Image Quality Assessment for Fake Biometric Detection

Vijayalakshmi G V[1], Alex Noel Joseph Raj[2]

[1.] Department of ECE, Dr T Thimmaiah Institute of Technology, KGF, India, vijayalakshmi@drttit.edu.in

[2.] Key Laboratory of Digital Signal and Image Processing of Guangdong Province, Shantou University, Shantou, China, jalexnoel@stu.edu.cn

***Abstract:* This paper presents Image quality assessment for fake biometric system. The key point of the process is to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. In the present work, we propose a novel parameterization using 25 general full referenced and non-referenced image quality measures. In order to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake. The work was carried using Iris (ATVS-Flr DB) and Fingerprint(Livedet09) datasets. The simulation results indicate a significant accuracy of 95% with Iris biometry and 92.5% from fingerprint.**

***Keywords:* Image Quality Assessment (IQA); Biometry; Quadratic Discriminant Analysis; Accuracy; Referenced IQA; Non referenced IQA**

I. Introduction

With the widespread deployment of biometric systems in various applications, there are increasing concerns about the security and privacy of biometric technology. In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research, publication of many research works disclosing and evaluating different biometric vulnerabilities, proposal of new protection methods, publication of several standards in the area, dedication of specific tracks, sessions and workshops in biometric-specific and general signal processing conferences [1].All these initiatives clearly highlight the importance given by all parties involved in the development of biometrics(i.e., researchers, developers and industry) to the improvement of the systems security to bring this rapidly emerging technology into practical use.

Day by day fake self-manufactured synthetic or reconstructed sample is significant problem in biometric authentication, therefore software based fake detection method is required that can detect different types of fraudulent access attempts that ensures security of biometric recognition, by adding liveness assessment in a fast, user friendly, and non-intrusive manner through the use of image quality assessment [2]. Among the different threats analyzed, the so-called director spoofing attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in different modalities such as iris, fingerprint, face, signature, and gait. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behavior of the genuine user (e.g., gait, signature), to fraudulently access the biometric system [3].

As these types of attacks are performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective. The aforementioned works and other analogue studies have clearly shown the necessity to propose and develop specific protection methods against this threat. Thus researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them and hence, improving robustness and security level of the systems. Besides other anti-spoofing approaches such as the use of multi biometrics or challenge-response methods, special attention has been paid by researchers and industry to the liveness detection techniques, which use different physiological properties [4] to distinguish between real and fake traits. The rest of the paper is organized as follows. Section II deals with liveness assessment. Section III describes Image quality assessment techniques. The information regarding the data set used in the work is provided in Section IV. Section V furnishes details about the Methodology. The results are discussed in Section VI and finally Section VII concludes the paper.

II. Liveness Assessment

Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements such as non-invasive, user friendly, speed, low cost and a good fake detection rate. Liveness detection methods are usually classified into hardware based and software based methods as shown in Figure.1.

These two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems [5]. As a coarse comparison, hardware-based

NC-EVEN was held at Brindavan College of Engineering, Bengaluru, India on 11th May, 2017.

schemes usually present a higher fake detection rate, while software-based techniques are in general less expensive (as no extra device is needed), and less intrusive since their implementation is transparent to the user.

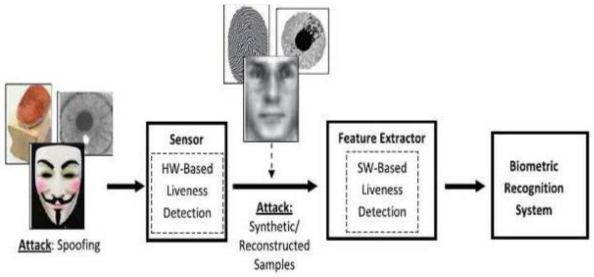

Fig 1. Liveness detection method

Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module which makes them potentially capable of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks [6].For instance, software-based methods can protect the system against the injection of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor. Although, a great amount of work has been done in the field of spoofing detection and many advances have been reached, the attacking methodologies have also evolved and become more and more sophisticated.

As a consequence, there are still big challenges to be faced in the detection of direct attacks. One of the usual shortcomings of most anti-spoofing methods [7] is their lack of generality. It is not rare to find that the proposed approaches present a very high performance detecting certain type of spoofs (i.e., gummy fingers made out of silicone), but their efficiency drastically drops when they are presented with a different type of synthetic trait(i.e., gummy fingers made out of gelatin). This way, their error rates vary greatly when the testing conditions are modified or if the evaluation database is exchanged. Moreover, the vast majority of current protection methods are based on the measurement of certain specific properties of a given trait (e.g., the frequency of ridges and valleys in finger prints or the pupil dilation of the eye) which gives them a very reduced interoperability, as they may not be implemented in recognition systems based on other biometric modalities (e.g., face), or even on the same system with a different sensor [8].

The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. In the present work we propose a novel parameterization using 25 general image quality measures. In order to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake (i.e., the same image acquired for biometric recognition purposes).

Furthermore, as the method operates on the whole image without searching for any trait-specific properties, it does not require any preprocessing steps (e.g., fingerprint segmentation, iris detection or face extraction) prior to the computation of the IQ features. This characteristic minimizes its computational load. Once the feature vector has been generated the sample is classified as real (generated by a genuine trait) or fake (synthetically produced), using Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA).The features are extracted out as per the four general criteria (i) Performance, (ii) Complementarity,(iii) Complexity and (iv)Speed , which intend that the final method complies to the highest possible extent with the desirable requirements set for liveness detection systems.

III. IMAGE QUALITY ASSESSMENT TECHNIQUE

Expected quality differences between real and fake samples include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both type of images (entropy), structural distortions or natural appearance. Besides, in an eventual attack in which a synthetically produced image is directly injected to the communication channel before the feature extractor, this fake sample will most likely lack some of the properties found in natural images. Following this "quality-difference" hypothesis, in the present research work we explore the potential of general image quality assessment as a protection method against different biometric attacks (with special attention to spoofing).

Human observers very often refer to the "different appearance" of real and fake samples to distinguish between them. As stated above, the different metrics and methods designed for IQA intend to estimate in an objective and reliable way the perceived appearance of images by humans. A different quality measure presents different sensitivity to image artifacts and distortions. For instance, measures like the mean squared error respond more to additive noise, whereas others such as the spectral phase error are more sensitive to blur; while gradient-related features react to distortions concentrated around edges and textures.

Therefore, using a wide range of Image Quality Measurements (IQMs) exploiting complementary image quality properties should permit to detect the afore mentioned quality differences between real and fake samples expected to be found in many attack attempts (i.e., providing the method with multi-attack protection capabilities). All these observations lead us to believe that there is sound proof for the "quality-difference" hypothesis and that image quality measures have the potential to achieve success in biometric protection

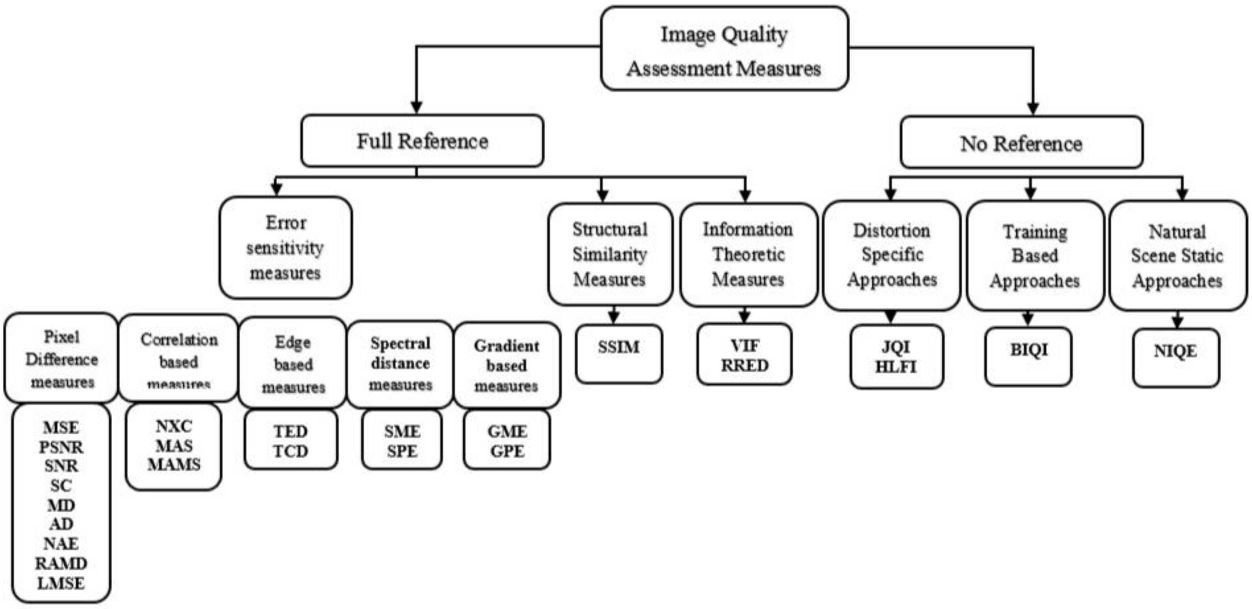
Image Quality Assessment Measures
Full Reference
No Reference
Error sensitivity measures
Structural Similarity Measures
Information Theoretic Measures
Distortion Specific Approaches
Training Based Approaches
Natural Scene Static Approaches
Pixel Difference measures
Correlation based measures
Edge based measures
Spectral distance measures
Gradient based measures
SSIM
VIF RRED
JQI HLFI
BIQI
NIQE
MSE PSNR SNR SC MD AD NAE RAMD LMSE
NXC MAS MAMS
TED TCD
SME SPE
GME GPE

Fig 2. Classification of the 25 image quality measures

tasks. Fig.2 shows the classification of different parameters under Full Reference IQA(FR-IQA) and No Reference IQA(NR-IQA) and Table I indicates the details of the features[9]. FR-IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample whereas NR-IQA algorithms try to handle the very complex and challenging problem of assessing the visual quality of images without the reference sample.

IV. DATASET

The Image Quality Analysis was carried out on Iris and Fingerprint biometrics. To carry out the work the images from the databases, [A]Iris (LivDet 09) and fingerprint[B] (ATVS-Flr DB) were used.

From [A]Iris (LivDet 09) database, data was obtained from 5 persons, in which each person left eye images were captured in 10 different sessions in different conditions. In same way right eye images of same person were captured .Therefore, 100 Images were obtained for 5 persons in real category. Similarly fake samples of the same 5 persons were obtained for both eyes using different spoofing techniques. Therefore, there are 100 images for the fake samples. Fig. 3 shows Iris sample images in which it has 5 users original images (top row) and same 5 users fake images (bottom).

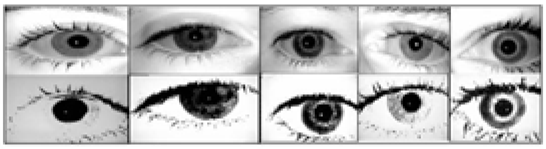

Fig 3. Input Iris images to the system

From Fingerprint[B] (ATVS-Flr DB) database, data was obtained from 5 persons, in which each person left thumb impression were captured in 20 different sessions in different conditions. Therefore, 100 Images were obtained for 5 persons in real category. Similarly fake samples of the 5 persons were obtained using different spoofing techniques. Therefore, there are 100 Images for fake samples. Fig.4 shows Fingerprint sample images in which it has 5 users original images (top row) and same 5 users fake images (bottom).

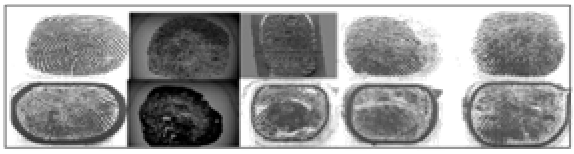

Fig 4. Input Fingerprint images to the system

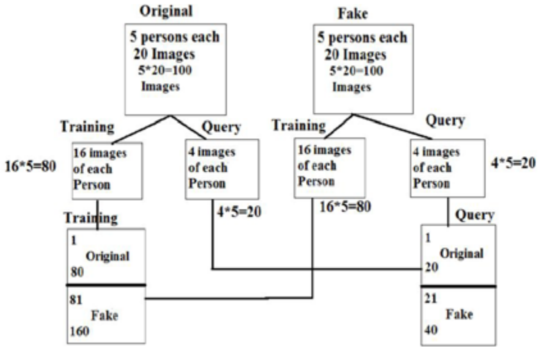

Fig 5. Classification of dataset

In dataset as said before, there are 100 real images and 100 fake images. These images are separated in to

[a] datasets@livdet.org
[b] http://atvs.ii.uam.es/

training and query set as shown in the Fig. 5. Out of real images, 80% of the images are considered for training purpose and remaining 20% of the images are separated into query set. Similarly even for the fake images 80% of the images are grouped into training set and 20% of the images are grouped into query.

In training set, 16 real Images and 16 fake Images of each person are present, therefore a total of 160 images of 5 persons are present. In query set 4 fake Images and 4 real Images of each person are present, therefore a total of 40 images of 5 persons are present. The images in the training set are used during the training phase, and the images in query set are used during the testing phase which is discussed in next section.

Mean Square Error (MSE)	$\mathrm{MSE}(I,\hat{I}) = \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})^2$
Peak Signal to Noise Ratio (PSNR)	$\mathrm{PSNR}(I,\hat{I}) = 10\log(\frac{\max(I^2)}{\mathrm{MSE}(I,\hat{I})})$
Signal to Noise Ratio (SNR)	$\mathrm{SNR}(I,\hat{I}) = (\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{N.M.\mathrm{MSE}(I,\hat{I})})$
Structural Content (SC)	$\mathrm{SC}(I,\hat{I}) = (\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{I}_{i,j})^2})$
Maximum Difference(MD)	$\mathrm{MD}(I,\hat{I}) = \max \lvert I_{i,j} - \hat{I}_{i,j}\rvert$
Average Difference (AD)	$\mathrm{AD}(I,\hat{I}) = \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})$
Normalized Absolute Error (NAE)	$\mathrm{NAE}(I,\hat{I}) = (\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j}-\hat{I}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}I_{i,j}})$
R-Averaged MD(RAMD)	$\mathrm{RAMD}(I,\hat{I},R) = \frac{1}{R}\sum_{r=1}^{R} max_r \lvert I_{i,j} - \hat{I}_{i,j}\rvert$
Laplacian MSE(LMSE)	$\mathrm{LMSE}(I,\hat{I}) = (\frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(I_{i,j})-h(\hat{I}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}h(I_{i,j})^2})$
Normalized Cross-Correlation (NXC)	$NXC(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j}.\hat{I}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})2}$
Mean Angle Similarity (MAS)	$\mathrm{MAS}(I,\hat{I}) = 1 - \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}\propto_{i,j}$
Mean Angle Magnitude Similarity (MAMS)	$MAMS(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(1-[1-\alpha_{i,j}]\left[1-\frac{\lVert I_{i,j}-\hat{I}_{i,j}\rVert}{255}\right]\right.$
Total Edge Difference (TED)	$TED(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{Ei,j} - \hat{I}_{Ei,j}\rvert$
Total Corner Difference (TCD)	$TCD(I,\hat{I}) = \frac{\lvert N_{cr} - N_{cr}\rvert}{\max(N_{cr}, N_{cr})}$
Spectral Magnitude Error (SME)	$SME(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert F_{i,j}\rvert - \lvert\hat{F}_{i,j}\rvert)2$
Spectral Phase Error (SPE)	$SPE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(F_{i,j}) - \arg(\hat{F}_{i,j})\rvert 2$
Gradient Phase Error (GPE)	$GPE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(G_{i,j}) - \arg(\hat{G}_{i,j})\rvert 2$
Structural Similarity Index Measurement (SSIM)	$SSIM(I,\hat{I}) = [(l_{i,j})^{\propto}][(c_{i,j})^{\beta}]\,[(s_{i,j})^{\gamma}]$
Gradient Magnitude Error (GME)	$GME(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert G_{i,j}\rvert - \lvert\hat{G}_{i,j}\rvert)2$
Visual Information Fidelity (VIF)	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.
Reduced Reference Entropy Difference (RRED)	$RRED_k^{\Lambda_k} = \frac{1}{L_k}\sum_{\lambda=1}^{\Lambda_k}\lvert g_{\lambda k}^{r} - g_{\lambda k}^{d}\rvert.$
Jpeg Quality Index (JQI)	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
High Low Frequency Index (HLFI)	$HLFI = \frac{\sum_{i=1}^{i_l}\sum_{j=1}^{j_l}\lvert\mathbf{F}_{i,j}\rvert - \sum_{i=i_h+1}^{N}\sum_{j=j_h+1}^{M}\lvert\mathbf{F}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{F}_{i,j}\rvert}$
Blind Image Quality Index Measurement (BQIM)	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)
Naturalness Image Quality Evaluator (NIQE)	The NIQE is a completely blind image quality analyzer based on the construction of a quality aware collection of statistical features

Table 1. Details of the Features

V. METHODOLOGY

A. *Block diagram*

The block diagram gives the methodology of the system. The input image is unseen image of either iris or fingerprint. Then the features from the query image are extracted and then it is classified using a classifier Quadratic Discriminative Analysis [10].

a) 2D image: It is the image given to the system, to be classified as real or fake. Images used in this project are of size 640x480 in case of iris images, for fingerprint images it is 300 x 300. In order to classify this image, all the parameters of this input image is being calculated.

b) Full-Reference IQ Measures: The input grey-scale image I (of size N × M) is filtered with a low-pass Gaussian kernel (σ = 0.5 and size 3 × 3) in order to generate a smoothed version Î. Then, the quality between both images (I and Î) is computed according to the corresponding full-reference IQA metric this approach assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples. Here 21 IQM parameters are extracted.

c) No-Reference IQ Measures: Unlike the objective reference IQA methods, in general the human visual system does not require of a reference sample to determine the quality level of an image. Automatic no-reference image quality assessment (NR-IQA) algorithms try to handle the very complex and challenging problem of assessing the visual quality of images, in the absence of a reference. Here 4 NR IQM parameters are extracted.

d) Final Parametrization: All the features or parameters of the given input image are being tabulated in the form of matrix in-order to make it easy for the classifier.

e) Training data: This contains the values of all parameters of 160 images used for training purpose in the form of 160x25 size matrix.

f) Classification:

i. Iris: For the iris modality the protection method is tested under two different attack scenarios, namely: (i) Spoofing attack and (ii) Attack with synthetic samples. For each of the scenarios a specific pair of real-fake databases is used. Databases are divided into totally independent (in terms of users): train set, used to train the classifier; and test set, used to evaluate the performance of the proposed protection method.

ii. Fingerprints: As in the iris experiments, the database are divided into a: train set, used to train the classifier; and test set, used to evaluate the performance of the protection method. In order to generate totally unbiased results, there is no overlap between both sets (i.e., samples corresponding to each user are just included in the train or the test set). The classifier used in this project is quadratic discriminant analyser.

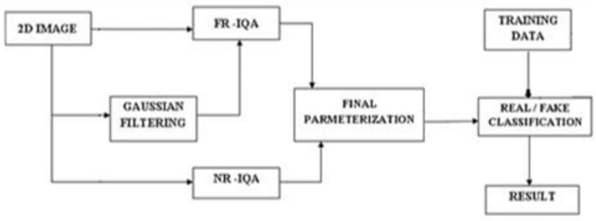

Fig 6. Block diagram of IQA

B. Implementation Phases

The work was carried out in 2 phases, namely

a) Training phase

b) Testing phase

a) Training phase

For training phase 80% of images from both the databases were used. For each image 25 parameters were calculated with this a training dataset of dimension 160x27 was obtained for both iris and fingerprint. The dataset is then labelled, trained and validated where it includes both real and fake images using quadratic classifier.

b) Testing Phase

For testing the system 40% of the images were considered these images do not overlap with Training data. These are unseen images for the system, for each of the image 25 parameters are calculated and applied to quadratic analyser, such that the classifier predicts whether the image given to the system is class 1/original or class 2/fake. And the efficiency of classifier is obtained.

VI. Results And Discussion

The entire work was carried out on two biometrics Iris and Finger print, using MATLAB 2014a(v8.3) 0n windows 7 platform. The databases obtained for Iris(ATVS-Flr DB) and Fingerprint(Livedet09) was subdivided into two sets Training and query (which is discussed in the section IV). Therefore in each of Iris and fingerprint training set there are 160 images which include both real and fake images, all these 160 images were first passed through Gaussian filter.

The input grey-scale image I (of size 640x480) is filtered with a low-pass Gaussian kernel (σ = 0.5 and size 3 × 3) in order to generate a smoothed version Î. Then, the quality between both images (I and Î) is computed according to the corresponding full-reference IQA metric this approach assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples. Using Gaussian filtered image as the reference image all 27 IQA parameters from 160 training images (which include both Fake and Real) from iris data set were extracted and stored in a form of 160x27 matrix. Similarly 27 IQA parameters were computed for Finger print data set to obtain a matrix of parameters of dimension 160x27. These values are labeled and then loaded into the quadratic discriminant classifier in order to train the system.

After training the system to differentiate between fake and real image an input unseen image from the query set is selected and given to the implemented program. Image is first pre-processed in order to extract the features, which describe its contents. The processing involves filtering normalization segmentation and object identification, which is already discussed.

Then using the filtered image, all the 27 parameters are calculated and then put into a form of matrix 1x27, which is then given as input to quadratic discriminant classifier. By using all the parameters, as it is already trained, classifier classifies the given input image as real or fake as shown in the Figures 7 and 8 and Table II. In order to calculate the efficiency of the implemented system, we considered

Actual class- Here CLASS 1 was considered as real images, CLASS 2 as Fake images. In actual class, we actually know which image belongs to class 1 or class 2, which was indicated in database.

Predicted class- It is the class predicted by the system when the unseen sample is given to the system after training the system.

All the query images of both iris and fingerprint were tested. Deviation from the predicted result was tabulated that provides classification error, which is defined as difference of predicted class and actual class. If its 0 then it implies that the image is been classified correctly or else it shows there is an error in classification of image.

After tabulation, the accuracy of the system was calculated using

$$\text{Accuracy} = \frac{\text{(Number of True classification)}}{\text{(Total number of classifications)}}$$

and Error = 1-Accuracy

Query Images	*Fingerprint*			*Iris*		
	PC	*AC*	*CE*	*PC*	*AC*	*CE*
1	2	2	0	2	2	0
2	2	2	0	2	2	0
3	2	2	0	2	2	0
4	2	2	0	2	2	0
5	2	2	0	2	2	0
6	2	2	0	2	2	0
7	2	2	0	2	2	0
8	2	2	0	2	2	0
9	2	2	0	2	2	0
10	2	2	0	2	2	0
11	2	2	0	1	2	-1
12	2	2	0	2	2	0
13	2	2	0	2	2	0
14	2	2	0	2	2	0
15	1	2	-1	2	2	0
16	2	2	0	2	2	0
17	2	2	0	2	2	0
18	2	2	0	2	2	0
19	2	2	0	2	2	0
20	2	2	0	2	2	0
21	1	1	0	1	1	0
22	1	1	0	1	1	0
23	1	1	0	1	1	0
24	1	1	0	1	1	0
25	1	1	0	1	1	0
26	1	1	1	1	1	0
27	2	1	0	1	1	0
28	1	1	0	1	1	0
29	1	1	0	1	1	0
30	1	1	0	1	1	0
31	1	1	0	1	1	0
32	1	1	0	1	1	0
33	1	1	0	1	1	0
34	1	1	0	1	1	0
35	2	1	0	1	1	0
36	1	1	0	1	1	0
37	1	1	0	2	1	0
38	1	1	0	1	1	0
39	1	1	0	1	1	0
40	1	1	0	1	1	0

Table 2. Classification error PC: Predicted Class, AC: Actual Class, CE: Classification Error

Parameters	*Iris*	*Fingerprint*
Number of query images	40	40
Number of images correctly classified	38	37
Number of errors	2	3
Efficiency of the system (%)	95	92.5
Error Rate	0.05	0.075

Table 3. Efficiency Calculation Table

Efficiency of the implemented system for the iris data obtained was 95% whereas efficiency for the fingerprint obtained was 92.5%, with the error rates for iris, fingerprint to be 0.05 and 0.075 respectively.

Fig.7 shows the plot for Classification Error of Iris. In the plot, zeroes indicate that the respective query images were classified correctly, where deviations from the zeroes indicate that the respective query images were not properly classified.

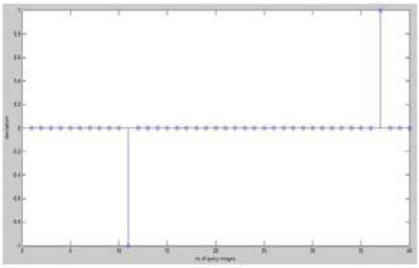

Fig 7. Plot for Classification Error of Iris

Fig.8 shows the plot for Classification Error of Iris. In the plot, zeroes indicate that the respective query images were classified correctly, where deviations from the zeroes indicate that the respective query images were not properly classified.

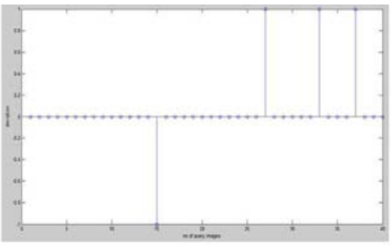

Fig 8. Plot for Classification Error of Fingerprint

VII. Conclusion

Image Quality Assessment was carried out to detect the fake biometric samples from the query images. The simulation results obtained with the proposed method are shown in Table III.

An Accuracy of 95%was obtained with iris database and 92.5% was obtained with fingerprint database. This clearly shows that the efficiency of the proposed system is higher than the previous systems and can come handy in implementation of other biometric security systems.

The other conclusion we can make through this system is that IQA technique can be effectively used to classify the biometric input samples into real and fake categories with higher efficiency and low error rates.

REFERENCES

[1] 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.

[2] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, “Can gait biometrics be spoofed?” in Proc. IAPR ICPR, 2012, pp. 3280–3283

[3] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, “Iris liveness detection based on quality related features,” in Proc. 5th IAPR ICB, Mar./Apr. 2012, pp. 271–276.

[4] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, “On the vulnerability of face verification systems to hill-climbing attacks,” Pattern Recognit., vol. 43, no. 3, pp. 1027–1038, 2010.

[5] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.

[6] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, “Evaluation of direct attacks to fingerprint verification systems,” J. Telecommun. Syst., vol. 47, nos. 3–4, pp. 243–254, 2011.

[7] (2010). Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available: http://www.tabularasa-euproject.org/

[8] ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.

[9] I. Avcibas, B. Sankur, and K. Sayood, “Statistical evaluation of image quality measures,” J. Electron. Imag., vol. 11, no. 2, pp. 206–223, 2002.

[10] McLachlan, G. (2004). Discriminant analysis and statistical pattern recognition (Vol. 544). John Wiley & Sons.