Providing Authentication by Merging Minutiae Template.

***Priya Raul*[*1] , Sayali Surve*[*2] , Sushma Gilbile*[*3] , Jasmine Hebbalkar*[*4] , Prof J.L. Chaudhari*[#5] ,** **B.E Students, #Assistant Professor, Department of Computer Science , JSPM's BSIOTR , University of Pune, Maharashtra , India*

Abstract— **Now a day's use of biometric technologies gains popularity as concern about the privacy and misuse of biometric data increases. Because of this, protecting biometric data becomes an important issue. The oldest and widely used form of biometric identification is the fingerprints. It has been widely used in both forensic and civilian applications. In existing system it is easily possible to revoke the original image from the minutia points. To overcome this drawback we propose a system in which we take two different fingerprints at the enrollment phase and same fingerprints at authentication phase. We extract the minutiae positions and reference Point of first fingerprint and the orientation and reference Point of second fingerprint. Then we merge these two fingerprints to produce a new mixed minutiae template. Incase if hacker hacks this mixed Template image then also He will not able access the data because he will not able to identify that it is combination of two fingerprints, and from which fingerprint we have extracted minutiae points and from which we have extracted orientation. This approach will provide more security to application or data.**

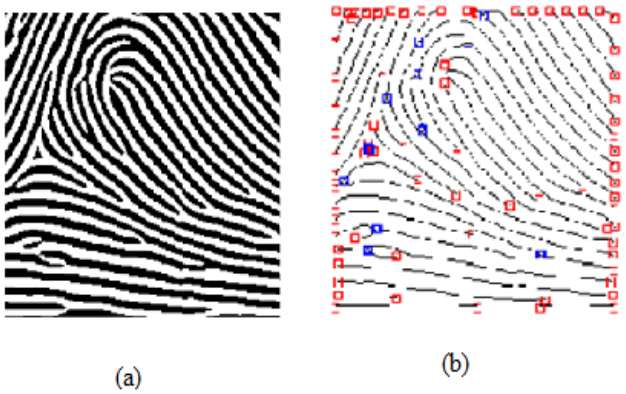
Index Terms— ***fingerprint, merged minutiae Template, minutiae, Orientation, Reference Point.***

I. INTRODUCTION

Fingerprint-based biometric systems are rapidly gaining acceptance as one of the most effective technologies to authenticate users in a wide range of applications: from PC logon to physical access control and from border crossing to voters authentication [22]. Human fingerprints are detailed, unique, difficult to alter, and durable over the life of an individual. This makes them suitable as long-term markers of human identity and other authorities to identify individuals who wish to conceal their identity or to identify human are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster. Fingerprint analysis has decreased many crimes by restricting authentication. Thus in our proposed system we are providing verification of human using fingerprints.

In the biometric process of finger_scanning, minutiae are specific points in a finger image. There are two main types, known as ridge endings and bifurcations. Sometimes, other details, such as the points at which scars begin or terminate, are considered minutiae fig [19].

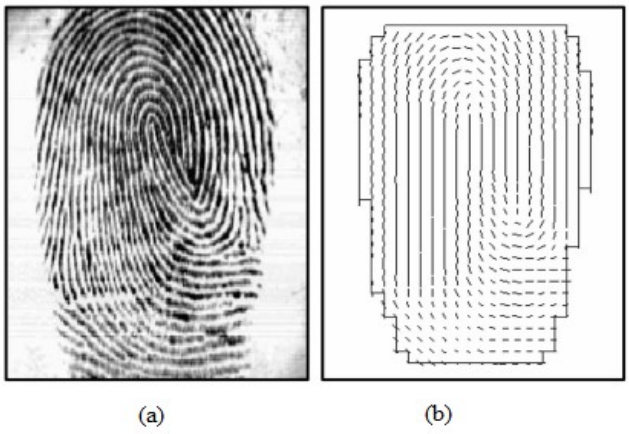
ISSN: 2278 – 1323



(a) (b)

Fig 1: (a) Noise removed fingerprint (b) Minutiae Points of Fingerprint

Orientation is a field of minutiae which describe the direction of minutiae points fig [2].



(a) (b)

Fig. 3.(a)Fingerprint image (b) Orientation image

1.Fingerprint Anatomy

A fingerprint is the reproduction of a fingertip epidermis, which is produced when a finger is pressed against a flat surface. The main structural characteristic of a fingerprint is a pattern of interleaved ridges (also called ridgelines) and valleys (see Fig. 2a), which often run in parallel.[1]

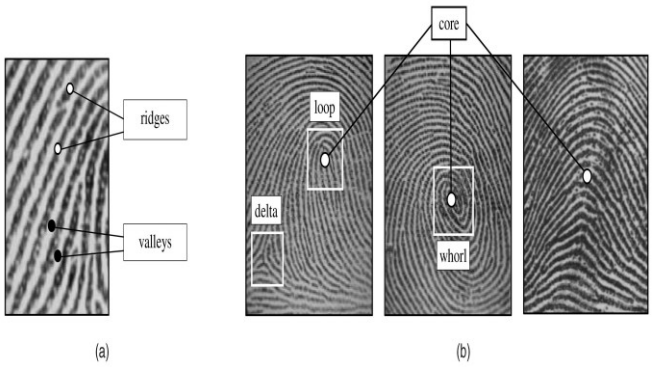


Fig 2. (a) Ridges and valleys on a fingerprint image. (b) Singular regions (white boxes) and core points (small circles) in fingerprint images.

The application of biometric technique is used in a verification system. It is an issue to providing a security to a biometric fingerprint. The encryption and decryption techniques are not enough for fingerprint security because; decryption technique is done before the fingerprint matching. This may helps to attacker to get fingerprint. So, in recent year, some efforts have been put for enhancing the security techniques for fingerprint. In many existing technique we use key for providing security to fingerprint. So the accuracy is fully depends on the key factor, which is never shared [13]. In this paper, we provide a security to the fingerprint by mixing two different fingerprints to form a new identity. In this work We generate merged minutiae template. In such template, the minutiae position are taken from one finger and the minutiae direction is depend on the orientation of other fingerprint.

II. LITERATURE REVIEW

In literature survey, study is done for checking data integrity and data storage technique that have been recently technologically advanced in the domain of cloud computing.

In earlier technique, the key is used for privacy protection using fingerprint which is not convincing. They are not protected when the key and the protected fingerprint are kept. Teoh et al.[2] use the approach of bio hashing which does the some calculations i.e. product between features of fingerprint and key. If we never shared or kept that key [3] then the approach can be correct. Ratha et al. [4] says that template of

fingerprint can be regenerated or reconstructed by apply reverse transform on feature points of fingerprint i.e. minutiae point of fingerprint. The reverse transform of key is guided as, it gives the reduction in the accuracy of matching fingerprint template. The work done in [2] and [4] are shown to be vulnerable to intrusion and linkage attacks when both the key and the transformed template is stolen [5]. Nandakumar et al. [6] propose to implement blur fault on the minutiae, which is defenseless to the key-inversion attack [7]. By using a key our work in [8] imperceptibly hide the user identity on the thinned fingerprint. When both the key and protected thinned fingerprint is stolen the user identity may also be compromised.

There are very less no. of schemes proposed in [9]-[13] which is not using the key for protect the privacy of fingerprint. Further the Ross and Othman [9] propose the use of visual cryptography for protecting the privacy of biometrics. At the time of authentication to generate the current fingerprint image for the purpose of matching, the two sheets are overlaid. The main advantage of this technique is that the feature of fingerprint is not recognized by the attacker in one database. But practically, it is impossible to maintain two databases for same application.

In the research paper [19], the study of providing security to a stored fingerprint image. To mix two fingerprints, each fingerprint is decomposed into two components, viz., the continuous and spiral components. After pre-aligning the two components of each finger- print, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint image in order to generate a mixed fingerprint. Experiments on the FVC2000 datasets show that the mixed fingerprint can be used for authentication and that the identity of the original fingerprint cannot be easily reduced from the mixed fingerprint. The mixed image incorporates characteristics from both the original fingerprint images, and can be used in the feature extraction and matching stages of a biometric system.

Research [18] defines the matching of two fingerprints and the privacy protection schemes. Minutiae based method is used generally for matching two fingerprint images. These methods give the importance to the accuracy of minutiae extraction and the detection of core and delta for pre-alignment. Noisy features introduced from environmental factors such as dust, scars, skin dryness, and scaring, are strongly desired to be removed or kept to a minimal level. [20] Securing a stored fingerprint template is of paramount importance because once fingerprints are compromised fingerprint cannot be easily regenerated. The fingerprints are the widely used form of biometric identification for the authentication purpose.

Fingerprint features [23] are generally Level 1 features mainly refer to ridge orientation field and features derived from it, i.e., singular points and pattern type. Level 2 features refer to ridge skeleton and features derived from it, i.e., ridge bifurcations and endings. Level 3 features include ridge contours, position, and shape of sweat pores and incipient ridges. Reconstruction can be done using the features point of the fingerprint image. Generally remove the noise from the fingerprint image and then skeletonizing perform on the same image. On the basis of this feature points or minutiae points we can get the original image.

III. PROPOSED SYSTEM

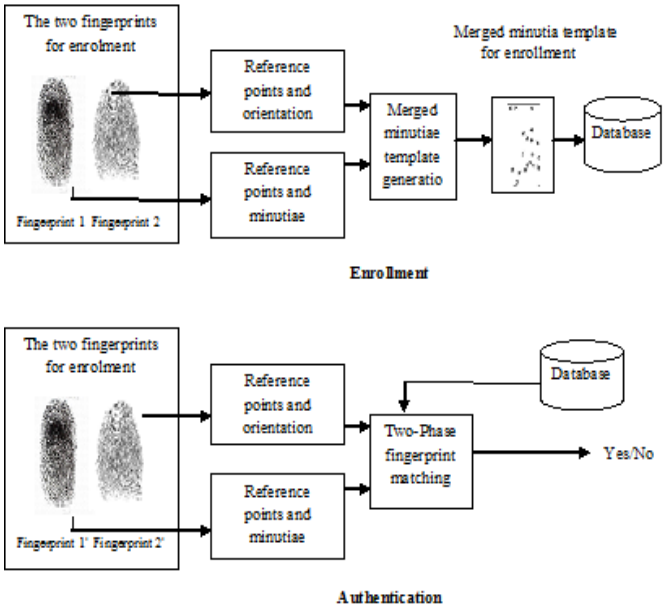


Fig 3. Architecture of the System

1) Enrollment Phase

At enrollment phase we entered the user name and then we

ISSN: 2278 – 1323

take two different fingerprints of the same user. Then we extract minutiae points and the reference points from the first fingerprint. Then in next step we extract orientation and reference points from the other fingerprint.

Then we merge these two fingerprint fields to form a new template which is merged minutiae template. We store this template into the database in the form of XYT file.

2) Authentication Phase

At authentication phase we enter the name of that user if the user ID get found and the merged minutiae template of that Check ID get loaded. Then we again do the same procedure of taking two fingerprints. Then extract reference point and minutiae of first finger and orientation and reference points of the other finger. Then we generate a merged minutiae template.

At the time of matching we match the newly formed template with the template which is stored into the database with that Check ID. If the match score is greater than threshold then the person is authenticated one, otherwise not.

A. Reference Points Detection

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

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

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

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

$$C_{ref} = Z * \overline{T}_{ref} \qquad (2)$$

Where "*" is the convolution and $\overline{T}_{ref}$ is the conjugate.

3) Calculate an improved certainty map [19] Where we get the value of argument of z (defined from $-\pi$ to π).

4) Locate a reference point satisfying the two criterions: (i) the amplitude of C'_{ref} of the point is a local maximum, and (ii) the local maximum should be over a fixed threshold . Suppose we locate a reference point at (r_x, r_y) , the corresponding angle can be estimated as $Arg(\mathbf{C'}_{ref}(r_x, r_y))$.

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

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

B. Combined Minutiae Template Generation

Given a set of minutiae positions $P_A = \{P_{ia} = (x_{ia}, y_{ia}), 1 < i < N$ of fingerprint , the orientation of fingerprint and the reference points of fingerprints *A* and *B* , a combined minutiae template is generated by minutiae position alignment and minutiae direction assignment, as shown in Fig. 2.

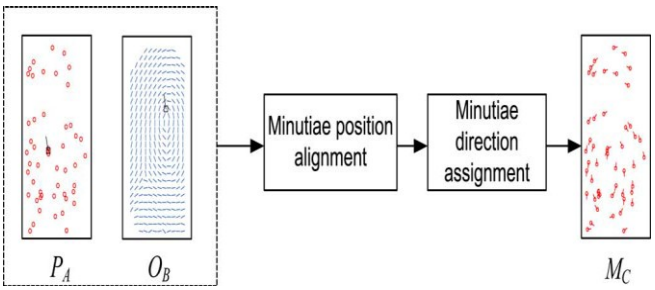


Fig. 2. Merged minutiae template generation process.

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 $r_a = (r_{xa}, r_{ya})$ at with the angle βa , and R_b is located at $r_b = (r_{xb}, r_{yb})$ with the angle βb . The alignment is performed by translating and rotating each minutiae point p_{ia} to $p_{ic} = (r_{ic}, r_{ic})$ to by

$$(p_{ic})^T = \mathbf{H} \cdot (p_{ia} - r_a)^T + (r_b)^T \quad (3)$$

where $()^T$ is the transpose operator and **H** is the rotation matrix.

2) Minutiae Direction Assignment:

Each aligned minutiae position $\mathbf{p}_{ic}$ is assigned with a direction θic as follows:

$$\theta ic = O_B(x_{ic}, y_{ic}) + \rho_i \pi \quad (4)$$

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 θic will be from 0 to 2π, which is the same as that of the minutiae directions from an original fingerprint. Following three coding strategies are proposed for determining the value of ρ_i.

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

2) is determined by

$$\rho_i = \begin{cases} 1 \text{ if } \mathrm{mod}(\theta ia + \beta b - \beta a, \pi) - O_B(x_{ic}, y_{ic}) > 0 \\ 0 \text{ otherwise} \end{cases} \quad (5)$$

where is the modulo operator and θia is the original direction of a minutiae position ρ_{ia} in fingerprint A.

In the following discussions, these two coding strategies are termed as *Coding Strategy* 1 and *Coding Strategy* 2 respectively. In such a case, we need to predict before the direction assignment. Some existing works for modeling the fingerprint orientation can be adopted to do the prediction. For example, the work in [20] can estimate the missing orientation structure even for a partial fingerprint. Here, we simply predict the value of (if it is not well defined) as the value of nearest well defined orientation. Once all the aligned minutiae positions are assigned with directions, a combined minutiae template is created for enrollment. In some cases, a global minutiae position translation may be necessary for such that all the minutiae points are located inside the fingerprint image.

C. Two-Stage Fingerprint Matching

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 [21]. Given a minutiae point m_{ic} and another minutiae point m_{jc} in M_C, we define

1) L_{ij} as the distance between m_{ic} and m_{jc}:

$$L_{ij} = \sqrt{(xic - xjc)^2 + (yic - yjc)^2} \quad (6)$$

2) γ_{ij} as the difference between the directions (after modulo π) of m_{ic} and m_{jc}:

$$\gamma_{ij} = \theta ic \bmod \pi - \theta jc \bmod \pi \quad (7)$$

3) σij as a radial angle:

$$\sigma ij = (\theta ic \bmod \pi, atan2(y_{ij} - y_{ic}, x_{jc} - x_{ic})) \quad (8)$$

where *atan2(y, x)* is a two-argument arctangent function in the range $(-\pi, \pi)$.

An illustration of the definitions of L_{ij}, σij , γ_{ij} and are shown in Fig. 4. For the *i*th minutiae point in m_{ic} in M_C , we extract a set of local features F_i as follows:

$$F_i = (L_{ij}, L_{ij}, L_{ij}, \gamma_{ij}, \gamma_{ik}, \gamma_{il}, \sigma ij, \sigma ij, \sigma ij) \quad (9)$$

where we assume m_{jc} is the nearest, m_{kc} is the second nearest and is the third nearest minutiae point of m_{ic}.

Suppose we detect K_1 (K_1>1) reference points from fingerprint A' and reference points from fingerprint B'.
The query minutiae is determined as follows:

ISSN: 2278 – 1323

1) Select a pair of reference points: one from fingerprint A' (say $R_{a'}$) and the other from fingerprint B' (say $R_{b'}$).

2) Perturb $\beta a'$ by $\tau = \beta a' + k \cdot \Delta$, where k is an integer and Δ is a perturbation size. We choose $\Delta = 3 \times \pi/180$ radians (i.e., 3 degrees) and $-5 < k < 5$. Thus, we have $K = 11$ perturbed angles for the reference point $R_{a'}$.

3) Generate a merged minutiae template $M_{C'}(\tau)$ for testing from $P_{A'}$, $O_{B'}$, $R_{a'}$ (with a perturbed angle) and using the proposed merged 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 $M_{C'}(\tau)$.

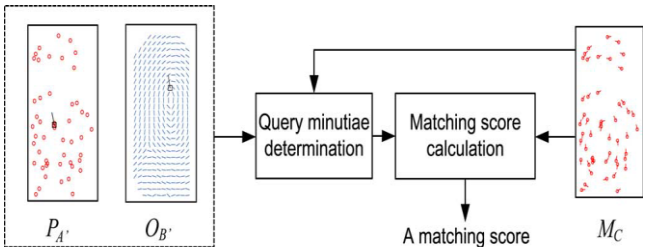


Fig. 3. Two-stage fingerprint matching process.

2) Matching Score Calculation:

For the merged minutiae templates that are generated using *Coding Strategy* 1, we do a modulo π for all the minutiae directions in M_Q and M_C, so as to remove the randomness. After the modulo operation, we use an existing minutiae matching algorithm [16] to calculate a matching score between M_Q and M_C for the authentication decision. For other combined minutiae templates, we directly compute a matching score between M_Q and M_C using an existing minutiae matching algorithm [16].

IV. COMBINED FINGERPRINT GENERATION

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 fingerprint. Therefore, the merged minutiae template has a similar topology to an original minutiae template. Some existing works [15], [22], [23] 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 method to generate a merged fingerprint for two different fingerprints. Given any two different fingerprints as input, we first generate a merged minutiae template using our merged minutiae template generation algorithm. Then, a merged fingerprint is reconstructed from the merged minutiae template using one of the existing fingerprint reconstruction approaches.

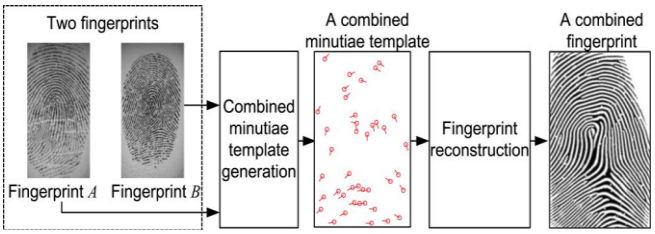


Fig. 5. Generating a merged fingerprint for two different fingerprints.

It should be noted that the combined minutiae template generated by adopting *Coding Strategy* 1 is not appropriate for generating a merged fingerprint. The reason is that we set ρ_i as 0 or 1 randomly during the minutiae direction assignment, i.e., we add π randomly for each minutiae direction in such a coding strategy.

VI . PERFORMANCE ANALYSIS

The main goal of this work is to propose a multi-modal biometric system which preserves privacy and increases accuracy. Privacy is preserved by fusing biometric information from fingerprint i.e. minutiae points and orientation points.

The EER of matching two mixed fingerprints is about 15% when two distinct fingerprints are formally chosen for creating a merged fingerprint. If the two different fingerprints are cleverly chosen according to a compatibility measure, the EER can be reduced to about 4%[1].

To compute the False Rejection Rate (FRR), the second impressions of a finger pair are matched against the corresponding enrolled template. The average FRR (at different FAR) computed from the 10 groups of finger pairs for the two cases .We can see that our system performs similarly for the two cases of coding strategies[1]. However, the error rates vary among different coding strategies, where the Coding Strategy 1 achieves the lowest error rate with (at) for both cases. While the results of using Coding Strategy 3 are the worst, with over 1% FRR (at) for both cases.

Result of the system mainly depends upon the following points :

i. The input image at the time of enrolment and authentication phase should be clean and clear.
ii. The reference point selection of the enrolled fingerprints should be same as that of authenticated phase.
iii. All device drivers of the scanner should be installed in the system for best performance.

For getting the authentication certificate to the user, the match score is calculated . The threshold we set is T=0.5. If the match score is above 0.5 , the person is a authenticated person and he can access the database. The minutiae counts while authenticating and enrolment can vary but the reference point should be equal at both the phases.

If the attacker knows that a stolen template has been protected by using our technique, he would try to launch the aforementioned attacks based on the minutiae positions only, . i.e., he would try to modify the minutiae matcher such that the minutiae directions are ignored during the matching.

	T				
	3	4	5	6	7
No	1141	1077	1588	162	209
True Detection Rate(%)	99.5	98.0	98.5	99.0	99.5
False Detection Rate(%)	0.5	0.5	1.5	1.5	1.5

Table : Performance of Reference Points Detection at Different Setting of Threshold T

VII .CONCUSION AND FUTURE SCOPE

In this paper, we are generating a new identity by merging two different fingerprints. To combine two fingerprints, each fingerprint is decomposed into two factors, viz., the minutiae points and the orientation. After aligning the components of each fingerprint, the minutiae point of one fingerprint is combined with the orientation i.e. of the other fingerprint image. At the time of Authentication phase, the template which is stored in the database is compared with the template generated at this phase. Our merged minutiae template has a similar topology to an original minutiae template. Thus, we are able to merge two different fingerprints into a new fingerprint by reconstructing a real-look alike combined fingerprint from the merged minutiae template.

As we can perform the reconstruction of a single fingerprint[1][15] from the various features of the fingerprint, thus our template produced provides higher security because of merging two fingerprints. Further work is required to enhance the performance due to merged fingerprints by

ISSN: 2278 – 1323

exploring alternate algorithms for selecting and uniting the different pairs.

ACKNOWLEDGEMENT

This work was guided by Prof.Mrs.Jayshree L Chaudhari. Authors would also like to thank Prof. Mrs.G.M. Bhandari Head of Computer Department, JSPM's BSIOTR & Prof. Mr B.Bhurghate, our Project Coordinator for providing all facility and every help for smooth progress of Project work.

REFERENCES

[1] Sheng Li and Alex C. Kot, "Fingerprint combination for privacy protection," in IEEE Trans. Information Forensics And Security, Vol. 8, No. 2,February 2013

[2] 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, and R. M. Bolle, "Generatingcancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach.Intell.*, vol. 29, no. 4, pp. 561–72, Apr. 2007.

[5] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzyvault: Implementation and performance," *IEEE Trans. Inf. ForensicsSecurity*, vol. 2, no. 4, pp. 744–57, Dec. 2007.

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

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

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

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

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

[11] A. Othman and A. Ross, "Mixing fingerprints for generating virtualidentities," 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 fingerprintanalysis: Are fingerprints holograms?," *Opt. Express*, vol. 15, pp.8667–8677, 2007.

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

[15][16] VeriFinger 6.3. [Online]. Available: http://www.neurotechnology.com

[16][17] 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.

[17][18]Abraham, J. (2010). Matlab code for fingerprint matching algorithm.

[18][19]Raffaele Cappelli, Alessandra Lumini, Dario Maio,Member, IEEE, and Davide Maltoni, Member,

IEEE Fingerprint Image Reconstruction from Standard Templates IEEE SEPTEMBER 2007.

[19] [20] 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.

[20] [21] J. Feng and A. K. Jain. Fingerprint reconstruction: From minutiae to phase. IEEE Transactions on Pattern Analysis and Machine Intelligence, 33(2):209 –223, Feb. 2011.

[21] [22] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook Fingerprint Recognition. Springer, 2003.

[22] [23] J. Feng and A.K. Jain, "FM Model Based Fingerprint Reconstruc- tion from Minutiae Template" Proc. Second Int'l Conf. Biometrics, pp. 544-553, June 2009.

Authors

Ms. Priya Raul – Currently she is pursuing B.E. (CSE) at JSPM's Bhivarabai Sawant Institute of Technology and Research, Maharashtra,
Pune, India.

Ms. Sayali Surve – Currently she is pursuing B.E. (CSE) at JSPM's Bhivarabai Sawant Institute of Technology and Research, Maharashtra,
Pune, India

Ms. Sushma Gilbile – Currently she is pursuing B.E. (CSE) at JSPM's Bhivarabai Sawant Institute of Technology and Research, Maharashtra,
Pune, India

Ms. Jasmine Hebbalkar – Currently she is pursuing B.E. (CSE) at JSPM's Bhivarabai Sawant Institute of Technology and Research, Maharashtra,
Pune, India

Prof.Mrs. J.L. Chaudhari – Currently she is Professor at JSPM's Bhivarabai Sawant Institute of Technology and Research, Maharashtra,
Pune, India

ISSN: 2278 – 1323