International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

Genetic Algorithm using Speech and Signature of Biometrics

Rajnish Rani [1] , Rajan Sachdeva[2]
[1] Research Fellow
[2] Assistant Professor
GGS College of Modern Technology, Kharar, Punjab, India

Abstract- Biometrics is described as the science of perceiving an individual dependent on her behavioural and physiological attributes, is starting to pick up an acknowledgement as a legitimate process for deciding the identity of an individual. Biometric systems have now been used in different forensic, civilian and commercial applications as a method for setting up an identity. Most of the biometric systems which are deployed in applications of real world are unimodal. These systems are vulnerable to various types of problems like spoofing, inter-class similarities and noisy data. Some of the limitations present in unimodal biometric systems can be removed by multimodal biometric systems. These systems allow the integration of two or more types of biometric systems. These systems are more reliable because of the presence of independent and multiple biometrics. In this paper, offline signature verification and speaker verification system are combined as both of these biometric are accepted widely. These modalities are utilized because of their ease and comparatively less cost. Multimodal biometric systems provide better recognition performance and enhance the real time verification and reliability rates.

***Keywords*— Biometrics, multimodal, signature verification, speech recognition,**

I. INTRODUCTION

In the present period of e-commerce, more administrations are being offered over the internet and electronic devices. These incorporate e-shopping, facility of credit card, banking etc. to guarantee legitimate utilization of these types of facilities just by the genuine and approved clients and keep away from any imposter or unauthorized clients, some scheme of individual authentication is installed into these administrations. At present, authentication of an individual is done basically by utilizing one of a greater amount of the accompanying means: identity cards, barcodes, personal identification numbers and text passwords. The main benefit of these methods is that they don't change their worth concerning time and furthermore unaffected by nature in which they are utilized. The primary disadvantage of them is that they can be forgotten or misused very easily. Likewise, with time more administrations are being provided over the internet and electronic devices. Consequently it gets to be unmanageable to stay informed concerning the secrets of authentication for distinctive clients. The option that gives help from one of these disadvantages is the utilization of features of biometric for authentication of an individual. Any behavioral or psychological qualities of human can be utilized as a feature of biometric and also it has the accompanying properties: acceptability, distinctiveness, performance, circumvention, collectability, permanence and universality. [1]

Biometric is a computerized technique of recognizing an individual taking into account behavioral or physiological characteristic. The past of biometrics incorporates the individual identification by particular features of body, scars or gathering of other criteria of physiological, for example, complexion, eye color and height. The present elements are recognition of fingerprints, iris, retinal scan, handwriting, voice, vein and face. As the breach security level and scam in transaction increases, the requirement for identification which is well secure and technologies of personal verification is getting to be evident. The events of recent world had led to a build enthusiasm in security hat will instigate biometric into use in major level. The areas of use in future contain travel and tourism, telephone transactions, workstation and network access and Internet transactions. There are various types of biometrics in which few are latest and few are old. Some technologies of biometric which are recognized are facial recognition, iris scanning, signature verification, hand geometry, voice recognition and fingerprinting. [2]

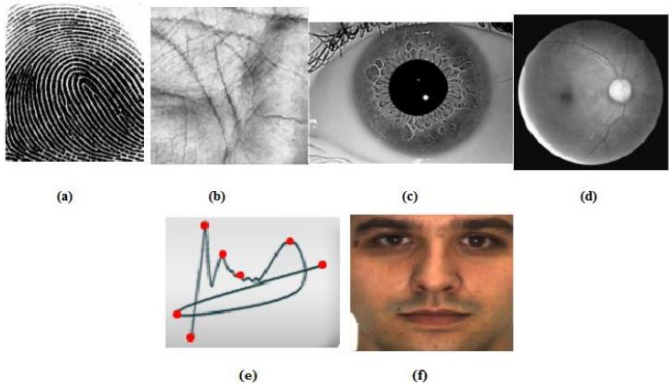


Fig. 1 Biometrics Traits: (a) fingerprint, (b) palm, (c) iris, (d) retina, (e) signature, (f) Face [2]

Identification and Verification (also called as authentication) are both utilized for declaring the user identity.

Identification: In a system of identification, recognition of an individual is done by contrasting with whole database of templates for discovering a match. The system conducts comparisons which are one-to-many for establishing the individual's identity. The individual which is to be identified does not need for claiming an identity. (Who am I?)

Verification: In a system of verification, the person to be identified needs to claim her/his identity (Am I whom I claim to be?) also this template is then contrasted with the characteristics of biometrics of an individual. The framework conducts comparisons which is one-to-one for establishing the individual's identity. Before the framework has the ability to identify/verify the particular person's biometrics, the framework needs something for contrasting it with. Along these lines, a template or profile having the properties of biometric is put away in the framework. Recording the person's characteristics is known as enrollment. [3]

II. SIGNATURE VERIFICATION

Signature verification is an essential area of research in the authentication field of an individual and also documents in banking and e-commerce. We can normally recognize two distinctive categories of systems of verification of signature: online, in which the signal of signature is captured during the process of writing, consequently making the information dynamically available, and offline in which the signature is captured once the process of writing is over and hence, a static image is only available. [4]

The written signature is viewed as the essential method of identifying the written document's signer taking into account the assumption which is implicit that normal signature of a person changes gradually and is extremely hard to forge, alter or erase without detection. The handwritten signature is one of the approaches for authorizing transactions and authenticates the identity of a human contrasted with other methods of electronic identification like screening of pattern of retinal vascular and scanning of fingerprints. It is very much easier for individuals to relocate from utilizing the popular pen-and-paper signature to one in which handwritten signature is electronically captured and verified. [5]

It is assumed that the elements of the procedure of signing begin from the inherent properties of neuromuscular system of human which creates the rapid movements which are aforementioned. Realizing that this system is constituted by numerous neurons and muscle, fibers is conceivable for declaration depending upon the theorem of central limit that a habitual and rapid movement profile of velocity inclines toward a normal equation of delta-log. This statement clarifies stability of the features of the signature. [5]

III. SPEECH RECOGNITION

The concept of interaction of human and machine prompted research in speech recognition. Automatic recognition of speech utilizes the process and technology which is related to it for changing over the signals of speech into a sequence of words or some another units of linguistics by method for an algorithm executed as a program of computer. The systems for understanding speech are presently having the ability of speech understanding in put for vocabularies of thousands of words in environments related to operation. Speech signal passes on two vital sorts of data: (a) speech content and (b) identity of speaker. The recognizers of speech expect to separate lexical data from the signal of speech autonomously of the speaker by diminishing the variability of inter-speaker. Speaker recognition is related with separating the character of an individual. [6]

Speaker recognition is the procedure of recognizing automatically who is speaking by utilizing particular information of speaker incorporated into waves of speech. This strategy can be utilized for verification of voice of claimed identified speaker. Speaker recognition can be divided into speaker identification and speaker verification. Speaker identification is the procedure of deciding from which of the speakers which are registered a given utterance comes. Speaker verification is the procedure of accepting or rejecting a claim of the identity of speaker. In majority of the applications, voice is utilized for confirming the identity claim of speaker. The system of speaker recognition can be seen as operating in mainly four stages named as Analysis, Features Extraction, Modeling and Testing as shown in Fig. 2. [7]

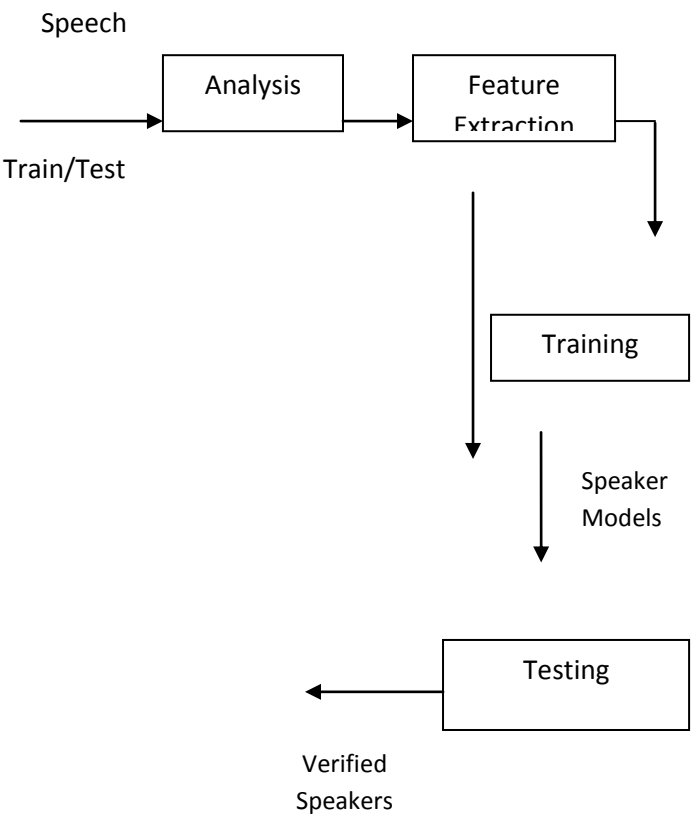


Fig. 2 Stages in the development of Speaker Recognition System. [7]

IV. MULTIMODAL BIOMETRIC SYSTEM

Conventional systems of biometric are unimodal i.e. they depend on single biometrics for authentication. Unimodal biometric system which is created by utilizing fingerprint is subjected to attack of spoofing in which impression of thumb can be effortlessly forged. Likewise in face recognition system, the variability problem of intra-class happens because of aging and facial expression variation. These types of problems can be determined in multimodal biometric systems. [8]

Multimodal biometric systems are anticipated that they would be more reliable because of the presence of fairly and numerous autonomous pieces of evidence. These frameworks have the capacity for meeting the requirements of stringent performance forced by different applications. They address the issue of non-universality, as the various traits guarantee adequate coverage of population. They additionally deter spoofing as it would be troublesome for spoofing traits of multiple biometrics simultaneously. Besides, they can encourage a type of challenge-response mechanism by asking for the client an arbitrary subset of traits of biometric and hence guaranteeing that a 'live' client is required at the purpose of acquisition of data. [8]

Fusion of modalities of biometric happens at distinctive stages in the system of biometric recognition. Some techniques of fusion which are generally employed in system of biometric authentication are given below [8]:

1. Sensor level fusion or Image level fusion: This fusion type is completed promptly in the wake of capturing modalities from sensor. For this situation, various modalities acquired from diverse sensors will be together joined and regarded as a single modality of biometric.

2. Feature level fusion: In this type of fusion, extraction of features is done from all the traits of biometrics. Later, the features which are extracted can be together combined into a feature vector which is final of higher dimension.

3. Score level fusion: This fusion level utilizes less data for fusion, in which the scores of similarity of the biometrics of individual are generated and then score are together fused for process of recognition.

4. Decision level fusion: The decisions which are acquired from the system of individual authentication are fused for authenticating a person.

V. MOTIVATION

Offline signature verification system and speaker verification system are combined as these modalities are widely accepted and natural to produce. Although this combination of multimodal enhances security and accuracy, yet the complexity of the system increases due to increased number of features extracted out of the multiple samples and suffers from additional cost in terms of acquisition time. So these days the key issue is at what degree features are to be extracted and how the cost factor can be minimized, as the number of features increases the variability of the intra-personal samples due to greater lag times in between consecutive acquisitions of the sample also increases. Increase in variability of the system will further increase FAR. Thus to resolve these issues an effective fusion level and fusion mode is required**.** Now our aim would be using more robust modelling techniques against forgeries and fusion at feature level can be used. For feature extraction of speech and signature, MFCC and SIFT are used respectively. After that fuse the extracted features and reduce the irrelevant features by using Genetic Algorithm.

The research work is based on following objectives:
1. To study types of biometric system.
2. To study speech and signature modalities.
3. To study fusion schemes in biometrics.
4. To remove irrelevant features by using Genetic Algorithm.

VI. PROPOSED SCHEME

In this research work, we have combined two biometric systems making it multimodal biometric system.

1. Choice of Modality: In this work, an offline signature verification system and speaker verification system are combined as these modalities are widely accepted and natural to produce. These days the key issue is at what degree features are to be extracted and how the cost factor can be

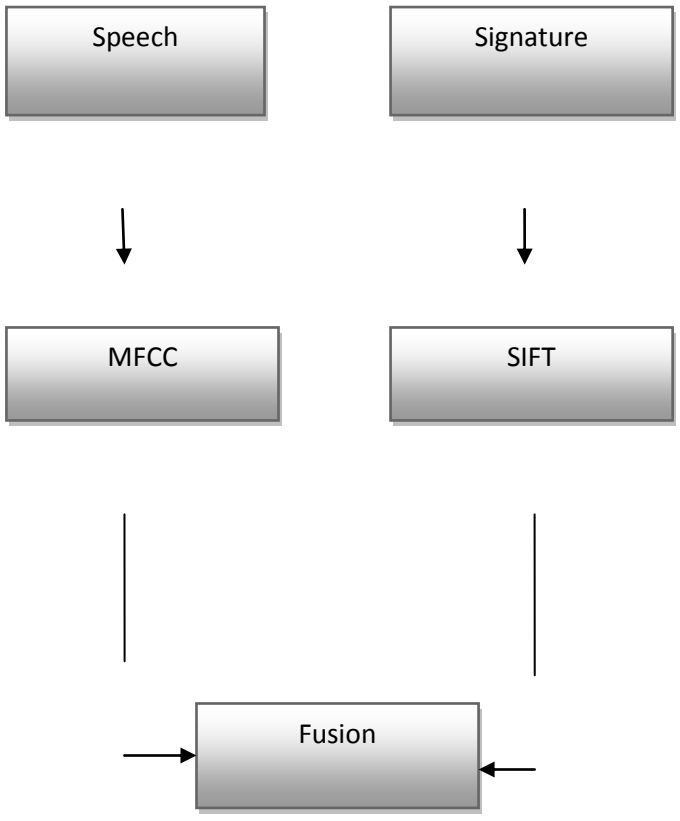
minimized, as the number of features increases the variability of the intra-personal samples due to greater lag times in between consecutive acquisitions of the sample also increases.

2. Feature Extraction

Signature: In this work, we use Scale-invariant feature transform (SIFT) to extract the features. It is widely used because it is invariant to changes in illumination, image noise, rotation, scaling and small changes in view point.
Speech: To extract features, we can use Mel Frequency Cepstral Coefficients because of the sensitivity of the low order cepstral coefficients to overall spectral slope.

3. Feature Reduction: In this work, to reduce irrelevant features from the extracted features, we follow Genetic algorithm. In the computer science field of artificial intelligence, genetic algorithm (GA) is a search-heuristic. It is used to generate useful solutions to optimization and search problems. Genetic algorithms belong to larger class of evolutionary algorithm (EA), which generates solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection and crossover.

The flowchart is shown below:



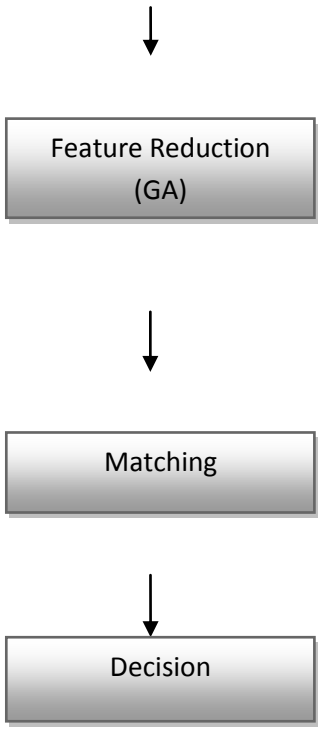


Fig. 3 Proposed algorithm

VII. RESULTS AND DISCUSSIONS

In this section, we present the results of the proposed work.

For speech and signature Samples:

Total Number of Samples in the database=36

Number of Sample that falsely accepted=0

$$FAR = \frac{\text{Total Number of Samples} - \text{Number of Samples that Falsely accepted}}{\text{Total Number of Samples}}$$

So, $\mathbf{FAR} = \frac{36-0}{36} = \frac{36}{36} 0.00\%$

For speech and signature Samples:

Total Number of Samples in the database=36

Number of Sample that falsely rejected=0

$$FRR = \frac{\text{Total Number of Samples} - \text{Number of Samples that Falsely rejected}}{\text{Total Number of Samples}}$$

So, $\mathbf{FRR} = \frac{36-0}{36} = \frac{36}{36} = 0.00\%$

FAR	FRR	Accuracy= [100-(FAR+FRR)]
0.00	0.00	100%

Table 1: FAR, FRR and ACCURACY

Sample No.	Speech	Signature	Fusion	Genetic Algorithm	Total
1	0.3	0.03	0.07	5.13	5.53
2	0.07	0.07	0.06	4.99	5.19
3	0.03	0.06	0.05	5.5	5.64
4	0.04	0.15	0.09	6.12	6.4
5	0.09	0.03	0.03	4.89	5.04
6	0.17	0.16	0.07	4.14	4.54
7	0.03	0.03	0.06	5.4	5.52
8	0.07	0.04	0.05	5.16	5.32
9	0.06	0.09	0.04	4.90	5.09
10	0.15	0.17	0.05	5.17	5.54
11	0.17	0.03	0.08	6.11	6.39
12	0.19	0.07	0.06	6.8	7.12
13	0.12	0.03	0.07	5.9	6.12
Sample No.	Speech	Signature	Fusion	Genetic Algorithm	Total
14	0.05	0.04	0.06	5.1	5.25
15	0.04	0.09	0.05	5.19	5.37
16	0.05	0.04	0.04	4.99	5.12
17	0.18	0.06	0.05	5.78	6.07
18	0.07	0.19	0.04	5.16	5.46
19	0.03	0.12	0.06	5.13	5.34
20	0.04	0.05	0.07	4.99	5.15

Table 2: Time analysis (seconds)

VIII. CONCLUSION & FUTURE SCOPE

The main aim of this research is to combine the two methods of biometric i.e. speech and signature to make the multimodal biometric system. A multimodal biometric system removes the problems which are present due to unimodal biometric systems i.e. unacceptable error rates, spoof attacks, non-universality etc. Multimodal biometric systems gives better results than unimodal biometric systems and are very popular even though they are complex. Multimodal biometric system capture two or more samples of biometric and then utilize fusion for combining their analyzes to create a decision of better match by decreasing the FRR and FAR simultaneously.

ACKNOWLEDGMENT

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

REFERENCES

[1] Eshwarappa M.N., Dr. Mrityunjava V. Latte, "Multimodal Biometric Person Authentication using Speech, Signature and Handwriting Features", International Journal of Advanced Computer Science and Applications, Special Issue on Artificial Intelligence.

[2] Renu Bhatia, "Biometrics and Face Recognition Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 5, May 2013.

[3] Sravya. V, Radha Krishna Murthy, Ravindra Babu Kallam, Srujana B, "A Survey on Fingerprint Biometric System", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 4, April 2012.

[4] Hassan Soliman, Abdelnasser Saber Mohamed, Ahmed Atwan, "Feature Level Fusion of Palm Veins and Signature Biometrics", International Journal of Video & Image Processing and Network Security, Vol. 12, No. 1, February 2012.

[5] O. C Abikoye, M. A Mabayoje, R. Ajibade, "Offline Signature Recognition & Verification using Neural Network", International Journal of Computer Applications, Vol. 35, No. 2, December 2011.

[6] Suma Swamy, K. V Ramakrishnan, "An Efficient Speech Recognition System", Computer Science & Engineering: An International Journal (CSEIJ), Vol. 3, No. 4, August 2013.

[7] Prof. Rupali Pawar, Miss. Hemangi Kulkarni, "Analysis of FFSR, VFSR, MFSR Techniques for Feature Extraction in Speaker Recognition: A Review", International Journal of Computer Science Issues, Vol. 7, Issue 4, No.1, July 2010.

[8] M. Fathima Nadheen, S. Poornima, "Feature Level Fusion in Multimodal Biometric Authentication System", International Journal of Computer Applications, Vol. 69, No. 18, May 2013.

[9] Arun Ross, Anil K. Jain, "Multimodal Biometrics: An Overview" ,Proc. Of 12th European Signal Processing Conference (EUSIPCO), pp. 1221-1224, September 2004.

[10] Shashi Kumar D R, K B Raja, R. K. Chhotaray, Sabyasachi Pattanaik, "Off-line Signature Verification Based on Fusion of Grid and Global Features Using Neural Networks", International Journal of Engineering Science and Technology, Vol. 2 (12), pp. 7035-7044, 2010.

[11] Mandeep Kaur, Akshay Girdhar, Manvjeet Kaur, "Multimodal Biometric System Using Speech and Signature Modalities", International Journal of Computer Applications, Vol. 5, No. 12, August 2010.