IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

Parametric Real Face Images Detection using Multiple Classifiers

H. Alebeed[1], M. Osman[2]

Computer Engineering Department, Eastern Mediterranean University, Famagusta via Mersin 10, Turkey[1,2]

Abstract: To discriminate between real genuine face and impostor printed face sample has been an important field in biometric authentication researches, recently researches were done on this particular field to improve protection on biometric systems. In this paper software-based approach is presented based on image quality assessments (IQA) to discriminate real genuine face images from impostor samples, a liveness assessment method is added to the present system to ensure friendly use, processing speed, and non-intrusive biometric system. The proposed method uses 15 image quality features to decrease the level of complexity and make the system applicable for real-time applications. The experimental results achieved from this implemented work on an available dataset generates a high degree of positive detection compared to other existing methods and that the 15 image quality measures are efficient in classifying real faces from printed impostor samples. There are some useful information's retrieved from real images using IQA that makes the system capable enough to discriminate them from printed traits, the implemented approach uses 15 classification methods to ensure the efficiency of our introduced work.

Keywords: Genuine face, biometric authentication, IQA, non-intrusive biometric, quality features.

I. INTRODUCTION

Nowadays, Biometric Recognition, or Biometrics can be defined as the recognition of individuals based on their physical and/or behavioural characteristics, is a prominent field of research [1]. Although among all the biometrics like: face, fingerprint, iris, signature etc. face has an outstanding importance over other systems because it's reliable, cheap and non-intrusive [2]. Although it's affected by some changes in sunglasses, lighting, facial hair etc. but all these affections can be enhanced using some filtering process. There are different threats that detect such systems such as spoofing attacks which has been an important and motivated area for biometric researchers to study the vulnerabilities against such types of actions in areas such as iris [3], fingerprint [4], face [2], etc.…

In such spoofing-attacks hackers use some synthetically produced materials such as gummy finger, printed faces or iris images, or tries to copy the behaviour of the genuine user such as signature [5], to access the system. Since this attacks are performed in the analogue domain with regular identifications, the usual known protection mechanisms are not effective such as (e.g. encryption, watermarking or digital signature).
The number of different works done on this particular field, has shown the necessity of implementing an advanced protection strategy to ensure more security [1]. Researchers in the recent years have focused on finding some specific quality measurements that changes the modification of biometric systems in order to target impostor samples and reject them, using this strategy to increase the security level of the biometric system.
In the paper, we implement a real face image detection software system using image quality assessment (IQA), with different classifiers to ensure the quality of our system that gives a good level of real face image detection. The rest of the paper is organized as follows. Section 2 presents a brief literature survey of existing methods based on spoofing detection and the problem definition, Section 3 is our implementation which presents a general diagram of our system and consist of how we implemented feature extraction and classifiers, Section 4 consist of our experiments done it shows the experimental setup and results obtained, Section 5 is where we concluded our work and recommended a feature development.

II. LITERATURE REVIEW

2.1 Definitions of known image quality measures and classifiers

The paper [6], defines 26 image quality measures and two types of classification methods. The presented measures are divided into two parts, Full Reference (FR) IQA which extracts quality features using two images, input image and the enhanced version of the same image using Gaussian filter, and No Reference (NR) IQA that evaluates the quality of the input image. This method [6] extracts 26 IQA features to reduce the level of complexity. It uses a discriminant analysis to discriminate between real and fake images namely linear discriminant analysis (LDA) and quadratic discriminant analysis (QDA).

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

a) FR image quality assessment measures

(FR) IQA is composed of five different parts [6], 11 pixel difference measures, 2 edge based measures, 2 spectral distance measures, 2 gradient based measures, and 3 information theoretic measures

b) No reference image quality measures

1- Distortion specific measures

- JPEG quality index (JQI): it evaluates image qualities distorted by known block artificial initiated in compression algorithms at a decreased number of bit rate as JPEG. (Practical implementation in [7] and See [8])
- High Low Frequency Index (HLFI): it's sympathetic with sharpness and works by estimating the difference between low and up frequency actions of Fourier spectrum.

2- Training based measures[6]

Blind Image Quality Index Measurement (BIQI): This technique is known in the past to train images, the idea behind this mode is that clear real images introduce some regular properties if calculated properly, aberrance from the uniformity of natural statistics can evaluate the quality of the given image. (See [9] and practical implementation in [7]).

3- Natural scene statistic approaches

- Natural Image Quality Evaluator (NIQE): This measurement is used to evaluate blind image quality based on extracting features of statistics associated to many alterations generating quality information's.

(See [10] and practical implementation in [7])

- Spatial Spectral Entropy Quality (SSEQ): this quality is calculated by converting the input image to spatial and spectral format, using Fourier transform the entropy amounts are evaluated, then match the two entropy values, calculate and consider the inequality between them.

(See [11] and practical implementation in [7])

c) Classification of real fake face images

This classification stage is to discriminate between real and fake samples, in these paper researchers mentioned two types of classifications namely:

- Linear Discriminant Analysis (LDA).
- Quadratic Discriminant Analysis (QDA).

Based on our proposed method we extended the classifiers to ensure the quality of our system and in order to report better result using other classifiers, our classifiers where:

- Linear Discriminant Analysis (LDA).
- Quadratic Discriminant Analysis (QDA).
- Logistic Regression (LG).
- Linear SVM.
- Quadratic SVM.

2.2 Methods based on image quality features

a) Methods with features less than 10

Recent approach [11] is using different identification systems, and machines that satisfies the user's needs and secure important resource, these paper [12] reviews biometric identification systems recently developed. This technique is implemented to ensure the identification of an individual weather its real or fake, the aim of this paper is to increase the safety of the biometric system by adding liveness assessment in a user-friendly, fast, simple and non-intrusive manner.

This method [12] introduce previous attacks on face, fingerprint, and iris. The proposed method is suitable for real-time applications as it presents a low degree of complexity. This system uses image quality assessments measures extracted from one image to discriminate between real and fake samples. It shows extremely competitive results compared with other existing state-of-the-art approaches, when we analyze the image quality measures there are valuable information's that can highly discriminate real samples from impostor traits.

b) Methods using 25 image quality feature and less

In [1], a software-based method is used for detecting spoofing attacks, they proposed multiple biometric system that detects face, fingerprint and iris. The objective of this paper is to enhance recognition and protection strategies, to develop the biometric security systems by using image quality assessments and adding liveness assessment in order to improve the quality of speed, make it user friendly and non-intrusive.

The proposed in [1] approach is designed in a suitable manner for real-time applications, with a low degree of complexity, using 25 image quality assessments features extracted from each input image (the same used for authentication purposes) to discriminate between genuine and impostor samples.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

The results obtained in [1] for face recognition show that their approach is highly competitive compared with other methods and that the use of image quality features extracted from real face samples is very efficient to discriminate them from fake images. The presented paper[13] is a biometric system used for face image classification, this implemented method uses image quality assessment features to indicate if the input image is real or fake, the proposed method shows that real biometric traits usually gives high valuable information's enough to efficiently discriminate between genuine and impostor traits. This paper[14] introduce REPLAY-MOBILE database, and compares existing face recognition approaches based on (IQA) image quality assessment measures, this method also provides a number of classifiers to discriminate between real and impostor samples.
In paper [15], they have proposed a biometric system based on iris and face fake detection, several existing methods on liveness detection were adapted and implemented to a limited-constrained scenario. The proposed method is a combination of the feature selection in the existing methods classifiers to perform a classification based on the best features (SVM) support vector machine which is used for training face and iris images. The input images result as real and fake images by matching with training real and fake samples.
Based on the existing method 2-sets [1], [16] of presentation attack detection (PDA) results are presented on face recognition based on image quality assessment, the results are presented on ISO standard metrics [see the ISO/IEC 30107-3 standard], (APCER) Attack Presentation Classification Error Rate; and (BPCER) Bona fide Presentation Classification Error Rate.
This proposed paper compares 2-sets of presentation attack detection (PDA) results based on face recognition and classification, Face-PAD using IQA [1], and Face-PAD based on Gabor-Jets [16].

c) SVM classification

Support vector machines (SVM) are supervised learning models associated learning algorithms used for analyzing data and classifying the input patterns.

SVM Classification Algorithm:

- Read the input iris or face training images from database.
- Calculate the 25 image quality assessments full reference and no reference features for the input training images.
- Combine the 25 quality measures as quality assessment features.
- Create SVM Classification Training Target and compare the trained features using SVM Classifier.
- Classify SVM training to two classes and give results of either real or fake image.

d) Methods using more than 25 image quality features

In paper [17] a software-based biometric system is introduced with a multi-attack method in order to improve the biometric system security.
This proposed method is based on image quality assessment to discriminate between real and fake traits. This system presented 30 image quality measurements extracted from the input query image for identifying the user's access attempt; these parameter vectors extracted from the image are classified using linear and quadratic discriminant analysis.
This system adds a liveness assessment technique to ensure the biometric system security and provides a low degree of complexity with good performance. In this multi-biometric system, attacks from face, iris, fingerprints, and hand palm images are detected. In hand palm classification of real or impostor users a discriminating method called Dempster-shafer theory [18] [19] is used, lots of rotations and translations are presented in hand palm images. Dempster-shafer method process by combining multiple results of decisions obtained by discriminant analysis and produces decisions between genuine or impostor users. The aim of [17] is to discriminate between real and fake images.
The method [20] is developed to increase the biometric security system by using 31 image quality features and adding a liveness assessment method to the system, spoofing attacks is an important field in biometrics, it has been divided into direct and indirect attacks, in this approach these attacks are detected by using 31 IQA and discriminant classifier to discriminate fake and real images, in [17] discriminant power analysis (DPA) is used in face recognition.

2.3 Problem Definition

- Implement and test real face image detection system
- Conduct experiments on real face image detection system as in [1]
- Increase number of classifiers Based on the classification methods used, by trying other classifiers rather than LDA, QDA like Linear SVM, Quadratic SVM, and Logistic Regression.
- Investigate how to define best 10 and best 5 features that are used but not clearly defined the way of choosing in [1].
- Compare with other methods based on face spoofing attacks
- Recent papers used different number of quality measures; we are going to investigate the use of 15 image quality measures.
- Examine our proposed method on different data sets.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

III.IMPLEMENTATION OF RFIDS

IQA refers to image quality measures, FR refers to full reference, and the diagrams show how the input image features are extracted and how the classification method is performed.

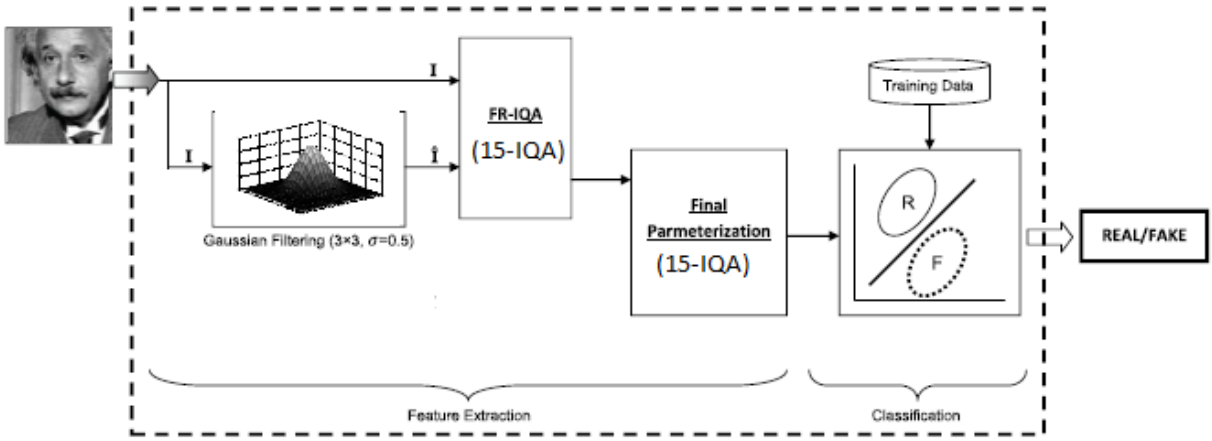

Fig1. General diagram structure of RFIDS

3.1 Implementation and testing of feature extraction sybsystem

We use Matlab2014 for implementation.

For testing of the implementation of the features shown below, we are going to use a 4*4 matrix, I(M,N) with M=N=4 to represent a gray scale image to make computation easier and clearer.

Original image (reference clean image)

0 10 7 5
0 2 9 12
4 2 2 6
10 3 9 15

Distorted image (smoothed version of the reference image), I(M,N) is as follows:

2 9 10 5
0 1 6 1
3 6 2 6
11 3 14 14

1- Implementation and testing of Mean Squared Error (MSE): MSE is given by equation (1).

MSE = sum(sum(error .* error)) / (M * N);

MSE= 1/16 * (0-2)^2 + (10-9)^2 + (7-10)^2 + (5-5)^2 + (0-0)^2 + (2-1)^2 + (9-6)^2 + (12-1)^2 + (4-3)^2 + (2-6)^2 + (2-2)^2 + (6-6)^2 + (10-11)^2 + (3-3)^2 + (9-14)^2 + (15-14)^2 =

=1/16*(189) = 11.8 (1)

2- Implementation and testing of Peak Signal To Noise Ratio(PSNR): PSNR is given by equation (2).

PSNR = 10*log10((255.*255)/MSE);

= 37.4 (2)

3- Implementation and testing of Signal To Noise Ratio (SNR): SNR is given by equation (3).

SNR = 10*log10((sum(sum(origImg.*origImg)))./(M .* N .* MSE));

SNR= 10log (2^2 + 10^2 + 7^2 + 5^2 + 0^2 + 2^2 + 9^2 + 12^2 + 4^2 + 2^2 + 2^2 + 6^2 + 10^2 + 3^2 + 9^2 + 15^2) / 4 * 4 * 11.8

=6.67 (3)

4- Implementation and testing of Structural Content (SC): SC is given by equation (4)

SC = sum(sum(origImg .* origImg)) ./ sum(sum(distImg .* distImg));

SC = (0^2 + 10^2 + 7^2 + 5^2 + 0^2 + 2^2 + 9^2 + 12^2 + 4^2 + 2^2 + 2^2 + 6^2 + 10^2 + 3^2 + 9^2 + 12^2) / (2^2 + 9^2 + 10^2 + 5^2 + 0^2 + 1^2 + 6^2 + 1^2 + 3^2 + 6^2 + 2^2 + 6^2 + 11^2 + 3^2 + 14^2 + 14^2)

= 1.026 (4)

5- Implementation and testing of Maximum Difference (MD): MD is given by equation (5)

MD = max(max(abs(error)));

MD=11 (5)

6- Implementation and testing of Average Difference (AD): AD is given by equation (6).

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

AD = sum(sum(error)) / (M * N);
AD = 1/16 ((2 - 0) + (9 - 10) + (10 - 7) + (5 - 5) + (0 - 0) + (2 - 1) + (9 - 6) + (12 - 1) + (4 - 3) + (2 - 6) + (2 - 2) + (6 - 6) + (10 - 11) + (3 - 3) + (9 - 14) + (15 - 14))
=1/16(-2 + 1 + -3 + 0 + 0 + 1 + 3 + 11 + -4 + -1 + 0 + -5 + 1 + 1)
=0.187 (6)

7- Implementation and testing of Normalized Absolute Error (NAE): NAE is given by equation (7).
NAE = sum(sum(abs(error))) ./ sum(sum(abs(origImg)));
NAE= | (0 - 2) + (10 - 9) + (7 - 10) + (5 - 5) + (0 - 0) + (2 - 1) + (9 - 6) + (12 - 1) + (4 - 3) + (2 - 6) + (2 - 2) + (6 - 6) + (10 - 11) + (3 - 3) + (9 - 14) + (15 - 14) |
| 0 + 10 + 7 + 5 + 0 + 2 + 9 + 12 + 4 + 2 + 2 + 6 + 10 + 3 + 9 + 15 |
=0.343 (7)

8- Implementation and testing of R-Averaged MD: RAMD is given by equation (8).
RAMD = sum((abs(resultat1)))/R;
RAMD =1/7 | 11 + 5 + 4 + 3 + 2 + 1 + 0 |
= 3.7142 (8)

9- Implementation and testing of Normalized Cross Correlation (NCC): NCC is given by equation (9).
NCC = sum(sum(origImg .* distImg)) ./ sum(sum(origImg .* origImg));
=(0 + 90 + 70 + 25 + 0 + 2 + 54 + 12 + 12 + 12 + 4 + 36 + 110 + 9 + 126 + 210) / (0 + 100 + 49 + 25 + 0 + 4 + 81 + 144 + 16 + 4 + 4 + 36 + 100 + 9 + 81 + 225)
=0.875 (9)

10- Implementation and testing of Total Edge Difference (14): TED is given by equation (10).
TED = sum(sum(abs(error))) / (M * N); (10)
Results of Total Edge Difference calculation by Code 10 is shown in Fig2.

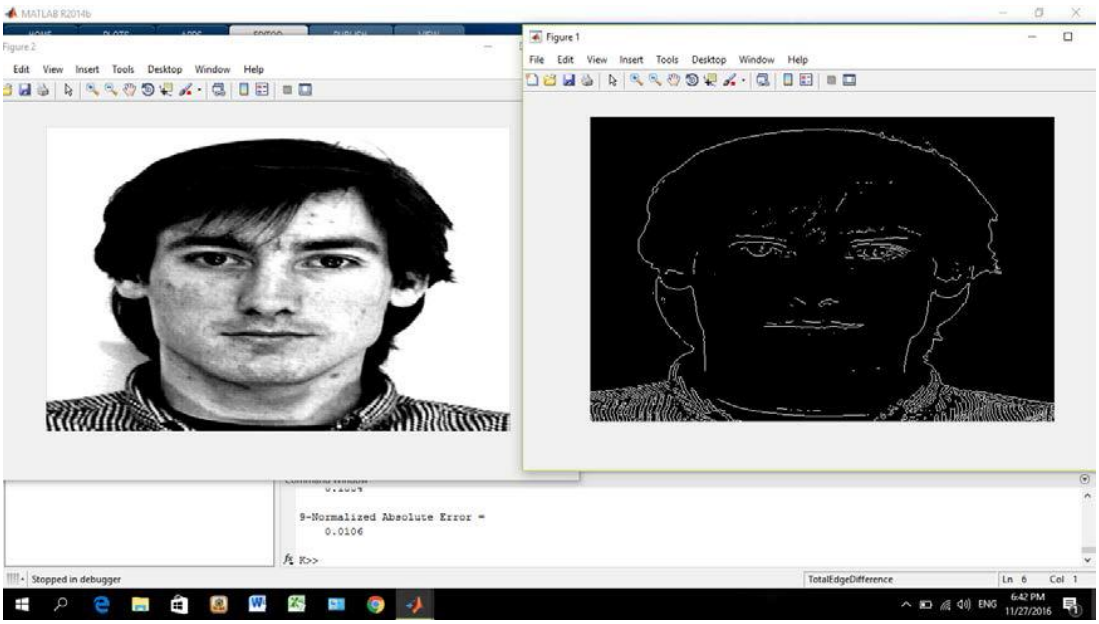

Fig2. Results obtained by equation (10)

11- Implementation and testing of Gradient Magnitude Error: GME is given by equation (11).
GME =sum(sum(error)) / (M * N);
=1/16 (7.3978+0.0449+1.6144+ 0.7619 + 2.925 + 7.1112 + 2.5287 + 3.9346 + 0.7740 + 4 + 11.290 + 4.3856 + 5 + 15.8467 + 7.9337)
= 4.7223 (11)

12- Implementation and testing of Gradient phase error: GPE is given by equation (12).

$$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} |\arg(\mathbf{G}_{i,j}) - \arg(\hat{\mathbf{G}}_{i,j})|^2$$

GPE = 1/16 (-0.2783^2 + 0.0512^2 + 0.4324^2 + -0.6178^2 + 0.3218^2 + 0.2630^2 + -1.1071^2 + -2.8768^2 + 0.8799^2 + 0.6435^2 + -1.5708^2 + -0.6604^2 + 0.0768^2 + 0.9273^2 + -0.2789^2 + -0.588^2)
= 4.7223 (12)

13- Implementation and testing of Spectral Magnitude Error (15): SME is given by equation (13).
SME =sum(sum(error.*error)) / (M * N);

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

SME = 1/16 (3^2 + 7.233^2 + 11^2 + 7.232^2 + -19.046^2 +-8.979^2 + 2.082^2 + 12.968^2 + 17^2 + 8.062^2 + -15^2 + 8.062^2 + -19.046^2 + 2.968^2 + 2.082^2 + -8.979^2)
=131.905 (13)

14- Implementation and testing of Spectral phase error: SPE is given by equation (14).

SPE =sum(sum(error.*error)) / (M * N)
SPE= 1/16 (0^2 + -0.604^2 +3.141^2 + -0.604^2 + -0.260^2 + -0.040^2 + 1.681^2 + 0.631^2 + 0^2 + 0.002^2 + 0^2 + 0.002^2 + 0260^2 + 0.631^2 + 1.681^2 + -0.040^2)
=1.074 (14)

15- Implementation and testing of Total corner difference: TCD is given by equation (15).

TCD =(abs(NCRorig-NCRdist))/max1;
TCD = |366 – 385| / 385
= 0.0494 (15)

Results of mean squared error calculation by Code 15 is shown in Fig3. It complies with (15)

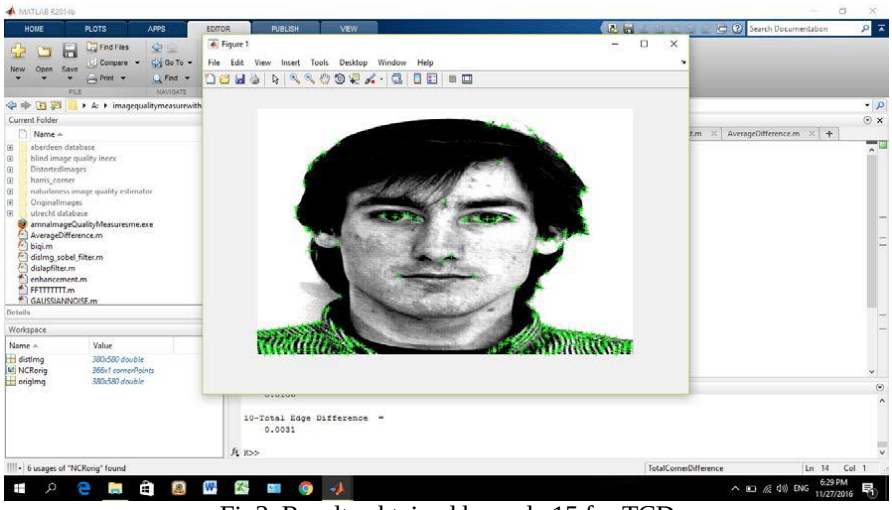

Fig3. Results obtained by code 15 for TCD

3.2 Implementation of classifiers

In MATLAB 2016 there is a ready application provided called classification learner that we can use to import tables from our work space, these application extracts predictors and observations and allows a number of classification algorithms (LDA, QDA, etc..) to classify the samples extracted.

Classification learner application in matlab:

Using the classification learner application we have to arrange our implemented results into a table and display them in workspace, the classification learner app imports all results in work space and ask for permission of which table you want to use, we select the table containing all results of implemented faces with all 15 features.

The classification methods used are:

1- LDA
3- Linear SVM
4- Quadratic SVM
5- Logistic Regression.

The following classification methods are provided in MATLAB 2016 and implemented results are in term of:

a) Scatter Plot [19]: is also known as scatter graph or chart, the input in these chart is two variables, with the use of Cartesian coordinate these variables values are plotted and displayed. These values are displayed in a number of points, each point has a value representing one variable showing the position on horizontal axis, and value showing the position in vertical axis.

b) Confusion Matrix[21]: it is also known as error matrix, it is composed in machine learning field, it is a table that views the efficiency of an algorithm , each column in the matrix show the occurrence in a predicted class where the row shows the occurrence in the actual class.

c) ROC Curve [22]: it is a graphical plot that represents the achievement of a binary classification system where the classification threshold is assorted. True positive and false positive rates are uses in plotting the curve using an assorted threshold settings.

d) Parallel Coordinates Plot [23]: it is used to visualize high dimensional geometry and to analyze data, it also represents a number of points in an n-dimension space, parallel lines are drawn in a vertical manner with equal spaces, the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

represented point in n-dimension space is a polyline with vertices sown on the parallel axes, the vertex position on the j-the axis correlates to the j-th coordinate of the point.
We developed an overall structure having the subsystems. Each subsystem was implemented and tested in MATLAB 2016. Then, the subsystems were integrated into RFIDS and tested. Classifiers subsystem implemented in MATLAB 206 as a separate application is incorporated into RFIDS using the following means: Scatter plot, Confusion matrix, ROC curve, Parallel coordinates.

IV. EXPERIMENTS ON RFIDS

This section 4 is showing the results of our experiments done on AUU database, the results are experimented on different datasets(tables [1], [2], [3], [4]) to ensure the presented methods quality, also we compared our proposed method with other state-of-art methods (table 7) and see the efficiency of our work, the results are also conducted (table [5], [6]) on different experiments on different types on quality features and show that with 15 features we get an excellent result.

4.1 Experiment setup

a) Experiment setup Hardware and software requirements

Our measurement will be made on a standard 64-bit windows10-pc, with core i7, 2.40 GHZ processor, and 16 GB RAM memory, Running MATLAB R2016a.

b) Database

NUAA Photograph Imposter Database [25], the database was collected in three sessions with about 2 weeks interval between two sessions, and the place and illumination conditions of each session are different as well. Altogether 11 subjects (numbered from 1 to 11) were invited to attend in this work.
Note that it contains various appearance changes commonly encountered by a face recognition system (e.g., sex, illumination, with/without glasses). All original images in the database are color pictures with the same definition of 640 x 480 pixels.
Illustration of different photo-attacks: (1) move the photo horizontally, vertically, back and front; (2) rotate the photo in depth along the vertical axis; (3) the same as (2) but along the horizontal axis; (4) bend the photo inward and outward along the vertical axis; (5) the same as (4) but along the horizontal axis.
We will use 600 genuine samples and 700 imposter samples of 11 different users for our test results. Images are resized to 380 × 580.

c) Type of spoofing attack

Photograph samples, we take high definition photo for each subject using a usual Canon camera in a way that the face area should take at least 2/3 of the whole area of the photograph. We then developed the photos in two ways. The first is to use the traditional method to print them on a photographic paper with the common size of 6.8cmx10.2cm (small) and 8.9cm x 12.7cm (bigger), respectively. In the other way, we print each photo on a 70g A4 paper using a usual color HP printer.

Classification methods

- LDA (linear discriminant analysis)
- QDA (Quadratic discriminant analysis)
- Linear SVM
- Quadratic SVM
- Logistic Regression

Results will be reported in terms of FFR(false fake rate)
FGR (false genuine rate)(2.22), HTER(2.23) = (FGR+FFR)/2.

d) Parameters

The features selected as best were considered using parallel coordinate plot that distinguish the real image features that result in high difference , from fake images, these features were selected in the following sets to consider experiments on best features.

- 5-sets: SNR, PSNR, R-AMD, NAE, GME.
- 10-sets: SNR, PSNR, R-AMD, NAE, GME, MSE, SPE, SC, AD, MD
- 15-sets: ALL

And a graph will be plotted to show the relationship between the measurements and HTER.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

4.2 Experimental Results based on AUU database

TABLE 1 RESULTS OBTAINED IN TERMS OF FFR, FGR, AND HTER FROM 4 CLASSIFIERS ON DATASET-4, WITH TRAINING AND PREDICTION TIME.

Data Set	Scenario	Classifier	FFR (%)	FGR (%)	HTER (%)	Training time (sec)	Prediction speed (obs/sec)
4	Controlled 60(30/30)	LDA	0	0	0	1.5614	~560
		QDA	0	0	0	1.8197	~490
		Linear SVM	0	0	0	2.8546	~500
		Quadratic SVM	0	0	0	1.6242	~670
		Logistic Regression	0	0	0	7.0507	~340

TABLE 2 RESULTS OBTAINED IN TERMS OF FFR, FGR, AND HTER FROM 4 CLASSIFIERS ON DATASET-5, WITH TRAINING AND PREDICTION TIME.

Data Set	Scenario	Classifier	FFR (%)	FGR (%)	HTER (%)	Training time (sec)	Prediction speed (obs/sec)
5	Controlled 60(30/30)	LDA	0	0	0	1.5287	~590
		QDA	0	0	0	1.9282	~500
		Linear SVM	0	0	0	2.9436	~510
		Quadratic SVM	0	0	0	1.4207	~710
		Logistic Regression	0	0	0	6.8621	~350

TABLE 3 RESULTS OBTAINED IN TERMS OF FFR, FGR, AND HTER FROM 4 CLASSIFIERS ON DATASET-7, WITH TRAINING AND PREDICTION TIME.

Data Set	Scenario	Classifier	FFR (%)	FGR (%)	HTER (%)	Training time (sec)	Prediction speed (obs/sec)
7	Controlled 60(30/30)	LDA	0	0	0	1.51	~600
		QDA	0	0	0	1.9658	~500
		Linear SVM	0	0	0	3.0336	~490
		Quadratic SVM	0	0	0	1.6247	~680
		Logistic Regression	0	1.6	0.8	7.021	~330

TABLE 4 RESULTS OBTAINED IN TERMS OF FFR, FGR, AND HTER FROM 4 CLASSIFIERS ON DATASET-8, WITH TRAINING AND PREDICTION TIME.

Data Set	Scenario	Classifier	FFR (%)	FGR (%)	HTER (%)	Training time (sec)	Prediction speed (obs/sec)
8	Controlled 60(30/30)	LDA	0	0	0	1.7991	~580
		QDA	0	0	0	2.1554	~470
		Linear SVM	0	0	0	3.1816	~450
		Quadratic SVM	0	0	0	1.6011	~720
		Logistic Regression	0	0	0	7.8577	~320

TABLE 5 RESULTS OBTAINED IN TERMS OF FFR, FGR, AND HTER FROM 4 CLASSIFIERS ON BEST-5, WITH TRAINING AND PREDICTION TIME.

	Quality measures	Classifier	FFR (%)	FGR (%)	HTER (%)	Training time (sec)	Prediction speed (obs/sec)
Best-5 60(30/30)	(SNR, PSNR, RAMD, NAE, GME)	LDA	10	0	5	1.4527	~600
		QDA	11.6	1.6	6.6	1.957	~530
		Linear SVM	5	0	2.5	2.9845	~550
		Quadratic SVM	3.3	0	1.6	1.5906	~740
		Logistic Regression	3.3	0	1.6	6.6972	~370

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

TABLE 6 RESULTS OBTAINED IN TERMS OF FFR, FGR, AND HTER FROM 4 CLASSIFIERS ON BEST-10, WITH TRAINING AND PREDICTION TIME.

	Quality measures	**Classifier**	**FFR (%)**	**FGR (%)**	**HTER (%)**	**Training time (sec)**	**Prediction speed (obs/sec)**
Best-10 60(30/30)	(SNR, PSNR, RAMD, NAE, GME, MSE, SPE, SC, AD, MD)	LDA	6.6	1.6	4.1	1.4527	~600
		QDA	3.3	1.6	2.54	1.957	~530
		Linear SVM	1.6	0	0.8	2.9845	~550
		Quadratic SVM	3.3	0	1.6	1.5906	~740
		Logistic Regression	8.3	1.6	4.95	6.6972	~370

From the results [1]-[4], that are done on different datasets[25] using 5 different classifiers LDA, QDA, Linear SVM, Quadratic SVM, Logistic Regression using our implemented code, we can consider our proposed system as a 100% discriminator system when it comes to detecting false from real samples, Linear SVM is considered as the best discriminator when number of measures are decreased, were logistic regression showed a 1.6% false genuine rate and consumes lot of time to train the images we can consider it as worst classifier, based on LDA it gives the best execution time in all dataset experiments. On tables [5], [6] we presented the results conducted on different number of features to ensure the performance of the total 15 features, the experiments were conducted on database [25].
Comparison between our proposed method and other state-of-art methods based on printed face note that our method uses linear SVM as a classifier:

TABLE 7 COMPARISON BETWEEN PROPOSED METHOD AND OTHER STATE-OF-ART METHODS IN TERM OF SPOOFED PRINTED FACES [1].

	FFR	**FGR**	**HTER**
Proposed-IQA	0.0	0.0	0.0
IQA-based[1]	0.0	1.0	0.5
AMILAB[24]	0.0	1.2	0.6
CASIA[24]	0.0	0.0	0.0
IDIAP[24]	0.0	0.0	0.0
SIANI[24]	0.0	21.2	10.6
UNICAMP[24]	1.2	0.0	0.6
UOULU[24]	0.0	0.0	0.0

We can see from table (7) that our implemented method is highly comparative to other state-of art methods and it gives excellent recognition rate similar to CASIA [24], IDIAP [24], and UOULU [24], were other methods give lower recognition rates.

V. CONCLUSION

We have made a literature survey. From the analysis of [1],[6],[11],[12], [13]-[15],[17],[20], we conclude that existing methods use different number of image quality features, and also present different types of classification methods, the results were tested on different databases and we can also say in the recent years that the result obtained were not 100% positive. We defined the problems of the paper: implemented and investigate experimentally real face image detection system (RFIDS).
Section 3 we showed how we implemented our RIDS. We developed an overall structure having the following subsystems: [3.1], [3.2]. Each subsystem was implemented and tested in MATLAB 2016. Then, the subsystems were integrated into RFIDS and tested. Classifiers subsystem implemented in MATLAB 206 as a separate application is incorporated into RFIDS using the following means: Scatter plot, Confusion matrix, ROC curve, Parallel coordinates.
Also the codes necessary for conduction experiments on RFIDS are developed.
Section 4 is showing the results of our experiments done on AUU database, the results are experimented on different datasets(tables [1]-[4]) to ensure the presented methods quality, also we compared our proposed method with other state-of-art methods (table 7) and see the efficiency of our work, the results are also conducted (table [5], [6]) on different experiments on different types on quality features and show that with 15 features we get an excellent result.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 7, July 2017

Our future work will be aiming implementation of different types on biometric traits such as finger print, iris, etc.., In order to conduct a multi-biometric system, and include more classifiers to discriminate between real and fake images to ensure protection strategy.

REFERENCES

[1] Javier Galbally, Sébastien Marcel, and Julian Fierrez (2014). Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. IEEE Transactions on Image Processing, Vol. 23, No. 2, February 2014.
[2] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.
[3] T. Matsumoto. (2004). Artificial irises: Importance of vulnerability analysis. in Proc. AWB.
[4] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, et al., "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," Pattern Recognit. Lett., vol. 31, no. 8, pp. 725–732, 2010.
[5] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366–375.
[6] S.Saranya, S.vinitha Sherline, and Mrs. Maheswari (2016). Fake Biometric Detection Using Image Quality Assessment: Application to Iris, Fingerprint, Recognition. 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM).
[7] (2012). LIVE [Online]. Available: http://live.ece.utexas.edu/research/ Quality/index.htm.
[8] Z. Wang, H. R. Sheikh, and A. C. Bovik, "No-reference perceptual quality assessment of JPEG compressed images," in Proc. IEEE ICIP, Sep. 2002, pp. 477–480.
[9] A. K. Moorthy and A. C. Bovik, "A two-step framework for constructing blind image quality indices," IEEE Signal Process. Lett., vol. 17, no. 5, pp. 513–516, May 2010.
[10] A. Mittal, R. Soundararajan, and A. C. Bovik, "Making a 'completely blind' image quality analyzer," IEEE Signal Process. Lett., vol. 20, no. 3, pp. 209–212, Mar. 2013.
[11] Mr. Steven Lawrence Fernandes, Dr. G Josemin Bala (2015). Developing a Novel Technique for Face Liveness Detection. International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015.
[12] Preethi.V and Prof.S.Chidambaram (2015). Fake Multi-biometric Detection for Applications of Fingerprint, Iris and Face Recognition, International Journal of Engineering Trends and Technology (IJETT) – Volume 21 Number 2 – March 2015
[13] P. Suresh (2014). Find Pretend Biometric Mistreatment Image Quality Assessment For Animateness Detection. Asian Journal of Technology & Management Research [ISSN: 2249 –0892] Vol. 04 – Issue: 02 (Jul - Dec 2014).
[14] Artur Costa-Pazo, Sushil Bhattacharjeey, Esteban Vazquez-Fernandez, and Sebastien Marcel (2016). The REPLAY-MOBILE Face Presentation-Attack Database. GRADIANT -Galician Research & Development Center in Advanced Telecommunications CITEXVI, loc. 14 — CUVI, 36310 Vigo (Po.) – Spain.
[15] S.Vigneshwaran, M.Suresh, and Dr.R.Meenakumari (2015). An SVM based Statistical Image Quality Assessment for Fake Biometric Detection. International Journal for Trends in Engineering & Technology Volume 4 Issue 1 – April 2015.
[16] M. Fontani, T. Bianchi , A. De Rosa, A. Piva , M. Barni., " A Dempster-Shafer Framework for Decision Fusion in Image Forensics".
[17] Sneha S, Mrs. R.Indumathi (2015). Fake Biometric Detection Using Improved Features in Image and Dempster-Shafer Method. International Journal On Engineering Technology and Sciences – IJETS.
[18] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, et al., "Competition on countermeasures to 2D facial spoofing attacks," in Proc. IEEE IJCB, Oct. 2011, pp. 1–6.
[19] Scatter Plot. (25 November 2016), Retrieved from https://en.wikipedia.org/wiki/Scatter_plot
[20] Rinu Prakash T, Vipin Thomas (2015). Biometric Security System for Fake Detection using image Quality Assessment Techniques. International Journal on Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 9.
[21] Confusion Matrix. (11 October 2016), Retrieved from https://en.wikipedia.org/wiki/Confusion_matrix
[22] ROC Curve. (4 January 2017), Retrieved from https://en.wikipedia.org/wiki/Reciever_operating_characteristics
[23] Parallel coordinate. (12 January 2017),Retrieved from https://en.wikipedia.org/wiki/Parallel_coordinates
[24] Imran Naseem and Mohamed Deriche Electrical Engineering Department, "A new algorithm for speaker identification using the Dempster-Shafer theory of evidence", Journal of Advanced Science and Technology Vol. 50, January, 2013.
[25] Database http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html