International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-3 Issue-12 September-2013

Hybrid Level Integration of Biometric Traits for Security Applications

Manjunath S Gabasavalagi[1], Sanjeevakumar M. Hatture[2], Nalinakshi B. G[3], Rashmi P. Karchi[4]

Abstract

In reality the security is to be provided in different levels based on the application and requirement. In attendance related applications require low level security, banking applications may need medium level security and defence applications require high level security. This paper presents a hybrid-modal (Unimodal or Multimodal) biometric system which is used to provide better security to applications based on their requirement. Based on the security level, the system uses both single evidence (unimodal) for lower level and multiple evidences (multimodal) for higher level security. The developed hybrid-modal system employs one or more biometric modalities such as face, voice and fingerprint by alleviating some of the challenges identified in fingerprint, face and voice biometrics modalities. These biometric modalities are selected as they are independent, non-intrusive and robust. Depends on the applications security level requirements like low, medium and high, the number of biometric modalities are provided as evidence to the system. The developed system is tested for 60 users. The accuracy for low level security applications using either fingerprint or face or voice the accuracy of around 94%, 93% and 82% respectively have achieved. The accuracy for medium level security applications using face & fingerprint, face & voice and voice & fingerprint are 91%, 81% and 88% respectively. Further, for high level security using all the three biometric traits the accuracy of 80% is achieved. The developed system provides promising results for all level of security applications.

Keywords

Biometrics, Multimodal, Unimodal, Hybrid Modal, Fingerprint, Face, Voice.

Manjunath S Gabasavalagi, Computer Science and Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka State, India.
Sanjeevakumar M. Hatture, Computer Science and Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka State, India.
Nalinakshi B. G, Computer Science and Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka State, India.
Rashmi P. Karchi, Research Scholar, Bharathiar University, Coimbatore, Tamilnadu, India.

1. Introduction

In day-today life in networking society the people perform many kinds of business and banking transactions. They use either token based or knowledge based approaches to secure their transactions from fraudulent. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies are becoming apparent. Biometric-based solutions are able to provide confidential transactions and personal data privacy. Biometrics is the automatic identification or verification of a person based on user physiological or behavioural characteristics. It is inherently more reliable and has a higher discrimination capability than the token-based and/or knowledge based approaches, because the physiological or behavioural characteristics are unique to every user. In the existing unimodal biometric system the user will provide single evidence/trait i.e. face or fingerprint or voice etc while registration to the system. The biometric system fails if the registered user is unable to provide his/her information due to some of the issues like in face biometrics, illumination variations, aging variations, pose, surgery, low resolution face images from video surveillance and forensic faces and so on. In fingerprint biometrics, dryness or dirty of the finger’s skin, with the age fingerprint will vary, displacement or rotation between different acquisitions, partial overlap, especially in sensors of small area, skin conditions and people who works in chemical industries are often affect. In voice biometrics, accuracy, user responsiveness, frequency, vocal track, fault tolerance etc. It is not possible to provide alternative biometric modality for authentication. In order to alleviate the limitations imposed by unimodal biometric system, the multimodal biometric systems are emerged. The multimodal biometric system, multiple evidence are to be provided by the user, hence is costlier in terms of processing time and performance of the system. For low level security applications the multimodal biometric system is not well suited due its cost. In order to enable a biometric system to operate effectively in different applications and environments, a hybrid modal (i.e. Unimodal and/or multimodal) biometric system which makes a personal identification based on single and / or multiple physiological or behavioural characteristics is preferred. The developed biometric system will work accordingly to the application and requirement of the level of security. Three biometric modalities are used namely fingerprint, face and voice. Three biometric modalities are selected as they are independent, non-intrusive and robust. In developed system user need to provide three biometric traits namely fingerprint, voice and face during registration. At the time of authentication, choice is given to users to select either single i.e. Face or voice or fingerprint or multiple i.e. combination of any two traits i.e. face + voice or face + fingerprint or voice + fingerprint for the low and medium level applications respectively. In case of high level security applications the user need to provide all the three biometric traits for authentication. Hybrid modal biometric systems capture one or more biometric traits and produce a better match decision by simultaneously decreasing the False Acceptance Rate (FAR) and False Rejection Rate (FRR).

This work was supported in part by the Department of Computer Science and Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka State India.

2. Literature Review

Most of the researchers addressed the issues in all biometric systems as a security measure by considering many scenarios where the user‘s physical or behavioral biometric characteristics are provided for security applications. Three biometric modalities used in this work are fingerprint, face and voice. The literature available for these modalities is summarized below;

The speech recognition, multilingual speaker identification and online examination for physically challenged people can be achieved by extracting Mel Frequency Central Coefficients (MFCC) [1, 2]. Along with MFCC features, vector quantization technique can be used to minimize the amount of data to be handled [3]. The Back propagation Artificial Neural Network is used for speaker identification in [4]. Speech recognition and Speaker verification can be achieved with the help of MFCC features and Gaussian Mixture Model (GMM). An online signature verification and speaker verification are combined to authenticate the user in [5]. The signature features such as x, y coordinates, pressure applied from the pen to the writing tablet, velocity and tangent angle and MFCC features of the voice are used [6].

Further, the major challenge in face recognition system is lighting variations. In pre-processing stage use Gamma Correction, Difference of Gaussian (DOG) filtering and contrast equalization methods to solve the lighting variations problem [7]. Face recognition is achieved using adaptive binning and adaboost technique. The framework is experimentally verified by the authors with FERET database and achieved higher recognition rate [8]. A methodology for face recognition based on information theory approach of coding and decoding the face image. The feature extraction using principle component analysis and recognition using the feed forward back propagation Neural Network are performed in [9]. Principal Component Analysis method is used to extract the features from face and palm prints separately. The normalized match (distance) scores generated by respective palm and face features before fusion are used to form fused match score. The Euclidean distance and the feature distance are calculated after fusion. These distances are used to arrive at final decision. Feedback routine implemented between the feature extraction and the matching modules of the biometric system can lead to substantial improvement in multimodal matching performance [10]. In multimodal i.e. face and voice, new fusion technique based on simple sum rule and product rule achieves higher performance as compared with existing fusion schemes such as sum rule, product rule, maximum rule and minimum rule [11]. A new multimodal biometric approach use face and periocular biometrics. By combining face and periocular data obtained from the same image may increase the performance of the recognition system. The featured extracted from these modalities are LBP-PCA and Gabor-PCA [12]. For fingerprint biometric, the minutiae are extracted from low quality image using new thinning algorithm [13]. A Euclidean distance based minutia matching algorithm is used to improve the matching accuracy in fingerprint verification system. The algorithm uses only the minutia location, to reduce the effect of non-linear distortion [14]. A novel fingerprint matching algorithm i.e. M3gl contains three components: a feature representation containing clockwise-arranged minutiae without a central minutia, a similarity measure that shifts the triplets to find the best minutiae correspondence, and a global matching procedure that selects the alignment by maximizing the amount of global matching minutiae [15].

Several issues and challenges related to face, fingerprint and voice are identified. In face biometrics, illumination variations, aging variations, pose, surgery, low resolution face images from video surveillance and forensic faces and so on. In fingerprint biometrics, dryness or dirty of the finger's skin, with the age fingerprint will vary, displacement or rotation between different acquisitions, partial overlap, especially in sensors of small area, skin conditions and people who works in chemical industries are often affect. In voice biometrics, accuracy, user responsiveness, frequency, vocal track, fault tolerance etc. The objective of the proposed work is to develop an affective biometric system, which will work accordingly to the requirement of the level of security by considering some of these challenges. Depends on the security level like low, medium and high, the number of biometric modalities (i.e. fingerprint, face and voice) are provided as evidence to the system.

3. Proposed Model

The proposed model gives the betterment of the existing biometric system in advancement of providing security by identifying the user being genuine or not. Depends on the security level like low, medium and high, the number of biometric modalities are selected to authenticate the user of the system. Fingerprint, face and voice biometric modalities are selected in this work due to their non-intrusiveness and robustness. The selected biometric modalities are better compare to other existing biometric modalities in terms of providing accuracy, user friendliness, security, cheapness, storage space and process time. The proposed model consists of six stages namely image acquisition, pre-processing, feature extraction, template generation, template matching and decision as shown in figure 1.

First step in the proposed model is acquiring the images of fingerprint, face and voice samples of a user. In order to remove the noise, unwanted portion and to enhance the biometric samples the pre-processing steps are to be carried out. The eigenface feature from face, the minutiae feature from fingerprint, and the MFCC feature from voice samples are extracted and stored in the database separately and securely. During user authentication compare the stored template from the database with the generated feature vector of the user using template matching i.e. with Euclidean Distance Classifier. At the time of authentication the user is given freedom to select the biometric trait as per his/her interest based on the degree of security.

a. Image Acquisition: The basic requirement of any biometric system is providing the input information through either scanner or camera or speaker etc. The proposed model employs the three biometric modalities namely fingerprint, face and voice. The fingerprint images from "IIIT-D Simultaneous Latent Fingerprint Database", the face images from "Face-96" database and the voice sample database is constructed for the experimentation.

Fingerprint: The fingerprint image from "IIIT-D Simultaneous Latent Fingerprint Database" consists of simultaneous latent fingerprint of 15 subjects along with their mated 500ppi optical slap fingerprints. Simultaneous latent fingerprint are obtained using black powder dusting technique with a plain tile as background. Optical fingerprints are captured using Cross match LScan Patrol. The dimension of each image is 300*300 pixel resolution. Horizontal and vertical resolutions of the images are 96dpi. The sample fingerprint images of the database are shown in figure 2.

Face: The Face96 database is constructed using a fixed camera; a sequence of 20 images per individual was taken. During the sequence the user takes one or several steps forward towards the camera. This movement is used to introduce significant head variations between images of same individual. There is about 0.5 seconds between successive frames in the sequence. The database contains 152 people images with 196x196 pixels resolution. The database contains images of male and female users. The images contain minor variation in these attributes. There is no hairstyle variation as the images were taken in a single session. As users moves forward, significant lighting changes occur due to the artificial lighting arrangement. The sample face images from Face96 database are as shown in figure 3.

Voice: The voice database is constructed using two channels, 16 bit, and 44100 Hz microphone. The voice samples are recorded from 60 users. User can register voice password in any of the language. The user/speaker need to provide his/her voice sample in a consistent manner while registration and during authentication. The developed system will accept text-independent voice passwords. It is required to give the input for at least 3seconds by the user. The reordered voice samples are plotted as shown in figure 4.

b. Pre-processing: The fingerprint, face images and the voice samples are to be enhanced with the help of pre-processing. Removing the noise, unwanted background, thinning steps are carried out in the pre-processing step. The separate pre-processing steps are required for every biometric trait. They are explained in the following;

Fingerprint: The histogram equalization process is carried out in order to perform the contrast enhancement. The FFT operation is used to connect broken ridges, removes the noise between the ridges and improve the ridge contrast in frequency domain. Convert the enhanced fingerprint image in to binary. Typically the two colours used for a binary image are black and white. The advantages of performing Binarization are small memory requirements, faster execution time and less expensive. Perform the **Region of interest** operation to find out actual size of the fingerprint frame. Employ the **thinning** operation to find the ridges of one pixel width. The process consists in performing successive erosions until a set of connected lines of unit-width is reached. Remove all horizontal breaks and spikes from the fingerprint. The pre-processed fingerprint images are shown in figure 5.

Face: Gray conversation is used to convert RGB colour image in to greyscale image in order to reduce the amount of memory required to store the image and also improve the performance. Gamma Intensity Correction enhances the local dynamic range of the image in dark or shadowed regions while compressing it in bright regions and is determined by the value of γ. The gamma values of less than 1.0 darken an image. Gamma values greater than 1.0 lighten an image and a gamma value equal to 1.0 produces no effect on an image. The pre-processed face images are shown in figure 6.

Voice: In order to enhance the voice samples performed the silence detection, windowing i.e. Hamming, FFT, and Mel-frequency Warping operations in pre-processing. The pre-processed voice samples are shown in figure 7.

Silence detection: This step is important in any frontend speaker recognition system. When the user provides any kind of voice sample i.e. word the system will never have control over the instant the word is uttered. Silence detection basically determines when the user has actually started uttering the word if any, thereby translates the frame (Chunk of the unique consecutive images) of reference to that instant. In developed system the frame size used is 240.

Windowing: Windowing each individual frame to minimize the signal discontinuities at the beginning and end of the frame. Minimize the spectral distortion by using the window to taper the signal to zero at the beginning and end of the frame. The window can be defined as,

$$w(n),\ 0 \le n \le N-1 \qquad (1)$$

Where N is the number of samples in each frame, then the result of windowing is the Signal.

$$Y1(n) = x1(n)w(n),\ 0 \le n \le N-1 \qquad (2)$$

In most of the speaker recognition system the Hamming window is used, which has the form:

$$w(n) = 0.54\text{-}0.46\cos\left(\frac{2\prod n}{N-1}\right),\quad 0 \le n \le N-1 \qquad (3)$$

Fast Fourier Transform (FFT): Fast Fourier Transform, which converts each frame of N samples from the time domain into the frequency domain. The FFT is a fast algorithm to implement the Discrete Fourier Transform (DFT) which is defined on the set of N samples { Xn }, as follows:

$$Xn = \sum_{k=0}^{N-1} Xk \exp(-2\prod / kn/N),$$

$$n = 0, 1, 2, \ldots, N-1 \qquad (4)$$

In general Xn's are complex numbers. The resulting sequence {Xn} is interpreted as follows: the zero frequency corresponds to n = 0, positive frequencies: 0 < f < Fs/2 correspond to values $1 \le n \le N/2-1$ while negative frequencies –Fs/2 < f < 0 correspond to $N/2+1 \le n \le N-1$.

Here, Fs denote the sampling frequency. The voice sample/signal obtained after this step is often referred to as signal's spectrum or periodogram.

Mel-frequency Warping: For each tone with an actual frequency, f, measured in Hz, a subjective pitch is measured on a scale called the 'Mel' scale. The Mel-frequency scale is linear frequency spacing below 1000 Hz and a logarithmic spacing above 1000 Hz. As a reference point, the pitch of a 1 kHz tone, 40 dB above the perceptual hearing threshold, is defined as 1000 mels. To compute the mels for a given frequency f in Hz the following expression is used:

mel=10log10(Window(FFT(signal)^2)) (5)

c. Feature Extraction: In image processing, feature extraction is a special form of dimensionality reduction. The input data will be transformed into a reduced representation set of features (also named features vector). Transforming the input data into the set of features is called **feature extraction**. In this step, extraction of the features for fingerprint, face and voice biometric modalities are explained.

Fingerprint: From fingerprint image extract the feature like Minutiae, direction and frequency of the ridge regions. In a fingerprint, minutiae points are correspond to either a ridge ending or a bifurcation. The position of the minutia point is at the tip of the ridge or the valley. The orientation is given by the orientation of the arrow formed by the ridge or the valley. The extracted minutiae from fingerprints are shown in the figure 8.

Algorithm to Extract Minutiae Feature: Step1: Crop the inner 128*128 pixel resolution sub image from the main fingerprint image.

Step 2: Scan the binary image from top to bottom, left to right order by following only ridges.

Step 3: Find the 0-1 transition, calculate the width of the ridge by noting the 1-0 transition.

Step 4: Repeat step 3 for all the ridges and compute the width.

Step 5: If the current_width >= previous_width, there exist top to bottom bifurcation. Locate the minutiae point. Else If the current_width =< previous_width, there exist bottom to top ridge bifurcation. Locate the minutiae point.

Step 6: Repeat step 5 for all the ridges and locate the minutiae points.

Step 7: Determine the Euclidean distances between all the Minutiae points.

Step 8: Construct the template of all distances of the minutiae points.

Face: From face image, extract the eigenvalues and eigenvectors. Eigenvector based features are extracted from the images. An eigenvector of a square matrix A is a non-zero vector V that, when the matrix is multiplied by v, yields a constant multiple of v, the multiplier being commonly denoted by λ.

That is: Av = λ v

The number of λ is called the eigenvalues of A corresponding to v. The face image constructed in Eigen space i.e. eigenface is shown in figure 9.

Algorithm to Extract Eigenface Feature:

Step 1: Detect the face and localize. The faces constituting the training set (τ) and compute the average value of each image and store in the variable ϕ.

Step 2: Subtract the mean. The average matrix Ψ has to be calculated, then subtracted from original faces (τ) and the result stored in the variable ϕ.

$$\Psi = \frac{1}{M} \sum \ ((\text{n-1}) \exp \text{M}) \ \tau \qquad (6)$$

$$\phi = \tau - \Psi \qquad (7)$$

Step 3: Calculate the covariance matrix.

$$\text{C} = \frac{1}{M} \sum_{n-1}^{M} \phi n \,.\, \Phi_n^T \qquad (8)$$

Step4: Calculate the eigenvectors and eigenvalues of the covariance matrix. The eigenvectors (eigenfaces) u_i and the corresponding eigenvalues λ_i should be calculated. The eigenvectors (eigenfaces) must be normalized so that they are unit vectors, i.e. of length 1.

Step5: Select the principle components. From M eigenvectors (eigenfaces) u_i, only *M*' should be chosen, which have the highest eigenvalues. The higher the eigenvalue, the more characteristic features of a face does the particular eigenvector describe. Eigenfaces with low eigenvalues can be omitted, as they explain only a small part of characteristic features of the faces. After *M*' eigenfaces u_i are determined, the "training" phase of the algorithm is finished.

Step6: Apply Euclidian distance algorithm for matching. Let an arbitrary instance x be described by the feature vector,

$$\text{x} = \left[\text{a1(x), a2(x), …. , an(x)} \right]. \qquad (9)$$

Where a(x), denotes the value of the rth attribute of the instance x. The distance between two instances xi and xj is defined to be d (xi, xj):

$$\text{d(xi, xj)} = \sqrt{\sum_{r=1}^{n} ((ar(xi) - ar(xj))2} \qquad (10)$$

Voice: From voice sample, extract the Mel Frequency Cepstrum also known as codebook. By computing the expression 10log10 (Window (FFT (signal) ^2)) gives Mel Frequency Cepstrum Coefficients. The length of the sample depends upon the window length and Mel frequency or codebook features are extracted using MFCC algorithm. The codebook is shown in the figure 10.

Algorithm to Extract Mel-Frequency Feature:

Step 1: Compute the Fourier transform of a voice signal extracted from windowing operation.

Step 2: Map the powers of the spectrum obtained above onto the Mel scale, using triangular overlapping windows.

Step 3: Compute the logs of the powers at each of the Mel frequencies.
Step 4: Evaluate the discrete cosine transform of the list of Mel log powers.
Step 5: The MFCCs are the amplitudes of the resulting spectrum.
Step 6: Construct the template of MFCCs coefficients.

d.Template Generation: Construct separate templates for each of the three traits from the extracted features from fingerprint, face and voice modalities.

e. Template Matching: Euclidian distance algorithm is used for template matching. In this algorithm compare the testing image feature vector with the stored template present in the database. The lowest distance below the threshold is classified / categorized. The Euclidian distance between two feature vectors p and q is the length of the line segment connecting them (pq). If p = (p1, p2, …. Pn) and q = (q1, q2, …, qn) are two feature vectors in Euclidian space, then the distance from p to q or from q to p is given by:

d(p,q) = d(q,p) =

$$\sqrt{(q1-p1)2+(q2-p2)2+.....+(qn-pn)2}$$

$$= \sqrt{\sum_{i=1}^{n}(qi-pi)2} \qquad (11)$$

f. Decision: Based on the result produced by the template matching phase, the lowest value of the Euclidean distance i.e. the nearest match will be decided. The user is authorized or unauthorized based on the threshold value set for the distance.

4. Experimentation

The experiments are carried out for all the three levels of security measures. The developed system is tested for 60 users. From every user three biometric modalities are selected. In order to evaluate the efficiency of the developed system, the standard databases for fingerprint (i.e. IIITD_SLF_Database) and face (IITK and face-96 databases) are selected. The voice samples are collected for the phrase "World is beautiful and we all live in it" from 60 users. But it is not compulsory to pronounce the same phrase in the English language. The user may provide the voice samples in any language. The template is designed separately for every biometric modality. From every user, five samples are used for training and 5 samples for testing purpose. The performance of the system is shown in table 1.

The performance of the design biometric system is evaluated with the parameters False Acceptance Rate (FAR), False Rejection Rate (FRR) and Genuine Acceptance Rate (GAR). The expressions to evaluate these parameters are given below;

False Acceptance Rate: The FAR is the ratio of the number of unauthorized users accepted by the biometric system to the total number of identification attempts made. It is stated as follows:

$$\text{FAR} = \frac{\text{Number of wrongly identified claims}}{\text{Total number of claims}} \times 100\% \quad (12)$$

False Rejection Rate: The FRR is the ratio of the number of authorized users rejected by the biometric system to the total number of attempts made. It is stated as follows:

$$\text{FRR} = \frac{\text{Number of wrongly rejected claims}}{\text{Total number of claims}} \times 100\% \quad (13)$$

and GAR = (1- FAR) * 100 % (14)

The results indicate the performance of all the three levels of authentication using three biometric traits namely fingerprint, face and voice. The developed system is tested for 60 persons and performed 300 test cases on each biometric modality i.e. fingerprint, face and voice. Developed system is also tested on combination of the three biometric modalities i.e. Face & Voice, Face & Fingerprint, Voice & fingerprint, and Face, Voice & Fingerprint. The accuracy for low level security applications using fingerprint, face and voice are 94%, 93% and 82% respectively. The accuracy for medium level security applications using face & fingerprint, face & voice and voice & fingerprint are 91%, 81% and 88% respectively. The accuracy for high level security using all three biometric traits is 80%. As the security level increases the accuracy of the system is reduced. The performance analysis chart is shown in figure 11.

5. Figures and Table

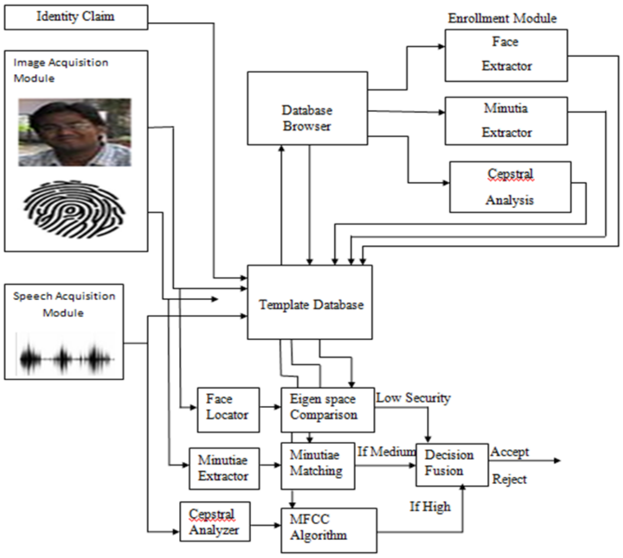

Figure 1: Proposed Model

Figure 2: Samples of Fingerprint Images

Figure 3: Sample Face Images

Figure 4: Voice Samples

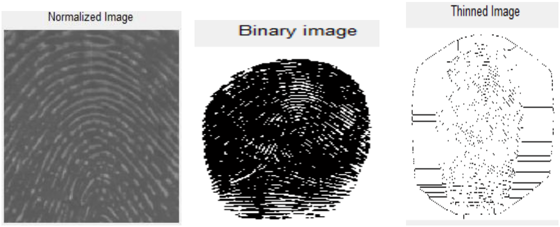

Figure 5: Preprocessed fingerprint images

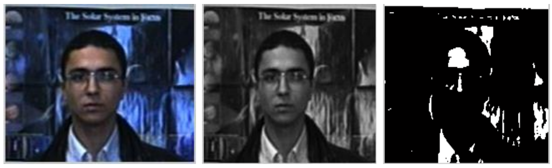

Figure 6: Pre-processed face images

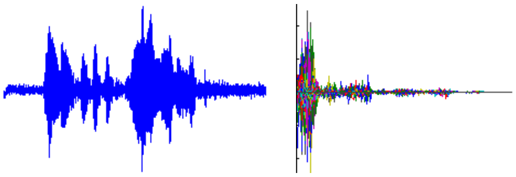

Figure 7: Pre-processed voice samples

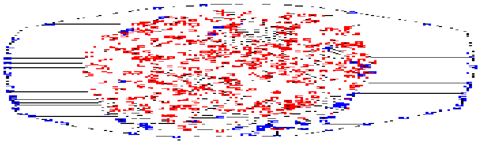

Figure 8: Minutiae

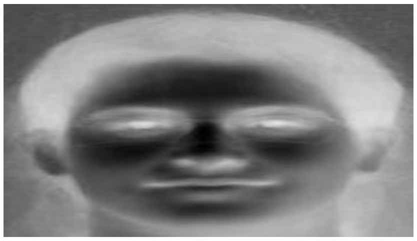

Figure 9: Eigen face

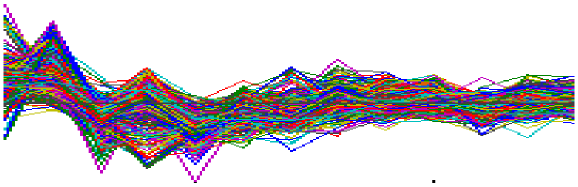

Figure 10: Mel Frequency/Codebook extraction

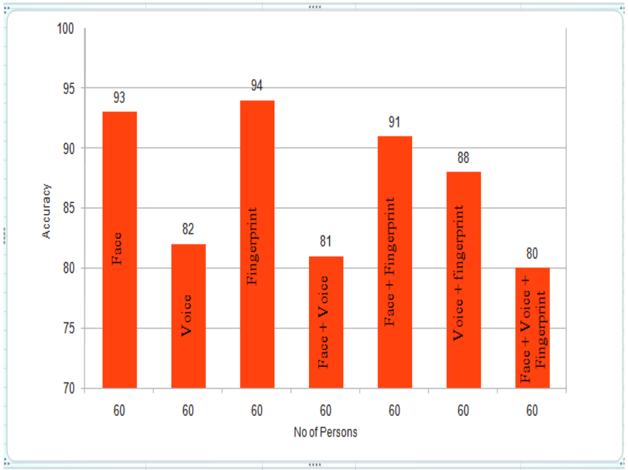

Figure 11: Performance Analysis Chart

Table 1: Performance Analysis Table

Biometric Traits	Number of test samples	Accuracy in % (GAR)	FAR in %	FRR in %
Face	300	93	1	6
Voice	300	82	6	12
Fingerprint	300	94	0.5	5.5
Face + Voice	300	81	7	12
Face + Fingerprint	300	91	2	7
Voice + Fingerprint	300	88	5	7
Face + Voice + Fingerprint	300	80	8	12

6. Conclusion and Future Work

The developed system utilizes the three modalities namely fingerprint, face and voice. In developed system Minutiae, Eigenvector and Mel Frequency Cepstrum Coefficients i.e. MFCC algorithms are used for fingerprint, face and voice biometric modalities respectively. Acquisition, Preprocessing, Feature Extraction, Template Generation, Matching and Decision steps are carried out for all the three modalities. The developed system is tested for 60 persons. The accuracy for low level security applications using fingerprint, face and voice are 94%, 93% and 82% respectively. The accuracy for medium level security applications using face & fingerprint, face & voice and voice & fingerprint are 91%, 81% and 88% respectively. The accuracy for high level security using all three biometric traits is 80%. In case of high level security need to compromise with accuracy but it will provide high level security. In future, different biometric modalities with multimodal biometric system, higher level of security may be provided. The issues and challenges of the modalities are to be addressed.

Acknowledgment

I would like to thank all the researchers for contributing valuable suggestions and motivating to carry out the work with face, fingerprint and voice recognition. I extend my gratitude to all the authors of reference papers, to my parents and beloved teachers.

References

[1] Akanksha Singh Thakur, Namrata Sahayam, "**Speech Recognition Using Euclidean Distance**", International Journal of Emerging Technology and Advanced Engineering, Vol.3, Issue 3, pp.587-590, March 2013.

[2] Dwijen Rudrapal, Smita Das, S. Debbarma, N. Kar, and N. Debbarma, "**Voice Recognition And Authentication As A Proficient Biometric Tool And Its Application In Online Exam For P.H People**", International Journal of Computer Applications (0975 – 8887) Vol 39– No.12, pp.6-12, February 2012.

[3] Helen Jenifer Archana, A. Kala and R. Surya, "**Preparation Multilingual Voice Biometrics Using Optimum Energy Frame In Noisy Environment**", International Conference on Computing and Control Engineering (ICCCE 2012), pp.1-3, April 2012.

[4] Kshamamayee Dash, Debananda Padhi, Bhoomika Panda and Sanghamitra Mohanty, "**Speaker Identification Using Mel Frequency Cepstral Coefficient And Bpnn**", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 4, pp.326-332, April 2012.

[5] Chenguang Yang, Ghaith Hammouri and Berk Sunar, "**Voice Passwords Revisited**", CRIS Lab, Worcester Polytechnic Institute, pp.1-9, 2012.

[6] Mandeep Kaur, Akshay Girdhar and Manvjeet Kaur, "**Multimodal Biometric System Using Speech and Signature Modalities**", International Journal of Computer Applications, Vol 5– No.12, pp.13-16, August 2010.

[7] S.Anila & Dr.N.Devarajan, "**Preprocessing Technique for Face Recognition Applications under Varying Illumination Conditions**", Global Journal of Computer Science and Technology Graphics & Vision, Vol.12 Issue 11, pp.1-7, February 2012.

[8] Srinivasan A, "**A Framework for Face Recognition Using Adaptive Binning and**

Adaboost Techniques", The International Journal of Multimedia & Its Applications, Vol.3, No.1, pp.76-88, February 2011.

[9] Mayank Agarwal, Nikunj Jain, Mr. Manish Kumar and Himanshu Agrawal, "**Face Recognition Using Eigen Faces And Artificial Neural Network**", International Journal of Computer Theory and Engineering, Vol. 2, No. 4, pp.624-629, August 2010.

[10] Gayatri Umakant Bokade and Ashok. M. Sapkal, "**Feature Level Fusion of Palm and Face for Secure Recognition**", International Journal of Computer and Electrical Engineering, Vol.4, No.2, pp.157-160, April 2012.

[11] Y. M. Fouda, "**Fusion of Face and Voice: an Improvement**", IJCSNS International Journal of Computer Science and Network Security, Vol.12 No.4, pp.37-43, April 2012.

[12] N. S. Lakshmiprabha, J. Bhattacharya and S. Majumder, "**Face Recognition Using Multimodal Biometric Features**", 2011 International Conference on Image Information Processing (ICIIP 2011), pp.1-6, June 2011.

[13] Sasan Golabi, Saiid Saadat, Mohammad Sadegh Helfroush, and Ashkan Tashk, "**A Novel Thinning Algorithm With Fingerprint Minutiae Extraction Capability**", International Journal of Computer Theory and Engineering, Vol. 4, No. 4, pp.514-517, August 2012.

[14] Ujjal Kumar Bhowmik, Ashkan Ashrafi, Reza R. Adhami, "**A Fingerprint Verification Algorithm Using The Smallest Minimum Sum Of Closest Euclidean Distance**", International Conference on Electrical, Communications, and Computers, pp.90-95, 2010.

[15] Miguel Angel Medina-P´erez, Milton Garc´ıa-Borroto, Andres Eduardo Gutierrez-Rodr´ıguez and Leopoldo Altamirano-Robles, "**Improving Fingerprint Verification Using Minutiae Triplets**", Sensors 2012, 12, 3418-3437; doi:10.3390/s120303418, pp.3419-3437, 2012.

[16] Shanumukhappa A Angadi, Sanjeevakumar M Hatture, "**A Novel Spectral Graph Theoretic Approach To User Identification Using Hand Geometry",** International Journal of Machine Intelligence ISSN: 0975–2927 & E-ISSN: 0975–9166, Volume 3, Issue 4, pp.282-288, December 2011.

[17] Facial Images "Faces96 images", online at http://cmp.felk.cvut.cz/~spacelib/faces/faces96.html.

[18] Fingerprint database "IIIT-D Simultaneous Latent Fingerprint Database", online at http://research.iiitd.edu.in/groups/iab/fpdatabases.html.

Manjunath S Gabasavalagi received the Bachelor's Degree in Computer Science and Engineering from, Basaveshwar Engineering College, Bagalkot, Visvesvaraya Technological University, Belgaum, Karnataka State, India, and currently pursuing his M.Tech degree in Computer Science and Engineering in Basaveshwar Engineering College Bagalkot, Karnataka State, India. His areas of interest are Biometrics, Image processing, Telecom and Computer Networking.

Sanjeevakumar. M. Hatture received the Bachelor's Degree in Electronics and Communication Engineering from Karnataka University, Dharwad, Karnataka State, India, and the Master Degree in Computer Science and Engineering from the Visvesvaraya Technological University, Belgaum, Karnataka, India, and currently pursuing PhD Degree in the Research Centre, Department of Computer Science and Engineering at Basaveshwar Engineering College, Bagalkot under Visvesvaraya Technological University, Belgaum, Karnataka, India. His research interests include biometrics, image processing, pattern recognition, Soft computing and network security. He is life member of professional bodies like IEI and ISTE.

Nalinakshi B G received the Bachelor's Degree in Information Science and Engineering from, Tontadarya College of Engineering, Gadag, Visvesvaraya Technological University, Belgaum, Karnataka State, India, and currently pursuing her M.Tech degree in Computer Science and Engineering in Basaveshwar Engineering College Bagalkot, Karnataka State, India. Her areas of interest are Biometrics, Image processing, and Computer Graphics.

Rashmi P. Karchi received her Bachelor's Degree in Computer Science, Basaveshwar Science College Bagalkot, Karnatak University, Dharwad, Karnataka State, India, and Masters Degree in Computer Cognition and Technology, University of Mysore, Karnataka, India. Currently pursuing her PhD degree in Computer Science from Bharatiar University, Coimbatore, Tamilanadu, India. Her areas of interest are Pattern Recognition, Biometrics Security, Netwrok security and Image processing.