Feature Level Fusion Based Bimodal Biometric Using Transformation Domine Techniques

[1]Ramachandra A C, [2]Abhilash S K, [2]K B Raja, [3]Venugopal K R, [4]L M Patnaik

[1]Department of Electronics and Communication, Alpha College of Engineering, Bangalore, 560077.
[2]Department of Electronics and Communication, University Visveswaraya College of Engineering, Bangalore,
[3]Principal, University Visveswaraya College of Engineering, Bangalore, Karnataka, India,
[4]Honorary Professor, Indian Institute of Science, Bangalore, Karnataka, India,

Abstract: *Bimodal biometric used to authenticate a person is more accurate compared to single biometric trait. In this paper we propose Feature Level Fusion based Bimodal Biometric using Transformation Domine Techniques (FLFBBT). The algorithm uses two physiological traits viz., Fingerprint and Face to identify a person. The Region of Interest (ROI) of fingerprint is obtained using preprocessing. The features of fingerprint are extracted using Dual Tree Complex Wavelet Transforms (DTCWT) by computing absolute values of high and low frequency components. The final features of fingerprint are computed by applying log on concatenated absolute value of high and low frequency components. The face image is preprocessed by cropping only face part and Discrete Wavelet Transforms (DWT) is applied. The approximation band coefficients are considered as features of face. The fingerprint and face image features are concatenated to derive final feature vector of bimodal biometric. The Euclidian Distance (ED) is used in matching section to compare test biometric in the database, it is observed that the values of EER and TSR are better in the case of proposed algorithm compared to individual transformation domain techniques.*

Keywords*: Biometrics, Face, Fingerprint, DWT and DTCWT*

I. INTRODUCTION

The authentication of a person using biometric is accurate and robust compared to traditional methods of identification. The security can be easily broken if the traditional methods of personal authentication using password and ID cards since they can be stolen or lost. In presence of sophisticated biometric identification system any unusual such as robbery, entry of an unauthorized person etc ., can be avoided. The biometric identification system is based on characteristics features of human body such as eyes, face, fingerprint, DNA etc., which are known as *Physiological Biometrics* which are constant throughout the life time and the behavior of person which depends on age and mood of a person such as signature, keystroke etc., known as *Behavioral Biometrics*, which are not constant throughout the life. The biometric system is operated in two different modes based on the application such as (i) *Verification Mode*: it is one to one comparison of test biometric with the template stored in database, (ii) *Identification Mode*: it is one to many comparisons of test with the database, if the comparison is nearer to the predefined threshold value then the person is identified.

The general biometric system has data acquisition section, preprocessing section, feature extraction section, matching section. The function of data acquisition section is to collect the number of sample of biometrics in different conditions and store it as a database. In preprocessing section the images are normalized by colour converting, cropping and resizing. The features are extracted from normalized image in feature extraction section by using spatial domine, transformation domine or combination of both. The final results are obtained from extracted features in matching section by using the distance formulas like Euclidian Distance (ED), Hamming Distance, Chi-square, Linear Discriminant Analysis, Support Vector Machine, Neural Networks etc., The biometric systems are very much essential in applications like Home Security, Airport Checking, Voting machine, Entry to high security zone like parliament House, ATM, Laptop, public places like shopping mall etc.,

The multimodal biometrics systems address the problem of single biometric system by considering multiple evidences produced by multiple biometric traits. Multimodal biometric systems also provide anti-poofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. An integration fusion scheme is required to fuse the information presented by the individual modalities.

Contribution: In this paper FLFBBT algorithm is proposed to identify a person. The fingerprint and face of each person is considered and features are extracted using DTCWT and DWT respectively. The ED is used in matching section to authenticate a person.

Organization: This paper is organized into following sections. Section 2 is an overview of Literature Survey. The proposed model is described in Section 3. Section 4 discusses the Algorithm; Performance analysis of the system is presented in Section 5 and Conclusions are contained in Section 6.

II. LETRAERETURE SURVEY

Wang Wenchao and Sun Limm [1] discussed a Fingerprint identification algorithm that combines point match and image match. This algorithm depends on singular point abstraction and wavelet transform coefficient. First singular points are extracted for rough match and image calibration. Ma Yinping and Huang Yongxing [2] introduced a kind of wavelet transform adaptive threshold of the Fingerprint image denoising method. The approach is one of the Fingerprint image wavelet decomposition, and then based on Bayes framework, selecting different optimal threshold, combined with soft threshold value method to Fingerprint image denoising, improve the Fingerprint image Peak Signal-to-Noise Ratio. Atif Iqbal and Anoop Namboodiri [3] explore the effectiveness of weak features in a cascade for filtering fingerprint databases considering a set of potential indexing features computed from minutiae triplets and minutiae quadruplets. Each stage of filtering consists of projecting the probe onto a specific line and the removal of database samples outside a window around the probe. Hao et al., [4] proposed an algorithm based on multiple minutiae partitions to match general distorted fingerprints. Minutiae in an input and a template fingerprint are globally partitioned into pairs of multiple neighbors, each of which consist of similar local minutia topology and features. The minutia similarity is additionally evaluated by investigating ridge shape and the geometric similarities of the corresponding neighbor minutiae. Jinhai Zhang [5] discussed methods of fingerprint image segmentation. Some of the segmentation methods are classified based on block variance method, Pattern methods, and synthesis method. The grading segmentation method automatically identifies some close value in a hierarchical segmentation.

Arun et al., [6] proposed the feature extraction techniques for three modalities viz. Fingerprint, iris and Face. The extracted information from each modality is stored as a template. The information are fused at the match score level using a density based score level fusion, Gaussian Mixture Model (GMM) followed by the Likelihood ratio test. Ngoc-Son Vu and Alice Caplier [7] invented a feature descriptor set called Patterns of Oriented Edge Magnitudes (POEM) for feature extraction by applying the self-similarity operator on accumulated edge magnitudes across different directions. Based on these Features, two feature descriptors are constructed. Carlos et al., [8] proposed an Active Shape Models (ASM) landmark selection scheme to improve the ASM performance in face recognition applications. The proposed scheme selects robust landmark points where relevant facial features are found and assigns higher weights to their corresponding features in the face classification stage. Xiaoni Liang and Weiqing Tong [9] presented an accurate and fast approach to estimate the pose of face in near-infrared images. The approach automatically extracts the feature points from a normalized face image. The pupils and nose tip are used to estimate the pose rotation of yaw and the pupils, nose tip and the center line of mouth is used to estimate the pose rotation of pitch.

Ajay Kumar and Yingbo Zhou [10] proposed a system which simultaneously acquires the finger-vein and low-resolution fingerprint images and combines these two evidences using a score-level combination strategy. The two score-level combinations are holistic and nonlinear fusion. Kolhandai et al., [11] present an intelligent hybrid features based face recognition method which combines the local and global approaches to produce a complete a robust and high success rate face recognition system. The global features are computed using principal component analysis while the local features are ascertained configuring the central moment, Eigen vectors and the standard deviation of the eyes, nose and mouth segments of the human face as the decision support entities of the Generalized Feed Forward Artificial Neural Network. Ramya et al., [12] proposed a system with key is generated from the fused feature which is of greater than 128 bit which is enough for AES encryption, Hash Encoding and AES decryption is done. Message is subjected to hash and hash of message is obtained and it is given to AES encryption as a message and the key is obtained from the fused feature.

Lili Liu and Tianjie Cao [13] defined an efficient verification system based on biometrics, which access real system resources without physical key. Based on the pattern matching, the feature are extracted from the fingerprint images, the feature depends on the position and angle of the input fingerprints. The ridges and valleys structure information integration is employed to perform the fingerprint minutiae alignment. Biggio et at., [14] have investigated the robustness of different score fusion rules for multimodal biometric verification systems, against spoofing attacks for Fingerprint and Face biometrics. The simulated worst-case scenario considered is not representative of the score distribution of real spoofing attacks. Abhishek Nagar et at., [15] discussed a feature-level fusion framework for the design of multi biometric cryptosystems that simultaneously protects the multiple templates of a user using a single secure sketch. The feasibility of such a framework has been demonstrated using both fuzzy vault and fuzzy commitment.

III. MODEL

In this section the block diagram of the proposed model as shown in Figure 1 is discussed. The two biometric traits viz., Fingerprint and Face of a person are considered together to identify a person. The transform domain techniques such as DTCWT and DWT are used to extract Features from Fingerprint and Face respectively.

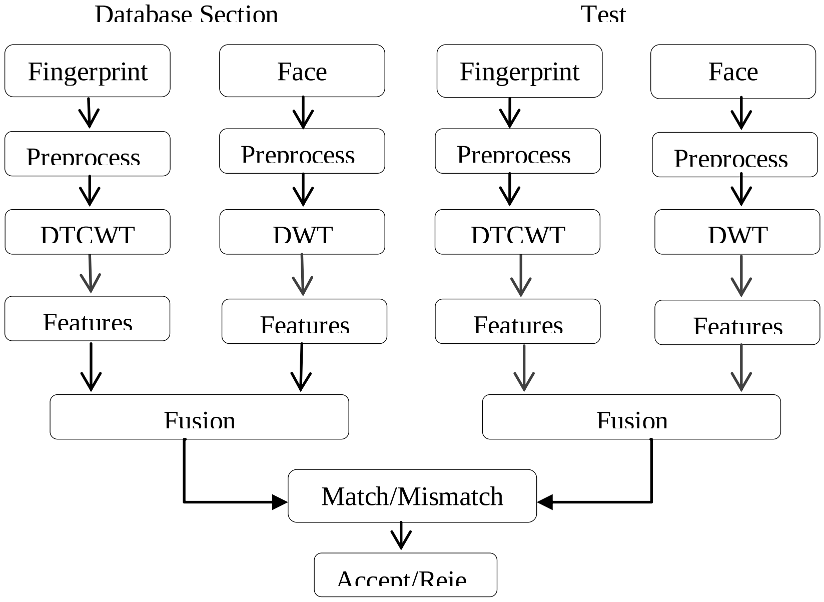


Figure 1: Block diagram of proposed algorithm

3.1. DATABASE:

3.1.1. *Fingerprint database*: The DB3 Fingerprint database from FVC2004 competitions is considered to test the algorithm. The database consists of 110 persons with 8 Fingerprint images per person having image size of 300x480 with a resolution of 512 dpi. The Fingerprint images are collected in three different sessions with at least two weeks' time separating each session using thermal sweeping sensor [16]. The DB3 has eight images of single person shown in Figure 2. The Fingerprint database is created in our proposed model by considering minimum of 10 persons and maximum of 40 persons with 6 images per persons. The number of images with database varies between 60 and 240. The Seventh and Eighth Fingerprint images of each person used in the test section. The number of persons considered with out off database varies from 5 to 30 with one Fingerprint images per person.

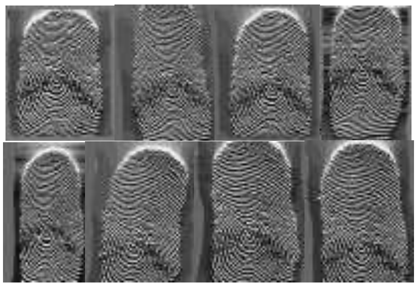


Figure 2: Fingerprint Images of DB3 FVC2004

3.1.2. *Face database*: The Olivetti Research Laboratory (ORL) gray scale [17] is considered to test the proposed model. The data base has 40 persons and 10 images per person i.e., 400 Face images in the database. The each Face image has frontal view with slight tilt of head with a size of 92 x 112. To test the proposed modal, the Face data base is created by considering 10 persons to 40 persons with six images per person. The seventh and eight images of each person are considered as test images. The out off database has five persons to 30 persons with one Face image per person is used to compute FAR. The Face image samples of one person are shown in figure 3.

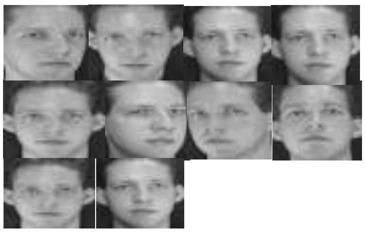
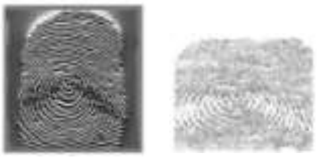


Figure 3: Face Images of ORL

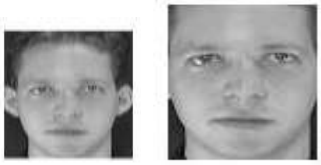
1.2. PREPROCESSING:

The Fingerprint image of size 300 x 480 is manually cropped to a dimension of 201 x 401 to obtain Region of Interest (ROI) Fingerprint area by eliminating four side edges. The size of ROI is resized to 256 x 256 to apply DTCWT for Features. The original Fingerprint image and its cropped and resized image are shown in figure 4. The original Face image of size 92 x 112 is manually cropped to obtain ROI of size 71 x 93 by eliminating edge of Face image. The ROI is resized to an arbitrary value say size of 192 x 192 to apply DWT to derive Features. The original Face image and its cropped and resized image are shown in figure 5.



(a) (b)

Figure 4: (a) Original Fingerprint Image (300 x 480)
(b) Preprocessed Fingerprint Image (256 x 256)



(a) (b)

Figure 5: (a) Original Face Image (92 x 112)
(b) Preprocessed Face Image (192 x 192)

1.3. FEATURE EXTRACTION:

The Transform Domain Features from the Fingerprint and Face image are obtained by using the Dual Tree Complex Wavelet Transforms (DTCWT) and Discrete Wavelet Transforms (DWT) transforms respectively. The logarithm is applied on DTCWT magnitudes of Fingerprint to obtain Final Features of Fingerprint image. The Final Fingerprint Features and Features of Face are fused by concatenating to derive the Final set of Features to test the algorithm.

3.3.1. *DTCWT:* It produces complex coefficients by using dual tree wavelet filters and gives real and imaginary parts, which consists of both low frequency and high frequency bands. The high frequency band is ignored and low frequency band is considered and decomposed into two parts for next levels and process is continued until the required six levels as shown in Figure 6. At level six all the low frequency coefficients and high frequency coefficients from both real and imaginary parts are considered. The magnitudes of both real and imaginary parts are calculated using Equations 1 and 2 respectively and have a dimension of 1 x 48. Magnitudes are concatenated as given in Equation 3 to obtain a single Vector with a dimension of 1 x 96. For the obtained single Vector logarithmic scale is applied as given in Equation 4 to normalize the magnitude, which is considered as Feature Vector F_{FP} for Fingerprint image.

$$M_L = \sqrt{[(R_L 6)^2 + (I_L 6)^2]} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$M_H = \sqrt{[(R_H 6)^2 + (I_H 6)^2]} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

$$M = [M_H : M_L] \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (3)$$

$$F_{FP} = Log(M) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

3.3.2 *DWT:* The preprocessed Face image of size 192 x 192 is considered and one level haar wavelet is applied using base Equation 5 to derive four sub bands such as Approximation band, Horizontal band, Vertical band and Diagonal band as shown in Figure 7. The Approximation band has low frequency components and has significant information of Face image. The Horizontal, Vertical and Diagonal bands are high frequency bands and have in significant information of Face image like edge information's. The approximation band coefficients are considered as Features of Face image F_F which is of dimension 1 x 9216.

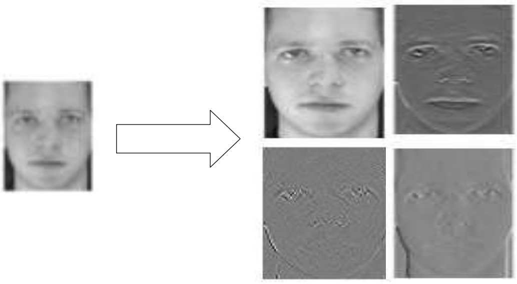


Figure 6: DWT sub bands of Face image.

$$\varphi(t)=\begin{cases}1 & 0\le t<1/2\\ -1 & 1/2\le t<1\\ 0 & otherwise\end{cases} \qquad \text{.............................. (5)}$$

1.4. Fusion of Features:

The Log DTCWT feature of Fingerprint F_{FP} and Approximation band coefficient F_F of DWT of Face image are concatenated to obtain Final feature Vector set for bimodal biometrics. The Final feature Vector FFV is given in Equation six Equation 5. The Final feature Vector size is of 1x 9312.

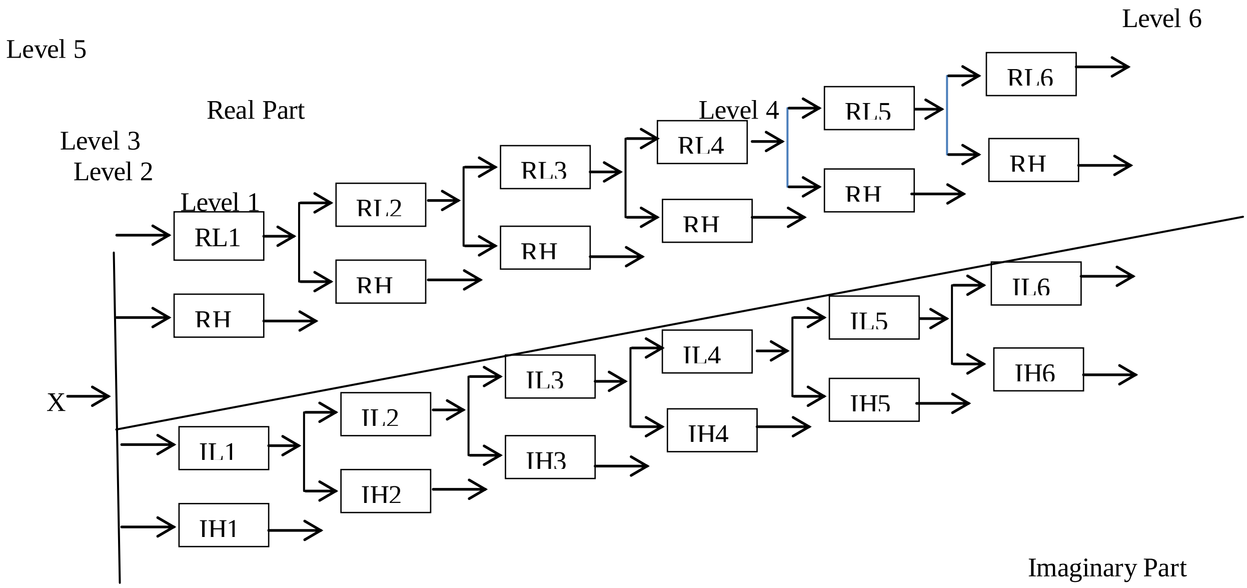


Figure 6: Different levels of DTCWT.

$$FFV=[F_{FP}:F_F] \qquad \text{...................... (6)}$$

1.5. Matching:

The Final fused feature Vector derived from both Fingerprint and Face images are considered to test match/non match of a person. The Final fused Features of test image are compared with Final fused Features of database images using Euclidian distance as given in Equation 7.

$$d(p,q)=\sqrt{\frac{1}{M}\sum_{i=1}^{M}(p_i-q_i)^2} \qquad \text{................ (7)}$$

M = Dimension of Vector.

P_i = Data Feature Vector

Q_i = Test Feature Vector

The TSR, FRR and FAR values are computed by compared ED values with predefined thresh hold values.

IV. ALGORITHM

Problem Definition: The proposed bimodal biometric algorithm using Log (DTCWT) and DWT to identify a person is discussed and is given in Table 1

The Objectives:

- The bimodal biometric recognition is identified using fusion of DTCWT and DWT coefficients.
- To reduce FAR,FRR and EER
- To increase TSR

Table 1: Algorithm of proposed System.

INPUT: Fingerprint and Face images.
OUTPUT: Matched /Non-matched Test image

1. Resize Fingerprint image to 256x256.
2. DTCWT is applied on Fingerprint of database and test Fingerprint.
3. The Fingerprint initial features are obtained by concatenation of magnitudes of low and high frequency components.
4. The Fingerprint final features are derived by Log of initial features.
5. Resizing of Face image to 192x192.
6. DWT is applied on database images and test image.
7. The Face features are obtained by considering coefficients of approximate bands.
8. The bimodal biometric final features are derived by concatenation of Fingerprint and Face features.
9. The final features of test image are compared with final features of images in the database using ED.

V. PERFORMANCE ANALYSIS:

The Fingerprint databaseFVC2004 DB3 and Face database ORL are considered to test the proposed algorithm in terms of the following performance parameters.

1. ***False Acceptance Rate (FAR):***

It is the probability that an unauthorized person is incorrectly accepted as authorized person and it is computed using Equation 8

$$FAR = \frac{\text{Number of unauthorized persons Identified}}{\text{Total Number of unauthorized persons}} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ (8)$$

2. ***False Rejection Rate (FRR):***

It is the probability that the authorized person is incorrectly rejected and it is computed using the Equation 9.

$$FRR = \frac{\text{Number of authorized persons rejected}}{\text{Total Number of authorized persons}} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..\ (9)$$

3. ***Equal Error Rate (EER):***

It is the rate at which both *FAR* and *FRR* are equal.

4. ***Total Success Rate (TSR):***

It is the rate at which match occurs successfully. The Numbers of persons recognized correctly in the database is given in the Equation 10.

$$\%TSR = \frac{\text{Number of persons recognized correctly}}{\text{Total Number of persons in the database}} * 100 \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ (10)$$

The proposed algorithm is robust in recognition of a person as it uses two biometric traits. The variation of FRR, FAR and percentage TSR with threshold is tabulated in the Table 2 As threshold value increases the FRR values decreases from 1 to zero whereas FAR and TSR values increases .The maximum percentage TSR value of 90% is achieved from 0.7 threshold value.

The variation of EER and TSR values for test images 7 and 8 of each person with Persons Inside Database (PIDB): Persons Outside Database (PODB) are given in Table 3.The values of EER increases with PODB and PIDB.The values of EER and TSR depends on the test images, i.e., for test image number 7, EER is 0.16 and TSR is 70% for PIDB and PODB combination of 10:30 and for test image number 8, EER is 0.13 and TSR is 90%. For PIDB and PODB combination10:30.

Table 2: FRR, FAR and % TSR for different Threshold.

Thresh Hold	FRR	FAR	%TSR
0	1	0	0
0.05	1	0	0
0.25	1	0	0
0.3	0.9	0	10
0.4	0.8	0	20
0.45	0.6	0	40
0.5	0.5	0	50

0.55	0.4	0.033	60
0.6	0.2	0.033	70
0.65	0.2	0.1	70
0.7	0	0.2	90
0.75	0	0.4	90
0.8	0	0.633	90
0.85	0	0.733	90
0.9	0	0.833	90
0.95	0	0.9	90
1	0	0.96	90

Table 3: Comparison of EER and Percentage of TSR for different PIDB: PODB.

The variations of FAR and FRR with threshold for PIDB and PODB combination 10:30 is given in Figure 7. As threshold increases FRR decreases and FAR increases the EER value of 0.13 is intersection of FRR and FAR plot.

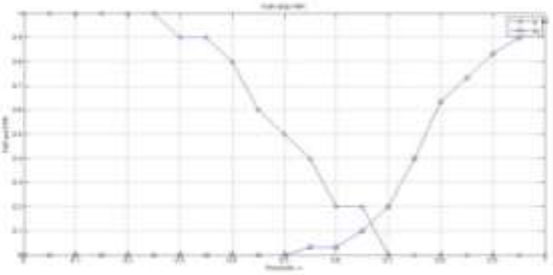


Figure 7: Plot of FAR and FRR V/S Thresh Hold with Log

The values of EER and TSR for DTCWT, DWT and combinations of LOG (DTCWT) and DWT i e., proposed algorithm is given in Table 4. It is observed that the proposed algorithm has low EER value compared to individual DTCWT and DWT algorithms. The value of percentage TSR is high in the case of proposed algorithm compared to individual transformation algorithms. Hence the proposed bimodal biometric algorithm has better efficiency and also robust as two biometric traits are used to identify a person compared to single biometric trait.

Table 4: Comparison of EER and Percentage of TSR for different Transforms and Proposed Algorithm.

Parameters	Method		
	DTCWT	DWT	Proposed FLFBBT
EER	0.18	0.485	0.13
%TSR	80	40	90

VI. CONCLUSION:

In this paper FLFBBT algorithm is proposed to identify a person accurately. The DTCWT is applied on ROI of fingerprint and computed magnitudes of low and high frequency components. The features of fingerprint are derived by applying log on concatenated magnitudes of low and high frequency components. The DWT is applied on face image and features are extracted by coefficients of approximate band. The final features of bimodal biometrics are computed by concatenating fingerprint and face features. The ED is used for comparison to authenticate a person. It is observed that the values of EER and TSR are better in the proposed algorithm compared to individual transform domain techniques. In future the algorithm can be verified by using both spatial domain techniques and transform domain techniques at different levels of fusion.

REFERENCES

[1] Wang Wenchao and Sun Limin, “A Fingerprint Identification Algorithm Based on Wavelet Transformation Characteristic Coefficient,” *International Conference on Systems and Informatics*, pp1-3, 2012.

[2] Ma Yinping and Huang Yongxing, “Adaptive Threshold Based on Wavelet Transform Fingerprint Image Denoising,” *International Conference on Computer Science and Electronics Engineering*, pp. 494- 497, 2012.

[3] Atif Iqbal and Anoop Namboodiri, “Cascaded Filtering for Fingerprint Identification using Random Projections,” Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp. 77- 82, 2012.

[4] Hao NI, Dongju LI, Tsuyoshi Isshiki and Hiroaki Kunieda, “Robust Multiple Minutiae Partitions for Fingerprint Authentication,” *International Symposium on Biometrics and Security Technologies*, pp. 35- 44, 2012.

[5] Jinhai Zhang, “The research of fingerprint image Segmentation method,” *Second International Conference on Consumer Electronics, Communications and Networks*, pp. 701- 704, 2012.

[6] S ArunVivek, J Aravinth and S Valarmathy, “Feature Extraction for Multimodal Biometric and Study of Fusion Using Gaussian Mixture Model,”*Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering,* pp. 391-392, 2012.

[7] Ngoc-Son Vu and Alice Caplier, “Enhanced Patterns of Oriented Edge Magnitudes for Face Recognition and Image Matching” *IEEE Transactions on Image Processing*, vol. 21, no. 3, 2012.

[8] Carlos A. R. Behaine and Jacob Scharcanski, “Enhancing the Performance of Active Shape Models in Face Recognition Applications,” *IEEE Transactions on Instrumentation and Measurement*, vol. 61, no. 8, 2012.

[9] Xiaoni Liang and Weiqing Tong, “Face Pose Estimation Using Near-Infrared Images,” *International Conference on Communication Systems and Network Technologies*, pp. 216- 220, 2012.

[10] Ajay Kumar and Yingbo Zhou, “Human Identification Using Finger Images,” *Transactions on Image Processing*, vol. 21, no. 4, April 2012.

[11] Kolhandai Yesu, Himadri Jyoti Chakravorty, Prantik Bhuyan, Rifat Hussain and Kaustubh Bhattacharyya, “Hybrid Features Based Face Recognition Method Using Artificial Neural Network,” Second National Conference on Computational Intelligence and Signal Processing, pp. 40 – 46, 2012.

[12] M.Ramya, A. Muthukumar and S.Kannan, “Multi biometric based Authentication using Feature Level Fusion,” *International Conference on Advances In Engineering, Science And Management*, pp. 191- 195, 2012.

[13] Lili Liu and Tianjie Cao, “The Research and Design of an Efficient Verification System Based on Biometrics,” *International Conference on Computer Science and Electronics Engineering*, pp. 707-710, 2012.

[14] B Biggio, Z Akhtar, G Fumera, G L Marcialis and F Roli, “Security Evaluation of Biometric Authentication Systems Under Real Spoofing attacks,” *IET Biometrics*, Vol. 1, pp. 11–24, 2012.

[15] Abhishek Nagar, Karthik Nandakumar and Anil K Jain, “Multibiometric Cryptosystems Based on Feature Level Fusion,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no.1, pp. 225-268, 2012.

[16] *http://bias.csr.unibo.it/fvc2004/default.asp,* FVC2004-Third International Fingerprint Verification Competition.

[17] Ferdinando Samaria and Andy Harter, “Parameterization of a Stochastic Model for Human Face Identification,” *Proceedings of Second IEEE Workshop on Applications of Computer Vision*, December 1994.