International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-05, Issue-04, July 2019

Idiosyncratic Identity Erection of Fingerprint By Template Generation

*Miss. Vaidehi A. Patil1, #Prof. Zainab Mizwan

*ME (EXTC), #HOD (EXTC), Shree L.R. Tiwari College of Engineering, Mira Road East, Thane, Maharashtra, India. *vaidehipatil608@gmail.com, #zainab.mizwan@gmail.com

Abstract :- **Now-a-days fingerprints are widely used for authentication, so there is need to protect this fingerprint from various attacks which may create problem to other security system. The motivation of selecting this project is to protect the privacy of fingerprints by creating virtual identity [24]. The motivation for the choice of fingerprint biometric features is founded by the wide use of fingerprints, however, little research attention has been paid to designing multi-biometric systems, which protect the privacy of individuals and provide for revocability of templates, based on them. Fingerprint matching algorithms system issued for protecting fingerprint Privacy by combining two different fingerprints into a new Identity [11]. This project is a system for protecting fingerprint privacy by fusion of two different biometric fingerprints into a new identity. In this system we generate an algorithm to create fuse minutiae template of two fingerprints. We are able to create a combined template which is a real look alike of single fingerprint. Thus a unique identity is created with very low error rate i.e. FRR=0.2% & FAR=0.01%.**

Keywords— Fingerprint, FRR, FAR, multi-biometric systems, template.

I. Introduction

Fingerprint techniques have widespread of applications in authentication systems. Hence protecting the privacy of the fingerprint becomes an important issue. Conventional encryption methods are not sufficient for protecting the privacy of the fingerprint, because decryption technique is needed before the fingerprint matching process [21]. This technique exposes the fingerprint to the intruders or attackers. Therefore, to avoid this many methods have been developed which helps in developing specific fingerprint protection techniques. In order to protect the privacy of the fingerprint most of the existing methods make use of key. This creates much inconvenience in the privacy. These techniques become inefficient when both the key and the fingerprint are stolen. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint [21].

Propose a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity. During the enrolment, 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 [3].

Our major goal is to improve the performance of the Bio-hashing method under the assumption that secret keys are stolen by using multi-biometrics. The motivation for the choice of fingerprint biometric traits is founded by the wide use of these traits, however, little research attention has been paid to designing multi-biometric systems, which protect the privacy of individuals and provide for revocability of templates, based on them.

The objectives of this project are as follows:

1. The identity of the biometrics is never exposed to the attacker in a single database.
2. It is difficult for the attacker to distinguish a mixed fingerprint from the original fingerprints.
3. The effectiveness of the projected two stage fingerprint matching, assess the enactment of our system by using a straight minutiae matching method for the similar fingerprint.
4. Our system is able to achieve a very low error rate with FRR= 0.2% when FAR= 0.01%. 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].

DOI : 10.35291/2454-9150.2019.0328

5. 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 [1].

II. LITERATURE SURVEY

1. Miss Dhanashri J. Ghate, Mrs. Savitri B. Patil, "Robust Combination Method for Privacy Protection Using Fingerprint and Face Biometrics" – Institute of Electrical and Electronics Engineering (IEEE), Vol. 2, 2015 [1].

This paper focuses on secure advance system for fingerprint privacy protection by combining different biometrics fingerprint and face into a new identity is proposed. In an enrollment, one fingerprint and face images are captured from same person. Then the minutiae positions and orientation from fingerprint and the reference points from both biometrics are extracted.

Based on this extracted information and proposed coding strategies, combined template is generated and then stored in a database. In the verification, the system requires two queries; one fingerprint and one face from the same person. The two-step fingerprint matching algorithm is used for matching the fingerprint of same person against the generated combined minutiae template. For the face, chi-square dissimilarity measure is used for matching feature vectors of the person which are compared with all feature vectors of persons present in dataset.

Fingerprint-face reconstruction approach is used to create combined fingerprint-face image from combined template. Hence, a virtual identity is nothing but the reconstructed image created from the two biometrics one fingerprint and one face and is used for matching purpose.FRR and FAR of the proposed system is low and is 1% each. Work proposed can create better identity when fingerprint-face images are randomly taken.

2. Kanagala Surya Chaitanya, Ch. Cury "Finger Print Combination for Privacy Protection and Security"- International journal of advanced Technology and Innovative research (IJATIR) ISSN 2348–2370 Vol.07, Issue. 11 , August-2015 [2].

In this paper the authors have mentioned a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity, in the enrollment, two fingerprints are captured from two different fingers. In Existing system, contain only Password authentication. So the hackers easily hack out password and communication to authentication server. So this system didn't provide fully supported security to users. The second one is that we just take a single finger print for signing in or logging in and it also doesn't provide complete security. 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.

3. Sheng Li Student Member, IEEE, and Alex C. Kot , Fellow, IEEE, "Fingerprint Combination for Privacy Protection", IEEE transactions on information forensics and security, vol. 8, no.2, February 2013 [3].

In this paper the authors have proposed a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity, in the enrollment, two fingerprints are captured from two different fingers. In Existing system, contain only Password authentication. So the hackers easily hack out password and communication to authentication server. So this system didn't provide fully supported security to users. The second one is that we just take a single finger print for signing in or logging in and it also doesn't provide complete security. 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.

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 [4].

This paper proposes a novel system for protecting the fingerprint privacy without using a token or key. In the enrollment, two fingerprints are captured from two of an user's fingers. We extract the minutiae positions from one fingerprint, the orientation from the other fingerprint and the primary cores from both fingerprints. Based on these extracted information, a combined minutiae template is generated and stored in a database. In the authentication, the user needs to provide two query fingerprints from the same two fingers which are used in the enrollment. 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 also difficult for the attacker to distinguish our template from the minutiae of an original fingerprint.

DOI : 10.35291/2454-9150.2019.0328

We evaluate the performance of our system over the FVC2002 DB2 A database. The results show that the False Rejection Rate of our system is 3% when the False Acceptance Rate is 0.01%.

5. 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 [5].

Securing a stored fingerprint image is of paramount importance because a compromised fingerprint cannot be easily revoked. In this work, an input fingerprint image is mixed with another fingerprint (e.g., from a different finger), in order to produce a new mixed image that obscures the identity of the original fingerprint. Mixing fingerprints creates a new entity that looks like a plausible fingerprint and, thus, (a) it can be processed by conventional fingerprint algorithms and (b) an intruder may not be able to determine if a given print is mixed or not. 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 fingerprint, 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 WVU and FVC2000 datasets show that the mixed fingerprint can potentially be used for authentication and that the identity of the original fingerprint cannot be easily deduced from the mixed fingerprint. Further, the mixed fingerprint can facilitate in the generation of cancellable templates.

6. D.Sriganesh1, B.Baskar2, K.Somasundaram3, C.Janani4 "Combined Fingerprint Verification for Privacy Protection" International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)(An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 2, February 2015 [6].

In this paper we have proposed an innovative fingerprint recognition system by combining two different fingerprints into a new identity which contains minutiae position and minutiae orientation. In the enrolment phase, two fingerprints are obtained from two different fingers and minutiae positions from one fingerprint, the orientation from the other fingerprint. Based on this extracted information, a combined template is generated and stored in database. In the verification phase, the system requires two query fingerprints from the fingers which are used in the enrolment. The fingerprint matching process is done by minutiae-based fingerprint matching algorithms. By storing the combined template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen.

7. 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 [7].

This paper has introduced a critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system will be robust with respect to the quality of input fingerprint images, it is essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module. We present a fast fingerprint enhancement algorithm, which can adaptively improve the clarity of ridge and valley structures of input fingerprint images based on the estimated local ridge orientation and frequency. We have evaluated the performance of the image enhancement algorithm using the goodness index of the extracted minutiae and the accuracy of an online fingerprint verification system. Experimental results show that incorporating the enhancement algorithm improves both the goodness index and the verification accuracy.

8. 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 [8].

In this research paper, the authors have suggested for the alignment of two fingerprints certain landmark points are needed. These should be automatically extracted with low misidentification rate. As landmarks we suggest the prominent symmetry points (singular points, SPs) in the fingerprints. We identify an SP by its symmetry properties. SPs are extracted from the complex orientation field estimated from the global structure of the fingerprint, i.e. the overall pattern of the ridges and valleys. Complex filters, applied to the orientation field in multiple resolution scales, are used to detect the symmetry and the type of symmetry. Experimental results are reported.

9. 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.

A majority of the minutiae based fingerprint verification algorithms rely on explicit or implict alignment of the minutiae points for matching the two prints. With no prior knowledge about point correspondences, this becomes a combinatorial problem. Global features of the fingerprints such as the core and delta points represent intrinsic points of reference that can be used to align the two prints and reduce

DOI : 10.35291/2454-9150.2019.0328

the computational complexity of the matcher. However, automatic extraction of singular points is usually error prone and is therefore not used by existing matchers. But, a systematic study of the impact on matching performance when core/delta points are available has not been done to date. In this paper, we explore the effects of the availability of reliable core and delta points on speed and accuracy of a matching algorithm. Towards this end, we present significant improvements to core and delta point detection algorithm based on complex filtering principles originally proposed by Nilsson et al. [9]. We also present a modified graph based matching algorithm that can run in O(n) time when the reference points are available. We analyse the resulting improvement in computational complexity and present experimental evaluation over FVC2002 database. We show that there is up to 43% improvement (70.2ms to 39.8ms) in average verification time and almost no loss in accuracy when reliable core and delta points are used.

10. X. Jiang and W. Yau , “Fingerprint minutiae matching based on the local and global structures,” in Proc. 15th Int. Conf. Pattern Recognition, 2000, vol. 2, pp. 1038–1041.

This paper proposes a new fingerprint minutia matching technique, which matches the fingerprint minutiae by using both the local and global structures of minutiae. The local structure of a minutia describes a rotation and translation invariant feature of the minutia in its neighbourhood. It is used to find the correspondence of two minutiae sets and increase the reliability of the global matching. The global structure of minutiae reliably determines the uniqueness of fingerprint. Therefore, the local and global structures of minutiae together provide a solid basis for reliable and robust minutiae matching. The proposed minutiae matching scheme is suitable for an on line processing due to its high processing speed. Experimental results show the performance of the proposed technique.

III. Fingerprint Protection is Necessary

Fingerprint protection is necessary

The system results are better as comparison with other fingerprints methods [4]–[6] are as follows:

1) Advance propose scheme is capable to get very low error rate with FRR = 0.2 % when FAR=0.01%.

2) Compared with featured level best technique, propose here create a new identity which is difficult to be separated from the original minutiae template.

3) Compared with the image level based technique, the new virtual identity created with the fusion of two fingerprints performs better, when two are randomly chosen.

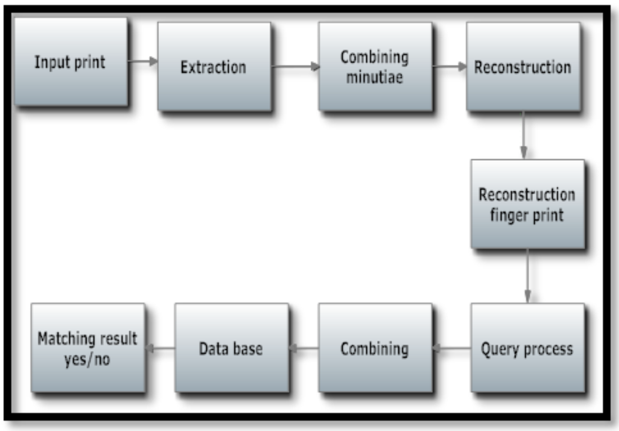


Fig. 1 Block Diagram

During Enrolment, First fingerprint image is loaded then it is binarize. From this binarized image Bifurcation, Termination & Ridge Detection called as minutiae points are extracted with coding strategies. From the second fingerprint image, X & Y gradients are extracted and then by combining gradients orientation is form using coding strategy. After reference point extraction both the fingerprints images are combining together to form a combined template which is real looks like a single fingerprint. For more accuracy and low error rate, this combined fingerprint images are further process for minutiae extraction. After minutiae extraction combined fingerprint is generated and stored in database.

During authentication, the two-stage fingerprints verification process is proposed for matching the two query fingerprints against the combined template. Topology of a combined template is similar to the original minutiae templates, so it is converted into the real resource.

IV. Math

A. *Reference Point Detection*

Step1: Compute the cosine and sine of orientation. Let the resulting matrices be a and b.
Step2: Apply gradient operator to both matrices.
Step3: Compute norms of these gradients. Let the resulting matrices be Ga and Gb.
Step4: Compute the global gradient matrix G which has minimum value between Ga and Gb.
Step5: Determine the maximum value of G as V.
Step6: Take all the points that are local maxima whose value is >=0.3V.
Step7: From that list of points, determine the point which is closest to the centre of mass of the region of interest.

B. *Algorithm for termination*

1: Break the image pixel in 3X3 window. matlab code fun=@minutiae; L = nlfilter(K, [3 3], fun);
2: while all 3X3 windows are not computed repeat steps 3 and 4

DOI : 10.35291/2454-9150.2019.0328

3: check if central pixel has only one neighbor
4: Mark it as red circle in image and store its location attributes.
5: end

C. *Algorithm for Bifurcation*

1: Break the image pixel in 3X3 window. matlab code fun=@minutiae; L = nlfilter (K, [3 3], fun);
2: while all 3X3 windows are not computed repeat steps 3 and 4
3: check if central pixel has three neighbor pixels
4: Mark it as green circle in image and store its location attributes.
5: end.

D. *Algorithm for Minutiae extraction*

• Minutiae are special points on ridges:

– Ridge bifurcation (3 neighbors are black)

– Ridge ending (1 neighbor is black)

• Direction of a ridge ending:

– Trace the associated ridge with a fixed distance (say 10 pixels) from x to a. The direction xa is the minutia direction.

• Direction of a bifurcation:

– Trace the ridges to get three directions. The direction is the mean of the two smallest

F *Minutiae position alignment*

Let Ra and Rb be the reference points of left and right fingerprints respectively. Let it be located at ra and rb and have angles a and b respectively. Alignment of minutiae points is done by translating and rotating each point Pib to Pic by

$$(P_{ic})^T = H.(P_{ia} - r_a)^T + (r_b)^T \qquad (5)$$

where H is the rotation matrix defined by

$$H = \begin{bmatrix} Cos(\beta_b - \beta_a) & Sin(\beta_b - \beta_a) \\ -Sin(\beta_b - \beta_a) & Cos(\beta_b - \beta_a) \end{bmatrix} \qquad (6)$$

F *Minutiae direction assignment*

To each aligned minutiae point a new direction is assigned by

where ρi is an integer whose value is either 1 or 0 and OA is the orientation of fingerprint image left thumb.

H *Algorithm for Minutiae verification*

• That method considers only 3 × 3 window, producing false minutiae due to:

– Artifacts in image processing

– Noise in a fingerprint

• A minutia is classified as false if it meets any of the following conditions:

– have no adjacent ridge on either side

– be close in location and opposite in direction

– Too many minutiae in a small neighborhood

I *Generalized Hough transform*

GHT is a well known method for aligning two sets of minutiae:

• For every possible pair of minutiae, compute the transformation parameter and cast a vote in the parameter space.

• Find the peak in the parameter space.

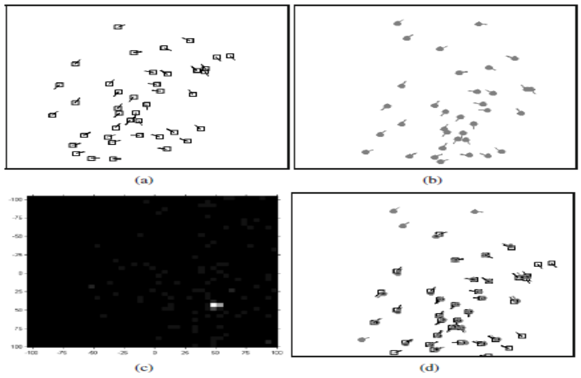


Fig 2 Transform

J *Pairing minutiae*

• When two minutiae sets are aligned, the corresponding minutiae are paired.

• A minutia in is paired with minutia in database.

– Their distance is within predefined distance threshold;

– The angle between their directions is within predefined angle threshold.

K *Match score generation*

• Matched minutiae and match scores of a genuine match and an imposter match using a commercial matcher, Verification of Finger.

• The match scores are computed by some function of # matched minutiae, # missed minutiae, distortion, and some other features that are proprietary.

FRR & FAR CALCULATIONS

$$FAR = FPR = \frac{FP}{FP + TN}$$

$$FRR = FNR = \frac{FN}{TP + FN}$$

System implementation Outcomes

DOI : 10.35291/2454-9150.2019.0328

Table No 1 Result Outcomes for FRR, FAR & GAR

S.N.	FRR %	FAR %	GAR %
1	0.0015	0.0172	99.9985
2	0.0015	0.011	99.9985
3	0.0015	0.0161	99.9985
4	0.0015	0.01	99.9985
5	0.0015	0.0118	99.9985
6	0.0015	0.017	99.9985
7	0.0015	0.0155	99.9985
8	0.0031	0.0207	99.9969
9	0.0015	0.0206	99.9985
10	0.0015	0.0256	99.9985
11	0.0015	0.0186	99.9985
12	0.0015	0.0181	99.9985
13	0.0015	0.0166	99.9985
14	0.0015	0.0201	99.9985
15	0.0031	0.0174	99.9969
16	0.0015	0.0187	99.9985
17	0.0015	0.0145	99.9985
18	0.0031	0.0205	99.9969
19	0.0015	0.0159	99.9985
20	0.0015	0.0178	99.9985
21	0.0015	0.019	99.9985
22	0.0015	0.0146	99.9985
Avg.	**0.0015**	**0.0164**	**99.9982**

From above observation it is cleared that, practical performance give result of FRR = 0.0015%, FAR = 0.0164% & GAR = 99.9982%.

Table Analysis

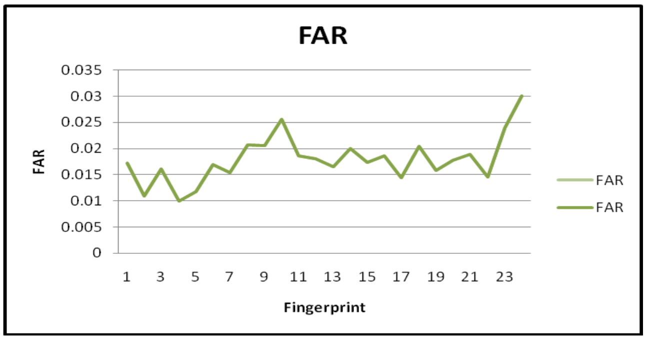


Fig 3 False Acceptance Rate

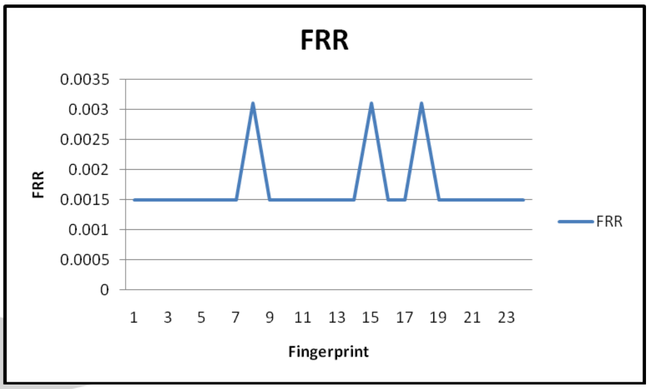


Fig 4 False Rejection Rate

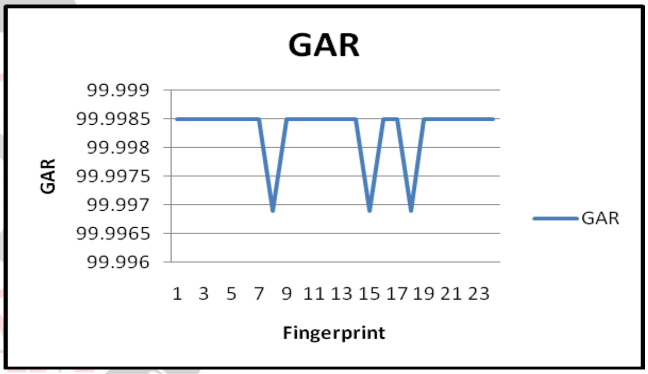


Fig 5 Genuine Acceptance Rate

V. The System Output

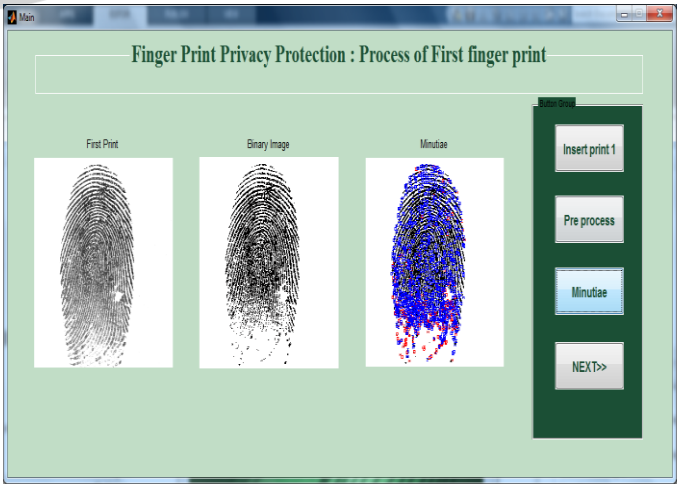


Fig 6 Minutiae of binary image

Analysis – First fingerprint is captured & converted into binary image then from this binary image minutiae's are detected using minutia based algorithm.

DOI : 10.35291/2454-9150.2019.0328

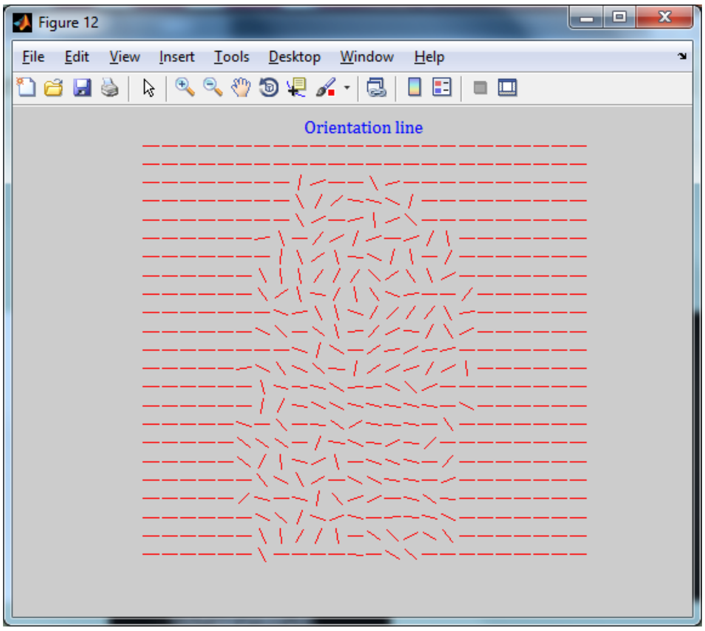


Fig 7 Orientation

Analysis –from second fingerprint orientation is detected.

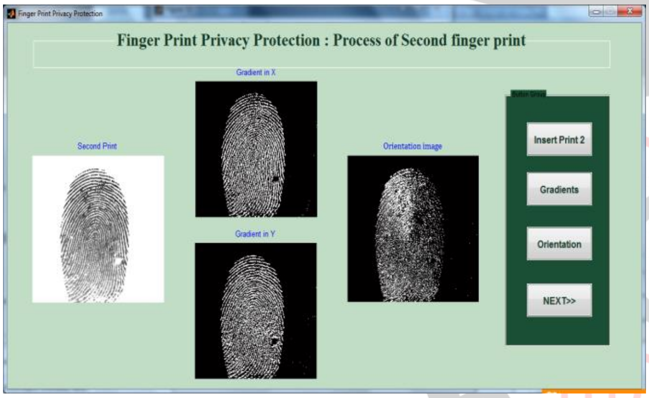


Fig 8 Orientation Image

Analysis –From second fingerprint X-gradient & Y-gradient are captured. According to X,-Y Gradient orientation is detected.

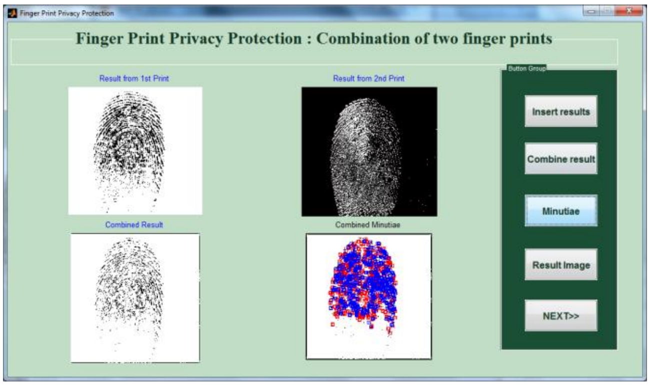


Fig 9 Minutiae Image

Analysis –Both the fingerprints are fused together to form combined template . after combination again minutiae's are the combined fingerprints are captured.& it will proceed further to remove the noise.

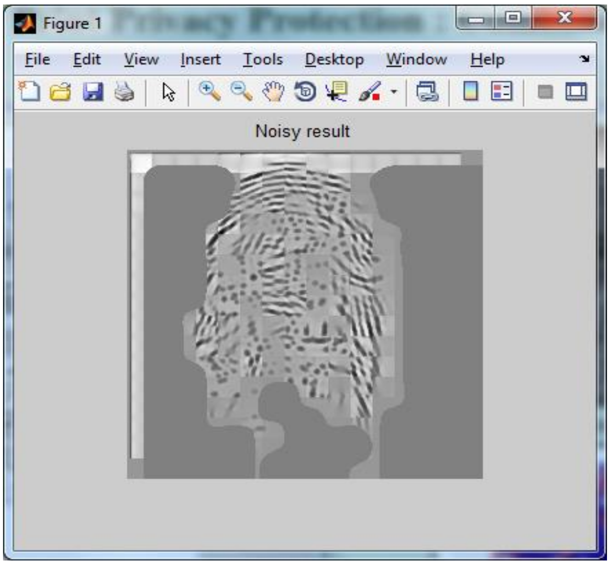


Fig 10 Output Image 1

Analysis –combined fingerprint template is now ready to store into the database.

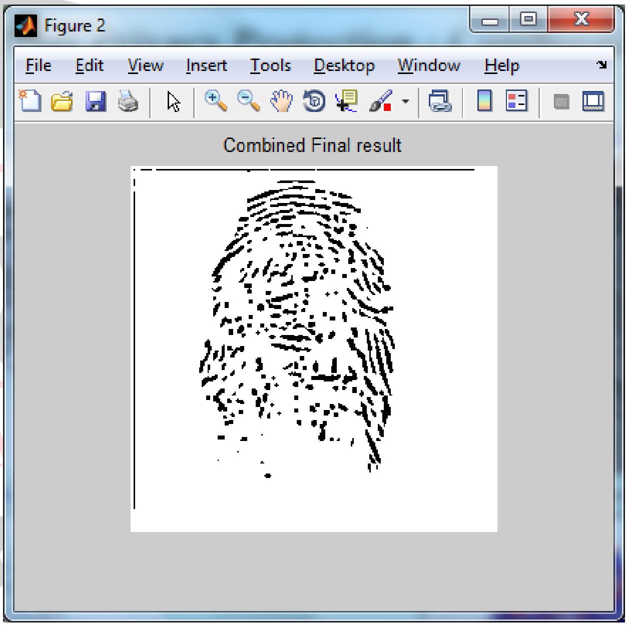
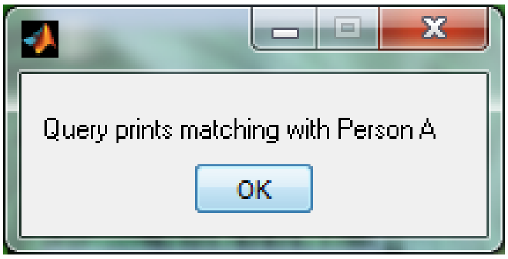


Fig 11 Output Image 1

Analysis –Noise from the combined fingerprint is removed using Gabor filter



Query prints matching with Person A

Fig 12 Matching

Analysis –At the end during authentication system will ask for two fingerprint after authenticating both the fingerprints, System will show above matching output.

DOI : 10.35291/2454-9150.2019.0328

A. Figures and Tabless

Figures:-

Tables:

VI. Conclusion

In this paper, we introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrolment, 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:

1. A very low error rate **with FRR=0.001 at FAR=0.01.**
2. It is also difficult for an attacker to break other traditional systems by using the combined minutiae templates.
3. 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.
4. 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.

Acknowledgment

I have taken a lot of efforts for this project. However, it would not have been possible without the kind support and help of many individuals. I would like to extend my sincere thanks to all of them. I would like to express my appreciation to my project guide Prof. Zainab Mizwan for her continuous support for my project study. Her guidance helped me in all the time of research and writing this paper.

References

[1] Robust Combination Method for Privacy Protection Using Fingerprint and Face Biometrics Miss Dhanashri J. Ghate, Mrs. Savitri B. Patil 2015 IEEE.

[2] Finger Print Combination for Privacy Protection and Security By Kanagala Surya Chaitanya1, Ch. Cury2 August-2015.

[3] Sheng Li Student Member, IEEE, and Alex C. Kot, Fellow, IEEE," Fingerprint Combination for Privacy Protection", IEEE transactions on information forensics and security, vol. 8, no.2, February 2013.

[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] A. Ross and Othman," Mixing fingerprints for templates security and privacy" in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain,29 August - 2 September, 2011.

[6] "Combined Fingerprint Verification for Privacy Protection" D.Sriganesh^1 , B.Baskar^2, K.Somasundaram3, C.Janani^4 B.Tech, Department of Electronic and Communication Engineering, Dr. S.J.S Paul Memorial College of Engineering and Technology, Pondicherry, India^1 2 3 Assistant Professor, Department of Electronic and Communication Engineering, Dr. S.J.S Paul Memorial College of Engineering and Technology, Pondicherry, India^4.

[7] "Fingerprint Image Enhancement: Algorithm and Performance Evaluation" Lin Hong, Student Member, IEEE, Yifei Wan, and Anil Jain, Fellow, IEEE, IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 20, NO. 8, AUGUST 1998.

[8] "Localization of corresponding points in fingerprints by complex filtering" Kenneth Nilsson, Josef Bigun School of Information Science, Computer and Electrical Engineering (IDE) Halmstad University, P.O. Box 823, SE-301 18 Halmstad, Sweden. Kenneth.Nilsson@ide.hh.se, Josef.Bigun@ide.hh.se.

DOI : 10.35291/2454-9150.2019.0328

[9] “Impact of Singular Point Detection on Fingerprint Matching Performance” Sharat Chikkerur Center for Unified Biometrics and Sensors University at Buffalo, NY, USA ssc5@cubs.buffalo.edu , Nalini Ratha IBM T. J. Watson Research Center Hawthorne, NY, USA ratha@us.ibm.com .

[10] “Fingerprint Minutiae Matching Based on the Local And Global Structures” Xudong Jiang and Wei-Yun Yau Centre for Signal Processing, Nanyang Technological University exdjiang@ntu.edu.sg.

[11] [Online] Website:-in.mathworks.com.

[12] [Online] Website:-www.ed.ac.uk.

[13] "An Approach to Fingerprint Image Pre-Processing" ,Om Preeti Chaurasia Amity School of Engineering and Technology, Amity University, Noida, India E-mail: preeti.princy.chaurasia@gmail.com I.J. Image, Graphics and Signal Processing, 2012, 6, 29-35 Published Online July 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijigsp.2012.06.05.

[14] Multimodal Biometric Identification System Using Fusion of Random Subset of Biometrics.

[15] MATLAB® Documentation:-The Language of Technical Computing .

[16] [Online] Website:- https://cimss.ssec.wisc.edu.

[17] [Online] Website:- https://www.wlu.edu/geology-department.

[18] [Online] Website:- www.the-ngsheer.

[19] [Online] Website:- www.ec.bgu.ac.in.

[20]"Biohashing two factor authentication featuring fingerprint data and tokenised random number (2004)", Author Name: B. J. A. Teoh, C. L. D. Ngo, and A. Goh.

[21]"Biometric Template Transformation: A Security Analysis (2010)", Author Name: A. Nagar, K. Nandakumar, and A. K. Jain.

[22] "Mixing fingerprints for template security and privacy (2011)" ' Author Name: A. Ross and A. Othman.

[23] "Multi-biometric Templates Using Fingerprint and Voice (2008)" ' Author Name: E. Camlikaya, A. Kholmatov, and B. Yanikoglu.
[24] "Fingerprint Recognition", Jianjiang Feng ,

Department of Automation,Tsinghua University

,jfeng@tsinghua.edu.cn.

DOI : 10.35291/2454-9150.2019.0328