|| Volume 3 || Issue 4 || April 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Image Quality Assessment for Fake Detection

J. Ashok kumar[1], E.soujanya[2], J.sharadha[3], D. Saikrupa goud[4], A.Sirivennela[5]
Asst. Professor, Dept. of Electronics and Communication Engineering V Raju Institute of Technology, Narsapur, Medak, Telangana, India[1]
U.G. Student, Dept. of Electronics and Communication Engineering V Raju Institute of Technology, Narsapur, Medak, Telangana, India[2 3 4 5]

Abstract— **Security is the major concern for today's scenario. A high level industry uses passwords like thumb, face, voice, iris, etc. There are many security systems are available but not so reliable for that here the developing system which is very precise and reliable. In this paper, we present a MATLAB- based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The main objective is to upgrade the security of biometric recognition, by adding liveness assessment in a fast, user-friendly, manner, through the use of image quality assessment. The complexity is very low, which is suitable for real-time applications, using 25 general image quality features extracted from one image.**

Key words- — Image quality assessment, biometrics, security, attacks.

I INTRODUCTION

In the present work we propose a novel software-based multi-biometric and multi-attack protection method which targets to overcome part of these limitations through the use of image quality assessment (IQA). It is not only capable of operating with a very good performance under different biometric systems and for diverse spoofing scenarios, but it also provides a very good level of protection against certain non-spoofing attacks (multi-attack). Moreover, 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 (transparent to the user); **Cheap and easy** to embed in already functional systems.

An added advantage of the proposed technique is its speed and very low complexity, which makes it very well suited to operate on real scenarios. As it does not deploy any trait-specific property (e.g., minutiae points, iris position), the computation load needed for image processing purposes is very reduced, using only general image quality measures fast to compute, combined with very simple classifiers

II LIVENESS DETECTION

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. For example, iris images captured from a printed paper are more likely to be blurred or out of focus due to trembling, 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. The different quality measures present different sensitivity to image arti-facts and distortions. The measures like the mean squared error respond more to additive noise, whereas other such as the spectral phase error are more sensitive to blur, while gradient-related features react to distortions concentrated around edges and textures. The image quality measures have the potential to achieve success in biometric protection tasks.

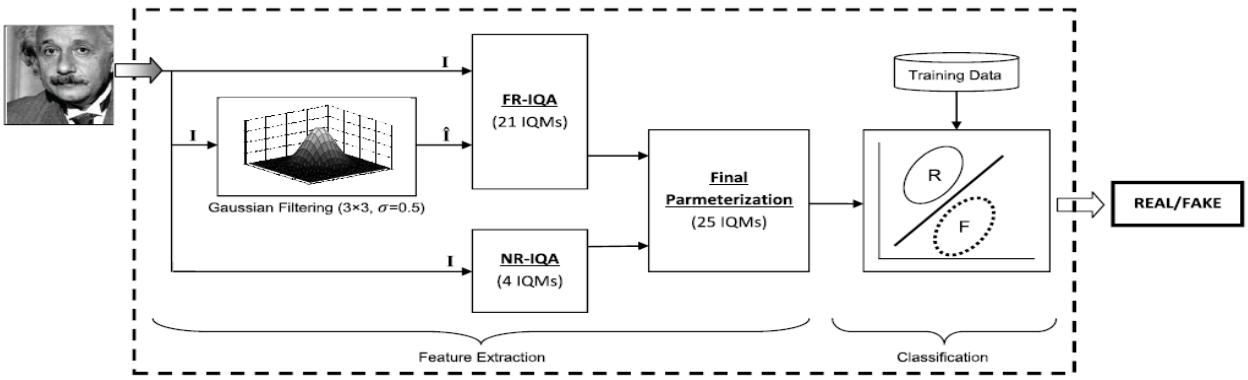


Figure. 1. Block diagram of fake detection

III PROTECTION METHOD

A general diagram of the protection approach proposed in this work is shown in Fig. 1. The method operates on the whole image without searching for any trait-specific properties, it does not require any pre-processing steps prior to the computation of the IQ features. This characteristic minimizes its computational load. The initial feature selection process to determine the set of 25 IQMs has been carried out according to four general criteria, for liveness detection. These four selection criteria are:

1) **Performance:** Only widely used image quality approaches which have been consistently tested showing good performance for different applications have been considered.
2) **Complementarity**: In order to generate a system as general as possible in terms of attacks detected and biometric modalities supported image (e.g., sharpness, entropy or structure).
3) **Complexity**: In order to keep the simplicity of the method, low complexity features have been preferred over those which require a high computational load.

Speed: In general, closely related to the previous complexity. 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.

A. Full-Reference IQ Measures:

In this method the input grey-scale image ‘I ‘is filtered with a low-pass Gaussian kernel in order to generate a smoothed version ˆI. Then, the quality between both images (I and ˆI) 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.

1) Error Sensitivity Measures:

Image quality assessment approaches are based on measuring the errors between the distorted and the reference images, and attempt to quantify these errors. For clarity, these features have been classified here into five different categories (see Fig. 2) according to the image property measurement.

a) Pixel Difference measures:

These features compute the distortion between two images on the basis of their pixel wise differences. Here we include: 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) and Laplacian Mean Squared Error (LMSE).

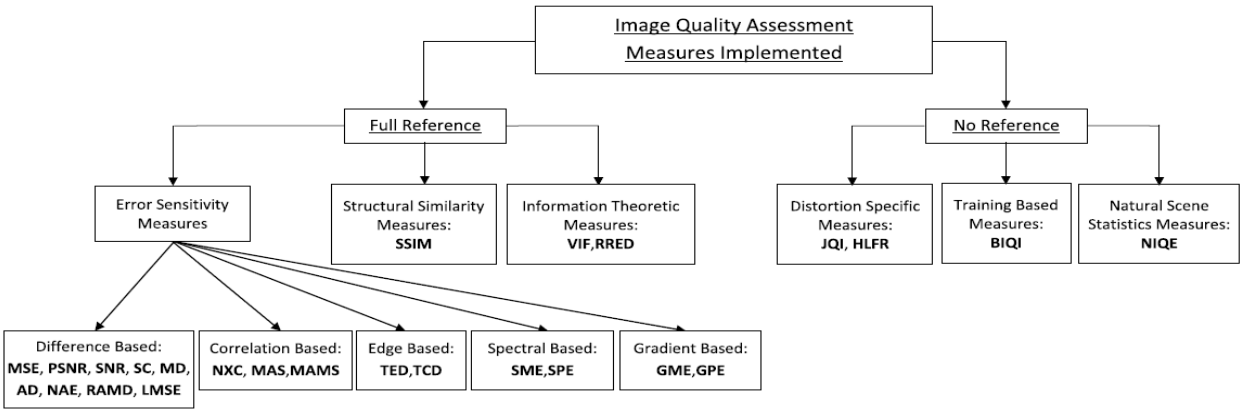


Figure 2. Classification of the 25Image Quality Measures

b) Correlation-based measures:

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).

c) 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 quality assessment applications. The here we have considered two edge-related quality measures: Total Edge Difference (TED) and Total Corner Difference (TCD). In order to implement both features, we use:

(i) The Sobel operator to build the binary edge maps IE and ^{A}IE. (i i) The Harris corner detector to compute the number of corners Ncr and *Ncr found in I and ˆI.

d) Spectral distance measures:

The Fourier transform is another traditional image processing tool which has been applied to the field of image quality assessment. In this work we will consider as IQ spectral-related features: the Spectral Magnitude Error (SME) and the Spectral Phase Error (SPE).

e) Gradient-based measures.

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. Two simple gradient-based features are included in the biometric protection system proposed in the present article: Gradient Magnitude Error (GME) and Gradient Phase Error (GPE).

2) Structural Similarity Measures:

Image 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. The Structural Similarity Index Measure (**SSIM**), has the simplest formulation and has gained widespread popularity in a broad range of practical applications.

3) Information Theoretic Measures:

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 image to the amount of information shared between the test and the reference signals. We consider two of these information theoretic features: the Visual Information Fidelity (**VIF**) and the Reduced Reference Entropic Difference index (**RREDI**).

B. No-Reference IQ Measures:

In general the human visual system does not require of a reference sample to determine the quality level of an image. NR-IQA methods generally estimate the quality of the test image according to some pre-trained statistical models and on the *a priori* knowledge required, the methods are coarsely divided into one of three trends.

1) Distortion-specific approaches:

The final quality measure is computed according to a model trained on clean images and on images affected by this particular distortion. Two of these measures have been included in the biometric protection method they are

- 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**) 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.

2) Training-based approaches:

The metrics intend to provide a general quality score not related to a specific distortion. Here different distortion-specific experts are combined to generate one global quality score.

3) Natural Scene Statistic approaches:

It use *a priori* knowledge taken from natural scene distortion-free images to train the initial model. The Natural Image Quality Evaluator (**NIQE**) is a completely blind image quality analyzer based on the construction of a quality aware collection of statistical features related to a multi variate Gaussian natural scene statistical model.

Table 1 list of the 25 image quality measures

#	Type	Acronym	Name	Ref.	Description
1	FR	MSE	Mean Squared Error	[29]	$MSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})^2$
2	FR	PSNR	Peak Signal to Noise Ratio	[30]	$PSNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\max(\mathbf{I}^2)}{MSE(\mathbf{I},\hat{\mathbf{I}})})$
3	FR	SNR	Signal to Noise Ratio	[31]	$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N\cdot M\cdot MSE(\mathbf{I},\hat{\mathbf{I}})})$
4	FR	SC	Structural Content	[32]	$SC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{\mathbf{I}}_{i,j})^2}$
5	FR	MD	Maximum Difference	[32]	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|$
6	FR	AD	Average Difference	[32]	$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})$
7	FR	NAE	Normalized Absolute Error	[32]	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|}{\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{I}_{i,j}\|}$
8	FR	RAMD	R-Averaged MD	[29]	$RAMD(\mathbf{I},\hat{\mathbf{I}},R) = \frac{1}{R}\sum_{r=1}^{R}\max_r\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|$
9	FR	LMSE	Laplacian MSE	[32]	$LMSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(\mathbf{I}_{i,j})-h(\hat{\mathbf{I}}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}h(\mathbf{I}_{i,j})^2}$
10	FR	NXC	Normalized Cross-Correlation	[32]	$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\cdot\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$
11	FR	MAS	Mean Angle Similarity	[29]	$MAS(\mathbf{I},\hat{\mathbf{I}}) = 1-\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\alpha_{i,j})$
12	FR	MAMS	Mean Angle Magnitude Similarity	[29]	$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1-[1-\alpha_{i,j}][1-\frac{\|\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|\|}{255}])$
13	FR	TED	Total Edge Difference	[33]	$TED(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{I}_{\mathbf{E}i,j}-\hat{\mathbf{I}}_{\mathbf{E}i,j}\|$
14	FR	TCD	Total Corner Difference	[33]	$TCD(I,\hat{I}) = \frac{\|N_{cr}-\hat{N}_{cr}\|}{\max(N_{cr},\hat{N}_{cr})}$
15	FR	SME	Spectral Magnitude Error	[34]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\|\mathbf{F}_{i,j}\|-\|\hat{\mathbf{F}}_{i,j}\|)^2$
16	FR	SPE	Spectral Phase Error	[34]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\|\arg(\mathbf{F}_{i,j})-\arg(\hat{\mathbf{F}}_{i,j})\|^2$
17	FR	GME	Gradient Magnitude Error	[35]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\|\mathbf{G}_{i,j}\|-\|\hat{\mathbf{G}}_{i,j}\|)^2$
18	FR	GPE	Gradient Phase Error	[35]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\|\arg(\mathbf{G}_{i,j})-\arg(\hat{\mathbf{G}}_{i,j})\|^2$
19	FR	SSIM	Structural Similarity Index	[36]	See [36] and practical implementation available in [37]
20	FR	VIF	Visual Information Fidelity	[38]	See [38] and practical implementation available in [37]
21	FR	RRED	Reduced Ref. Entropic Difference	[39]	See [39] and practical implementation available in [37]
22	NR	JQI	JPEG Quality Index	[40]	See [40] and practical implementation available in [37]
23	NR	HLFI	High-Low Frequency Index	[41]	$SME(\mathbf{I}) = \frac{\sum_{i=1}^{i_l}\sum_{j=1}^{j_l}\|\mathbf{F}_{i,j}\|-\sum_{i=i_h+1}^{N}\sum_{j=j_h+1}^{M}\|\mathbf{F}_{i,j}\|}{\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{F}_{i,j}\|}$
24	NR	BIQI	Blind Image Quality Index	[42]	See [42] and practical implementation available in [37]
25	NR	NIQE	Naturalness Image Quality Estimator	[43]	See [43] and practical implementation available in [37]

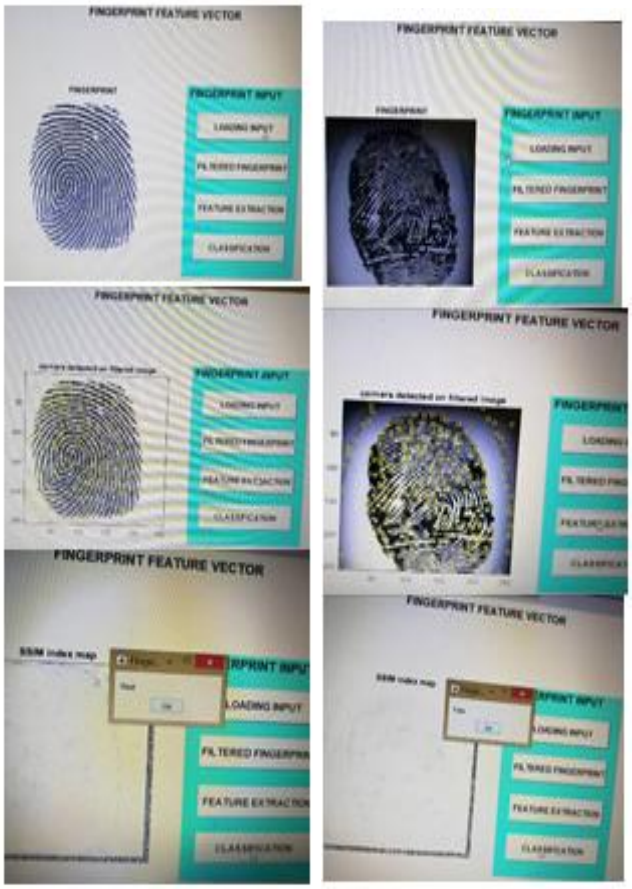
IV RESULTS

First, evaluate the "multi-biometric" dimension of the protection method, to achieve a good performance. Second, evaluate the "multi-attack" dimension of the protection method to detect not only spoofing attacks but also fraudulent access attempts carried out with

Iris-Spoofing:

Face –Spoofing

Finger-Spoofing:



REFERENCE

[1] 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.

[2] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in *Proc. AWB*, 2004.

[3] 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.

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

[5] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," *Future Generat. Comput. Syst.*, vol. 28, no. 1, pp. 311–321, 2012.

[6] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," *Handbook of Biometrics*. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.

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

[8] *Biometric Evaluation Methodology. v1.0*, Common Criteria, 2002.

[9] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, *Proceedings of the IEEE Int. Joint Conf. on Biometrics*. Piscataway, NJ, USA: IEEE Press, 2011.

[10] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, *et al.*, "First international fingerprint liveness detection competition— LivDet 2009," in *Proc. IAPR ICIAP*, Springer LNCS-5716. 2009, pp. 12–23.

[11] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, *et al.*, "Competition on countermeasures to 2D facial spoofing attacks," in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–6.

[12] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks