International Journal of Engineering and Techniques - Volume 3 Issue 1, Jan – Feb 2017

RESEARCH ARTICLE OPEN ACCESS

Fake Biometric Detection using Image Quality Assessment for Enhancement of Security

Madhavi B. Danane[1], Vikram A. Mane[2]

Department of Electronics and Telecommunication, Shivaji university, Kolhapur.
Assistant professor, Department of Electronics and Telecommunication, Annasaheb Dange college of Engineering, Ashta affiliated to Shivaji university, Kolhapur, India.

Abstract:

To ensure that the object presented in front of biometric device is real or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. This paper, presents a software-based fake biometric detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition devices through the use of image quality assessment in a fast and user friendly manner. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image to distinguish between real and imposed samples. The proposed method is highly competitive compared with other as the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits.

Keywords — **Image Quality Assessment (IQA), Biometrics, security, *attacks*, countermeasures.**

I. INTRODUCTION

Security is main aspect of any organization, to improve security and privacy now a day's automatic access of persons to services is becoming increasingly important. This leads to a new technology known as biometric recognition. The basic aim of biometrics is to discriminate automatically between subjects in a reliable way and application based on one or more signals derived from physical or behavioral traits, such as fingerprint, face, iris, voice, hand, or written signature. Biometric technology presents several advantages over classical security methods. It is not required to carry key or card and remember password or PIN every time that could be lost or stolen.

However, along with these advantages biometric systems present a number of drawbacks such as the lack of secrecy as it is possible to access face pictures from social media or can be clicked unknowingly, anybody could get finger prints. Among the different threats analyzed, the *direct* or *spoofing* attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris [2], the fingerprint [3], the face [2], the signature [4], or even the gait [5] and multimodal approaches [6]. 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. 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 research studies on vulnerabilities in fake biometric detection have clearly shown the necessity to propose and develop specific protection methods against this threat. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them, improving the robustness and security level of the systems.

Besides other anti-spoofing approaches such as the use of multibiometrics or challenge-response methods, special attention has been paid by researchers and industry to the *liveness detection* techniques. Liveness detection methods are usually classified into one of two groups (see Fig. 1): *(i) Hardware-based* techniques, which add some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye); *(ii)Software-based* techniques, in this case the fake trait is detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself).

The 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. Hardware-based 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. Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself). [7], [8].The present work we propose a suited to operate on real scenarios.

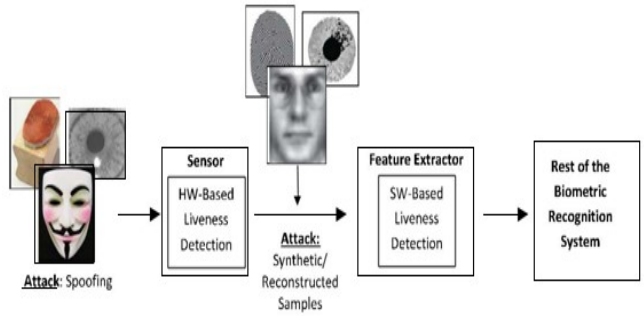


Fig.1. Block diagram showing different types of attacks

II. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

The use of image quality assessment for liveness detection is motivated by the assumption that "*It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed.*"

Expected quality differences between real and fake samples may 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. For example, iris images captured from a printed paper are more likely to be blurred or out of focus due to trembling; face images captured from a mobile device will probably be over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local acquisition artifacts such as spots and patches. Furthermore, 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.

By using this "*quality-difference*" hypothesis, in the present research work the proposed work explore the potential of *general* image quality assessment as a protection method against different biometric attacks.

III. METHOD FOR ENHANCEMENT OF SECURITY

A. Face Recognition System:

software-based multi-biometric and multi-attack protection method through the use of image quality assessment (IQA). It is capable of operating with a very good performance under different biometric systems. Being software-based, it presents the usual advantages of this type of approaches: fast, as it only needs one image (i.e., the same sample acquired for biometric recognition) to detect whether it is real or fake; non-intrusive; user-friendly, cheap and easy to embed in already functional systems. An added advantage of the proposed technique is it's speed and very low complexity, which makes it very wel

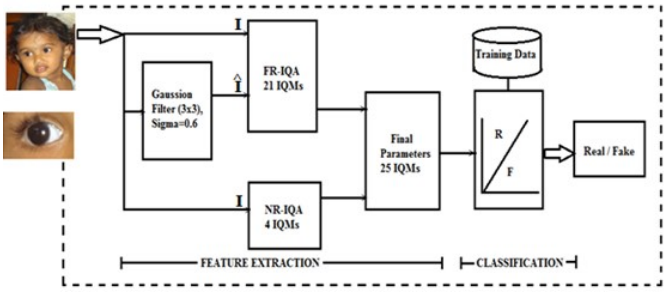


Fig.2. Block diagram of biometric protection method based on Image Quality Assessment in proposed work.

A block diagram of the proposed work is shown in Fig. 3.1. The system needs only one input the biometric sample to be classified as real or fake which is the same image acquired for biometric recognition purposes. In the problem of fake detection addressed in this work is reference image is unknown, as the detection system only has access to the input sample. This limitation is recovered using the same Gaussian filter. As shown in Fig. 2, the input grayscale image $\boldsymbol{I}$ (of size $N \times M$) is filtered with a low-pass Gaussian kernel ($\sigma = 0.5$ and size 3×3) in order to generate a smoothed version $\hat{\boldsymbol{I}}$. Then, the quality between both images ($\boldsymbol{I}$ and $\hat{\boldsymbol{I}}$) is computed according to the corresponding full-reference IQA metric [6]. Once the feature vector has been generated the sample is classified as real or fake, using some simple classifiers. For proposed work standard implementations in Matlab of the Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) classifiers are used.

As the method operates on the whole image it does not require any preprocessing steps like fingerprint segmentation, iris detection or face extraction prior to the computation of the IQ features. This characteristic minimizes its computational load.

B. IQA Measures Selection:

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 result whether the image is real or fake depending upon

extracted set of features. The features are selected according to following criteria

- *Performance*- Only widely used image quality approaches which have been consistently tested showing good performance for different applications have been considered.
- *Complementarities*- In order to generate a system as general as possible in terms of attacks detected and biometric modalities supported, priority is given to IQMs based on complementary properties of the image (e.g., sharpness, entropy or structure).
- *Complexity*- In order to keep the simplicity of the method, low complexity features has been preferred over those which require a high computational load.
- *Speed*- To assure a user-friendly non-intrusive application, users should not be kept waiting for a response from the recognition system. For this reason, big importance has been given to the feature extraction time, which has a very big impact in the overall speed of the fake detection algorithm.

The 25 measures which reduce complexity and computation are explained below. Out of these 25 selected measures for the present work we have considered 11 FR-IQAs and 2 NR-IQAs

Full-Reference IQ Measures:

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample.

(i) FR-IQMs: Error Sensitivity Measures: Traditional image quality assessment approaches are based on measuring the errors (i.e., signal differences) between the distorted and the reference images as they are easy to calculate and usually have very low computational complexity these features have been classified here into five different

- Pixel Difference measures [7], [8] - These features compute the distortion between two images on the basis of their pixel wise differences. In proposed work following measures are included: Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Structural Content (SC), Maximum Difference (MD), Average Difference (AD), Normalized Absolute Error (NAE), R-Averaged Maximum Difference (RAMD), (R=10 is considered in proposed work) and Laplacian Mean Squared Error (LMSE).
- Correlation-based measures [7], [8] - The similarity between two digital images can also be quantified interims of the correlation function. A variant of correlation-based measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and distorted images. These features include Normalized Cross-Correlation (NXC), Mean Angle Similarity (MAS) and Mean Angle-Magnitude Similarity (MAMS) defined in Table I where $\alpha_{i,j}$ denotes the angle between two vectors $(\mathbf{I}i, j, \hat{\mathbf{I}}i, j)$ denotes the scalar product.
- Edge-based measures- Edges and other two-dimensional features such as corners are some of the most informative parts of an image, which play a key role in the human visual system and in many computer vision algorithms including quality assessment applications [9]. Since the structural distortion of an image is tightly linked with its edge degradation two edge-related quality measures are considered Total Edge Difference (TED) and Total Corner Difference (TCD).
- Spectral distance measures- The Fourier transform is another traditional image processing tool which has been applied to the field of image quality assessment [7]. In this work following spectral-related features are: the Spectral Magnitude Error (SME) and the Spectral Phase Error (SPE) defined in Table 3.1 where $\boldsymbol{F}$ and $\hat{\boldsymbol{F}}$ are the respective Fourier transforms of $\boldsymbol{I}$ and $\hat{\boldsymbol{I}}$), and arg$(\mathbf{F})$ denotes phase.
- Gradient-based measures- Gradients convey important visual information which can be of great use for quality assessment. Many of the distortions that can affect an image are reflected by a change in its gradient. Therefore, using such information, structural and contrast changes can be effectively captured [15].Two simple gradient-based features are included in thebiometric protection system proposed in the present article: Gradient Magnitude Error (GME) and Gradient Phase Error (GPE) defined in Table 3.1 where $\boldsymbol{G}$ and $\hat{\boldsymbol{G}}$ are the gradient maps of $\boldsymbol{I}$ and $\hat{\boldsymbol{I}}$ defined as $\boldsymbol{G} = \boldsymbol{G}x+i\boldsymbol{G}y$, where $\boldsymbol{G}x$ and $\boldsymbol{G}y$ are the gradients in the x and y directions..

(ii) Structural Similarity Measures: Error sensitivity measures are convenient and widely used but when compared with human visual system they present several problems therefore quality assessment based on structural similarity was proposed following the hypothesis that the human visual system is highly adapted for extracting structural information from the viewing field [10]. Therefore, distortions in an image that come from variations in lighting, such as contrast or brightness changes (nonstructural distortions), should be treated differently from structural ones. The Structural Similarity Index Measure (SSIM) has the simplest formulation and has gained widespread popularity in a broad range of practical applications [10], [16].

(iii) Information Theoretic Measures: The quality assessment problem may also be understood, from an information theory perspective, as an information-fidelity problem (rather than a signal-fidelity problem). The core idea behind these approaches is that an image source communicates to a receiver through a channel that limits the amount of information that could flow through it, thereby

introducing distortions. The goal is to relate the visual quality of the test image to the amount of information shared between the test and the reference signals, or more precisely, the mutual information between them. Under this general framework, image quality measures based on information fidelity exploit the relationship between statistical image information and visual quality.

The Visual Information Fidelity (VIF) and the Reduced Reference Entropic Difference index (RRED) [11] metrics are based on the information theoretic perspective of IQA but each of them take either a global or a local approximation to the problem. The VIF metric measures the quality fidelity as the ratio between the total information measured in terms of entropy ideally extracted by the brain from the whole distorted image and the total information conveyed within the complete reference image. This metric relies on the assumption that natural images of perfect quality, in the absence of any distortions, pass through the human visual system (HVS) of an observer before entering the brain, which extracts cognitive information from it. For distorted images, it is hypothesized that the reference signal has passed through another "distortion channel" before entering the HVS. The VIF measure is derived from the ratio of two mutual information quantities: the mutual information between the input and the output of the HVS channel when no distortion channel is present (i.e., reference image information) and the mutual information between the input of the distortion channel and the output of the HVS channel for the test image. Therefore, to compute the VIF metric, the entire reference image is required as quality is assessed on a global basis.

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. The RRED algorithm computes the average difference between scaled local entropies of wavelet coefficients of reference and projected distorted images in a distributed fashion. This way, contrary to the VIF feature, for the RRED it is not necessary to have access the entire reference image but only to a reduced part of its information. This required information can even be reduced to only one single scalar in case all the scaled entropy terms in the selected wavelet sub band are considered in one single block.

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. Following this same principle, 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. NR-IQA methods generally estimate the quality of the test image according to some pre-trained statistical models. Depending on the images used to train this model and on the priori knowledge required, the methods are coarsely divided into one of three trends

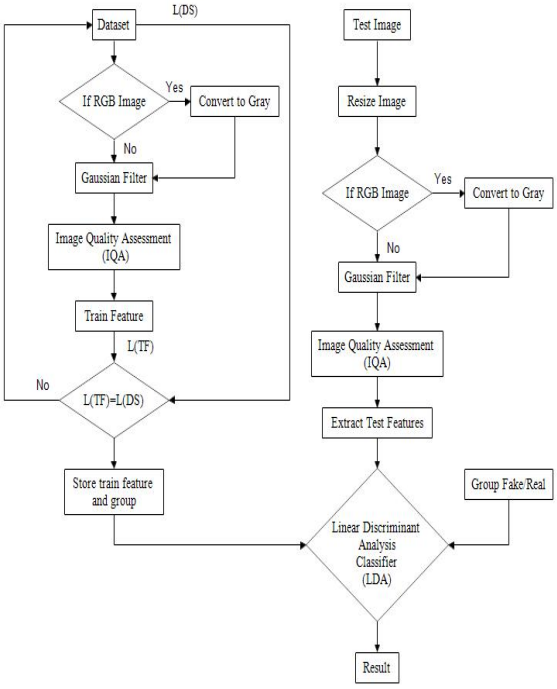
- Distortion-specific approaches- These techniques rely on previously acquired knowledge about the type of visual quality loss caused by a specific distortion. The final quality measure is computed according to a model trained on clean images and on images affected by this particular distortion. The 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. The High-Low Frequency Index (HLFI), which was inspired by previous work which considered local gradients as a blind metric to detect blur and noise. 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. In the HLFI entry in Table 3.1, i_l , i_h , j_l , j_h are respectively the indices corresponding to the lower and upper frequency thresholds considered by the method [12].
- Training-based approaches- Similarly to the previous class of NR-IQA methods, in this type of techniques a model is trained using clean and distorted images. Then, the quality score is computed based on a number of features extracted from the test image and related to the general model. However, unlike the former approaches, these metrics intend to provide a general quality score not related to a specific distortion. To this end, the statistical model is trained with images affected by different types of distortions. This is the case of the Blind Image Quality Index (BIQI), which is part of the 25 feature set used in the present work. The BIQI follows a two-stage framework in which the individual measures of different distortion-specific experts are combined to generate one global quality score [13].
- Natural Scene Statistic approaches- These blind IQA techniques use *a priori* knowledge taken from natural scene distortion-free images to train the initial model. The reason behind this trend relies on the hypothesis that undistorted images of the natural world present certain *regular* properties which fall within a certain subspace of all possible images. If quantified appropriately, deviations from the regularity of natural statistics can help to evaluate the perceptual quality of an image. This approach is followed by the Natural 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 derived from a corpus of natural undistorted images related to a multi variant Gaussian natural scene statistical model [14].

TABLE I LIST OF 25 IMAGE QUALITY MEASURES USED FOR BOMETRIC PROTECTION

Sr.	Type	Acronym	Name	Ref.	Description
Full Reference Parameters					
1.	FR	MSE	Mean Squared Error	7	$MSE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})^2$
2.	FR	PSNR	Peak Signal To Noise Ratio	21	$PSNR(I,\hat{I}) = 10\log(\frac{\max(I^2)}{MSE(I,\hat{I})})$
3.	FR	SNR	Signal To Noise Ratio	22	$SNR(I,\hat{I}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{N.M.MSE(I,\hat{I})})$
4.	FR	SC	Structural Content	8	$SC(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{I}_{i,j})^2}$
5	FR	MD	Maximum Difference	8	$MD(I,\hat{I}) = max\lvert I_{i,j} - \hat{I}_{i,j}\rvert$
6	FR	AD	Average Difference	8	$AD(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})$
7	FR	NAE	Normalized Absolute Error	8	$NAE(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j} - \hat{I}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j}\rvert}$
8	FR	RAMD	R-Averaged MD	22	$RAMD(I,\hat{I},R) = \frac{1}{R}\sum_{r=1}^{R} max_r\lvert I_{i,j} - \hat{I}_{i,j}\rvert$
9	FR	LMSE	Laplacian MSE	8	$LMSE(I,\hat{I}) = \frac{\sum_{i=1}^{N-1}\sum_{j=1}^{M-1}(h(I_{i,j}) - h(\hat{I}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=1}^{M-1}h(I_{i,j})^2}$
10	FR	NXC	Normalized Cross-Correlation	8	$NXC(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j}.\hat{I}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{I}_{i,j})^2}$
11	FR	MAS	Mean Angle Similarity	7	$MAS(I,\hat{I}) = 1 - \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\alpha_{i,j})$
12	FR	MAMS	Mean Angle Magnitude Similarity	7	$MAMS(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1 - [1-\alpha_{i,j}]\left[1 - \frac{\lVert I_{i,j} - \hat{I}_{i,j}\rVert}{255}\right])$
13	FR	TED	Total Edge Difference	9	$TED(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{Ei,j} - \hat{I}_{Ei,j}\rvert$
14	FR	TCD	Total Corner Difference	9	$TCD(I,\hat{I}) = \frac{\lvert N_{cr} - \hat{N}_{cr}\rvert}{\max(N_{cr},\hat{N}_{cr})}$
15	FR	SME	Spectral Magnitude Error	23	$SME(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert F_{i,j}\rvert - \lvert\hat{F}_{i,j}\rvert)^2$
16	FR	SPE	Spectral Phase Error	23	$SPE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(arg\lvert F_{i,j}\rvert - arg\lvert\hat{F}_{i,j}\rvert)^2$

17	FR	GME	Gradient Magnitude Error	24	$GME(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert G_{i,j}\rvert - \lvert \hat{G}_{i,j}\rvert)^2$
18	FR	GPE	Gradient Phase Error	24	$GPE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(arg\lvert G_{i,j}\rvert - arg\lvert \hat{G}_{i,j}\rvert)^2$
19	FR	SSIM	Structural Similarity Index Measurement	10	Built In function in MATLAB R2015a
20	FR	VIF	Visual Information Fidelity	25	
21	FR	RRED	Reduced Reference Entropic Difference	11	
No Reference parameters					
22	NR	JQI	JPEG Quality Index	12	
23	NR	HLFI	High-Low Frequency Index	12	$HLFI(I) = \frac{\sum_{i=1}^{i_k}\sum_{j=1}^{j_l}\lvert F_{i,j}\rvert - \sum_{i=i_{k+1}}^{N}\sum_{j=j_{k+1}}^{M}\lvert F_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert F_{i,j}\rvert}$
24	NR	BIQI	Blind Image Quality Index	13	
25	NR	NIQI	Naturalness Image Estimator	14	

. Algorithm for Face Recognition System**:**



Modules

- Test Image
- RGB to Gray Conversion
- Filter
- Extraction of Features
- Classification

Test Image:

It is the input image which we are applying to the system to detect whether it is genuine image or fraudulent image. The background scenario of each image is different. It may be controlled or adverse scenario therefore input image is processed and resized.

RGB to Gray Conversion:

Color is a powerful descriptor that often simplifies object identification and extraction from a scene and human can discern thousands of color shades and intensities. A true color image is an image in which each pixel is specified by three values one each for the red, blue, and green components of the pixel scalar. For single or double arrays, values range from [0, 1], for 8 bit RGB image, values range from [0, 255] for 16 bit RGB image, values range from [0, 65535]. Because of this wide range of values color image is very difficult to operate upon. Image formation using sensor and other image acquisition equipment denote the brightness or intensity I of the light of an image as two dimensional continuous function F(x, y) where (x, y) denotes the spatial coordinates when only the brightness of light is considered. Image involving only intensity are called gray scale images. There are 256 gray levels in an 8 bit gray scale image, and the intensity of each pixel can have values from 0 to 255, with 0 being black and 255 being white. Therefore if the image is gray image then it is processed as it is but if image is RGB image then it is converted into grayscale image.

Filter:

The input image is first filtered to get a smoothed version of the input. A Gaussian low pass filter of size 3x3 and $\sigma = 0.5$

is used. For each pixel in the image, Gaussian filter produces, a weighted average such that central pixel contributes more significantly to the result than pixels at the mask edges the weights are computed according to the Gaussian function.

Gaussian filter:

Gaussian filtering is used to blur images and remove noise. In one dimension, the Gaussian function G(x) is expressed as,

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}}$$

Where σ is the standard deviation of the distribution. The distribution is assumed to have a mean of 0.5. The Gaussian function is used in numerous research areas: It defines a probability distribution for noise or data, it is a smoothing operator, and it is used in mathematics.

Extraction of Features:

In present work Image Quality Assessment (IQA) technique is used. Out of 25 selected measures which reduce computational load and complexity for this work total 13 measures are selected.

A set of 11 FR-IQA Measures selected for proposed work are:

1. Signal to Noise Ratio
2. Peak Signal to Noise Ratio
3. Average Difference (AD)
4. Mean square error (MSE)
5. Structural Content (SC)
6. Normalized Cross-Correlation (NXC)
7. Maximum Difference(MD)
8. Laplacian Mean Square Error (LMSE)
9. Normalized Absolute Error (NAE)
10. Structural Similarity Index (SSI)
11. R-Averaged Maximum Difference (RAMD)

NR-IQA Measures selected for proposed work are:

1. Blind Image Quality Index (BIQI)
2. Naturalness Image Quality Estimator (NIQE)

Image quality assessment approaches are based on measuring the errors (i.e., signal differences) between the distorted and the reference images, and attempt to quantify these errors in a way that simulates human visual error sensitivity features. These are probably the most widely used methods for IQA as they conveniently make use of many known psychophysical features of the human visual system they are easy to calculate and usually have very low computational complexity. These features compute the distortion between two images on the basis of their pixel wise differences

Classification:

For Face detection Linear Discrminant Analysis classifier is used and for Iris recognition Quadratic Discriminant Analysis Classifier is used. LDA is a classification method originally developed in1936 by R. A. Fisher. It is simple, mathematically robust and often produces models whose accuracy is as good as more complex methods. In Linear discriminant analysis we provide the following steps to discriminant the input images.

Step1: We need a training set composed of a relatively large group of subjects with diverse characteristics. The appropriate selection of the training set directly determines the validity of the final results. The database should contain several examples of biometric images for each subject in the training set and at least one example in the test set. These examples should represent different frontal views of subjects with minor variations in view angle. They should also include different facial expressions, different lighting and background conditions, and examples with and without glasses. All images are normalized to m x n arrays.

Step 2: For each image and sub image, starting with the two dimensional m x n array of intensity values I(x, y), we construct the vector expansion φ (m x n). This vector corresponds to the initial representation of the face. Thus the set of all faces in the feature space is treated as a high-dimensional vector space. For the proposed work we have considered set of 13 parameters so vector Z is represented as

$Z=\beta1x1+\beta2x2+\beta3x3+\beta4x4+\beta5x5+\ldots\ldots+\beta13x13$

Where x1, x2…..x13 are variables and β1, β2….. β13 are coefficients of vector Z.

Step 3: By defining all instances of the same person's characteristics as being in one class and of different subjects as being in different classes for all subjects in the training set, we establish a framework for performing a cluster separation analysis in the feature space. Also having labeled all instances in the training set and having defined all the classes, we compute the within-class and between-class scatter matrices.

IV. RESULTS

The database of 50 different subjects is collected with a resolution of 300X300 and experiment is performed on collected database. Simple classifier based on general IQMs is built and results are reported in terms of: the False Genuine Rate (FGR), which accounts for the number of false samples that were classified as real and the False Fake Rate (FFR), which gives the probability of an image coming from a genuine sample being considered as fake. The Half Total Error Rate (HTER) is computed as HTER = (FGR + FFR)/2.

Results: 2D Face

For fake face detection a specific pair of real-fake data-bases is used. Databases are divided into totally independent train set, used to train the classifier; and test set, used to evaluate the performance of the proposed protection method. The

database for face recognition contains 50 users × 2 images (one Real and one fake) × 2 sessions (Test set and train set) = 200 images. The classifier used for fake face detection is Linear Discriminant Analysis (LDA). Three different types of attacks were considered: *i*) *print*, illegal access attempts are carried out with hard copies of high-resolution digital photographs of the genuine users; *ii*) *mobile*, the attacks are performed using photos and videos taken with the smart phones *iii*) *highdef*, in this case the photos and videos are displayed using high definition camera 1024 × 768.

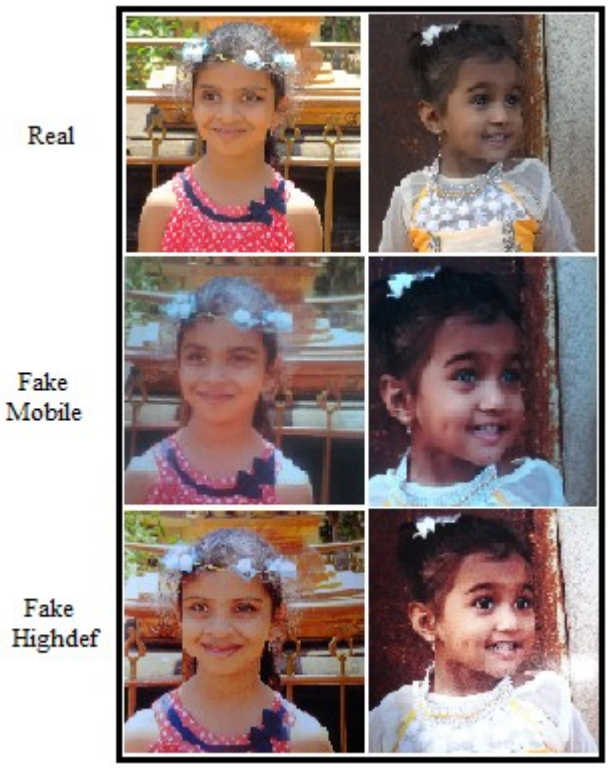


Fig. 3. Typical examples of real and fake (mobile and highdef) face images

The competition held on countermeasure to 2D facial spoofing act. Numbers of algorithms were presented to competition. These algorithms are based on motion detection of face and therefore ability to detect fake access attempts carried out with replayed motion video. Table 3 shows results of different participants using different algorithms. The results are mentioned in terms of print and motion

TABLE II
RESULTS FOR PRINT AND VIDEO SUBSETS.

Algorithm	FFR	FGR	HTER
AMILAB(Motion)	0.0	1.2	0.6
CASIA(Motion)	0.0	0.0	0.0
IDIAP (Print)	0.0	0.0	0.0
SIANI (motion)	0.0	21.2	10.6
UNIAMP(Motion)	1.2	0.0	0.6
UOULU (Print)	0.0	0.0	0.0

Table III gives quantitative performance of different algorithms on face. Results are reported in terms of the False Genuine Rate (FGR/FPR), which accounts for the number of false samples that were classified as real and the False Fake Rate (FFR/FNR), which gives the probability of an image coming from a genuine sample being considered as fake. The Half Total Error Rate (HTER) is computed as HTER = *(*FGR + FFR*)/*2 = 14.

Performance of the system is also decided by receiver operating characteristics (ROC). ROC is created plotting true positive rate (real image is classified as real) versus false positive rate (fake image is classified as real) at various threshold settings. Area under curve indicates the performance of system. Fig. 4 shows ROC curve for Face detection system and area under this curve determines performance of classifier. Performance of Face detection system using LDA classifier = 86.6%.

TABLE III
RESULTS FOR FACE RECOGNITION

Sr. No.	Algorithm	HTER
1.	LBP-LDA [17]	15.02
2.	LBP-SVM [17]	13.09
3.	DOG-SVM [18]	26.72
4.	Proposed system[1] (IQA using LDA)	14

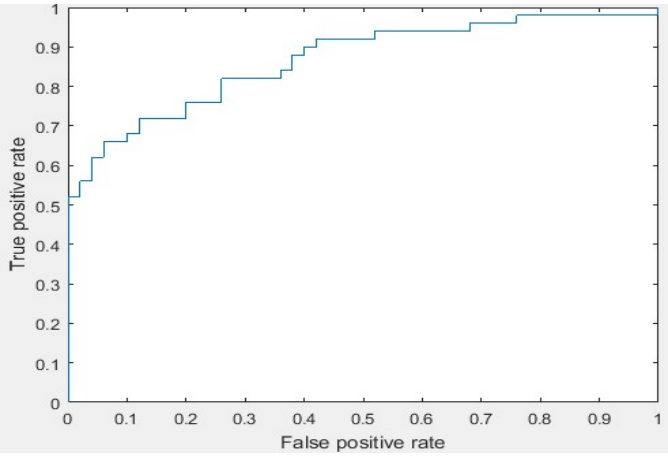


Fig. 4. ROC curves showing performance of LDA classifier for face recognition which is 86.6%.

Results: Iris

The database for iris recognition contains 15 users × 2 images (one Real and one fake) × 2 sessions (Test set and train set) = 60 images. The classifier used for fake iris detection is Quadratic Discriminant Analysis (QDA). Result is calculated in terms of Half Total Error Rate (HTER).

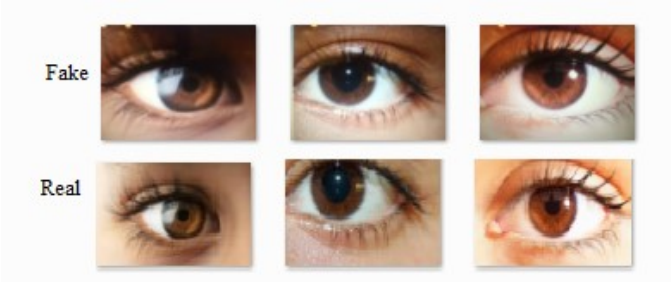


Fig. 5. Typical examples of real and fake iris images

Table IV gives quantitative performance of different algorithms on Iris. Half Total Error Rate (HTER) using QDA algorithm in present work = 2.5. Fig. 6 shows ROC curve for Iris detection system and area under this curve determines performance of classifier. Performance of Iris detection system using QDA classifier = 99.6%.

TABLE IV
RESULTS FOR IRIS RECOGNITION

Sr. No.	Algorithm	HTER
1.	Quality features [19]	3.10
2.	GLCM [20]	5.60
3.	Proposed system[1] (IQA using QDA)	2.5

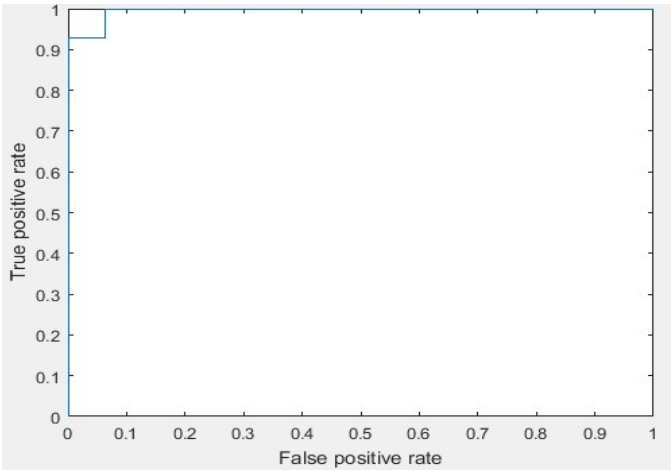


Fig. 6. ROC curves showing performance of QDA classifier for iris recognition which is 99.6%.

V. CONCLUSION

The image quality properties of real accesses and fraudulent attacks will be different. In the proposed work this "*quality-difference*" hypothesis is used and explored the potential of *general* image quality assessment as a protection tool against different biometric attack.

For this purpose feature space of 13 complementary image quality measures which have combined with simple classifiers to detect real and fake access attempts. The protection method has been evaluated on iris and 2D face.

i. The proposed method is able to consistently perform at a high level for different biometric traits ("multi-biometric");
ii. The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection ("multi-attack");
iii. The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios;
iv. The error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions;
v. In addition to its very competitive performance, and to its "multi-biometric" and "multi-attack" characteristics, the proposed method presents some other very attractive features such as it is simple, fast, non-intrusive, user-friendly and cheap, all of them very desirable properties in a practical protection system.

VI. FUTURE SCOPE

Following are the possibilities in project for future work

i. It is possible to extend 25-feature set with new image quality measures to improve the results further.
ii. Other image based modalities like palm print, Hand geometry, vein can be used for detection of fraudulent entry.
iii. In the systems which are working with face videos it is possible to include temporal information.
iv. Video quality measures can be used for video attacks.

VI. REFERENCES

[1] Javier Galbally, and Julian Fierrez Sébastien Marcel, "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] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
[3] 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.
[4] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in *Proc. IEEE 5th Int. Conf. BTAS*, Sep. 2012, pp. 283–288.
[5] S. Shah and A. Ross, "Generating synthetic irises by feature agglomeration," in *Proc. IEEE ICIP*, Oct. 2006, pp. 317–320.

[6] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," *J. Electron. Imag.*, vol. 15, no. 4, pp. 041102-1–041102-17, 2006.
[7] I. Avcibas, B. Sankur, and K. Sayood, "Statistical evaluation of image quality measures," *J. Electron. Imag.*, vol. 11, no. 2, pp. 206–223, 2002.
[8] A. M. Eskicioglu and P. S. Fisher, "Image quality measures and their performance," *IEEE Trans. Commun.*, vol. 43, no. 12, pp. 2959–2965, Dec. 1995.
[9] M. G. Martini, C. T. Hewage, and B. Villarini, "Image quality assessment based on edge preservation," *Signal Process. Image Commun.*, vol. 27, no. 8, pp. 875–882, 2012.
[10] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[11] R. Soundararajan and A. C. Bovik, "RRED indices: Reduced reference entropic differencing for image quality assessment," *IEEE Trans. Image Process.*, vol. 21, no. 2, pp. 517–526, Feb. 2012.
[12] X. Zhu and P. Milanfar, "A no-reference sharpness metric sensitive to blur and noise," in *Proc. Int. Workshop Qual. Multimedia Exper.*, 2009,pp. 64–69.
[13] 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.
[14] 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.
[15] J. Zhu and N. Wang, "Image quality assessment by visual gradient similarity," *IEEE Trans. Image Process.*, vol. 21, no. 3, pp. 919–933, Mar. 2012.
[16] D. Brunet, E. R. Vrscay, and Z. Wang, "On the mathematical properties of the structural similarity index," *IEEE Trans. Image Process.*, vol. 21, no. 4, pp. 1488–1499, Apr. 2012.
[17] I. Chingovska, A. Anjos, and S. Marcel, "on the effectiveness of local binary pattern in face anti-spoofing" *Proc. IEEE Int. Conf. Biometric Special Interest Group*, Sep. 2012, pp. 1–7.
[18] Zhiwei zhang, jnjie Yan, Sifie Liu, Zhen Lei, Dong Yi and S.Z. Li, "A face antispoofing database with diverse attacks," *in 5th IAPR International Conference on Biometrics (ICB),* March 2012, pp. 26-31.
[19] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris livenes detection based on quality related features," in *Proc. 5th IAPR ICB*, Mar./Apr. 2012, pp. 271–276.
[20] Ana F. Sequeira, Juliano Murari, and Jaime S. Cardoso, "Iris liveness detection methods in mobile applications," *in 9th International conference on Computer Vision Theory and Application*, 2013, pp. 1-5.
[21] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electron. Lett.*, vol. 44, no. 13, pp. 800–801, 2008.
[22] S. Yao, W. Lin, E. Ong, and Z. Lu, "Contrast signal-to-noise ratio for image quality assessment," in *Proc. IEEE ICIP*, Sep. 2005, pp. 397–400.
[23] N. B. Nill and B. Bouzas, "Objective image quality measure derived from digital image power spectra," *Opt. Eng.*, vol. 31, no. 4, pp. 813–825, 1992.
[24] A. Liu, W. Lin, and M. Narwaria, "Image quality assessment based on gradient similarity," *IEEE Trans. Image Process.*, vol. 21, no. 4, pp. 1500–1511, Apr. 2012.
[25] H. R. Sheikh and A. C. Bovik, "Image information and visual quality," *IEEE Trans. Image Process.*, vol. 15, no. 2, pp. 430–444, Feb. 2006.