IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Fingerprint Combination for Resisting Attacks

Austin J Gladston[1], Ashitha .S.S[2]

Student, Computer Science, Lourdes Matha College of Science and Technology, Trivandrum, India[1]

Assistant Professor, Computer Science, Lourdes Matha College of Science and Technology, Trivandrum, India[2]

Abstract: The success fingerprint combination and their extensive deployment all over the world have prompted some individuals to take extreme measures to evade identification by altering their fingerprints. The problem of fingerprint alteration or obfuscation is very different from that of fingerprint spoofing, where an individual uses a fake fingerprint in order to adopt the identity of another individual. While the problem of spoofing has received substantial attention in the literature, the problem of obfuscation has not been addressed in the biometric literature, in spite of numerous documented cases of fingerprint alteration for the purpose of evading identification. 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. The algorithm based on the features extracted from the orientation field and minutiae satisfies the three essential requirements for alteration detection algorithm.

Keywords: Minutiae, Orientation, Template, Fingerprint combination.

I. INTRODUCTION

Fingerprint recognition systems are considered as one of identification systems with confidence. Commonly used features are ridge orientation, ridge bifurcation, ridge contour, position.

II. LITERATURE REVIEW

Feng and Jain [1] proposed a reconstruction algorithm to reconstruct plain and rolled fingerprints. Such systems are used in recognition systems where same finger is enrolled with different impression. In this method a fingerprint image is represented as a 2D amplitude and frequency modulated signal. The phase is calculated using the steps like orientation field reconstruction, estimation of gradient of continuous phase, continuous phase reconstruction, combination of spiral phase and the continuous phase. The local ridge orientation of each 8*8 block is calculated using nearest minutia in each of the eight sectors. The singular points in the finger print are handled using enhanced techniques to avoid shift of singularity. The reconstructed fingerprints are found to be almost same as original one.

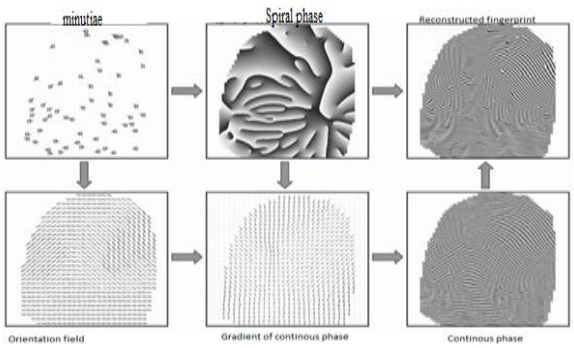

Fig 2.1 Fingerprint reconstruction algorithm

The gradient of continuous phase at each block is obtained from the gradients of composite phase and spiral phase. To avoid discontinuity problems the initial orientation field is unwrapped. To unwrap fingerprints without singularity, depth-first, breadth-first or other techniques are used. A third order polynomial is commonly used to calculate the gradient. Then function is applied to gradient to obtain the explicit function of continuous phase. The reconstructed fingerprints are very smooth without any spurious minutiae. The reconstructed picture is as shown in fig 2.1
In [2], the application of fuzzy vault for fingerprints is used. But a single finger never contains sufficient information for secure implementation's minutiae data of several finger prints are used to improve security. The stored minutiae are hidden as a set of chaff points. A polynomial is used to encode the biometric data. The query is changed as a set of attributes, which is compared with the stored fuzzy vault using Reed-Solomon decoding.

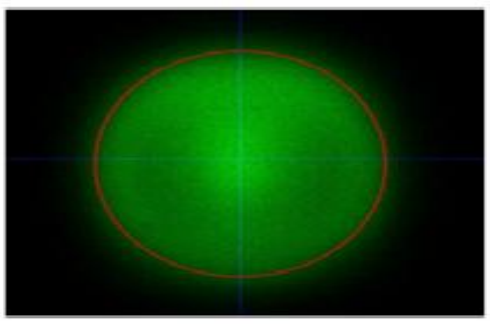

Fig 2.2 minutiae distribution

This fuzzy vault technique is error tolerant. To improve the correctness of the recovered polynomial, a hash value of polynomial's coefficient is used. The minutiae of all fingers are stored as a feature vector in encoded form. To

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

get optimized result a restriction is placed on the area of finger print. Only reliable fingerprints minutiae feature vectors are allowed to be inserted into the data base. The minimum Euclidean distance from genuine minutiae to the chaff points are considered during retrieval process. The pre-alignment algorithm scales down the fingerprint image and uses a threshold on pixel brightness to obtain the image displaying the shape of fingerprint. The cross matching of the vaults from several independent enrolments of a user remains as a serious threat to fuzzy vault. The result is as shown in the fig 2.2.

Another approach for fingerprint protection is combining the features of two fingerprints as shown in fig 2.3,2.3.1[3].The minutiae features of one finger is combined with the orientation features of another finger to create a new identity.

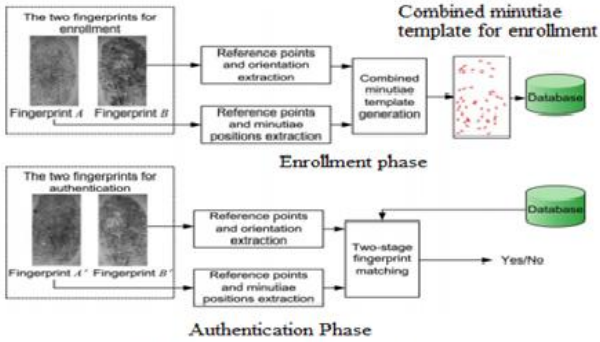

Fig 2.3 Enrollment And Authentication phase

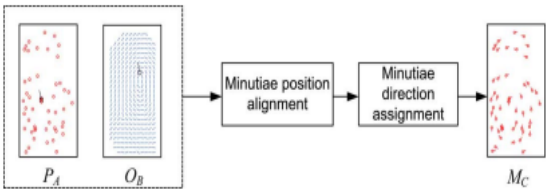

Fig 2.3.1 Combined minutiae template generation

Reference detection helps to locate a reference point with maximum certainty value. The range of minutiae direction is from 0 to 360.A query minutiae determination and finger print matching score is used for image retrieval process. So attackers cannot recover the original minutiae template from combined minutiae fingerprints.

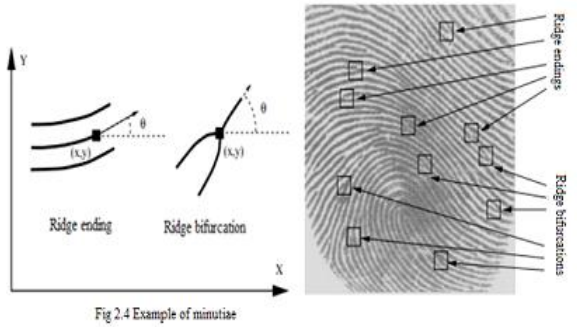

Fig 2.4 Example of minutiae

The performance of minutiae extraction information relies on quality of images [4].So image enhancement algorithms are used along with minutiae extraction modules. This helps to improve the clarity of ridges.

Experimentally it is proven in this work that enhancement algorithms improve the goodness index. Most of the poor quality images may create significant number of spurious minutiae. Some of the significant minutiae may be ignored. The region of interest in fingerprint images can be divided as well defined regions, recoverable corrupted region and unrecoverable corrupted region.

The major steps of image enhancement algorithm used in [4] are normalization, local orientation, local frequency estimation, region mask estimation and filtering as shown in fig 2.4.The normalization helps to reduce variations in the grey level values along the ridges. A smoothed orientation field for each 16*16 block is estimated. The local ridge frequency estimation is an intrinsic property of image. For a fingerprint at a fixed resolution, the value of the frequency of ridges and furrows in a local neighbourhood lies in a particular range [1/3,1/25].The fingerprints may be recoverable or unrecoverable regions. Assessment of shape based on amplitude, frequency and variance are used to classify the pixels into regions using squared error clustering algorithm. If the percentage of recovered regions is above a threshold, the input fingerprint image will be accepted. Gabor filters are used to remove noise from the inputted image. The goodness index (GI) is used to measure the quality of the extracted minutiae.

Handwritten signature images are used to secure private cryptographic keys. The first OSFV implementation uses a machine learning approach to select reliable feature representation [5].

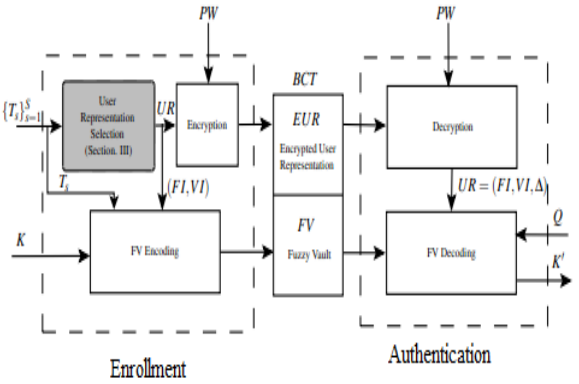

Fig 2.5 OSFV implementation

The steps needed for OSFV is as shown in fig 2.5.Enhanced methods of this system are used to improve accuracy and security. The new method with key size adaptation achieves good performance. This system consists of two subsystems-enrolment and authentication. The enrolment phase is used to collect signature templates. The user representation matrix,UR consists of the vectors

DOI 10.17148/IJARCCE.2016.51018

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

of feature information. This information is used for the authentication phase. The user representation matrix UR is encrypted by means of user password PW. Both FV and password are stored as a part of user bio-cryptography template(BCT).The user parameters FI and VI are used to lock the user cryptography key K by means of a single signature template T_S in a fuzzy vault FV.

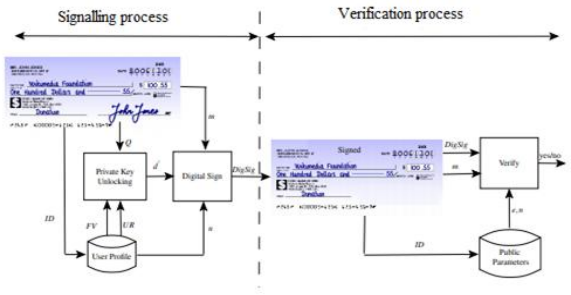

Fig 2.5.1 OSFV based digital signature method

The authentication subsystem uses the user query sample Q and the password PW. This helps to decode the fuzzy vault FV and restore the user cryptography key K.The password PW is used to decrypt the UR matrix. The vectors F1, V1 and Δ are used to decode the FV.

The OSFV based digital signature techniques are used for the automation of business processes. The user signs the document, by hand. The handwritten signature image is used to unlock his private key. The unlocked key produces a digital signature by encrypting some message extracted from document. The encrypted message is considered as a digital signature and it is attached to the digital document. Any person with the user public key can verify the digital signature. The detailed explanation is as shown in fig 2.5.1. For performance improvement, the global features are represented once enough no: of enrolled samples becomes available. Multi-scale feature fusion method seems to be useful where different feature vectors are extracted based on different extraction scales. Fusing multiple feature types also increase the FV decoding accuracy. The margin between intra and interclass of regions seems to differ when using different signature prototypes for FV encoding. The accuracy of OSFV system relies on the quality of features used. Additional variants like adaptive matching, assembling of fuzzy vaults, using additional passwords and cascading with traditional SV modules are used to improve accuracy.

Adaptive chaff generation and adaptive key size approaches are used to improve the security features. Several offline signature based FV implementation works are analyzed in this work. But the novel method to adapt cryptography key sizes for different users has shown good accuracy and security values. For forgery detection, better techniques with intelligence are needed.

Automatic fingerprint matching technique helps to automatically extract minutiae from images. The performance of the algorithm depends on the quality of images. Because of the variations in impression conditions, ridge configurations, skin condition and acquisition devices, the acquired fingers are of poor quality. This leads to the following problems like significant number of spurious minutiae may be created, a large percent of genuine minutiae may be ignored and large errors in their localization may be introduced.

Fingerprint enhancement algorithms improve the clarity of ridge and furrow structures [6]. The steps used in enhancement techniques are normalization, local orientation estimation, local frequency estimation, region mask estimation and filtering.

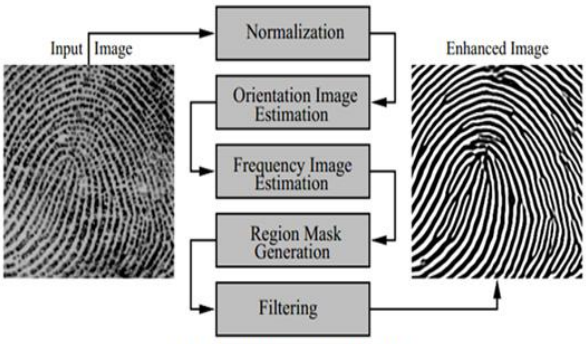

Fig 2.6 Fingerprint enhancement algorithm

Incorporating the enhancement algorithms improves the verification accuracy of matching systems. Experimental results show that the enhancement algorithms improve both the goodness index and verification performance.

III. EXISTING SYSTEM

If the attacker tries to make illetimate access to the database means it will be blocked because the information available ie, the template in the database consists only partial information such as, minutiae details from the one finger and the orientation details from the second finger, so it is difficult to made a complete fingerprint. So if attacker gets the fingerprint database means he has no use.

Existing Method Implementation

The existing system ie, protecting the privacy of fingerprint was totally done in the java language Here are the requirements.ie,

- **Jdk-8u45-windows-i586.**
- **Netbeans-8.1-windows.**
- **Xampp control panel.**

- **Jdk-8u45-windows-i586.** It is the development environment for building applications and components using the Java programming language.
- **Netbeans-8.1-windows**. It is a software development platform written in java. It allows applications to be developed from a set of modular software components called modules.
- **Xampp control panel.**XAMPP stands for Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing and deployment purposes.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

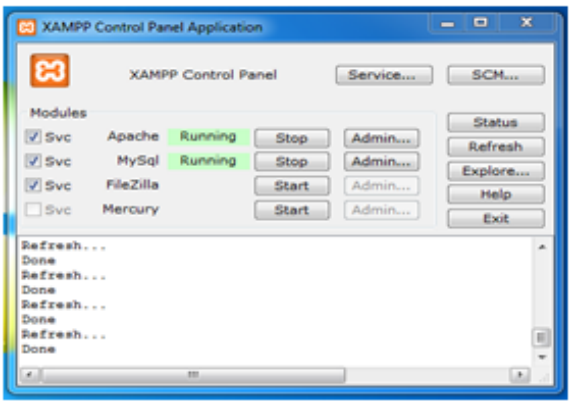

Fig 3.1 Xampp control panel

Malfunctioning arises from two sides. One from the illegitimate user and the other one from the trusted entity. And this fixes the issues of the problem arises from the illegitimate user or attacker. At the enrolment phase the details from both the fingerprints are selected. With the help of a proposed coding strategy the fingerprints will be combined to form a template. And this template is stored in the **Xampp control panel** database.

At the authentication phase the details from the person is checked with fingerprint template in the database. If a match occurs the individual is considered as the trusted person. The attacker is unable to hack the database, because the fingerprint template was made from the partial features from both the fingerprint and the attacker can't determine whether it is the fingerprint combination template or not. The attacker can't create the exact fingerprint from the available template. So the attempt from the attacker side will be worthless.

IV. PROPOSED METHOD IMPLEMENTATION

Our system shows best results on attack from both sides ie, one from the attacker side and other from the legitimate user side itself. The attacker can't reconstruct an exact fingerprint from the template in the database because the database contains partial information only. The fingerprints may change over time. This is handled during enrolment phase itself. At the enrolment phase itself it will be rejected. The rejection will be based on the "Threshold value as 20". The fingerprint with error rate less than 20% will be selected and subjected to next stage process.

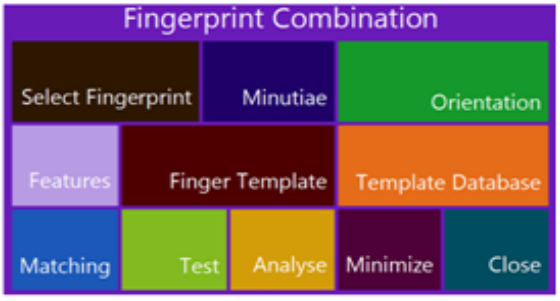

Fig 4.1 GUI

The system has two phases, Enrolment and Authentication. We use two fingerprint details to improve privacy. In the enrolment phase the details are collected and the reference points from both the fingerprints are collected using a GUI interface as shown in fig 4.1.

In the enrolment phase the minutiae from the one fingerprint and the orientation from the other fingerprint and the reference points from both the fingerprints are collected as shown in fig 4.2

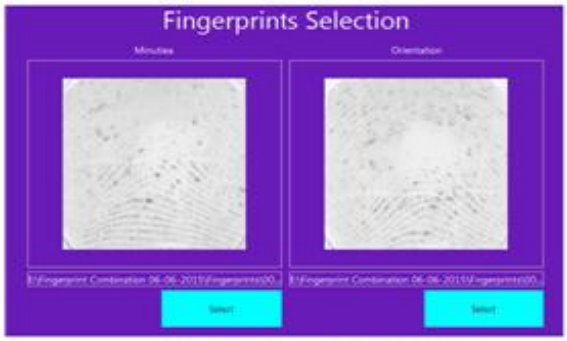

Fig 4.2 fingerprint selection

And with the help of a proposed coding strategy, the fingerprint will be combined and stored into the database in the form of a template as shown in the fig 4.3

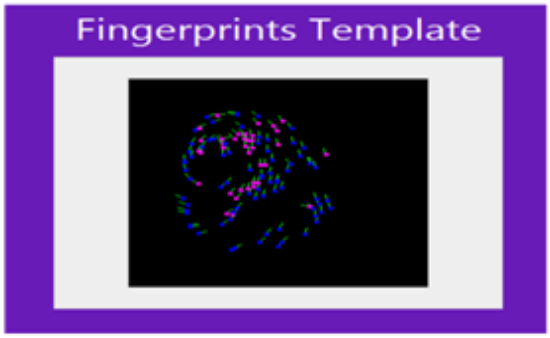

Fig 4.3 Fingerprint template

In the Authentication phase, fingerprint matching between the template and the query fingerprint is checked.

The percentage of matching in database is displayed as the result as shown in fig 4.4.

Fig 4.4 Matching results

DOI 10.17148/IJARCCE.2016.51018

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Here the problem arises from the legitimate user itself. If the fingerprint has partial impressions or breaks or cuts, the content in the database may not be matching. The fingerprints are considered as the biometric feature of an individual. So it has to be treated as that much of importance.In this time the system will announce the percentage of difference occurred in the new captured input as shown in fig 4.5

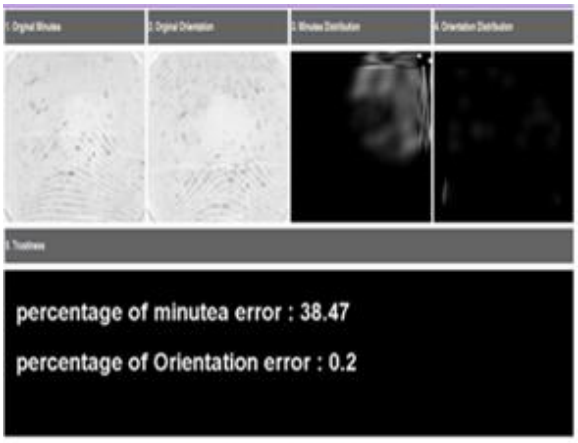

Fig 4.5 Percentage of error

The fingerprint has to possess enough details such as the availability of endpoints and availability of the intersections. So to handle the information loss the threshold of 20 is set. If a fingerprint has details less than 20 means the fingerprint is rejected and will ask to give another fingerprint as shown in fig 4.6

Fig 4.6 Trustiness

V. PERFORMANCE EVALUATION

The analysis is done by adding more fingerprints into the database. The matching process works well for all inputs if matching is identified in the database. Same for the both processes ie, it just analyse the matching between the template at the database and the currently given fingerprint at the time of authentication. The fingerprint is compared with 8 templates in the database as shown in the fig 5.1 It is well suited for more no: of input images and can be used for authentication processes in applications like banking, payroll etc.

Fig 5.1 Matching analysis

V1. CONCLUSION

When considering a system, that have to resist the attack from anyways.May the attack from the attacker side or it arises from the legitimate user side. So a system has to consider both the ways. So this system will resist the attack from both the sides. And it is not viable to any faulty informations. The informations taken to the system also accurate because of threshold value. The fingerprint above the threshold will be selected as the passed one and it will be continued to further process and otherthan this will be rejected.

REFERENCES

[1] J. Feng and A. K. Jain, "Fingerprint reconstruction: From minutiae to Phase," IEEE Trans. Pattern Anal.Mach. Intell. , vol. 33, no. 2, pp.
[2] 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. 209–223, Feb. 2011.
[3] Sheng Li, Student Member, IEEE, and Alex C. Kot, Fellow, Fingerprint combination for privacy protection, IEEE
[4] L.Hong, Y.F.Wan, and A.Jain, "Fing erprint image enhancement: Algorithm and performance evaluation," IEEE Trans. Pattern Anal. Mach. Intell., vol. 20, no. 8, pp. 777–789, Aug. 1998.
[5] G.S. Eskander., R. Sabourin, and E. Granger, Signature based Fuzzy Vaults with boosted feature selection.IEEE Workshop on Computational Intelligence and Identity Management (SSCI-CIBIM 2011), pp.131-138, Paris, 2011
[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] Austin J Gladston, and Ashitha. S.S"A survey on fingerprint protection techniques", IRJET, Volume: 03, Issue: 01, January 2016.

BIOGRAPHY

Austin J Glaston received the B.Tech degree in Information Technology from Anna University, Chennai and doing M.Tech degree in Computer Science and Engineering from Lourdes Matha College of Science and Technology, Kerala University.

DOI 10.17148/IJARCCE.2016.51018