

Biometrics Liveness Detection by Using Image Quality Assessment

[¹] Akash S. Dange, [²] Mrs. M. R. Banwaskar

[¹] M. E. Student, [²] Professor, Dept. of Electronics & Telecommunication, MGM's COE Nanded

Abstract— A biometric system is a system that uses behavioral and physiological characteristic (e.g. iris, fingerprint, face, keystroke, signature, voice) of a person to identify that person. Now days, these biometric systems are vulnerable to adversary attacks. So, the development of novel and efficient security measure is required for the identification of fake trait. In this paper, we have presented a software based multi-biometric liveness detection system which is used to identify a live trait and intruder. The proposed system uses 30 image quality measures (IQMs). These quality features are extracted from single image which is acquired for verification purpose. The present system assures that the use of liveness detection enhances security of biometric system and provides better performance and also reduces complexity of the system. It has been observed that, the proposed method is very much effective in detecting liveness of iris, fingerprint and face compared with different progressive approaches.

Index Terms— biometrics, biometric security, image quality assessment, liveness detection

I. INTRODUCTION

Biometric system is the automatic person recognition system based on physiological or behavioral characteristics. It verifies individual's identity by analyzing his physical characteristics or behaviors. Biometric characteristic must satisfy the requirements like: universality, distinctiveness, permanence and collectability.

A general biometric system contains three basic blocks that are sensing, feature extraction and template matching module. Biometric system works in two modes:

- 1) **Identification mode:** the system performs a one to many comparisons with a biometric database in order to establish the identity of an unknown user.
- 2) **Authentication mode:** the system performs one to one comparison of test biometric sample with a specific template stored in database in attempt to verify the individual.

In recent years, hackers or organized groups are trying to intrude in biometric systems for their personal gains. Most of the attackers use direct or spoofing attack to circumvent the biometric system. In this paper, we have considered this type of attack to different modalities such as iris, fingerprint and face. In spoofing attack, the intruder tries to fake genuine person's identity by presenting fake samples of that person's trait to the

acquisition sensor. In iris spoofing, the imposter may show printed image of an iris of genuine user. For fingerprint modality, gummy fingers made up of silicon or gelatin can be used by intruder. The facial photographs of genuine user can be used for face spoofing attacks. Now a day, due to information globalization biometric data of genuine user is easily available. The imposter can get user's photo and videos through various sites on internet, fingerprint molds can be easily constructed from the marks left on coffee mugs or some other materials. Several countermeasures are Proposed to overcome spoofing attacks, but liveness detection method is most popular in biometric community due to its low complexity and best performance. as the liveness detection is physiological characteristic based technique, it should satisfy following characteristics [26]: i) *noninvasive*, the technique should not be harmful to the user. ii) *user-friendly*, user must not be reluctant to use it. iii) *fast*, results should be created in a short time because the user should not wait for detector's response for a long time. iv) *low price*, large number of people cannot use the system if the cost is high. v) *performance*, additionally to get a decent pretend detection rate, the liveness detection method should maintain good performance of the system.

Liveness detection method can be categorized into two types:

- i) **Hardware Based Technique:** In this method, a specific hardware is added to a sensor, to detect particular properties of living trait

**International Journal of Engineering Research in Electronics and Communication
Engineering (IJERECE)
Vol 3, Issue 9, September 2016**

(e.g. fingerprint sweat, blood pressure or specific reflection properties of the eye).

- ii) **Software Based Technique:** The fake trait is detected once the sample has been acquired with the standard sensor.

As the hardware based techniques require additional sensors, its cost gets increased. On the other hand, software based techniques are cheap because it does not require any extra device. It is less intrusive; it can be embedded in feature extraction module which makes it capable of detecting other types of attacks. The proposed method has various advantages over the previous methods: - i) Multibiometric ii) Fast iii) User-friendly iv) Cheap and v) Low complexity.

II. RELATED WORK

In 2012, U. M. Chaskar, Z. Wei has focused on the quality factors which affect iris images [3].

There are large numbers of fingerprint matching techniques like minutiae based matching, correlation based matching, genetic algorithms based matching, etc. But, these methods give poor results in fingerprint recognition because correlation cannot recognize elastic distorted versions between two fingers [2].

In 1991, M. A. Turk, Alex P. Pentland performed face recognition based on Eigen faces and 3D face recognition [1]. But, changes in lightening, distance and angle, changes the results. Also, 2D face recognition systems do not capture the actual size of the face.

Most of the antispoofing methods presented lack the generality of the system. All the above methods represent very valuable work in spoofing detection but they fail to generalize to different problems as they are usually designed to work on one specific modality and also to detect one specific type of spoofing attack. Although researchers have done great work in the field of spoofing detection and many advances have been reached, the attacking methods have also evolved. So, there are big challenges to be faced in the detection of direct attacks.

In the present work, software based multibiometric liveness detection method is given which overcomes some of these limitations through by using Image Quality Assessment (IQA). Image quality has been successfully used in previous works for image manipulation detection [4], [5] and steganalysis [6], [7] in the forensic field.

III. PROPOSED METHOD

In the proposed work to detect liveness of the user, quality difference hypothesis is used. Quality of the test sample is measured by using 30 image quality measures (iqms). Out of these quality measures 25 are full reference and 5 are no reference iqms. Quality difference hypothesis states that, “a fake image captured in an attack attempt will have lower quality than a real sample acquired in the normal operation scenario” [26]. The quality difference between real and fake samples include degree of sharpness, color and luminance level, local artifacts, entropy, structural distortions or natural appearance.

There are large numbers of quality measures which can be used for measuring the quality of image. A different quality measure presents different sensitivity to image artifacts and distortions. For example, measures like mse are more sensitive to additive noise whereas spectral phase errors react to blur. While gradient related features respond more to distortions concentrated around edges and textures. Hence, the combination of different quality measures gives better performance than single quality measure. So, here we have used combination of 30 image quality measures. The image quality measures are selected on the basis of four criteria: performance, complementarity, complexity and speed.

In the presented system, an input sample has to be assigned to one of the two classes i.e. Real or fake. Here, the main task is to find discriminant features from input sample that are used to build a classifier.

**International Journal of Engineering Research in Electronics and Communication
Engineering (IJERECE)
Vol 3, Issue 9, September 2016**

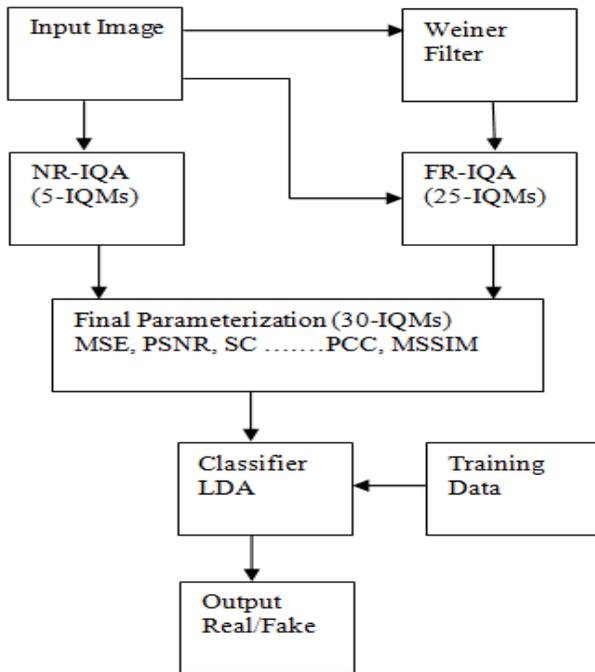


Fig.1. Block diagram of proposed Liveness Detection method

The block diagram is shown in Fig.1. In order to design more general and simple system, it takes only one input that is the biometric sample to be classified as real or fake. As shown in the block diagram the input image is test image which is to be classified as image of live user or fake. Firstly, the quality features of the test image are extracted by using full reference and no reference quality measures. Then these 30 quality features are given to the classifier. We have used Linear Discriminant Analysis (LDA) classifier for classification purpose. By using 30 quality measures and trained data, the classifier classifies the test image as real or fake.

A. Full Reference Image Quality Measures (IQMs)

Full reference quality measures needs a clean reference image to calculate the quality score of the test image. But in the proposed method such a reference image is not available, because the present system has access to only one input sample. So to get this reference image,

the test image is filtered through a weiner filter. The output of the weiner filter is a clean smoothed version of test image. Then the quality of the test image with respect to reference image is computed by using full reference quality measures. This method compares the quality of test image and reference image. If quality difference is more than threshold value, the test sample is fake otherwise it is real.

B. No Reference Image Quality Measures

The human visual system assesses the quality of the test image without using a reference image. No reference quality measures are based on the principle of human visual system.

**TABLE I. 30 IQMS USED IN THE PROPOSED WORK.
(T-Denotes test image and R-denotes Reference Image.)**

Sr.	Acronym	Name	Formula	Ref.
1	MSE	Mean Square Error	$MSE(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M (T - R)^2$	16
2	PSNR	Peak Signal to Noise Ratio	$PSNR(T, R) = 10 \log_{10} \frac{MAX(T, R)^2}{MSE(T, R)}$	17
3	SNR	Signal to Noise Ratio	$SNR(T, R) = 10 \log_{10} \frac{E\{T^2\}}{E\{T - R\}^2}$	18
4	SC	Structural Content	$SC(T, R) = \frac{E\{T \cdot R\}}{E\{T\} \cdot E\{R\}}$	19
5	MD	Maximum Difference	$MD(T, R) = \max(T, R)$	19
6	AD	Average Difference	$AD(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M (T - R)$	19
7	NAE	Normalized Absolute Error	$NAE(T, R) = \frac{\sum_{n=1}^N \sum_{m=1}^M T - R }{NM}$	19
8	RAMD	R-Averaged MD	$RAMD(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M T - R $	16
9	LMSSE	Laplacian MSE	$LMSSE(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M (T - R - 0.5)^2$	19
10	NXC	Normalized Cross correlation	$NXC(T, R) = \frac{E\{T \cdot R\}}{\sqrt{E\{T^2\} \cdot E\{R^2\}}}$	19
11	MAS	Mean Angle Similarity	$MAS(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M \cos(\theta)$	16
12	MAMS	Mean Angle Magnitude Similarity	$MAMS(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M [1 - \sin(\theta)] [1 - \frac{ \cos(\theta) }{2}]$	18
13	TED	Total Edge Difference	$TED(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M E_T - E_R $	20
14	TCD	Total Corner Difference	$TCD(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M C_T - C_R $	20
15	SSE	Spectral Magnitude Error	$SSE(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M (F_T - F_R)^2$	21
16	SPE	Spectral Phase Error	$SPE(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M \arg(F_T) - \arg(F_R) ^2$	21
17	GME	Gradient Magnitude Error	$GME(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M (G_T - G_R)^2$	22
18	GPE	Gradient Phase Error	$GPE(T, R) = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M \arg(G_T) - \arg(G_R) ^2$	22
19	SISA	Structural Similarity Index	Refer Ref. No.8	8
20	VIF	Visual Information Fidelity	Refer Ref. No.9	9
21	RRFD	Reduced reference error-free difference	Refer Ref. No.10	10
22	IQG	IPEG Quality Index	Refer Ref. No.11	11
23	HLFI	High/Low Frequency Index	$HLFI(T) = \frac{\sum_{n=1}^N \sum_{m=1}^M F_T - 25}{\sum_{n=1}^N \sum_{m=1}^M F_T }$	23
24	BIQI	Blind Image Quality Index	Refer Ref. No.12	12
25	NIQE	Natural Image Quality Estimate	Refer Ref. No.13	13
26	UIQI	Universal Image Quality Index	Refer Ref. No.14	14
27	PCC	Pearson Correlation Coefficient	$PCC = \frac{cov(T, R)}{\sigma_T \sigma_R}$	19
28	EME	Enhancement Error Measure	$EME = \frac{1}{NM} \sum_{n=1}^N \sum_{m=1}^M \frac{ T - R }{20 \ln(\frac{max}{min})}$	24
29	MSSIM	MultiScale Structural Similarity Index	Refer Ref. No.15	15
30	SSNR	Visual Signal to Noise Ratio	Refer Ref. No.25	25

It checks the quality of the test image in the absence of reference image. No reference IQMs

**International Journal of Engineering Research in Electronics and Communication
Engineering (IJERECE)
Vol 3, Issue 9, September 2016**

generally estimates the quality of test image according to a pre-trained statistical model. Among 30 IQMs, JQI, HLF, BIQI, NIQE and EME are no reference IQMs.

C. Additional Image Quality Measures

In the proposed method, we have used five additional quality measures in order to increase the accuracy of the system. We have used Universal Image Quality Index (UIQI), Pearson Correlation Coefficient (PCC), Enhancement Error (EME), Multi Scale Structural Similarity Index (MSSSIM) and Visual Signal to Noise Ratio (VSNR). Among these IQMs, UIQI, PCC, MSSIM, VSNR are full reference IQMs and EME is no reference IQM.

The Formulae And References Of 30 IQMS Used In The Proposed Work Are Given In Table I.

D. Classifier

Classification is done by calculating the value of discriminate function for each class. We have used linear discriminate analysis (LDA) classifier. LDA is based on covariance matrix. It is used for dimensionality reduction i.e. If we have large number of variables then we can reduce the number of variables while preserving most of the information. Lda is based upon the concept of searching for linear combination of variables that best separates two classes [27].

STEPS TO CLASSIFY INPUT SAMPLE:

- 1) Separate the data into two classes.
- 2) Calculate no. Of instances in each class i.e. N1- number of instances in first class and n2- number .of instances in second class.
- 3) Then Find Probability Of Each Class, P1 And P2.
- 4) Calculate the mean of every feature of first class and represent it in vector form. Denote It By μ_1 .
- 5) Calculate the mean of every feature of second class and represent it in vector form. Denote it by μ_2 .
- 6) Find The Covariance Matrices Of Two Classes I.E. C1 and C2.

- 7) Calculate Pooled Covariance Matrix C:

$$A. C = (N1 \times C1 + N2 \times C2) / (N1 + N2).$$

- 8) Take Inverse Of Pooled Covariance Matrix I.E. INV (C).

- 9) Calculate Discriminate Function:

$$F_1 = (\mu_1 \times C^{-1} \times T^t) - \left(\frac{1}{2} \times \mu_1 \times C^{-1} \times \mu_1^t\right) + \log(P_1)$$

$$F_2 = (\mu_2 \times C^{-1} \times T^t) - \left(\frac{1}{2} \times \mu_2 \times C^{-1} \times \mu_2^t\right) + \log(P_2)$$

Here, T Is Vector Of Features Extracted From Test Sample. μ_1^t and μ_2^t are transpose matrices of μ_1 and μ_2 . If $f_1 > f_2$ the test sample goes to first class otherwise it will goes to second class.

The proposed system can be used in industry for checking quality of the product. We have tested the system for sorting of good quality mangoes and rotten mangoes. It was working fine for sorting of mangoes with uniform background. The typical images of mangoes are shown below:



Good quality mango rotten mango

Fig.2. Typical images of mangoes

IV. EXPERIMENTAL RESULTS

In the presented system, we have considered three different modalities i.e. Iris, fingerprint and face. The results are attained on publicly available database. So, we can compare the performance of the proposed system with other systems. We have compared our results with image quality assessment (IQA) based method [26]. In [26], the authors have compared their results with previously implemented methods and found better results than others. From the experimental results obtained, we can observe that proposed system have better results than IQA method and previous methods which are compared with IQA method [26]. Here we have used linear discriminant analysis classifier for classification of real and fake samples. Therefore

**International Journal of Engineering Research in Electronics and Communication
Engineering (IJERECE)
Vol 3, Issue 9, September 2016**

results are reported in terms of false acceptance rate (FAR) and false rejection rate (FRR). Far is the number of fake samples which are falsely accepted as real and fir is the number of real samples which are falsely rejected considering it as fake. Half total error rate (HTER) is computed as, $HTER = (FAR + FRR) / 2$. The proposed system is implemented using matlab r2012b software on windows 8-pc having 2.4 GHZ processor and 4gb ram.

A. IRIS

For iris modality, we have used ATVS-FLR db database. This database is available on the website of biometric recognition group-ATVS. The database consists of 1600 iris images. It is divided into train set and test set. Train set consists of 400 real images and 400 fake images. Similarly, test set consists of remaining 400 real and 400 fake images. Liveness detection results derived from the proposed approach are shown in table ii. Fig. 3 shows typical real and fake iris images from ATVS-FLR db database.



Real IRIS fake IRIS
Fig.3.real and fake iris images

TABLE II RESULTS: IRIS

	FRR	FAR	HTER
Proposed Method	0.0	0.0	0.0
IQA Method [26]	4.2	0.25	2.2

B. Fingerprints

For fingerprint modality we have used ATVS-FFP db dataset. This dataset is obtained from the website of biometric recognition group-ATVS. The database consists of 3168 fingerprint samples. The database is divided into train set and test set. Train set is used to

train the classifier and test set is used to test the performance of the system. Both train set and test set are totally different. They are not overlapped with each other. Here, 768 real and 768 fake images were used for training purpose. And 800 real and 800 fake samples were used as test set. The results derived from the proposed method are shown in table iii. Fig.4 shows a real and fake fingerprint samples.



Real Fingerprint Fake Fingerprint

FIG.4.REAL AND FAKE FINGERPRINT IMAGES

TABLE III RESULTS: FINGERPRINT

	FRR	FAR	HTER
Proposed Method	7.5	6.0	6.75
IQA Method [26]	14.0	11.6	12.8

C. Face

The database used for face modality is the REPLAY-ATTACK DB. It is obtained from the website of IDIAP Research Institute. The database consists of short videos in .mov format of both real-access and spoofing attack attempts. These videos are acquired with a 320x240 resolution webcam of a 13-inch MAC book laptop. The videos were recorded under two different conditions: i) controlled, with a uniform background and artificial lightening and ii) Adverse, with natural illumination and non-uniform background. For the experimental results we have considered 160 videos. These videos are divided into train and test sets. Train set consists of 40 real and 40 fake videos, i.e. 40x300=12000 real and 12000 fake frames. Similarly, test set consists of remaining 40 real and 40 fake videos, i.e. 12000 real and 12000 fake frames.

**International Journal of Engineering Research in Electronics and Communication
Engineering (IJERECE)
Vol 3, Issue 9, September 2016**

The proposed method needs only one input image and not a sequence of them. So, each frame of the videos in the database has been considered as an independent image sample. Therefore classification is done on a frame by frame basis and not per video. Fig.5 shows typical examples of real and fake face images that are available in the public REPLAY-ATTACK DB under two different scenarios i.e. adverse and controlled. Liveness detection results derived from the proposed method are shown in Table IV.

TABLE IV Results: Face

	FRR	FAR	HTER
Proposed Method	13.4	11.9	12.65
IQA Method [26]	17.9	12.5	15.2

ADVERSE SCENARIO CONTROLLED SCENARIO



Real attempt
Fake attempt
Fig.5. Typical Real and Fake Face Images

V. CONCLUSION

By simple visual examination, human eyes cannot distinguish between images of genuine and fake biometric samples as they are very similar. But when the images are translated into correct feature space, one

can detect the variations between them. These disparities exist between real and fake sample because the 3D objects have some optical qualities while fake sample (2D sample) do not possess it. Also, biometric sensors are designed to produce good quality samples in ideal surroundings with a true 3D attribute. If the attribute in front of the scanner is not genuine, the characteristics of the captured image may vary.

In this system, we have extracted 30 quality features from test sample. These features are given to classifier to detect real and fake samples. The liveness detection of the test sample is based on quality difference hypothesis.

The proposed five additional image quality metrics for liveness detection are Universal Image Quality Index (UIQI), Pearson Correlation Coefficient (PCC), Enhancement Error Measure (EME), Multi Scale Structural Similarity Index (MSSSIM) and Visual Signal to Noise Ratio (VSNR). By using these measures the accuracy of the system is increased. The experimental result shows that the proposed work have better results than previous methods. The presented method can work for various biometric traits. Also, it can detect different types of attacks. The proposed method is ready to generalize different databases, acquisition conditions and attack scenarios. The error rates of the proposed method are lower than other anti-spoofing method.

In future, for face spoofing detection, in video attack we can reduce the FFR, FGR by training ensemble classifier instead of training a single classifier. We can use video quality measures for video attacks.

REFERENCES

- [1] M.A. Turk and A.P. Pentland, "Face recognition using eign faces," IEEE Conference on Computer Vision and Pattern Recognition, pp. 586-591, 1991.
- [2] A. Ross and S. Prabhakar, "Fingerprint matching using minutiae and texture features," International

**International Journal of Engineering Research in Electronics and Communication
Engineering (IJERECE)
Vol 3, Issue 9, September 2016**

- Conference on Image Processing, pp.282-285, 2001.
- [3] U.M. Chaskar, N.S. Shah and T. Jaison, "Iris Image quality assessment for biometric applications," International Journal of Computer Science, vol.3, no.1.
- [4] S.Bayram, I.Avcibas, B.Sankur and N.Menon, "Image manipulation detection," J.Electron.Imag., vol.15,no.4,pp.041102-1-041102-17,2006.
- [5] M.C. Stamm and K.J.R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," IEEE Trans.Inf. Forensics Security, vol.5, no.3, pp.492-496, Sep.2010.
- [6] I.Avcibas, B.Sankur and N.Menon, "Steganalysis using image quality metrics," IEEE Trans.Imag. Process., vol.12, no.2, pp.221-229, Feb.2003.
- [7] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," IEEE Trans.Inf. Forensic Security, vol.1, no.1, pp.111-119, Mar..2006.
- [8] Z.Wang, A.C.Bovic, H.R.Sheikh and P.Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Trans.Image Process, vol.13, no.4, pp.600-612, Apr. 2004.
- [9] H.R. Sheikh and A.C.Bovic, H, "Image information and visual quality," IEEE Trans.Image Process, vol.15, no.2, pp.434-444, Feb. 2006.
- [10] R.Soundararajan and A.C.Bovic, "RRED: indices: Reduced reference entropic differencing for image quality assessment," IEEE Trans.Image Process, vol.21, no.2, pp.517-526, Feb. 2012.
- [11] Z.Wang, A.C.Bovic and H.R.Sheikh, "No-reference perceptual quality assessment of JPEG compressed images," in proc. IEEE ICIP, pp.477-480, Sep. 2002
- [12] A.K.Moorthy and A.C.Bovic, "A two-step framework for constructing blind image quality indices," IEEE Signal Process. Lett., vol.17, no.5, pp.513-516, May. 2010
- [13] A.Mittal, R. Soundararajan and A.C.Bovic, "Making a completely blind image quality analyzer," IEEE Signal Process Lett., vol.20, no.3, pp.209-212, Mar. 2013.
- [14] Z.Wang and A.C.Bovic, "A Universal Image Quality Index," IEEE Signal Process. Lett., vol.9, no.3, Mar. 2002.
- [15] Z.Wang, A.C.Bovic and P.Simoncelli, "Multi structural similarity for image quality assessment,".
- [16] I.Avcibas, B.Sankur and K.Syood, "Statistical evaluation of image quality measure," J. Electron. Imag., vol.11,no.2,pp.206-223,2002.
- [17] 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.
- [18] S. Yao, W. Lin, E. Ong and Z. Lu, "Contrast signal to noise ratio for image quality assessment," in proc. IEEE ICIP, pp.397-400, Sep. 2005.
- [19] 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.
- [20] 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.
-

**International Journal of Engineering Research in Electronics and Communication
Engineering (IJERECE)
Vol 3, Issue 9, September 2016**

- [21] N.B. Nill and B. Bouzas, "Objective image quality measures derived from digital image power spectra," *Opt. Eng.*, vol.31, no.4, pp.813-825, 1992.
- [22] 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.
- [23] X. Zhu and P. Milanfar, "A no reference sharpness metric sensitive to blur and noise," in *Proc.Int.Workshop Qual.Multimedia Exper*, pp.64-69
- [24] Karen Panetta, Chen Gao and S. Aghaian, "No reference color image contrast and quality measure," *IEEE Trans. On Consumer Electronics*, vol.59, no.43, August 2013.
- [25] D.M. Chandler and S. Hemami, "VSNR: A wavelet based visual signal to noise ratio for natural images," *IEEE Trans. On Image Process.*, vol.16, no.9, Sep.2007.
- [26] J. Galbally, S. Marcel and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint and face recognition," *IEEE Trans. On Image Process.*, vol.23, no.2, Feb.2014.
- [27] T. Hastie, R. Tibshirani and J. Fridman, "The elements of statistical learning", New york,USA Springer-Verlog, 2001.