# Fingerprint Combination by Minutiae and Coordination Extraction for Privacy Protection

Devi. P
*Department of Electronics and Communication Engineering*
*Sri Ramakrishna Institute of Technology, Coimbatore, Tamilanadu, India*

Saranya. B
*Department of Electronics and Communication Engineering*
*Sri Ramakrishna Institute of Technology, Coimbatore, Tamilanadu, India*

Malathi. L
*Department of Electronics and Communication Engineering*
*Sri Ramakrishna Institute of Technology, Coimbatore, Tamilanadu, India*

**Abstract- Biometric-based personal verification has increasingly gained popularity due to the importance of security and privacy protection. This approach is for protecting fingerprint confidentiality by merging two different fingerprints into novel identity. Two fingerprints are taken from two diverse fingers in the enrolment. Minutiae positions are isolated from one fingerprint and coordination positions from another fingerprints and reference points from both fingerprints. Different fingerprint recognition system store minutiae based fingerprint templates differently. Here minutiae templates stored in a server database. Based on the isolated information and the proposed strategies, a combined minutiae templates is generated. In the authentication, the system needs two query fingerprints from the identical two fingers which are used in the registration. A two-stage fingerprint matching process is planned for matching the two query fingerprints against a combined minutiae templates. A complete minutiae feature of a particular fingerprint will not be conceded with the database stolen and it is difficult for the attacker to distinguish a original minutiae templates from a combined minutiae templates. The experimental result shows that our proposed scheme achieves better results than the available technique.**

**Keywords – Fingerprint, Combination, Minutiae, Coordination, Privacy Protection.**

## I INTRODUCTION

Nowadays, fingerprints are commonly used in biometric recognition systems. With the wide range applications of fingerprint techniques in authentication system, protecting the privacy of the fingerprint becomes an major issue. For fingerprint privacy protection encryption is not sufficient, since decryption is essential before the fingerprint matching, which depictions the fingerprint to the attacker. The significant efforts have been put into evolving specific safeguard techniques for fingerprint[1-3].

Most of the existing techniques uses the key for the fingerprint privacy safeguard, which creates the inconvenience. It can also be vulnerable if both the key and the secured fingerprint are stolen. Teoh *et al* propose a biohashing approach by computing the inner products among the user's fingerprint features and the key(i.e.,pseudorandom number). In this approach the key is never stolen or shared[2].

Ratha *et al.* propose to generate cancelable fingerprint templates by applying noninvertible transforms on the minutiae. The reduction in matching accuracy is guided by noninvertible transform[4]. The works are shown to be helpless to disturbance and linkage attacks during both the key and the transformed template are stolen. Nandakumar *et al.* propose to implement fuzzy fault logic on the minutiae, it is susceptible to the key-inversion attack. Our work in imperceptibly hide the user individuality on the thinned fingerprint using a key[5,6]. When both the key and the protected thinned fingerprint are stolen, the user identity can be compromised. There are only a few schemes that are without using a key and it is able to protect the confidentiality of the fingerprint.

Ross and Othman proposed to use visual cryptography for protecting the privacy of biometrics. By using a visual cryptography scheme to produce two noise like images (termed as sheets) which are stored in two separate databases, then the fingerprint image is decomposed[9].The two sheets are overlaid to create a temporary fingerprint

image for matching during the authentication. The identity of the biometrics is never exposed to the attacker in a single database. This is the advantage of the system. It requires two separate databases to work together, which is not practical in same application. The work combines the two different fingerprints into a single new identity either in the feature level or in the image level. For combining the two different fingerprints into a new identity is proposed, where the new identity is developed by joining the minutiae positions isolated from the two fingerprints.

The original minutiae locations of each fingerprint can be protected by the new identity. It contains many more minutiae positions than that of an actual fingerprint, so it is easy for the attacker to identify such a new identity. This shows that the BER of matching the new identities is 2.1% when the original minutiae positions are marked manually from the actual fingerprints. A similar structure is proposed where the minutiae positions isolated from a fingerprint and the artificial points produced from the voice are joined to produce a new identity. In this method, the BER are shown to be fewer than 2% conferring to the experimental results. The authors first propose to combine two different fingerprints in the image level and each fingerprint is decomposed into the continuous component and the spiral component based on FM-AM model. After some orientation process, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint to create a new virtual identity which is known as a mixed fingerprint. The image level based fingerprint combination method has two advantages: 1.It is difficult for the attacker to distinguish a mixed fingerprint from the actual fingerprints, and 2. Existing fingerprint matching algorithms are applicable for matching two mixed fingerprints[11,12].

This method is proposed for protecting fingerprint privacy by combining two different fingerprints into a new identity. During the enrolment, the system captures two different fingerprints. This method combines the minutiae template generation algorithm to make a combined minutiae template from two fingerprints. The template will be saved in a database for verification which requires two query fingerprints. The two stage fingerprint matching process is again matching with the two query fingerprints against a combined minutiae templates. When the database is stolen, by using the combined minutiae template, the whole minutiae feature of a fingerprint will not be compromised. The advantages of the proposed methods are:

1. Compared with feature level based technique, we are able to generate a novel identity (i.e., the combined minutiae template) which is difficult to distinguish from original minutiae template.
2. Compared with the image level based technique, we are able to generate a novel virtual identity (i.e., the combined fingerprint) that performs well when two different fingerprints are randomly chosen.

## II THE PROPOSED FINGERPRINT PRIVACY PROTECTION SYSTEM

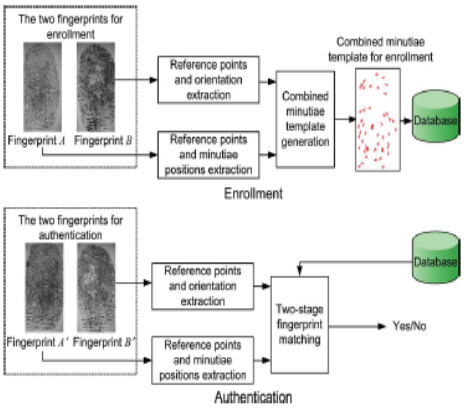


Figure 1. Proposed Fingerprint Privacy Protection System

In the registration phase, the system captures two fingerprints from two different fingers, i.e. fingerprints X and Y from fingers X and Y respectively. We extract the minutiae position from fingerprint X and coordination from fingerprint *Y* using some existing techniques. By using our proposed system, the coding strategies are used to combine the minutiae template which is generated based on minutiae positions. Then the coordination and the reference points are detected from both fingerprints and the combined minutiae template is stored in the database. In the authentication phase, the two query fingerprints are necessary from the same two fingers, i.e. fingerprints X' and Y' from fingers X and Y. In the enrolment, the extracted minutiae position from fingerprint X' and the coordination from fingerprint Y' is done and the reference points are detected from both the query fingerprints. The isolated

information will be matched in contradiction of the corresponding template stored in the database using a two-stage fingerprint matching.

*A.MINUTIAE BASED MATCHING ALGORITHM*

The most popular matching approach for fingerprint identification is usually based on minor level features obtained by singularities in finger ridge pattern called minutiae. The ridge ending and ridge bifurcation features are used.


Figure 2. a) Ridge ending b) Ridge bifurcation

*B.COMPONENTS OF A MINUTIAE FEATURE*

The other high-level features that can be used in reducing the search space during a match. For this purpose the pattern class of a fingerprint is the important feature. Fingerprints are classified into five types; they are arch, tented arch, left loop, right loop, and Whorl.

For noisy fingerprints the pattern class may be ambiguous in partial fingerprints and indeterminate. The another high-level feature is the ridge density in a fingerprint. It is the number of ridges per unit distance. To make this as invariant to position, the ridge density between two singular points in a fingerprint is computed. Singular points of interest are described as the *core* and *delta* points.

Minutiae is described by four parameters

$$m = (p, q, \Theta, t)$$

Where,

p,qy=coordinates of minutiae points
Θ=minutiae direction typically obtained from local ridge coordination
t=type of minutiae point (ridge ending or ridge bifurcation)

## III LINEARIZATION

Linearization is a method of transforming grayscale image pixels into black or white pixels by selecting a threshold. This process can be fulfilled by using the multitude of techniques. Linearization is relatively easy by comparing with other image processing techniques. The binary image is a digital image which has only two possible values for each pixel. Typically the black and white are used for a binary image eventhough any two colors can be used. The color used for the object(s) in the image is the foreground color and the rest of the image is the background color. In the document scanning industry this is frequently referred to as bi-tonal. Binary images are called as bi-level or two-level. This means that each pixel is stored as a bit (0 or 1). The terms black and white, B&W, monochrome or monochromatic are often used for this idea, but may also designate any images that have just one sample per pixel, such as gray scale images. In Photoshop phrasing, the binary image resembles same as "Bitmap" image mode. Binary images often arise in digital image processing such as thresholding, dithering and segmentation. The input/output devices which can handle bi-level images are laser printers, fax machines, and bi-level computer displays.

Figure 3. a) Linearization b) Shrinking

## IV. SHRINKING

The aim of shrinking is to reduce the fingerprint to lines one pixel wide. It is a morphological operation performed in the binary images. From the different sides of each image the successive deletions of pixels are achieved. Each of the four sides are eroded away according to some set template. The image is being dispersed which is no longer than possess any points to match the deletion templates. This remaining image will be the thinned representation of the original image. If the image template matches, the middle pixel is removed. Once all eight matrices have been sampled on the entire image, the process is repeated on the newly formed Image. No more points can be deleted when processing only stops. Four point shrinking algorithms are also available; these algorithms have only one template for each position. The resulting thinned image isn't as refined as the eight matrices algorithms because it places fewer criterions on the image. The result usually possesses more spur points. For this reason, four matrices processing will not be implemented.

## V. STEERING IMAGE

The steering image is usually used to derive the average direction of a minor segment of the image. The image is divided into sub directions and then sorted for greater segmentation. The technique is used on the unprocessed gray scale images. The greater number of respective sub-direction results as darker pixels. A test area 16 pixels wide was selected. The entire image dimension depends on the actual test area and it should comprise at least 1 ridge (dark area) and 1 valley.

Sub-direction = greatest [ $\sum$(pixel_value – average)½ ]

The pixel next to the endpoint directions easily implemented. Endpoint directions and the contrasting the bifurcation direction are unidirectional.

## VI. COORDINATION ESTIMATION

Several methods of coordination estimation have been proposed including matched-filter based approach, high-frequency power method, and the simplest and most frequently adopted gradient-based approach. By using the gradient-based approach with different operators, the coordinations are calculated (Kirsch, Robinson and Prewitt). The comparison of fingerprint is done by two fingerprint images from the same finger. By using biometric techniques, the fingerprint based identification is used in various applications. The unique, immutable fingerprints are notorious. The fingerprint is made of a series of ridges and contracts in the finger. The individuality of a fingerprint is determined by the pattern of ridges, contracts and minutiae points. The Minutiae points are describe the characteristics of local ridge and that occur at either a ridge bifurcation or a ridge ending.

## VII. AUGMENTATION

From the input fingerprint images, the critical step in fingerprint matches automatically and reliably of extract minutiae. The quality of the input fingerprint images depends on the performance of a minutiae extraction algorithm. The quality of the fingerprint images is used to ensure the performance of fingerprint identification or verification system automatic ally, which would be robust. In the minutiae extraction module it would be essential to incorporate a fingerprint augmentation algorithm. The quality of the image is really good and need not to enhance the image.

## VIII. JOINT MINUTIAE TEMPLATE GENERATION

The minutiae positions and directions are isolated from two different fingerprints separately in the combined minutiae template. From the original fingerprint these minutiae positions and directions uses the same method for this. The original minutiae template has the same method as the combined minutiae template.

### *A. Minutiae Locus Alignment:*

The reference point with the maximum certainty value defined among all the reference points of a fingerprint for the enrolment process. Hence two primary reference points $U_a$ and $U_b$ for fingerprints *X and Y,* respectively. Let's assume $U_a$ is located at $u_a = (u_{xa},u_{ya})$ with an angle $\beta_a$ and $U_b$ is located at $u_b=(u_{xb},u_{yb})$ with an angle $\beta_b$. This alignment is done by translating and rotating each minutiae point $v_{ia}$ to $v_{ic} = (x_{ic},y_{ic})$ by

$$(V_{ic})^T = \mathbf{H} \cdot (V_{ia}-u_a)^T + (u_b)^T$$

### *B. Minutiae Direction Assignment:*

Every aligned minutiae position $\mathbf{p}_{ic}$ is assigned with direction $\Theta_{ic}$ is as follows:

$$\Theta_{ic} = O_B(x_{ic},y_{ic}) + ri\pi$$

where ri is an integer that is either 0 or 1. The range of $O_B(x_{ic},y_{ic})$ is from 0 to π and the range of $\Theta_{ic}$ will be from 0 to 2π. It is same as the minutiae directions from an original fingerprint. ri will be defined by,

1) ri is randomly selected from {0,1}.
2) $r_{i\,is}$ determined by

$ri = 1$ if $\text{mod}(\Theta_{ia} + \beta_b - \beta_{a,}\pi) - O_B(x_{ic,}y_{ic}) > 0$

$ri = 0$ otherwise

where mod is the modulo operator and $\Theta_{ia}$ is the actual direction of a minutiae position $\mathbf{p}_{ia}$ in fingerprint X.

3) *ri* is determined by

$ri = 1$ if $\text{mod}(ave_b(x_{ic},y_{ic}),\pi) - O_B(x_{ic,}y_{ic}) > 0$

$ri = 0$ otherwise

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 Y

$$ave_b\,(x_{ic},y_{ic}) = 1/N\ \Sigma N_{k=1}\ \Theta^k_b\,(x_{ic},y_{ic})$$

where $\Theta^k_b(x_{ic},y_{ic})$ means the direction of the $k^{th}$ minutiae point of the location $(x_{ic},y_{ic})$ in fingerprint Y, and n is empirically set as 5 which provides a good balance between the diversity and matching accuracy of the combined minutiae templates.

### *C. Reconstruction:*

When the database is stolen, the whole minutiae feature of a particular fingerprint will not be compromised by storing the combined minutiae template. It is hard for the attacker to distinguish a combined minutiae template from the original minutiae templates because of the same process. It converts the combined minutiae template into a real-look combined fingerprint by the existing fingerprint reconstruction. By using minutiae-based fingerprint matching algorithms, the new virtual identity matches the two different fingerprints.

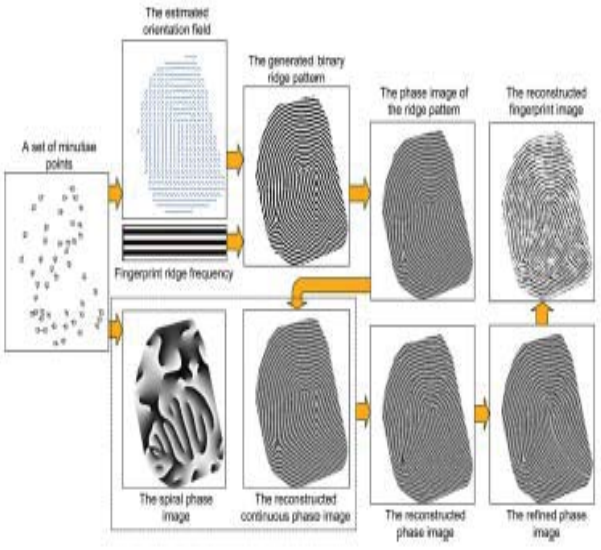


Figure 4.Reconstructing a look-alike fingerprint image from a set of minutiae points

## IX. EXPERIMENTAL RESULT

Figure 5. Input Image 1

Figure 6. Input Image 2

Figure 7. Linearization

Figure 8. Shrinking

Figure 9.Minutiae

Figure 10.Coordination

Figure 11.Combined

The combined image of the query fingerprint is compared to the combined minutiae template. If both the images are matched, then authentication will be success. If it is not matched, then the authentication is failed.

## X. CONCLUSION

In this paper, we proposed a system which has highly secured fingerprint database. For this, we consider two fingerprints of two different fingers of a same individual, and we extract minutiae from one fingerprint and coordination map from the other fingerprint and also reference points for both the fingerprints. Then, we combine isolated points of the two fingerprints and stored in a database. Now this database contains combined minutiae template of two fingerprints, with this we complete our enrolment process. During authentication process, we consider two query fingerprints and we extract the same features mentioned above. With the help of matching algorithm we compared query template with the original template stored in a database. The main advantage of our paper is database contains combined minutiae template so that trespassers cannot be able to split the combined fingerprint. Hence, we mentioned this as a highly secured database.

## 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 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, 2006.

[4] N.K.Ratha, S.Chikkerur, J.H.Connell, andR.M.Bolle,"Generating cancellable 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,"Biometrictemplate transformation: A security analysis," in Proc. SPIE, Electron. Imaging, Media Forensics and Security, San Jose, Jan. 2010.

[6] K.Nandakumar,A.K.Jain,andS.Pankanti,"Fingerprint - basedfuzzy 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," inProc.BiometricsSymp.,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, "Visualcryptographyforbiometricprivacy," 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.