IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-8 E-ISSN: 2347-2693

A Review of Face and Speech multimodal Biometrics for security using Genetic Algorithm

Nancy Bansal

Dept. of Computer Science & Engineering, Chandigarh College of Engineering-Landran Punjab

Samanpreet Singh

Department of Computer Science & Engineering, Landran, Punjab

Available online at: www.ijcseonline.org

Received: 22/Jul/2016 Revised: 30/Jul/2016 Accepted: 18/Aug/2016 Published: 31/Aug/2016

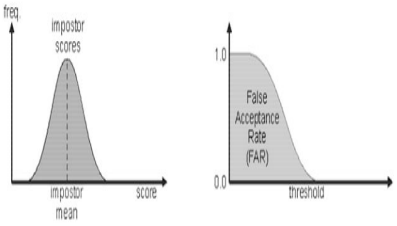
Abstract— Multimodal biometrics is the combination of two or more modalities such as face and speech modalities. In two modalities have been presented with genetic algorithm to show the effect of Genetic algorithm in the accuracy level of a biometric system. Face recognition is the most popular physiological characteristic used to identify a person in biometric systems, because of feasibility, permanence, distinctiveness, reliability, accuracy, and acceptability. On the other hand speech recognition is the most popular behavioral characteristic used in biometric systems. Thus, we believe that the combination of these two methods will have reliable and accurate results. So, this paper has provided the review using an evolutionary method.

Keywords- Multimodal Biometrics, Genetic Algorithm, Security

I. INTRODUCTION

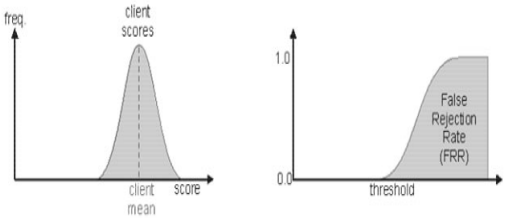
Biometric systems automatically determine or verify a person's identity based on his anatomical and behavioral characteristics such as fingerprint, palm print, vein pattern, face and iris [1]. A method of identifying or verifying the identity of an individual person or subject based on the physiological and behavioral characteristics is called biometric recognition. Multimodal biometrics increase accuracy by considering other highly specific biological traits to limit the number of applicant for an identity [2, 3]. Multimodal biometric systems utilize more than one physiological or behavioral characteristic for enrollment, verification and identification. The reason to combine different modalities is to improve recognition rate. The aim of multimodal biometrics is to reduce one (or) more of the following:

- ***False Accept Rate [FAR]*** is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.



FAR= imposter scores exceeding threshold / all imposter scores

- ***False Reject Rate [FRR]*** is the instance of a security system failing to verify or identify an authorized person. A system's FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts.



FRR= client scores falling below threshold / all client scores

- ***Failure to enroll rate [FTE]*** is the percentage of the population which fails to complete enrollment for a biometric solution or application. Failure can be due to physical differences, to lack of training, environmental conditions or ergonomics.

Any physiological or behavioral feature may be used as a biometric verifier as long as it satisfies the following requirements [4]:

- ***Universal:*** Each individual must own this characteristic.
- ***Distinctiveness:*** Two persons possessing the same type of characteristic does not exist.
- ***Permanence:*** The characteristic must be invariant for a time period as long as possible.
- ***Collectability:*** Indicates the fact that biometric may be quantitatively measured.

- ***Performance:*** This directs towards the accuracy of the tangible recognition, speed, robustness, as well as the prerequisites for touching a definite level of performance.
- ***Acceptability:*** This indicates the degree in which the given biometric characteristic is accepted by the clients.
- ***Resistance to circumvention:*** This indicates the facility through which a system can avoid fraud.

1.1 Operations on Biometrics

There are mainly two types of operations:

Verification phase – In verification phase the system check the identity of the person by relating the taken biometric data with the template data that is stored in the database. In this system a person claims the identity who needs to be recognize via username,a Personal Identification number, a smart card,after that a one to one comparison is conducted that whether the claim is right or wrong [5].Verification is important so that several persons could not use the same identity or individuality. It is critical component for positive recognition.

Identification phase - In identification phase recognition of an individual's take place by examining the templates of every person in the databank for matching. For establishing the identity of the individual to many comparisons are conducted. No claiming is done in this phase. Identification is done to check that whether the person is not denying. Is main purpose is to stop the individual from using various individualities [5].

Four modules of biometric system are in figure 2:

- ***Sensor modules –*** sensor module to get the biometric data of the person. In this raw data is captured and then send to the feature extraction module.
- ***Feature Extraction –*** In this the data that is captured in the sensor module is processed and then features has to be extracted,
- ***Matcher module-*** In matcher modules the features are compared with the template data that is stored in the database and generate the matching scores. It is also consider as the decision making module.
- ***System Module-*** In this module the biometric template of the registered persons are stored in the template [6].

1.2 Types of Biometrics

a. Face

Face recognition is a non-intrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled "mug-shot" verification to an active, uncontrolled face identification in a cluttered background [7]. The most popular approaches to face recognition are based on either the location or shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or the overall analysis of the face image that represents a face as a weighted grouping of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available. They impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple surroundings or special clarification.

b. Speech

Speech recognition process is basically done by the Speech Recognition System. In the speech recognition procedure, speech response signal is handled into acknowledgement of speech by means of a manuscript form [8]. Speech Acknowledgement System aids the technique to bring computers and human being's much closer than before. There is elementary terms which an individual need to know in order to implement or develop a Speech Recognition System.

- ***Utterances-*** client response speech is entitled as utterances, in simple words when user speaks something it is called utterances.
- ***Pronunciations-*** Single word has multiple meanings and multiple recognitions. It all depends on accent. A solitary word is spoken in dissimilar means in agreement to age, country, and so on.
- ***Accuracy-*** It is the performance measurement tool. It is measured by number of means but in this case, if speaker utters "NO", then Speech Recognition System must recognize it as word "NO". If it is done precisely then accuracy of system is efficiently very good or else.
- Separation of speech recognition system in different classes can be made based on what type of utterance they have ability to recognize.

II. LITERATURE SURVEY

A multimodal biometric system integrating fingerprint and speech in making a personal identification was introduced. The processed information was combined with the help of fusion algorithm in score level in which feature vectors were made independently for query images and are then compared to the enrollment templates which are stored during database preparation for each biometric attribute. Reliant on the proximity of the particular feature vector as well as template, each single subsystem calculates its individual matching score. These systems provided preferable False Acceptance Rate (FAR) and False Rejection Rate (FRR) enjoying better recognition.[9]

It presents our implementation of the Gamma tone filter-based feature and the experimental results on Mandarin speech information. By way of some detailed designs, they acquired noteworthy performance gains with the new feature in various noise conditions when compared with the widely used MFCC and PLP characteristics. The actual novelty of their execution is that the filter design is purely in the present time domain. This means that the channel signals present there are obtained with a set of Gamma tone filters applied directly on the speech signals in present time domain that is entirely dissimilar from the

generally adopted frequency domain design that first converts signals to spectra and then applies the filter banks upon them. The actual time-domain execution going on the one hand avoids the approximation introduced by short-time spectral analysis and hence is more precise; and conversely, it eludes the multifaceted spectral calculation and hence simplifies hardware realization.[10]

In Mel Frequency Central Coefficient is a very communal as well as efficient method for signal handling. This paper demonstrates a novel purpose of functioning with MFCC by means of utilizing it particularly for Hand gesture acknowledgement. The main aim of utilizing MFCC for hand gesture acknowledgement which is utilized to discover the usefulness of the MFCC for image handling. Until now it has remained utilized solely in speech acknowledgement, for speaker verification. The existing system is dependent upon transforming the hand gesture into 1-D signal and also then take out first 13 MFCCs by the transformed 1-D signal. Grouping is done by utilizing Support Vector Machine. Investigational consequences signifies that projected application of utilizing MFCC for gesture acknowledgement have very good accurateness and therefore it can be utilized for identification of symbol linguistic or else for additional household application by means of utilizing them as the combination for several other methods for example Gabor filter, DWT to intensification of the exactness rate as well as to make it furthermore proficient.[11]

Explained the experimental result to show a way to combine a password with a speech biometric cryptosystem. The authors presented two schemes to enhance verification performance in a biometric cryptosystem utilizing a password. Together they could easily counter attack a password brute-force exploration if the biometrics are not co-operated. Even after, if the biometrics are negotiated, the attackers have to create countless more efforts in searching for cryptographic keys in the system described in this particular work, matched towards an old-fashioned password-reliant approach. Finally, it is shown the error rate of the proposed scheme is the same as in a traditional password-based approach even when genuine biometrics or templates are compromised.[12].

III.GENETIC ALGORITHM BASED MUILTIMODAL SYSTMES

Genetic algorithm is the type of algorithm that is used to solve both constrained and non-constraint problems based on selection criteria. Genetic algorithm modifies the new population and generate new solutions until best solution has not been reached. From large set of population, genetic algorithm uses the random chromosomes to make it parent then make it to produce children. The repetition goes on until good solutions has not been achieved on the basis on the fitness function

❖ Genetic algorithm has mainly three operators;

1. Selection, in which selection of chromosome is done.

2. Mutation, in which two chromosomes gets mutated to generate child.

3. Crossover, to apply new changes.

It is not possible always to generate optimal solutions for complex problems.

❖ *Genetic Algorithm can be described as below:*

- ***[Fitness]*** Evaluate the wellness f(x) of every chromosome x in the populace,F fitness function.
- ***[New population]*** Create another populace by rehashing after ventures until the new populace is finished.
- ***[Replace]*** Use new produced populace for a further run of calculation
- ***[Test]*** if the end condition is fulfilled, stops, and returns the best arrangement in current population.

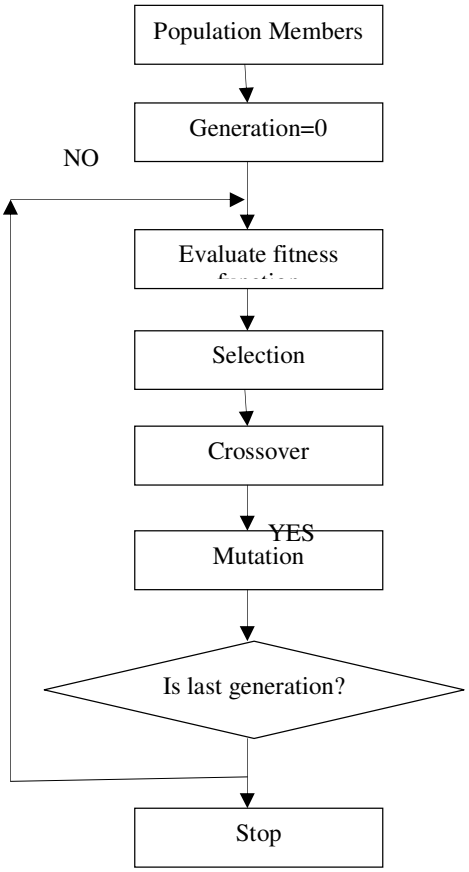


Figure.1: GA Process

Steps of Genetic Algorithm

Step1: Initialize random population consists of chromosomes.

Step 2: Compute fitness function in the population.

Step3: Develop new population consists of individuals.

Step4: Selection of parent chromosomes to get best fitness function.

Step5: Perform crossover to get copy of parents.

Step6: Perform mutation to mutate new off springs.

Step7: Place new offspring into the population.

Step8: Repeat steps to get a satisfied solution.

Step 9: Stop

IV.COMPARISON TABLE

Technique	Accuracy (%)	Application
For Speech Recognition		
LPC [14]	91	Robot movement
MFCC[14]	90	Numeral reading
ZCPA [14]	96	Isolated word re-cognition
DTW [14]	90	Isolated numeral recognition
Technique	**Accuracy (%)**	**Application**
For Face Recognition [15]		
SVM	97	Dummy face re-cognition
LBP	94	Chinese face re-cognition
SRC	90	Dummy face re-cognition

V. CONCLUSION AND FUTURE SCOPE

Biometric authentication systems verify an individual's claimed-identity from traits of behavioral (signature, voice) or physiological traits (face, iris, and ear). Multimodal biometric system overcomes the limitations of unimodal biometric systems such as non-universality, spoofing, noise in sensed data, intra-class variability, inter -class variability. Multimodal biometric system can be constructed by utilizing more than one characteristics of physiological or behavioral for identification and verification purposes. So this paper has reviewed two multimodal biometrics i.e. face and speech with genetic algorithm advantages.

REFERENCES

[1] A. K. Jain, K. Nandakumar, X. Lu, and U. Park. "Integrating Faces, Fingerprints and Soft Biometric Traits for User Recognition. In Proceedings of ECCV International Workshop on Biometric Authentication (BioAW)", volume LNCS 3087, pages 259–269, Prague, Czech Republic, May 2004, Springer.

[2] A. Ross and R. Govindarajan. "Feature Level Fusion Using Hand and Face Biometrics". In Proceedings of SPIE Conference on Biometric Technology for Human Identification II, volume 5779, pages 196–204, Orlando, USA, March 2005.

[3] A. Ross, K. Nandakumar, and A. K. Jain. "Handbook of Multibiometrics". Springer, 2006.

[4] Inthavisas, K., and D. Lopresti. "Secure speech biometric templates for user authentication." IET biometrics, vol. 1, pp. 345-349, 2012.

[5] Jun Qi et.al "Auditory Features Based on Gamma tone Filters for Robust Speech Recognition" May 2013

[6] K.D.Mitnick,W.L.Simon."The Art of Deception:Controlling the Human Element of Security" Wiley, 2002.

[7] S.T.Pan,"A canonic-signed-digit coded genetic algorithm for designing finite impulse response digital filter", Digital Signal Process. 20 (2) (2010) 314– 327.

[8] Seyed Hassan Sadeghzadeh, Morteza Amirsheibani and Anseh Danesh Arasteh "Fingerprint and Speech Fusion: A Multimodal Biometric System", International Journal of Electronics Communication and Computer Technology (IJECCT), Volume 4 Issue 2, pp. 456-459, March 2014

[9] Seyed Hassan Sadeghzadeh, Morteza Amirsheibani and Anseh Danesh Arasteh "Fingerprint and Speech Fusion:A Multimodal Biometric System",International Journal of Electronics Communication and Computer Technology (IJECCT), Volume 4 Issue 2, pp. 456-459, March 2014

[10] Shikha Gupta, Jafreezal Jaafar, Wan Fatimah wan Ahmad and Arpit Bansal, "Feature Extraction Using Mfcc" Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.4, August 2013.

[11] W. E. Burr, D. F. Dodson, and W.T.Polk. "Information Security: Electronic Authentication Guideline". Technical Report Special Report 800-63, NIST, April 2006.

[12] X. Liu and T. Chen."Geometry-assisted Statistical Modeling for Face Mosaicing". In Proceedings of IEEE International Conference on Image Processing (ICIP),volume 2,pages 883–886,Barcelona,Spain,September 2003.

[13] Yohei Ishii, "Face and Head Detection for a Real-Time Surveillance System", Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04) 1051-4651/04 $ 20.00 IEEE .

