Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1097 – 1104

RESEARCH ARTICLE

Virtual Identity Creation by Fingerprint Combination for Privacy Protection

Ms. Namrata Yesansure[1], Prof. Rushi Longadge[2]

[1]Department of CSE G.H. Raisoni Academy of Engineering and Technology, Nagpur University Maharashtra India
[2]Department of CSE G.H. Raisoni Academy of Engineering and Technology, Nagpur University Maharashtra India

[1] nm.yesansure@gmail.com, [2] rushilongadge@gmail.com

Abstract*-- Now a days both forensic and civilian applications makes use of biometric data as concerns about privacy and misuse of data increases. Thus protecting biometric data is one of the prime issues. Although, over the years many template protection schemes have been discovered and much research and progress have been made on fingerprint authentication system, performance of even state-of-the-art matchers is still much low. In addition to this, securing a stored fingerprint template is of paramount importance because compromised fingerprint cannot be easily revoked. Therefore, to tackle these problems, much effort is still needed to improve the performance, security and speed of fingerprint authentication systems. In this project a biometric authentication system for protecting fingerprint privacy is proposed. The idea is to combine two different fingerprints, pertaining to two different fingers into a new identity. The proposed work of this project is carried out in two phases. In the first phase combined minutiae template will be generated based on the information extracted from two different fingerprints. And in the next phase a Fingerprint-Matching process is proposed for matching the query fingerprints against a combined minutiae template by using minutiae matching algorithm. Furthermore, the proposed work is more robust to attacks in sense that by storing combined minutiae template into the database, the complete minutiae feature of a single fingerprint will not be compromised when database is stolen. The experimental results show that our system can achieve a very low error rate with FRR = 0.1% at FAR = 0.1%. Compared with the state-of-the-art technique, our work has the advantage in creating a better new virtual identity.

***Keywords*—Fingerprint, Biometric templates, Virtual identity, Authentication, Minutiae**

I. INTRODUCTION

In recent years, verification is becoming a security backbone in the modern distributed systems environment. The biometric is a stirring and emerging field of technology that offers solutions in many applications for instance verification, recognition, security monitoring, border control and immigration, financial transactions, law enforcement agencies, retail sales [12]. In authentication systems the fingerprints are the widely used form of biometric identification. Although fingerprint recognition has been studied for many years and many such security techniques have been discovered, the performance of even state-of-the-art matcher is still much low. Furthermore, traditional encryption techniques are not enough for fingerprint privacy protection as decryption is needed before fingerprint matching, which exposes the fingerprint to the opponents. Thus protecting the privacy of the fingerprint becomes an important issue.

© 2014, IJCSMC All Rights Reserved

Most of the existing techniques exploit the key or token for the fingerprint privacy protection, which creates the difficulty. They may also be open to attacks when both the key or token and the protected fingerprint are stolen. Several approaches have been proposed in the literature to protect biometric templates from revealing important information. Teoh et al. [5] propose a biohashing approach in which the inner products between the user's fingerprint features and a tokenized pseudorandom number (i.e. the key) is computed. The accuracy of this approach primarily depends on the key or token, which assumed to be never shared or stolen [14].Ratha *et al* [6] propose to generate cancellable fingerprint templates by applying noninvertible transforms on the minutiae. The noninvertible transform is guided by a key, which will usually lead to a reduction in matching accuracy. The work in [5] and [6] are shown to be exposed to intrusion and linkage attacks when both the key and the transformed template are stolen [13]. Sheng Li and Alex Cot [7] imperceptibly hide the user identity on the thinned fingerprint using a key. The user identity may also be compromised when both the key and the secured thinned fingerprint are stolen.

There are some schemes [1],[2],[4] and [8]–[11] that are able to protect the privacy of the fingerprint without using a key. These schemes provide security to the fingerprint template by creating a virtual identity. Virtual identity is created with the fusion of features extracted from two or more biometric template which is then stored into the database instead of storing original template. For example as shown in fig. 1 the virtual identity is created by combining features extracted from two fingerprints.

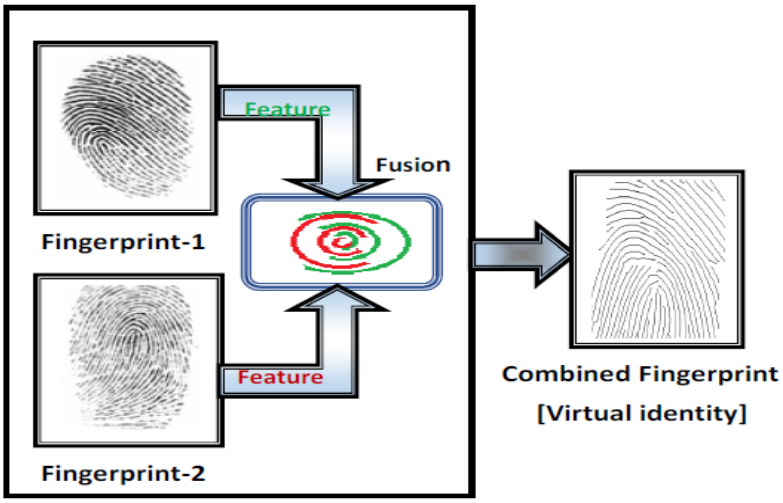

Fig.1 Virtual identity creation by combining features acquired from two fingerprints.

Our survey in [3] gives a detail review of schemes that are explored for fingerprint privacy protection without using a key, along with their merits and demerits.

II. THE PROPOSED FINGERPRINT PRIVACY PROTECTION SYSTEM

In this project a biometric authentication system for protecting fingerprint privacy is proposed. The idea is to combine two different fingerprints, pertaining to two different fingers into a new identity. The proposed work of this project is carried out in two phases. In the first phase combined minutiae template will be generated based on the information extracted from two different fingerprints. And in the next phase aFingerprint-Matching process is proposed for matching the query fingerprints against a combined minutiae template by using image processing algorithm. Furthermore, the proposed work is more robust to attacks in sense that by storing combined minutiae template into the database, the complete minutiae feature of a single fingerprint will not be compromised when database is stolen.

Fig. 1 shows proposed fingerprint privacy protection system. As shown in figure the work is divided into two phases. During enrollment phase, the system captures two fingerprints from two different fingers, say source fingerprints SF_A and SF_B from fingers F_A and F_B, respectively, the minutiae locations are extracted from fingerprint SF_A and the minutiae direction from fingerprint SF_B using some existing techniques [15], [16], [17] and [18]. Then, a combined minutiae template is generated based on the minutiae locations, the directions and the primary core 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 QF_A and QF_B from fingers F_A and F_B. Then, same procedure as what done in the enrollment phase is applied, i.e., the minutiae locations are extracted from fingerprint QF_A and the directions from fingerprint QF_B. Primary

© 2014, IJCSMC All Rights Reserved

core points are extracted from both query fingerprints. These extracted information will be matched against the corresponding template stored in the database by using an minutiae based matching algorithm.

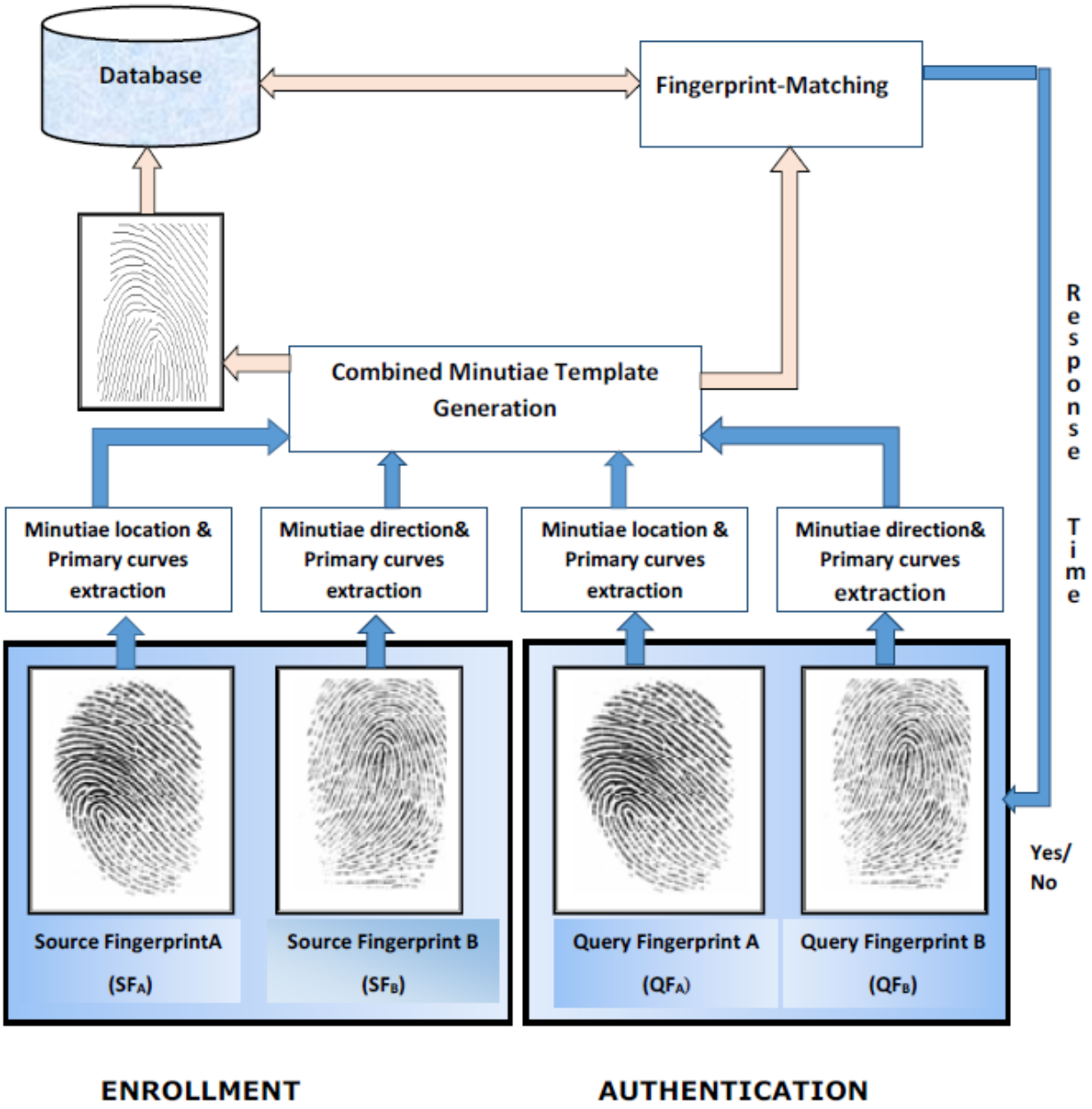

Fig. 2. Proposed fingerprint privacy protection system.

We adopt the algorithms [15], [16], [17] for extracting the minutiae positions and the minutiae directions. While the reference point detection is performed by using the scheme provided in[18] this method is improved version of method proposed in[19]. We used this reference point detection algorithm to estimate the location and the angles of the reference point of a fingerprint.

A] Combined Minutiae template generation

Given a set of minutiae *N* positions $P_A = \{\mathbf{p}_{ia} = (x_{ia}, y_{ia}), 1 \le i \le N\}$ of fingerprint F_A , the orientation O_B of fingerprint F_B and the reference points of fingerprints F_A and F_B , a combined minutiae template MS_C is generated by minutiae position alignment and minutiae direction assignment, as shown in Fig. 3.

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 *Ra* and *Rb* for

© 2014, IJCSMC All Rights Reserved

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

$$(\mathbf{p}_{ic})^T = \mathbf{H} \cdot (\mathbf{p}_{ia} - \mathbf{r}_a)^T + (\mathbf{r}_b)^T \quad \textbf{(1)}$$

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

$$\mathbf{H} = \begin{bmatrix} \cos(\beta_b - \beta_a), \sin(\beta_b - \beta_a) \\ -\sin(\beta_b - \beta_a), \cos(\beta_b - \beta_a) \end{bmatrix} \quad \textbf{(2)}$$

As such, *Ra* and *Rb* are overlapped both in the position and the angle after the minutiae position alignment.

2) Minutiae Direction Assignment: Each aligned minutiae position $\mathbf{p}_{ic}$ is assigned with a direction θ_{ic} as follows:

$$\theta_{ic} = O_B(x_{ic}, y_{ic}) + \rho_i \pi \quad \textbf{(3)}$$

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.

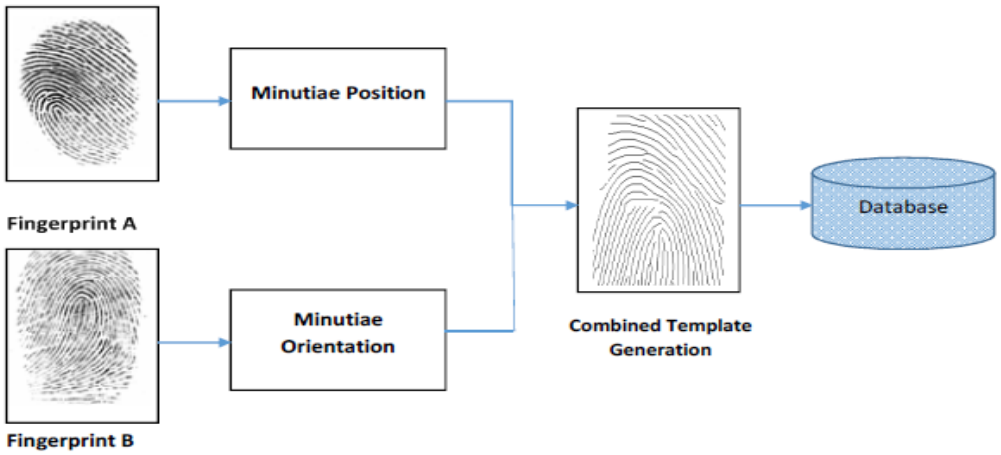

Fig. 3. Combined minutiae template generation process.

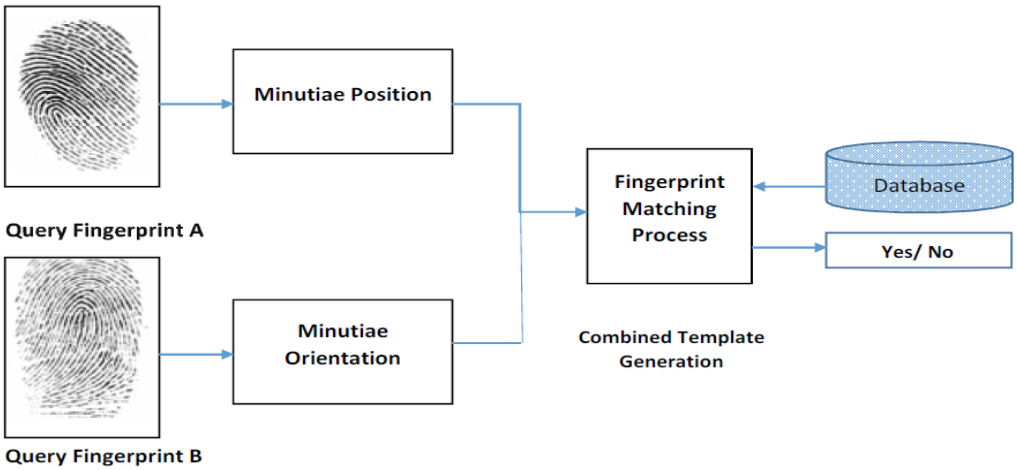

Fig. 4. Fingerprint matching process.

© 2014, IJCSMC All Rights Reserved

B] Fingerprint Matching

Given the minutiae positions of fingerprint, the orientation of fingerprint and the reference points of the two query fingerprints. In order to match the stored in the database, we propose a fingerprint matching process including query minutiae determination and matching as shown in Fig. 4.

1) *Query Minutiae Determination:* In this process, two query fingerprints are required from the same two fingers, say fingerprints QF_A and QF_B from fingers F_A and F_B. As what we have done in the enrollment, process, extract the minutiae positions from fingerprint QF_A and the orientation from fingerprint QF_B. Reference points are detected from both query fingerprints. Then combined minutiae template is generated by using our proposed combined minutiae template generation approach.
2) *Template Matching:* For the combined minutiae template MQ_C that are generated using proposed algorithm is then match with combined minutiae template MSc stored in a database during enrollment by minutiae based matching algorithm[21].

III. EXPERIMENTAL RESULTS AND DISCUSSIONS

A] Evaluating Performance of proposed system over different databases.

For evaluating the performance of proposed system the experiment is conducted on different fingerprint databases such as FVC2000, FVC2002 and FVC2004.

We use the first two impressions in the FVC2002 DB2_A [22] to evaluate system performance, which contains 200 fingerprints from 100 fingers as each finger has two impressions. Therefore, we have a 100 finger pairs the first two impressions of each fingerprint are combined to generate combine minutiae template during enrolment process. The algorithm Ratha 1995 and Sherlock 1994 are used for extracting features such as minutiae position and direction. The image processing algorithm convolution filter is used for fingerprint matching. To compute the False Rejection Rate (FRR), the second impressions of a finger pair are matched against the corresponding enrolled template, producing 100 genuine tests. To compute the False Acceptance Rate (FAR), the first impressions of a finger pair are matched against the other 99 enrolled templates, producing 100 ×99 imposter tests.

TABLE I
PERFORMANCE OF PROPOSED SYSTEM OVER DIFFERENT DATABASES

FAR / FRR	0.001	0.01	0.1	1	FVC Databases
0.0011	0.0012	0.012	0.11	0	2000
0.0014	0.0016	0.018	0.19	0	2002
0.001	0.0018	0.016	0.3	0	2004

Similarly our system performance evaluated for FVC2000 [23] and FVC2004 [24] Databases. The Table I shows the evaluated resultant value of FRR at various values of FAR. From table I we can see that, FRR of our system is 0.1% when FAR= 0.1%. The fig. 5. shows that the performance of proposed system is better over FVC2000 database

© 2014, IJCSMC All Rights Reserved

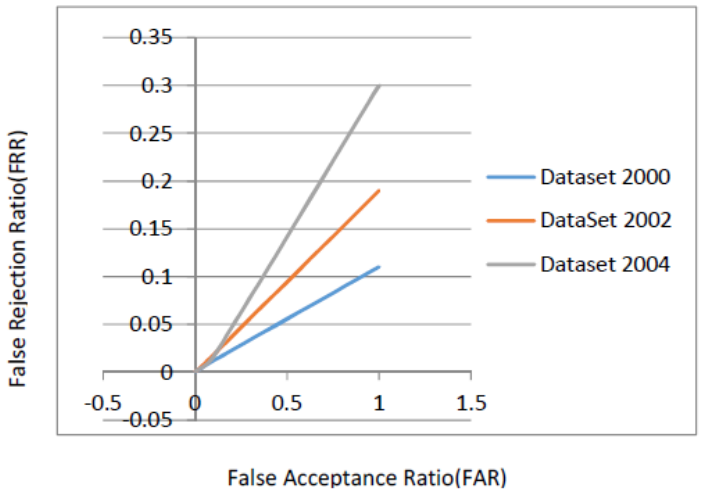

Fig.5. The performance evaluation of proposed system over different datasets.

The Table-II shows the performance comparison between proposed system and existing techniques that are explored for fingerprint privacy protection. The comparison illustrates the performance of our system is better than the work in [6], [20], and [4].

TABLE II

PERFORMANCE COMPARISION BETWEEN OUR PROPOSED SYSTEM AND SOME EXISTING PRIACY PROTECTION SCHEMS

Techniques	Performance	Database for evaluation
Ratha et al.[6]	FRR= 16 % at FAR = 0.01%	The first two impressions in FVC2002 DB2_A
Nagar et al. [20]	FRR= 5% at FAR= 0.01%	
Sheng Li et al [4]	FRR= 3% at FAR= 0.01%	
The Proposed system	FRR= 0.1 % at FAR = 0.01%	

In our proposed system as we extract partial features from two fingerprints separately (i.e., minutiae position from one fingerprint and minutiae direction from another fingerprint). If it is stolen by imposters the complete minutiae feature of each fingerprint are compromised. Therefore it is not easy for hacker to recover the original minutiae templates from a combined minutiae templates.

IV. CONCLUSION

This paper introduces a novel system for fingerprint privacy protection by combining partial features of two fingerprints into a new virtual identity. In the enrolment, the system captures two fingerprints pertaining to two different fingers. A combined minutiae template is then generated which contains only a partial features of the two fingerprints and stored in a database. Therefore, even if the fingerprint template is stolen, the complete minutiae feature of a single fingerprint will not be compromised. In the authentication process, two query fingerprints are needed from the same two fingers. A fingerprint matching process is proposed for matching the query fingerprints against the enrolled template stored in a database. The features provided by our system are summarized below: i) the experimental result shows that, our system achieves a very low error rate with FRR=0.1% at FAR= 0.1%. ii) No key or token is required in the enrolment and authentication. iii) Compared with existing schemes our system can generate better new virtual identity.

© 2014, IJCSMC All Rights Reserved

REFERENCES

[1]S. Li, A. C. Kot," Fingerprint Combination for Privacy Protection", *IEEE Transactions on Information Forensics and security, Vol. 8, No. 2, February 2013.*

[2]A. Othman, A. Ross, "On Mixing Fingerprints",*IEEE Transactions on Information Forensics and security, Vol. 8, No. 1, January 2013.*

[3] N. M. Yesansure, A. Mahajan and R. Longadge," Technology Review: A Fingerprint Privacy Protection Schemes , *International Journal of Advanced Research in Computer Science and Software Engineering, Vol 4, pp. 486-489, February – 2014.*

[4]S. Li and A. C. Kot, "A novel system for fingerprint privacy protection," *in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), Dec. 5–8, 2011, pp. 262–266.*

[5] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and toke1nized random number," *Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.*

[6] 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.*

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

[8] 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.*

[9] 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.*

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

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

[12] Md. R. Islam, Md. S. sayeed and A. Samraj,"Technology Review: Image Enhancement, Feature Extraction and Template Protection of a Fingerprint Authentication System," *Journal of Applied Sciences 10(14):1397-1404, 2010.*

[13]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.*

[14] 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.*

[15]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.

[16] [13] R. Bansal, P. Sehgal and P. Bedi,"Minutiae Extraction from Fingerprint Images- a Review," *in Proc.IJCSI,Vol.8, Issue 5, No3, September 2011.*

[17] N. K. Ratha, S. Chen and A. K. Jain," Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images", *Pattern Recoonition, Vol. 28, No. 11, pp. 1657 1672, 1995.*

[18]S. Chikkerur and N. Ratha, "Impact of singular point detection on fingerprint matching performance," *in Proc. Fourth IEEE Workshop on Automat. Identification Advanced Technologies, O*ct. 2005, pp. 207–212.

[19] 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.

[20]A. Nagar, K. Nandkumar, and A. K. Jain, " A hybrid biometric cryptosystem for securing fingerprint minutiae templates", Patterns Recognition Letters, Vol. 31, no.8,pp 733-741,2010.

© 2014, IJCSMC All Rights Reserved

[21]S. D. Patil and S. A. Patil, " Fingerprint Recognition using Minutiae Matching", *World journal of Science & Technology*, pp.178-181, Apr 2012.

[22]FVC2000 web site: http://bias.csr.unibo.it/fvc2000

[23] FVC2002 web site http://bias.csr.unibo.it/fvc2002

[24] FVC2004 web site: http://bias.csr.unibo.it/fvc2004

AUTHORS BIOGRAPHY

Ms. Namrata M. Yesansure, received the B. E. degree in Information Technology from Yeshwantrao Chavan College of Engineering, Nagpur, India, in 2009.She is currently pursuing M.Tech in Computer Science & Engineering from G. H. Raisoni Academy Of Engineering and Technology, Nagpur. Her research interests include Biometric template protection, Pattern recognition and Image Processing. nm.yesansure@gmail.com

Prof. Rushi Longadge, received the Bachelor of Engineering degree in Information Technology from North Maharashtra University, Jalgon, India, in 2010 and Master of technology in Computer Science & Engineering from G.H. Raisoni College of Engineering, Nagpur. Mr. Rushi Longadge, currently working as Asst. Professor in Department of Computer Science & Engineering, G. H. Raisoni Academy Of Engineering and Technology, Nagpur. His Research areas are Data Mining, Machine Learning and Image Processing. rushilongadge@gmail.com

© 2014, IJCSMC All Rights Reserved