International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Multimodal Biometric Authentication System using Face and Fingerprint Features with Feature Level Fusion

Randeep Kaur[1], Rishmjot Kaur[2]

[1]Research Scholar in Computer Science Department, Baba Farid College of Engineering and Technology, Bathinda

[2]Assistant Professor in Computer Science Department, Baba Farid College of Engineering and Technology, Bathinda

Abstract: ***Multimodal biometric is used for authentication of an individual a secure place. In the process of multimodal authentication different biometric traits have been used for authentication of an individual. The pursuits of knowledge on the diverse biometric system envisage single biometrics feature is not sufficient to provide secure authentication. This dictates the importance of multi-modal system. Most of the multi-modal techniques are lacking in security aspect. In this paper a multimodal recognition system approach has been purposed that has been utilized for recognition of individual based on multiple traits.in this paper LTP and minutia based approach has been used for feature extraction from face and finger images. These features have been fused using feature level fusion. This approach provides better accuracy than previous approaches***

Keywords: Biometric, Multi-modal, Face, Finger, LTP, Minutia and feature level fusion

1. Introduction

1.1 Digital Image

A digital remotely sensed image is typically composed of picture elements (pixels) located at the intersection of each row i and column j in each K bands of imagery. Associated with each pixel is a number known as Digital Number (DN) or Brightness Value (BV), that depicts the average radiance of a relatively small area within a scene (Fig. 1). A smaller number indicates low average radiance from the area and the high number is an indicator of high radiant properties of the area. The size of this area effects the reproduction of details within the scene. As pixel size is reduced more scene detail is presented in digital representation.

1.2biometric Systems

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode. In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not. Identity verification is typically used for positive recognition, where the aim is to pre-vent multiple people from using the same identity.

1.3 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 a dynamic, uncontrolled face identification in a cluttered background. The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available is reasonable, they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination. These systems also have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence. In order for a facial recognition system to work well in practice, it should automatically: 1) detect whether a face is present in the acquired image; 2) locate the face if there is one; and 3) recognize the face from a general viewpoint.

1.4 Fingerprint

Unique mark Identification is the technique for recognizable proof utilizing the impressions made by the moment edge arrangements or examples found on the fingertips. No two persons have precisely the same plan of edge examples, and the examples of any one individual stay unaltered all through life. Fingerprints offer an in fallible method for individual ID. Other individual qualities may change, yet

fingerprints don't. Fingerprints can be recorded on a standard unique mark card or can be recorded digitally and transmitted electronically to the FBI for examination. By contrasting fingerprints at the scene of a wrongdoing with the unique mark record of suspected persons, authorities can build supreme evidence of the vicinity of character of an individual. In 1924 the distinguishing proof division for the Federal Bureau of Investigation (FBI) was secured to give one focal store of fingerprints. At the point when the distinguishing proof division was secured, its motivation was to give a focal store of criminal ID information for law requirement offices all through the Nation. However in 1933 the United States Civil Service Commission (now known as the Office of Personnel Management) turned the fingerprints of more than 140,000 administration representatives and candidates over to the FBI. In this manner a Civil Identification Section was secured, these developments denoted the start for the FBI's Civil File, which was bound to midget the criminal records in size. In 1992 the Identification Division was re-secured as the Criminal Justice Information Services Division (CJIS).

1.4.1 Fingerprint Pattern Type

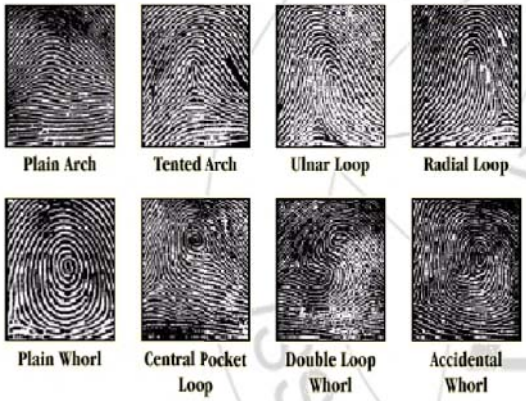

Figure 1.2: Fingerprint samples

1.4.2 Fingerprint acquisition

The most established and most known unique finger impression obtaining procedure is the "ink method", that is, pressing the finger against a card in the wake of spreading the finger skin with ink; this system is these days still to a great extent utilized by the police as a part of AFIS. The cards are changed over into advanced structure by method for scanners indistinguishable to those ordinarily utilized for broadly useful paper records. The default determination is 500 dpi. This procedure can deliver pictures including districts which miss some data, because of intemperate inkiness or to ink lack, and is clearly constrained to measurable applications. The Frustrated Total Internal Reflection (FTIR) is the most utilized and develop live-sweep sensing strategy. The finger is enlightened from one side of a glass crystal with a LED, while the other side transmits the picture through a viewpoint to a CDD/CMOS sensing component which changes over light into computerized data. The absence of reflection brought about by the vicinity of water particles where the edges touch the crystal permits edges to be separated from valleys.

1.4.3 Fingerprint Anatomy

A fingerprint is the representation of the epidermis of a finger. At a macroscopic analysis, a fingerprint is composed of a set of ridge lines which often flow parallel and sometimes produce local macro-singularities called whorl, loop and delta.

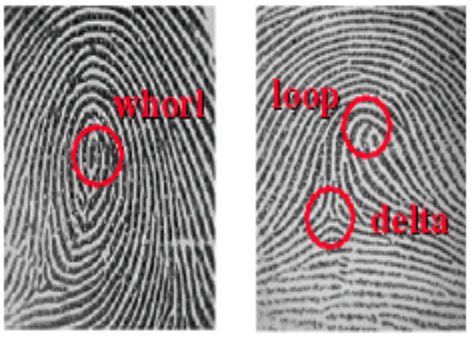

Figure 1.3: Fingerprint Anatomy

The number of cores and deltas in a single fingerprint is regulated in nature by some stringent rules; fingerprints are usually partitioned into five main classes (arch, tented arch, left loop, right loop, whorl) according to their macro-singularities.

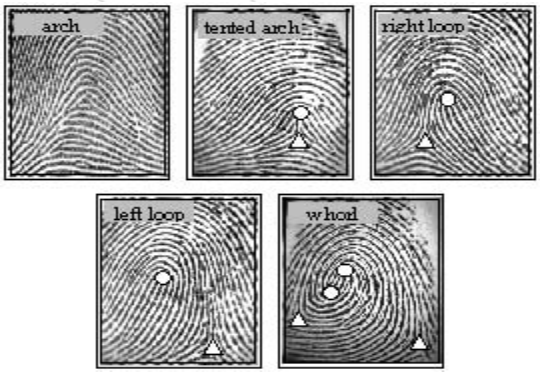

Figure 1.4: Arch, tented arch, left loop, right loop, whorl

2. Review of Literature

O. Deniz, et al [1] "Face recognition using independent component analysis and support vector machines" proposed a combination of two techniques used in the face recognition. SVM and ICA are two approaches that have been used in different facial applications. SVM is a classifier that classifies the different objects into different classes on the basis of different features. This divided the object on the basis of their properties and feature values. SVM classifier is widely used in the object recognition problems. ICA is an approach that is used to extract the features from the facial images. This approach divides the image into different segments and computes the independent components from the facial image. This approach mainly works on the principal of PCA.

Lu Zhao Wenyong Wang et al [2] "ICA and BP neural network based fingerprint recognition" In recent years, the research of fingerprint recognition has become to a research focus of the field of image processing and pattern recognition. In this paper According to the recognition of fuzzy fingerprint and the ones with strong noise, proposed a

new method which combining the ICA (Independent Component Algorithm) and BP (Back Propagation) neural network. First, using the Fast ICA method to extract fingerprint characteristics, then classify and recognize them by a three- layers BP neural network.

Caixia Liu et al [3] "The development trend of evaluating face-recognition technology", provided in a face recognition system, face image acquisition equipment and algorithm processor hardware will also affect speed and effect of the recognition. Therefore, when evaluating face-recognition technology, we should not only carry out the static test of algorithm, but also carry out the dynamic face recognition test of actual faces. At the same time, considering the influence of hardware configuration, hardware configuration parameters of face recognition products or systems should be paid more attention. In the future, the development trend of evaluating face-recognition technology will become both static test in algorithm level and dynamic test of recognition effect to actual faces in application level should be carried out. Even the videotaped face-recognition test and system hardware configuration check should be carried out simultaneously.

Peng Xinrong et al [4]"A Survey of Palm-print Feature Extraction Algorithms", an approach for face recognition using the Local Binary pattern (LBP) and Local Phase Quantization (LPQ). In this paper the information from the image spatial domain and frequency domain has been retrieved. This information is combined which can provides the important information about the image that cannot be given by the individual of these features.

Hui His et al [5] "Application of Fast Independent Component Analysis on Extracting the Information of Remote Sensing Imagery", In this paper LPQ is purposed for the recognition of face from the blur images. LPQ is based on the Fourier Transform phase in local neighbourhoods. The face images are with blur invariant property under different conditions. The face image is subdivided into different sub region. The histograms of LPQ phases has been computed and concatenated for the face descriptor.

3. Proposed Work

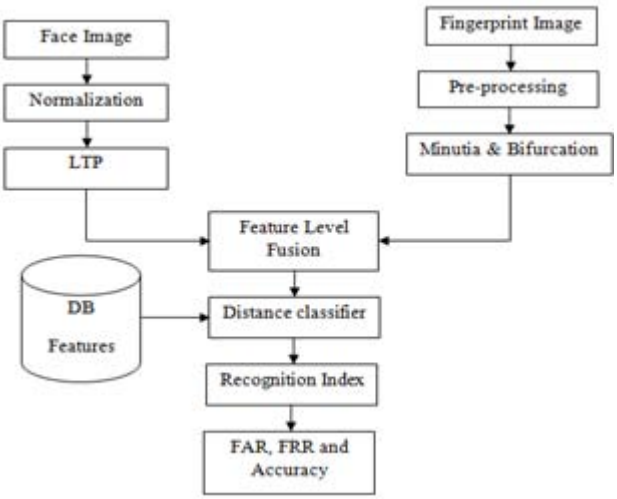

Figure 3.1: Flow of work

Figure 3.1 represents the flow chart for purposed 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 purposed work. By performing these operations that have been explained in the flow chart of purposed work multimodal biometric system can be generated and reformed for authentication of the different users at different platforms. The various steps of purposed model have been explained below for illustration. These steps have been used for computation of different features from the dataset and compute performance evaluation parameters from purposed system.

4. Results

Multimodal biometric has been used for authentication purpose in security systems. In the purposed system face and fingerprint has been used as multimodal biometric system that contains different images of face and fingerprint samples for recognition process. In the purposed work face dataset has been used as ORL dataset that contains 6 different samples of 10 individual and FVC 2004 finger dataset has been used for fingerprint dataset of 10 individuals. These datasets images have been used for development of multimodal system.

Figure 5.1: Fingerprint dataset samples

This figure represents different fingerprint samples of the FVC dataset that have been used for development of multimodal biometric system. This figure represents 10 different individual samples available in the dataset for feature extraction.

Figure 5.2: Face Dataset images

This figure represents face dataset images of 10 different individuals used in the purposed for multimodal biometric

system. These images have been used for extraction of texture features and fused with fingerprint features for recognition process.

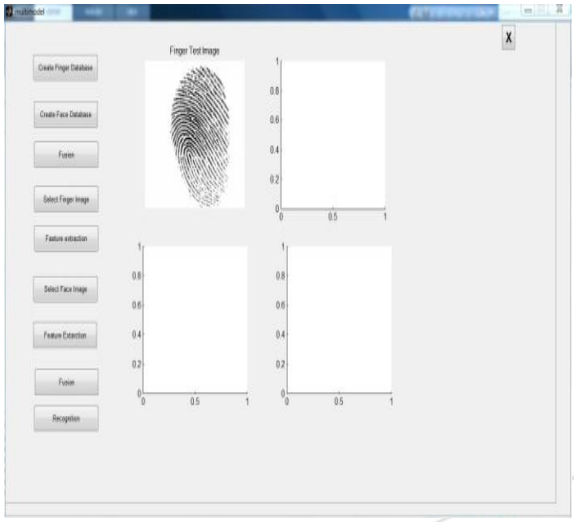

Figure 5.3: Fingerprints Test image loaded to system

This figure represents testing fingerprint image has been loaded to the system using image accusation process. After this process image information has been extraction from that image that contain information about height, width, color information. This information has been used for pre-processing and feature extraction of fingerprint image.

In the pre-processing of the image sample image has been undergoes different normalization process so that minutiae can be easily extracted front eh image. In the process of pre-processing image has been binary converted and thinned so that rigid ending, rigid bifurcation and dots can be extracted from the image.

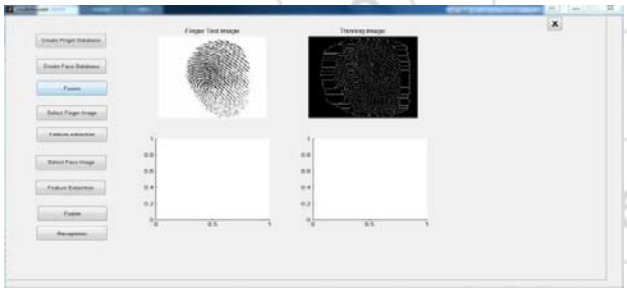

Figure 5.4: Thinning of binary image

This figure representsfingerprint image has been converted into binary format so that bi-level color can be converted on the basis of neighbor pixel values. These pixels have been converted into black and white pixels that contain only two bits of color information in whole image that are 0 and 1. After binary conversion thinning of binary image so that rigid endings, bifurcation and dots can be easily extraction from the image. Thing process removes the unnecessary information from the image so that easily values can be used for extraction of best points available in the image. After process of thing minutiae points have been detected on the image. These points location has been computed and stored as a feature template that has been used for matching process.

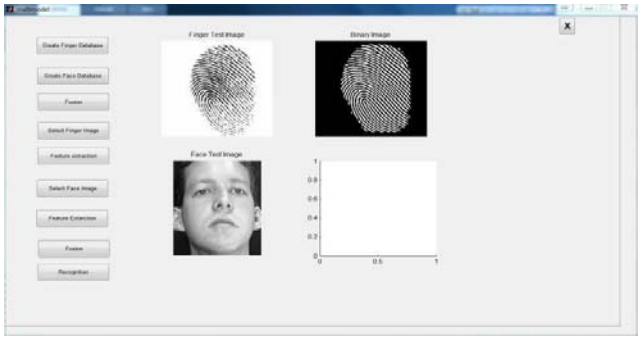

Figure 5.5: Face image capturing for purposed model

This figure represents face image has been loaded to the system. Face image has been used for extraction of texture features using LTP 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.

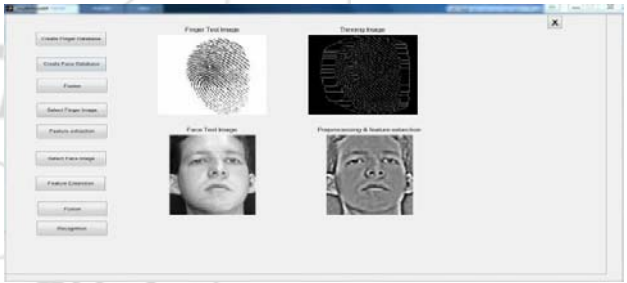

Figure 5.6: LTP based features extraction from face image

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.

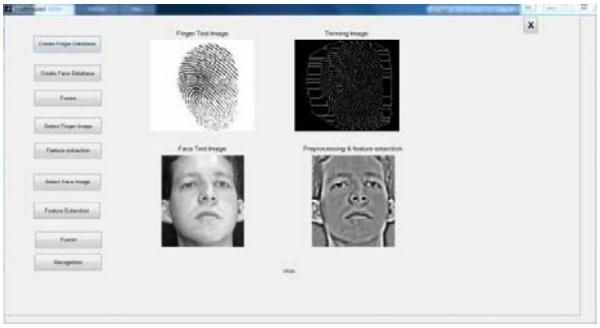

Figure 5.7: Feature Fusion and recognition

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.

- **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.

FAR: False acceptance rate has been measured for a system that false accepts an imposter 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.

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.

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)

Table 5.1: Comparison table for FAR, FRR and GAR

Approach	FAR	FRR	GAR
Previous	2.3	4.5	96.5
LTP + Minutiae	0.7	1.3	98.7

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

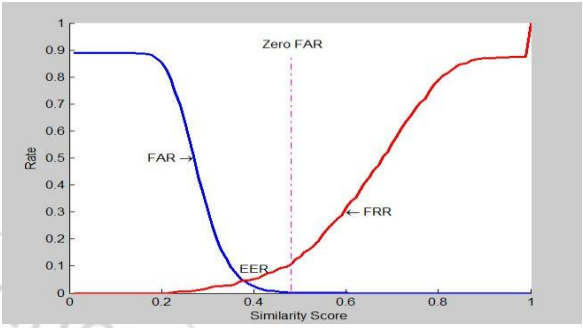

Figure 5.8: FAR, FRR and EER curve

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.

5. Conclusion

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 authenitication of different identies 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 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. Computatiom speed increasses due to reduction in feature dimension of fused features. This propsed 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.

References

[1] 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.
[2] Lu Zhao "ICA and BP neural network based fingerprint recognition", *International Conference on Artificial Intelligence and Software Engineering*, 2013, pp 59-61.
[3] Caixia Liu "The development trend of evaluating face-recognition technology", *IEEE Conf. on Mechatronics and Control (ICMC),* 2014, pp 1540 - 1544
[4] Peng Xinrong **"**A Survey of Palm-print Feature Extraction Algorithms", *IEEEM Conf. on Palm print feature extraction*, 2014, pp 34-43.
[5] Hui His "Application of Fast Independent Component Analysis on Extracting the Information of Remote Sensing Imagery", *IEEE Conf. on Machine Learning and Cybernetics*, 2006, pp 1066 – 1071.
[6] Jing Luo "Application of Dimensionality Reduction Analysis to Fingerprint Recognition", *IEEE Conf. onComputational Intelligence and Design*, 2008, pp 102 – 105.
[7] 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.
[8] 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.
[9] Fernandez-Saavedra, B., Liu-Jimenez, J.; Sanchez-Avila, C., "Quality Measurements for Iris Images in Biometrics*". The International Conference on &#34, 2007,* pp. 759 – 764.
[10] Rathgeb, C. "On application of bloom filters to iris biometrics" pp. 207 – 218, vol. 4, IEEE, 2014.
[11] Kanade, S.,Camara, D.; Krichen, E.; Petrovska Delacrétaz, D. "Three factor scheme for biometric-based cryptographic key regeneration using iris" *Biometrics Symposium, 2008,* pp. 59 – 64.
[12] Cardoso, L, Barbosa, A., Silva, F.,Pinheiro, A.M.G. "Iris Biometrics: Synthesis of Degraded Ocular Images" *IEEE Transactions on Information Forensics and Security, 2012,Volume* 8,pp. 1115 – 1125.