FINGERPRINT BASED ATTENDANCE SYSTEM TO ENHANCE SECURITY

KIRUTHIKA R[#1], SARANYA M[#2]
[12]*PG Scholar*
R.V.S College Of Engineering And Technology
Coimbatore, TamilNadu,
India
[1]kiruthika.t.radhakrishnan@gmail.com
[2]m.saramya7591@gmail.com

Abstract-Fingerprint matching algorithms system is used for protecting fingerprint Privacy by combining two different fingerprints into a new Identity. To mix two fingerprints, each fingerprint is decomposed into two different components. 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. In the enrollment, two fingerprints are captured from two different fingers. The extraction minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored in a database. Thus, a new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based fingerprint matching algorithms. Experimental results show that this method is feasible in the cases where the privacy of the data is more important than the accuracy of the system and the obtained computational time is satisfactory.

Keywords **- Combined Minutiae Template Generation, Query Minutiae Determination, and Two-Stage Fingerprint Matching.**

I. INTODUCTION

A fingerprint is the pattern of ridges and valleys; each individual has fingerprints [1]. The uniqueness of a fingerprint is exclusively by the local ridge characteristics ad their relationships. The two most prominent local ridge characteristics, called minutiae, are the ridge ending and the ridge bifurcation unique. The first is defined as the point where a ridge ends abruptly. The second is defined as the point where a ridge forks or diverges into branch ridges. In the concept of combining two different fingerprints into a new identity is first proposed, where the new identity is created by combining the minutiae positions extracted from the two fingerprints. The original minutiae positions of each fingerprint can be protected in the new identity. However, it is easy for the attacker to identify such a new identity because it contains many more minutiae positions than that of an original fingerprint [13]. Each fingerprint is decomposed into the continuous component and the spiral component based on the fingerprint FM-AM model. After some alignment, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint, so as to create a new virtual identity which is termed as a mixed fingerprint [2]. 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. The template will be stored in a database for the authentication which requires two query fingerprints. A two-stage fingerprint matching process is further proposed for matching the two query fingerprints against a combined minutiae template. By using the combined minutiae template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen.

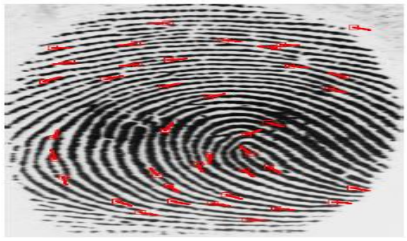


Fig 1. Fingerprint Minutiae Detection

The advantages of our technique over the existing fingerprint combination techniques are as follow[10]:

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

ii) 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.

iii) 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. This will be successful if the matching score is over a predefined threshold.

II. METHODS

1. EXISTING SYSTEM

A. Combined Fingerprint Generation:

In a combined minutiae template, the minutiae positions and directions (after modulo) are extracted from two different fingerprints separately. These minutiae positions and directions share a similar topology to those from an original fingerprint[3]. Therefore, the combined minutiae template has a similar topology to an original minutiae template.

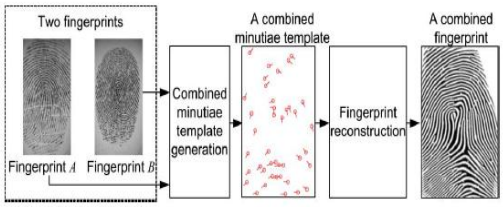


Fig 2. Generating a combined fingerprint for two differentfingerprints

To create a real-look alike fingerprint image from a set of minutiae points, this process can apply a noising and rendering step after adopting the work in, where the following 7 stages are carried out[14]:

i) Estimate an orientation field from the set of minutiae points by adopting the orientation reconstruction algorithm.

ii) Generate a binary ridge pattern based on and a predefined fingerprint ridge frequency (which is set as 0.12) using Gabor filtering.

iii) Estimate the phase image of the binary ridge pattern using the fingerprint FM-AM model.

iv) Reconstruct the continuous phase image by removing the spirals in the phase image.

v) Combine the continuous phase image and the spiral phase image (calculated from the minutiae points), producing a reconstructed phase image.

vi) Refine the reconstructed phase image by removing the spurious minutiae points to produce a refined phase image.

vii) Apply a noising and rendering step (which is similar to the work proposed in), so as to create a real-look alike fingerprint image.

B. *Evaluating The Performance Of The Combined Fingerprints:*

In this section, the performance of our combined fingerprints can be compared with the mixed fingerprints generated by the proposed technique (hereinafter referred to as the mixed fingerprints for simplicity)[4]. The VeriFinger is adopted for matching two combined fingerprints or two mixed fingerprints. We use the same 10 groups of 50 no overlapped finger pairs that are randomly paired at the beginning. For each group of finger pairs, we consider the same two cases for enrollment[9]:

1) The first impressions of each finger pair are used to produce only one combined fingerprint for enrollment. The corresponding second impressions

are used to generate a query combined fingerprint. The query combined fingerprint will be matched against its counterpart enrolled in the database to

compute the FRR, producing 50 genuine tests. The FAR is computed by matching an enrolled combined fingerprint against other 49 enrolled combined fingerprints, producing imposter tests, where the symmetric imposter tests are not executed.

2) The first impressions of each finger pair are used to produce two combined fingerprints for enrollment. The corresponding second impressions are used to generate two query combined fingerprints. Similarly, we have 100 genuine tests and imposter tests. The above evaluation is also performed by using the mixed fingerprint approach for comparison.

Note that the work in does not incorporate a noising and rending step to create the mixed fingerprints. Therefore, in order to do a fair comparison, all our combined fingerprints are created without noising and rendering.

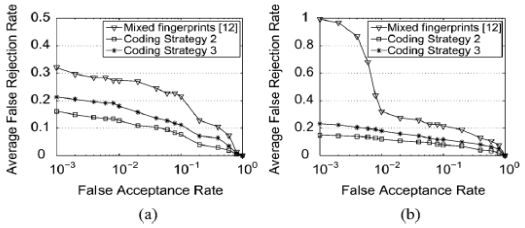


Fig 3. Performance comparison between the combined fingerprints and the mixed fingerprints for (a) Case I, and (b) Case II.

The poor performance of the mixed fingerprints approach for Case II is due to the small overlapping area of some finger pairs. The two mixed fingerprints generated by such a finger pair will be quite similar, which may produce a very high imposter matching score.

C. Evaluating The Probability To Attack Other Systems By Using The Combined Minutiae Templates:

In this section, the evaluation can achieved the successful rates to attack other traditional systems by using the combined minutiae templates[15]. Assume that the attacker can do a perfect job to reconstruct a full fingerprint image from combined minutiae template, i.e., the minutiae of the reconstructed fingerprint is exactly the same as the combined minutiae template.

1) The combined minutiae template is used to attack the system which stores the corresponding fingerprint (mainly provides the minutiae positions).

2) The combined minutiae template is used to attack the system which stores the corresponding fingerprint (mainly provides the minutiae directions).

Fig 4. Different types of new identities that are generated from two different fingerprints.

For simplicity, the above two types of attacks are termed as Attack Type A and Attack Type B, respectively. Suppose the 10 databases built for Case II are stolen, where each database contains 100 combined minutiae templates[16]. To evaluate the successful rates of the two types of attacks, each stolen template is matched against the corresponding fingerprint and fingerprint using the VeriFinger, respectively. Thus, we have 1000 matches for Attack Type A and 1000 matches for Attack Type B. Again, in order to compare with the work , the same evaluation is performed by using the mixed fingerprint approach.

2. PROPOSED SYSTEM

A. Fingerprint Privacy Protection System:

A fingerprint can be viewed as an oriented texture pattern. A fingerprint image, they demonstrate that a compact and reliable translation- and rotation-invariant representation can be built based entirely on the inherent properties of the underlying fingerprint texture[5]. They further illustrate that the representation thus derived, is useful for robust discrimination of the fingerprints.

In the enrollment phase, the system captures two fingerprints from two different fingers, say fingerprints A' and B' from fingers A and B respectively. The extraction of minutiae positions from one fingerprint and the orientation from another fingerprint using some existing techniques .Then, by using the proposed coding strategies, a combined minutiae template is generated based on the minutiae positions, the orientation and the reference points detected from both fingerprints[17]. Finally, the combined minutiae template is stored in a database.

In the authentication phase, two query fingerprints are required from the same two fingers, say fingerprints A' and B' from fingers A and B .This can be done which is similar to the enrollment phase. This extracted information will be matched against the corresponding template stored in the database by using a two-stage fingerprint matching. The authentication will be successful if the matching score is over a predefined threshold

1) Biohashing: The biometric features are transformed using a function defined by a user-specific key or password. Usually this transformation is invertible. This system is based on the face, but similar techniques can be applied to different biometric traits (e.g. iris and fingerprint).

2) Noninvertible transform: The biometric template I secured by applying an on invertible transformation function to it. There are methods based on different biometric traits.For example, it is used in the fingerprint, and in the iris. The main problem is that it is necessary to study the tradeoff between discriminability and noninvertibility of the transformation function. This is presented a study on the measurement of the noninvertibility of methods based on the fingerprint.

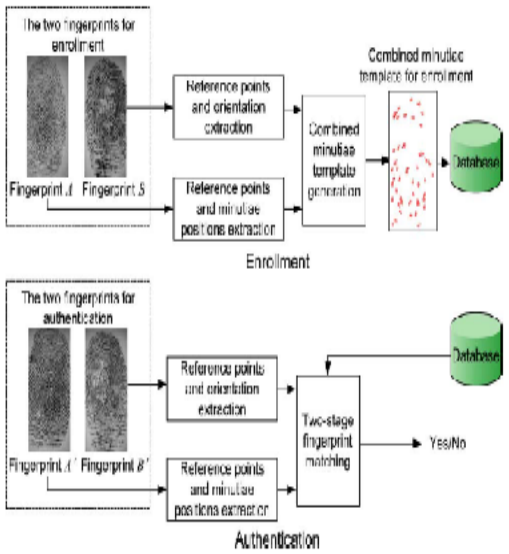


Fig 5. Proposed fingerprint privacy protection system

3) Key-binding biometric cryptosystem: The template is secured by applying cryptographic algorithms. Usually, the system must compute a transformation of the encrypted templates in the plain domain. This task is usually time expansive. Examples of methods used by this approach are the fuzzy commitment scheme and the fuzzy vault.

4) Key generating biometric cryptosystem: These methods compute the cryptographic key directly from the biometric data. The main problem is that it is difficult to generate keys with high stability and entropy.

B. Combined Minutiae Template Generation:

A combined minutiae template is generated by minutiae position alignment and minutiae direction assignment[7].

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 for fingerprints respectively.

2) Minutiae Direction Assignment: Each aligned minutiae position is assigned with a direction. The range is from 0 to π. Therefore, the range of will the same as that of the minutiae directions from an original fingerprint.

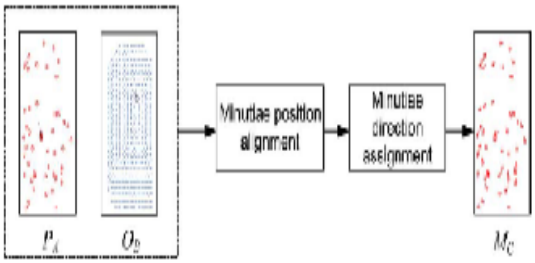


Fig 6. Combined minutiae template generation process

C. Two-Stage Fingerprint Matching:

Give minutiae positions of one fingerprint, the orientation of another fingerprint and the reference points of the two query fingerprints[9]. In order to match the stored database, this can be proposed by a two-stage fingerprint matching process including query minutiae determination and matching score calculation.

i) Query Minutiae Determination: The query minutiae determination is a very important step during the fingerprint matching[12]. In order to simplify the description of our algorithm, we first introduce the local features extracted for a minutiae point.

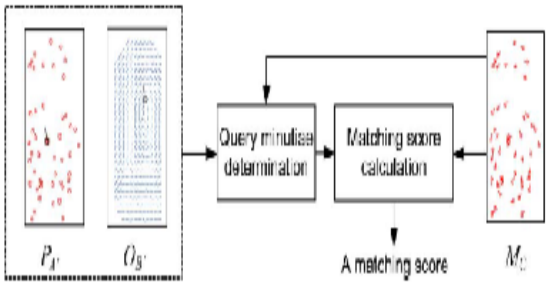


Fig 7. Two-stage fingerprint matching process

ii) Matching Score Calculation: For the combined minutiae templates those are generated using Coding Strategy by using modulo concept for all the minutiae directions, so that the randomness can be removed easily. After the modulo operation, this concept use an existing minutiae matching algorithm to calculate a matching score between the authentication decision[8]. For other combined minutiae templates, this can be directly used to calculate a matching score between an existing minutiae matching algorithm.

III. RESULT AND DISCUSSION

In the experiment, Equal Error Rate (EER) was used to evaluate the system performance of the proposed method[18]. The experimental results reveal that our system identifies the most of minutiae present in the original acquired image. However the final number of minutiae obtained depends heavily of the acquired system.

SCREENSHOTS:

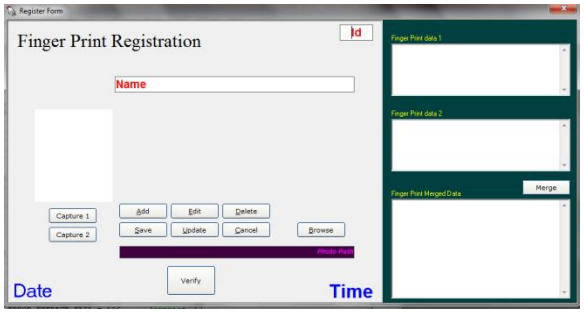
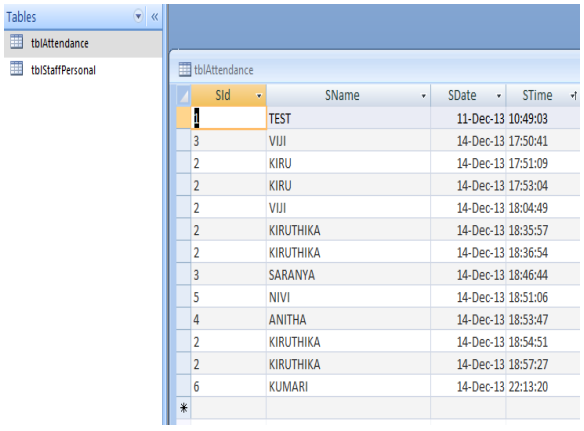


Fig 8. Finger Print Registration

This screenshot shows the registration form for the finger print to register the details of the particular person.



SId	SName	SDate	STime
1	TEST	11-Dec-13	10:49:03
3	VIJI	14-Dec-13	17:50:41
2	KIRU	14-Dec-13	17:51:09
2	KIRU	14-Dec-13	17:53:04
2	VIJI	14-Dec-13	18:04:49
2	KIRUTHIKA	14-Dec-13	18:35:57
2	KIRUTHIKA	14-Dec-13	18:36:54
3	SARANYA	14-Dec-13	18:46:44
5	NIVI	14-Dec-13	18:51:06
4	ANITHA	14-Dec-13	18:53:47
2	KIRUTHIKA	14-Dec-13	18:54:51
2	KIRUTHIKA	14-Dec-13	18:57:27
6	KUMARI	14-Dec-13	22:13:20

Fig 9. Database Storage

This screenshot shows the database storage for attendance details by capturing their fingerprint and the current date and time will be displayed.

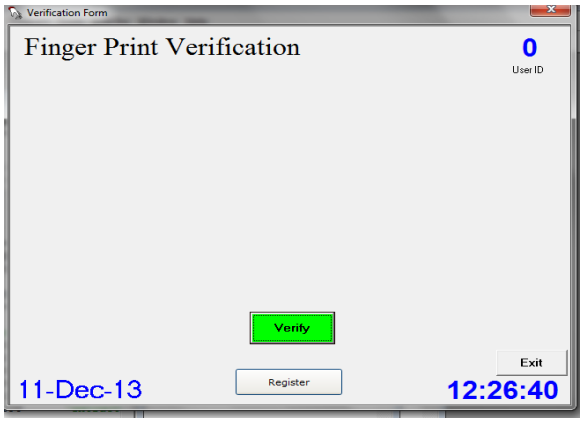


Fig 10. Verification Form

This screenshot shows the verification form to verify whether the access is granted or denied.

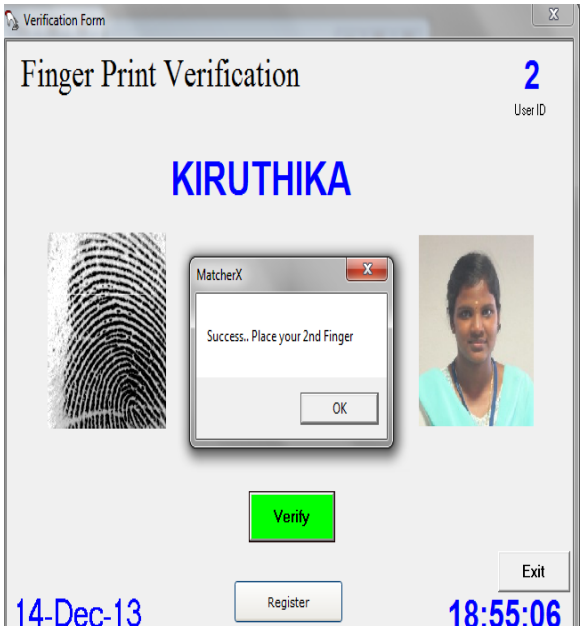


Fig 11. Verification Process For One Fingerprint

This screenshot shows the fingerprint verification step after placing our first finger.

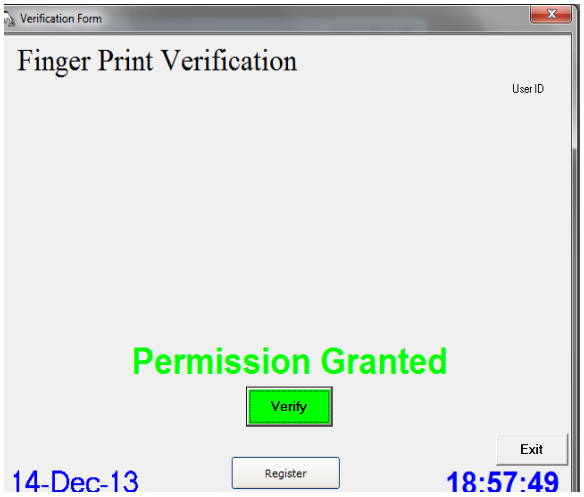


Fig 12. Verification Process For Another Fingerprint

This screenshot shows the verification step for second fingerprint. If the verification process is success full then the permission will be granted or the access will be denied.

IV.CONCLUSIONS AND FUTURE ENHANCEMENT

A. Conclusions:

This paper proposes a novel minutiae-based fingerprint matching approach. It is important to recall the objectives of the development of new algorithms suitable for custom designed hardware architecture. The development of a software implementation of these algorithms is used to prove the correctness and suitability for fingerprint images. The study of a hardware architecture design is used to implement the algorithms. The new fingerprint matching algorithms have shown enough correctness to consider this a good path. All the outcomes are shown over the same fingerprint. This fingerprint has been chosen because it presents all the fingerprint features important for the analysis of the different methods. The results show that the extraction of the Delta and Core points and Minutiae has reached promising results at a very low operational complexity.

ACKNOWLEDGMENT

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The authors would like to thank R.V.S College for providing necessary facilities to carry out this work.

REFERRENCES

[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] 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.

[3] K.Ito, H.Nakajima, K.Kobayashi, T.Aoki, and T.Higuchi,"A Fingerprint Matching Algorithm Using Phase-OnlyCorrelation," *IEICE Trans. Fundamentals*, Vol. E87-A, Pp. 682-691, 2004.

[4] D.Maltoni, D.Maio, A.K.Jain, and S.Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer, 2003.

[5] Federal Bureau of Investigation, *The Science of Fingerprints: Classification and Uses*, Washington, D.C., 1984, U.S. Government Printing Office.

[6] 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] 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.

[8] Y. Wang and J. Hu, "Global ridge orientation modeling for partial fingerprint identification," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 1, pp. 72–87, Jan. 2011.

[9] J.Zhang, Z.Ou, and H.Wei, "Fingerprint matching using phase-only correlation and fourier mellin transforms," presented at *The Sixth International Conference on Intelligent Systems Design and Applications (ISDA'06)*, 2006.

[10] J.Feng Fingerprint reconstruction: From minutiae to phase. *PAMI*, 33(2):209 –223, Feb. 2011.

[11] John Berry and David A. Stoney, "The history and development of fingerprinting," in *Advances in Fingerprint Technology*, Henry C. Lee and R.E. Gaensslen, Eds., pp. 1–40. CRC Press, Florida, 2nd edition, 2001.

[12] Anil K. Jain, Salil Prabhakar, Lin Hong, and Sharat Pankanti, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846–859, May 2000.

[13] 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.

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

[15] N. Yager and A. Amin. Fingerprint alignment using a two stage optimization. PRL, 27(5):317–324, 2006.

[16] Y. Zhang, J. Yang, and H. Wu. A hybrid swipe fingerprint mosaicing scheme. In AVBPA, pages 131–140, 2005.

[17] R. Thai. *Fingerprint image enhancement and minutiae extraction*. PhD thesis, CSSE, The University of Western Australia, 2003.

[18] Anil K. Jain, Lin Hong, Sharat Pankanti, and RuudBolle, "An identity authentication system using fingerprints, *"Proceedings of the IEEE*, vol. 85, no. 9, pp.1365–1388, 1997.

