Volume 5, Issue 3, March 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Identification of Fake Biometric Access on Irish and Fingerprint Recognition Using Image Quality Assessment

H. Seyed Sulthan Areef[1], J. Venkateshan[2], S. Thabithal[3], S. Priyasivakumar[4]
[1, 2] Assistant Professor, [3, 4] UG Scholar
[1, 2, 3, 4] Department Computer Science & Engineering,
RVS College of Engineering &Technology, Karaikal, Puducherry, India

Abstract -Biometric systems encounter variability in data that influence capture, treatment, and u-sage of a biometric sample. It is imperative to first analyze the data and incorporate this understanding within the recognition system, making assessment of biometric quality an important aspect of biometrics. Though several interpretations and definitions of quality exist, sometimes of a conflicting nature, a holistic definition of quality is indistinct. Several factors that cause different types of degradations of biometric samples, including image features that attribute to the effects of these degradations, are discussed. Evaluation schemes are presented to test the performance of quality metrics for various applications. A survey of the features, strengths, and limitations of existing quality assessment techniques in fingerprint, iris, and face biometric are also represented. Finally, a representative set of quality metrics from these three modalities are evaluated on a multimodal database consisting of 2D images, to understand their behaviour with respect to match scores obtained from the state-of-the-art recognition systems. The analysis of the characteristic function of quality and match scores shows that a careful selection of complimentary set of quality metrics can provide more benefit to various applications of biometric quality.

Keywords- Image quality assessment, biometrics, security, attacks, countermeasures.

I. INTRODUCTION

Fake biometrics means by using the real images (iris images captured from a printed paper and Fingerprint captured from a dummy finger) of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first capture the original identities of the genuine user and then they make the fake sample for authentication but biometric system have more method to detect the fake users and that's why the biometric system is more secure, Because each person have their unique characteristics identification. Biometrics system is more secure than other security methods like password, PIN, or card and key. A Biometrics system measures the human characteristics so users do not need to remember passwords or PINs which can be forgotten or to carry cards or keys which can be stolen. Biometric system is of different type that are face recognition system, fingerprint recognition system, iris recognition system, hand geometry recognition system (physiological biometric), signature recognition system, voice recognition system (behavioral biometric). Multi biometric system means a biometric system is used more than one biometric system for one multi-biometric system. A multi biometric system is use the multiple source of information for recognition of person authentication. Multi biometric system is more secure than single biometric system. In this Survey Base seminar report Image quality assessment for liveness detection technique is used for find out the fake biometrics. Image assessment is force by supposition that it is predictable that a fake image and real sample will have different quality acquisition. Predictable quality differences between real and fake samples may contain: color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. For example, iris images captured from a printed paper are more likely to be fuzzy or out of focus due to shaky; face images captured from a mobile device will almost certainly be over-or under-discovered; and it is not rare that fingerprint images which is captured from a dummy finger. In addition in ultimate attack in which an unnaturally produced image is directly injected to the communication channel before the feature extractor, this fake sample will most probably not have some of the properties found in natural images.

Image quality assessment is a most important topic in the image processing area. Digital images are subject to a large range of distortions during storage, achievement, compression, processing, transmission and reproduction, several of which may result in a degradation of visual quality. Imaging systems introduces some amount of distortion or artifacts which reduces the quality assessment. In general quality assessment is of two type one is subjective visual quality assessment and second one is objective visual quality assessment. Objective image quality metrics can be classified on the basis of availability of an original image, with the distorted image is to be compared. Accessible approaches are known as full-reference, meaning that a complete reference image is assumed to be known. In many practical applications, however, the reference image does not exist, and a no-reference or "blind" quality assessment approach is desirable.

II. THE SECURITY PROTECTION METHOD

The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. In the present work we propose a novel parameterization using 25 general image quality measures.

In order to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake (i.e., the same image acquired for biometric recognition purposes). Furthermore, as the method operates on the whole image without searching for any trait-specific properties, it does not require any pre-processing steps (e.g., fingerprint segmentation, iris detection or face extraction) prior to the computation of the IQ features. This characteristic minimizes its computational load. Once the feature vector has been generated the sample is classified as real (generated by a genuine trait) or fake (synthetically produced), using some simple classifiers.

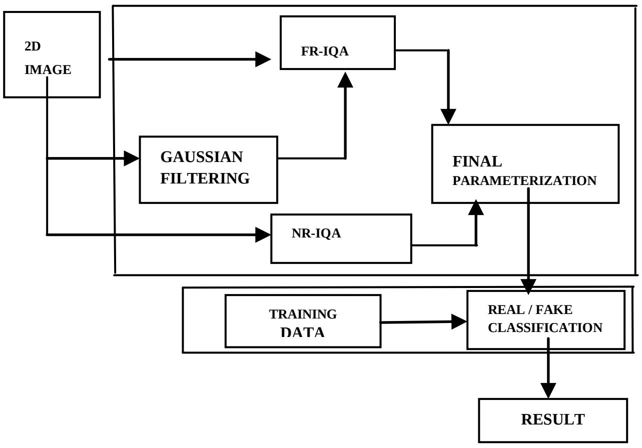

Fig. 1 General diagram of the biometric protection method based on image quality assessment proposed in the present work

CRITERIA:

- **Performance:** Only widely used image quality approaches which have been consistently tested showing good performance for different applications have been considered.
- **Complementarity:** In order to generate a system as general as possible in terms of attacks detected and biometric modalities supported, we have given priority 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 have 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.

A. Full-Reference Image Quality Measures (FR-IQMs)

1. Mean Square Error:

The mean squared error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. The difference occurs because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate.

The MSE is the second moment (about the origin) of the error, and thus incorporates both the variance of the estimator and its bias. In an analogy tostandard deviation, taking the square root of MSE yields the root-mean-square error or root-mean-square deviation (RMSE or RMSD), which has the same units as the quantity being estimated; for an unbiased estimator, the RMSE is the square root of the variance, known as the standard deviation.

2. Peak Signal to Noise Ratio:

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression).

3. Signal to Noise Ratio:

Signal-to-noise ratio (often abbreviated SNR or S/N) is a measure used in science and engineering that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power, often expressed in decibels. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise. While SNR is commonly quoted for electrical signals, it can be applied to any form of signal (such as isotope levels in an ice core or biochemical signaling between cells).

The signal-to-noise ratio, the bandwidth, and the channel capacity of a communication channel are connected by the Shannon–Hartley theorem. Signal-to-noise ratio is sometimes used informally to refer to the ratio of useful information to false or irrelevant data in a conversation or exchange.

4. Structural Content:

The ratio between the square of sum of original image to the square of sum of reference image is often defined by structural content. In the form of equation is given by,

$$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N\cdot M\cdot MSE(\mathbf{I},\hat{\mathbf{I}})}\right)$$

5. Maximum Difference:

The maximum value of absolute difference image (original image is subtracted to the reference image. In the form of equation is given by,

$$MD(\mathbf{I},\hat{\mathbf{I}}) = \max|\mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j}|$$

6. Average Difference:

The average value per pixel of absolute difference image (original image is subtracted to the reference image. In the form of equation is given by,

$$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j})$$

7. Normalized Absolute Error:

The ratio between sum of absolute of difference image to the sum of absolute of original image. In the form of equation is given by,

$$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}|}{\sum_{i=1}^{N}\sum_{j=1}^{M}|\mathbf{I}_{i,j}|}$$

8. R-averaged MD:

The sum of maximum of R numbers value is summed and divided by R to calculate average maximum difference. In the form of equation is given by,

$$RAMD(\mathbf{I},\hat{\mathbf{I}},R) = \frac{1}{R}\sum_{r=1}^{R}\max_r|\mathbf{I}_{i,j} - \hat{\mathbf{I}}_{i,j}|$$

In the RAMD formulae, max*r* is defined as the *r* -highest pixel difference between two images. For the present implementation, *R* = 10.

9. Laplace MSE:

Based on this h(image) = **I**i+1, j +**I**i−1, j +**I**i, j+1 + **I**i, j−1 − 4**I**i, j equation .the h(**I**i, j) and h(**I**^i, j) will be calculated .the ratio between the square of difference of these two values to the sum of original image h(**I**i, j) value. In the form of equation is given by,

$$LMSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(\mathbf{I}_{i,j})-h(\hat{\mathbf{I}}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}h(\mathbf{I}_{i,j})^2}$$

10. Normalized Cross-Correlation

For image-processing applications in which the brightness of the image and template can vary due to lighting and exposure conditions, the images can be first normalized. This is typically done at every step by subtracting the mean and dividing by the standard deviation. In the form of equation is given by,

$$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\cdot\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$$

11. Mean angle similarity

The mean angle similarity is the measure of similarity of mean angle between the original image and reference image. In the form of equation is given by,

$$MAS(\mathbf{I},\hat{\mathbf{I}}) = 1 - \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\alpha_{i,j})$$

12. Mean Angle Magnitude Similarity

The mean angle magnitude similarity is the measure of similarity of mean angle's magnitude between the original image and reference image. In the form of equation is given by,

$$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1 - [1-\alpha_{i,j}][1 - \frac{||\mathbf{I}_{i,j}-\mathbf{I}_{i,j}||}{255}]$$

13. Total Edge Difference::

The ratio between the differences of total number of edges between the two images to the total number of pixels. In the form of equation is given by,

$$TED(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}|\mathbf{I}_{\mathbf{E}i,j} - \hat{\mathbf{I}}_{\mathbf{E}i,j}|$$

14. Total Corner Difference:

The ratio between the differences of total number of corners between the two images to the total number of pixels. In the form of equation is given by,

$$TCD(I,\hat{I}) = \frac{|N_{cr}-\hat{N}_{cr}|}{\max(N_{cr},\hat{N}_{cr})}$$

15. Spectral Magnitude Error:

The difference between the Fourier transform of original image to the Fourier transform of reference image is averaged by total number of pixel. In the form of equation is given by,

$$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(|\mathbf{F}_{i,j}| - |\hat{\mathbf{F}}_{i,j}|)^2$$

16. Spectral Phase Error:

The difference between the angles of Fourier transformed original image to the angle of Fourier transformed reference image is averaged by total number of pixel. In the form of equation is given by,

$$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}|\arg(\mathbf{F}_{i,j}) - \arg(\hat{\mathbf{F}}_{i,j})|^2$$

17. Gradient Magnitude Error:

The difference between the gradient of original image to the gradient of reference image is averaged by total number of pixel. In the form of equation is given by,

$$GME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(|\mathbf{G}_{i,j}| - |\hat{\mathbf{G}}_{i,j}|)^2$$

***18. Gradient Phase Error*:**

The difference between the angles of gradient of original image to the angle of gradient of reference image is averaged by total number of pixel. In the form of equation is given by,

$$GPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{i=1}^{M}|\arg(\mathbf{G}_{i,j}) - \arg(\hat{\mathbf{G}}_{i,j})|^2$$

19. Structural Similarity Index Measurement:

The Structural Similarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index can be viewed as a quality measure of one of the images being compared, provided the other image is regarded as of perfect quality.

20. Visual Information Fidelity:

The Visual Information Fidelity (VIF) metric is based on the assumption that images of the human visual environment are all natural scenes and thus they have the same kind of statistical properties.

21. Reduced Reference Entropy Difference:

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 subband of the wavelet domain. In essence, the RRED algorithm computes the average difference between scaled local entropies of wavelet coefficients of reference and projected distorted images in a distributed fashion.

B. No-Reference Image Quality Measures (NR-IQMs)

22. JPEG Quality Index:

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.

23. High Low Frequency Index:

The High-Low Frequency Index (**HLFI**) 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.

$$HLFI = \frac{\sum_{i=1}^{i_l}\sum_{j=1}^{j_l}|\mathbf{F}_{i,j}| - \sum_{i=i_h+1}^{N}\sum_{j=j_h+1}^{M}|\mathbf{F}_{i,j}|}{\sum_{i=1}^{N}\sum_{j=1}^{M}|\mathbf{F}_{i,j}|}$$

24. Blind Image Quality Index Measurement:

These blind IQA techniques use *a priori* knowledge taken from natural scene distortion-free images to train the initial model (i.e., no distorted images are used). The rationale behind this trend relies onthe hypothesis that undistorted images of the natural world present certain *regular* properties which fall within a certain subspace of all possible images.

25. Naturalness Image Quality Estimator:

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 variants Gaussian natural scene statistical model

III. EXPERIMENTAL AND RESULTS

A. Results: Iris

For the iris modality the protection method is tested under two different attack scenarios, namely: *i*) spoofing attack and *ii*) attack with synthetic samples.

Results: Iris-Spoofing:The database used in this spoofing scenario is the ATVS-Fir DB which may be obtained from the Biometric Recognition Group-ATVS.The database comprises real and fake iris images (printed on paper) of 50 users randomly selected from the Bio Sec baseline corpus. It follows the same structure as the original Bio Sec dataset, therefore, it comprises 50 users × 2 eyes × 4 images × 2 sessions = 800 fake iris images and its corresponding original samples.

Results: Iris-Synthetic:The real and fake databases used in this case are:

Real database: CASIA-IrisV1. This dataset is publicly available through the Biometric Ideal Test (BIT) platform of the Chinese Academy of Sciences Institute of Automation (CASIA). It contains 7 grey-scale 320×280 images of 108 eyes captured in two separate sessions with a self-developed CASIA close-up camera and are stored in bmp format.

Synthetic database: WVU-Synthetic Iris DB. The synthetic irises are generated following the method described in, which has two stages. In the first stage, a Markov Random Field model trained on the CASIA-IrisV1 DB is used to generate a background texture representing the global iris appearance. In the next stage, a variety iris features such as radial and concentric furrows, collarette and crypts, are generated and embedded in the texture field.

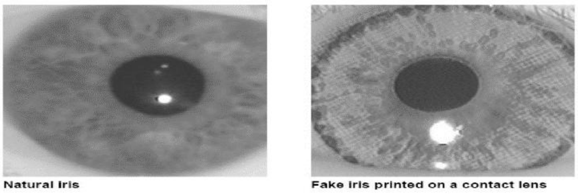

Fig. 2 Image of a real and fake iris

B. Results: Fingerprints

For the fingerprint modality, the performance of the proposed protection method is evaluated using the LivDet 2009 DB [10] comprising over 18,000 real and fake samples.

Results: Fingerprints-Spoofing LivDet:The LivDet 2009 DB [10] was captured in the framework of the 2009 Fingerprint Liveness Detection Competition and it is distributed through the site of the competition.[1]It comprises three datasets of real and fake fingerprints captured each of them with a different flat optical sensor: *i*) Biometrika FX2000 (569 dpi), *ii*) CrossMatch Verifier 300CL (500 dpi), and *iii*) Identix DFR2100 (686dpi). The gummy fingers were generated using three different materials: silicone, gelatine and playdoh, always following a consensual procedure (with the cooperation of the user). As a whole, the database contains over 18,000 samples coming from more than 100 different fingers.Some typical examples of the images that can be found in this database, the material used for the generation of the fake fingers is specified (silicone, gelatine or playdoh).

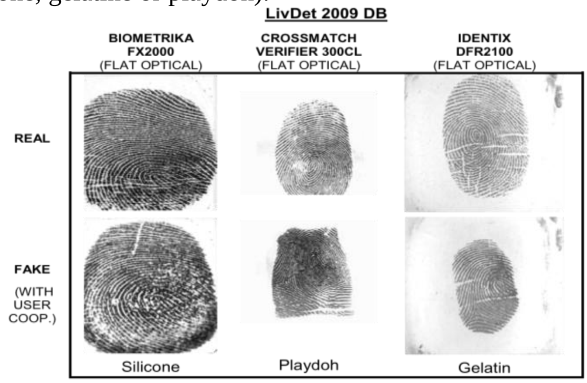
LivDet 2009 DB
BIOMETRIKA FX2000 (FLAT OPTICAL)
CROSSMATCH VERIFIER 300CL (FLAT OPTICAL)
IDENTIX DFR2100 (FLAT OPTICAL)
REAL
FAKE (WITH USER COOP.)
Silicone
Playdoh
Gelatin

Fig. 3 Typical examples of Real and Fake fingerprint images

IV. CONCLUSION

Image quality assessment for liveness detection technique is used to detect the fake biometrics. Due to Image quality measurements it is easy to find out real and fake users because fake identities always have some different features than original it always contain different color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. It is more secure than unibiometric system. Multi biometric system is used for various applications. And in future for making this system more secures adding the one more biometric system into this system and trying to improve the system.

REFERENCES

[1] 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.

[2] Tormod Emsell Larsen, A book for ”Biometric Solutions for Personal Identification”, Norwegian University of Science and Technology Department of Telematics- may 2008. Page 1-10, 19-23

[3] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, “Fingerprint image reconstruction from standard templates,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 9, pp. 1489–1503, Sep. 2007

[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] 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.

[6] (2012). BEAT: Biometrices Evaluation and Testing [Online]. Available: http://www.beat-eu.org/

[7] Biometrics Institute, London, U.K. (2011). [7]Biometric Vulnerability Assessment Expert Group [Online]. Available: http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expertgroup-bvaeg.html

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

[9] Padma Polash Paul, Md. Maruf Monwar,” Human Iris Recognition forBiometric Identification”, Ahsanullah University of Science and Technology, Dhaka, Bangladesh.

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