Fingerprint Combination for Privacy Protection

Mr. Bharat V Warude, Prof. S.K.Bhatia
ME Student, Assistant Professor
Department of Electronics and Telecommunication
JSPM's ICOER, Wagholi, Pune India

***Abstract* - We propose here a novel system 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.**

***Index Terms* - fingerprint, Combination, minutiae, privacy, protection.**

I. INTRODUCTION

Identification systems rely on three key elements: 1) attribute identifiers (e.g., Social Security Number, driver's license number, and account number), 2) biographical identifiers (e.g., address, profession, education, and marital status), and 3) biometric identifiers (e.g., fingerprint, iris, voice, and gait). It is rather easy for an individual to falsify attribute and biographical identifiers; however, biometric identifiers depend on intrinsic physiological characteristics that are difficult to falsify or alter.

Automated human identification using physiological and/or behavioral characteristics, biometrics, is increasingly mapped to new civilian applications for commercial use. The tremendous growth in the demand for more user-friendly and secured biometrics systems has motivated researchers to explore new biometrics features and traits. The anatomy of human fingers is quite complicated and largely responsible for the individuality of fingerprints and finger veins. The high individuality of fingerprints has been attributed to the random imperfections in the friction ridges and valleys, which are commonly referred to as minutiae or level-2 fingerprint features. Therefore, several live ness countermeasures to detect such sensor-level spoof attacks have been proposed, e.g., finger response to electrical impulse, finger temperature and electrocardiographic signals, time-varying perspiration patterns from fingertips, and a percentage of oxygen-saturated hemoglobin in the blood. Despite the variety of these suggestions, only a few have been found suitable for online fingerprint identification, and these techniques require close contact of respective sensors with the fingers, which makes them unsuitable for unconstrained finger images or when the presented fingers are not in close proximity with the sensors.

As biometrics is gaining popularity, there is increased concern over the loss of privacy and potential misuse of biometric data held in central repositories. The association of Fingerprints with criminal raises further concerns. On the other hand, the alternative suggestion of keeping biometric data in smart cards does not solve the problem, since forgers can always claim that their card is broken to avoid biometric verification altogether. So it is important to generate a better and robust fingerprint privacy protection system.

II THE PROPOSED FINGERPRINT PRIVACY PROTECTION SYSTEM

Fig. 1 shows our proposed fingerprint privacy protection system. In enrollment phase, the system captures two fingerprints from two different fingers, say fingerprints A&B from fingers A and B, respectively. We extract the minutiae positions from fingerprint A and the orientation from fingerprint B using some existing techniques . Then, by using our proposed coding strategies, a combined 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 A_1 and B_1 from fingers A and B. As what we have done in the enrollment, we extract the minutiae positions from fingerprint A_1 and the orientation from fingerprint B_1. Reference points are detected from both query fingerprints. These 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.

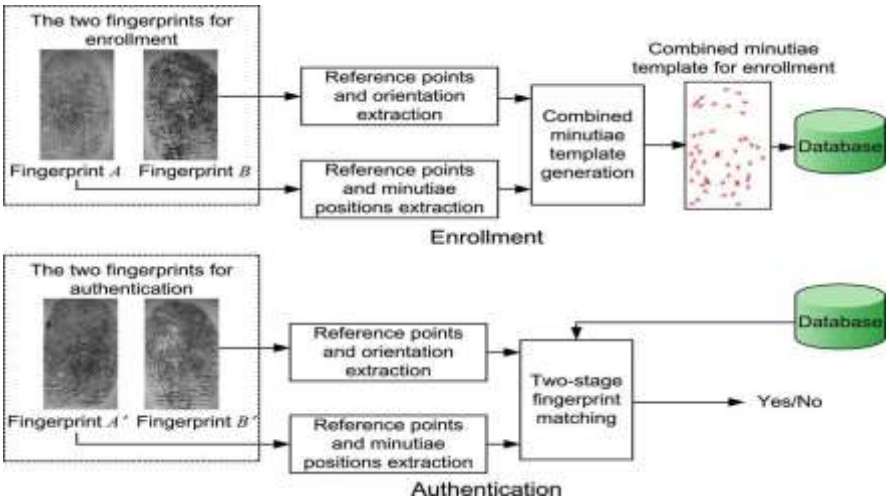

Fig. 1. Proposed fingerprint privacy protection system.

A. Reference Points Detection

The reference points detection process is motivated by Nilsson *et al.* , 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:

Given a fingerprint, the main steps of the reference points detection are summarized as follows:

1) Compute the orientation from the fingerprint. The orientation in complex domain, where

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

2) Calculate a certainty map of reference points

$$C_{ref} = Z * \bar{T}_{ref}$$

Where "*" is the convolution operator and is the conjugate of

$$T_{ref} = (x + iy) \cdot \frac{1}{2\pi\sigma^2} \cdot \exp\left(-\frac{x^2 + y^2}{2\sigma^2}\right)$$

This is the kernel for reference point detection.

2) Calculate the reference points using following equation:

$$C'_{ref} = \begin{cases} C_{ref} \cdot \sin(Arg(C_{ref})) & \text{if } \mathrm{Arg}(C_{ref}) > 0 \\ 0 & \text{otherwise} \end{cases}$$

B. Combined Minutiae Template Generation

Here the combined minutiae template is generated based on the extracted information from the fingerprints and by minutiae position alignment and minutiae direction assignment.

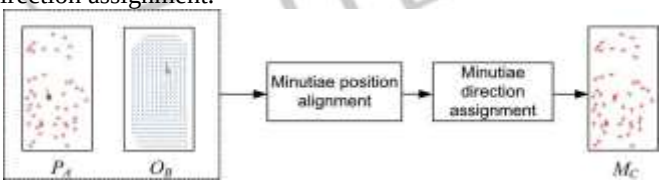

Fig. 2. Combined minutiae template generation process.

Minutiae position alignment

The alignment is performed by translating and rotating each minutiae point. Two primary reference points are overlapped both in the position and the angle after the minutiae position alignment.

Minutiae direction assignment

Here each aligned minutiae position is assigned with a direction. Once all the aligned minutiae positions are assigned with directions, a combined minutiae template is created for enrollment.

C. Two-Stage Fingerprint Matching

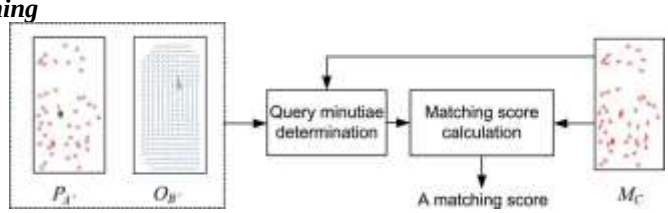

Fig. 3. Two-stage fingerprint matching process.

Given the minutiae positions P_A, of fingerprint A, the orientation O_B, of fingerprint B, and the reference points of the two query fingerprints. In order to match the M_C stored in the database, we propose a two-stage fingerprint matching process including query minutiae determination and matching score calculation as shown in Fig. 3.

1) Query Minutiae Determination:

The query minutiae determination is a very important step during the fingerprint matching. In order to simplify the description of our algorithm, we first introduce the local features extracted for a minutiae point in M_C. The local feature extraction is similar to the work proposed in previous paper. Given a minutiae point $\boldsymbol{m}_{ic}$ and another minutiae point $\boldsymbol{m}_{jc}$ in M_C, we define

1) L_{ij} as the distance between $\boldsymbol{m}_{ic}$ and $\boldsymbol{m}_{jc}$.

$$L_{ij} = \sqrt{(x_{ic} - x_{jc})^2 + (y_{ic} - y_{jc})^2}$$

2) γ_{ij} as the difference between the directions (after modulo π) of $\boldsymbol{m}_{ic}$ and $\boldsymbol{m}_{jc}$

$$\gamma_{ij} = \theta_{ic} \bmod \pi - \theta_{jc} \bmod \pi$$

3) σ_{ij} as a radial angle:

$$\sigma_{ij} = \Re(\theta_{ic} \bmod \pi, \operatorname{atan2}(y_{jc} - y_{ic}, x_{jc} - x_{ic}))$$

Where $\operatorname{atan2}(y, x)$ is a two-argument arctangent function in the range $(-\pi, \pi]$ and

$$\Re(\mu_1, \mu_2) = \begin{cases} \mu_1 - \mu_2 & \text{if } -\pi < \mu_1 - \mu_2 \le \pi \\ \mu_1 - \mu_2 + 2\pi & \text{if } \mu_1 - \mu_2 \le -\pi \\ \mu_2 - \mu_1 + 2\pi & \text{if } \mu_1 - \mu_2 > \pi. \end{cases}$$

For the i^{th} minutiae point $\boldsymbol{m}_{ic}$ in M_C, we extract a set of local features $\boldsymbol{F}_i$ as follows:

$$\mathbf{F}_i = (L_{ij}, L_{ik}, L_{il}, \gamma_{ij}, \gamma_{ik}, \gamma_{il}, \sigma_{ij}, \sigma_{ik}, \sigma_{il})$$

Where we assume $\boldsymbol{m}_{jc}$ is the nearest, $\boldsymbol{m}_{kc}$ is the second nearest and $\boldsymbol{m}_{lc}$ is the third nearest minutiae point of $\boldsymbol{m}_{ic}$.
Suppose we detect $k_1\,(k_1 \geq 1)$ reference points from fingerprint A' and $k_2 (k_2 \geq 1)$ reference points from fingerprint B'. The query minutiae is determined as follows:

1) Select a pair of reference points: one from fingerprint A' (say $R_{a'}$) and the other from fingerprint B' (say$R_{b'}$). Assume $R_{a'}$ is located at $\boldsymbol{r}_{a'} = (\boldsymbol{r}_{xa'}, \boldsymbol{r}_{ya'})$ with the angle $\beta_{a'}$, $R_{b'}$ is located at $\boldsymbol{r}_{b'} = (\boldsymbol{r}_{xb'}, \boldsymbol{r}_{yb'})$ with the angle $\beta_{b'}$, respectively.

2) Perturb $\beta_{a'}$ by $\tau = \beta_{a'} + k.\Delta$, where k is an integer and Δ is a perturbation size. We choose $\Delta = 3 \times \pi/180$ radians (i.e., 3 degrees) and $-5 \leq k \geq 5$. Thus, we have $k = 11$ perturbed angles for the reference point $R_{a'}$.
3) Generate a combined minutiae template $M_{C'}(\tau)$ for testing (hereinafter simply termed as a testing minutiae) from $P_{a'}, O_{b'}, R_{a'}$, (with a perturbed angle τ) and using the proposed combined minutiae template generation algorithm. Note that the same coding strategy should be adopted for generating $M_{C'}(\tau)$ and M_C . In total, we generate K testing minutiae $M_{C'}(\tau)$.

4) Suppose $\boldsymbol{F}_u$ are the local features extracted for the u^{th} minutiae point in $M_{C'}(\tau)$, while are the local features extracted for the v^{th} minutiae point in M_C. Calculate the difference between $\boldsymbol{F}_u$ and $\boldsymbol{F}_v$ by

$$D_\tau(u,v) = w_1 \cdot \sum_{j=1}^{3} |\mathbf{F}_u(j) - \mathbf{F}_v(j)| + w_2 \cdot \sum_{j=4}^{9} |\mathbf{F}_u(j) - \mathbf{F}_v(j)|$$

Where $\boldsymbol{F}_{ij}$ refers to the j^{th} component of $\boldsymbol{F}_i$, ω_1 and ω_2 are the weights for different features. We follow the same weight settings as in existing, where ω_1 and ω_2 are empirically set as $\omega_1 = 1$ and $\omega_2 = 0.3 \times \pi/180$. Then, we define the difference between $M_{C'}(\tau)$ and M_C as

$$d_\tau = \min_{u,v} D_\tau(u,v).$$

5) Repeat steps 1) to 4) until all the possible pairs (in total pairs) of reference points are selected and processed. Among all the testing minutiae ($K \times k_1 \times k_2$ in total), the one which has the minimum difference from M_C (i.e., the minimum d_τ) will be considered as the query minutiae

B. Matching Score Calculation: For the combined minutiae templates that are generated using *Coding Strategy* 1, we do a modulo π for all the minutiae directions in $M_{C'}$ and M_C, so as to remove the randomness. After the modulo operation, we

use an existing minutiae matching algorithm to calculate a matching score between M_Q and M_G for the authentication decision. For other combined minutiae templates, we directly calculate a matching score between M_Q and M_G using an existing minutiae matching algorithm

III. COMBINED FINGERPRINT GENERATION

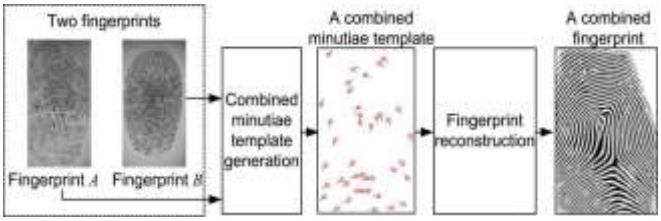

Fig. 5. Generating a combined fingerprint for two different fingerprints.

In a combined minutiae template, the minutiae positions and directions (after modulo π) are extracted from two different fingerprints separately. These minutiae positions and directions share a similar topology to those from an original fi ngerprint. 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 .

IV. EXPERIMENTAL RESULTS

The experiment is conducted on the first two impressions of the database, which contains 200 fingerprints from 100 fingers (with 2 impressions per finger). The VeriFinger is used for the minutiae positions extraction and the minutiae matching. The algorithm is used for the orientation extraction.

The reference points detection has a significant impact on the accuracy and efficiency of our proposed system.

In order to evaluate the performance of our system, we randomly pair the 100 fingers in the 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 non overlapped finger pairs.

For the two fingerprints captured from two different fingers, we can generate two combined minutiae templates in total, where 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 pro-duce 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 cor-responding 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 $50\times49=2450$ imposter tests.

Fingerprint *A* Fingerprint *B*

1) 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 $100\times99=9900$ imposter tests are performed to compute FAR.

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 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 . Under such an assumption, the performance of our system is shown in Fig. 6. Note that the combined minutiae templates generated using *Coding Strategy* can not be matched directly using a conventional minutiae. After that we get a reconstructed image which is shown in fig7

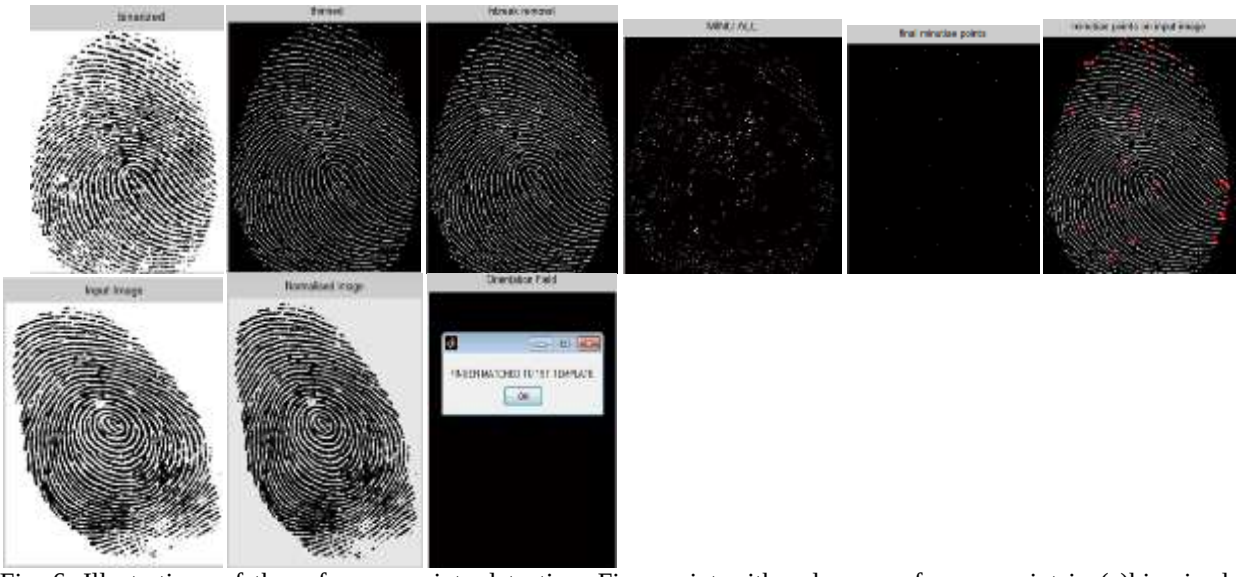

Fig. 6. Illustrations of the reference points detection. Fingerprint with only one reference point in (a)binarized (b)thinned (c) Hbreak Removal (d)All Minutiae position.(e) Final minutiae points(f) Minutiae points on input image(g)Input image(h)Normalised image (i) Actual result

Fig7 Reconstructed image

V. CONCLUSION

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 alike combined fingerprint from the
combined minutiae template. The experimental results show that our system achieves a very low error rate.

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,
[2] 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.
[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,
[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. 744–57, 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.

[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. 2
[11] 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.
[12] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multi-biometric templates using fingerprint and voice," *Proc. SPIE*, vol. 69440I, pp. 69440I-1–69440I-9, 2008.
[13] K. G. Larkin and P. A. Fletcher, "A coherent framework for fingerprint analysis: Are fingerprints holograms?," *Opt. Express*, vol. 15, pp. 8667–8677,
[14] L. Hong, Y. F. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, no. 8, pp. 777–789, Aug. 1998. [18] K. Nilsson and J. Bigun, "Localization of corresponding points in fingerprints
by complex filtering," *Pattern Recognit. Lett.*, vol. 24, no. 13, pp. 2135–2144,.
[15] S. Chikkerur and N. Ratha, "Impact of singular point detection on fingerprint matching performance," in *Proc. Fourth IEEE Workshop on Automat. Identification Advanced Technologies*, Oct. 2005, pp. 207–212.
[16] 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.
[17] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.
[18] J. Feng and A. K. Jain, "Fingerprint reconstruction: From minutiae to phase," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 2, pp. 209–223,
[19] U. Ulugdag, "Secure Biometric Systems," Ph.D. thesis,Michigan State Univ., East Lansing, MI, 2006.