Privacy Augmenting for Fingerprint detection using RSA

S. Swathi[1*], A. Poojitha Reddy[2], M. Karuna Pavani[3] & B. Devendra Naik[4]

[1] Department of Computer Science and Engineering, G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India

*E-mail: sethlam12.swathi@gmail.com

Abstract:

In this paper we proposed a versatile encryption based protection change for unique fingerprint recognition. Amid enlistment, two fingerprints are caught from two separate fingers and afterward extricate the particulars positions from one unique mark, the introduction from the other finger impression, and the reference focuses from both fingerprints. In view of this concentrated data a consolidated details format is produced and put away in a database in the wake of performing RSA encryption. In the confirmation, the framework obliges two inquiry fingerprints from the same two fingers which are utilized as a part of the enlistment. Here utilizations Fv2002 Db_1 database. A two-stage finger impression matching methodology with choice tree classifier is proposed for matching the two inquiry fingerprints against a joined details format. As a result of this, it is troublesome for the assailant to hack the database and recover the fingerprints. By utilizing choice tree classifier the exactness can be enhanced with low mistake rate is normal.

Keywords:

Combination; fingerprint; minutiae; privacy; RSA; protection

I. Introduction

Fingerprints are one of numerous manifestations of biometrics used to recognize people and confirm their personality. Securing the protection of the unique finger impression turns into a critical issue. Customary encryption is not sufficient for unique mark protection assurance. As of late, critical exertions have been put into creating particular insurance procedures for fingerprint. It has such a large number of uses like Keeping money Security - ATM security, card transaction, Physical Access Control (e.g. Airplane terminal), Information System Security, National ID Systems, Passport control (INSPASS), Detainee, prisoner guests, prisoner control, Voting, Distinguishing proof of Lawbreakers, ID of missing youngsters, Secure E-Business (Still under research)etc. So assurance of finger impression database is a genuine issue. A large portion of the current strategies make utilization of the key for the finger impression protection assurance, which makes the weakness. They might likewise be powerless when both the key and the ensured unique mark are stolen.

Literature Review

The works in [10]–[12] consolidate two separate fingerprints into a solitary new character either in the peculiarity level [10] or in the picture level [11], [12]. In [10], the idea of consolidating two separate fingerprints into another personality is initially proposed, where the new character is made by joining the details positions extricated from the two fingerprints. Fig 1.1 demonstrates the different particulars focuses int the unique finger impression. The first details positions of each one finger impression can be secured in the new character. In any case, it is simple for the assailant to distinguish such another personality in light of the fact that it contains a lot of people more details positions than that of an unique finger impression. In [11], [12], the creators first propose to join two separate fingerprints in the picture level. Above all else, each one finger impression is disintegrated into the consistent segment and the winding part focused around the unique mark FM-AM model [14]. After some arrangement, the ceaseless part of one unique finger impression is joined with the winding segment of the other unique mark, to make another virtual character which is termed as blended unique marks.

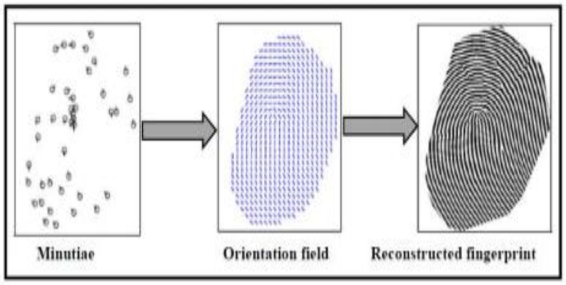

Fig 1. Minutiae features

In this paper, propose a versatile framework for securing finger impression security by joining two separate fingerprints into another character and guaranteeing more security by utilizing RSA encryption. Amid the enlistment, the framework catches two fingerprints from two separate fingers and afterward it is consolidated to structure another from the two fingerprints. In such a format, the details positions are concentrated from one unique finger impression, while the particulars bearings rely on upon the introduction of the other finger impression and some coding systems. The layout will be put away in a database for the confirmation which obliges two inquiry fingerprints. A two-stage unique finger impression matching procedure is utilized for matching the two inquiry fingerprints against a consolidated details layout. By utilizing the consolidated details layout, the complete particulars peculiarity of a solitary unique finger impression won't be bargained when the database is stolen. Be that as it may in [1] it is said that in the event that the consolidated details formats are stolen, the assailant can utilize them to assault other customary frameworks which store the first fingerprints. He can remake a finger impression picture from a stolen joined particulars format and make a fake finger focused around the remade unique mark. By checking the fake finger, the assailant may have the capacity to break into other conventional frameworks. Also, if a consolidated unique mark or a blended finger impression is stolen, the assailant can straightforwardly make a fake finger from the fingerprints and dispatch the assault. Utilizing this proposed system this drawback can be evacuated by giving more security utilizing RSA.

Fingerprint Recognition System

Everybody is known to have remarkable, permanent fingerprints. For confirmation reason, finger impression format is concentrated from unique mark pictures and spared into the focal storehouses. The unique mark distinguishment framework made out of taking after stages: finger impression enrolment, confirmation and finger impression ID. The objective of check is to keep various people from getting to the same personality and it is regularly utilized for constructive distinguishment. Unique mark confirmation is procedure used to check the credibility of one individual by his finger impression. Amid the distinguishing proof stage, the framework perceives an individual via looking the layouts of every last one of clients in the database for a match. The stages confirmation and distinguishing proof both makes utilization of specific plans for finger impression matching this is shown in the accompanying subsection. A] Methods for Unique mark Matching Different finger impression matching systems talked about in writing [13] are as per the following:

- **Minutiae based technique:** Most of the fingerprint authentication systems are based on Minutiae. Minutia based techniques represent the fingerprint by its local ridge characteristics, like ridge endings and bifurcations. This approach is the mainstay of the current available fingerprint authentication systems has been fiercely studied.

- **Image Based Techniques**: This is an advanced and newly emerging method for fingerprint recognition. Image based techniques try to do matching based on the global features of a whole fingerprint image. Image based technique is useful to solve some stubborn problems of the minutiae based approach.

The Proposed Fingerprint Privacy Protection System

In the enlistment stage, the framework catches two fingerprints from two separate fingers, say fingerprints an A and B. from fingers and, individually. Fig 2 demonstrates the proposed framework. Initially extricate the particulars positions from finger impression and the introduction from unique mark utilizing some current strategies [16], [17]. At that point, by utilizing proposed coding methodologies, a consolidated particulars layout is produced focused around the details positions, the introduction and the reference focuses recognized from both fingerprints. At long last, the joined details layout is put away in a database after encryption utilizing RSA. In the confirmation stage, two question fingerprints are needed from the same two fingers, say fingerprints An' and B' from fingers An and B. As in the enlistment, remove the particulars positions from unique mark An' and the introduction from finger impression B'. Reference focuses are recognized from both inquiry fingerprints. This concentrated data will be matched against the relating format put away in the database by utilizing a two-stage unique finger impression matching. The verification will be effective if the matching score is over a predefined limit. Prior to all steps the preprocessing steps are carried out, for example, standardization, contrast improvement, concealing, separating and so forth. Therefore all the more clear edges can be acquired.

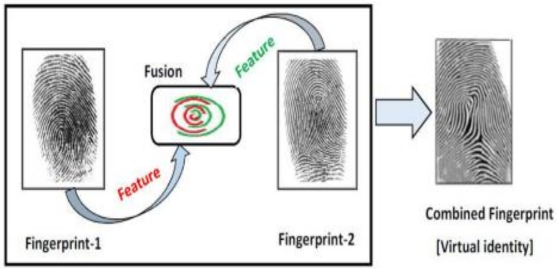

Fig. 2 Proposed fingerprint privacy protection system

A. Reference point detection

The reference point's 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 point's 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 is 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.

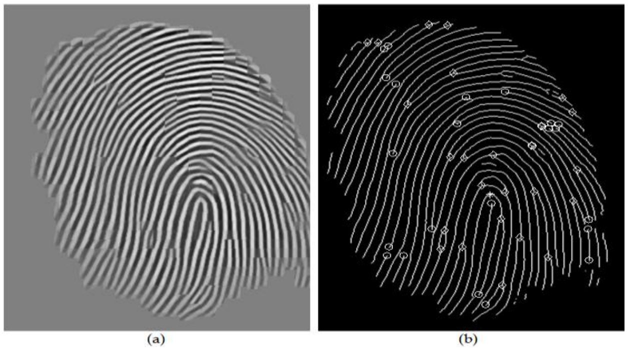

Fig. 3 Minutiae points of selected two fingerprints are extracted.

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.

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 system.

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.

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.

Conclusion

A novel framework for unique mark security assurance by consolidating two fingerprints into another character can be executed with less blunder rate. It guarantees more security to the database and all fingerprints in the validated framework.

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.