ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE
Your uh-MATE Research Paper !!!

International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. II, Issue IV, April 2016.

Biometric Recognition of Face and Signature by Using Image Quality Assessment Techniques

J.Agnel (P.G Scholar)
Department of Computer Science and Engineering
V.V College of Engineering.

Dr. S. Raja Ratna M.Tech., Ph.D.,
Department of Computer Science and Engineering
V.V College of Engineering.

Abstract— **Establishing identity of humans is becoming critical in our vastly interconnected society. Human can be recognized in two ways either by physical or by behavioral. One of the ways to do this is by comparing selected features from the image and a database. By comparing a single feature like only face can lead us to real legitimate trait to a fake sample. In order to overcome this, we are grouping more than one feature from a person like physical and behavioral features. In physical method, the humans face structure is take for recognition. The face of a human contains much information to be unique information. To extract the features from the face, the Local Derivative Pattern is used. By this, we can get the features from the second order derivative, which gives a deep down features for each person. And in the behavioral method, the signature of the person is taken. Since, the signature is one of the most important behaviors of a person; it should be extracted in an accurate manner. For feature extraction, the image quality assessment technique is used, which uses much quality assessment to measure the fake and to recognize the real person. By extracting and combining the features from the two methods, the classification of the human is more accurate. By adding more than one feature makes the system crack proof. The proposed system enhances the security of biometric recognition frameworks.**

Keywords—*Local Derivative Pattern, Image Quality Assessment, Biometric Recognition*

I.INTRODUCTION

Biometrics refers to metrics that related to human characteristics. Biometrics authentication is used as a form of identification and access control. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information. And as measurable for Physical and Behavioral characteristic that can be used for automated recognition. Performance relates to the accuracy, speed, and robustness of technology used and acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. Face recognition is a process of automatically identifying or verifying a person from a digital image or a video frame from a video source. An image of the face is captured and analyzed in order to derive a template. This analysis may take various forms from plotting geometric points to Grey-scale analysis of pixels to determine boundaries. Face recognition was introduced in the 1960s. Some recognition algorithms identify faces by extracting landmarks, or features from an image of the face. For example, an algorithm may analyze the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Signature recognition the analysis of signature is also a bio-metrical authentication solution and it was introduced in the year of 1965s. The device is a tactile screen. The user performs a signature with a “pen” on this tactile screen. The parameters that are computed for the authentication are the shape of the signature, the time taken to do it, the stroke order and the pen pressure. With the computation of these parameters, the system provides to you a unique authentication method. It is virtually impossible to reproduce in the same way somebody signature. It can be operated in two different ways: Static:In this mode, users write their signature on paper, digitize it through an optical scanner or a camera, and the biometric system recognizes the signatureanalyzing its shape. This group is also known as “off-line”. Dynamic:In this mode, users write their signature in a digitizing tablet, which acquires the signature in real time. Another possibility is the acquisition by means of stylus-operated PDA. Some systems also operate on smart-phones or tablets with a capacitive screen, where users can sign using a finger or an appropriate pen. Dynamic recognition is also known as “on-line”.

II. LITERATURE SURVEY

Aarti Sharma et al., (2014) had described that to learn and detect the structure facial textures that characterize the real faces but not the fake ones. And the biometrics offer in two ways and one is Non Repudiation in which an individual who access a certain facility can't deny later using it [1]. Arathi .M et al., (2014) finding the signature is genuine or forgery and in this work the sign image is converted into time series data with linear scanning method for distinguish the signature is genuine or forged one and in the method uses Mahalanobis distance measure and the automatic signature verification system is able to verify the signature identity of an person individually to find the signature is genuine or forgery. Offline has the advantage of existing manual recognition method [2]. Anjos .A et al., (2011) has screened three basic methods for face recognition systems for easy spoofing systems and here anti-spoofing for 2D face recognition system and the database for the face recognition is PRINT-ATTACK database which contains 200 videos of real accesses and 200 videos of spoof attempts using printed photographs of 50 different identities [3]. Harpreet Anand et al., (2014) present that the offline signature verification and which is projected using neural network. Here signature is written on a paper and obtained by a scanner or a camera which is captured and presented in an image format. By using Neural Network the main attractions are the first one is Expressiveness which is well-suited for continuous inputs and outputs, and the second one is Ability to generalize which will copy the diversity and variations of the handwritten signatures. And the Graceful Degradation which is sharp drop-off for performance. Finally the last one is the Execution Speed and it would take large amount of time for the execution of training phase [4]

III. METHODOLOGY

The focus of this paper is to find the person that he/she is real or fake and the methods are presented below:

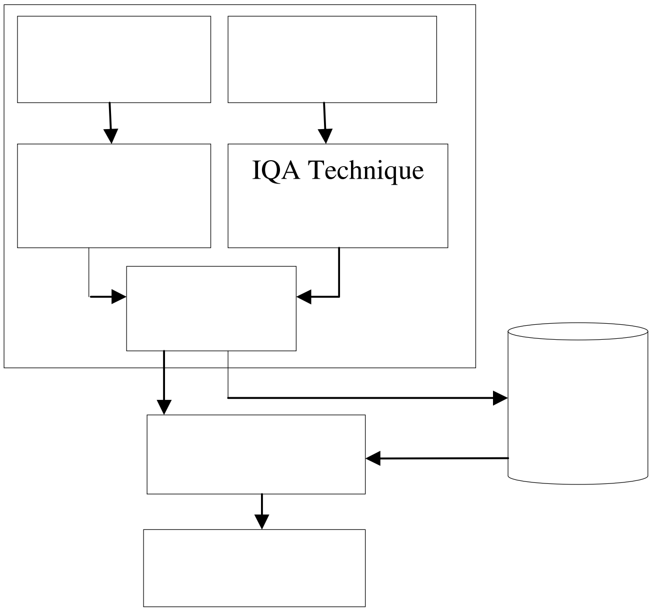


Fig 3.1 System Architecture

3.1. Face Acquisition:

In this work, the input images are obtained from the JAFFE (Japanese Female Facial Expression Database) which consists of 213 images (Face) and the size of each image is 640 x 480 pixels with, 256 Grey levels per image and with 7 facial expressions (6 basic facial expressions + 1 neutral). The data could be set for the performance of classify and to perform for this method for finding the person is real or fake by different expressions, and so on.

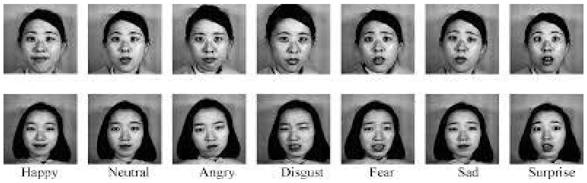
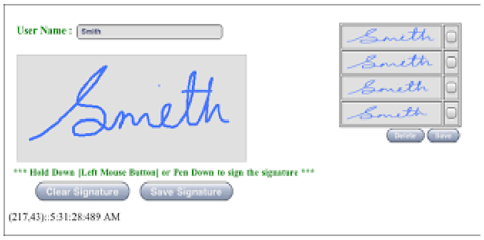


Fig 3.2 JAFFE Database

3.2. Signature Acquisition:

By, performing with input image of signature is obtained from GPDS 100hand 3Band databaseof 3acquistions from100people which has taken the users of right hand and the resolution will be 640x480 pixels. And the signatures are in jpg format.



User Name : Smith

*** Hold Down [Left Mouse Button] or Pen Down to sign the signature ***

(217,43)::5:31:28:489 AM

Fig 3.3 Signature verification

3.3. Feature Extraction using LDP:

First, we need to extract the feature by LDP using the degree values such as 0°, 45°, 90°, and 135° respectively. And the equations for these degrees given below,

$$I'_{0^\circ}(Z_0) = I(Z_0) - I(Z_4) \qquad (1)$$

$$I'_{45^\circ}(Z_0) = I(Z_0) - I(Z_3) \qquad (2)$$

$$I'_{90^\circ}(Z_0) = I(Z_0) - I(Z_2 \qquad (3)$$

$$I'_{135^\circ}(Z_0) = I(Z_0) - I(Z_4) \qquad (4)$$

Using these functions the extraction features of Face and Signature is extracted using the LDP values. And the LDP has the basic function with the LBP whereas it took the surrounding values in 5x5 matrixes it will take only 3x3 matrix for verification and it would keep the values as binary of 0s and 1s. And the LDP will take 5x5 matrix as itself and it not consider the other matrix inside it and it will take a group of three values and compare values with other values where the larger values will be become 1's and the smaller values will be as 0's. Here the node value will be denoted as Z0. For a 3 point template assigns a "0" to a monotonically increasing or decreasing pattern and "1" is assigned to turning point. Similarly for a 4 point template a gradient turning pattern is labeled as "1" and monotonically increasing or decreasing pattern is labeled as "0".

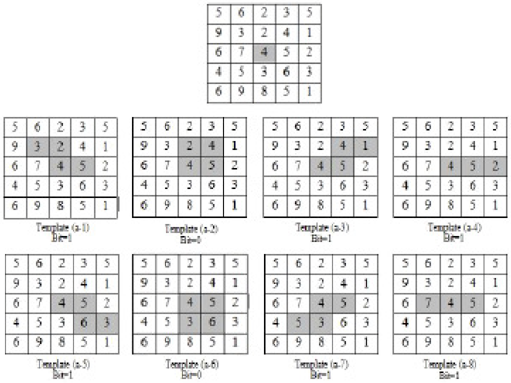


Fig 3.4 3 Point and 4 Point LDP Template

3.4. IQA (Image Quality Assessment) Techniques:

Using a wide range of IQMs exploiting complementary image quality properties should permit to detect the aforementioned quality differences between real and fake samples expected to be found in many attack attempts.

3.4.1. Full Reference IQ Measure:

(i). Mean Square Error:

The mean square error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. For an unbiased estimator, the MSE is the variance of the estimator. Like the variance, MSE has the same units of measurement as the square of the quantity being estimated. In an analogy to standard deviation, taking the square root of MSE yields the root-mean-square error or root-mean-square deviation (RMSE or RMSD). The RMSE is the square root of the variance, known as the standard deviation.

(ii).Peak Signal to Noise Ratio:

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. Although a higherPSNR generally indicates that the reconstruction is of higher quality, in some cases it may not.

(iii).Signal to Noise Ratio:

Signal-to-noise ratio (often abbreviated SNR or S/N) and it is defined as the ratio of signal power to the noise power, often expressed in decibels. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise. The signal-to-noise ratio, the bandwidth, and the channel capacity of a communication channel are connected by the Shannon–Hartley theorem.

(iv). Structure Content:

The ratio between the square of sum of original image to the square of sum of reference image is often defined by structural content.

(v). Maximum Difference:

The maximum value of absolute difference image from original image which is subtracted to the reference image.

(vi). Average Difference:

The average value per pixel of absolute difference image that means the original image is subtracted to the reference image for the average value.

(vii). Normalized Absolute Error:

The ratio between sums of absolute of difference image to the sum of absolute of original image.

(viii). R-Average Mean Difference:

The sum of maximum of R numbers value is summed and divided by R to calculate average maximum difference. In the RAMD formula, max r is defined as the r -highest pixel difference between two images. For the present implementation, $R = 10$.

(ix). Laplacian Mean Square Error:

Based on this h(image) = Ii+1, j +Ii−1, j +Ii, j+1 + Ii, j−1 − 4Ii, j equation .the h(Ii, j) and h(I^i, j) will be calculated .the ratio between the square ofdifference of these two values to the sum oforiginal image h(Ii, j) value.

(x). Normalized Cross-Correlation:

For image-processing applications in which the brightness of the image and template can vary due to lighting and exposure conditions, the images can be first normalized.

(xi). Mean Angle Similarity:

The mean angle similarity is the measure of similarity of mean angle between the original image and reference image.

(xii). Mean Angle Magnitude Similarity:

The mean angle magnitude similarity is the measure of similarity of mean angle's magnitude between the original image and reference image.

(xiii). Total Edge Difference:

The ratio between the differences of total number of edges between the two images to the total number of pixels.

(xiv). Total Corner Difference:

The ratio between the differences of total number of corners between the two images to the total number of pixels.

(xv). Spectral Magnitude Error:

The difference between the Fourier transform of original image to the Fourier transform of reference image is averaged by total number of pixel.

(xvi). Spectral Phase Error:

The difference between the angles of Fourier transformed original image to the angle of Fourier transformed reference image is averaged by total number of pixel.

(xvii). Gradient Magnitude Error:

The difference between the gradient of original image to the gradient of reference image is averaged by total number of pixel.

(xviii). Gradient Phase Error:

The difference between the angles of gradient of original image to the angle of gradient of reference image is averaged by total number of pixel.

(xix). Structural Similarity Index Measurement:

The Structural Similarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index can be viewed as a quality measure of one of the images being compared and provided the other image is regarded as of perfect quality. It is an improved version of the universal image quality index proposed before.

(xx). Visual Information Fidelity:

The Visual Information Fidelity (VIF) metric is based on the assumption that images of the human visual environment are all natural scenes and thus they have the same kind of statistical properties.

(xxi). Reduces Reference Entropy Difference:

On the other hand, the RRED metric approaches the problem of QA from the perspective of measuring the amount of local information difference between the reference image and the projection of the distorted image onto the space of natural images, for a given sub band of the wavelet domain.

3.4.2. No Reference IQ Measures:

(xxii). JPEG Quality Index:

The JPEG Quality Index (**JQI**), which evaluates the quality in images affected by the usual block artifacts found in many compression algorithms running at low bit rates such as the JPEG.

(xxiii). High Low Frequency Index:

The High-Low Frequency Index (HLFI), which is formally, defined in Table I. It was inspired by previous work which considered local gradients as a blind metric to detect blur and noise [41]. Similarly, the HLFI feature is sensitive to the sharpness of the image by computing the difference between the power in the lower and upper frequencies of the Fourier Spectrum.

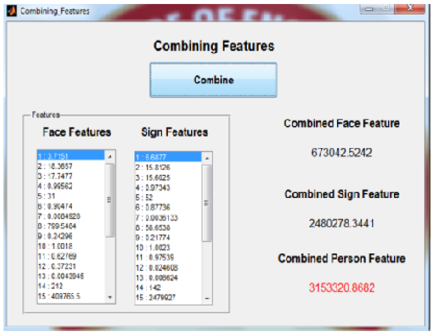
(xxiv). Blind Image Quality Index Measurement:

These blind IQA techniques use a priori knowledge taken from natural scene distortion-free images to train the initial model (i.e., no distorted images are used).

(xxv). Naturalness Image Quality Evaluator:

The NIQE is a completely blind image quality analyzer based on the construction of a quality aware collection of statistical features (derived from a corpus of natural undistorted images) related to a multi variate Gaussian natural scene statistical model.

3.5. Combining Features:



Features

Face Features

```
1 : 3.7151
2 : 18.3657
3 : 17.7477
4 : 0.96563
5 : 31
6 : 0.90474
7 : 0.0084828
8 : 799.5404
9 : 0.24296
10 : 1.0018
11 : 0.62769
12 : 0.37231
13 : 0.0043946
14 : 212
15 : 409765.5
```

Sign Features

```
1 : 6.6877
2 : 15.8126
3 : 15.6025
4 : 0.97343
5 : 52
6 : 0.87736
7 : 0.0036133
8 : 58.6536
9 : 0.21774
10 : 1.0023
11 : 0.97539
12 : 0.024608
13 : 0.008624
14 : 142
15 : 2479027
```

Combined Face Feature

673042.5242

Combined Sign Feature

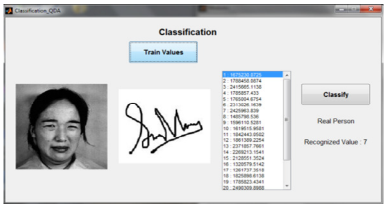
2480278.3441

Combined Person Feature

3153320.8682

In Combining Features, using 25 Reference and No Reference values the Face Feature values and Signature Feature values are given separately and the values for the Combined Face Feature value is shown by adding the whole values in face feature and for Combined Signature Feature value is shown by adding the whole values of Signature Feature. And the combined value of a person's feature is given to find that the is fake or not.

3.6. Classification by QDA:



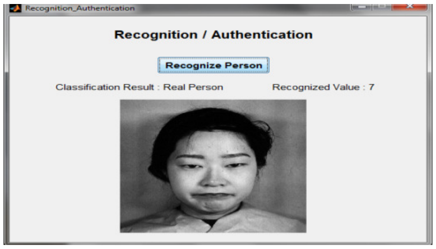
1 : 1675230.0725
2 : 1788458.0874
3 : 2415665.1138
4 : 1785857.433
5 : 1765004.6754
6 : 2313026.1639
7 : 2425963.839
8 : 1485798.536
9 : 1596110.5281
10 : 1619515.9581
11 : 1842443.0502
12 : 1861389.2254
13 : 2371857.7661
14 : 2269213.1541
15 : 2128551.3524
16 : 1320579.5142
17 : 1261737.3518
18 : 1825898.6138
19 : 1785823.4341
20 : 2490309.8988

Real Person

Recognized Value : 7

By Classifying using QDA, the values are classified and they are extracted from the training section values for the feature extraction. And then the values are classified using train values and to recognize the value which the person is and the value would proceed that the person is real or fake.

3.7. Recognition/Authentication:



Classification Result : Real Person

Recognized Value : 7

To Recognize and to Authenticate that to find the person is real or not, I need to classify with the QDA and finally by classifying with the Face and Signature feature the result using classification can find the person by using the recognized value to find that the person is real.

IV. RESULT

In this Paper, the process for Recognition/Authentication for the Face and Signature image that can recognize and authenticate using Local Derivative Pattern (LDP). And by combining the values which the values are extracted using QDA form the training images which are taken form the database. And these values are combined using both Full-Reference and No Reference IQ measure for giving 25 combined values.

CONCLUSION

The study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years. This interest has led to big advances in the field of security-enhancing technologies for biometric-based applications. However, in spite of this noticeable improvement, the development of efficient protection methods against known threats has proven to be a challenging task. Simple visual inspection of an image of a real biometric trait and a fake sample of the same trait shows that the two images can be very similar. Yet, some disparities between the real and fake images may become evident once the images are translated into a proper feature space. These differences come from the fact that biometric traits, as 3D objects, have their own optical qualities (absorption, reflection, scattering, refraction), which other materials (paper, gelatin, electronic display) or synthetically produced samples do not possess. Furthermore, biometric sensors are designed to provide good quality samples when they interact, in a normal operation environment, with a real 3D trait. If this scenario is changed, or if the trait presented to the scanner is an unexpected fake artifact (2D, different material, etc.), the characteristics of the captured image may significantly vary. In the present work, using LDP the values are calculated by using Full and No reference (IQM) Image Quality Measures for the Face and Signature and then classified using Quadratic Discriminant Analysis (QDA) for the Recognition and Authentication to find it Real/Fake.

References:

[1] Aarti Sharma and Dr. SurenderDahiya, "SPOOF DETECTION: Application to Face Recognition" in IJSRD Vol. 2, Issue 04, 2014.

[2] Arathi M and Govardhan A, "An Efficient Offline Signature Verification System" International Journal of Machine Learning and Computing (IJMLC), Vol. 4, No. 6, December 2014.

[3] Anjos .A and Marcel .S, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.

[4] Harpreet Anand, and Prof. Bhombe D.L, "ENHANCED SIGNATURE VERIFICATION AND RECOGNITION USING MATLAB" International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1 Issue 4 (May 2014).

[5] Hennebert J, Loeffel R, Humm A, and Ingold R, "A new forgery scenario based on regaining dynamics of signature" in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366–375.

[6] KandlaArora, "Real Time Application of Face Recognition Concept" International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-5, November 2012.

[7] Meena K, Suruliandi A, and Reena Rose R, "Enhancing the performance of texture-based face recognition through multi-resolution techniques" Int. J. Biometrics, Vol. 6, No. 4, 2014.

[8] Prathamesh M. Sonavane, “Fake Biometric Trait Detection Using Image Quality Features” IJEDR, Volume 3, Issue 2, 2015.

[9] Tarange A.L, Gulve A.K, Pawar B.S, “FEATURE EXTRACTION METHODS FOR OFFLINE SIGNATURE VERIFICATION: A REVIEW” IJPRET, 2014; Volume (8), April 2014.

[10] Wang Z, Bovik A C, Sheikh H R, and Simoncelli E P, “Image quality assessment: From error visibility to structural similarity” IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.