Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel Fake Detection System for Biometric Modalities

[1]Tija Thomas*, [2]Halice K Babu, [3]Ambikadevi Amma T
[1]M.Tech CSE, [2]Assistant Professor, [3]Professor
[1, 2, 3] Department of Computer Science and Engineering, Jawaharlal College of Engineering and Technology, Lakkidi, Kerala, India

Abstract *— The development of novel and proficient security measures is required for the real occurrence of a legitimate behaviour in comparison to a fake self-manufactured synthetic or reconstructed sample which is a major dilemma in biometric authentication. A new fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts is described in this paper. The goal of the suggested system is to improve the safety measures of biometric identification frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive way, through the use of image quality assessment. In order to differentiate between legitimate and impostor samples, the suggested approach is simple and makes it appropriate for real-time applications, using 30 general image quality features extracted from a single image. It can be concluded that the proposed method is very much competitive when compared to other state-of-the-art approaches from the experimental results obtained on the available data sets of fingerprint, iris, hand palm and 2D face. The study of the general image quality of real biometric samples gives very important information which can be proficiently used to distinguish them from fake behaviour.*

Keywords — Image quality assessment, biometrics, security, fraudulent access, liveness assessment.

I. INTRODUCTION

In the last few years, there has been an increase in the focus on strategies, created in the field of biometric systems security. Direct or spoofing attack is one of the main threats faced by biometric systems of different modalities. In the attack, the attacker use synthetic artifacts (e.g., printed images or biometric modalities made of synthetic materials) or tries to imitate the behavior of real user. This helps the attacker to fraudulently access the biometric system. So it is very much essential to propose and develop a particular protection method against the threat. For this purpose, a countermeasure based on liveness detection technique, which uses various physiological properties to differentiate between original and fake samples is considered.

Liveness evaluation techniques should satisfy certain requirements:(i) user friendly, easy for the users to use it;(ii) non-invasive, should not need extra contacts with the user or not cause any harm for the user;(iii) fast, result should be produced with in short span of time and user interaction with the sensor should be less;(iv) low cost, used widely if cost is less;(v) performance, should have high recognition performance and good fake detection rate.

Liveness detection techniques are divided into two types (see Fig 1): (i) Hardware based method, in order to detect specific properties of a living trait (e.g., reflection properties of the eye, fingerprint sweat),some specific devices are added to the sensor;(ii) Software based method, in this case after acquiring the sample using a standard sensor fake trait is detected. The two methods have certain advantages and disadvantages over the other. Software based method is less intrusive and less expensive while hardware based method has got a higher fake detection rate. Software based method protect the system from injecting the synthetic or reconstructed sample into the communication channel between the sensor and the feature extractor. It operates directly on the acquired sample rather than specific biometric trait.

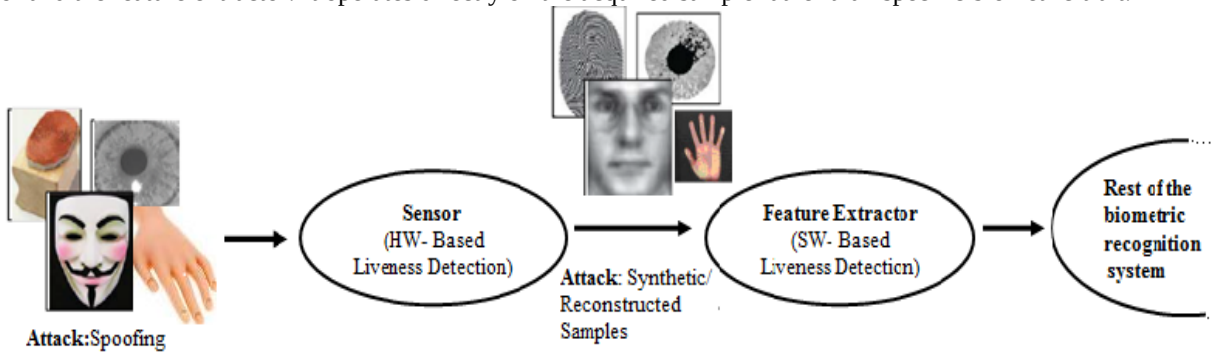

Fig.1 Types of attacks potentially detected by hardware and software-based liveness detection techniques

Lack of generality is one of the main shortcomings of most anti-spoofing methods. Specific properties of a given trait (e.g., pupil dilation of the eye, ridges and valleys in fingerprints) are used as the measurement for most of the current protection methods. This introduces reduced interoperability because recognition systems based on other biometric modalities cannot be implemented based on that.

A novel software based multi-biometric fake detection method through the use of image quality assessment (IQA) is introduced in this paper. This system operates with good performance in multi-biometric systems and has got various other advantages also. It is fast, uses only one input image to distinguish whether it is real or fake; user friendly; cheap; non-intrusive and easy to embed in already functional systems because no hardware is required.

The main advantage of the system is its speed and very low complexity that helps it to use in real time applications. This system does not depend on trait specific property, so the computation load needed is very less. General image quality features which are fast to compute are considered and simple classifiers are used to distinguish between real and fake sample. It is carried out on publicly available attack databases of fingerprint, iris, 2D face and hand palm images and 2D face in real time.

II. BACKGROUND STUDY

Lack of generality is one of the main shortcomings of most anti-spoofing methods. Specific properties of a given trait (e.g., pupil dilation of the eye, ridges and valleys in fingerprints) are used as the measurement for most of the current protection methods. This introduces reduced interoperability because recognition systems based on other biometric modalities cannot be implemented based on that.

In previous works, fingerprint and iris liveness detection is measured by using different trait-specific quality properties [13], [14]. However, there is no biometric system in general which uses image quality as a protection method. For e.g., to detect certain fingerprint spoofs, ridge and valley frequency may be used as a good parameter for measuring but it cannot be used in iris liveness detection. In the same way, the amount of occlusion of the eye is applicable in iris anti-spoofing mechanism, but it is not useful in fake fingerprint detection. Even though all of these helps to solve the problem of spoofing detection, they fail to generalize as they are designed to work on specific modality and, in most of the cases, used to detect one specific type of spoofing attack. Image manipulation detection [23], [18] has been successfully carried out by image quality in previous works. In the present work, to a certain extent, spoofing attacks with printed iris or face images is considered as a type of image manipulation that can be successfully detected, by the use of different image quality features.

Liveness detection using image quality assessment is based on the hypothesis that:"It is expected that the quality of the fake image taken in an attack attempt will be different from that of real image."

Real and fake samples have quality differences in degree of sharpness, colour and luminance levels, local artifacts, amount of information found in images (entropy), structural distortions or natural appearance. For example, iris images taken from a printed paper are more probably unclear or out of focus due to wavering; face images taken from a mobile device maybe over or under-exposed; gummy finger print contain local acquisition artifacts such as spots and patches. A synthetically produced image is directly given to the communication channel before the feature extraction in an ultimate attack. This fake sample lacks some of the properties found in original images.

G*eneral* image quality assessment is used as a protection method against different biometric attacks. The features used, do not calculate any specific property of a given biometric modality or of a specific attack, it calculates on any image. New multi-biometric dimension is achieved with the proposed method which is different from that of earlier protection schemes.

III. METHODOLOGY

In fake biometric detection system, an input biometric sample is classified as either real or fake. The main role of the method is to find a set of different features which helps to construct a suitable classifier which provides the probability of the image "realism", given the extracted feature set. In the proposed system, a novel parameterization using 30 general image quality measures is considered.

A general diagram of the proposed protection approach is shown in Fig 2. The system uses only one input, the biometric sample to be classified as real or fake, in order to keep its generality and easiness. This method considers the whole image rather than considering any trait-specific properties, no pre-processing steps (e.g., fingerprint segmentation, iris detection or face extraction) are done prior to the calculation of the IQ features. This feature reduces the computational load. After computing all the features, the necessary features are selected using Principal Component Analysis (PCA). PCA helps in finding out, the features which are important for best describing the variance in a data set. It is most often used for reducing the dimensionality of a large data set [27]. Once the feature vector has been generated the sample is classified as real (produced by a genuine trait) or fake (synthetically produced), using classifiers like Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) classifiers [25]. Final decision is taken by the fusion of above two classifications using Dempster Shafer method [17].

Thirty IQMs are classified according to four general criteria. These four selection criteria are:

a) ***Performance:*** Generally used image quality approaches, which have been constantly tested showing good performance for various applications have been considered.

b) ***Complementarity:*** IQMs based on complementary properties of the image (e.g., sharpness, entropy or structure) are used in order to create a system as general as possible in terms of attacks detected and biometric modalities supported.

c) ***Complexity:*** Low complexity features are considered rather than which requires a high computational load. This helps to keep the simplicity of the system.

d) ***Speed:*** This criteria is closely related to the previous one (complexity). To comfort a non-intrusive and user-friendly application, users are not allowed to keep waiting for a long time to get response from the recognition system. In order to avoid this, greater significance has been given to the feature extraction time, which has a main role in considering the overall speed of the fake detection system.

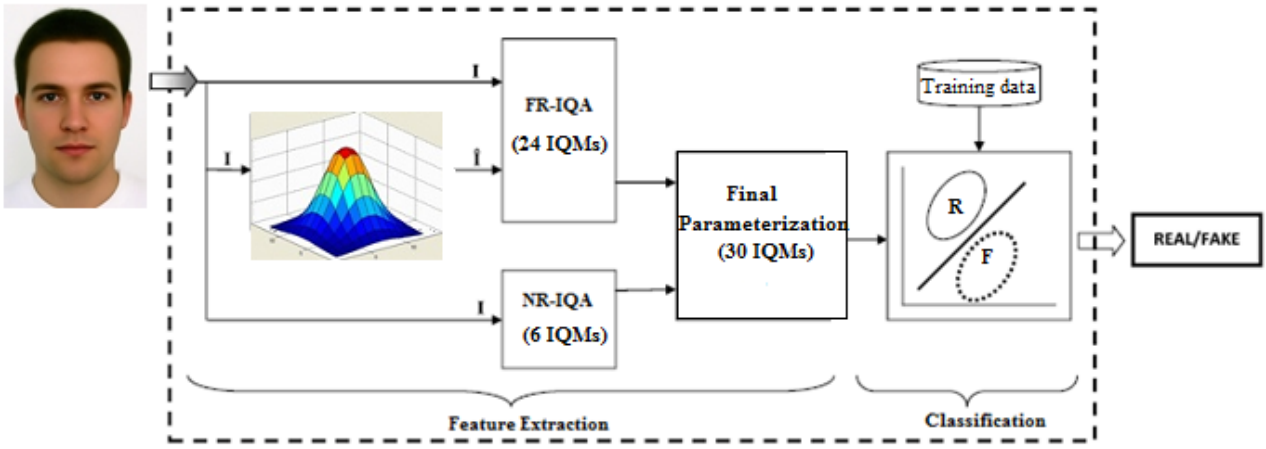

Fig. 2 General diagram of the fake detection system based on Image Quality Assessment (IQA)

Image quality measures are classified into two types: Full-Reference and No Reference IQ measures (Fig 3).

A. Full-Reference IQ Measures

Full-reference (FR) IQA methods estimates the quality of the test sample using clean undistorted reference image. The fake detection system used here access only the input sample and the reference image is unknown. In order to overcome this limitation, the method used for image manipulation detection in [23] and for steganalysis in [12], is used in this case. A low-pass Gaussian kernel filters the input grey-scale image **I** (of size $N \times M$) and thus generates a smoothed version **Î**, as shown in Fig 2. Based on the corresponding full-reference IQA metric, the quality between the images (**I** and **Î**) is calculated. The method assumes that the Gaussian filtering produces a loss of quality difference between real and fake biometric samples.

1) FR-IQMs: Error Sensitivity Measures: Conventional image quality assessment methods are based on measuring the errors between the distorted and the reference images. This is the most commonly used method for IQA because it uses many known psychophysical features of the human visual system [5], very easy to calculate and usually have very low computational complexity. Error sensitivity features are classified into five categories in order to provide clarity:

a) ***Pixel Difference measures*** [11], [3]**:** Based on their pixel wise differences, these features compute the distortion between two images. It includes: Mean Squared Error (**MSE**), Peak Signal to Noise Ratio (**PSNR**) [21], Signal to Noise Ratio (**SNR**) [24], Structural Content (**SC**), Maximum Difference (**MD**), Average Difference (**AD**), Normalized Absolute Error (**NAE**), R-Averaged Maximum Difference (**RAMD**) and Laplacian Mean Squared Error (**LMSE**).

b) ***Correlation-based measures*** [11], [3]**:** Calculates the similarity between two digital images. It is calculated in terms of the correlation function. Angles between the pixel vectors of the original and distorted images is used as an alternative of correlation based measures. This feature includes: Normalized Cross-Correlation (**NXC**), Mean Angle Similarity (**MAS**) and Mean Angle- Magnitude Similarity (**MAMS**).

c) ***Edge-based measures:*** Edges and corners are the most informative parts of an image [19]. Two edge-related quality measures like Total Edge Difference (**TED**) and Total Corner Difference (**TCD**) are considered, since the structural distortion of an image is tightly linked with its edge degradation. The Sobel operator and the Harris corner detector [6] are used to implement these features.

d) ***Spectral based measures:*** Another conventional image processing tool used in the field of image quality assessment is Fourier transform [11]. IQ spectral-related features like the Spectral Magnitude Error (**SME**), the Spectral Phase Error (**SPE**) and Spectral Energy (**SE**) [9] are used.

e) ***Gradient-based measures:*** Gradients play a great role in quality assessment. It gives important visual information about the image. Change in the gradient reflects the distortions that affect an image. Structural and contrast changes can be effectively captured using such information. Two gradient-based features used in the system includes: Gradient Magnitude Error (**GME**) and Gradient Phase Error (**GPE**) [2].

2) FR-IQMs: Structural Similarity Measures: Image quality assessment based on structural similarity is based on the assumption that the human visual system is highly adapted for extracting structural information from the viewing field [29]. It is calculated using the features, Structural Similarity Index Measure (**SSIM**) [29], [7] and Universal Image Quality Index (**UIQI)** [28].

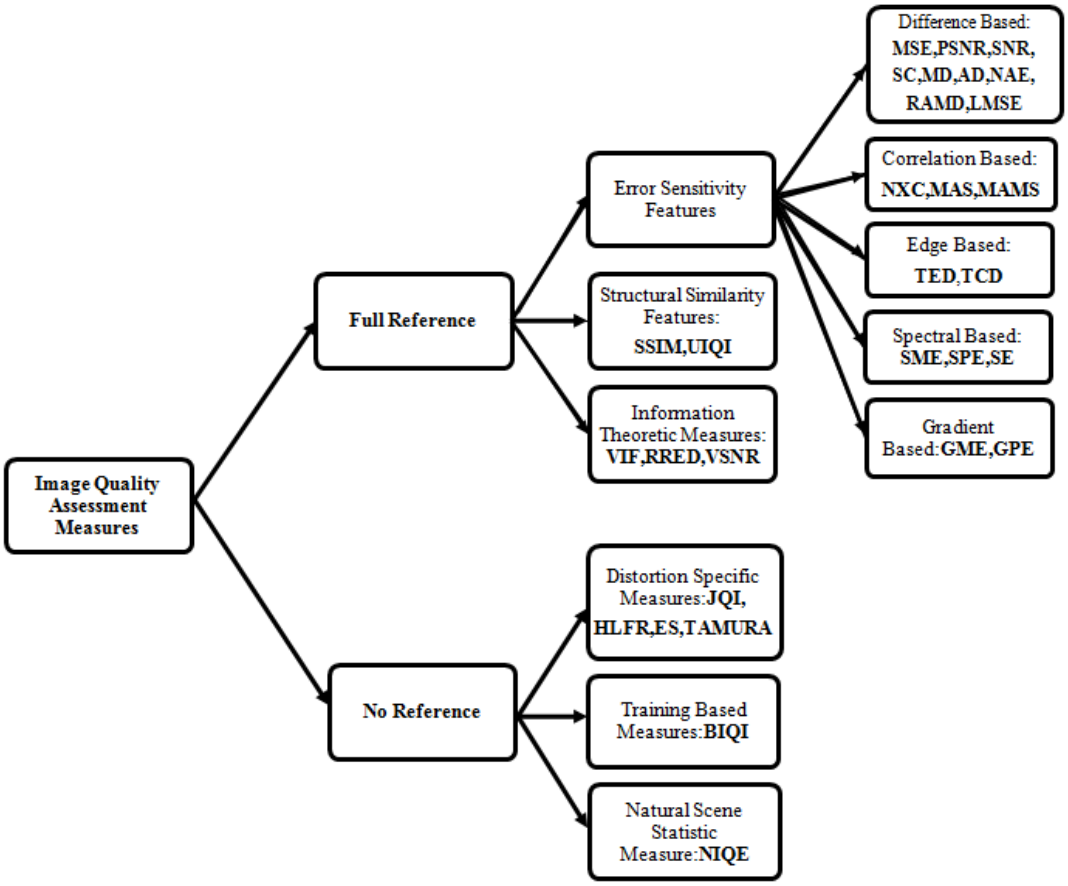

Fig. 3 Classification of 30 image quality measures used in the proposed system

3) FR-IQMs: Information Theoretic Measures: Based on information theory perspective, the quality assessment problem may be considered as an information-fidelity problem. A source image communicates to a receiver through a channel which limits the amount of information that flows through it, thereby introducing distortions, is the main idea of the method. The primary goal of this measure is to relate the visual quality of the test image to the mutual information shared between the test and the reference signal. In the proposed system three information theoretic features are considered: the Visual Information Fidelity (**VIF**) [10], Reduced Reference Entropic Difference index (**RRED**) [22] and Visual Signal to Noise Ratio (**VSNR)** [8].

The VIF calculates the quality fidelity as the ratio between the total information of the whole distorted image and the total information conveyed within the complete reference image. RRED metric measures the amount of local information difference between the reference image and the projection of the distorted image onto the space of natural images. RRED is contrary to VIF feature because it accesses only the reduced part of its information. VSNR operates based on physical luminance and visual angle of the image.

B. No-Reference IQ Measures

No-reference image quality assessment (NR-IQA) algorithms assess the visual quality of images without using a reference image. Based on some pre-trained statistical models, NR-IQA methods estimate the quality of the test image. This method is divided into three types based on the on the *a priori* knowledge required and the images used to train the model [16]:

1) Distortion-specific approaches: Depends on prior knowledge of visual quality loss caused by a particular distortion. Using a trained model of clean samples and samples affected by the particular distortion is used to calculate the final quality measure. This includes 4 measures. The JPEG Quality Index (**JQI**) [30], calculates the image quality in images, caused by the common block artifacts seen in many compression algorithms like JPEG, which runs at low bit rates. The High-Low Frequency Index (**HLFI**) [26], measure is calculated by the power difference between the lower and upper frequencies of the Fourier Spectrum. It is sensitive to the sharpness of the image. Edge Spread (**ES**) [20], Calculates the effect of irregularity based on the image intensity difference with respect to the local maxima and minima of pixel intensity at every row of the image. **Tamura** feature is an approach that explores texture representation from a different angle since it is motivated by the psychological studies on human visual perception of textures.

2) Training-based approaches: In this technique a model is trained using clean and distorted images, similar to that of above class. Depends on the extracted number of features from the test sample and based on the general model, quality score is calculated [1]. The statistical model is trained with samples affected by different distortions types. Blind Image Quality Index (**BIQI**) [1], follows a two-stage framework. It creates one global quality score by combining the individual measures of various distortion-specific experts.

3) Natural Scene Statistic approaches: This technique trains the initial model depending on the previously acquired knowledge of natural scene distortion-free images. This is based on the assumption that the natural world undistorted images contain certain *regular* properties that falls within a certain subspace of all possible images [4].Natural Image Quality Evaluator (**NIQE**) is used as a measure in this work [4].

IV. RESULT AND DISCUSSION

The novel software based multi-biometric fake detection method helps to distinguish whether the given input sample is real or fake through the use of image quality assessment (IQA). This system helps in detecting different types of fraudulent access attempts and also helps to improve the safety measures of biometric identification frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive way, through the use of image quality assessment. In order to differentiate between legitimate and impostor samples, the suggested approach is simple and makes it appropriate for real-time applications.

V. CONCLUSION

In the last few years, the analysis of the risk of various types of attacks against biometric systems has been a very prominent field of research. This has lead to great progress in the area of safety enhancing technologies for biometric-based applications. The development of proficient safety technique against known threats has proven to be a not easy assignment in spite of this evident advance.

After a brief examination, the human eye might find it hard to distinguish between an image of a real biometric trait and its fake sample. But once the images are translated into a proper feature space, few disparities between the real and fake images might become apparent. This is due to the reality that biometric traits, as 3D objects, possess their own optical merits (absorption, reflection, scattering, refraction), which other resources (paper, gelatin, electronic display) or synthetically created samples don't have. Moreover, in regular operation surroundings, biometric sensors gives good quality samples when they interrelate with a real 3D trait. The qualities of the captured image may drastically vary if this circumstance changes, or if the trait offered to the scanner is an unpredicted fake artifact (2D, different material, etc). It can be concluded that the image quality of real accesses and fraudulent attacks will be different. The potential of general image quality assessment, as a safeguard tool against diverse biometric attacks (especially spoofing) is explored in this proposed system.

Hence, to detect various kinds of fraudulent access attempts in multiple biometric systems a new software-based fake detection system that can be used is introduced, which ensures the actual presence of a real legitimate trait in contrast to a fake unreal sample. The aim of the suggested system is to improve the security of biometric recognition frameworks by using image quality estimation. The proposed approach depicts a very low degree of complexity, making it appropriate for real-time applications. The new security technique has been assessed on iris, the fingerprint, 2D face and hand palm images using publicly obtainable databases with related protocols and 2D face in real time.

The fake detection method can execute constantly at a high level, for various biometric modalities and gives high level of safeguard against various kind of attacks. The suggested system is fast, simple, non-intrusive, cheap and user-friendly, which are most required in a practical protection system.

ACKNOWLEDGEMENT

First of all, praise is to God, who has helped me to complete this paper. I express my sincere gratitude to the HOD of Computer Science and Engineering, Mrs. Ambikadevi Amma and my Guide, Miss. Halice K Babu for providing me constant guidance, support and encouragement all the way along the project. I also express my profound sense of gratitude and respect to all those who helped me throughout the duration of this project.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] A. M. Pons, J. Malo, J. M. Artigas, and P. Capilla, "Image quality metric based on multidimensional contrast perception models," DisplaysJ., vol. 20, no. 2, pp. 93–110, 1999.

[6] C. Harris and M. Stephens, "A combined corner and edge detector," in Proc. AVC, 1988, pp. 147–151.

[7] 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.

[8] Damon M. Chandler, Sheila S. Hemami, "VSNR: A Wavelet-Based Visual Signal-to-Noise Ratio for Natural Images*," IEEE Trans on image processing, vol. 16, no. 9, Sep 2007*

[9] Himanshu S. Bhatt, Samarth Bharadwaj, Mayank Vatsa, Richa Singh, ''A framework for quality-based biometric classifier selection*," IEEE Biometrics (IJCB), International Joint Conference on Biometrics Compendium, 11-13 Oct. 2011*

[10] 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.

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

[12] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," IEEE Trans. Image Process., vol. 12, no. 2, pp. 221–229,Feb.2003.

[13] 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.

[14] 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.

[15] J. Galbally, Sebastien Marcel, "Image quality assessment for fake biometric detection: An application to Iris,Fingerprint and Face recognition," *IEEE Trans. on image processing, vol 23 ,no.2.,Feb 2014*

[16] M. A. Saad, A. C. Bovik, and C. Charrier, "Blind image quality assessment: A natural scene statistics approach in the DCT domain," IEEE Trans. Image Process., vol. 21, no. 8, pp. 3339–3352, Aug. 2012.

[17] M. Arif, Rawalpindi, Brouard, T. ; Vincent, N.," A fusion methodology based on Dempster-Shafer evidence theory for two biometric applications," IEEE International conference on Pattern Recognition, Vo:4, 2006.

[18] 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.

[19] 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.

[20] P. M. Frederic, F. Dufaux, S. Winkler, T. Ebrahimi, and G. Sa. A no-reference perceptual blur metric. In *Proceedings of International Conference on Image Processing*, pages 57–60, 2002.

[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] 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.

[23] 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.

[24] 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. T. Hastie, R. Tibshirani, and J. Friedman., The Elements of Statistical Learning. New York, NY, USA: Springer-Verlag, 2001.

[25] T. Hastie, R. Tibshirani, and J. Friedman., The Elements of Statistical Learning. New York, NY, USA: Springer-Verlag, 2001.

[26] 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.

[27] Yijuan Lu , Ira Cohen , Xiang Sean Zhou and Qi Tian, "Feature Selection Using Principal Feature Analysis," ACM Multimedia, Augsburg, Germany, September 23-29, 2007.

[28] Z. Wang and A.C. Bovik, "A universal image quality index," *IEEE Signal Processing Letters* ,vol.9, no.3pp.81-84, Mar 2002.

[29] 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.

[30] Z. Wang, H. R. Sheikh, and A. C. Bovik, "No-reference perceptual quality assessment of JPEG compressed images," in Proc. IEEE ICIP, Sep. 2002, pp. 477–480.

