ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Survey on Efficient Approach Determination for Fake Biometric Detection

Nilima Ashok Kulkarni, Prof. L.J. Sankpal

M.E Student, Dept. of Computer Engineering, Sinhgad Academy Of Engineering, Pune, Maharashtra, India

Professor, Dept. of Computer Engineering, Sinhgad Academy Of Engineering, Pune, Maharashtra, India

ABSTRACT: Biometric systems are vulnerable to spoofing attacks. A reliable & efficient countermeasure is needed to prevent these attacks. Liveness assessment is one of the techniques which is very effective & can be applied to guard the system against harmful spoofing attack. In this paper, a software based protection approach is presented to prevent fraudulent access attempts. This software based system computes various quality measures extracted from one image depending on the specific biometric modality to distinguish between legitimate and fake samples. This makes the system more efficient without compromising the accuracy.

KEYWORDS: Liveness Detection, Image Quality Assessment, Biometrics, Security, Spoofing, Fraudulent Attacks

I. INTRODUCTION

Traditional methods for providing computer security such as passwords, PIN etc; are based on the properties that can be forgotten, disclosed, lost or stolen. e.g. Passwords often are easily accessible to colleagues and even occasional visitors and users tend to pass their tokens or share their passwords with their colleagues to make their work easier. Thus these methods do not authenticate the "user" as such. These methods try to validate what someone remembers (e.g. Password/PIN etc;) or what someone possess (e,g. ID card / token) instead of validating the identity of the particular user.

In last few years, biometrics has been increasingly used in providing computer security due to its distinct advantages over the conventional authentication techniques. Biometrics refers to authentication techniques that rely on measurable physiological & behavioural characteristics that can be automatically checked. There are several types of schemes that can be deployed for biometrics identification such as face, fingerprints, iris, hand geometry, retina, gait etc; [2] Some of the key advantages offered by biometrics over the traditional techniques are

- a scalable solution
- reliable
- increased accuracy
- difficult to breach

However, with increased usage of biometrics, one of the main threats faced by biometric systems of different modalities is direct or spoofing attack. In the attack, the attacker uses synthetic artifacts (e.g., printed images or biometric modalities made of synthetic materials, gummy fingers, face masks etc;) or tries to imitate the behaviour of real user [10]. This helps the attacker to fraudulently access the biometric system. So it is essential to propose and develop a protection method against the threat.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

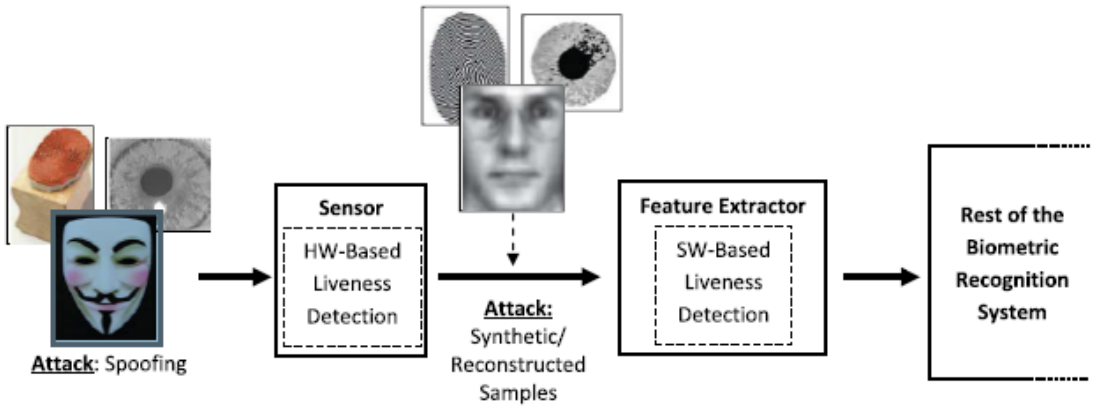


Fig.1 : Types of attacks potentially detected by hardware-based (spoofing) and software-based (spoofing & reconstructed/synthetic samples) liveness detection techniques

In this paper, different approaches for identifying, whether the particular biometric sample is real or fake, are discussed and an efficient approach is described.

II. RELATED WORK

Researchers are focused on the design of specific counter-measures, that enable biometric systems to detect fake samples, improving the robustness & security level of the system. Besides other anti-spoofing approaches, special attention has been paid by researchers & industry to the Liveness Detection technique. It uses different physiological properties such as odor, sweat etc; to distinguish between real & fake trait. The key requirements that need to be satisfied by liveness detection methods are : [26] (i) non-invasive - the technique should in no case be harmful for the individual or require an excessive contact with the user; (ii) user friendly - people should not be reluctant to use it; (iii) fast - results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time; (iv) low cost – a wide use cannot be expected if the cost is excessively high; (v) performance - in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

Liveness detection methods are usually classified into two groups Hardware based & Software based. Hardware based techniques which add some specific device to the sensor in order to detect particular properties of a living trait such as blood pressure [3] , odor [4], heart beat [5]. These hardware based techniques present higher prediction rate but they are very costly and require complex implementation. Unlike hardware based techniques, software based techniques are generally less expensive & less intrusive as no extra device such as spatial sensor is needed. Software techniques satisfy almost all requirements of liveness detection mentioned above.

One of the approaches for discriminating fake fingers from real ones [6] is based on analysis of skin distortion. The user is required to move the finger while pressing it against the scanner surface. The reference distortion code sequence is obtained from a well-trained user with a uniform & smooth movement. It was able to correctly represent most of real finger distortions. This approach is privacy-friendly & does not require additional expensive hardware besides a finger print scanner capable of capturing & delivering frames at proper rate. It achieves better results when the users are well-trained and habituated. However this approach requires additional training to the users as well as multiple image frames in order to get better results.

In another approach [7], which is based on quality measures, the liveness detection method presented has an added advantage that it requires just one image from a finger to decide whether it is real or fake. It extracts the necessary features such as local angle, power spectrum, pixel intensity etc; from the image and then decides whether the image presented is real or fake. This fact shortens the acquisition process & reduces the inconvenience for the final user also eliminates the need for training the users.

Similar to finger, an Iris image can also be used for liveness detection. In this approach [8], liveness detection scheme for Iris based on quality related measures has been presented.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Image manipulation detection [9] has been successfully carried out in previous work. In this work, spoofing attack with Finger, Iris or face images is considered as a type of image manipulation that can be successfully detected to a certain extent.

However, there is no biometric system in general which uses image quality as a protection method e.g. to detect certain fingerprint spoofs, ridge & 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. All these help to solve the problem of spoofing detection, they fail to generalize as they are designed to work on specific modality & usually used to detect one specific type of spoofing attack.

Liveness detection using image quality assessment is based on hypothesis that : "It is expected that the quality of the fake image taken in an attack will be different from a real image". [1]

Real & fake samples have quality differences in color, luminance levels, degree of sharpness, amount of information found in images, structural distortions, local artifacts. For example, iris images taken from a printed paper may be more unclear or out of focus, face images taken from mobile may be over-exposed or under-exposed, gummy finger may contain spots or patches. These fake samples lack some of the properties in the original image.

General 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.

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 out a set of features which help to construct a suitable classifier. In the proposed system, a novel parameterization using 25 general image quality measures are considered. A general diagram of fake detection system is shown in Fig. 2

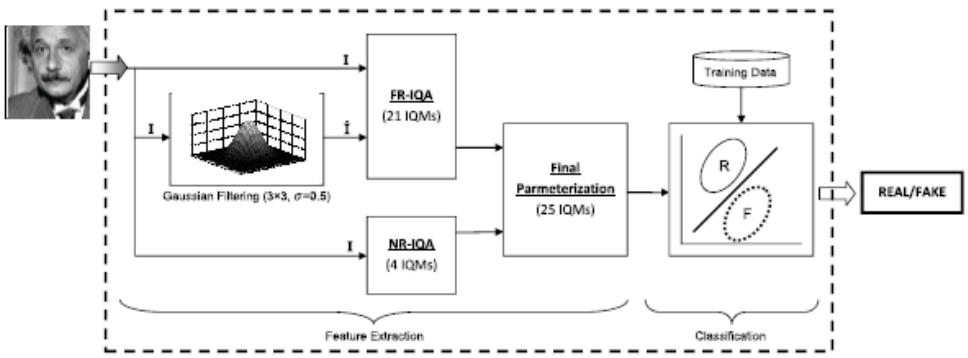


Fig.2 : General Diagram of the biometric protection method based on Image Quality Assessment (IQA)

The system uses only one input as a biometric sample in order to keep its generality & easiness. This method considers the whole image rather than considering any trait specific properties. It has no pre-processing steps (e.g. fingerprint segmentation, iris detection or face extraction etc;) are done prior to calculation of the IQ features. It reduces the computational load. Once the feature vector has been generated, the sample is classified as real or fake using classifiers like Linear discriminant analysis (LDA) & Quadratic discriminant analysis (QDA). It uses both Full Reference & No Reference image quality measures which are classified according to 4 general criteria:

1. Performance
2. Complementarity
3. Complexity
4. Speed

General image quality measures are fast to compute and easy to combine with simple classifiers. This bio-metric method is applicable to multi-modal modalities.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Sr. No.	Type	Acronym	Name	Description
1	FR	MSE	Mean Squared Error [11]	$MSE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})^2$
2	FR	PSNR	Peak Signal to Noise Ratio [12]	$PSNR(I,\hat{I}) = 10log(\frac{max(I^2)}{MSE(I,\hat{I})})$
3	FR	SNR	Signal to Noise Ratio [13]	$SNR(I,\hat{I}) = 10log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{N.M.MSE(I,\hat{I})})$
4	FR	SC	Structural Content [14]	$SC(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{I}_{i,j})^2}$
5	FR	MD	Maximum Difference [14]	$MD(I,\hat{I}) = max\,\lvert I_{i,j} - \hat{I}_{i,j}\rvert$
6	FR	AD	Average Difference [14]	$AD(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - \hat{I}_{i,j})$
7	FR	NAE	Normalized Absolute Error [14]	$NAE(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j} - \hat{I}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{i,j}\rvert}$
8	FR	RAMD	R-Averaged MD [11]	$RAMD(I,\hat{I},R) = \frac{1}{R}\sum_{r=1}^{R} max_r\,\lvert I_{i,j} - \hat{I}_{i,j}\rvert$
9	FR	LMSE	Laplacian MSE [14]	$LMSE(I,\hat{I}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(I_{i,j}) - h(\hat{I}_{i,J}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(I_{i,j}))^2}$
10	FR	NXC	Normalized Cross-Correlation [14]	$NXC(I,\hat{I}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j}.\hat{I}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j})^2}$
11	FR	MAS	Mean Angle Similarity [11]	$MAS(I,\hat{I}) = 1 - \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\alpha_{i,j})$
12	FR	MAMS	Mean Angle Magnitude Similarity [11]	$MAMS(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1 - [1-\alpha_{i,j}]\,[1 - \frac{\lVert I_{i,j} - \hat{I}_{i,j}\rVert}{255}])$
13	FR	TED	Total Edge Difference [15]	$TED(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert I_{E_{i,j}} - \hat{I}_{E_{i,j}}\rvert$
14	FR	TCD	Total Corner Difference [15]	$TCD(I,\hat{I}) = \frac{\lvert N_{cr} - \hat{N}_{cr}\rvert}{max(N_{cr},\hat{N}_{cr})}$
15	FR	SME	Spectral Magnitude Error [16]	$SME(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert F_{i,j} - \hat{F}_{i,j}\rvert)^2$
16	FR	SPE	Spectral Phase Error [16]	$SPE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert arg(F_{i,j}) - arg(\hat{F}_{i,j})\rvert^2$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Sr. No.	Type	Acronym	Name	Description
17	FR	GME	Gradient Magnitude Error [17]	$GME(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert G_{i,j}\rvert - \lvert\hat{G}_{i,j}\rvert)^2$
18	FR	GPE	Gradient Phase Error [17]	$GPE(I,\hat{I}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert arg(G_{i,j}) - arg(\hat{G}_{i,j})\rvert^2$
19	FR	SSIM	Structural Similarity Index [18]	Available in reference [19]
20	FR	VIF	Visual Information Fidelity [20]	Available in reference [19]
21	FR	RRED	Reduced Ref. Entropic Difference [21]	Available in reference [19]
22	NR	JQI	JPEG Quality Index [22]	Available in reference [19]
23	NR	HLFI	High-Low Frequency Index [23]	$HLFI(I) = \frac{\sum_{i=1}^{i_l}\lvert F_{i,j}\rvert - \sum_{i=i_h+1}^{N}\sum_{j=j_h+1}^{M}\lvert F_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert F_{i,j}\rvert}$
24	NR	BIQI	Blind Image Quality Index [24]	Available in reference [19]
25	NR	NIQE	Naturalness Image Quality Estimator [25]	Available in reference [19]

IV. PROPOSED WORK

Existing work has made contributions to the state of the art in the field of biometric security. Some of the key contributions are

a. validation of new biometric system

b. demonstrate "Image quality assessment" as a technique for securing biometric systems against various kinds of attacks

c. comparative results with other existing solutions

d. utilize publically available databases for reproducible evaluation of multiple biometric traits

The proposed research work presents software-based fake biometric detection method by identifying optimum set of image quality measures and thus provides an efficient approach for evaluation of multimodalities. In the current research, currently identified 25 parameters may be extended further by considering following additional quality measures [27] [28] [29] [30].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

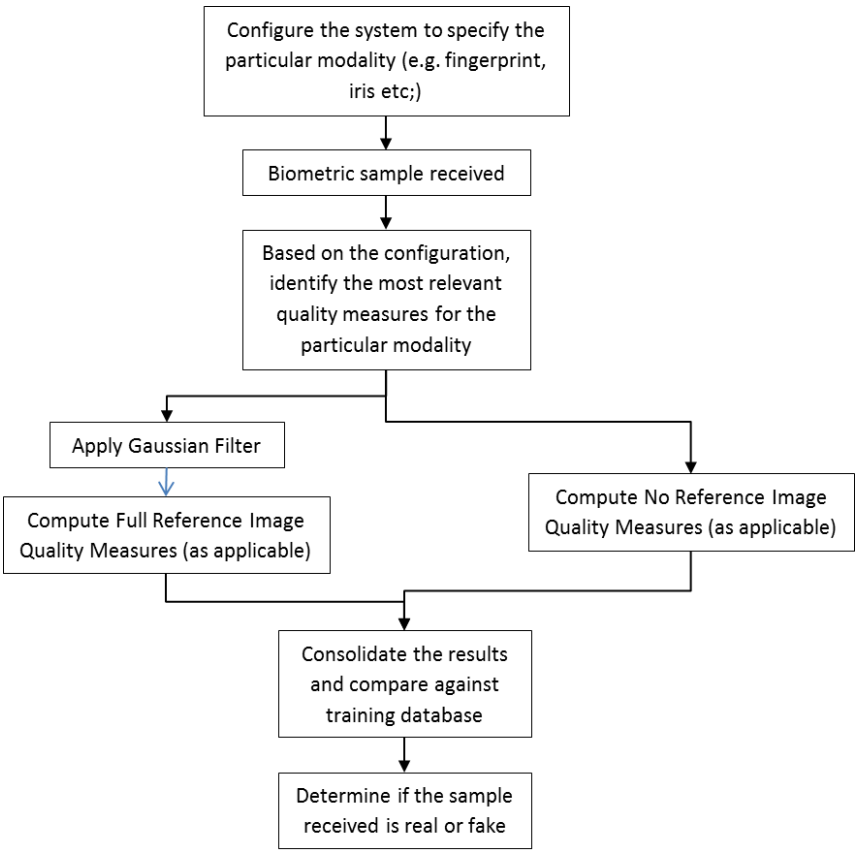
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Sr. No.	Name	Acronym
1	Multi-Scale SSIM Index	MSSIM
2	Visual Signal-To-Noise Ratio	VSNR
3	Gradient Similarity Based Metric Index (GSM)	GSM
4	Spectral Residual Based Similarity	SR-SIM
5	Pixel-Based VIF	VIFP
6	Universal Quality Index	UQI
7	Information Fidelity Criterion	IFC
8	Noise Quality Measure	NQM
9	A Visual Saliency Induced Index	VSI
10	Spatial Spectral Entrophy Quality	SSEQ
11	Information Content Weighted SSIM Index	IW-SSIM
12	Riesz Transforms Based Feature Similarity Index	RFSIM

Based on the existing research, it is determined that certain quality measures are more relevant for certain modalities. Hence in the proposed system, there will be a provision to configure the system for a specific modality as per the specific implementation. The flowchart below illustrates the high level functioning of the system. In this way, the performance of the system can be optimized without compromising accuracy.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

V. CONCLUSION AND FUTURE WORK

In the last few years, the analysis of risks of various types of attacks against biometric systems has been a prominent field of research. This leads to a great progress in the area of safety for biometric based applications to protect biometric systems from vulnerabilities like spoofing attacks. Liveness assessment can be applied to the biometric systems to protect them against harmful attacks. In this paper, a novel, software-based protection measure is proposed to protect the system against fraudulent biometric system access attempts.

It is observed that image quality properties of real access & fraudulent attacks will be different. This software-based method computes relevant features based on the specific modality from more than 25 image quality features of biometric sample to verify its legitimacy. This would result in optimum performance of the system without impacting the accuracy.

Future enhancement for this work can be, a) Assessment of video quality measures, b) Further added modalities such as hand geometry, veins, c) Extension of new image quality measures implemented.

REFERENCES

[1] Javier Galbally, Sebastien Marcel, and Julian Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 2, FEBRUARY 2014
[2] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003
[3] P. Lapsley, J. Lee, D. Pare, N. Hoffman, "Anti-fraud biometric sensor that accurately detects blood flow", US Patent, 1998
[4] Denis Baldisserra , Annalisa Franco , Dario Maio , Davide Maltoni, "Fake fingerprint detection by odor analysis", " in Proc. IAPR ICB. Springer LNCS-3832, pp. 265–272, 2006.
[5] Biel L, Pettersson O, Philipson L, Wide P. "ECG analysis: a new approach in human identification", " IEEE Trans. on Instrumentation and Measurement, vol. 50, pp. 808–812, 2001.
[6] A. Antonelli , R. Cappelli , D. Maio , D. Maltoni, "Fake finger detection by skin distortion analysis", IEEE Transactions on Information Forensics and Security, vol.1, pp. 363-373, 2006.
[7] 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, 2012
[8] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in Proc. 5th IAPR ICB, pp. 271–276, Mar./Apr. 2012
[9] 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
[10] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.
[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] 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.
[13] 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.
[14] 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.
[15] 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.
[16] N. B. Nill and B. Bouzas, "Objective image quality measure derived from digital image power spectra," Opt. Eng., vol. 31, no. 4, pp. 813–825, 1992.
[17] 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.
[18] 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.
[19] (2012). LIVE [Online]. Available: http://live.ece.utexas.edu/research/Quality/index.htm
[20] 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.
[21] 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.
[22] Z. Wang, H. R. Sheikh, and A. C. Bovik, "No-reference perceptual quality assessment of JPEG compressed images," in Proc. IEEE ICIP, pp. 477–480, Sep. 2002
[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, 2009
[24] 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.
[25] 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.
[26] D. Maltoni, D. Maio, A.Jain and S.Prabhakar, "Handbook of Fingerprint Recognition", New York, NY, USA: Springer-Verlag, 2009

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

[27] Lin Zhang, Lei Zhang, Xuanqin Mou, and David Zhang," A COMPREHENSIVE EVALUATION OF FULL REFERENCE IMAGE QUALITY ASSESSMENT ALGORITHMS", IEEE Int. Conf. Image Process. 2012
[28] L. Zhang and H.Y. Li, "SR-SIM: A fast and high performance IQA index based on spectral residual," ICIP'12, pp. 1473-1476, 2012
[29] Z. Wang, E. P. Simoncelli, and A. C. Bovik, "Multi-scale structural similarity for image quality assessment," in Proc. Asilomar Conf. Signals, Syst. Computers, Vol. 2, p. 1398 Nov. 2003
[30] Lin Zhang, Ying Shen, and Hongyu Li,, "VSI: A Visual Saliency-Induced Index for Perceptual Image Quality Assessment", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 10, OCTOBER 2014

BIOGRAPHY

Nilima Ashok Kulkarni is a Master of Engineering (M.E.) student in Department of Computer Engineering, Sinhgad Academy Of Engineering, Pune, Maharashtra, India. She received Bachelor of Engineering (B.E.) degree in 1997 from BAMU, Aurangabad, MS, India. Her research interests are Image Processing, Computer Security & Biometrics.