iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 5 Issue: I Month of publication: January 2017

DOI:

Volume 5 Issue I, January 2017
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Generate new identity from fingerprints for privacy protection

Ujma A. Mulla[1]
[1]PG Student of Electronics Department of, B.I.G.C.E., Solapur, Maharashtra, India

Abstract : We propose here a novel system for privacy protection of fingerprint by merging two fingerprints & generate new identity. In the enrollment phase, two fingerprints are taken from two different fingers of one person. From one fingerprint we extract the minutiae positions, from the other fingerprint we extract the orientations, and from both fingerprints we extract the reference points. From this extracted information and our coding strategies, we generate combined minutiae template and that generated combined minutiae template stored in a database. During authentication phase, the system requires two query fingerprints from the same two fingers of one person which are used during enrollment phase. A two-stage fingerprint matching system is used for matching the two query finger-prints from the same two fingers of one person against a combined minutiae template which is stored in database. By storing the combined minutiae template in the database, the complete minutiae positions of a single fingerprint will not be compromised when the database is stolen. Furthermore, because of the similarity in topology, it is very difficult for the attacker to differentiate a combined minutiae template from the original minutiae templates. With the help of an existing fingerprint reconstruction approach, we are able to reconstruct the combined minutiae template into a new virtual identity of merged fingerprints. Thus, a new virtual identity is generated from merging the two different fingerprints of one person, which can be matched using minutiae based fingerprint matching algorithms. The experimental results shows that our system can achieve a very low error rate.

Keywords: fingerprint, minutiae extraction, orientation, privacy, protection.

I. INTRODUCTION

The Greek word “biometrics” is divided it into two roots: “bio” means life and “metrics” means to measure. Biometrics refers to technologies for measuring, and analyzing a person's physiological or behavioral characteristics. These unique characteristics are used to verify and identify to individuals. Fingerprints are most commonly represented by a set of points, called minutiae. At present many Fingerprint Authentication Systems are based on minutiae matching. Minutiae are generally indicated as the terminations and bifurcations of the ridge lines in a fingerprint image. The two most important local ridge characteristics of minutiae are the ridge ending and the ridge bifurcation unique. Ridge ending is termed as the point where the ridge ends abruptly. Ridge bifurcation is termed as the point where a ridge forks or diverges into branch ridges. A fingerprint authentication system can be generally divided into two parts namely

Enrollment

Identification or Verification

The enrollment part is responsible for registering individuals into the biometric system. In this enrollment phase, the characteristic of an individual is first scanned by a biometric reader to produce a raw digital representation of the characteristic. Fingerprint verification is to verify the authenticity of one person by his fingerprint.

A novel system is proposed for providing privacy to the fingerprint biometric system by combining two different fingerprints into a new identity. The system captures two fingerprints from two different fingers which may be from same person or from different person while registering. The combined minutiae template is generated based on three features. In such a combined template, the minutiae positions are extracted from one fingerprint, while the orientation from other fingerprint and reference points from both the fingerprints. The template will be stored in a database for authentication which requires two query fingerprints during verification.

II. RELATED WORK

"Combining Multiple Biometrics to Protect Privacy"- B. Yanikoglu and A. Kholmatov,-2004

In this work a biometric authentication framework which uses two separate biometric features, combined to obtain a non-unique identifier of the individual, in order to address privacy concerns. As a particular example, we demonstrate a fingerprint verification system that uses two separate fingerprints of the same individual. A combined biometric ID composed of two fingerprints is stored in the central database, and imprints from both fingers are required in the verification process, lowering the risk of misuse and privacy loss. We demonstrate the performance of the proposed method on only a small fingerprint database.

"Mixing fingerprints for generating virtual identities,"- A. Othman and A. Ross,-2011

This work explores the possibility of mixing two different fingerprints at the image level in order to generate a new fingerprint. To mix two fingerprints, each fingerprint is decomposed into two different components, viz., the continuous and spiral components. After pre-aligning the components of each fingerprint, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint image.

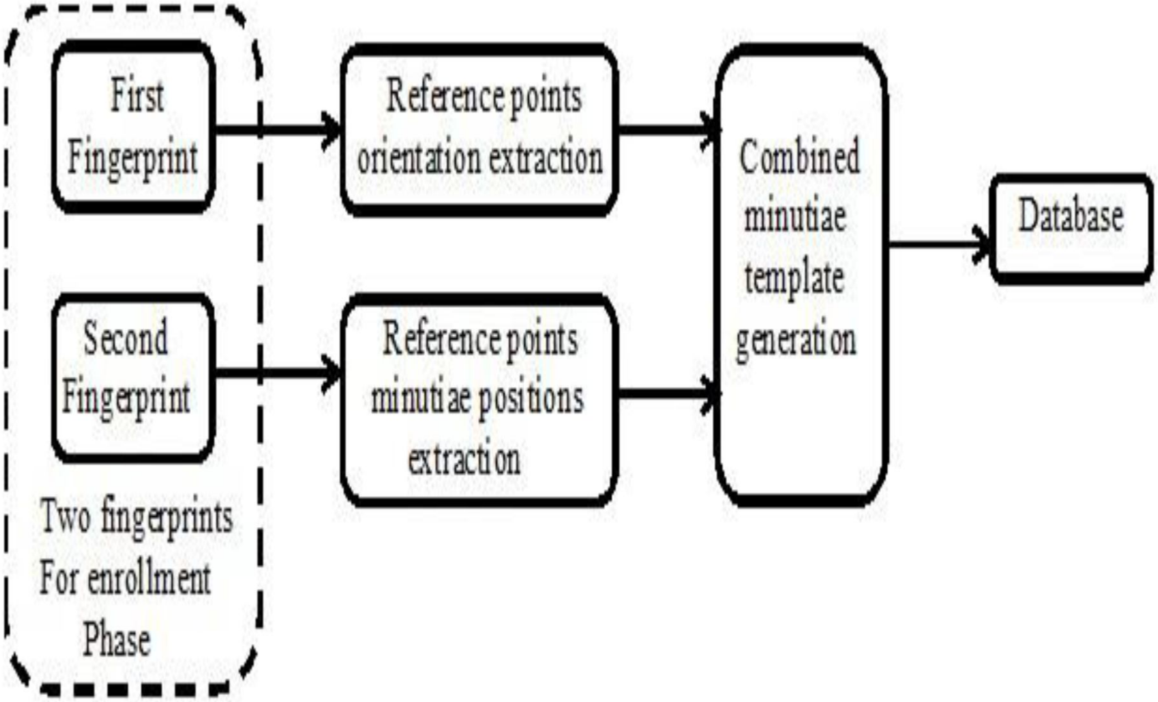
"Fingerprint image reconstruction from standard templates,"- R. Cappelli, A. Lumini, D. Maio, and D.
Maltoni,-2007

A minutiae-based template is a very compact representation of a fingerprint image, and for a long time, it has been assumed that it did not contain enough information to allow the reconstruction of the original fingerprint. This work proposes a novel approach to reconstruct fingerprint images from standard templates and investigates to what extent the reconstructed images are similar to the original ones (that is, those the templates were extracted from). The efficacy of the reconstruction technique has been assessed by estimating the success chances of a masquerade attack against nine different fingerprint recognition algorithms.

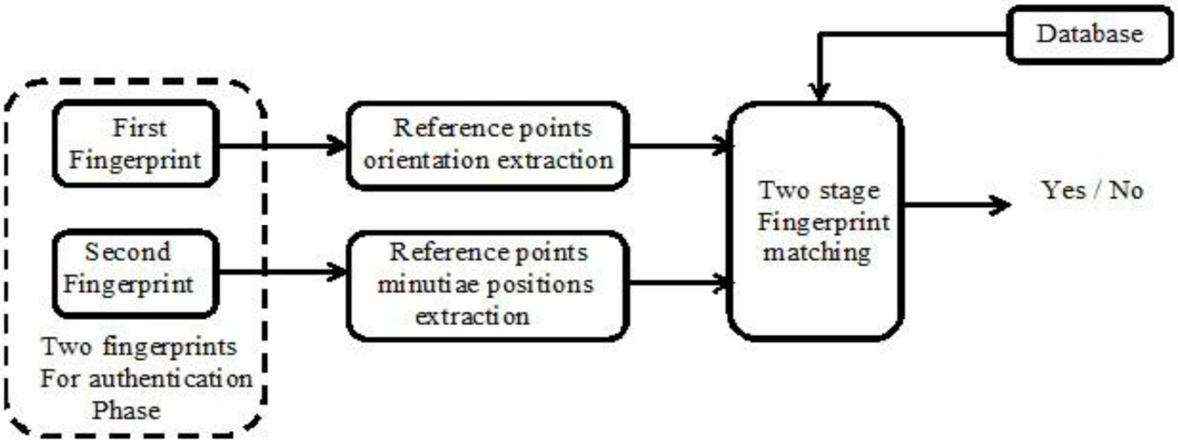
III. THE PROPOSED FINGERPRINT PRIVACY PROTECTION SYSTEM

Identification systems rely on three key elements: 1) attribute identifiers (e.g., Social Security Number, driver's license number, and account number), 2) biographical identifiers (e.g., address, profession, education, and marital status), and 3) biometric identifiers (e.g., fingerprint, iris, voice, and gait). It is rather easy for an individual to falsify attribute and biographical identifiers; however, biometric identifiers depend on intrinsic physiological characteristics that are difficult to falsify or alter.

This paper deals with combined fingerprint which requires two fingerprints used for verification and authentication and minutiae positions from one fingerprint, the orientation from the other fingerprint. Based on this extracted information, a combined template is generated and stored in database. In the verification phase, the system requires two query fingerprints from the fingers which are used in the enrolment. The fingerprint matching process is done by minutiae based fingerprint matching algorithms. By storing the combined template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen**.**


First Fingerprint
Second Fingerprint
Two fingerprints For enrollment Phase
Reference points orientation extraction
Reference points minutiae positions extraction
Combined minutiae template generation
Database

Enrollment Phase


Database
First Fingerprint
Second Fingerprint
Two fingerprints For authentication Phase
Reference points orientation extraction
Reference points minutiae positions extraction
Two stage Fingerprint matching
Yes / No

Authentication Phase

Fig.1 - Proposed system for privacy protection of fingerprint by merging two fingerprints.

Fig.1 shows our proposed privacy protection of fingerprint by merging two fingerprints. In the enrollment phase, the system captures two fingerprints from two different fingers, say fingerprints and from fingers and respectively.

We extract the minutiae positions from fingerprint and the orientation from fingerprint using some existing techniques. Then, by using our coding strategies, we generate combined minutiae template is 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. In the authentication phase, two query fingerprints are required from the same two fingers, say fingerprints and from fingers and. As what we have done in the enrollment, we extract the minutiae positions from fingerprint and the orientation from fingerprint. 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.

IV. MERGED FINGERPRINT GENERATION

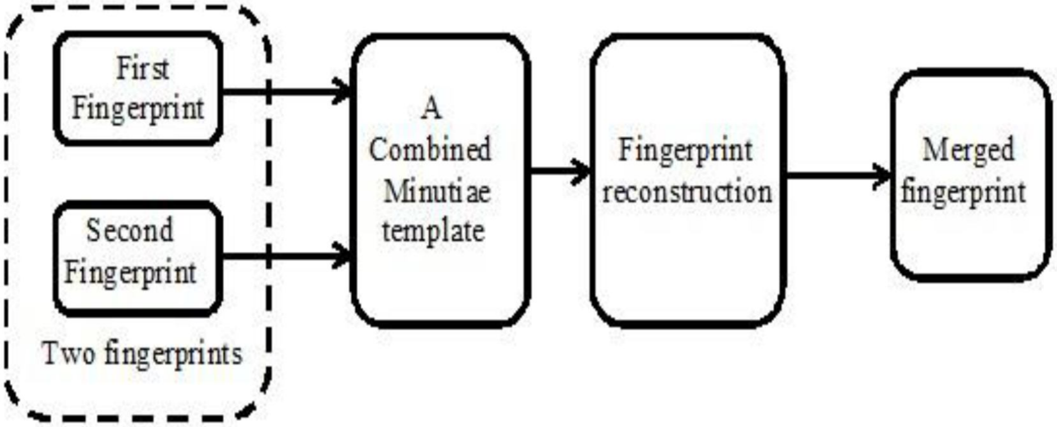


Fig.2 - Generating a merged fingerprint from two different fingerprints.

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. Therefore, the combined minutiae template has a similar topology to an original minutiae template. Some existing works have shown that it is possible to reconstruct a full fingerprint image from a minutiae template. By adopting one of these fingerprint reconstruction approaches, we are able to convert our combined minutiae template into a combined fingerprint image.

V. ALGORITHM

A. Jiang algorithm

Initially comparison is done using Jiang algorithm. The steps are given below

The Euclidean distance between each of the pairs of input and template fingerprints is calculated.

The average angle is also calculated.

Similarity level is then calculated by choosing weights of each of the feature vectors and applying respective equations.

$$\mathrm{sl}(i,j) = \begin{cases} \dfrac{\mathrm{bl} - \mathbf{W}\,|\,\mathrm{Fl}_i^I - \mathrm{Fl}_j^T|}{\mathrm{bl}} & , \text{If } \mathbf{W}\,|\,\mathrm{Fl}_i^I - \mathrm{Fl}_j^T| < \mathrm{bl} \\ 0 & , \quad \text{otherwise} \end{cases}$$

$$\mathbf{W} = (w_d\ w_d\ \ w_\theta\ w_\theta\ w_\varphi\ w_\varphi\ w_n\ w_n\ w_t\ w_t\ w_t)$$

The row number and column number where the maximum similarity level occurs is retrieved.

Using the above obtained values the corresponding feature vectors are obtained.

Due to Non linear deformation and false minutiae matching, global structures is used for final alignment.

A Bounding box is taken with parameters [10 16 10] and similarity level is computed using the below equations.

$$\mathrm{Fg}_k = \begin{pmatrix} r_{bk} \\ \varphi_{bk} \\ \theta_{bk} \end{pmatrix} = \begin{Bmatrix} \sqrt{(x_b - x_k)^2 + (y_b - y_k)^2} \\ d\phi\left(\tan^{-1}\left(\frac{y_b - y_k}{x_b - x_k}\right), \theta_b\right) \\ d\phi(\theta_h, \theta_k) \end{Bmatrix}$$

□□The final matching score is computed using

$$\mathbf{Ms} = 100 \times \frac{\sum_{i,j} \mathrm{ml}(i,j)}{\max\{M, N\}}$$

B. Novel algorithm

Due to more time and more no of computations, a Novel algorithm is proposed which is an improvement over Jiang algorithm.

For each minutiae from the input and template fingerprint, we create their local structures.

For each pair of local structure, we calculate its similarity value using Jiang algorithm equation

We eliminate all pairs of local structures that have a similarity value less than LocalScoreTHr (new threshold).Only the principal minutiae for each pair of local structures is retained.

We sort all minutiae pairs selected in local matching phase descendent order according to their similarity value.

We align all minutiae of input fingerprint and validate them using the Boundary box parameters.

Finally, we compute the final matching score Ms.

C. Our proposed algorithm

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. Therefore, the combined minutiae template has a similar topology to an original minutiae template. Some existing works have shown that it is possible to reconstruct a full fingerprint image from a minutiae template. By adopting one of these fingerprint reconstruction approaches, we are able to convert our combined minutiae template into a combined fingerprint image.

VI. EXPERIMENTAL RESULTS

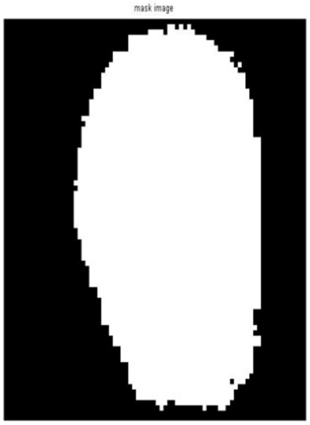


Fig.4.Mask Image

In Binarization, the grey scale image is converted into binary image. Binary images are easy to process. The basic principle ofconverting an image into binary is to decide a threshold value, and then the pixels whose value are more than the threshold are converted to white pixels, and the pixels whose value are below or equal to the threshold value are converted to black pixels. The threshold value has been decided using Otsu method. For better result, instead of calculating the threshold of the entire image we calculated threshold value of a small window (10 * 10) of the image and converted that segment into binary. Then the window is shifted to the next position and binarization is done. In this way the entire image is converted to binary.

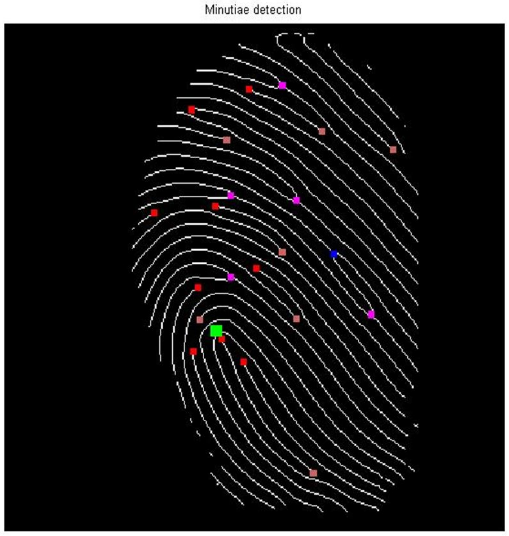


Fig.5.Minutiae Detection

In Minutiae based algorithm, minutiae of fingerprints of both fingers are used to construct a new template. The new template is formed by the combination of two minutiae of fingers. The combined fingerprint image is constructed in two phase, in first phase fingerprint image is captured from both fingerprint .A reference point and orientation from first fingerprint and reference point & minutiae extraction is taken from both fingerprints to create a new combined fingerprint which is stored in database. By using the minutiae based algorithm, the complete minutiae feature of a both in new combined fingerprint will not be reconstructed when the database is robbed. By using different coding strategy it is found that the error rate is reduced i.e. FRR ratio gets reduced. Also the database is less prone to get information when it gets robbed.

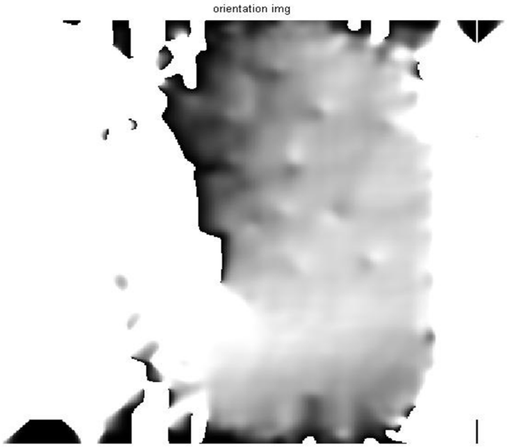


Fig.6.Orientation

An orientation image is defined as an N x N image, where O (i, j) represents the local ridge orientation at pixel (i, j). Local ridge orientation is usually specified for a block rather than at every pixel; an image is divided into a set of w x w non-overlapping blocks and a single local ridge orientation is defined for each block. Note that in a fingerprint image, there is no difference between a local ridge orientation of 90o and 270o, since the ridges oriented at 90o and the ridges oriented at 270o in a local neighbourhood cannot be differentiated from each other.

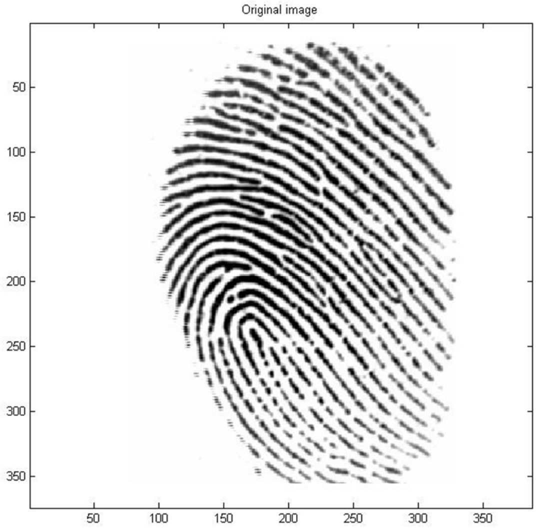


Fig.7.Orignal Image

When results from identification or verification procedures are discussed, the following terms will be used in this report:
Success rate: The rate at which successful verifications or identifications are made compared to the total number of trials.
False rejection rate (FRR): The rate at which the system falsely rejects a registered user compared to the total number of trials.
False acceptance rate (FAR): The rate at which the system falsely accepts a nonregistered (or another registered) user as a registered one compared to the total number of trials. The FAR is in this report used in the identification version, as a contrast to verification procedures, where it measures if a user is accepted under a false claimed identity.
Equal error rate (EER): The common value of the FAR and FRR when the FAR equals the FRR. This is the value where both the FAR and FRR are kept as low as possible at the same time. A low EER value indicates a high accuracy of the system.

VII. CONCLUSION

In this paper, we introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints will be generated and stored in a database. To make the combined minutiae template look real as an original minutiae template, three different coding strategies are introduced during the combined minutiae template generation process.

In the authentication process, two query fingerprints from the same two fingers are required. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Our combined minutiae template has a similar topology to an original minutiae template. Therefore, we are able to combine two different fingerprints into a new virtual identity by reconstructing a real-look alike combined fingerprint from the combined minutiae template.

REFERENCES

[1] Sheng. Li and Alex. C. Kot, “Fingerprint Combination for Privacy Protection,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 2, pp. 350-360,Feb. 2013.

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

[3] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, “An analysis of biohashing and its variants,” PatternRecognit., vol. 39, no. 7 pp. 1359–1368, 2006..

[4] 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.

[5] A. Nagar, K. Nandakumar, and A. K. Jain, “Biometric template trans-formation: A security analysis,” in Proc. SPIE, Electron.Imaging, Media Forensics and Security, San Jose, Jan. 2010.

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

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

[8] 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.

[9] 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.

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

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

[12] Sheng Liand Alex C. Kot, “Fingerprint Combination for Privacy Protection” IEEE Trans on Info, Forensics and Security, Vol. 8, NO. 2, Feb 2013.

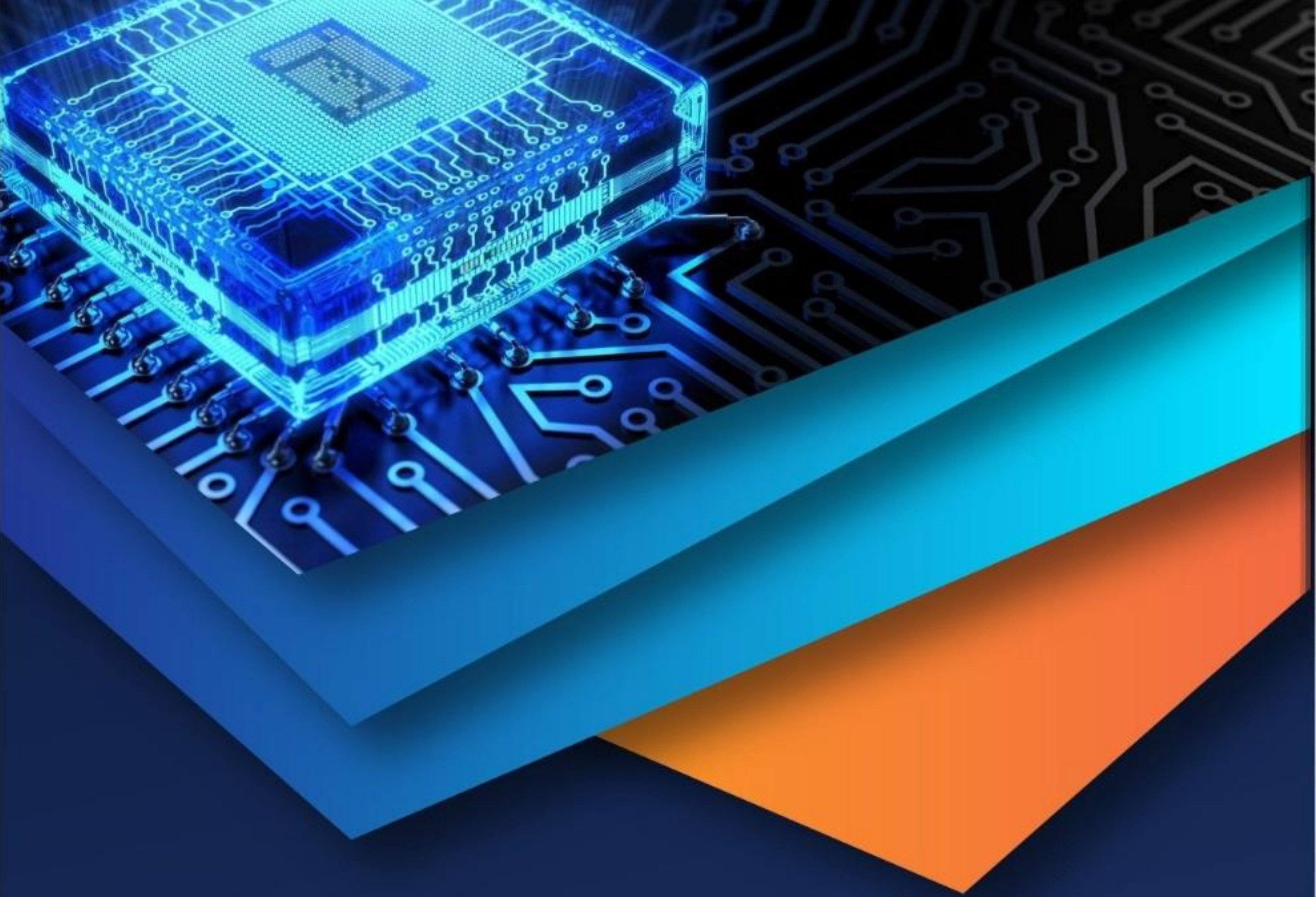
[13] N. Yager and A. Amin. Fingerprint alignment using a two stage optimization. PRL, 7(5):317–324, 2006.

[14] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authenticationsystems.IBM Systems Journal, 40(3):614–634, 2001.

[15] A. Ross, J. Shah, and A. Jain. From template to image: reconstructing fingerprints from minutiae points.PAMI, 29(4):544–560, 2007.

[16] Amengual J. C., Juan A., Prez J. C., Prat F., Sez S. and Vilar J. M. Real-time Minutiae Extraction in Fingerprint Images.Proc. of the6thInt. Conf. on Image Processing and its Applications, July 1997.

[17] 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.



doi crossref

10.22214/IJRASET

INDEX COPERNICUS

45.98

ISRA JIF

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

ISI

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY