iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** Issue I **Month of publication:** May 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3, Special Issue-1, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Combined Fingerprint Template for Virtual Identity

V. Kayalvizhimeenal
Department of Computer Science and Engineering
P.A College of Engineering and Technology, Pollachi, India

Abstract - The most mature, reliable and proven technique among biometrics is Fingerprint recognition. A Fingerprint is made up with ridges and furrows. Ridges are high relief lines on Fingertip surface while furrows (or valleys) are those lines that separate ridges from one another. Ridges and furrows run in parallel lines and curves to each other, forming complicated patterns. The image enhancement and binarization is first applied on fingerprints before the evaluation to achieve good minutiae extraction in fingerprints with varying quality. Many methods have been combined to build a minutia extractor and a minutia matcher. Minutia marking with special consideration of the triple branch counting and false minutiae removal methods is used in the work. Two-stage fingerprint matching algorithm has been developed for minutia matching. This algorithm is capable of finding the correspondences between input minutia pattern and the stored template minutia pattern without resorting to exhaustive search. The decision tree classifier improves matching with low error rate.
Keyword-- Combination, fingerprint, minutiae, privacy protection.

I. INTRODUCTION

Image processing comes under the domain of Artificial Intelligence. Image processing is a form of signal processing. It is the process of giving an image as the input to the processing algorithm and to produce the output. The output may be in form of image itself or a set of characteristics or parameters related to the image according to the algorithm used. In the wide spread of applications the fingerprint technique is used in authentication system for protecting the privacy.

Traditional encryption is not sufficent for the fingerprint privacy protection because decryption is requried before the fingerprint matching. It is inconvient to use the techniques that use key for the fingerprint privacy protection. It is vulnerable to both key and the protected fingerprint stolen. At the time of distinctive patterns are fully developed and are permanent throughout the life. From different survey papers it has been observed that the fingerprints are unique in nature because of the properties, fingerprints are very secure for biometrics applications. Finger print matching is a very complex pattern recognition problem so finger print matching is not only time taking but experts also takes long time for education and training. The combination of two fingerprints in to a virtual identity can be implemented to increase the efficiency and security of fingerprints. Combining two different fingerprints can be done in two levels either image level or feature level. Fingerprints have remarkable permanency and uniqueness throughout the time. The computers and mobile phones equipped with fingerprint sensing devices for fingerprint based password protection are being implemented to replace ordinary password protection methods. The novel system for enhancing security of the fingerprint template without including a token or key. The performance is evaluated over the FVC2004 DB2_A database.

The figure 1 shows the fingerprint minutiae features



Figure 1: Fingerprint Minutiae Features

©IJRASET 2015: All Rights are Reserved

II. RELATED WORKS

The practical approach in [6] is to combine two or more factor authenticator to reap benefits in security or convenient or both. A novel two factor authenticator based on iterated inner products between patterns. Tokenized pseudo-random number and the user specific fingerprint feature, generated from the integrated wavelet and Fourier–Mellin transform, and hence produce a set of user specific compact code that coined as Bio Hashing. Biometrics-based authentication systems offer obvious usability advantages over traditional password and token-based authentication schemes [12]. The biometrics raises several privacy concerns. A biometric is permanently associated with a user and cannot be changed. Hence, if a biometric identifier is compromised, it is lost forever and possibly for every application the biometric is used. If the same biometric is used in multiple applications, a user can potentially be tracked from one application to the next by cross-matching biometric databases. There are several methods to generate multiple cancelable identifiers from fingerprint images to overcome these problems. In essence, a user can be given as many biometric identifiers as needed by issuing a new transformation key. The identifiers can be cancelled and replaced compromised. Empirically compare the performance of several algorithms such as Cartesian, polar, and surface folding transformations of the minutiae positions. It is demonstrated through multiple experiments that can achieve revocability and prevent cross-matching of biometric databases. It is also shown that the transforms are noninvertible by demonstrating that it is computationally as hard to recover the original biometric identifier from a transformed version as by randomly guessing. Based on these empirical results and a theoretical analysis the feature-level cancelable biometric construction is practicable in large biometric deployments. The security analysis of leading privacy enhanced technologies for biometrics including biometric fuzzy vaults and biometric encryption [13]. The lack of published attacks, combined with various proven security properties has been taken by some as a sign that these technologies are ready for deployment. While some of the techniques do have proven security properties, those proofs make assumptions that may not, in general, be valid for biometric systems. The three disturbing classes of attacks against Pseudo Enhancing Techniques (PET) including attack via record multiplicity, surreptitious key-inversion attack, and novel blended to address the privacy and security requirements substitution attacks. In [5] proposed a path for 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. 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 it can be processed by conventional fingerprint algorithms and or an intruder may not be able to determine if a given print is mixed or not. The paperwork on biometric verification systems face challenges arising from noise and intra-class variations [10]. A multimodal biometric verification system combining fingerprint and voice modalities is used to overcome the problems. The system combines the two modalities at the template level, using multi biometric templates. The fusion of fingerprint and voice data successfully diminishes privacy concerns by hiding the minutiae points from the fingerprint, among the artificial points generated by the features obtained from the spoken utterance of the speaker.

In [11] the Reliable information security mechanisms are framed to combat the rising magnitude of identity theft in society. The cryptography is a powerful tool to achieve information security, one of the main challenges in cryptosystems is to maintain the secrecy of the cryptographic keys. Though biometric authentication can be used to ensure that only the legitimate user has access to the secret keys, a biometric system itself is vulnerable to a number of threats. A critical issue in biometric systems is to protect the template of a user is typically stored in a database or a smart card.

The Preservation of privacy of digital biometric data stored in a central database has become of paramount importance. Possibility of using visual cryptography for imparting privacy to biometric data such as fingerprint images, iris codes, and face images [3]. A private face image is dithered in to two face images that are stored in two separate database server such that the private image can be delivered. The possibility of hiding a private face image in to two host face image and successful matching of face images are reconstructed from the sheets. The inability of sheets to reveal the identity of private face images have the difficulty of cross-database matching for determining identities. It can be processed by fingerprint conventional algorithm. The fingerprint is composed into two components as spiral and continuous component. The performance of minutiae extraction algorithm relies heavily on the quality of the input fingerprint. The enhancement algorithm improves both goodness index and the verification accuracy.

The survey on attack using reconstructed finger print [15], the combined template share the similar topology to the original minutiae templates it can be converted into real look alike combined fingerprint using fingerprint reconstruction algorithm. The combined fingerprint is used for minutiae based matching algorithm. A fingerprint matching is an important technique for personal identification, the main reason for this is that every person is believed to have distinct fingerprints.

Minutiae based methods involve to extract minutiae like terminations and bifurcations from the fingerprint images, and then

©IJRASET 2015: All Rights are Reserved

Volume 3, Special Issue-1, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

compare this data to the previously stored template data sets. Generally, minutiae based methods require a significant amount of pre-processing to produce accurate results. In correlation based techniques two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments the direct application of it rarely leads to acceptable results, mainly due to the problems such as Non-linear distortion and expensive In Non-minutiae feature based techniques some other features of the fingerprint ridge pattern may be extracted more reliably than minutiae. The minutiae-based methods require an image of good quality, ridge features offer an alternative for poor images

In [4] gave a research on virtual identity creation by fingerprint combination for privacy protection the idea is to combine two different fingerprints, pertaining to two different fingers into a new identity. The proposed work is carried out in two phases. In the first phase combined minutiae template will be generated based on the information extracted from two different fingerprints. And in the next phase fingerprint-Matching process is proposed for matching the query fingerprints against a combined minutiae template by using image processing algorithm.

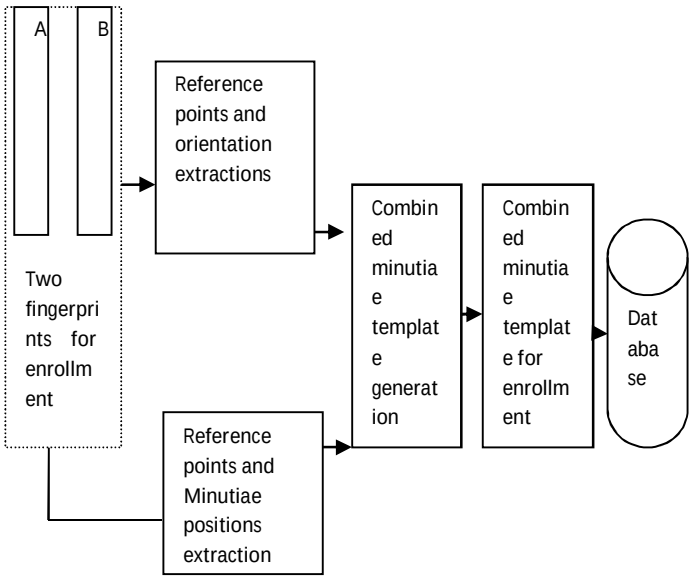
III. VIRTUAL IDENTITY GENERATION SYSTEM

In the proposed fingerprint privacy protection system consist of two phases as enrollment phase and authentication phase during the enrolment, the system captures two fingerprints from two different fingers. Use 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 using Gabor filtering technique, and the reference points are detected from both the fingerprints. While the minutiae directions depend on the orientation of the other fingerprint and some coding strategies. From these features generate combined minutiae template. This template is stored in database for authentication.

In the authentication phase the same two fingers used in the enrollment are given as the input the reference points and the minutiae features are extracted from the fingerprint A' and the orientation points and the reference points are extracted from the fingerprint B' and the minutiae template is generated. The template is matched with the reconstructed fingerprint with two stage fingerprint matching.

A two-stage fingerprint matching process is further for matching the two query fingerprints against a combined minutiae template. In addition, the combined minutiae template share a similar topology to the original minutiae templates, it can be converted into a real-look alike combined fingerprint by using a fingerprint reconstruction approach. The combined fingerprint issues a new virtual identity for two different fingerprints, can be matched using minutiae based fingerprint matching algorithms.

Figure 2 shows the block diagram for the proposed system



©IJRASET 2015: All Rights are Reserved

Volume 3, Special Issue-1, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

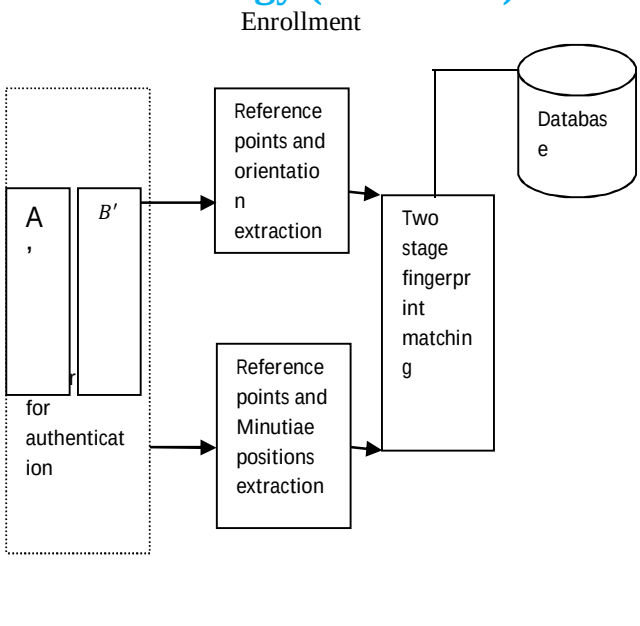


Figure 2. Block Diagram for the Virtual Identity Generation System

A. Reference point and orientation detection

The reference point's detection process is motivated by the use of complex filters for singular point detection [13]. Given a fingerprint, the main steps of the reference point's detection are summarized as follows

1) Compute the orientation O from the fingerprint using the Orientation Estimation Algorithm.

2) Obtain the orientation Z in complex domain, In Equation (1) represents the orientation angle of the fingerprint

i. Z=cos(2O)+jsin(2O) (1)

3) Calculate a certainty map of reference points as shown in Equation (2)

i. Cref =Z*Tref (2)

"*" is the convolution operator and Tref is the reference points detection.

4) Locate a reference point satisfying the two criterions:

i. The amplitude should be a local maximum

ii. The local maximum should be over a fixed threshold.

5) If no reference point is found for the fingerprint, locate a reference point with the maximum certainty value in the whole fingerprint image.

B. Reference Point and Minutiae Position Detection

Most finger print minutiae extraction methods are thinning-based skeletonization process converts each ridge to one pixel wide. Minutiae points are detected by locating the end points and bifurcation points on the thinned ridge skeleton based on the number of neighboring pixels. The end points are selected if have a single neighbor and the bifurcation points are selected if have more than two neighbors. The methods based on thinning are sensitive to noise and the skeleton structure does not conform to intuitive expectation. This category focuses on a binary image based technique of minutiae extraction without a thinning process. Gabor filters are used to enhance the minutiae positions.

C. Combined Minutiae Template Generation

This module is done by using Minutiae Position Alignment, Minutiae Direction Assignment.

©IJRASET 2015: All Rights are Reserved

Volume 3, Special Issue-1, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Among the reference point of a fingerprint for enrolment the reference point of maximum certainty value is taken as the primary reference point. Let us assume R_a *and* R_b

Primary reference point of the fingerprint A and B is defined in the Equation (4)

$$(\text{Pic})T = H.\ (P_{ia} - r_a)\ T + (r_b)\ T \qquad (4)$$

Each aligned minutiae position is assigned with a direction. The range is from 0 to π. The range of will the same as that of the minutiae directions from an original fingerprint.

$$\Theta i = Oe(xi,yi)+\rho\pi \qquad (5)$$

In Equation (5) ρ is an integer is randomly selected from {0, 1}. The range of Oe (xi,yi) is from 0 to π.The range of Θi will be from 0 to 2π, is the same as that of the minutiae directions from an original fingerprint. pi may be located outside of the fingerprint B, Oe (xi,yi) is not well defined. In such case, predict Oe (xi,yi) before the direction assignment.

Some works for modelling the fingerprint orientation can be adopted for the orientation prediction. Once the N aligned minutiae positions are assigned with directions a combine minutiae template Me= {mi = (pi, θi), 1<i<N}. In some cases, a global position translation may be necessary for all the minutiae points are located inside the fingerprint image

D. False Minutia Removal

The preprocessing stage does not totally heal the fingerprint image. The false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking or totally eliminated. In the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia. This false minutia will significantly affect the accuracy of matching if they are simply regarded as genuine minutia. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective. The figure 3 shows the possible false minutiae feature.

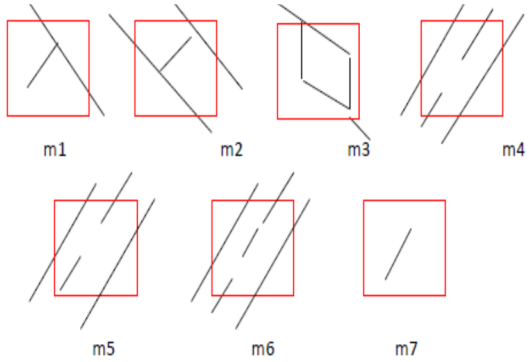


Figure 3. False Minutiae Features.

The procedures for the removal of false minutia are:

1) If the distance between one bifurcation and one termination is less than D and the two minutia are in the same ridge (m1 case), both of them are removed. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.
2) If the distance between two bifurcations is less than D and they are in the same ridge, the two
3) If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed. (Case m4, m5, m6).
4) If two terminations are located in a short ridge with length less than D, remove the two terminations (m7).

©IJRASET 2015: All Rights are Reserved

Volume 3, Special Issue-1, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

E. Two Stage Fingerprint Matching

After calculating combined minutiae template generation, Two-stage fingerprint scheme is proposed. During the authentication stage two-stage fingerprint matching is used to match the query fingerprints against stored template[7].

Minutiae positions of fingerprint A' and orientation of fingerprint B' and the reference points for the both A' and B' are matched against the Mc. Figure 4 shows two-Stage fingerprint matching.

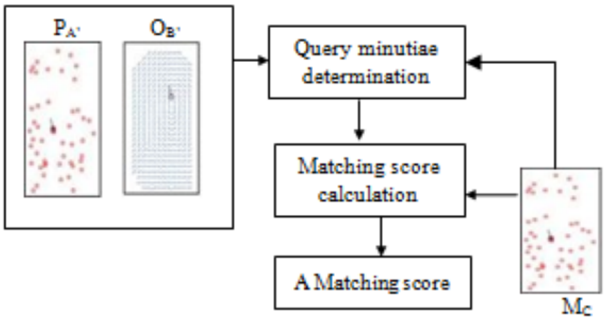


Figure 4. Two stage fingerprint matching process

This module contains two processes

1) Query Minutiae Determination

2) Matching Score Calculation

Here generating the minutiae, reference point of query image. Using this generate combined minutiae template of query image In combined minutiae template generation, minutiae position and direction assessments are calculated Sometimes minutiae position and direction assessment has same topology of the original fingerprint. After calculating combined minutiae template generation and two-stage fingerprint matching, combined fingerprint generation to be considered. Some existing works shows that, it is possible to reconstruct the original fingerprint. Some of these reconstruction techniques can only generate a partial fingerprint. By using minutiae based scheme can generate a full fingerprint. In [10], the full fingerprint will be generated by using minutiae based scheme. By adopting one of these fingerprint reconstruction approaches allows to convert combined minutiae template into a combined fingerprint image. Figure 5 shows process to generate a combined fingerprint for two different fingerprints. The combined fingerprint will be reconstructed by using some fingerprint reconstruction approaches from combined minutiae template.

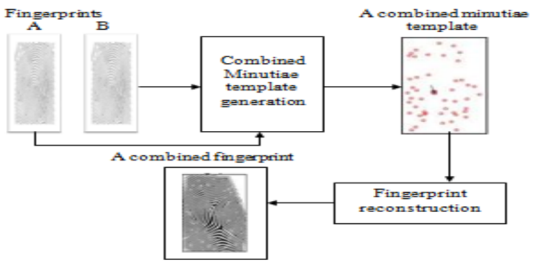


Figure 5. Combined Finger Print Template Generation

For the combined minutiae templates those are generated using Coding Strategy, a module for all the minutiae directions in and so as to remove the randomness. After the module operation, use a minutiae matching algorithm to calculate a matching score between and for the authentication decision.

$$\text{Match Score} = \frac{\text{No.of total matched minutiae pair}}{\text{number of minutiae in fingerprint template}}$$

IV. RESULTS

The experiment is conducted on the first two impressions of the FVC2004DB2_A database which contains 400 fingerprints from 200 fingers. The verifinger 6.3 is used for minutiae position extraction and the minutiae matching.

The reference point detection has an impact on the accuracy and efficiency of the proposed system. The two parameters need to be

©IJRASET 2015: All Rights are Reserved

Volume 3, Special Issue-1, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

determined for the reference point detection, σ for complex filters and T is the threshold for the references point detection. The value for σ = 1.5 and T=5.

The input images labelled A and B is taken as sample fingerprint image for the experiment as shown in figure 6 and figure 7.



Figure 6. Input image of a Fingerprint



Figure 7. Input Image Of Fingerprint

The minuiae points and the refernce points from both the fingerprints are extracted the minutiae points referring ridge ending, bifurication, core are extracted from the two fingerprints as shown in the figure 8.

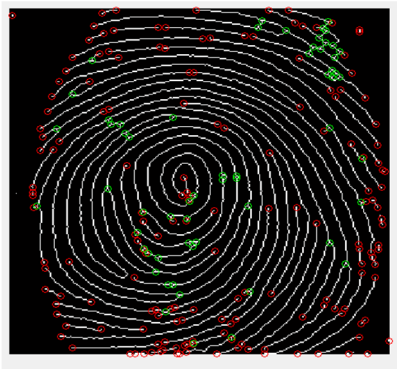


Figure 8. Minutiae Point Detection

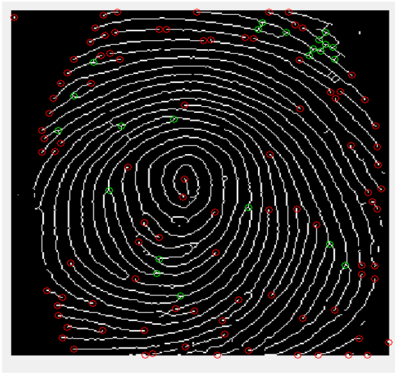


Figure 9. False Minutiae Removal

The false minutiae are removed from the combined minutiae template as shown in the figure 9. The region of interest can be detected automatically or manually the manual detection is done for security as shown in the figure 10.

©IJRASET 2015: All Rights are Reserved

Volume 3, Special Issue-1, May 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

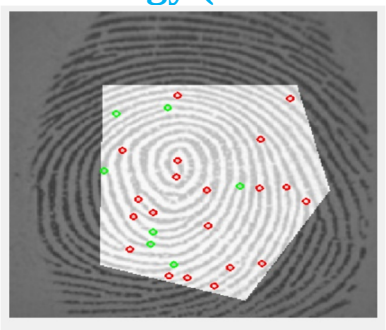


Figure 10 Region of Interest

The orientation points are detected from the combined minutiae template in the basis of ridge ending, bifurification, core points with orientation estimation algorithm by distance computation as shown in the figure 11.

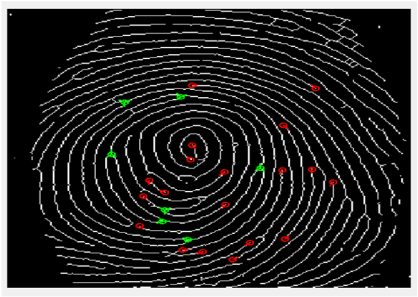


Figure 11. Orientation Point Detection

The validation of the combined fingerprint and the similarity measure of matching with the combined minutiae template and the reconstructed fingerprint are shown in the figure 12 and 13.

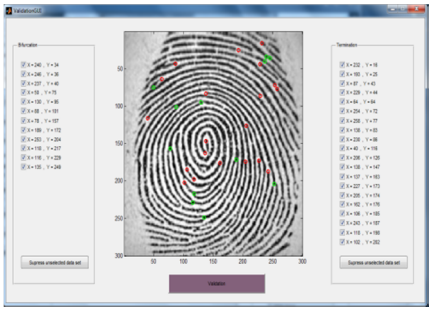


Figure 12. Validation of the Fingerprint

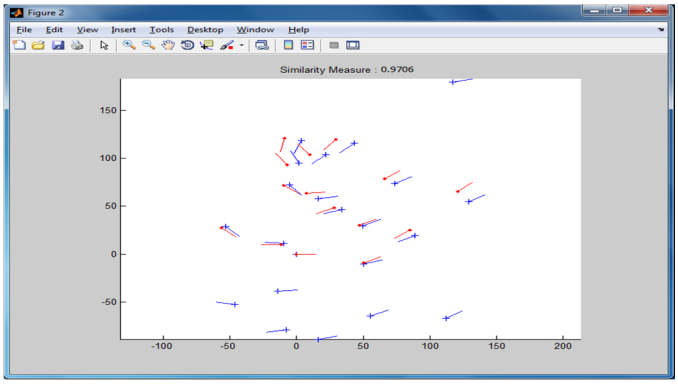


Figure 13. Similarity Measure of Matching

©IJRASET 2015: All Rights are Reserved

V. CONCLUSION

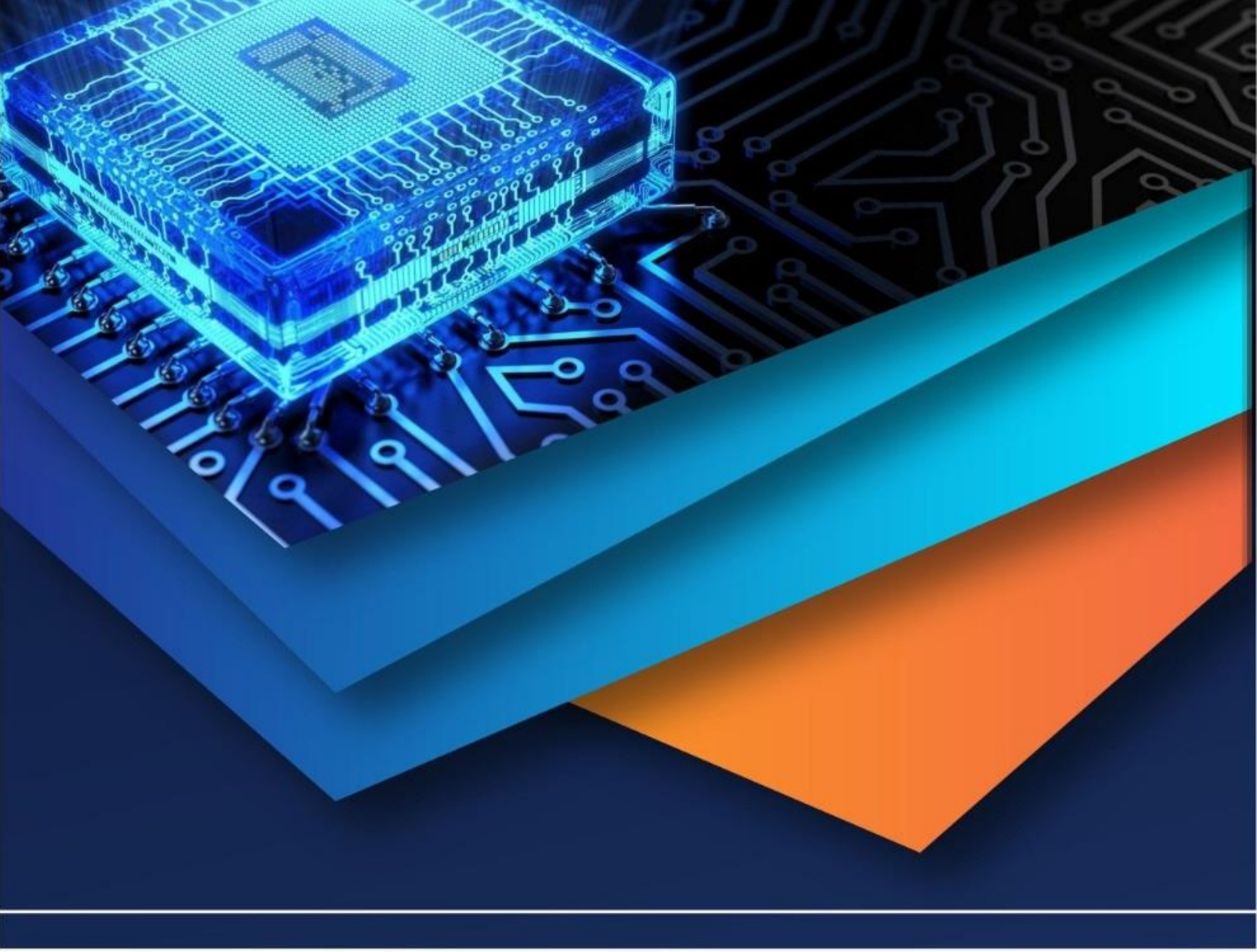
A novel minutiae-based fingerprint matching approach is used in the paper. It is important to recall the objectives of the development of new algorithms suitable for custom designed hardware architecture. The development of a software implementation of these algorithms is used to prove the correctness 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. The attacker cannot attack the database in any means. So it will be more protecting system for the fingerprint database.

In the future work the combined fingerprint can be developed in the combination of three fingers and maximum minutiae points the running time complexity arises the fingerprint enhancement algorithm can be used for maintaining the better performance and for achieving a better security.

REFERENCES

[1]. Kong A. and Cheung K. H. and Zhang D. and Kamel M. and You J. (2006), 'An analysis of bio hashing and its variants', Pattern Recognit., vol. 39, no. 7, pp. 1359
[2]. Nagar A. and Nandakumar K. and Jain A. K. (2010), 'Biometric template transformation: A security analysis' in Proc. SPIE, Electron. Imaging, Media Forensics and Security, San Jose
[3]. Othman A. and Ross A. (2004), 'Mixing fingerprints for generating virtual identities', in Proc. IEEE Int. Workshop on Inform. Forensics and Security(WIFS),FozdoIguacu,Brazil,Nov. 29–Dec.
[4]. Ross A. and Othman A. (2011), 'Visual cryptography for biometric privacy', IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81.
[5]. Ross A. and Othman A.(2003), 'Mixing fingerprints for template security and privacy', in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain.
[6]. Teoh B. J. A. and Ngo C. L. D. and Goh A. (2004), 'Bio hashing: Two factor authentication featuring fingerprint data and tokenised random number' Pattern Recognit., vol. 37, no. 11, pp. 2245–2255.
[7]. Yanikoglu B. and Kholmatov A. (2004), 'Combining multiple biometrics to protect privacy', in Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug.
[8]. Cappelli R. and Erol A. and Maio D. and Maltoni D. (2007), 'Synthetic fingerprint image generation', in Proc. 15th Int. Conf. Pattern Recognition, Sep 3–7, 2000, vol. 3, pp. 471–474.
[9]. Feng J. and Jain A.K. (2011), 'Fingerprint reconstruction: From minutiae phase', IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 2, pp. 209–223.
[10]. Jiang X. and Yau W. (2007), 'Fingerprint minutiae matching based on the local and global structures', in Proc. 15th Int. Conf. Pattern Recognition, 2000, vol. 2, pp. 1038–1041.
[11]. Nandakumar K. and Jain A.K. and Pankanti S. (2007), 'Fingerprint-based fuzzy vault: Implementation and performance', IEEE Trans. Inf. Forensics security, vol. 2, no. 4, pp. 744–57.
[12]. Ratha N.K. and Chikkerur S. and Connell J.H. and Bolle R.M. (2007), 'Generating cancelable finger print templates', IEEE Trans. Pattern Anal. March. Intell., vol. 29, no. 4, pp. 561–72
[13]. Scheirer W.J. and Boult T,E. (2008), 'Cracking fuzzy vaults and biometric encryption', in Proc. Biometrics Symp., Sep. 2007, pp. 34–39.
[14]. Li S. and Kot A.C. (2011), 'Privacy protection of fingerprint database', IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118.
[15]. Li S. and Kot A.C. (2012), 'A novel system for fingerprint privacy protection', in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), pp. 262–266.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)