Fingerprint Combinations for Privacy Protection: A Performance Analysis

Aafa J S
Dept of CSE
SCT College of Engineering
Papanamcode
Trivandrum, Kerala

Soja Salim
Dept of CSE
SCT College of Engineering
Papanamcode
Trivandrum, Kerala

ABSTRACT
Protecting the privacy of the fingerprint in authentication systems is become a major issue now-a-days because of the widespread use of fingerprint recognition systems. Traditional encryption and transformation techniques are shown to be more vulnerable to attacks. Therefore, fingerprint combination at the image and feature level has been proposed. This paper introduces two approaches for protecting fingerprint privacy by combining two different fingerprints into a new identity. This paper compares two systems that were introduced to protect the privacy of fingerprint. First is a novel system for fingerprint privacy protection by mixing features of two different fingerprints and thus generate a new identity. During enrolment, the system captures left and right thumb impression from a user. The new identity contains minutiae points of right thumb and has an orientation of left thumb impression. Second is a technique that combines minutiae features of two different fingerprints of a user. The minutiae points of each fingerprints is protected in the new identity. In addition minutiae filtering is done in order to remove spurious minutiae for improving the performance of both the systems. Finally the performance of each technique in terms of FRR, ERR and FAR is compared. For evaluating the performance of two techniques, this work uses same algorithms for the pre-processing and post-processing of fingerprint image.

Keywords
Privacy, Combinatione, Fingerprint, Protection, Minutiae, Orientation

1. INTRODUCTION
For the past few years, fingerprint techniques are used widely in authentication systems. Unlike other authentication techniques that uses passwords, tokens, and smartcards, fingerprint authentication recognition systems doesn't require memorization of their passwords or tokens. Moreover, passwords can be stolen or may get forgotten. Each person has unique features in their fingerprint such as minutiae points, orientation, ridge count etc. Since the physiological traits are unique to each individual, it can prevent theft or fraud. But at sometimes, the stored features can be used by an attacker to construct a fake fingerprint that can be used to enrol into a particular system. Once the template gets compromised, user can't issue a new one. Therefore, protecting the privacy of fingerprint template is very crucial.

Although fingerprint authentication systems have numerous advantages when compared to traditional password systems, it is vulnerable to attacks that may affect the security of the system. The work in [1] addresses these attacks and categorised into eight classes. Type 1 defines the situation of presenting a fake fingerprint to the scanner. Type 2 is the replay attack in which a previously intercepted fingerprint data is submitted to the system. Compromising the feature module to generate the feature values is the third type of attack. In the fourth type of attack the imposter may replace the genuine values with some other values. Matcher module can be altered in order to output a high matching score and this is the fifth type of attack. Sixth type of attack defines the attack on template database and may include replacing a template, modifying a template, adding a new one or deleting an existing one. Alteration of the transmitted template from the database to the matcher module is the seventh type of attack. Finally, overriding the matcher result (accept or reject) by an attacker is the eighth type. The work in [2] addresses the issues related to biometric systems when compared with traditional security systems. Since we leave our thumb impression on the surfaces we touch, it has a lack of secrecy. Non-replaceability is another issue since once the template is compromised we can't replace it with another one like passwords or key. The work in [3] proposed an attack system for the minutiae based fingerprint recognition system.

Several techniques have been introduced for providing security to fingerprint recognition systems. Applying cryptographic techniques doesn't guarantee a high level of security because before matching decryption is required which exposes the fingerprint to the imposter. So significant methods were proposed in order to develop specific protection techniques for fingerprint.

This work compares two systems that were introduced to protect the privacy of fingerprint. First is a novel system for fingerprint privacy protection by mixing features of two different fingerprints and thus generate a new identity. During enrolment, the system captures left and right thumb impression from a user. The new identity contains minutiae points of right thumb and has an orientation of left thumb impression. Second is a technique that combines minutiae features of two different fingerprints of a user. The minutiae points of each fingerprints is protected in the new identity. For improving the performance and accuracy of the system, minutiae filtering is done. Finally the performance each technique in terms of FRR, ERR and FAR is compared. For evaluating the performance of two techniques, this work uses same algorithms for the pre-processing and post-processing of fingerprint image.

The organization of the paper is as follows. Section II covers some of the existing techniques for protecting the privacy of fingerprint. The techniques are outlined in Section III. Section IV covers the experimental results of the work and followed by conclusion.

2. RELATED WORKS

A number of techniques have been developed to improve the privacy and security of fingerprint templates. There are hardware based and software based solutions. At the very beginning keys were used to protect the privacy of fingerprint information [4]. Biometric cryptosystems is a new technique which combines biometrics and cryptography [5], and is popularly known as crypto-biometric systems. The system is also called helper data-based system. Biometric cryptosystems are classified into two classes based on how helper data is generated: key binding schemes and key generating schemes. In key binding schemes, the key or helper data is obtained by binding a chosen key to the biometric template. At authentication, keys are generated from the helper data by applying a key retrieval algorithm [6]. Fuzzy commitment scheme [7], fuzzy vault scheme [8], shielding functions [9] are various approaches to this technique. While in key generating schemes, the helper data is obtained only from the biometric template. Keys are generated from the helper data and a given biometric template [10]. Various approaches to this technique are private template scheme [11] and quantization schemes [12].

The technique based on cryptosystem is so inconvenient that the original fingerprint can be reconstructed if the key and protected fingerprint is stolen. Teoh *et al.* [13] proposed a biohashing approach in which the fingerprint features are combined with a pseudo random number before storing into the database. The technique has significant advantages than solely biometric systems in the sense that it has zero equal error rate and it makes a clear separation between genuine and imposter users. Hence the technique allows the elimination of false accept rates without suffering from increased occurrence of false reject rates. The work in [13] introduces a novel two factor authentication approach in which the fingerprint feature is combined with user specified tokenized random number or data to generate a unique compact code for each user. Two processes are carried out discretization and wavelet Fourier–Mellin transform (FMT). Direct mixing of pseudo-random number and biometric data—BioHashing is an extremely efficient mechanism with which to incorporate physical tokens, such as smart card, USB token etc. thereby resulting in two factors (token + biometrics) credentials via tokenised randomisation. Hence, it protects against biometric fabrication without adversarial knowledge of the randomisation or equivalently possession of the corresponding token. Tokenised discretisation also enables straightforward revocation via token replacement, and furthermore, biohashing has significant functional advantages over solely biometrics i.e. zero equal error rate (EER) point and eliminate the occurrence of FAR without overly imperil the FRR performance.

Later biometric key generation algorithm [14] were introduced which uses the concept of key generation. The enrolled fingerprint template is transformed to a key and the key is stored instead of the template. During authentication a key is generated from the input template by using the same function that was used during enrolment. The keys are compared using any matching algorithm. The technique has a poor matching performance thereby increasing the FAR. Ratha *et al.* [15] proposed cancellable biometric transforms which are designed in a way that it should be computationally hard to recover the original biometric data. The technique is also called feature transformation. Two main categories of cancellable templates are non-invertible transforms and biometric salting. In non-invertible transforms, biometric data are obtained by applying a non-invertible function. The advantage of applying this technique is that potential imposters are not able to construct the entire biometric data even if transform is compromised. However, applying non-invertible transforms mostly results in a loss of accuracy. Poor performance is caused by the fact that transformed biometric templates are difficult to align in order to perform a proper comparison and in addition information is reduced. Biometric salting usually denotes transform of biometric templates which are selected to be invertible. Invertible transform of biometric feature vector elements represent an approach to biometric salting even if biometric templates have been extracted in a way that is not feasible to reconstruct the original biometric signal. As a consequence parameters have to be kept secret. If user-specific transforms are applied, the parameters of the transform have to be presented at each authentication. Imposters are able to recover the original template in case the transform parameters are compromised.

There are some schemes that didn't use key to protect the privacy of fingerprint. The works in [16] [17] combine fingerprint features from two different fingerprints into a new identity. Combination can be done either in image level [16] or in feature level [17]. The concept is first introduced in the work [18] where minutiae points from two fingerprints are combined to generate a new identity. This concept is not as efficient since an attacker can guess it is a combined identity because it contains more minutiae points than that of original fingerprint. The work proposed in [19] defines a technique in which minutiae points are combined with artificially generated points from voice. Combination at the feature level [20] combines the continuous and spiral component of two different fingerprints to generate a new identity. The continuous component represents the orientation of the fingerprint image while spiral component represents the minutiae positions of the fingerprint image. The ridge flow of a fingerprint can be represented as a 2-D Amplitude and Frequency Modulated signal. This phase is then decomposed into continuous and spiral component. A remote fingerprint system maintains a small set of preselected auxiliary fingerprints corresponding to multiple fingerprints. During enrolment local machine decomposes the fingerprint into continuous and spiral component. To ensure the privacy of the fingerprint image in the local system, the remote system transmits the fingerprints in the auxiliary set and the local machine searches through the received fingerprints to locate a "compatible" fingerprint based on the continuous component of enrolled fingerprint which is then decomposed into continuous component and mixed with spiral component of enrolled fingerprint. The new mixed template is enrolled in the remote system database. During authentication, when the subject presents a sample of the left index finger, it is decomposed and its continuous component is used to search through the fingerprints in the auxiliary set from the remote fingerprint system to determine the most "compatible" fingerprint. In the local machine, the spiral component of enrolled template is mixed with the continuous component retrieved from the remote machine to generate a mixed fingerprint, which is then compared against the database entry.

3. PRIVACY PROTECTION TECHNIQUES

Two privacy protection techniques are done in this work and finally the performance is compared. For both approaches the basic features such as minutiae, orientation and reference points should be extracted. The enhancement of the

fingerprint image is done using Fourier transform and then after the image is subjected to local adaptive binarization in order to convert the image in gray level to 2-level image. Later orientation and region of interest are extracted using the algorithm explained in [21]. Since thinning of fingerprint image may help to easily extract the minutiae points, skeletonization algorithm based on [22] is done to enhanced fingerprint image. After thinning the image, minutiae points were extracted using the method as explained in [23]. For removing the minutiae points that were produced as a result of noise content or improper placement of finger in the scanner, false minutiae removing process (minutiae filtering) is done.

3.1 Combination using minutiae points

The system accepts two input fingerprints from each user left thumb impression and right thumb impression. Minutiae points from both templates are extracted and centre of mass is aligned by superimposing both set of minutiae points. The new identity obtained is stored in the database [18]. Fig 1 shows the system. During the enrolment phase, the system captures two input fingerprint image from a user.

A new identity is created by concatenating both the minutiae points obtained from two input fingerprint images of same user. The obtained identity is stored in the database. Even if the database is stolen, an imposter can't reconstruct the original fingerprint images very easily. During authentication, the system captures fingerprint images of left thumb and right thumb, say A' and B'. Minutiae points were extracted from A' and B' and superimposed to get a combination of minutiae points. The newly created template is matched against each template that was stored in the database. Alignment based matching algorithm [24] is used to match the fingerprint images. If a matching score exceeds some threshold value, then the user is identified.

3.2 Combination using minutiae points and orientation

The work is explained in [25]. In this approach, the system accepts left and right thumb impression from a user. The orientation of left thumb and minutiae points of right thumb is mixed together to form a new identity. For aligning the minutiae points of right thumb in the new coordinating system, reference points of both the fingerprint images should be computed. Generation of new identity is a two step process: minutiae position alignment and minutiae direction assignment.

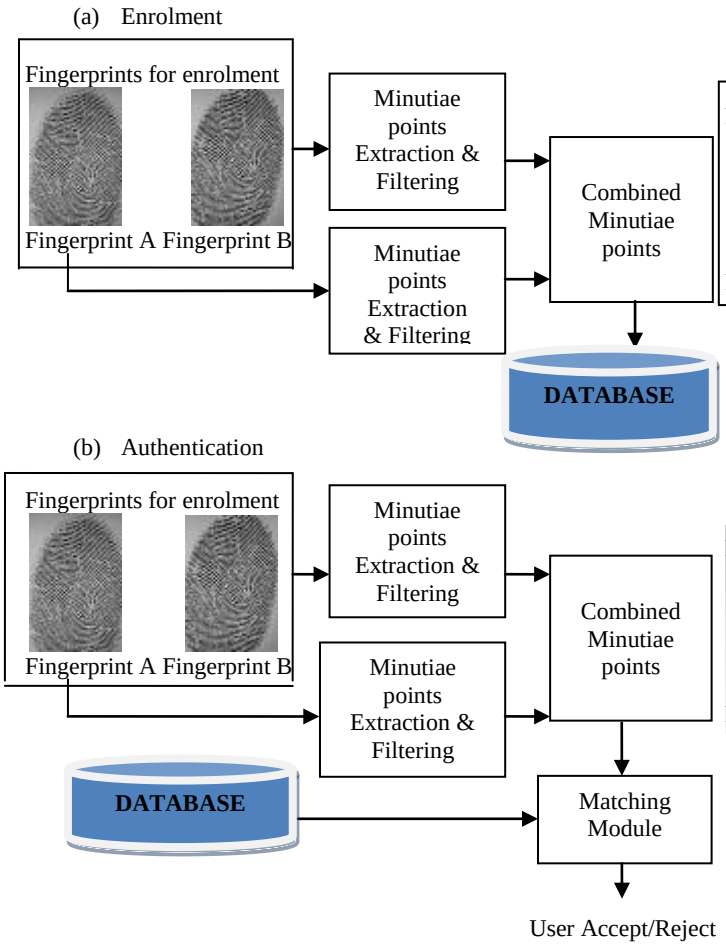

Figure 1. Fingerprint privacy protection system by minutiae combination

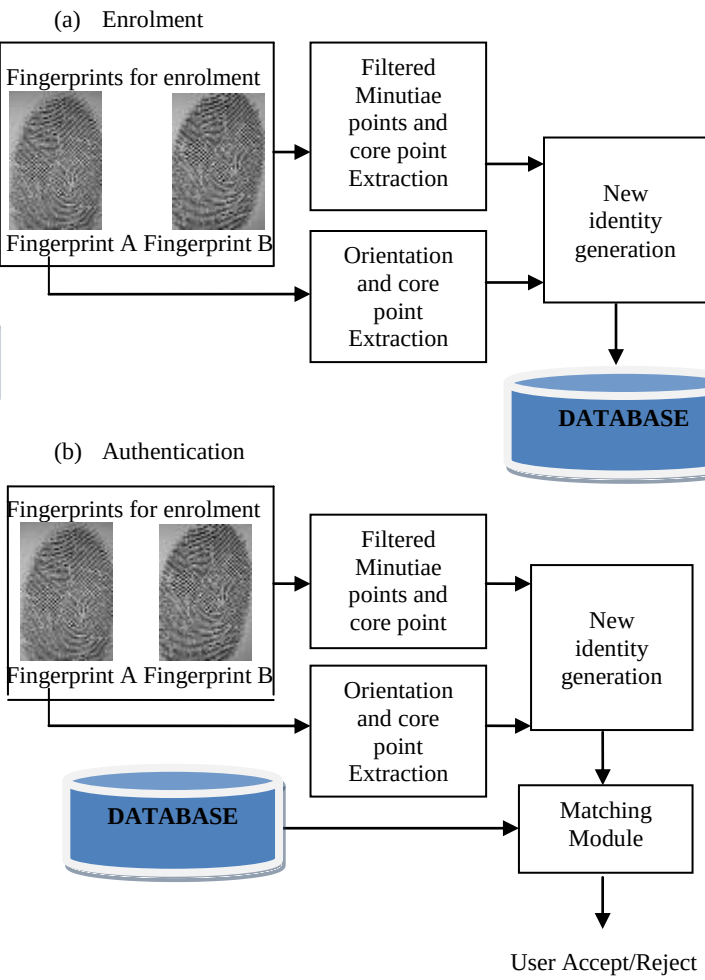

Figure 2. Fingerprint privacy protection system by fingerprint combination

3.2.1 Reference Point Detection

Step1: Compute the cosine and sine of orientation. Let the resulting matrices be a and b.

Step2: Apply gradient operator to both matrices.

Step3: Compute norms of these gradients. Let the resulting matrices be G_a and G_b.

Step4: Compute the global gradient matrix G which has minimum value between G_a and G_b.

Step5: Determine the maximum value of G as V.

Step6: Take all the points that are local maxima whose value is >=0.3V.

Step7: From that list of points, determine the point which is closest to the centre of mass of the region of interest.

3.2.2 Minutiae position alignment

Let R_a and R_b be the reference points of left and right fingerprints respectively. Let it be located at r_a and r_b and have angles a and b respectively. Alignment of minutiae points is done by translating and rotating each point P_{ib} to P_{ic} by

$$P_{ic}{}^T = H.(P_{ib} - r_b)^T + r_a{}^T$$

where H is the rotation matrix defined by

$$H = \begin{bmatrix} cos\,(a-b) & sin\,(a-b) \\ -sin\,(a-b) & cos\,(a-b) \end{bmatrix}$$

3.2.3 Minutiae direction assignment

To each aligned minutiae point a new direction is assigned by

$$\theta_{ic} = O_A(x_{ic}, y_{ic}) + \rho_i \pi$$

where ρ_i is an integer whose value is either 1 or 0 and O_A is the orientation of fingerprint image left thumb.

3.3 Minutiae matching

The work done in [25] uses a two stage matching algorithm for matching the templates. But in this work alignment based fingerprint matching algorithm is used which have two stages alignment stage and matching stage. The algorithm first finds the correspondence between minutiae points and then between the direction of matched points.

3.4 Minutiae Filtering

Due to ridge breaks a lot of false minutiae points may detected during the minutiae extraction process. Original minutiae points plus the false minutiae points may generate a number of minutiae points. Different impressions of same fingerprint thus may generate different set of minutiae points. This may increase the FRR. That is, an authorized user gets not identified. Moreover, amount of information that is going to store becomes higher. The stored template may possess large amount of information in case of minutiae points. So in order to avoid false minutiae points, filtering is done. The minutiae points that formed from ridge breaks are eliminated. The ridge breaks are found by applying threshold approach. If two minutiae points are less than some constant distance apart, then both points represent the points that are generated as a result of ridge break. Such points should be eliminated.

4. EXPERIMENTAL RESULTS

The experiment is performed on the first two impressions of the FVC2002 DB2_A database which contains 200 fingerprints of 100 users with two fingerprints per user. The minutiae points were extracted using the method explained in [23]. The algorithm proposed in [21] is used to extract the orientation of fingerprint image. For the fingerprint matching, alignment based matching algorithm is used [24]. The pre-processing and post-processing steps play a major role in improving the efficiency of both the systems. The binarization techniques usually follow a global thresholding method and which may introduce false non-match results during verification. So it's better to follow the adaptive threshold method. Moreover, removal of H-breaks, spurs and spurious minutiae may improve the matching performance thereby reduce the FRR. For removing the spurious minutiae, the threshold is set to 10. If two minutiae points are less than 10 distance apart, then such points are eliminated.

Initially the fingerprints taken from the database is subjected to both techniques and stores them in different databases. During the verification phase, the input template is matched against each template that is already stored in the database. The matching algorithm is done in a one-to-many manner. Some threshold value is set to identify the user. If the matching score is above that threshold the user is identified.

Three parameters used for fingerprint matching are x, y coordinates of minutiae points and the direction of that point. For effective matching, ridge length is initially matched by computing the similarity factor.

$$Similarity\ factor = \sum_{i=0}^{m} x_i X_i \Big/ [\sum_{i=0}^{m} x_i^2 X_i^2]^{0.5}$$

Then the minutiae points are matched only if the factor is greater than a threshold value. Here the threshold is set to 0.8. The threshold value is set to 0.8 to reduce the FAR rate. Then the minutiae points are matched. If the pair of minutiae to be matched have less than a distance of 10, and there is a small variation in direction then the pair is considered as a minutiae matched pair. The matched pairs are then removed from further processing. The direction variation should be less than $\pi/3$.

Final minutiae matching score is calculated by using the following formula:

$$Matching\ score = 100 * Matching\ ratio$$

where matching ratio is defined as:

$$Matching\ ratio = \frac{Total\ no.of\ matched\ pairs}{no.of\ minutiae\ points\ in\ template}$$

If the score is greater than 80 (pre-specified threshold) the user is identified.

4.1 Performance Evaluation

In order to evaluate the performance of both systems, 20 fingers in the FVC2002 DB2_A database is randomly chosen to produce a group of 10 non overlapped finger pairs, where each finger pair contains two different fingers and each pair is considered to belongs to different users. The random pairing process is repeated 10 times to have 10 groups of 10 non overlapped finger pairs.

For the two fingerprints captured from two different fingers, we can generate two combined minutiae templates in total. The system designer can choose to enroll one or both of the two templates in the database, which depends on the applications. Thus, in building the system database for each group of finger pairs the following cases are considered:

1) The first impression of each finger pair is used to produce only one combined minutiae template for enrolment. Therefore, there are 10 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 10 genuine tests. To compute the False Acceptance Rate (FAR), the first impressions of a finger pair are matched against the other 9 enrolled templates, producing 10*9=90 imposter tests.

2) The first impression of each finger pair is used to produce two combined minutiae templates for enrollment. Thus, there are 20 templates stored in the database. Similarly, 20 genuine tests are performed to compute FRR and imposter tests are performed to compute FAR.

The first technique achieves a FRR of 0.04% for a FAR of 0.1% while the technique 2 achieve a FRR of 3.1% for a FAR of 2% for the same data set. From this analysis we can find that technique 1 gives better performance in terms of FAR and FRR.

Compared with a traditional fingerprint recognition system, both the fingerprint combination methods offers more choices for a single user to do the enrolment and authentication. A traditional system can only enroll 10 fingerprint templates for the ten fingers of a user. While fingerprint combination technique is able to enroll 9*10=90 combined minutiae templates. Among these 90 combined minutiae templates, many may have the same minutiae positions or orientations, which could be easily linked.

Table 1. FRR at varying values of FAR for case 1

FAR	1	0.1	0.01	0.001
FRR of Fingerprint combination	0	0.04	0.13	0.18
FRR of minutiae mixing	0	0.14	0.28	0.32

Table 2. FRR at varying values of FAR for case 2

FAR	1	0.1	0.01	0.001
FRR of Fingerprint combination	0	0.1	0.17	0.19
FRR of minutiae mixing	0	0.21	0.26	1

Moreover, attacks may possible on both systems. For fingerprint combination technique, the attacks cane be defined as:

Type 1 Attack: The combined template can be used to attack the system that stores the corresponding fingerprint B which provides the minutiae positions.

Type 2 Attack: the combined template can be used to attack the system that stores the corresponding fingerprint A which provides the minutiae directions.

For minutiae mixing approach the attack that may be possible is:

Type 1 Attack: The combined minutiae template can be used to enroll into the system that stores either fingerprint A or fingerprint B.

Another attack that is common to both techniques is altering of matcher. The minutiae matcher can be altered in order to give a positive response to a unauthorized template.

At FAR 0.1%, the successful rate of Type 1 Attack for fingerprint combination and minutiae mixing are 25% and 70% respectively. For Type 2 Attack in fingerprint combination the successful rate is almost 0% at FAR 0.1%. The successful rate of third type of attack that is altering of minutiae matcher for fingerprint combination is 0.3% at FAR of 0.1 while for minutiae mixing it is 86%.

5. CONCLUSION

This work compared two novel systems for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrolment, 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. 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. The combined minutiae template has a similar topology to an original minutiae template. Minutiae filtering reduce the unwanted minutiae points. The experimental result shows that fingerprint combination using minutiae and orientation achieves a better ERR with a FRR of 0.04% at FAR 0.1% when compared to minutiae combination technique. Moreover, it is not easy for the attacker to recover the original minutiae templates from a combined minutiae template or a combined fingerprint.

6. REFERENCES

[1] N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", *Proc. AVBPA 2001, Third* International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 223-228, 2001.

[2] B. Schneier, "The uses and abuses of biometrics", *Comm. ACM*, vol. 42, no. 8, pp. 136, Aug. 1999.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems", Proc. of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, vol. 4677, pp. 275-289, 2002.

[4] 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.

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

[6] AK Jain, K Nandakumar, A Nagar, Biometric template security. EURASIP J Adv Signal Process, 1–17 (2008).

[7] A Juels, M Wattenberg, A fuzzy commitment scheme. 6th ACM Conf on Computer and Communications Security, 28–36 (1999).

[8] A Juels, M Sudan, A fuzzy vault scheme. Proc 2002 IEEE Int Symp on Information Theory, 408 (2002).

[9] J-P Linnartz, P Tuyls, New shielding functions to enhance privacy and prevent misuse of biometric templates. Proc 4th Int Conf Audio- And Video-Based Biometric Person Authentication, 393–402 (2003).

[10] AK Jain, K Nandakumar, A Nagar, Biometric template security. EURASIP J Adv Signal Process, 1–17 (2008).

[11] G Davida, Y Frankel, B Matt, On enabling secure applications through off-line biometric identification. Proc of IEEE, Symp on Security and Privacy, 148–157 (1998).

[12] H Feng, CC Wah, Private key generation from on-line handwritten signatures. Inf Manag Comput Secur **10**(18), 159–164 (2002).

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

[14] H Feng, CC Wah, Private key generation from on-line handwritten signatures. Inf Manag Comput Secur **10**(18), 159–164 (2002).

[15] 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.

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

[17] 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.

[18] Berrin Yanikoglu and Alisher KholmatovSabanci University, "Combining Multiple Biometrics to Protect Privacy", in *Proc. ICPR- BCTP Workshop*, Cambridge, U.K.,Aug. 2004.

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

[20] 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.

[21] Y. Wang and J. Hu, "Global ridge orientation modeling for partial fingerprint identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 1, pp. 72–87, Jan. 2011.

[22] Zhao Feng, Xiaou Tang, "Preprocessing and post processing for skeleton-based fingerprint minutiae extraction", Pattern Recognition vol. 40, 2007, pp. 1270-1281.

[23] M. Kaur, M. Singh, P.S. Sandhu, "Fingerprint Verification system using Minutiae Verification Technique", Proceedings of world Academy of Science, Engineering and Technology, vol. 36, 2008.

[24] N. Yager and A. Amin. Fingerprint alignment using a two stage optimization. *PRL*, 27(5):317–324, 2006.

[25] Sheng Li and Alex C. Kot, "Fingerprint Combination for Privacy Protection" IEEE Trans on Info, Forensics and Security, Vol. 8, NO. 2, Feb 2013