ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

Privacy Improvement for Fingerprint Recognition Based On RSA

Vidya.P[1], Aswathy.R.S[2]

PG Scholar, Dept of Computer Science, Mohandas College of Engg and Technology, Anad ,TVM, Kerala, India[1]

Assistant Professor, Dept of Computer Science, Mohandas College of Engg and Technology, Anad ,TVM, Kerala, India[2]

ABSTRACT: Here proposed an adaptive encryption based privacy improvement for fingerprint recognition. During enrollment, two fingerprints are captured from two different fingers and then extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information a combined minutiae template is generated and stored in a database after performing RSA encryption. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. Here uses FV2002 DB_1 database. A two-stage fingerprint matching process with decision tree classifier is proposed for matching the two query fingerprints against a combined minutiae template. Because of this, it is difficult for the attacker to hack the database and retrieve the fingerprints. By using decision tree classifier the accuracy can be improved with low error rate is expected.

KEYWORDS: Combination, fingerprint, minutiae, privacy, RSA, protection.

I. INTRODUCTION

Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Protecting the privacy of the fingerprint becomes an important issue. Traditional encryption is not sufficient for fingerprint privacy protection. In recent years, significant efforts have been put into developing specific protection techniques for fingerprint.

It has so many applications like Banking Security - ATM security, card transaction, Physical Access Control (e.g. Airport), Information System Security, National ID Systems, Passport control (INSPASS), Prisoner, prison visitors, inmate control, Voting, Identification of Criminals, Identification of missing children, Secure E-Commerce (Still under research)etc. So protection of fingerprint database is a serious issue. Most of the existing techniques make use of the key for the fingerprint privacy protection, which creates the inconvenience. They may also be vulnerable when both the key and the protected fingerprint are stolen.

II. LITERATURE REVIEW

The works in [10]–[12] combine two different fingerprints into a single new identity either in the feature level [10] or in the image level [11], [12]. In [10], 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. Fig 1.1 shows the various minutiae points int the fingerprint. 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.

In [11], [12], the authors first propose to combine two different fingerprints in the image level. First of all, each fingerprint is decomposed into the continuous component and the spiral component based on the fingerprint FM-AM model [14]. 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.

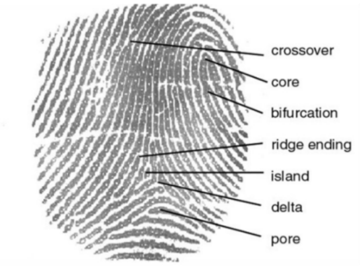


Fig.1.1 Minutiae feaatures

In this paper, propose an adaptive system for protecting fingerprint privacy by combining two different fingerprints into a new identity and assuring more security by using RSA encryption. During the enrollment, the system captures two fingerprints from two different fingers and then it is combined to form a new 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.

A two-stage fingerprint matching process is used 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. But in [1] it is said that in case the combined minutiae templates are stolen, the attacker can use them to attack other traditional systems which store the original fingerprints. He can reconstruct a fingerprint image from a stolen combined minutiae template and make a fake finger based on the reconstructed fingerprint. By scanning the fake finger, the attacker may be able to break into other traditional systems. Similarly, if a combined fingerprint or a mixed fingerprint is stolen, the attacker can directly make a fake finger from the fingerprints and launch the attack. Using this proposed method this disadvantage can be removed by providing more security using RSA.

III. THE PROPOSED FINGERPRINT PRIVACY PROTECTION SYSTEM

In the enrollment phase, the system captures two fingerprints from two different fingers, say fingerprints A and B. from fingers and, respectively. Fig 2 shows the proposed system. First extract the minutiae positions from fingerprint and the orientation from fingerprint using some existing techniques [16], [17]. Then, by using proposed coding strategies, a combined minutiae template is generated based on the minutiae positions, the orientation and the reference points detected from both fingerprints. Finally, the combined minutiae template is stored in a database after encryption using RSA. In the authentication phase, two query fingerprints are required from the same two fingers, say fingerprints A’ and B’ from fingers A and B. As in the enrollment, extract the minutiae positions from fingerprint A’ and the orientation from fingerprint B’. Reference points are detected from both query fingerprints. 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. Before all steps the pre- processing steps are done such as normalization, contrast enhancement, masking, filtering etc. Thus more clear ridges can be obtained.

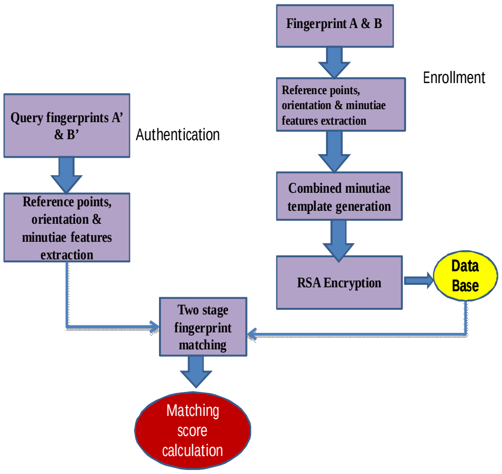

Fingerprint A & B
Enrollment
Reference points, orientation & minutiae features extraction
Combined minutiae template generation
RSA Encryption
Data Base
Query fingerprints A' & B'
Authentication
Reference points, orientation & minutiae features extraction
Two stage fingerprint matching
Matching score calculation

Fig. 3.1 Proposed fingerprint privacy protection system.

A. *Reference point detection*

The reference points detection process is motivated by Nilsson et al. [18], who first propose to use complex filters for singular point detection. Fig3 shows the extracted minutiae points of two fingerprints. Given a fingerprint, the main steps of the reference points detection are summarized as follows:

1) Compute the orientation from the fingerprint using the orientation estimation algorithm proposed in [17].
2) Calculate a certainty map of reference points [18]
3) Calculate an improved certainty map [19]
4) Locate a reference point satisfying the two criterions:
(i)the amplitude of the point is a local maximum, and
(ii) the local maximum should be over a fixed threshold .
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.

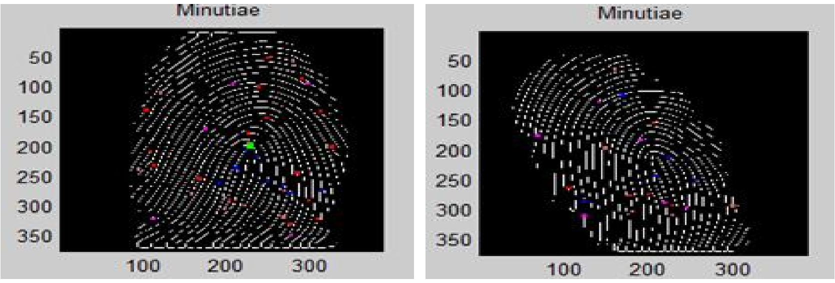
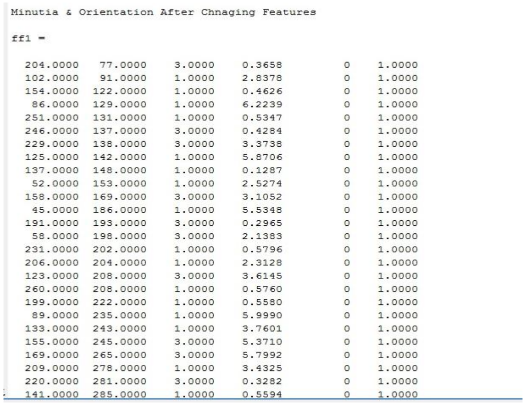


Fig. 3.2. Minutiae points of selected two fingerprints are extracted.

B. Combined Minutiae Template Generation

A combined minutiae template is generated by minutiae position alignment and minutiae direction assignment. The alignment is performed by translating and rotating each minutiae point. Each aligned minutiae position is assigned with a direction.



```
Minutia & Orientation After Chnaging Features

ff1 =

  204.0000   77.0000    3.0000    0.3658         0    1.0000
  102.0000   91.0000    1.0000    2.8378         0    1.0000
  154.0000  122.0000    1.0000    0.4626         0    1.0000
   86.0000  129.0000    1.0000    6.2239         0    1.0000
  251.0000  131.0000    1.0000    0.5347         0    1.0000
  246.0000  137.0000    3.0000    0.4284         0    1.0000
  229.0000  138.0000    3.0000    3.3738         0    1.0000
  125.0000  142.0000    1.0000    5.8706         0    1.0000
  137.0000  148.0000    1.0000    0.1287         0    1.0000
   52.0000  153.0000    1.0000    2.5274         0    1.0000
  158.0000  169.0000    3.0000    3.1052         0    1.0000
   45.0000  186.0000    1.0000    5.5348         0    1.0000
  191.0000  193.0000    3.0000    0.2965         0    1.0000
   58.0000  198.0000    3.0000    2.1383         0    1.0000
  231.0000  202.0000    1.0000    0.5796         0    1.0000
  206.0000  204.0000    1.0000    2.3128         0    1.0000
  123.0000  208.0000    3.0000    3.6145         0    1.0000
  260.0000  208.0000    1.0000    0.5760         0    1.0000
  199.0000  222.0000    1.0000    0.5580         0    1.0000
   89.0000  235.0000    1.0000    5.9990         0    1.0000
  133.0000  243.0000    1.0000    3.7601         0    1.0000
  155.0000  245.0000    3.0000    5.3710         0    1.0000
  169.0000  265.0000    3.0000    5.7992         0    1.0000
  209.0000  278.0000    1.0000    3.4325         0    1.0000
  220.0000  281.0000    3.0000    0.3282         0    1.0000
  141.0000  285.0000    1.0000    0.5594         0    1.0000
```

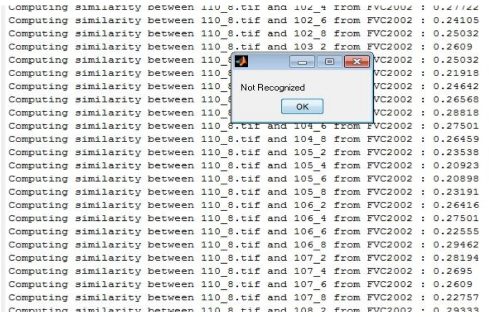
Fig. 3.3. Combining features of two fingerprints

C. Two-Stage 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, here uses a two-stage fingerprint matching process including query minutiae determination and matching score calculation.

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, first the local features are extracted for a minutiae point. In [1] Euclidean distance matching is used for matching. Here I am supposed to use decision tree classifier for getting better result with low error rate. I think that it should give low FAR rate than the existing method.

2) *Matching Score Calculation:* Here a matching score is calculated and if it is under a threshold value then that person will be authenticated to that particular system.



```
Computing similarity between 110_8.tif and 102_4 from FVC2002 : 0.27722
Computing similarity between 110_8.tif and 102_6 from FVC2002 : 0.24105
Computing similarity between 110_8.tif and 102_8 from FVC2002 : 0.25032
Computing similarity between 110_8.tif and 103_2 from FVC2002 : 0.2609
Computing similarity between 110_8                         VC2002 : 0.25032
Computing similarity between 110_8                         VC2002 : 0.21918
Computing similarity between 110_8                         VC2002 : 0.24642
Computing similarity between 110_8                         VC2002 : 0.26568
Computing similarity between 110_8                         VC2002 : 0.28818
Computing similarity between 110_8.tif and 104_6 from FVC2002 : 0.27501
Computing similarity between 110_8.tif and 104_8 from FVC2002 : 0.26459
Computing similarity between 110_8.tif and 105_2 from FVC2002 : 0.23538
Computing similarity between 110_8.tif and 105_4 from FVC2002 : 0.20923
Computing similarity between 110_8.tif and 105_6 from FVC2002 : 0.20898
Computing similarity between 110_8.tif and 105_8 from FVC2002 : 0.23191
Computing similarity between 110_8.tif and 106_2 from FVC2002 : 0.26416
Computing similarity between 110_8.tif and 106_4 from FVC2002 : 0.27501
Computing similarity between 110_8.tif and 106_6 from FVC2002 : 0.22555
Computing similarity between 110_8.tif and 106_8 from FVC2002 : 0.29462
Computing similarity between 110_8.tif and 107_2 from FVC2002 : 0.28194
Computing similarity between 110_8.tif and 107_4 from FVC2002 : 0.2695
Computing similarity between 110_8.tif and 107_6 from FVC2002 : 0.2609
Computing similarity between 110_8.tif and 107_8 from FVC2002 : 0.22757
Computing similarity between 110_8.tif and 108_2 from FVC2002 : 0.29333
```

Not Recognized

Fig. 3.4 Computing similarity score of an unauthorized person

D. *Fingerprint reconstruction*

After generating a combined minutiae template it is reconstructed to a new fingerprint so that the attackers cannot identify the technique used.

E. *Protecting the database*

If a combined fingerprint or a mixed fingerprint is stolen, the attacker can directly make a fake finger from the fingerprints and launch the attack. The database will be protected by using encryption technique. I propose to use RSA encryption method to protect the combined fingerprint images in the database. As it is a public key cryptographic technique the attacker can't easily attack the system. Thus more security can be ensured.

IV. DECISION TREE APPROACH

A new approach is implementing for getting more accuracy ie, Decision Tree Classification. It is implementing during two stage fingerprint matching at the authentication step. Decision trees are powerful and popular tools for classification and prediction. Decision trees classify instances or examples by starting at the root of the tree and moving through it until a leaf node. Decision tree performs classification without much computation. Also it can handle continuous and categorical variables.

Here decision trees can be generated according to the distance between minutiae points. The leaf nodes will be generated based on the distance selected as root node. Thus we will get a more accurate decision that is whether the user is an authenticated person or not. By using this here expects low error rate with more accuracy. For this comparison of both approaches will be performed. Thus we can find that the proposed method is better.

V. EXPECTED RESULTS

I am expecting more accuracy with low error rate than the existing method. So the FAR will be very less. Also the attacker cannot attack the database in any means. So it will be more protecting system for the fingerprint database.

VI. CONCLUSION

A novel system for fingerprint privacy protection by combining two fingerprints into a new identity can be implemented with very less error rate. It ensures more security to the database and all fingerprints in the authenticated system.

REFERENCES

[1] 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

[2] 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.

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

[4] 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.

[5] 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.

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

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

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

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

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

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

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

[12] A. Othman and A. Ross, "Mixing fingerprints for generating virtual identities," in *Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS)*, Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

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

[14] 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.

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

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

[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.

[18] 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.

[19] 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.

[20] 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.

[21] X. Jiang andW.Yau, "Fingerprintminutiaematching based on the local and global structures," in *Proc. 15th Int. Conf. Pattern Recognition*, 2000, vol. 2, pp. 1038–1041.

[22] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[23] www.google.com