

Secure Multimodal Biometric Recognition Based on Speech, Face and Fingerprint Using Feature Level Fusion Approach

Ravdeep Kaur¹, Baldip Kaur²

Student, LLRIET, Moga¹

Assistant Professor, LLRIET, Moga²

Abstract: Biometric is the field for user authentication and verification as well as for providing security from unauthorized access. Various biometric traits have been utilized for development of secure model to provide security. Uni-modal biometric system has been designed to authorize user identity. These systems use single biometric traits that can be used for recognition process. Biometric traits are face, finger, iris, palm, vein and speech. On the basis of these systems authentication models have been prepared that can be used for user validation. The main problem in uni-modal biometric system is that due to use of single trait of biometric it is an easy process to capture biometric identification of individual. In recent research multimodal biometric authentication systems have been developed that can be used for authentication of the users. To overcome security threats in the proposed work face finger and voice based traits have been included to develop more accurate and secure system.

Keywords: Biometric, Speech, Face, Finger, Iris, Palm

1. INTRODUCTION

1.1 Biometric Systems

A biometric system is basically a pattern recognition system that works by getting biometric information from an individual, extracting a feature set from the given data, and comparing these features with the feature set in the database. Depend upon the application setting; a biometric framework may work either in verification mode or Identification mode [1]. In the verification mode, the frame work accepts a person's identity by contrasting the caught biometric information and her own biometric template(s) stored in the system database. In such a framework, a person who desires to be recognized claims a character, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one to one correlation with figure out if the case is valid or not. Identity verification is used for acknowledgment, where the point is to prevent multiple individuals from utilizing the same character [2].

1.2 Types Of Biometric Multi-Modals

- Face
- Gait
- Voice
- Hand Geometry
- Fingerprint

1.2.1 Face

Face recognition is a non-meddlesome technique, and facial pictures are likely the most widely recognized biometric trademark utilized by people to make an individual recognition. The utilizations of facial recognition range from a static, controlled "mug-shot" confirmation to a dynamic, uncontrolled face recognizable proof in a jumbled foundation [3]. The most well-known ways to deal with face recognition depend on either: 1) the area and state of facial characteristics, for example, the eyes, eyebrows, nose, lips and button, and their spatial connections, or 2) the overall (worldwide) examination of the face picture that speaks to a face as a weighted combination of a number of canonical faces [4].

1.2.2 Fingerprint

- Unique mark Identification is the procedure for recognizable verification using the impressions made by the moment edge arrangements or cases found on the fingertips. No two people have exactly the same arrangement of edge illustrations, and the case of any one individual stay unaltered all through life. Fingerprints offer an in fallible strategy

for individual ID [5]. Other individual qualities may change, yet fingerprints don't. Fingerprints can be recorded on a standard unique card or can be recorded digitally and transmitted electronically to the FBI for examination. By differentiating fingerprints at the scene of a wrong doing with the unique mark record of suspected people, Authorities can construct incomparable confirmation of the region of character of an individual. In 1924 the recognizing evidence division for the Federal Bureau of Investigation (FBI) was secured to give one central store of fingerprints [6].

- **Fingerprint Pattern Type**

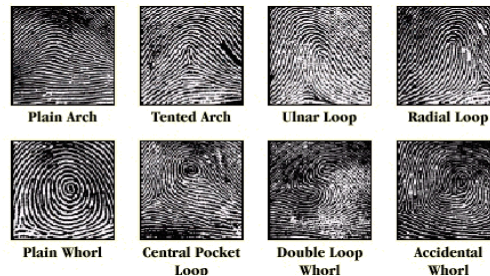


Figure 1.4: Fingerprint samples

- **Fingerprint acquisition**

The most established and most known unique finger impression getting strategy is the "ink technique", that is, squeezing the finger against a card in the wake of spreading the finger skin with ink; this framework is nowadays still, all things considered, used by the police as a piece of AFIS [7]. The cards are changed over into cutting edge structure by technique for scanners undefined to those conventionally used for comprehensively valuable paper records. The default determination is 500 dpi. This methodology can convey pictures including regions which miss a few information, on account of over the top inkiness or to ink need, and is unmistakably compelled to quantifiable applications [8]. The Frustrated Total Internal Reflection (FTIR) is the most used and develops live-sweep detecting system. The finger is illuminated from one side of a glass precious stone with a LED, while the opposite side transmits the photo through a perspective to a CDD/CMOS detecting segment which changes over light into mechanized information. The nonattendance of reflection achieved by the region of water particles where the edges touch the precious stone grants edges to be isolated from valleys.

1.3 Speech

Speech recognition basically means talking to a computer, having it recognize what we are saying, and lastly, doing this in real time. This process fundamentally functions as a pipeline that converts PCM (Pulse Code Modulation) digital audio from a sound card into recognized speech. The elements of the pipeline are: Transform the PCM digital audio into a better acoustic representation– The input to speech recognizer is in the form of a stream of amplitudes [9], sampled at about 16,000 times per second. But audio in this form is not useful for the recognizer. Hence, Fast-Fourier transformations are used to produce graphs of frequency components describing the sound heard for 1/100th of a second. Any sound is then identified by matching it to its closest entry in the database of such graphs, producing a number, called the "feature number" that describes the sound. Unit matching system provides likelihoods of a match of all sequences of speech recognition units to the input speech. These units may be phones, diaphones, syllables or derivative units such as fanons and acoustic units. They may also be whole word units or units corresponding to group of 2 or more words. Each such unit is characterized by some HMM whose parameters are estimated through a training set of speech data. Lexical decoding constraints the unit matching system to follow only those search paths sequences whose speech units are present in a word dictionary [10].

1.4 Applications Of Biometric Systems

Biometric applications fall into three primary gatherings:

- Business applications, for example, PC system logins, electronic information security, e-trade, Internet access, ATMs, credit cards, physical access control, PDAs, PDAs, medical records administration, and distance learning [11];
- Government applications, for example, national ID cards, restorative offices, driver's licenses, social security, border control, visa control, and welfare-payment; and
- Forensic applications, for example, corpse distinguishing proof, criminal examination, terrorist identification, parenthood determination, and missing youngsters. Traditionally, business applications have utilized information based frameworks utilizing PINs and passwords, government applications have used frameworks taking into account tokens, for example, ID cards and identifications, and legal applications have depended on human specialists to coordinate biometric highlights. In the business class, applications require positive acknowledgment and may utilize the biometric framework either in check or ID mode. The administration and criminological classifications comprise of principally negative-acknowledgment applications that require ID [12].

2. REVIEW OF LITERATURE

Jiali Yu et. al. [1] proposed another method for face recognition utilizing the texture features. Texture features regularly have a turning disfigurement, and have solid resistibility to commotion. The paper first develops the dim level co-event framework of face picture to portray surface component of face picture, and after that uses the order strategy for least weighted Euclidean separation to satisfy the coordinating and distinguishing proof of face. Tests results have demonstrated that acknowledgment rate was incredibly expanded by the blend of weighted Euclidean separation and surface component.

P. Mohanaiah, et. al. [2] proposed a new approach for feature extraction of images for indexing and retrieval. Low level image features such as extraction of color, texture and shape. This paper represent grey level co-occurrence matrix(GLCM) to extract statistical texture features. The result shows texture features have high accuracy and less computation time.

Matti Pietikainen et. al.[3]Proposed approach for texture feature face recognition utilizing LBP (Local Binary Patterns). Highlights utilized for texture investigation have been effectively utilized as a part of some biometric applications. Texture-based locale descriptors can be extremely helpful in perceiving countenances and outward appearances, recognizing faces and different facial segments, and in other face related assignments. This paper exhibits this issue by considering the nearby double example (LBP) for instance of surface based approach and demonstrating its efficiency in facial picture analysis. Local binary pattern example utilized a 3*3 framework on the picture sections and figured the paired example utilizing limit esteem from the centre pixel values.

Koneru Anuradha et. al. [4] given another technique to face recognition. In this paper mix of KLDA (combination of LBP and GABOR features) with inclination face features (which are more resistive to the commotion impacts) for more powerful acknowledgment process. This make three principle commitments: (i) exhibit a basic and proficient pre-handling chain that wipes out a large portion of the impacts of changing light while as yet protecting the vital appearance points of interest that are required for acknowledgment; (ii) present Local Ternary Patterns (LTP), a speculation of the Local Binary Pattern (LBP) nearby surface descriptor that is more segregate and less touchy to calm or in uniform areas, and demonstrate that supplanting correlations in view of neighborhood spatial histograms with a separation change based likeness metric further enhances the execution of LBP/LTP based face acknowledgment; and (iii) enhance heartiness by including Kernel PCA highlight extraction and joining rich neighborhood appearance signals from two integral sources –Gabor wavelets and LBP – demonstrating that the mix is extensively more precise than either highlight set alone.

Timo Ahonen et. al. [5] proposed a methodology Local Phase Quantization (LPQ). This technique depends on the quantizing the Fourier changes stage in nearby neighborhood. The stage can be appeared to be an obscure invariant property under certain generally full-filled conditions. In face picture examination, histograms of LPQ names figured inside neighborhood areas are utilized as a face descriptor also to the generally utilized Local Binary Pattern (LBP) strategy for face picture portrayal. The test results on CMU PIE and FRGC 1.0.4 datasets demonstrate that the LPQ descriptor is exceptionally tolerant to obscure

3. METHODOLOGY

In the purposed work speech features have been extracted using MFCC approach. The MFCC approach divides the signal into different short frames. The periodogram power estimator has been used for each frame available. Then after computing power spectra filter bank has been implemented on each short fame and energy of these frames has been summed up. By taking the logarithm of all filter banks discrete cosine transformation has been implemented on these frames to extract the coefficient of these frames. In the purposed work face and fingerprints samples of different individual have been used for authentication process. These samples have been used for extraction of features from the face and fingerprint samples. After extraction of the features from different samples these features have been fused using feature level fusion approach that has been used for fusing of all the feature values. These features have been fused on the basis of different phase and magnitudes.

After fusion these features have been stored in a dataset file so that can be used for recognition process. In the process of recognition different testing samples have been loaded to the system and these samples have been used for extraction of features using extraction approaches. These samples features have been fused and distance classifier has been used for matching of testing fused features with dataset features. Distance classifier computes distance of testing features from all the features available in the dataset. The minimum index distance is the best matching features to a particular set. This process is used for different samples to evaluate performance of the purposed work. In this distance classifier and machine learning based classifier has been used for matching process. In the purposed system biometric sensors can be used for capturing of testing face and fingerprint samples that can be used for matching process.

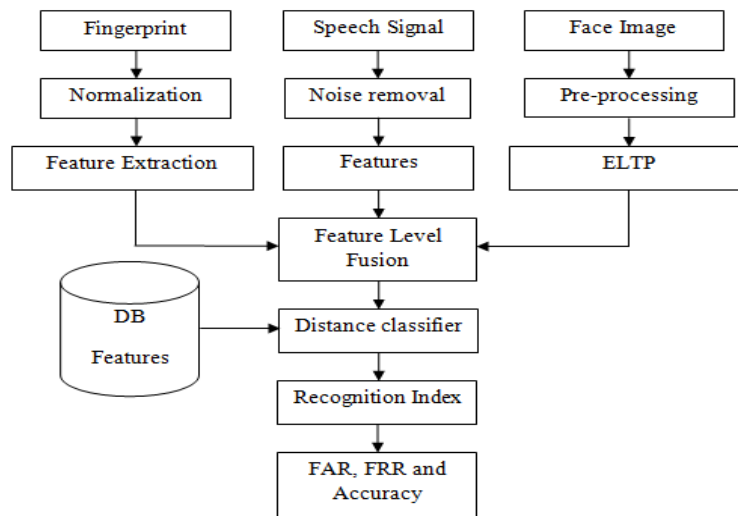


Fig 3.1 Flow chart of proposed work

Figure 3.1 represents the flow chart for proposed work that has been done for feature extraction using multimodal biometric authentication system. The various steps have been represents in the flow graph that has to be carried out in the proposed work. By performing these operations that have been explained in the flow chart of proposed work multimodal biometric system can be generated and reformed for authentication of the different users at different platforms.

4. RESULTS

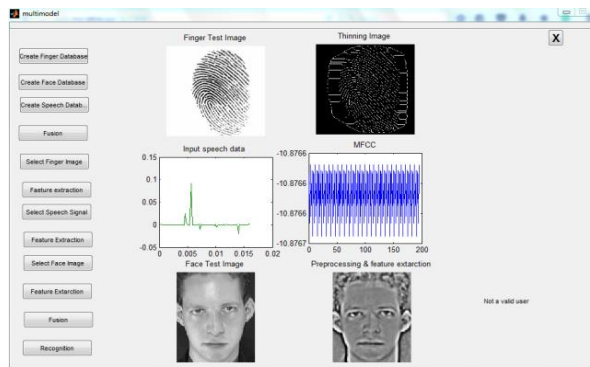


Figure 4.1: Face image capturing for proposed model

This figure represents face image has been loaded to the system. Face image has been used for extraction of texture features using ELTP approach. Before extraction of features image has been normalized using pre-processing approach. In the process of pre-processing image has been filtered using Gaussian filter that removes noise available in the image. In the process of pre-processing of the image different gamma, sigma and contrast enhancement operator has been used for noise removal. Noise available in the image is much sensitive to texture feature that can change features available in the image. Uniform patterns have been extracted from the image and illumination changed has been normalized in pre-processing that degrades different lightening affect available in the image. After process of normalization image has been used for extraction LTP based features using 3*3 masks on the image. That moves on single image pixel by pixel and computes feature value of different face images.

This figure represents after normalization process LTP based features have been computed from the image. Mask has been moved pixel by pixel and centered pixel value with threshold has been compared with neighbor pixel value. On the basis of pixel value comparison upper and lower ternary codes have been generated for single patch of the images. Upper and lower ternary codes has been based 3 values that are computed on the basis of neighbor pixel difference with centre pixel values. These codes have been generated for all the patches by rotating mask on all pixels available in the image.

Codes from all the patches are concatenated using histogram concatenation approach. Histogram concatenation approaches combines all upper and lower ternary codes can histogram values vector has been created that is used for computation LTP based features from face image.

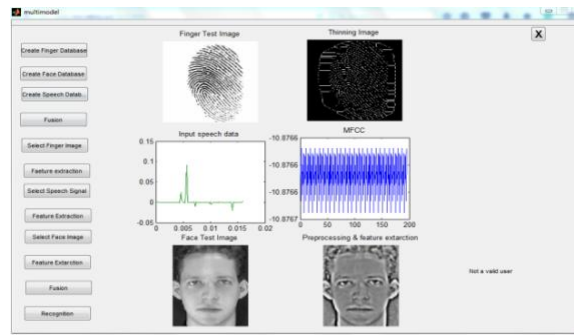


Figure 4.2: LTP based features extraction from face image

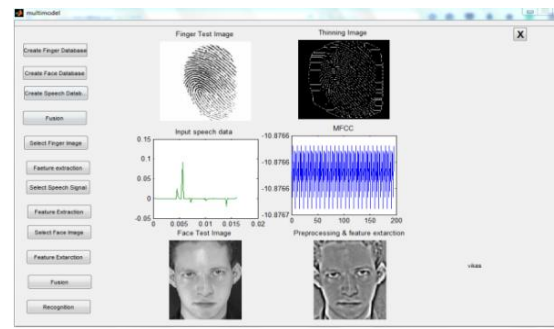


Figure 4.3: Feature Fusion and recognition

After extraction of face and finger images features feature level fusion has been done for combining of face and fingerprint features. In feature level fusion feature dimension has been made equal and magnitude and the phase has been measured for individual feature set. These features set have been combined tighter to form a new feature vector that contains properties of face and fingerprint features. After process of fusion histogram based distance computation approach has been used for computing distance between testing samples features and dataset samples features. On the basis of minimum distance recognition index has been measured. At which point minimum distance between testing and dataset features has been measured that is maximum matched point for purposed system. After matching various performance evaluation parameters have been measured for purposed system.

4.1. PERFORMANCE EVALUATION PARAMETERS

A biometric recognition system can run in two different modes: identification or verification. Identification is the process of trying to find out a person's identity by examining a biometric pattern calculated from the person's biometric features. In the identification case, the system is trained with the patterns of several persons. For each of the persons, a biometric template is calculated in this training stage. A pattern that is going to be identified is matched against every known template, yielding either a score or a distance describing the similarity between the pattern and the template. The system assigns the pattern to the person with the most similar biometric template. To prevent impostor patterns from being correctly identified, the similarity has to exceed a certain level. If this level is not reached, the pattern is rejected. In the verification case, a person's identity is claimed a priori. The pattern that is verified only is compared with the person's individual template. Similar to identification, it is checked whether the similarity between pattern and template is sufficient to provide access to the secured system or area.

4.1.1. FAR

False acceptance rate has been measured for a system that false accepts an impostor on the recognition system. The threshold depending fraction of the falsely accepted patterns divided by the number of all impostor patterns is called False Acceptance Rate (FAR). Its value is one, if all impostor patterns are falsely accepted and zero, if none of the impostor patterns is accepted.

4.1.2. FRR

The fraction of the number of rejected client patterns divided by the total number of client patterns is called False Rejection Rate (FRR). According to the FAR, its value lies in between zero and one.

4.1.3. EER

If the score distributions overlap, the FAR and FRR intersect at a certain point. The value of the FAR and the FRR at this point, which is of course the same for both of them, is called the Equal Error Rate (EER)

This table represents comparison table for false acceptance rate, false rejection rate and genuine acceptance rate for purposed with existing one.

Table 4.1 comparison table for FAR, FRR and GAR

Approach	FAR	FRR	GAR
Previous	2.3	4.5	95.5
LTP + Minutiae + MFCC	0.7	1.3	98.7

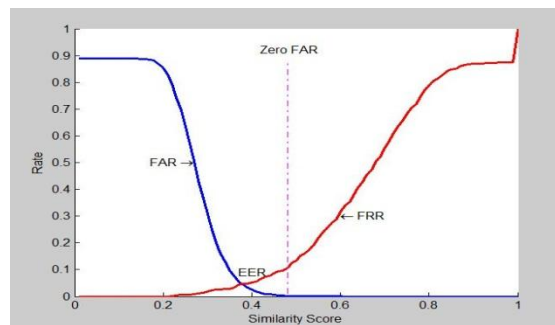


Figure 4.1: FAR, FRR and EER curve

This figure represents FRR and FAR curve at different similarity scores available in the purposed system. EER is the point where these both curves matches is known as equal error rate.

CONCLUSION & FUTURE SCOPE

Biometric system utilize in various system for the identification or authentication approval. Biometric authentication system utilizes various biometric traits for the matching between various biometric traits. Various approaches have been used for the extraction of features from various types of biometric traits. In the proposed work the biometric traits utilize are face and fingerprint. Single Biometric trait system is fail to provide accuracy for the authentication of different identities because due to single bimetric trait the chances of mis-matching increases. So to overcome these disadvantages of single trait biometric system, multimodel biometric system come into existance.

Multimodel biometric system use face and finger images and voice signals for the development of proposed system. feature from each biometric credential has been extracted and fused on the basis of score level fusion to reduce feature dimension. Computation speed increases due to reduction in feature dimension of fused features. This prospsed system provides accuracy of 98.7%. This provides bettere security than other biometric system because illegal availability of all the traits of single person is not available to match and perform any illegal operation. So one can conclude that multimodel biometric system provides better result as compare to single biometric trait system. In future some other techniques are also used. This system can be implemented in real world.

REFRENCES

- [1]. Bhairannawar, S.S. "FPGA Implementation of Fingerprint Recognition System using Adaptive Threshold Technique", IEEE conf. on Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015, pp. 1-5.
- [2]. Herzog, T "JPEG Optimization for Fingerprint Recognition: Generalization Potential of an Evolutionary Approach", IEEE Conf. on Biometrics Special Interest Group (BIOSIG), 2015, pp. 1-6.
- [3]. Sim, T., Baker, S. and Bsat M. "The CMU Pose, Illumination, and Expression Database" IEEE Transactions on Pattern Analysis and Machine Intelligence, 2015, pp 116-124.
- [4]. MattiPietikainen and AbdenourHadid: "Texture Features in Facial Image Analysis", International Journal of Scientific and Research Publications of Machine Vision Group, 2014, pp. 2-7.
- [5]. Deniz O., Castrillon M. and Hernández "Face recognition using independent component analysis and support vector machines" IEEE Conf. onPattern Recognition Letters, 2014, pp 291-302.
- [6]. Rathgeb, C. "On application of bloom filters to iris biometrics" pp. 207 – 218, vol. 4, IEEE, 2014.
- [7]. Caixia Liu "The development trend of evaluating face-recognition technology", IEEE Conf. on Mechatronics and Control (ICMC), 2014, pp. 1540 - 1544
- [8]. PengXinrong "A Survey of Palm-print Feature Extraction Algorithms", IEEEEM Conf. on Palm print feature extraction, 2014, pp. 34-43.
- [9]. Milborrow, S., Morkel, J. and Nicolls, F. (2010) "The MUCT Landmarked Face Database" IEEE conf. on PRASA, 2014, pp. 67-72.
- [10]. Martinez, A. M. and Benavente, R. "The AR Face Database" IEEE Conf. on Face Database, 2014, pp. 12-22.
- [11]. Dong-JuKim, Sang Heon Lee and MyoungKyuSohn (2013) "Face Recognition with Local Directional Patterns", International Journal of Security and Its Applications Vol. 7, No. 2.
- [12]. Lu Zhao "ICA and BP neural network based fingerprint recognition", International Conference on Artificial Intelligence and Software Engineering, 2013, pp. 59-61.