop*, New York, August 2005, pp. 111–116.

[6] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," in *Proc. 6th ACM Conference on Computer and Communications Security*, Singapore, November 1999, pp. 28–36.

[7] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," in *Proc. IEEE Int'l Symp. on Information Theory*, Lausanne, Switzerland, 2002, p. 408.

[8] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *SIAM Journal on computing*, vol. 38, no. 1, pp. 97–139, 2008.

[9] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance," *IEEE Trans. Information Forensics and Security*, vol. 2, no. 4, pp. 744–757, 2007.

[10] W. J. Scheirer and T. E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," in *Proc. Biometrics Symposium*, Baltimore, 2007.

[11] J.D. Golic and M. Baltatu, "Entropy analysis and new constructions of biometric key generation systems," *IEEE Trans. Information Theory*, vol. 54, no. 5, pp. 2026–2040, May 2008.

[12] L. Ballard, S. Kamara, F. Monrose, and M. K. Reiter, "Towards practical biometric key generation with randomized biometric templates," in *Proc. 15th ACM conference on Computer and communications security*, New York, 2008, pp. 235–244.

[13] K. Simoens, P. Tuyls, and B. Preneel, "Privacy Weaknesses in Biometric Sketches," in *Proc. IEEE Symposium on Security and Privacy*, 2009, To appear.

[14] C. Lee, J. Y. Choi, K. A. Toh, and S. Lee, "Alignment-Free Cancelable Fingerprint Templates Based on Local Minutiae Information," *IEEE Trans. Systems, Man, and Cybernetics, Part B*, vol. 37, no. 4, pp. 980–992, 2007.

[15] K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening Fingerprint Fuzzy Vault Using Password," in *Proc. Int'l Conference on Biometrics*, Seoul, August 2007, pp. 927–937.

[16] A. K. Jain and R. C. Dubes, *Algorithms for Clustering Data*, Prentice Hall, 1988.

[17] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, McGraw-Hill, 1965.

[18] Nurotechnology, "Verifinger SDK 4.2," http://www.neurotechnology.com.

[19] A. Anderson and T. Moore, "Information Security: where computer science, economics and psychology meet," *Philosophical Transactions of the Royal Society A*, vol. 367, no. 1898, pp. 2717–2727, July 2009.