International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

Generation of Combined Minutiae Template for Enrollment and Fingerprint Authentication

Dr.G.S.ANANDHA MALA
Professor & Head
Dept. of CSE,
St. Joseph's College of Engineering,
Chennai-6001119.
gs.anandhamala@gmail.com

CEJIA CEBY (M.E)
Student, Computer Science,
Dept. of CSE,
St. Joseph's College of Engineering,
Chennai-6001119.
scorpio930@yahoo.com

***Abstract*— A new novel system is proposed for fingerprint recognition by the combination of three significant stages: Preprocessing, Post-processing and Matching stage that improves accuracy by overcoming the existing challenges. In this system, for protecting fingerprint privacy two different fingerprints are combining into a new identity. For fingerprint image alignment purpose Minutiae position Alignment, Minutiae Direction Assignment is used. In the enrollment, two fingerprints are captured from two different fingers, and then extract the minutiae positions from one fingerprint, the orientation from the other fingerprint and the reference points from both fingerprints. Curvelet transformation tool is used for the extraction of feature set from the image in different scale and orientation. 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. The fingerprint reconstruction approach converts 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. The statistical experiments show that this system can achieve a very low error rate. This work has the advantage in creating a better new virtual identity when the two different fingerprints are randomly chosen.**

***Index Terms*—Combination, fingerprint, 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 liveness 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.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

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. 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.

In this paper, we propose a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity.

During the enrollment, the system captures two fingerprints from two different fingers. We propose a combined minutiae template generation algorithm to create a combined minutiae template from the two fingerprints. In such a template, the minutiae positions are extracted from one fingerprint, while the minutiae directions depend on the orientation of the other fingerprint and some coding strategies. The template will be stored in a database for the authentication which requires two query fingerprints. A two-stage fingerprint matching process is further proposed for matching the two query fingerprints against a combined minutiae template. By using the combined minutiae template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen. In addition, the combined minutiae template share a similar topology to the original minutiae templates, it can be converted into a real-look alike combined fingerprint by using an existing fingerprint reconstruction approach. The combined fingerprint issues a new virtual identity for two different fingerprints, which can be matched using minutiae based fingerprint matching algorithms.

The advantages of our technique over the existing fingerprint combination techniques are as follows:

1) Our proposed system is able to achieve a very low error rate with FRR = 0.4 % when FAR = 0.1%.

2) Compared with the feature level based technique, we are able to create a new identity (i.e., the combined minutiae template) which is difficult to be distinguished from the original minutiae templates.

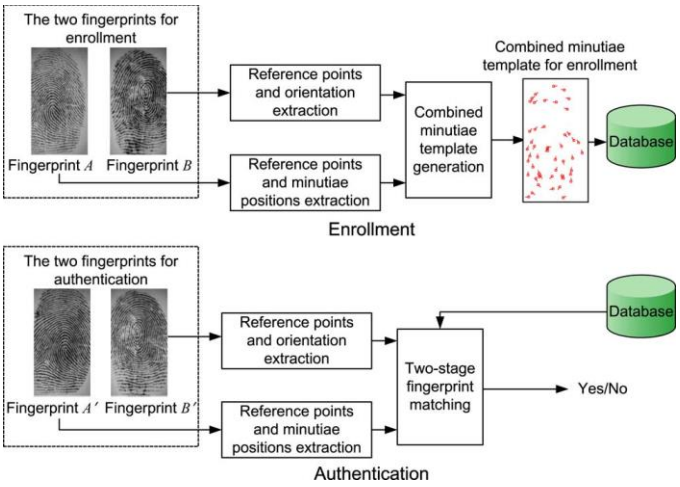
3) Compared with the image level based technique, we are able to create a new virtual identity (i.e., the combined fingerprint) which performs better when the two different fingerprints are randomly chosen.

The organization of the paper is as follows. Section II introduces our proposed fingerprint privacy protection system. Section III explains how to generate a combined fingerprint for two different fingerprints. Section IV presents the experimental results. Section V analyzes the information leakage in a combined minutiae template, followed by the conclusions in the last section.

II. The 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 A and 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’ and B’ from fingers A and B. As what we have done in the enrollment, we extract the minutiae positions from fingerprint A’ and the orientation from fingerprint B’. 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.



International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

Fig. 1. Proposed fingerprint privacy protection system.

A. RGB TO GRAY CONVERSION

Take the input image. And it converts into grayscale image.

RGB IMAGES

An RGB image represents each pixel color as a set of three values, representing the red, green, and blue intensities that make up the color. In MATLAB, the red, green, and blue components of an RGB image reside in a single m-by-n-by-3 array. m and n are the numbers of rows and columns of pixels in the image, and the third dimension consists of three planes, containing red, green, and blue intensity values. For each pixel in the image, the red, green, and blue elements combine to create the pixel's actual color.

An RGB array can be of

- Class double, in which case it contains values in the range [0, 1].
- Class uint8, in which case the data range is [0,255].
- Class uint16, in which case the data range is [0, 65535].

GRAYSCALE IMAGES

Contain only brightness information. No color information. Typically contain 8 bits/pixel data, which corresponds to 256 (0 to 255) different brightness (gray) levels

- Useful when a small section of the image is enlarged.
- Allows the user to repeatedly zoom a specific area in the image.

Fig.2.RGB to gray scale conversion.

B. NORMALIZATION

In image processing, normalization is a process that changes the range of pixel intensity values. Applications include photographs with poor contrast due to glare, for example. Normalization is sometimes called contrast stretching. In more general fields of data processing, such as digital signal processing, it is referred to as dynamic range expansion.

The purpose of dynamic range expansion in the various applications is usually to bring the image, or other type of signal, into a range that is more familiar or normal to the senses, hence the term normalization. Often, the motivation is to achieve consistency in dynamic range for a set of data, signals, or images to avoid mental distraction or fatigue.

Let, I(i, j) denote the gray-level value at pixel (i, j), M and VAR denote the estimated mean and variance of I, respectively, and G(i, j) denote the normalized gray-level value at pixel (i, j). The normalized image is defined as follows:

$$G(i,j) = \begin{cases} M_0 + \sqrt{\frac{VAR_0 (I(i,j)-M)^2}{VAR}} & \text{if } I(i,j) > M \\ M_0 - \sqrt{\frac{VAR_0 (I(i,j)-M)^2}{VAR}} & \text{otherwise} \end{cases}$$

Where, M_0 and VAR_0 are the desired mean and variance values, respectively. Normalization is a pixel-wise operation. It does not change the clarity of the ridge and valley structures. The main purpose of normalization is to reduce the variations in gray-level values along ridges and valleys, which facilitates the subsequent processing steps.

C. FINGERPRINT BASICS

Fingerprints are known to be unique to every individual. We can extract minutiae and orientation from a fingerprint.

- *MINUTIAE*

A Minutia is defined as the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings.

Types of ridges:

- ridge endings - a ridge that ends abruptly
- ridge bifurcation - a single ridge that divides into two ridges

Short ridges, island or independent ridge - a ridge that commences, travels a short distance and then ends

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

- ridge enclosures - a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge
- spur - a bifurcation with a short ridge branching off a longer ridge
- crossover or bridge - a short ridge that runs between two parallel ridges

Fig.3. Minutiae Positions in Fingerprint

- ORIENTATION

An orientation image is defined as an N x N image, where
O(i, j) represents the local ridge orientation at pixel (i, j). Local ridge orientation is usually specified for a block rather than at every pixel; an image is divided into a set of w x w non-overlapping blocks and a single local ridge orientation is defined for each block. Note that in a fingerprint image, there is no difference between a local ridge orientation of 90^o and 270^o, since the ridges oriented at 90^o and the ridges oriented at 270^o in a local neighborhood cannot be differentiated from each other.

Given a normalized image, G, the main steps of the algorithm are as follows:
1) Divide G into blocks of size w x w (16 x 16).
2) Compute the gradients at each pixel, (i, j). The gradient operator Sobel is used.
3) Estimate the local orientation of each block centered at pixel (i, j) using the following equations:

$$\mathcal{V}_x(i,j) = \sum_{u=I-\frac{w}{2}}^{I+\frac{w}{2}} \sum_{v=J-\frac{w}{2}}^{J+\frac{w}{2}} 2\partial_x(u,v)\partial_y(u,v),$$

$$\mathcal{V}_y(i,j) = \sum_{u=I-\frac{w}{2}}^{I+\frac{w}{2}} \sum_{v=J-\frac{w}{2}}^{J+\frac{w}{2}} \left(\partial_x^2(u,v)\partial_y^2(u,v)\right),$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{\mathcal{V}_y(i,j)}{\mathcal{V}_x(i,j)}\right),$$

Where $\theta(i, j)$ is the least square estimate of the local ridge orientation at the block centered at pixel (i, j). Mathematically, it represents the direction that is orthogonal to the dominant direction of the Fourier spectrum of the w x w window.
4) Due to the presence of noise, corrupted ridge and valley structures, minutiae, etc. in the input image, the estimated local ridge orientation, $\theta(i, j)$ may not always be correct. Since local ridge orientation varies slowly in a local neighborhood where no singular points appear, a low-pass filter can be used to modify the incorrect local ridge orientation. In order to perform the low-pass filtering, the orientation image needs to be converted into a continuous vector field, which is defined as follows:

$$\Phi_x(i,j) = \cos(2\theta(i,j)),$$

$$\Phi_y(i,j) = \sin(2\theta(i,j)),$$

Where Φ_x and Φ_y are the x and y components of the vector field, respectively. With the resulting vector field, the low-pass filtering can then be performed.

5) Compute the local ridge orientation O at (i, j) using,

$$O(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{\Phi_y(i,j)}{\Phi_x(i,j)}\right)$$

D. 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:

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.

Calculate the reference points using following equation:

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

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

E. COMBINED MINUTIAE TEMPLATE GENERATION ALGORITHM

Given a set of minutiae positionspositions $P_A = \{\boldsymbol{p}_{ia} = (x_{ia,}y_{ia,}), 1 \le i \le N\}$, of fingerprint$A$, the orientation O_B of fingerprint B and the reference points of fingerprints A and B, a combined minutiae template M_C is generated by minutiae position alignment and minutiae direction assignment.

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 R_a and R_b for fingerprints A and B, respectively. Let's assume R_a is located at $\boldsymbol{r}_a = (r_{xa,}r_{ya})$ with the angle β_a, and R_b is located at $\boldsymbol{r}_b = (r_{xb,}r_{yb})$ with the angleβ_b. The alignment is performed by translating and rotating each minutiae point $\boldsymbol{p}_{ia}$ to $\boldsymbol{p}_{ic} = (x_{ic}, y_{ic})$ by,

Where $(\quad)^T$ is the transpose operator and $\mathbf{H}$ is the rotation matrix where,

$$\mathbf{H} = \begin{bmatrix} \cos(\beta_b - \beta_a), \sin(\beta_b - \beta_a) \\ -\sin(\beta_b - \beta_a), \cos(\beta_b - \beta_a) \end{bmatrix}.$$

As such, R_a and R_b are overlapped both in the position and the angle after the minutiae position alignment.

2) Minutiae Direction Assignment:

Each aligned minutiae position is assigned with a direction as follows:

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

Where ρ_i is an integer that is either 0 or 1. The range of $O_B(x_{ic}, y_{ic})$ is from 0 to π . Therefore, the range of θ_{ic} will be from 0 to 2 π, 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 .

$$(\mathbf{p}_{ic})^T = \mathbf{H} \cdot (\mathbf{p}_{ia} - \mathbf{r}_a)^T + (\mathbf{r}_b)^T$$

F. Two-Stage Fingerprint Matching

1) ρ_i is randomly selected from $\{0,1\}$.

2) ρ_i is determined by

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

Where mod is the modulo operator and θ_{ia} is the original direction of a minutiae position $\boldsymbol{p}_{ia}$ in fingerprint A.

3) ρ_i is determined by

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

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

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

Where $\theta_b^k(x_{ic}, y_{ic})$ means the direction of the k^{th} 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.

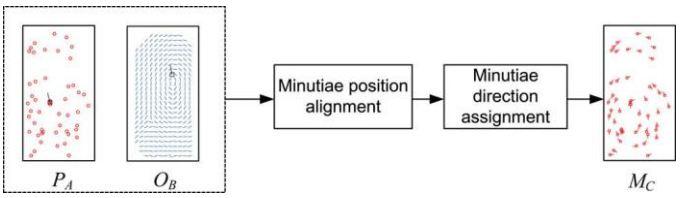


Fig.4. Combined minutiae template generation process.

Given the minutiae positions PA' of fingerprint A', the orientation OB'of fingerprint B' and the reference points of the two query fingerprints. In order to match the MC stored in the database, we
propose a two-stage fingerprint matching process including query minutiae determination and matching score calculation.

1) Query Minutiae Determination: The query minutiae determination is a very important step during the fingerprint

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

matching. In order to simplify the description of our algorithm, we first introduce the local features extracted for a minutiae point in MC.

2)Matching Score Calculation: For the combined minutiae templates that are generated , we do a modulo π for all the minutiae directions in MQ and MC , so as to remove the randomness. After the modulo operation, we use an existing minutiae matching algorithm to calculate a matching score between MQ and MC for the authentication decision. For other combined minutiae templates, we directly calculate a matching score between MQ and MC using an existing minutiae matching algorithm.

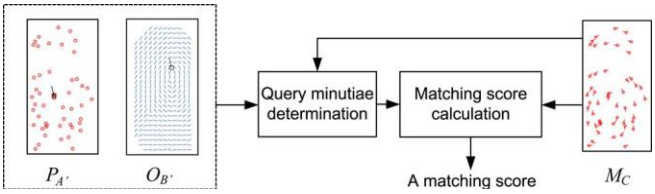


Fig.5. Two-stage fingerprint matching process.

III. Combined Fingerprint Generation

In a combined minutiae template, the minutiae positions
and directions are extracted from two different fingerprints separately. These minutiae 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. 5 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. 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. We here adopt this approach for generating a combined fingerprint from a combined minutiae template. However, the work in 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 from a set of minutiae points, we further apply a noising and rendering step after adopting the work , where the following 7 stages are carried out.

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 of the binary ridge pattern using the fingerprint FM-AM model.
4) Reconstruct the continuous phase image by removing the spirals in the phase image .
5) Combine the continuous phase image and the spiral phase image (calculated from the minutiae points), producing a reconstructed phase image .
6) Refine the reconstructed phase image by removing the spurious minutiae points to produce a refined phase image.
7) Apply a noising and rendering step, so as to create a real-look alike fingerprint image.

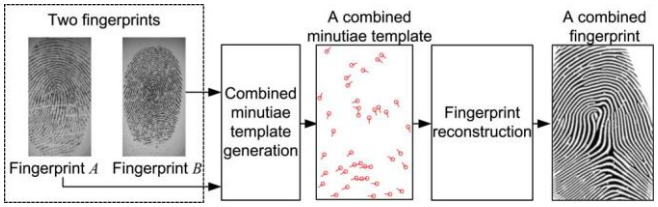


Fig.6. Generating a combined fingerprint for two different fingerprints.

IV. EXPERIMENTAL RESULTS

A 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 proposed is used for the orientation extraction.

TABLE I
Performance of The Reference Points Detection At Different Settings OF Threshold T

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

	T			
	3	4	5	6
No.	1141	650	291	207
True Detection Rate (%)	99.5	99.5	99.5	98.5
False Detection Rate (%)	0.5	0.5	0.5	1.5

Evaluating the Performance of the Proposed System

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 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 × 49 = 2450 imposter tests.

3) 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 × 99 = 9900 imposter tests are performed to compute FAR.

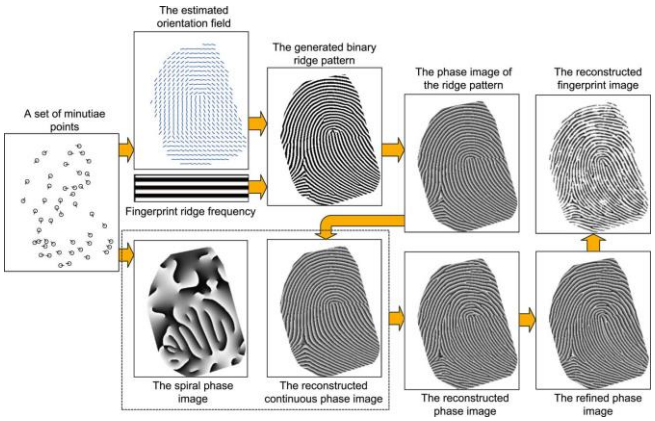


Fig.7. Reconstructing a real-look alike fingerprint image from a set of minutiae points.

Fig.8. Original Image

Fig.9. Normalized Image

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical,Aeronautical,Computer,Civil,Electrical and Electronics Engineering (ICMACE14)

Fig.10. Gradient X

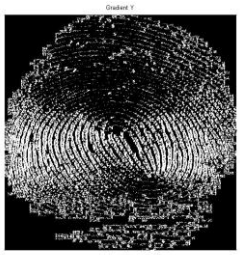


Fig.11.Gradient Y

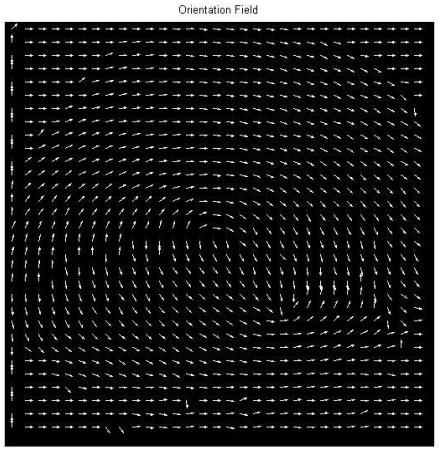


Fig.12. Orientation Field

V. 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 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.

VI. References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

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

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

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

[8] 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.

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

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

[11] 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, 2003.

[12] 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.

[13] 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.

[14] 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.

[15] Sheng Li and Alex C. Kot "An Improved Scheme for Full Fingerprint Reconstruction," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 6, DECEMBER 2012.

[16] Tat Loong Chan & Ling Guan "IMAGE RETRIEVAL," Crux Cybernetics Pty Ltd, GPO Box 464, Sydney, NSW 2001, Australia Ryerson Polytechnic University, Toronto, Ont M5B 2K3, Canada.

[17] K. Nilsson. Symmetry Filters Applied to Fingerprints. PhD thesis, Chalmers University of Technology, Sweden, 2005.