Secure Reliable Multimodel Biometric Face Recognition and Text Message

[1]Kashif Majed, [2]Prof. Himanshu Nautiyal

M. Tech. Scholar, Department of Electronics and Communication, SIRT, Bhopal[1]

Assistant Professor, Department of Electronics and Communication, SIRT, Bhopal[2]

Abstract— **A biometric system which relies only on a single biometric identifier in making a personal identification is often not able to meet the desired performance requirements. Identification based on multiple biometric represents an emerging trend. We introduction is multimodal biometric system, which integrates fingerprint and text message authentication in making a personal identification. This system takes advantage of the capabilities of each individual biometrics. It can be used to overcome some of the limitation of a single biometrics. Preliminary experimental results demonstrate that the identity established by such an integrated system is more reliable than the identity established by a face recognition system and text message verification system.**

Keywords—**Fingerprint recognition, text message authentication, Multimodal system.**

I. Introduction

In the present era of e-commerce more and more services are being offered over the electronic devices and internet. These include banking, credit card facility, e-shopping, etc. To ensure proper use of these facilities only by the authorized or genuine users and avoid any misuse by the unauthorized or imposter users, some person authentication scheme is embedded into these services. Currently, person authentication is done mostly using one or more of the following means: text passwords, personal identification numbers, barcodes and identity cards. The merit of these schemes is that they do not change their value with respect to time and also unaffected by the environment in which they are used. The main demerit of them is that they can be easily misused or forgotten. Also, with time more and more services are being offered over the electronic devices and internet. Hence it becomes unmanageable to keep track of the authentication secrets for different services. The alternative that provides relief from all these demerits is the use of biometric features for person authentication. Any physiological and/or behavioral characteristics of human can be used as biometric feature provided it possesses the following properties: universality, distinctiveness, permanence, collectability, circumvention, acceptability and performance [1]. Some of the commonly used biometric features include speech, face, signature, finger print, handwriting, iris, DNA, Gait, etc. In practice, no single biometric can satisfy all the desirable characteristics mentioned above for it to be used for person authentication. This is due to the problems associated with noisy data, intra-class variation, non-universality, spoof attacks and high error rates [2]. To overcome this limitation, multiple biometric features can be used for person authentication. This resulted in the development of multimodal biometric person authentication system [2]. Thus biometric system can be classified as unimodal system and multimodal system based on whether single or multiple biometric features are used for person authentication. Biometric security system becomes a powerful tool compared to electronics based security systems [3]. Biometrics is fast becoming applicable in various walks of life. Basically, it deals with the use of computer technology and signal processing to identify people based on their unique physical and behavioral characteristics such as fingerprints, voice scans, retinal patterns, facial characters and human DNA mapping. Typically, a biometric system comprises a sensor, interface and a signal processor with driver software. The various different biometric procedures fall into two categories: Static process relating to the identification of fingerprints, hand geometry, Iris or retina and face, and Dynamic processes relating to the recognition of handwriting, keyboard typing patterns, voice, lip movement and behavior analysis [4].

A biometric sensor works on the inputs provided by any of the human characteristics and applies an algorithm on the scanned biometric data. This is then compared with, and matched to, a template that has already been created earlier and approved by the user. The most specific and reliable biometric data is obtained from the DNA sequencing of any subject. The matching and comparing process creates a „score‟ based on how closely the sampled biometric matches with the template already obtained. A match score is known as genuine score if it is a result of matching two samples of a biometric trait of the same user. It is known as an imposter score if it is the result of matching two samples of a biometric trait originating from different users [5]. An imposter score that exceeds the predefined threshold results in a false accept, while a genuine score that falls below the predefined threshold results in a false reject. The False Accept Rate (FAR) of a biometric system is the fraction of imposter scores exceeding the threshold. Similarly, the False Reject Rate (FRR) of a system is defined as the fraction of genuine scores falling below the threshold. Regulating the value of threshold changes the FRR and the FAR values, but for a given biometric system, it is not possible to decrease both these errors simultaneously. In real-world biometric system, biometric measure is referred in terms of FAR and FRR. The FAR measures the percentage of invalid users who are incorrectly accepted of genuine users and the FRR measures the percentage of valid users rejected as imposters. The Equal Error Rate (EER) refers to the point where the FAR equals the FRR. Lower the value of EER, the more accurate the biometric system [6].

II. Minutiae Extraction

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. An iterative, parallel thinning algorithm is used. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3) and finally removes all those marked pixels after several scans. The thinned ridge map is then filtered by other Morphological operations to remove some H breaks, isolated points and spikes. In this step, any single points, whether they are single-point ridges or single-point breaks in a ridge are eliminated and considered processing noise.

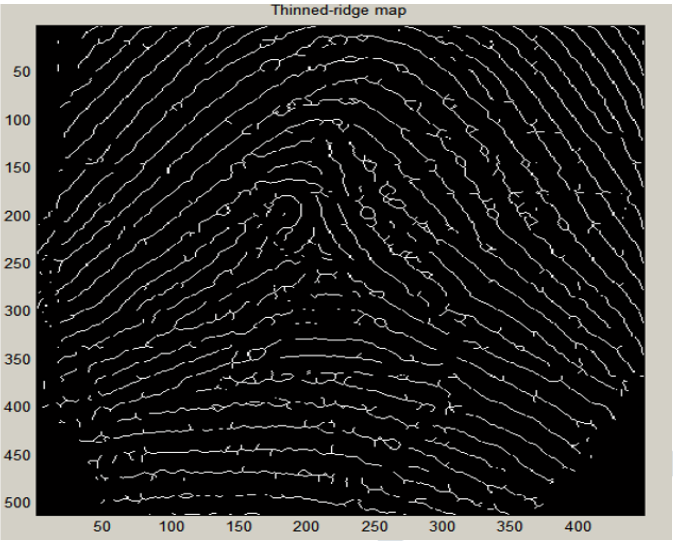


Figure 1: Thinned image

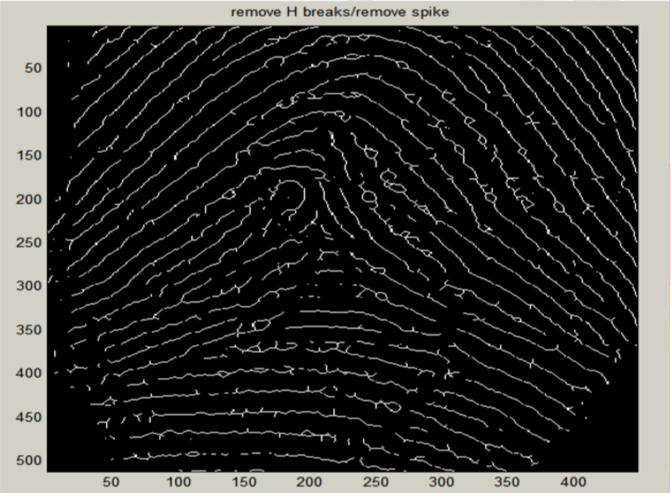


Figure 2: image after removing H-breaks and spikes

An alignment-based match algorithm is used in my project. It includes two consecutive stages: one is alignment stage and the second is match stage.

1. Alignment stage: Given two fingerprint images to be matched, choose any one minutia from each image; calculate the similarity of the two ridges associated with the two referenced minutia points. If the similarity is larger than a threshold, transform each set of minutia to a new coordination system whose origin is at the reference point and whose x axis is coincident with the direction of the referenced point.

2. Match stage: After we get two set of transformed minutia points, we use the elastic match algorithm to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical.

III. APPROACH FOR FACIAL EXPRESSION RECOGNITION

An FER (facial expression recognition) system has three components, namely Face-detection, Features extraction from face and Classification. Flow chart for proposed system is shown in the figure given below.

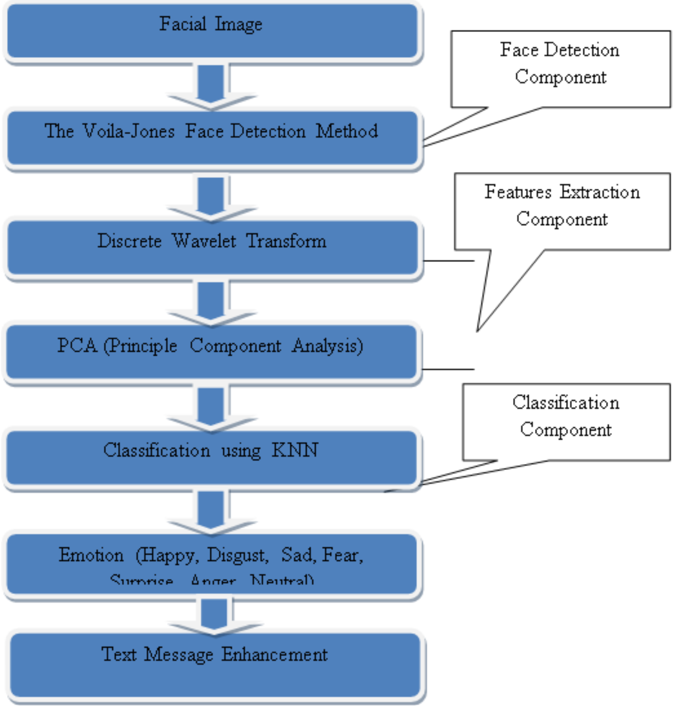

Facial Image
Face Detection Component
The Voila-Jones Face Detection Method
Discrete Wavelet Transform
Features Extraction Component
PCA (Principle Component Analysis)
Classification using KNN
Classification Component
Emotion (Happy, Disgust, Sad, Fear, Surprise, Anger, Neutral)
Text Message Enhancement

Figure 3: Proposed Biometric Face and Text Message

Face Detection: - This is the first and fundamental step of proposed facial expression recognition system. In this step, locate (identify) the face Viola region of the subject. For this purpose, Voila-Jones face detection method was used. -Jones method has successfully used for real time object identification in many computer visions and pattern recognition tasks. Drawback of this method is slow training, but advantages are very fast and accurate method for face detection [4]. Key feature of Voila-Jones face detection method is low false positive rate that is why we use this method in our proposed approach. Three major parts which contributes to Voila-Jones face detection [7]. First is “integral image” representation which allows features (used for detector) computation very fast. The second one is for selecting tiny set of features from very large set of features. For this very easy, accurate and precise classifier which is based on Ad boost learning algorithm is used. And third one is procedure for cascade combination of classifier, which spends more computation to assuring face like region while background region of the image discarded very fast. In the [8] authors revealed that this method has high detection rate so we use this in our system. In the figure below, shows the output of face detection on one image of JAFFE database.

Text Message:-

LSB Technique

Cover-Image: An image in which the secret information is going to be hidden. The term "cover" is used to describe the original, innocent message, data, audio, still, video etc. The cover image is sometimes called as the "host".

Stego-Image: The medium in which the information is hidden. The "stego" data is the data containing both the cover image and the "embedded" information. Logically, the processing of hiding the secret information in the cover image is known as embedding.

Payload: The information which is to be concealed. The information to be hidden in the cover data is known as the "embedded" data.

This technique works best when the file is longer than the message file and if image is grayscale.

When applying LSB technique to each byte of a 24 bit image, three bits can be encoded into each pixel.

If the LSB of the pixel value of cover image C(i, j) is equal to the message bit SM of secret message to be embedded C(i, j) remain unchanged; if not, set the LSB of C(i, j) to SM.

Message embedding procedure is given below:

S(i, j) = C(i, j)-1, if LSB (C(i, j)) = 1 and SM = 0
S(i, j) = C(i, j)+1, if LSB (C(i, j)) = 0 and SM = 1
S(i, j) = C(i, j), if LSB (C(i, j)) = SM

Where LSB (C(i, j)) stand for LSB of cover image C(i, j) and "SM" id the next message bit to be embedded. S(i, j) is the Stego image.

LSB technique is implemented in spatial domain. The technique converts image into shaded Gray Scale image. This image will be act as reference image to hide the text. Using this grey scale reference image any text can be hidden. Single character of a text can be represented by 8-bit. If the reference image and the data file are transmitted through network separately, we can achieve the effect of Steganography. Here the image is not at all distorted because said image is only used for referencing. Any huge amount of text material can be hidden using a very small image. Decipher the text is not possible intercepting the image or data file separately. So, it is more secure. In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. Here we have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to stegano-analysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains - for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today. From one of our reference paper we found that in LSB steganography, to conceal the message the least significant bits of the cover media's digital data are used. The useful feature of the LSB steganography techniques is LSB replacement that makes LSB stegnography as simple. To reflect the message it needs to be hidden, LSB replacement steganography flips the last bit of each of the data values.

Consider an 8-bit gray scale bitmap image where each pixel is stored as a byte. And it also representing in a gray scale value. Suppose the first eight pixels of the original image have the following gray scale values:

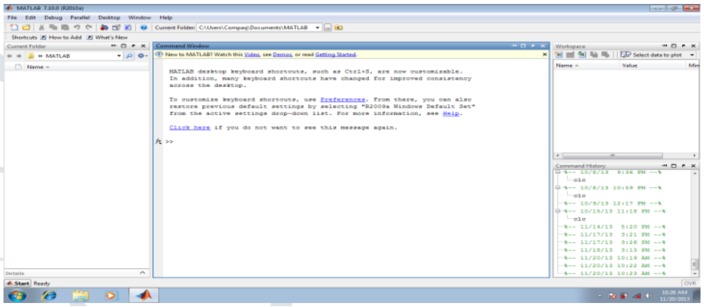
11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

The letter C whose binary value is 1000001. To hide this binary value it can replace the LSBs of these pixels to have the following new gray scale values:

11010011
01001010
10010110

IV. Simulation Tools

In the below figure we show the starting screen of MATLAB. We use MATLAB because it is user friendly and it contains a number of libraries which is used in the work.



```
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

MATLAB desktop keyboard shortcuts, such as Ctrl+S, are now customizable.
In addition, many keyboard shortcuts have changed for improved consistency
across the desktop.

To customize keyboard shortcuts, use Preferences. From there, you can also
restore previous default settings by selecting "R2009a Windows Default Set"
from the active settings drop-down list. For more information, see Help.

Click here if you do not want to see this message again.

fx >>
```

Figure 4: MATLAB Starting Window

testing and training module.

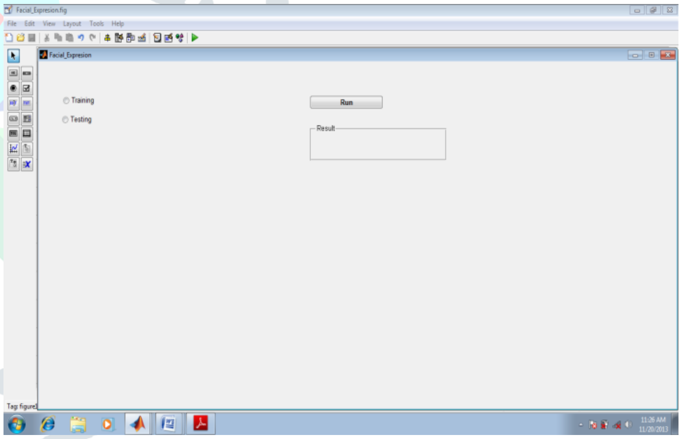


Figure 5: GUI of the Application

V. Simulation

In this section we expose and discuss the results of FER system which is based on proposed methodology for FER. We perform two experiments on proposed FER system with different number of training and testing images of JAFFE dataset. In first experiment out of 213 images, 143 images (on average of 2 images per expression per subject) for training purpose and rest 70 images (on average of 1 image per expression per subject) for testing purpose. Result of this experiment for 7 expressions is shown in the table below:

Table I: Result of Experiment FER System

	Anger	Disgust	Fear	Happy	Neutral	Sad
Anger	10	0	0	0	0	0
Disgust	0	10	0	0	0	0
Fear	0	0	8	0	1	1
Happy	0	0	0	8	1	1
Neutral	0	0	0	0	10	0
Sad	0	0	0	0	0	10
Surprise	0	0	0	0	0	0

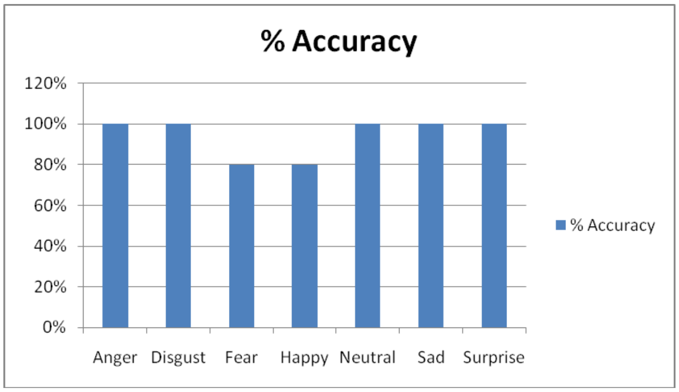


Figure 6: Accuracy of each expression for experiment

VI. Conclusion

This paper provides an overview of multiple features based biometric systems, including both physiological characteristics and behavioral characteristics. In this proposed system a multimodal approach is put forward using fingerprint and face recognition traits. Here, SIFT features are analyzed best for fingerprint & VPP/HPP features are suggested for face recognition. Then extracted feature vectors are fused using sum rule at feature level. By combining multiple biometrics these increase population coverage, improve matching performance, deter spoofing, and facilitate indexing. Multimodal system brings systematically a clear improvement of the results in comparison to either modality used alone.

REFRENCES

[1] Shweta Gaur, V.A.Shah, Manish Thakker, “Biometric Recognition Techniques: A Review”, IJARE, Vol. 1, Issue 4, October 2012.

[2] Gaganpreet Kaur, Dheerendra Singh, Sukhpreet Kaur, “Pollination Based Optimization for Feature Reduction at Feature Level Speech & Signature Biometrics”, ICRITO, AIIT, Amity University Uttar Pradesh, Noida, India, 8-10-2014.

[3] FahadAL-Harby, RamiQahwaji, Mumtaz Kamala, “Secure Biometrics Authentication: A brief review of the Literature”, School of Informatics, University of Bradford BD7 1DP, UK.

[4] ArunRossand Anil K. Jain, “Multimodal Biometrics: an Overview”, EUSIPCO, September 2004.

[5] Adesesan B. Adeyemo, Adeyinka O. Abiodun, “Adaptive SIFT/SURF Algorithm for Off-line signature Recognition”, ECS,Vol. 39 No. 1 January.

[6] A. JameerBasha, V. Palanisamy, T. Purusothaman, “Efficient Multimodal Biometric Authentication Using Fast Fingerprint Verification and Enhanced Iris Features”, JCS, 2011.

[7] Prof. M.N. Eshwarappa, Prof. (Dr.) Mrityunjaya V. Latte, “Bimodal Biometric Person Authentication System Using Speech and Signature Features”, IJBB, Volume (4): Issue (4).

[8] Dapinder Kaur, Gaganpreet Kaur, Dheerendra Singh, “ Efficient and Robust Multimodal Biometric System for Feature Level Fusion (Speech and Signature)”, IJCA (0975 – 8887) Volume 75– No.5, August 2013.

[9] Maridalia Guerrero Peña, “A Comparative Study of Three Image Matching Algorithms: SIFT, SURF, and FAST”, Utah State University Logan, Utah 2011.

[10] C. Shan, S. Gong, and P.W. McOwan, “Facial expression recognition based on local binary patterns: A comprehensive study,” Image and Vision Computing, vol. 27(4), pp. 803–816, 2008.

[11] Y. Tian, T. Kanade, and J. Cohn, Handbook of Face Recognition, chapter 11, Springer, 2005.

[12] M.S. Bartlett, G. Littlewort, M. Frank, C. Lainscsek, I. Fasel, and J. Movellan, “Recognizing facial expression: Machine learning and application to spotaneous behavior,” in IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2005, vol. 2, pp. 568–573.

[13] M.J. Lyons, J. Budynek, and S. Akamatsu, “Automatic classification of single facial images,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 21(12), pp. 1357–1362, 1999.

[14] T. Mandal, A. Majumdar, and Q.M.J. Wu, “Face recognition by curvelet based feature extraction,” in International Conference on Image Analysis and Recognition, LNCS, 2007, vol. 4633, pp. 806–817.