iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** II **Month of publication:** February 2015

DOI:

www.ijraset.com

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

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

Combined Fingerprint Verification Method

Sri.Ganesh.D[1], Kaanchana.M [2], Vishnudharan.B[3]
[1,2,3] Dr. S.J.S Paul Memorial College of Engineering and Technology,
Puducherry, India

Abstract— Our 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. We go for combining two finger prints to increase security levels. During Registration dual fingerprint input is taken. We extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. We then combine the fingerprints to increase the level of security. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored in a database. While testing the efficiency of the system it requires two query fingerprints from the same two fingers which are used in the enrollment. A dual fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template.
Index Terms—minutiae, minutiae template, continuous and spiral components, database.

I. INTRODUCTION

Fingerprint fusion refers to the consolidation of (a) multiple samples of the same biometric trait obtained from different sensors or (b) multiple instances of the same biometric trait obtained using a single sensor, in order to generate a new image [8]. In the context of fingerprints, image-level fusion has been used to combine multiple impressions of the same finger as exemplified in the following scenarios: Multispectral sensor: Rowe et al. [12] fused multiple images acquired from a multispectral fingerprint scanner into a single high quality fingerprint image. Small-area sensor: Some sensors capture only a small portion of the fingertip [1]. Therefore, several fingerprint mosaicking techniques [15], [11] have been developed to stitch multiple impressions of the same finger and create a larger fingerprint. Multi-view sensor: Touch less fingerprint sensors capture multiple views of a finger using several calibrated cameras [5] or a single camera with two planar mirrors [3]. These multiple views are mosaicked together to yield a single nail-to-nail fingerprint.

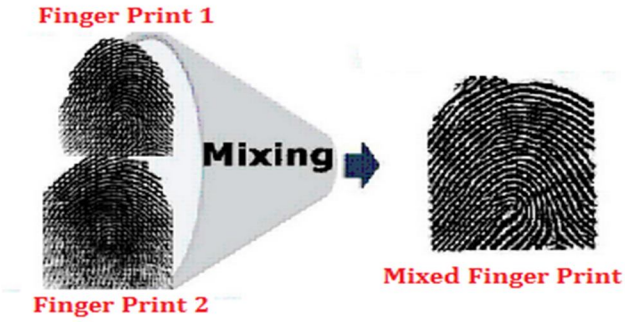


Fig:-1 Proposed Finger Print Mixing

The previous work on “Combining multiple biometrics to protect privacy,” used to combine two different fingerprints into a single new identity in the feature level. Image level based fingerprint combination techniques proposed in “Mixing fingerprints for template security and privacy,” and “Mixing fingerprints for generating virtual identities,” are used to combine two different fingerprints in the image level. The previous work on “Generating cancelable fingerprint templates,” proposed to generate cancelable fingerprint templates by applying non invertible transforms on the minutiae.

A. Overview

We concentrate for using a biometric system is to provide non-cheatable authentication. Authentication implies that (i) only legitimate or authorized users are able to access the physical or logical resources protected by the biometric system and (ii) impostors are prevented from accessing the protected resources. While a biometric system can be compromised in a number of

ways, one of the potentially damaging attacks is the leakage of biometric template information. The leakage of this template information to unauthorized individuals constitutes a serious security and privacy threat. Therefore in this paper we propose a model of creating 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.

B. *Finger Print Combination*

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 [15], [22], [23] 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. Fig. 3 shows our process to generate a combined fingerprint for two different fingerprints. Given any two different fingerprints as input, we first generate a combined minutiae template using our combined minutiae template generation algorithm. Then, a combined fingerprint is reconstructed from the combined minutiae template using one of the existing fingerprint reconstruction approaches.

It should be noted that the combined minutiae template generated by adopting *Coding Strategy* 1 is not appropriate for generating a combined fingerprint. The reason is that we set as 0 or 1 randomly during the minutiae direction assignment, i.e., we add randomly for each minutiae direction in such a coding strategy. As what has been discussed in Section II-C2, we need to perform a modulo operation for the minutiae directions during the fingerprint matching, so as to remove such randomness. Therefore, we will not be able to match the corresponding combined fingerprint by using a general fingerprint matching algorithm. While the purpose of generating a combined fingerprint is to issue a new virtual identity for two different fingerprints, which should be matched using general fingerprint matching algorithms.

C. *Reference Point Identification*

Given the minutiae positions $P_{a'}$ of fingerprint A', the orientation $O_{b'}$, of fingerprint B' and the reference points of the two query fingerprints. In order to match the stored in the database, we propose a two-stage fingerprint matching process including query minutiae determination and matching score calculation.

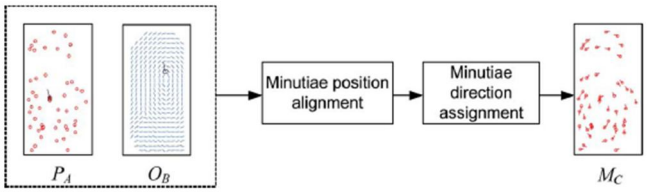


Fig:-2 Template Generation Process

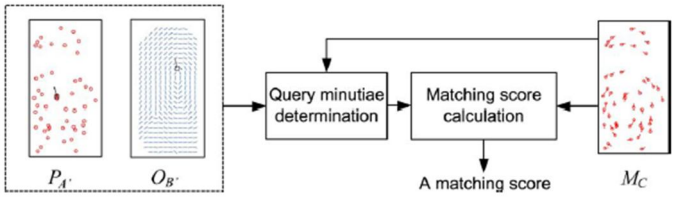


Fig:-3 Two-stage fingerprints matching process.

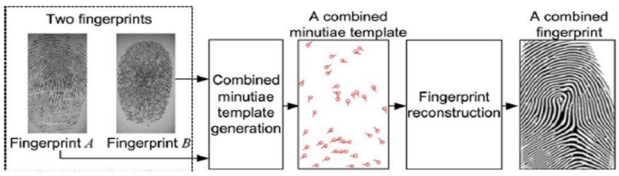


Fig:-4 Combined Fingerprint for two different fingerprints.

Performance of the reference points detection at different settings of threshold T

	T			
	3	4	5	6
No.	1141	650	291	207
True Detection Rate (%)	99.5	99.5	99.5	98.5
False Detection Rate (%)	0.5	0.5	0.5	1.5

D. Reference Point Tracking

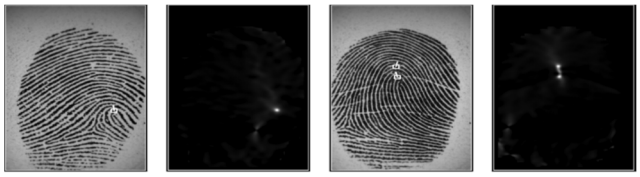
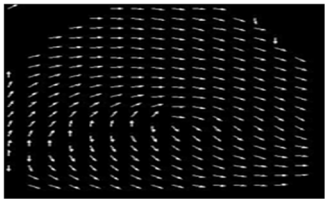


Fig.5. Illustrations of the reference points detection. Fingerprint with only one reference point in (a) and the corresponding certainty value map in (b); fingerprint with two reference points in (c) and the corresponding certainty value map in (d).

II. MODULE OUTPUT

1. Normalised Image

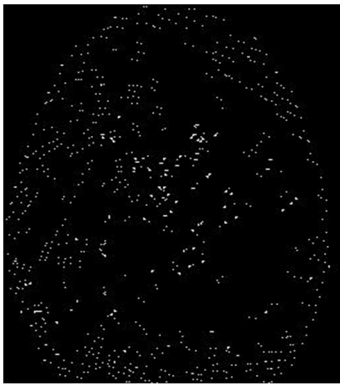
2. Normalised Image



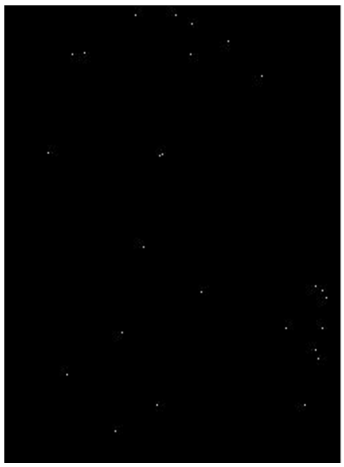
3. Binarized Image

4. H-Break Removal

5. All Minutiae Positions

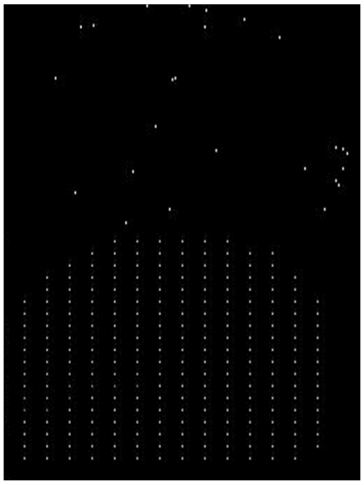


6. False Removal Minutiae Points



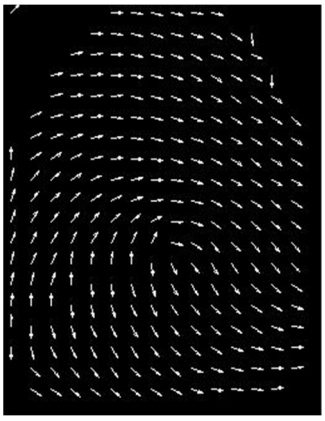
7. Minutiae Positions after Removing False Minutiae

8. Template



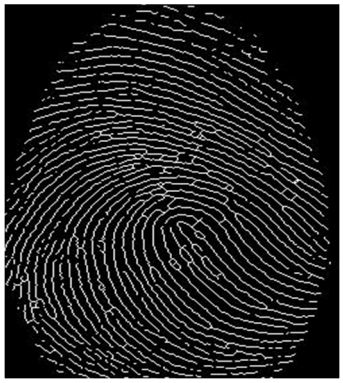
9. Query Normalized Image

10. Orientation Image

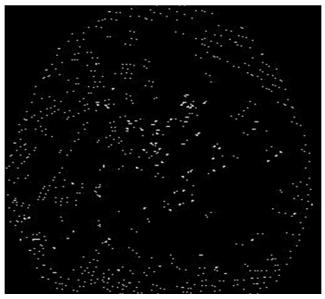


11. Query Binarized Image

12. Query H-Break Removal

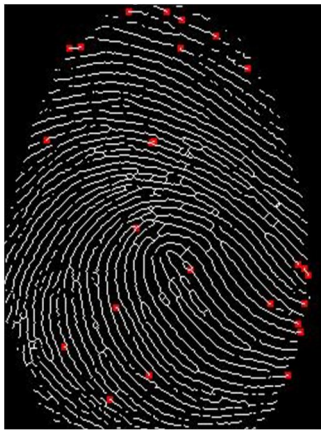


13. All Minutiae Positions



14. False Removal Minutiae Image

15. Minutiae Positions after Removing False Minutiae



III. APPLICATION

Image change detection is a process that analyzes images of the same scene taken at different times in order to identify changes that may have occurred between the considered acquisition dates. In the last decades, it has attracted widespread interest due to a large number of applications in diverse disciplines such as remote sensing, medical diagnosis, and video surveillance. With the development of remote sensing technology, change detection in remote sensing images becomes more and more important. Among them, change detection in synthetic aperture radar (SAR) images exhibits some more difficulties than optical ones due to the fact that SAR images suffer from the presence of the speckle noise. However, SAR sensors are independent of atmospheric and sunlight conditions, which make the change detection in SAR images still attractive.

For the remote sensing images, differencing (subtraction operator) and rationing (ratio operator) are well-known techniques for producing a difference image. In differencing, changes are measured by subtracting the intensity values pixel by pixel between the considered couple of temporal images. In rationing, changes are obtained by applying a pixel-by-pixel ratio operator to the considered couple of temporal images. However, in the case of SAR images, the ratio operator is typically used instead of the subtraction operator since the image differencing technique is not adapted to the statistics of SAR images and non-robust to calibration errors.

In addition, because of the multiplicative nature of speckles, the ratio image is usually expressed in a logarithmic or a mean scale. In the third step, changes are usually detected by applying a decision threshold to the histogram of the difference image. In general, it appears clearly from the literature that the whole performance of SAR-image change detection is mainly relied on the quality of the difference image and the accuracy of the classification method. In order to address the two issues, in this paper, we propose an unsupervised distribution-free SAR-image change detection approach. It is unique in the following two aspects: 1) producing difference images by fusing a mean-ratio image and a log-ratio image, and 2) improving the fuzzy local-information c-means (FLICM) clustering algorithm, which is insensitive to noise, to identify the change areas in the difference image, without any distribution assumption.

IV. 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. The experimental results show that our system achieves a very low error rate.

V. ACKNOWLEDGMENTS

We thank our HOD Dr.T.Thirumurugan, Ph.D. (Department of Electronics and Communication Engineering) to help us for creating this paper with his sincere guidance and Technical Expertise in the field of communication. The help of our guide Ms. C.Janani, M.Tech, Department of ECE, Dr, SJS Pauls College of Engineering and Technology is really immense and once again I thank her for her great motivation. I thank Dr. SJS Pauls College of Engineering and Technology to provide me such a standard educational environment so that I am able to understand the minute concepts in the field of Engineering and Technology.

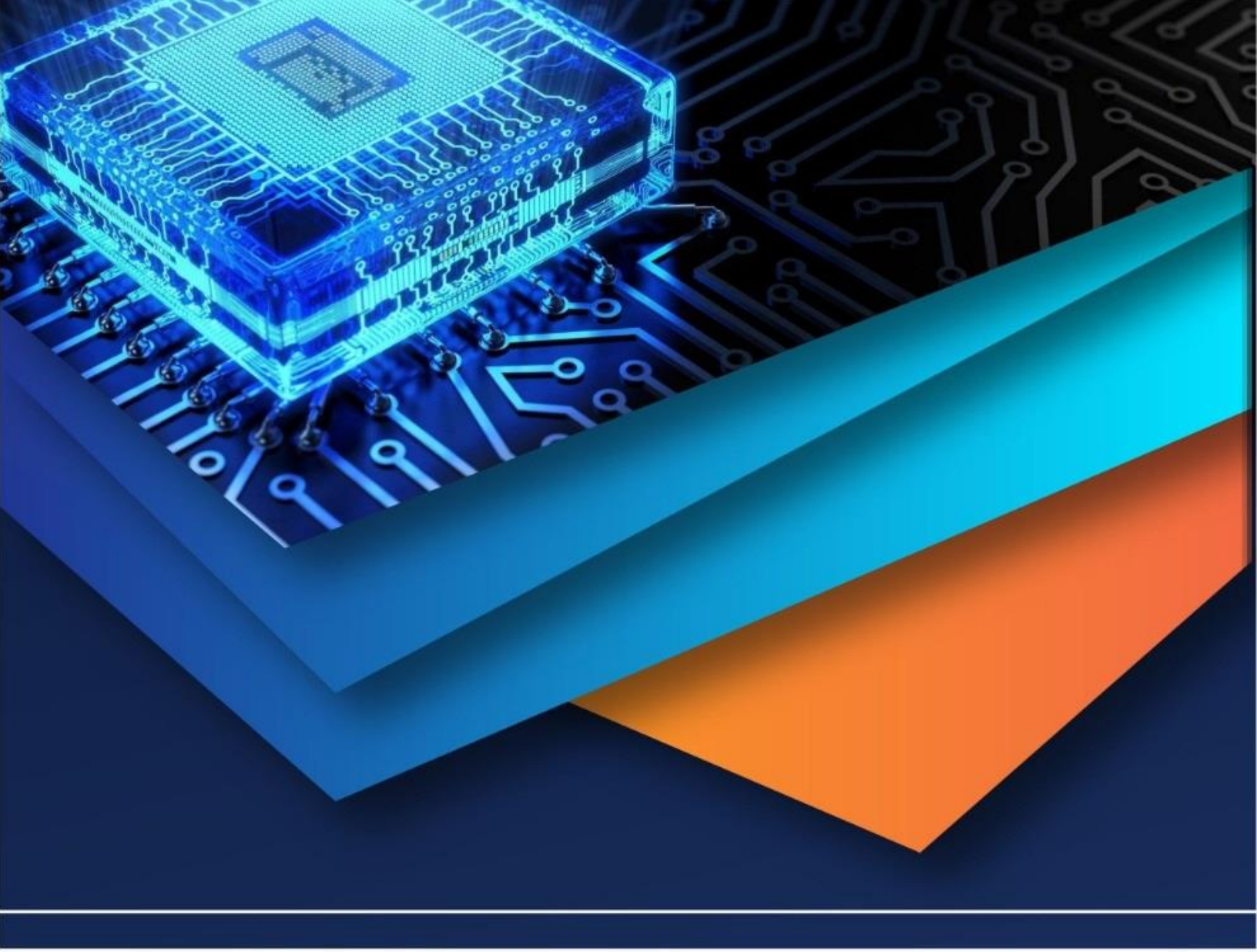
REFERENCES

[1] A. Adler, "Can Images Be Regenerated from Biometric Templates," Proc. Biometrics Consortium Conf., Sept. 2003.
[2] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis," IEEE Trans. Information Forensics and Security, vol. 1, no. 3, pp. 360-373, Sept. 2006.
[3] D. Baldisserra, A. Franco, D. Maio, and D. Maltoni, "Fake Fingerprint Detection by Odor Analysis," Proc. Int'l Conf. Biometric Authentication, Jan. 2006.
[4] A.M. Bazen and S.H. Gerez, "Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 7, pp. 905-919, July 2002.
[5] BioSec European Research Project-FP6 IST-2002-001766, http://www.biosec.org, 2005.
[6] J. Blomme´, "Evaluation of Biometric Security Systems against Artificial Fingers," master's thesis, 2003.
[7] R. Cappelli, "Synthetic Fingerprint Generation," Handbook of Fingerprint Recognition, D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, eds., Springer, 2003.
[8] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Can Fingerprints be Reconstructed from ISO Templates," Proc. Ninth Int'l Conf. Control, Automation, Robotics and Vision, Dec. 2006.
[9] R. Cappelli, D. Maio, D. Maltoni, J.L. Wayman, and A.K. Jain, "Performance Evaluation of Fingerprint Verification Systems," IEEE Trans. Pattern Analysis Machine Intelligence, vol. 28, no. 1, pp. 3-18, Jan. 2006.
[10] M. Donahue and S. Rokhlin, "On the Use of Level Curves in Image Analysis," Image Understanding, vol. 57, no. 3, pp. 185-203, 1993.
[11] Proc. Second Int'l Competition for Fingerprint Verification Algorithms (FVC 2002), http://bias.csr.unibo.it/fvc2002, 2002.
[12] US General Accounting Office, "Using Biometrics for Border Security," Technical Report GAO-03-174, Government Accountability Office, 2002.
[13] C. Hill, "Risk of Masquerade Arising from the Storage of Biometrics," master's thesis, Australian Nat'l Univ., 2001.
[14] Int'l Biometric Group, "Generating Images from Templates,"white paper, IBG, 2002.
[15] ILO SID-0002, "Finger Minutiae-Based Biometric Profile for Seafarers' Identity Documents," Int'l Labour Organization, 2006.
[16] ANSI-INCITS 378-2004, Information Technology—Finger Minutiae Format for Data Interchange, 2004.
[17] ISO/IEC 19794-2:2005, Information Technology—Biometric Data Interchange Formats—Part 2: Finger Minutiae Data, 2005.
[18] H. Kang, B. Lee, H. Kim, D. Shin, and J. Kim, "A Study on Performance Evaluation of the Liveness Detection for Various Fingerprint Sensor Modules," Proc. Seventh Int'l Conf. Knowledge- Based Intelligent Information and Engineering Systems, pp. 1245-1253, 2003.
[19] J. Li, W.Y. Yau, and H. Wang, "Constrained Nonlinear Models of Fingerprint Orientations with Prediction," Pattern Recognition, vol. 39, no. 1, pp. 102-114, 2006.
[20] D. Maio and D. Maltoni, "Direct Gray-Scale Minutiae Detection in Fingerprints," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 1, pp. 27-40, Jan. 1997.
[21] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, and A.K. Jain, "Second Int'l Competition for Fingerprint Verification Algorithms (FVC 2002)," Proc. 16th Int'l Conf. Pattern Recognition, vol. 3,pp. 811-814, Aug. 2002.
[22] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer, 2003.
[23] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," Proc. Int'l Soc. Optical Eng. (SPIE), vol. 4677, Jan. 2002.
[24] NIST Minutiae Interoperability Exchange Test (MINEX), http://fingerprint.nist.gov/minex, 2006.
[25] NIST Special Publication 800-76, "Biometric Data Specification for Personal Identity Verification," Feb. 2005.
[26] W.H. Press, B.P. Flannery, S.A. Teukolsky, and W.T. Vetterling, Numerical Recipes in C: The Art of Scientific file:///C:/Users/SS2/Downloads/kaanchana.jpgComputing. Cambridge Univ. Press, 1988.
[27] T. Putte and J. Keuning, "Biometrical Fingerprint Recognition:Don't Get Your Fingers Burned," Proc. IFIP TC8/WG8.8 Fourth Working Conf. Smart Card Research and Advanced Applications, pp. 289-303, 2000.
[28] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," IBM Systems J., vol. 40, no. 3, pp. 614-634, 2001.
[29] N.K. Ratha, J.H. Connell, and R.M. Bolle, "An Analysis of Minutiae Matching Strength," Proc. Third Int'l Conf. Audio and Video-Based Biometric Person Authentication, pp. 223-228, 2001.

[30] A. Ross, J. Shah, and A.K. Jain, "Toward Reconstructing Fingerprints from Minutiae Points," Proc. Int'l Soc. Optical Eng. (SPIE), Biometric Technology for Human Identification II, A.K. Jain
and N.K. Ratha, eds., pp. 68-80, Mar. 2005.
[31] B. Sherlock and D. Monro, "A Model for Interpreting Fingerprint Topology," Pattern Recognition, vol. 26, no. 7, pp. 1047-1055, 1993.
[32] L. Thalheim and J. Krissler, "Body Check: Biometric Access Protection Devices and Their Programs Put to the Test," c't Magazine, Nov. 2002.
[33] U. Uludag and A.K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints," Proc. Int'l Soc. Optical Eng. (SPIE), Security, Steganography, and Watermarking of Multimedia Contents VI, E.J. Delp III and P.W. Wong, eds., pp. 622-633, June 2004.
[34] P. Vizcaya and L. Gerhardt, "A Nonlinear Orientation Model for Global Description of Fingerprints," Pattern Recognition, vol. 29, no. 7, pp. 1221-1231, 1996.
file:///C:/Users/SS2/Downloads/kaanchana.jpg
[35] C. Watson and M. Garris, "NIST Fingerprint Image Software 2 (NFIS2)," Nat'l Inst. of Standards and Technology, http://fingerprint.nist.gov/NFIS, 2006.
[36] A. Wiehe, T. Sondrol, O.K. Olsen, and F. Skarderud, "Attacking Fingerprint Sensors," NISlab/Gjovik Univ. College, technical report, Dec. 2004, http://olekasper.no/articles/attacking_finger
print_sensors.pdf.
[37] J. Zhou and J. Gu, "Modeling Orientation Fields of Fingerprints with Rational Complex Functions," Pattern Recognition, vol. 37, no. 2, pp. 389-391, 2004.

Sri.Ganesh.D : Author Studies in Final Year Engineering, Department of ECE , Dr. S.J.S Paul Memorial College of Engineering and Technology.

Kaanchana.M : Author Studies in Final Year Engineering, Department of ECE , Dr. S.J.S Paul Memorial College of Engineering and Technology.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY