iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

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

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Efficient Technique for Fingerprint Features Protection and Person Identification Using Wavelet Transform

C. Abirami[1], Dr. M. Baritha Begum Ph.D.[2]
[1]PG Scholar, [2]Assistant Professor, Dept of ECE
Saranathan College of Engineering, Trichy, India

Abstract- Fingerprint recognition is a widely used technique for person identification. The two major techniques for fingerprint identification are minutiae based technique and non-minutiae based technique. In this paper we propose a Discrete Wavelet Transform (DWT) based Fingerprint Recognition technique. The main objective of this paper is to secure the fingerprint features stored in the database and for person identification. Here, Fingerprint image is decomposed into multi resolution sub bands namely LL, LH, HL and HH by applying 3 level DWT. The dominant values like mean energy, Shannon entropy and standard deviation are computed. Feature vectors are generated from the above values and they are encrypted using Hadamard transform technique and stored in the database. In Identification stage, comparison of test fingerprint with the database fingerprint is made based on Euclidean distance value for all the features. Finally, the parameters like FAR, FRR, TSR are estimated. It is found that the experimental results based on Discrete Wavelet Transform are efficient over other existing techniques.
Keywords- Fingerprint Recognition, Wavelet Transform, Feature vector, Hadamard Transform, Feature matching.

I. INTRODUCTION

Biometric technique is used for identifying an individual based on some physiological or behavioral characteristics. Fingerprint, palm print, iris, face comes under physiological characteristics whereas voice, signature and keystroke comes under behavioral characteristics. Fingerprint is a feature pattern of a finger. It is the pattern of Ridges and valleys. The local ridge characteristics that occur either at ridge bifurcation or at ridge ending are called Minutiae points. Fingerprint is an efficient identification technique. The uniqueness of the individual fingerprints, immutability and low cost of the fingerprint system have made it to be the most widely used identification system. Forensic applications like criminal identification and National security issues are in need of efficient fingerprint identification system. Fingerprint identification systems are also used in government agencies; computer based testing, electronic registration and library access. In general, the fingerprint system is basically of two types. They are identification system and verification system. Identification is the process of one to many mapping of test fingerprint with the fingerprint stored in the database. Whereas, verification is the process of one to one mapping of test fingerprint with the fingerprint stored in the database. Fingerprint identification can be carried out with any of the following four approaches. They are minutiae based approach, Ridges based approach, Pore Extraction approach and Image based approach. Minutiae based approach is time consuming since it involves the process like binarization, removal of unwanted spikes, normalization, segmentation, direction estimation, thinning etc. The Ridge based approach involves the process of extraction of ridges in the fingerprint and finding the distance between them using Euclidean distance technique. The pore extraction approach involves extraction of fingerprint feature like pores. The Image based approach requires minimum preprocessing time since the minutiae, ridges and pores are not considered in this approach.

II. RELATED WORK

In [1], the authors have proposed an algorithm based on wavelet transform and Gabor features for fingerprint identification. They detected the center point area of the fingerprint image by calculating Poincare index value and region of interest. By using wavelet transform, the image around the centre of fingerprint is decomposed into sub images to get more features. The Gabor wavelet features were extracted from the sub images and feature vector are generated for matching. In [2], the authors have proposed an algorithm based on wavelets and pseudo Zernike moments for fingerprint verification. By using Wavelet the ridges were extracted. The features which carry the descriptive information about the fingerprint image where extracted using the pseudo Zernike moments. In [3], the author proposed an algorithm to compare the test fingerprint image with the fingerprint image stored in the database as template. From the test fingerprint he extracted minutiae orientation field and the quality map. The features from both level 1 and 2 are used for calculating the match score. In [4], the author proposed a technique based on three stages of matching which includes local orientation structure matching, local minutiae structure matching and global structure matching. By using local minutiae structure, matching the similarity of neighborhood minutiae distribution around minutiae is found. The global minutiae structure is used to evaluate global similarity. From the matching score calculated from the local orientation structure matching, local minutiae structure and global structure matching the final similarity is found. In [5], the author introduced an algorithm for fingerprint verification based edge detection and wavelet. First, the fingerprint image was decomposed to get the high frequency coefficients. Then, the author used prewitt’s edge detector on the images to extract the edge pixel sets. Finally based on threshold value the fingerprint matching was performed.

III. PROPOSED WORK

A. Wavelet Decomposition Of Fingerprint Image

In this paper, a 3 level Discrete Wavelet Transform (DWT) technique have been used. In general, The DWT technique decomposes an image into sub-images or sub-bands. For instance, let us consider 1-level decomposition which consists of the bands LL1, LH1, HL1 and HH1 as shown in fig. 1.

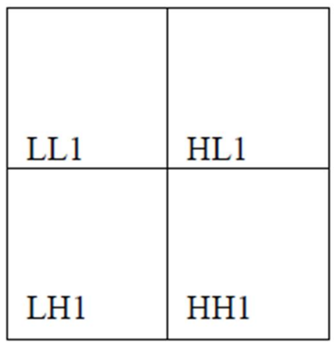


Fig. 1 One level DWT based Fingerprint image decomposition

LL1 band contains the low frequencies both in horizontal and vertical direction. HH1 band contains the high frequencies both in horizontal and vertical direction. HL1 band contains the high frequencies in horizontal direction and the low frequencies in vertical direction. LH1 band contains the low frequencies in horizontal direction and the high frequencies in vertical direction. LL1 is the most significant band because it contains most of the image energy and it also represents the approximations of the image. The remaining bands like HH1, HL1 and LH1 represent the details such as texture of the image. The sub-band LL1 corresponds to coarse level coefficients that is the approximation image while the sub-bands labeled LH1, HL1 and HH1 represents the finest scale wavelet coefficients that is detail images. In order to obtain the next level of wavelet coefficients, the sub-band LL1 alone is further decomposed and critically sampled. This results in two level wavelet decomposition as shown in Fig. 2. Similarly, the sub-band LL2 will alone be considered for next level decomposition.

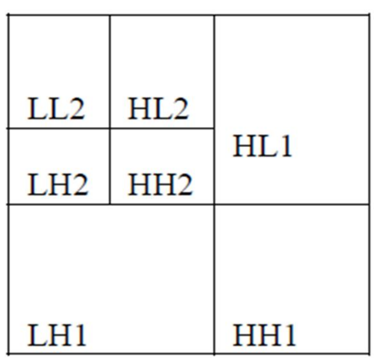


Fig. 2 Two levels DWT based Fingerprint image decomposition

B. Feature Extraction

After three level wavelet decomposition, we are going to consider only HL1, LH1 and HH1 for our analysis. First, consider the band

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

HL3 and find out mean energy, entropy, standard deviation. The mean energy, Shannon entropy and standard deviation are statistical measure of transform domain.

$$e_1^j = \frac{1}{N^2} \sum_{k=1}^{N} |c_k^j| \qquad (1)$$

$$e_2^j = \sqrt{\frac{1}{N^2} \sum_{k=1}^{N} (|c_k^j| - \mu)^2} \qquad (2)$$

$$e_3^j = \frac{1}{N^2} \sum_{K=1}^{N} |C_k^j|^2 \log |C_k^j|^2 \qquad (3)$$

Where e_1^j, e_2^j, e_3^j represents mean energy, standard deviation and shannon entropy respectively and j=1,2,3 represents horizontal, vertical and diagonal sub bands respectively. c_k^j denotes the wavelet coefficients of the three high frequency sub bands. The feature vector F is estimated using the following expression,

$$F = \{e_1, e_2, e_3\} \qquad (4)$$

Similarly, the feature vectors for the remaining bands like LH3 and HH3 are also calculated and finally a feature vector matrix of order 3x3 is formed.

C. Data Encryption Using Hadamard Transform Technique

The overall block diagram of the proposed system is shown in Fig 3. In this proposed scheme, we are going to use Hadamard transform for the protection of feature vector. First, we are going to form a 3x3 matrix from the features extracted from the sub bands. That is, the feature vector F value is calculated after three level of wavelet decomposition. Then, a 4x4 matrix is generated by appending zeros to the already generated 3x3 feature vector matrix. Then, multiply the 4x4 feature vector matrix with the non-binary 4x4 Hadamard matrix. It is hard to break the transformed message because the transformation is carried out at various levels. Finally the transformed data is stored in the database. The inverse transform is carried out during identification stage.

The proposed method consists of two stages, namely Enrollment stage and Identification stage as shown in Fig. 3. In the enrollment stage first, fingerprint image is fetched and the preprocessing is carried out. Then, 3 level decomposition is performed on the preprocessed image. The feature vector F is calculated from the values of mean energy, standard deviation and Shannon entropy. Then, feature vector set is generated. After the generation of feature vector matrix, it is protected using Hadamard transform technique.

Enrollment Stage

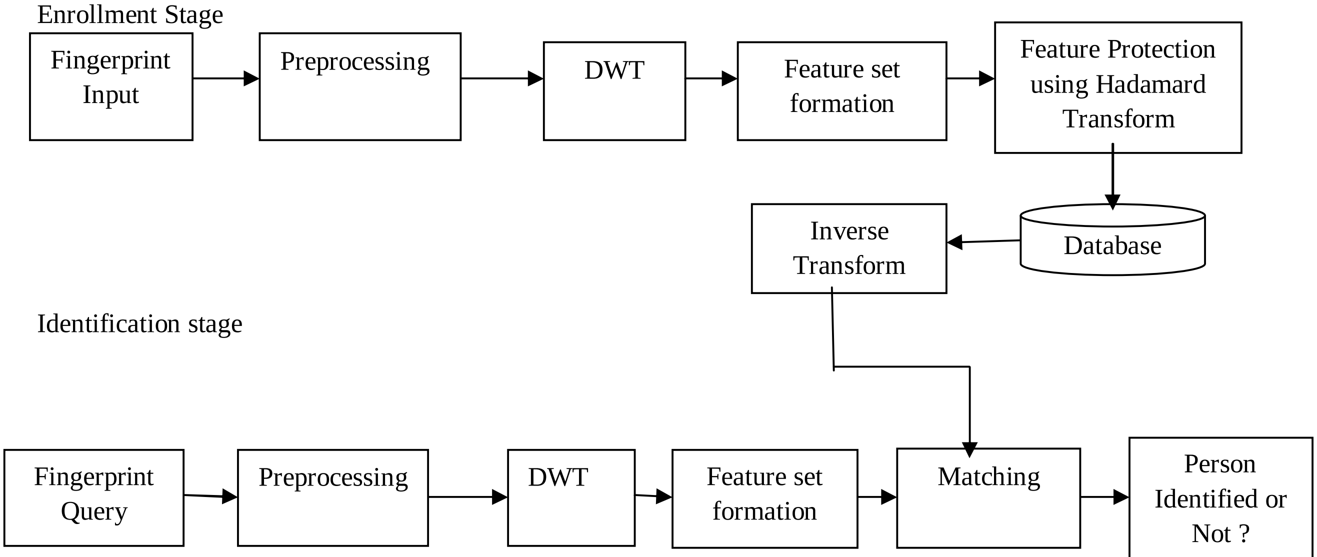


Fig 3. Block diagram of the proposed technique

In the identification stage, the similar process is carried out till feature vector formation. Then, inverse transform is taken for values stored in the database and it is used for matching with the feature set formed from the identification stage.

IV. EXPERIMENTAL RESULTS

The proposed scheme is implemented using the MATLAB Software. Here, we are going to consider fingerprint template of different persons. The experiment is carried out in two stages namely enrollment stage and identification stage. The performance of the proposed system is estimated using the parameters like FAR, FRR, TSR.

False Acceptance Rate (FAR): It is the probability of an imposter being accepted as an authorized user.
FAR is the ratio of the number of False Acceptances (FA) to the number of identification attempts.

$$FAR = \frac{\text{Number of FA}}{\text{Number of identification attempts}} \times 100\% \quad (5)$$

False Rejection Rate (FRR): It is the probability of a legitimate user being rejected as an imposter.

FRR is the ratio of the number of False Rejections (FR) the number of identification attempts.

$$FRR = \frac{\text{Number of FR}}{\text{Number of identification attempts}} \times 100\% \quad (6)$$

Total Success Rate (TSR): It is the rate at which match occurs successfully.

Fig 4. Input Fingerprint Image

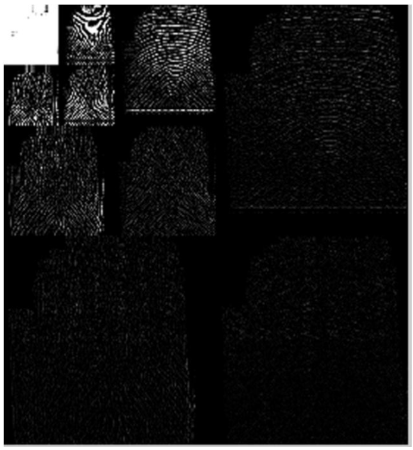


Fig 5. Decomposition of fingerprint image using three levels DWT

TABLE I PERFORMANCE EVALUATION

Parameters	N=7	N=10	N=15
FAR	3.90 %	2.89%	2.81 %
FRR	0	0	0
TSR	96.10 %	97.11 %	97.19 %

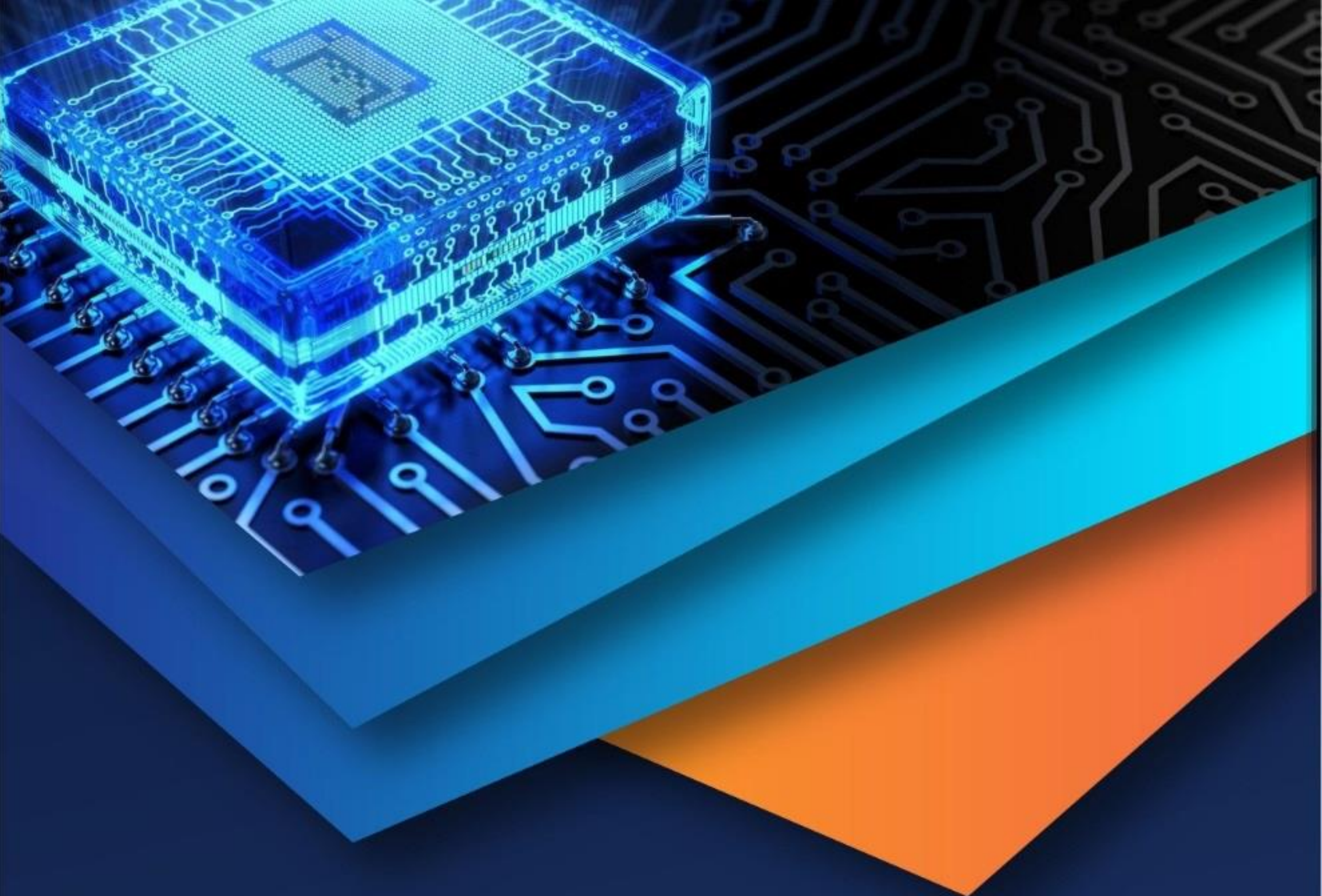
Table I shows the performance evaluation of fingerprint features after three level wavelet decomposition. The parameters like FAR, FRR and TSR are calculated by varying the No. of feature vectors stored in the database.

V. CONCLUSION

Biometric Fingerprint can be used for both identification and verification purpose. In this paper, we used Discrete Wavelet transform based system for person identification. Here, we used Hadamard transform technique for feature vector data protection which increases the security level of the proposed system. This technique provides reduced FAR and FRR values compare to the conventional systems.

REFERENCES

[1] Xu Cheng, CHENG Xin-Ming, “An Algorithm for Fingerprint Identification Based on Wavelet Transform and Gabor Features,” Third IEEE International Conference on Genetic and Evolutionary Computing, pp. 827-830, 2009.
[2] Avinash Pokhriyal and Sushma Lehri, "A New Method of Fingerprint Authentication using 2-D wavelets", Journal of Theoretical and Applied Information Technology, vol. 13, no.2, pp. 131 - 138, March , 2010.
[3] Anil K. Jain, Jianjiang Feng, Abhishek Nagar and Karthik Nandakumar, “On Matching Latent Fingerprints,” IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp.1-8, 2008.
[4] Honglie Wei and Danni Liu, “A Multistage Fingerprint Matching Algorithm,” Proceedings of the IEEE International Conference on Automation and Logistics, pp.197-199, 2009.
[5] Zhou Weina, HanJun, Zeng Xiaoyang, and Yan WeiWei, “Fingerprint Verification Based on Wavelet and Edge Detection,” Ninth IEEE International Conference on Electronic Measurement and Instruments, vol 3, pp. 1001-1004, 2009.
[6] Ting Tang, “Fingerprint Recognition using Wavelet Domain Features” (ICNC) 8th International Conference on Natural Computation, 2012,pp 531-534.
[7] Marius Tico, Eero Immonen, Pauli Ramo, Pauli Kuosmanen and Jukka Saarinen, “Fingerprint Recognition Using Wavelet Features” 0-7803-6685-9/01/2001 IEEE.



10.22214/IJRASET

INDEX COPERNICUS 45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY