ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

LOGISTIC REGRESSION BASED DECISION TREE CLASSIFIER FOR COMBINED FINGER PRIVACY PROTECTION

Nidhi Sudhakaran[1] and M.Mary Synthuja Jain Preetha[2]

[1]PG Student, [2]Asst Professor, Dept. of ECE, Noorul Islam University

ABSTRACT

A novel system is proposed for protecting fingerprint privacy by combining two different fingerprints into a new identity. In the enrollment, two fingerprints are captured from two different fingers. We extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored in a database. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template. By storing the combined minutiae template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen. Furthermore, because of the similarity in topology, it is difficult for the attacker to distinguish a combined minutiae template from the original minutiae templates. With the help of an existing fingerprint reconstruction approach, we are able to convert the combined minutiae template into a real-look alike combined fingerprint. Thus, a new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based fingerprint matching algorithms. Improving the classification accuracy by applying logistic regression based Decision tree classifier. The experimental results show that our system can achieve a very low error rate compared to conventional method.

KEYWORDS: minutiae, template, classifier, logistic regression *etc.*

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

INTRODUCTION

Biometrics, those unique traits that do not change significantly over a lifetime, present interesting challenges to the security researcher, because of their inherent properties. Unlike familiar cryptographic techniques, biometric data is inexact and can only be approximately matched; hence simple hashing cannot protect it. We also care a great deal about privacy - our biometrics may be used to identify who we are, in circumstances where anonymity is expected. Or, even worse, we may become the victims of identity theft if our biometrics is compromised. The most serious flaw of biometrics, however, is non-revocability. If a biometric is compromised, the user cannot simply generate a new one, as with passwords or PINs. Once a biometric is compromised, it can never be recovered.

Biometrics-based authentication systems offer obvious usability advantages over traditional password and token-based authentication schemes. However, biometrics raises several privacy concerns. A biometric is permanently associated with a user and cannot be changed. Moreover, if the same biometric is used in multiple applications, a user can potentially be tracked from one application to the next by cross-matching biometric databases. Ratha *et al.* [4] propose to generate cancelable fingerprint templates by applying noninvertible transforms on the minutiae. The noninvertible transform is guided by a key, which will usually lead to a reduction in matching accuracy. The work in [2] and [4] are shown to be vulnerable to intrusion and linkage attacks when both the key and the transformed template are stolen [5]. Nandakumar *et al.* [6] propose to implement fuzzy fault on the minutiae, which is vulnerable to the key-inversion attack [7]. Our work in [8] imperceptibly hide the user identity on the thinned fingerprint using a key. The user identity may also be compromised when both the key and the protected thinned fingerprint are stolen.

There are only a few schemes [9].[13] that are able to protect the privacy of the fingerprint without using a key. Ross and Othman [9] propose to use visual cryptography for protecting the privacy of biometrics. The fingerprint image is decomposed by using a visual cryptography scheme to produce two noise-like images (termed as sheets) which are stored in two separate databases. During the authentication, the two sheets are overlaid to

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

create a temporary fingerprint image for matching. The advantage of this system is that the identity of the biometrics is never exposed to the attacker in a single database. However, it requires two separate databases to work together, which is not practical in same applications.

The works in [10],[12] combine two different fingerprints into a single new identity either in the feature level [10] or in the image level [11], [12]. In [10], the concept of combining two different fingerprints into a new identity is first proposed, where the new identity is created by combining the minutiae positions extracted from the two fingerprints. The original minutiae positions of each fingerprint can be protected in the new identity. However, it is easy for the attacker to identify such a new identity because it contains many more minutiae positions than that of an original fingerprint. The experiment shows that the EER of matching the new identities is 2.1% when the original minutiae positions are marked manually from the original fingerprints. A similar scheme is proposed in [13], where the minutiae positions extracted from a fingerprint and the artificial points generated from the voice are combined to produce a new identity. In this work, the EER are shown to be under 2% according to the experimental results.

THE PROPOSED FINGERPRINT PRIVACY PROTECTION SYSTEM

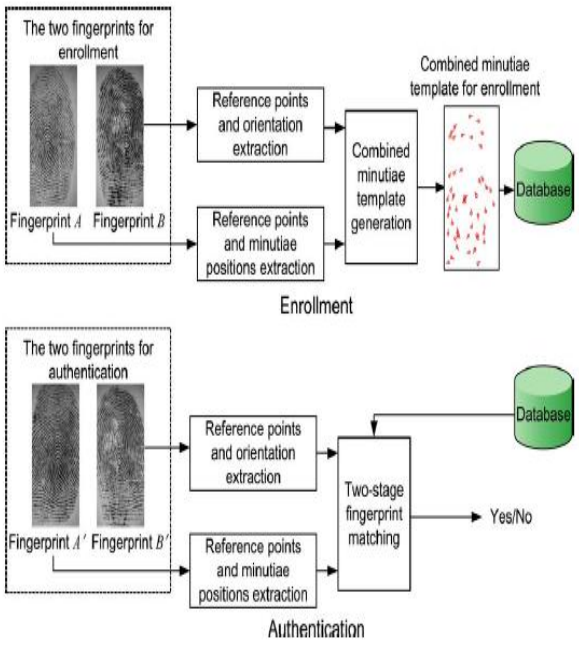

Fig. 1. Proposed fingerprint privacy protection system.

Fig. 1 shows our proposed fingerprint privacy protection system. In the enrollment phase, the system captures two fingerprints from two different fingers, say fingerprints and from fingers and, respectively. We extract the minutiae positions from fingerprint and the orientation from fingerprint using some existing techniques [16], [17]. Then, by using our proposed coding strategies, a combined

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

minutiae template is generated based on the minutiae positions, the orientation and the reference points detected from both fingerprints. Finally,the combined minutiae template is stored in a database.

In the authentication phase, two query fingerprints are required from the same two fingers, say fingerprints and from fingers. As what we have done in the enrollment, we extract the minutiae positions from fingerprint and the orientation from fingerprint. Reference points are detected from both query fingerprints. This extracted information will be matched against the corresponding template stored in the database by using a two-stage fingerprint matching. The authentication will be successful if the matching score is over a predefined threshold.

A. REFERENCE POINTS DETECTION

The reference point's detection process is motivated by

Nilsson *et al.* [18], who first propose to use complex filters for singular point detection. Given a fingerprint, the main steps of the reference points detection are summarized as follows:

1) Compute the orientation from the fingerprint using the orientation estimation algorithm proposed in [17]. Obtain the orientation in complex domain, where

$$Z=\cos(2O)+j\sin(2O) \quad (1)$$

2) Calculate a certainty map of reference points [18]

$$Cref = Z * \widetilde{Tref} \quad (2)$$

where "Tref " is the convolution operator and is the conjugate of

$$Tref=(x+iy).\ 1/2\pi\sigma^2.\ \exp(-\ x^2+y^2/2\sigma^2) \quad (3)$$

which is the kernel for reference points detection.

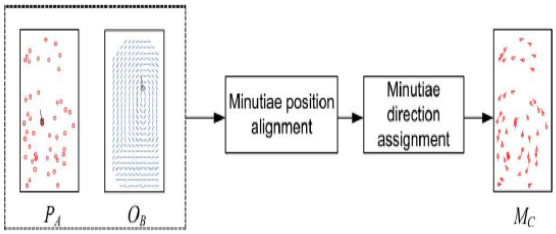

Fig. 2. Combined minutiae template generation process.

3) Calculate an improved certainty map [19]:

$$C'ref = \{Cref.\sin(Arg(Cref)) \text{ if } Arg(Cref)>0$$
$$0$$
$$\text{otherwise} \quad (4)$$

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

Where Arg(z) returns the principal value of the argument of (defined from-π to π).

4) Locate a reference point satisfying the two criterions:

(i) the amplitude of C'ref of the point (hereinafter termed as the certainty value for simplicity) is a local maximum, and

(ii) the local maximum should be over a fixed threshold T .

Suppose we locate a reference point at (rx,ry),the corresponding angle can be estimated as Arg(C'ref(rx,ry)).

5) Repeat step 4) until all reference points are located.

6) If no reference point is found for the fingerprint in steps 4) and 5) (e.g., an arch fingerprint), locate a reference point with the maximum certainty value in the whole fingerprint image.

B. COMBINED MINUTIAE TEMPLATE GENERATION

Given a set of N minutiae positions PA={pia=(xia,yia),1≤i≤N} of fingerprint A , the orientation OB of fingerprint and the reference points of fingerprints A and B ,a combined minutiae template is generated by minutiae position alignment and minutiae direction assignment, as shown in Fig. 2.

1) Minutiae Position Alignment: Among all the reference points of a fingerprint for enrollment, we define a reference point with the maximum certainty value as the primary reference point. Therefore, we have two primary reference points Ra and Rb for fingerprints A and B, respectively. Let's assume is located at ra=(rxa,rya)with the angle βa , and Rb is located at rb= (rxb,ryb) with the angle βb . The alignment is performed by translating and rotating each minutiae point pia to pic=(xic,yic) by

$$(p_{ic})^T = H.(p_{ia} - r_a)^T + (r_b)^T \qquad (5)$$

Where $()^T$ is the transpose operator and H is the rotation matrix

where

$$H=\begin{bmatrix} \cos(\beta_b - \beta_a) & \sin(\beta_b - \beta_a) \\ -sin(\beta_b - \beta_a) & cos(\beta_b - \beta_a) \end{bmatrix} \qquad (6)$$

As such, Ra and Rb are overlapped both in the position and the angle after the minutiae position alignment.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

2) Minutiae Direction Assignment: Each aligned minutiae position is assigned with a direction as follows:

$$\theta_{ic} = O_B(x_{ic}, y_{ic}) + \rho_i \pi \quad (7)$$

where ρ_i is an integer that is either 0 or 1. The range of is from 0 to . Therefore, the range of $O_B(x_{ic}, y_{ic})$ will be from 0 to 2π , which is the same as that of the minutiae directions from an original fingerprint. Following three coding strategies are proposed for determining the value of ρ_i.

1) ρ_i is randomly selected from .

2) ρ_i is determined by

$$\rho_i = \begin{cases} 1, & if\ mod(\theta_{ia} + \beta_b - \beta_a, \pi) - O_B(x_{ic}, y_{ic}) > 0 \\ 0, & otherwise \end{cases} \quad (8)$$

Where mod is the modulo operator and is the original direction of a minutiae position in fingerprint .

3) ρ_i is determined by

$$\rho_i = \begin{cases} 1, & if\ mod(ave_b(x_{ic}, y_{ic}), \pi) - O_B(x_{ic}, y_{ic}) > 0 \\ 0, & otherwise \end{cases}$$

Where $ave_b(x_{ic}, y_{ic})$ is the average direction of the nearest neighboring minutiae points of the location in fingerprint

$$ave_b(x_{ic}, y_{ic}) = \frac{1}{n}\sum_{k=1}^{n} \theta_b^k(x_{ic}, y_{ic}) \quad (10)$$

where $\theta_b^k(x_{ic}, y_{ic})$ means the direction of the kth nearest neighboring minutiae point of the location (x_{ic}, y_{ic}) in fingerprint B, and n is empirically set as 5 which is able to provide a good balance between the diversity and matching accuracy of the combined minutiae templates.

ICOMBINED FINGERPRINT GENERATION

In a combined minutiae template, the minutiae positions and directions (after modulo) are extracted from two different fingerprints separately. These minutiae

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

positions and directions share a similar topology to those from an original fingerprint. Therefore, the combined minutiae template has a similar topology to an original minutiae template. Some existing works have shown that it is possible to reconstruct a full fingerprint image from a minutiae template. By adopting one of these fingerprint reconstruction approaches, we are able to convert our combined minutiae template into a combined fingerprint image. Fig. 3 shows our process to generate a combined fingerprint for two different fingerprints. Given any two different fingerprints as input, we first generate a combined minutiae template using our combined minutiae template generation algorithm. Then, a combined fingerprint is reconstructed from the combined minutiae template using one of the existing fingerprint reconstruction approaches.

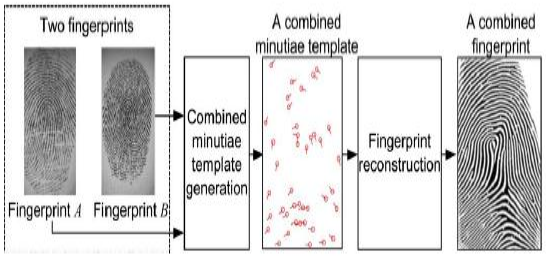

Fig. 3. Generating a combined fingerprint for two different fingerprints

It should be noted that the combined minutiae template generated by adopting *Coding Strategy* 1 is not appropriate for generating a combined fingerprint.

The reason is that we set ρ_i as 0 or 1 randomly during the minutiae direction assignment, i.e., we add π randomly for each minutiae direction in such a coding strategy. We need to perform a modulo operation for the minutiae directions during the fingerprint matching, so as to remove such randomness. Therefore, we will not be able to match the corresponding combined fingerprint by using a general fingerprint matching algorithm. While the purpose of generating a combined fingerprint is to issue a new virtual identity for two different fingerprints, which should be matched using general fingerprint matching algorithms.

Among the existing fingerprint reconstruction approaches, our previous work [15] achieves excellent performance. We here adopt this approach for generating a combined fingerprint from a combined minutiae template. However, the work in [15] does not incorporate a noising and rendering step to make the reconstructed fingerprint image real-look alike. To create a real-look alike fingerprint image

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

from a set of minutiae points, we further apply a noising and rendering step after adopting the work in [15], where the following 7 stages are carried through as illustrated in Fig. 4.

1) Estimate an orientation field O from the set of minutiae points by adopting the orientation reconstruction algorithm

2) Generate a binary ridge pattern based on O and a predefined fingerprint ridge frequency (which is set as 0.12) using Gabor filtering.

3) Estimate the phase image φ of the binary ridge pattern using the fingerprint FM-AM model [14].

4) Reconstruct the continuous phase image φ_c by removing the spirals in the phase image φ.

5) Combine the continuous phase image φ_c and the spiral phase image φ_s (calculated from the minutiae points), producing a reconstructed phase image φ_f .

6) Refine the reconstructed phase image φ_f by removing the spurious minutiae points to produce a refined phase image φ_{fr}.

7) Apply a noising and rendering step on φ_{fr} , so as to create a real-look alike fingerprint image.

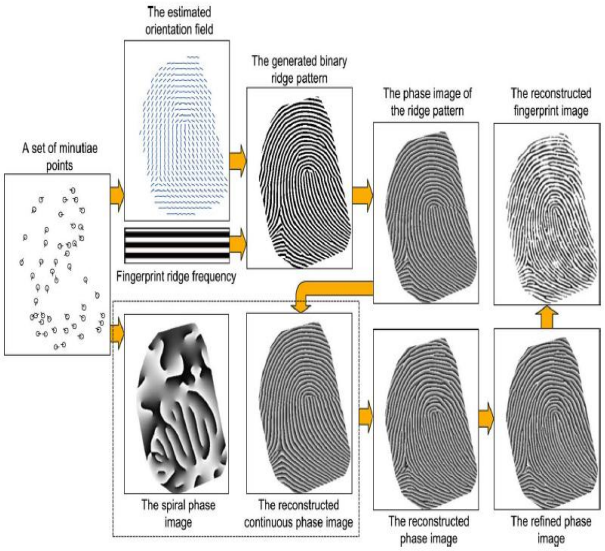

Fig. 4. Reconstructing a real-look alike fingerprint image from a set of minutiae points

EVALUATING THE PERFORMANCE OF THE PROPOSED SYSTEM

In order to evaluate the performance of our system, we randomly pair the 100 fingers in the FVC2002 DB2_A database to produce a group of 50 non overlapped finger pairs, where each finger pair contains two different fingers. The random pairing process is repeated 10 times to have 10 groups of 50 nonoverlapped finger pairs.

For the two fingerprints captured from two different fingers, we can generate two combined minutiae templates in total, where

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

one fingerprint serves as fingerprint A , the other serves as fingerprint B or vice versa. The system designer can choose to enroll one or both of the two templates in the database, which depends on the applications. Thus, we consider the following two cases in building the system database for each group of finger pairs:

1) The first impressions of each finger pair are used to produce only one combined minutiae template for enrollment. Therefore, there are 50 templates stored in the database. To compute the False Rejection Rate (FRR), the second impressions of a finger pair are matched against the corresponding enrolled template, producing 50 genuine tests. To compute the False Acceptance Rate (FAR), the first impressions of a finger pair are matched against the other 49 enrolled templates, producing $50 \times 49 = 2450$ imposter tests.

2) The first impressions of each finger pair are used to produce two combined minutiae templates for enrollment. Thus, there are 100 templates stored in the database. Similarly, 100 genuine tests are performed to compute FRR and $50 \times 49 = 2450$ imposter tests are performed to compute FAR.

In the following discussions, the above two cases are termed as Case I and Case II, respectively.

Fig. 5 plots the average FRR (at different FAR) computed from the 10 groups of finger pairs for the two cases .We can see that our system performs similarly for the two cases. However, the error rates vary among different coding strategies, where the *Coding Strategy* 1 achieves the lowest error rate with $FRR = 0.4\%$ (at $FAR = 0.1\%$) for both cases. While the results of using *Coding Strategy* 3 are the worst, with over 1% FRR (at FAR=0.1%) for both cases.

In order to show the effectiveness of the proposed two two stage fingerprint matching, we evaluate the performance of our system by using a conventional minutiae matching technique [16] for the fingerprint matching. That is to say, during the authentication, we generate a combined minutiae template from two query fingerprints, which is then matched against the corresponding enrolled template by using a conventional minutiae matching algorithm [16]. Under such an assumption, the

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

performance of our system for Case II is shown in Fig. 6. Note that the combined minutiae templates generated using *Coding Strategy* 1 cannot be matched directly using a conventional minutiae matching algorithm because of the randomness in the minutiae direction.

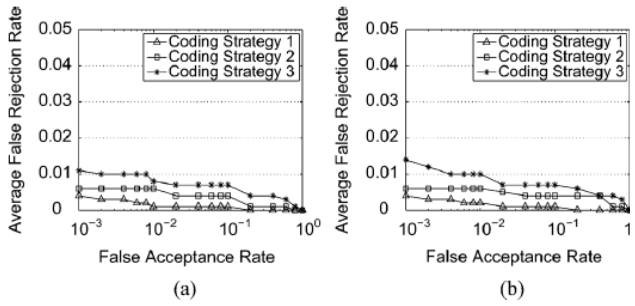

Fig. 5. Performance of the proposed system for (a) Case I, and (b) Case II

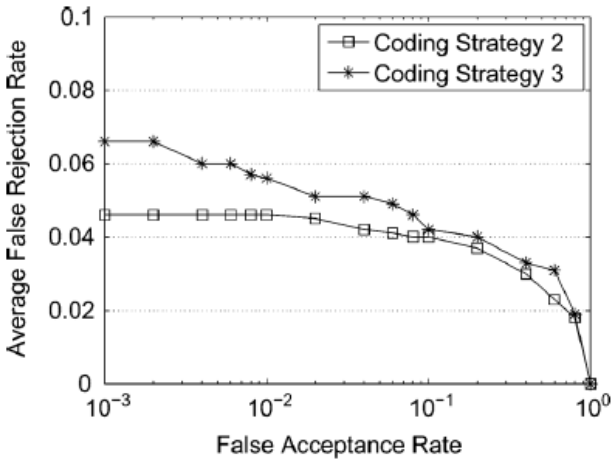

Fig. 6. Performance of the proposed system for Case II by using a conventional minutiae matching technique [16] for the fingerprint matching

It can be seen that the error rates significantly increase. Compared with the results shown in Fig. 5(b), there are 4.0% and 5.2% increase in FRR at for *Coding Strategy* 2 and 3, respectively.

CONCLUSIONS

In this paper, we introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints will be generated and stored in a database. To make the combined minutiae template look real as an original minutiae template, three different coding strategies are introduced during the combined minutiae template generation process. In the authentication process, two query fingerprints from the same two fingers are required. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Our combined minutiae template has a similar topology to an original minutiae template. Therefore, we are able to combine two different fingerprints into a new virtual identity by reconstructing a real-look

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

alike combined fingerprint from the combined minutiae template. The experimental results show that our system achieves a very low error rate with FRR = 0.4% at FAR = 0.1% . It is also difficult for an attacker to break other traditional systems by using the combined minutiae templates. Compared with the state-of-the-art technique, our technique can generate a better new virtual identity (i.e., the combined fingerprint) when the two different fingerprints are randomly chosen. The analysis shows that it is not easy for the attacker to recover the original minutiae templates from a combined minutiae template or a combined fingerprint.

In the existing method we have a major problem of low classification accuracy which leads to poorer combined fingerprint generation. Here we resolve the classification problem by improving the classification accuracy by the method of logistic regression based on decision tree classifier.

REFERENCES

[1] S. Li and A. C. Kot, "A novel system for fingerprint privacy protection,"in *Proc. 7th Int. Conf. Inform. Assurance and Security (IAS)*, Dec. 5–8, 2011, pp. 262–266.

[2] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and enised random number,"*Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, 2004.

[3] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You,"An analysis of biohashing and its variants," *Pattern Recognit.*, vol. 39, no. 7, pp. 1359–1368, 2006.

[4] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–72, Apr. 2007.

[5] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: A security analysis," in *Proc. SPIE, Electron. Imaging, Media Forensics and Security*, San Jose, Jan. 2010.

[6] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint- based fuzzy vault: Implementation and performance,"*IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 744– 757, Dec. 2007.

[7] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and Biometric encryption," in *Proc. Biometrics Symp.*, Sep. 2007, pp. 34–39.

[8] S. Li and A. C. Kot, "Privacy protection of fingerprint database," *IEEE Signal Process. Lett.*, vol. 18, no. 2, pp.115–118, Feb. 2011.

ISSN 2321-743X
International Journal of Research in
Engineering and Bioscience
Volume 2 (Issue 4) Pages (136-147)
IJREB
Journal home page: www.ijreb.org

[9] A. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 70–81,Mar. 2011.

[10] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in *Proc. ICPR- BCTP Workshop*, Cambridge, U.K., Aug. 2004.

[11] A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," in *Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO)*, Barcelona, Spain, Aug. 29–Sep.2, 2011.

[12] A. Othman and A. Ross, "Mixing fingerprints for generating virtual identities," in *Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS)*, Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

[13] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multi-biometric templates using fingerprint and voice," *Proc. SPIE*, vol. 69440I, pp. 69440I-1–69440I-9, 2008.

[14] K. G. Larkin and P. A. Fletcher, "A coherent framework for fingerprint analysis: Are fingerprints holograms?," *Opt. Express*, vol. 15, pp. 8667–8677, 2007.

[15] S. Li and A. C. Kot, "Attack using reconstructed fingerprint," in *Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS)*, Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

[16]VeriFinger 6.3. [Online]. Available http://www.neurotechnology.com