A Dual Security Scheme Based On DWT for Personnel Authentication

P. Sivananthamaitrey, V. Venkata Krishna, Addanki Purna Ramesh, P. Satyanarayana Murty

Abstract: ***A biometric identification system that audits the presence of a person using real or behavioral features is safer than passwords and number systems. Present applications are mostly recognize an individual using the single modal biometric system. However, a single characteristic sometimes fails to authenticate accurately. Multimodal biometric technologies solve the problems that exist in the single biometric systems. It is very hard to identify images with low lighting environments using facial recognition system. By utilizing fingerprint recognition, this issue can be better addressed. This paper presents a dual personnel authentication system that incorporates face and fingerprint to improve security. For face identification, the Discrete Wavelet Transform (DWT) algorithm is used to acquire features from the face and fingerprint pictures. The technique used to integrate fingerprint and face is decision level fusion. By adding fingerprint recognition to the scheme, the proposed algorithm decreases the false rejection rate (FRR) in the face and fingerprint recognition and hence increases the accuracy of the authentication.***

Keywords: Biometric system, face recognition, fingerprint recognition, discrete wavelet transform (DWT), false rejection rate (FRR), fusion, Eigen values, Eigenfaces.

I. INTRODUCTION

Generally, passwords, tokens or cards are used to facilitate access into security systems. In addition, safety can crash if someone else knows a password or a token or card that an impostor has stolen or misused. Biometrics may diminish the problems related to traditional verification methods. Biometrics implies the automatic identification (or verification) of an individual. A biometric model utilizes an individual's unique physiological or behavioral characteristics to distinguish between a person and another. A few examples are as follows: face, fingerprint, iris pattern, voice analysis, gait analysis, matching veins and etc. These are individual characteristics and are often highly difficult to fake. The biometric system's primary aim is to obtain a person's biometric data, extract a set of characteristics to the stored database to make a decision about the authenticity of the user.Unimodal biometric devices have limitations such as uniqueness, high spoofing frequency, high error rate, non-universality, and noise. A multimodal authentication system that makes personal recognition depends on various physiological or behavioral features [1]. A biometric multimodal system is used to fix these problems. A multimodal biometric structure is a mix of two or more biometric characteristics.

In the biometric fusion, the system extracts data of each image and in the final merged image obtains the efficient representation. The main problem in developing a multi-biometric scheme is dependent on the type of data to be fused [2]. In this paper, a dual security system for people authentication is implemented, that depends on face and fingerprint recognition. Using the Eigenface approach, face and fingerprints are detected and the features are obtained by using DWT based algorithm.

II. LITERATURE REVIEW

Mostly in multimodal biometric systems two or more biometric traits are used to authenticate a person, due to this it consumes more time for authentication. Similarly it occupies more space for storing the user's information.

"A Multimodal multi-algorithm biometric security" An integration of two biometric characteristics like face and fingerprint is proposed by N. Fathima et.al. [3]. in this paper Linear discriminant analysis (LDA) and principal component analysis (PCA) are used to recognize the face. The LDA output is provided to the input of PCA. Crossing number algorithm is used for fingerprint authentication. As the number of samples for authentication of a person increases the time consumption for authentication also increases.

"A Combined Face, Fingerprint Authentication System" is proposed by A.S.O.Ali et.al [4]. In this paper face image features are extracted using canny edge method and Gabor wavelet, and the fingerprint is processed by using minutia matching algorithm. Here, the time consumption for authentication of an individual with combination of face and finger is less than that of Fathima et.al.[3].

Recognition of face and fingerprint with fuzzy logic is suggested by P. Sharma et.al. [5]**.** Face recognition is implemented by using PCA and for fingerprint recognition minutia matching algorithm is used**.** The decisions made by the two biometric traits are getting fused at the decision level and the final decision is fed to the fuzzy logic. By using fuzzy logic the accuracy of the system is enhanced compared to the system without fuzzy logic.

A multimodal biometric system with match scores level fusion is

Revised Manuscript Received October 05, 2019

* Correspondence Author

Mr. P. Sivananthamaitrey*, Associate Professor, Electronics and Communication Engineering, Vishnu Institute of Technology, Bhimavaram,

V. Venkata Krishna, Electronics and Communication Engineering, Vishnu Institute of Technology, Bhimavaram, India.

Dr. Addanki Purna Ramesh, Professor, Department of ECE, Vishnu Institute of Technology, Bhimavaram, India.

Dr. P. S. N. Murthy, Professor, Electronics and Communication Engineering, Vignan's Institute of Information Technology, Visakhapatnam, India.

implemented by Grace Wangari Mwaura et.al. [6]. Scale Invariant Feature Transform (SIFT) algorithm is used for extracting the features of face and fingerprint images. The distance between the key points is measured with the hamming distance method. The feature extraction with SIFT algorithm is very complicated and gives less accuracy.

L.Nisha Evangelin et.al. [7] proposed a "Feature Level Fusion Approach For Personal Authentication In Multimodal Biometrics". In this paper Modalities such as Finger print, Palm print and Finger Knuckle prints are used for authentication. Grey Level Co Occurrence Matrix (GLCM) feature extraction Technique is used to extract the unique characteristics of these Modalities. The accuracy of the system is found to be 85% through this technique.

The different techniques used to fuse biometric systems are introduced by Puja S Prasad et.al. [8]. This paper describes, how two single biometric systems are get fused at the various levels and discussed about the complications involved in the integration of biometric traits. It also concludes that decision level fusion technique is better than the other fusion techniques.

Adrian Rhesa et.al. [9] Executed a face recognition application "Implementation of Face Recognition Algorithm for Biometrics Based Time Attendance System". This paper compares the Receiver operating characteristics (ROC) curves of face recognition using the Eigen face approach and Fisher face algorithm. It shows that the Eigenface algorithm gives the best accuracy than the Fisher face algorithm.

Authentication of an individual with fingerprint based on Minutia matching algorithm is implemented in [10],[11]. This technique is used very often in multiple algorithms and methods for fingerprint recognition.

False rejection rate, accuracy and time consumption for authentication of a person are the major problems in biometric systems. The proposed technique addresses the problems of false rejection rate and accuracy.

III. PROPOSED METHOD

A dual security system has been developed to improve the accuracy and FRR. Eigenface approach is used for detection. A two level DWT based algorithm is used to extract the features from the images. The two biometric systems are combined with the decision level fusion technique. In the first step, it is gone through the face recognition, if in case face recognition fails it uses fingerprint as an authentication system. Fig. 1 shows the block diagram of the proposed method. The face and fingerprint images of different persons are used as a database. Specifically, two different views of face and a latent fingerprint image of different persons are stored as a database. Face biometric data is captured as an input test image for detection. In the feature extraction module the features of input image and the database image's features are extracted and these features are compared in the matching module. The decision module is used to make a decision about the authenticity of the user. If the user is genuine then it displays the portrait of that person which is stored in the database, otherwise the person authentication is performed with the fingerprint recognition. The same procedure is repeated for the fingerprint recognition.

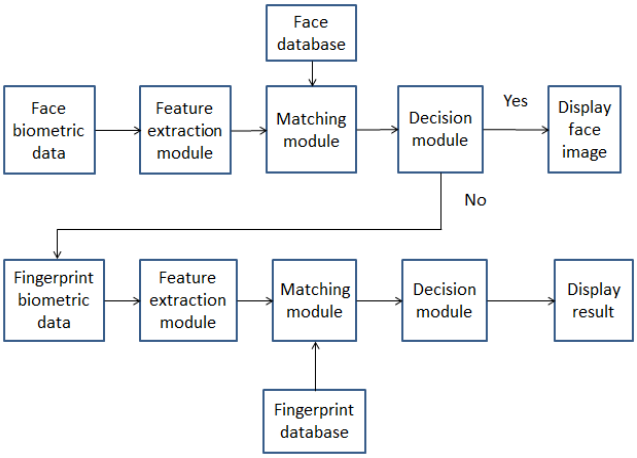

Fig. 1. Block diagram of the proposed system

The algorithm for the proposed system is described below

Step1: A face image from the database is converted to a gray image of dimensions PXP and the dimensions of the gray image are reduced to MXM by applying 2 level DWT, it is vectorized to M^2X1 matrix subsequently.

Step2: A dataset of (Γ_i) of M^2XN dimensions is created from N number of images.

Step3: The average of the total image set is calculated as follows.

$$\psi = \frac{1}{N}\sum_{i=1}^{N}\Gamma_i \quad (1)$$

Where ψ= Average image of M^2X1.

N= number of images;

Γ_i = image vector.

Step4: The difference between the image vector and average image is computed as given below

$$\phi_i = \Gamma_i - \psi \quad (2)$$

Where i=1, 2, 3,….., N.

Step5: An augmented matrix A of size M^2XN is formed as

$$A = [\phi_1, \phi_2, \phi_3, \ldots\ldots, \phi_N]$$

Step6: Then covariance matrix of A of size NXN is found as

$$C1 = A^T A \quad (3)$$

Step7: The eigenvalues and eigenvectors of the covariance matrix are calculated and the set of eigenvectors are multiplied by the matrix A to create the corresponding eigenfaces of the dataset. Once the eigenvectors of each face image are computed, the eigenvector of the input face image is matched with each computed eigenvectors. The Euclidean distance between the test image and the dataset images is calculated. The face image with the minimum Euclidean distance is detected as authentic image if their Euclidean distance is less than a threshold value of 20. If the distance is larger than the threshold value then it turns on the fingerprint recognition system which works exactly similar to face recognition system but only accepts fingerprint images as input.

IV. RESULTS

In the face detection, the face images of 40 people with two different views are collected from Yale face database.

Fig. 2. Face database samples

Fig. 2 shows the 10 different persons face dataset image samples; these are used in the proposed system to authenticate face. Similarly for detection of fingerprint 40 persons fingerprint images are collected from the FVC 2004 finger database.

Fig. 3. Fingerprint dataset samples

Fig. 3 denotes the 10 different persons fingerprint samples, and these images are used to authenticate a person with fingerprint . To authenticate a person using face recognition, a face image is picked from the test database as input and the output is the corresponding front view of the test image

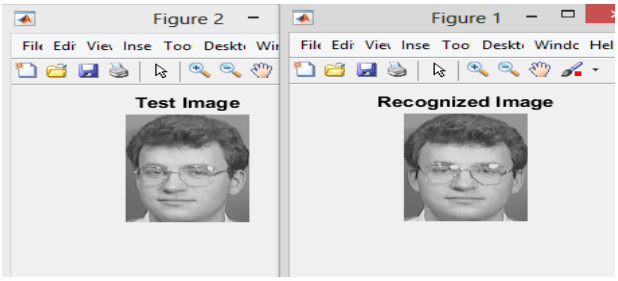

Fig. 4. Face recognition

which is retrieved from the database. Fig. 4 shows the results of face recognition. The input image is right side view of the person and the recognized image is front view of the image of the same person.

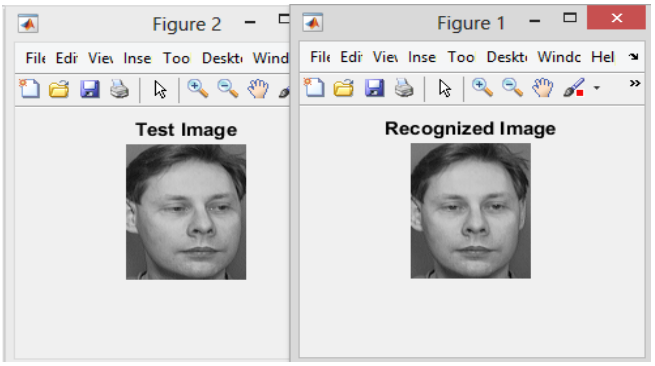

Fig. 5. Face recognition for data.

Another example of face recognition result is presented in Fig 5. Here the test image is left side view of the person and the recognized image is front view of the same person shown in Fig. 5.

If the face authentication works well it displays the person face image, sometimes the system may fail to authenticate the person with the face recognition due to low light conditions and improper threshold selection. Then, the person authentication can be done with fingerprint recognition.

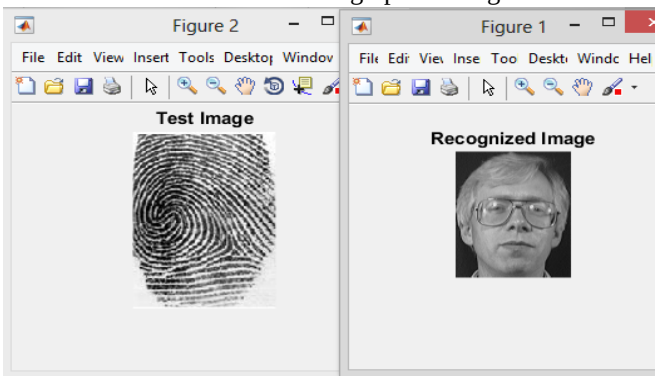

Fig. 6. fingerprint recognition

The fingerprint recognition results are shown in Fig. 6. The test image is the dark fingerprint image of a person is shown in left and the recognized front view of the face image of the person is shown in right.

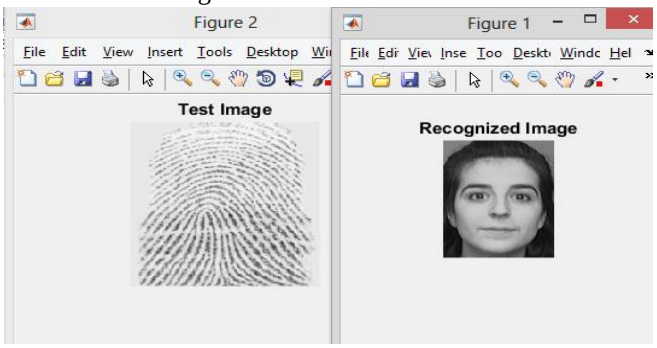

Fig. 7. Fingerprint recognition

Fig. 7 represents person's recognition with fingerprint. Here the test image is fingerprint image of a person is shown in left and the recognized face image of the person shown in right.

Usually the performance of a biometric system is measured with the following parameters,

False acceptance rate (FAR): It is the measure of the likelihood that an unauthorized user will incorrectly accept by the biometric security system. Typically, the FAR of a system is defined as the ratio of the number of false acceptations

to the number of identification attempts.

False Rejection Rate (FRR): It is the performance measure of the security system that indicates incorrect rejection of an access attempt by an authorized user. A system's FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.

Accuracy: The rate at which the number of registered persons accepted by the system to the total amount of attempts.

Table -I Comparison of FRR and accuracy

Number of users	Face		Fingerprint		Face and fingerprint	
	FRR	Accuracy	FRR	Accuracy	FRR	Accuracy
10	30%	70%	10%	90%	0.5%	99.5%
20	30%	70%	15%	85%	0.7%	99.3%
30	33%	67%	16%	84%	0.9%	99.1%
40	35%	65%	20%	80%	2%	98%

The above table-I shows the FRR and accuracy comparison of the face recognition, fingerprint recognition and the proposed system. The FRR and accuracy of the face and fingerprint unimodal biometric systems are calculated with different number of users, and these results of the proposed system are presented. As the number of users increases the FRR is marginally increased and the accuracy of the system is slightly reduced, but proposed system improves the FRR and accuracy.

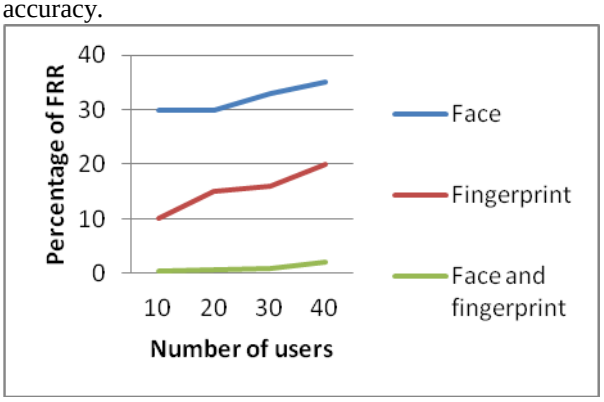

Fig. 8. FRR Vs Number of users

The graphical analysis of the proposed system FRR with the face and fingerprint unimodal biometric systems is shown in Fig. 8. The FRR of face unimodal biometric system and fingerprint biometric system are high when compared with the proposed system. The FRR of face and fingerprint biometric systems are 35% and 20% respectively for 40 users. The proposed security system reduced the FRR to 2% for same number of users.

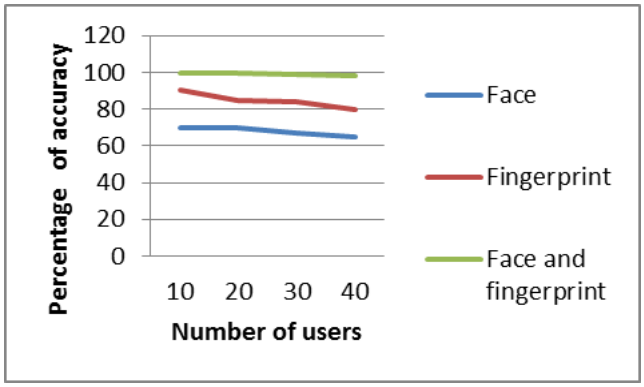

Fig. 9. Accuracy vs number of users

Fig. 9 shows the graphical analysis of the accuracy of the proposed system with the face and fingerprint unimodal systems. For 40 users the accuracy of face unimodal biometric system is 65% and the fingerprint biometric is 80%. Combining the face and fingerprint the accuracy of the system improved to 98%.

Table -II comparison with the existing methods

Related works	FRR	Accuracy
G. W. Mwaura et.al. [6]	7.5%	92.5%
X. Wang et.al. [11]	2.98%	97%
P. Mote et.al. [12]	3.25%	96%
A.S.O. Ali et.al. [4]	3.14%	96.4%
Proposed Method	2%	98%

The table-II shows the comparison of the proposed system performance parameters with the several existing systems. The proposed system produces more accuracy when compared with the existing methods.

V. CONCLUSION

An authentication system based on face and fingerprint recognition is implemented using 2 level Discrete Wavelet Transform and decision level fusion. The fingerprint authentication comes into play when face recognition fails to authenticate a person. The proposed system enhances the security and the accuracy of recognition is found to be 98% for a dataset of 40 samples which is significantly better when compared with unimodal biometric authentication systems. The false rejection rate (FRR) is considerably reduced. The proposed system achieves the FRR of 2% and is comparably better than some of the state of the art techniques of similar kind.

REFERENCES

1. Sona Agarwal and Yogita Gulati "A Multimodal Biometric System Using Fingerprint and Face" international Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012
2. Puja S Prasad, Prof G N Purohit, Dr.Sourabh Mukherjee proposed "Fusion Techniques in Multi Biometric Systems" International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 3, May – Jun 2017.
3. Fathima N and Smitha Satheesh proposed "Multi-Modal Biometric Security with Multi- Algorithm"

International Conference on Trends in Electronics and Informatics ICEI 2017 978-1-5090-4257-9/17/©2017 IEEE.

4. Amal Seralkhatem Osman Ali, Vijanth Sagayan, Aamir Saeed Malik, Waqas Rasheed proposed "A Combined Face, Fingerprint Authentication System" IEEE ISCE 2014 1569926437.
5. Poonam sharma and Kulvinder singh proposed a "multimodal biometric system fusion using fingerprint and face with fuzzy logic" ijarcsse Volume 7, Issue 5, May 2017.
6. Grace Wangari Mwaura, Prof. Waweru Mwangi, Dr. Calvins Otieno proposed "Multimodal biometric system fusion of face and finger print biometrics at match score fusion level" international journal of scientific & technology research volume 6, issue 4, APRIL 2017, ISSN 2277-8616..
7. Randeep kaur and Rishmjot kaur introduces a "multimodal biometric authentication system using face and fingerprint features with feature level fusion" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Volume 5 Issue 10, October 2016.
8. Puja S Prasad, Prof G N Purohit, Dr.Sourabh Mukherjee proposed "Fusion Techniques in Multi Biometric Systems" International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 3, May – Jun 2017, ISSN: 2347-8578
9. Adrian Rhesa Septian Siswanto, Anto Satriyo Nugroho and Maulahikmah Galinium proposed "Implementation of Face Recognition Algorithm for Biometrics Based Time Attendance System". 2014 International Conference on ICT For Smart Society (ICISS).
10. Deepika Sahu and Rashmi Shrivas introduced "Fingerprint Reorganization Using Minutiae Based Matching for Identification and Verification" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 , Volume 5 Issue 5, May 2016
11. Yin Li-qiang and Gao Ling proposed "Feature Extraction of Fingerprint Image Based on Minutiae Feature Points" 2012 International Conference on Computer Science and Service System. 978-0-7695-4719-0/12 © 2012 IEEE

AUTHORS PROFILE

P. Sivananthamaitrey, Research Scholar, Andhra University College of Engineering (A). He received his M. Tech in 2006 from Jawaharlal Nehru Technological University, Ananthapur. He has 13 years of teaching experience. He has been working as Associate Professor at Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India. He has guided various projects at UG, PG level. He is also a member of IETE and ISTE. His research Area is Digital Image Processing.

V. Venkata Krishna, pursuing M.Tech, Department of Electronics and Communication Engineering, Vishnu Institute of Technology, Bhimavaram, Andhra Pradesh, India.

Addanki Purna Ramesh has more than 21 years of teaching and research experience. He obtained his Master's degree from JNTU, Hyderabad and Ph.D. from JNTUK, Kakinada. He is Member of IETE, ACEEE, Fellow of Institute of Engineers (India). His areas of interest are VLSI, DIP, and Embedded Systems. He has 30 publications in various International and National Journals and conferences.

Dr. P. Satyanarayana Murty is currently working as Professor in ECE Department, Vignan's Institute of Information Technology, Visakhapatnam, India. He received his M.Tech from Jawaharlal Nehru Technological University, Hyderabad, India. He received his Ph.D from Andhra University, Visakhapatnam, India. He has 20 years of teaching experience and guided many projects for undergraduate and post graduate students. Presently he is guiding two Ph.D scholars. His research interests are in the areas of Digital Image Watermarking, Image Compression and Multimedia Security.