**International Journal of Electrical and Electronics Research** ISSN 2348-6988 (online)
Vol. 2, Issue 2, pp: (78-83), Month: April - June 2014, Available at: www.researchpublish.com

# Efficient Methods of Multimodal Biometric Security System- Fingerprint Authentication, Speech and Face Recognition

J.Deny[1], Dr.M.Sudhararajan[2]

[1] Research Scholar, Bharath University, Chennai, India,
[2] Principal, Lakshmi Narain College of Technology, Indore, India

***Abstract*: This paper proposes the efficient methods in multimodal biometric i.e. Fingerprint, Speech, Face. Multimodal system is developed through fusion of fingerprint, Speech and face recognition. The proposed system is designed for applications where the training database contains a face, fingerprint images and voice data. This proposed system may be used in various application areas such as, for authentication number of employees working in offices, in military applications and also in all possible security applications.**

**Key Words: Multimodal Biometric. Fingerprint Authentication, Speech and Face Recognition**.

## I. INTRODUCTION

"Biometrics" means "life measurement", but the term is usually associated with the use of unique physiological characteristics to identify an individual. One of the applications which most people associate with biometrics is security. However, biometrics identification has eventually a much broader relevance as computer interface becomes more natural. It is an automated method of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face fingerprints, hand geometry, handwriting, iris, retinal, vein, voice etc. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions [1]. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performance. However, even the best biometric traits till date are facing numerous problems; some of them are inherent to the technology itself. In particular, biometric authentication systems generally suffer from enrollment problems due to non-universal biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data acquisition in certain environments.

This paper proposes an efficient multimodal biometric system which can be used to reduce/remove the limitations of unimodal systems. Next section presents an overview of multimodal biometric system.

## II. MULTIMODAL BIOMETRICS SYSTEM

Multimodal biometric systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of reducing false non-match and false match rates, providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

Ross and Jain (2003) have presented an overview of Multimodal Biometrics and have proposed various levels of fusion, various possible scenarios, the different modes of operation, integration strategies and design issues. A multimodal system can operate in one of three different modes: serial mode, parallel mode, or hierarchical mode. In the serial mode of operation, the output of one modality is typically used to narrow down the number of possible identities before the next

modality is used. Therefore, multiple sources of information (e.g., multiple traits) do not have to be acquired simultaneously. Further, a decision could be made before acquiring all the traits. This can reduce the overall recognition time. In the parallel mode of operation, the information from multiple modalities is used simultaneously in order to perform recognition. The levels fusion proposed [2] for multimodal systems are broadly categorized into three system architectures which are according to the strategies used for information fusion as shown in Figure 1:

- Fusion at the Feature Extraction Level
- Fusion at the Matching Score Level
- Fusion at the Decision Level

In *Fusion at the Feature Extraction Level*, information extracted from the different sensors is encoded into a joint feature vector, which is then compared to an enrollment template (which itself is a joint feature vector stored in a database) and assigned a matching score as in a single biometric system.

In *Fusion at the Matching Score Level***,** feature vectors are created independently for each sensor and are then compared to the enrollment templates which are stored separately for each biometric trait. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score which is passed to the decision module.

In *Fusion at the Decision Level*, a separate authentication decision is made for each biometric trait. These decisions are then combined into a final vote. This architecture is rather loosely coupled system architecture, with each subsystem performing like a single biometric system.

## III. FINGERPRINT AUTHENTICATION USING MINUTIAE MATCHING ALGORITHM

The fingerprint recognition system has been developed by the Minutiae Matching Techniques [3]. The key steps involved are fingerprint enhancement, feature extraction using Minutiae Matching approach and computation of matching score. The goal of fingerprint enhancement is to increase the clarity of ridge structure so that minutiae and the reference points can be easily and correctly extracted.

***Minutiae Matching***

The input fingerprint image is enhanced using Gabor Filters The enhanced image is further binarized and thinned using a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. The thinned image is used to detect minutiae points [4] by locating ridge ending and bifurcations using Crossing Number (*CN*) method. The matching score $MS_{MIN}$ between the database and query image is computed using Elastic matching approach [5]. Figure 1 show various steps involved in minutiae extraction.

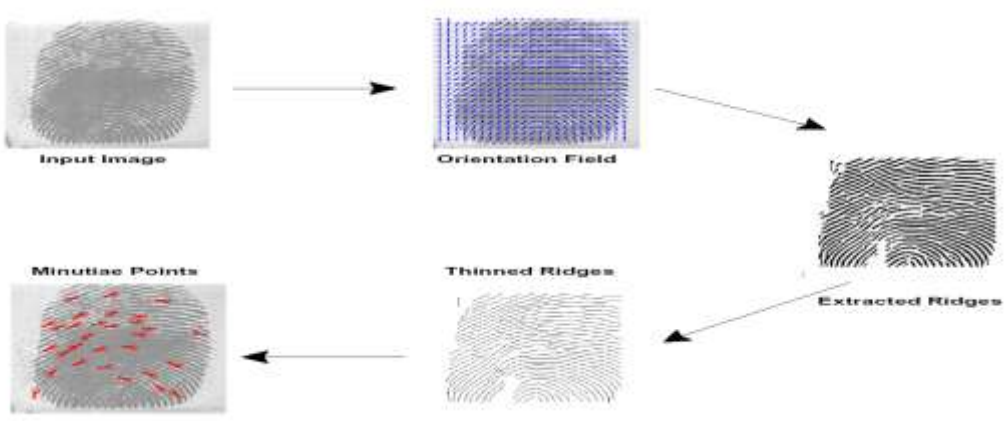


Figure1. Steps involved in minutiae extraction

## IV. SPEECH/ VOICE RECOGNITION

The speech signal is compared with that of the speech signals already stored in the database in the absence of noisy environments. This includes two modules. [6]

1 Feature extraction module.

2 Speech signal recognition module.

In the feature extraction module, the features of n number of speech signals of various speakers are stored in the database.

In the speech signal recognition module, the speech signal which is given as the input is compared with those of the signals stored in the database and is authenticated.

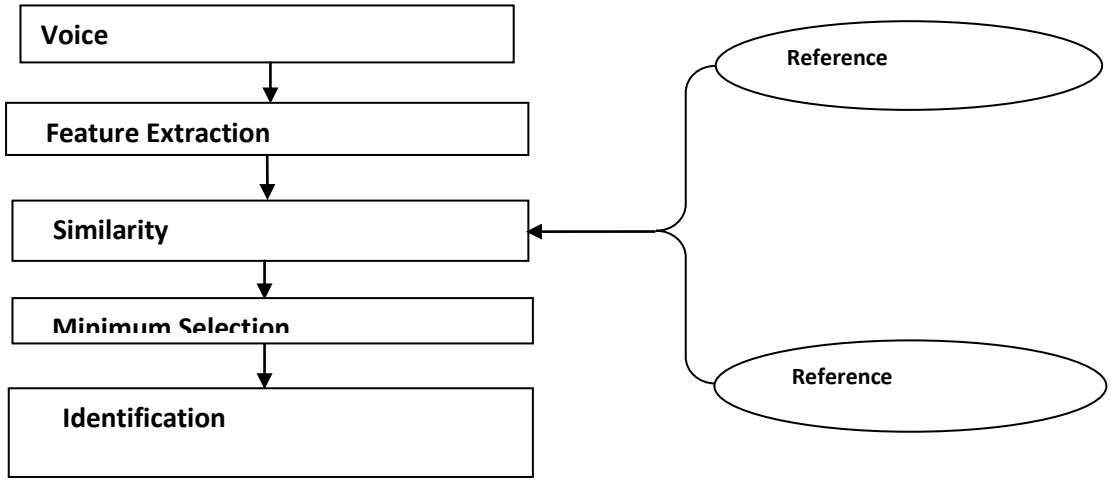


Figure 2. Flow diagram for speaker recognition

### 4.1 Speech Signal Recognition and Authentication

The real time speech signal which is given as the input in the absence of noisy environments is compared with that of the speech signals stored in the database and is recognized and authenticated. This process is performed by HMM algorithm.

#### 4.1.1 Hidden Markov Model – a Basic Description

The Hidden Markov Model is used for speech recognition, thus it is useful in particular for text-dependent speaker recognition [7]. HMM is a stochastic model. The HMM can be viewed as a finite state machine. Each state (node) in it has an associated probability density function (PDF) for the feature vector. On moving from one state to another the probability of that transition is defined. Only the first and the last states are not-emitting states, since the first is always where it is started and the last one is the one where we always end our transitions, i.e. there are no incoming transitions into the start state and there are no output transitions from the end state. Every emitting state has a set of outgoing transitions and the sum of the probabilities for those transitions is equal to one, since the transition from non-final state always must occur.

#### 4.1.2 Feature comparison

In the Speaker Verification module, each Mel-Cepstral Co-effecient vector of the test speech is compared with the codebooks to calculate its distances (e.g., Euclidean distance) to each codebook. The codebook vector closest to the test vector is found. The corresponding minimum Euclidean Distance, or Distortion Factor, is then stored until the Distortion Factor for each test vector has been calculated. The Average Distortion Factor is then found and normalized.

#### 4.1.3 The Speech Recognition and Authentication Process

The speech signal recognition module involves a series of steps.

- Apply the features to the signal to be compared.

- Compute the difference
- Compute the sum of trials.
- Perform mapping of the signal.
- Perform Mutation.
- Speech Verification Process

*Apply the features to the signal to be compared:* When the speech signal is given at real time, in the absence of noisy environments, the features of the speech signal such as cepstral co-effecients, linear prediction co-effecients, perceptual linear co-effecients are calculated. Then the file in which the signals stored in the database is opened. The end of file process is then verified. Then the minmax value for the output matrix is obtained. The minmax is the range of matrix rows which implies the minimum and maximum values for each row of the specified matrix.

*Compute the difference:* The speech signals which are stored in the database are called *reference signals or database signals*, which is in the form of reference matrix. The signal given for comparison with the signals stored is called *test signal*, which is stored in the form of test matrix. After applying the features to the signal given for verification, the difference between each of the database signal and test signal is computed. After applying the features to the signal given for verification, the difference between each of the database signal and test signal is computed.. Then the sum of this value is stored in the array containing the difference between the test signal and each of the database signals. The matrix element which returns the value zero is considered as the signal to be recognized. Example - If the $1^{st}$ element of the matrix is zero then that is the speech signal which matches with the database. Hence the first signal is matched with the real time speech input given. This is a rough computation of the authentication process.

*Compute the sum of trials:* This involves the computation of cumulative matrix , trial matrix and the comparison of the cumulative and trial matrix. The cumulative sum of the output matrix is obtained. Then the repeat index is calculated by storing the row elements and column elements in separate arrays. The trials is calculated by multiplying the matrix of cumulative sum with that of the rand function which generates arrays of random numbers whose elements are uniformly distributed in the interval (0,1).The trial matrix is generated by using the trials and the address value of the cumulative matrix with respect to the output matrix obtained by calculating the repeat index. The new matrix is hence generated by first determining the largest of the both matrices and estimating the sum of the largest matrix and adding it with one. This is the new matrix obtained.

*Perform mapping of the signal:* The next step involes mapping of the obtained output matrix from the previous process. This process is performed to improve the effeciency of the speech signal.

*Perform mutation:* Mutation is the process of obtaining a new matrix by applying random changes to the older matrix.

*Speech verification process:* After performing the trial computation and mutation the difference between the test signal and each of the reference signals are computed again. Then the absolute value of the obtained output matrix is calculated and its sum is estimated. This is stored in a matrix. In the final step mapping is performed and the minimum value is considered (which will be zero).The minimum value and its location address are stored in two different arrays. Then the appropriate voice is recognized and hence it gives the authentication. In this paper, speech samples of frequency less than 15000Hz are considered. Hence if the speech sample of frequency greater than 15000Hz are given, that signal is not authenticated.

## V. FACE RECOGNITION USING KERNEL DIRECT DISCRIMINANT ANALYSIS

Face Recognition is a noninvasive process where a portion of the subject's face is photographed and the resulting image is reduced to a digital code. Facial recognition records the spatial geometry of distinguishing features of the face [8][9][10]. The recognition algorithm takes facial image, measures the unique characteristics and computes the template corresponding to each face. Using templates, the algorithm then compares that image with another image and produces a score that measures how similar the images are to each other.

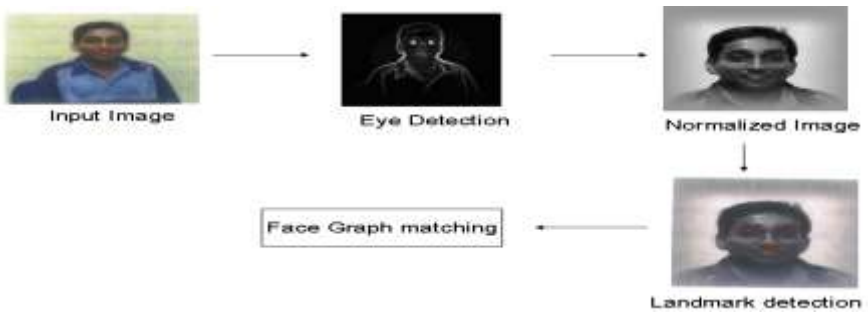


Figure 3 Steps involved in face recognition

***Kernel Direct Discriminant Analysis (KDDA)***

Face recognition using KDDA [10] is based on computation of feature space F (from training set) and projection of input pattern into the feature space to calculate significant discriminant features. For each of the *m* features in the database and *n* features in the query image, reference features are chosen depending on the distance and rotation between the positions of features in the feature space. The matching score for each transformation of database and query feature vectors are calculated with respect to reference feature chosen using bounding box technique. $MS_{KDDA}$ is defined by the maximum of all matching scores divided by the maximum number of features (among the query and the database).

## VI. EXPERIMENTAL RESULTS

The reliability of the proposed multimodal biometric system is described with the help of experimental results. The system has been tested on a database of 100 individuals. The training database contains a face, voice and fingerprint images. The multimodal system has been designed at multi-classifier and multi-modal level. At multi-classifier level, multiple algorithms/classifiers are combined to generate better results. The figure 4 shows the accuracy level of biometrics.

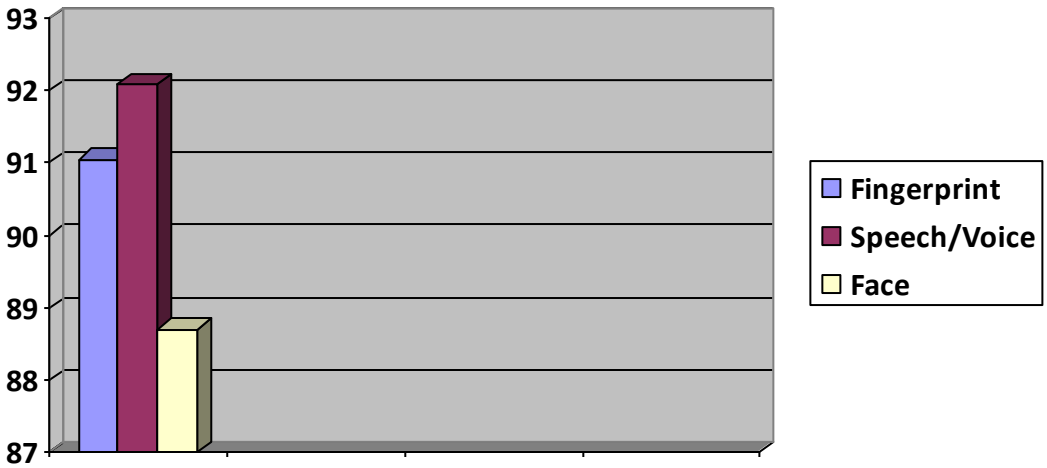


Figure 4 Accuracy level of biometrics

## VII. CONCLUSION

Biometrics systems are widely used to overcome the traditional methods of authentication. But the unimodal biometric system fails in case of lack of biometric data for particular trait. The efficient methods used to improve security level i.e. Minutiae matching for fingerprint, HMM for speech/voice recognition and Kernel Direct Discriminant Analysis for face recognition. In future in this methods implement to MANET nodes combined with Intruder detection. That is improving security level in Military network.

## REFERENCES

[1] L. Hong, A. Jain & S. Pankanti, *Can Multibiometrics Improve performance*, Proceedings of AutoID 99, pp. 59-64, 1999

[2] A. Ross & A. K. Jain, *Information Fusion in Biometrics*, Pattern Recognition Letters, 24 (13), pp. 2115-2125, 2003.

[3] J.Deny, N.Sivasankari, *Biometric Security in Military Application*, Journal of Engineering Procedia ELSEVIER,Vol.38,pp-1138-1144, 2012.

[4] A. Ross, A. K. Jain & J.A. Riesman, *Hybrid fingerprint matcher*, Pattern Recognition, 36, pp. 1661–1673, 2003

[5] N.K.Ratha, K.Karu, S.Chen & A.K.Jain, *A Real-time Matching System for Large Fingerprint Database*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 18 (8), pp. 799-813, 1996

[6] J.Deny, J.Densi, N.Sivasankari,M.Karupaharajkumar, *Approaches to iterative Speech Feature Enhancement and Recognition using HMM and Modified HMM*, International Journal of Advanced Information Science and Technology(IJAIST),Vol.6,pp.48-53,2012.

[7] Mahmoud I. Abdalla and Hanaa S.Ali, "Wavelet- Based Mel-Frequency Cepstral Coeffecients for Speaker Identification using Hidden Markov Models"

[8] I. Craw, D. Tock & A. Bennett, *Finding Face Features*, Proceedings Second European Conference Computer Vision, pp. 92-96, 1992.

[9] C. Lin & Kuo-Chin Fan, *Triangle-based approach to the detection of human face*, Pattern Recognition, 34, pp. 1271-1284, 2001.

[10] Juwei Lu, K. N. Plataniotis & A. N. Venetsanopoulos, *Face Recognition Using Kernel Direct Discriminant Analysis Algorithms*, IEEE Transactions on Neural Networks, 14 (1), pp. 117-126, 2003.