Fake Biometric Trait Detection Using Image Quality Features

Prathamesh M. Sonavane
Research Scholar
Government College of Engineering, Aurangabad, India

***Abstract* - Biometric systems are vulnerable to spoofing attack. A reliable and efficient countermeasure is needed in order to combat the epidemic growth in identity theft. To ensure biometric system security, liveness assessment can be applied in order to guard against such harmful spoofing attacks. In this paper, we present novel software based protection measure against fraudulent biometric system access attempt. Legitimate biometric sample comprises of efficient information that can be analyzed to discriminate it from self-manufactured, synthetic or reconstructed fake biometric trait used in fraudulent system access. This novel software based method computes more than 25 Reference and No-Reference image quality features of biometric sample to verify its legitimacy. These extracted features are efficient to judge between legitimate and imposter sample. Proposed approach makes biometric system more users friendly, fast, less complex than the hardware based system and more suitable for real time applications.**

***Index Terms* – Biometric system protection, liveness assessment, Reference and No-Reference image Quality features, security, spoof**

I. INTRODUCTION

Biometric is epidemically growing technology for automated recognition or verification of the identity of a person using unique physical or behavioral characteristics such as fingerprints, face, iris, retina, voice, signature and hand geometry etc. To establish a personnel identity biometric relies on - who you are or what you do , as opposed to what you remember -such as a PIN/password or what you possess -such as an ID card.

However, significant advances have been achieved in biometrics, several spoofing techniques have been developed to deceive the biometric systems, and the security of such systems against attacks is still an open problem. Among the different threats analyzed, the direct or spoofing attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in traits such as the fingerprint, the face, the signature, or even the gait and multimodal approaches. Spoofing attacks occur when a person tries to masquerade as someone else falsifying the biometrics data that are captured by the acquisition sensor in an attempt to circumvent a biometric system and thereby gaining illegitimate access and advantages. Some type of synthetically produced artifact e.g. gummy finger, printed iris image, face mask, photograph, video, 3d Model or mimic the behavior of the genuine user (e.g., gait, signature) etc. are used by the imposter to spoof the biometric system. Therefore, there is an increasing need to detect such attempts of attacks to biometric systems.

Liveness detection is one of the existing countermeasure against spoofing attack. It aims at physiological signs of life in biometric sample such as eye blinking, facial expression changes, mouth movements, finger skin sweat, blood pressure, specific reflection properties of the eye etc. by adding special sensors to biometric system. Use of multimodal system is an another beneficial countermeasure against spoofing attack. Combining face or iris or fingerprint recognition with other biometric modalities such as gait and speech is notion of multimodal system . Indeed, multimodal systems are intrinsically more difficult to spoof than uni-modal systems. Multimodal system are more complex than the uni-modal systems.

Liveness detection methods are usually classified into one of two groups: Hardware based (special sensor based) schemes usually present a higher fake detection rate, but they are very costly and complex. Software based techniques are in general less expensive than hardware based as no extra device such as special sensor is needed. Unlike hardware based technique, Software technique satisfy almost all the requirement of challenging engineering problem of liveness detection– i.e. a)Non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user b)User friendly, people should not be reluctant to use it c)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 d) Low cost, a wide use cannot be expected if the cost is excessively high e)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. These two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems.

In this work we present novel software based protection measure against fraudulent biometric system access attempt. Legitimate biometric sample comprises of efficient information that can be analyzed to discriminate it from self-manufactured, synthetic or reconstructed fake biometric trait used in fraudulent system access by imposter. This novel software based method computes more than 25 Reference and No-Reference image quality features of biometric sample to identify its legitimacy. These extracted features are efficient to judge between legitimate and imposter sample. Proposed approach makes biometric system more user friendly, fast, less complex than the hardware based system and more suitable for real time applications.

The rest of this paper is organized as follows. In Section II, we describe the existing work which has done in aforementioned research topic . In Section III, we present proposed and possible extension for the existing research work. In last section we conclude this research work.

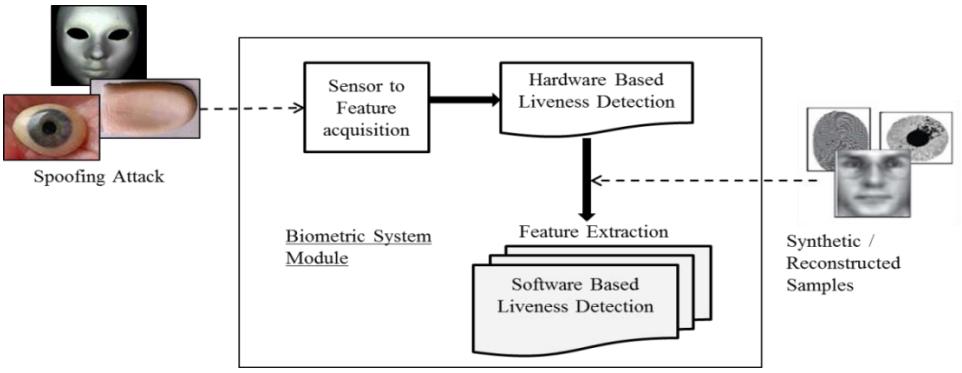

Figure 1 Types of attacks: Spoofing Attack on Hardware-based Biometric liveness detection system and Spoofing or Reconstructed/Synthetic Samples attack on Software-based Biometric liveness detection System

II. LITERATURE SURVEY

Following assumption must be considered while using the image quality assessment for liveness detection - "It is expected that quality of a fake image captured in an attack attempt will be different than a quality of real sample acquired in the normal operation scenario for which the sensor was designed".

In the present research work "quality-difference" hypothesis, explores the potential of general image quality assessment as a protection method against different biometric attacks. Various image quality aspects can be assessed using different quality measures. Each quality measure present different sensitivity to image artifacts and distortions viz. additive noise can be assessed using mean squared error(MSE), whereas others such as the spectral phase error are more sensitive to blur; while gradient-related features react to distortions concentrated around edges and textures. Therefore, using a wide range of IQMs exploiting complementary image quality properties, should permit to detect the aforementioned quality differences between real and fake samples expected to be found in many attack attempts. Expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both type of images i.e. entropy, structural distortions or natural appearance etc. For example, biometric sample images captured from a printed paper are more likely to be blurred or out of focus due to trembling; face images captured from a mobile or another camera device will probably be over- or under-exposed; and it is not rare that local acquisition artifacts are visible in fingerprint images captured from a gummy finger 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.

Existing Work

Existing protection method performs novel parameterization using 25 general image quality measures . Input biometric sample is classified into one of two classes: real or fake based on simple classifier built using parameterization performed using efficient 25 general image quality measures .

The process involves 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 . Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) Classifiers are used in existing work . It uses both Full reference and No reference image quality measures, which are selected using four general criteria : performance, complementarity, complexity, speed. General image quality measures are fast to compute and easy to combined with simple classifiers. This biometric protection method is applicable to multimodalities such as face, fingerprint and iris. Following section overviews the 25 image quality measures set used in research work.

Full-Reference Image Quality Measures

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample.

A. Error Sensitivity Measures

Traditional perceptual image quality assessment approaches are based on measuring the errors (i.e., signal differences) between the distorted and the reference images, and attempt to quantify these errors in a way that simulates human visual error sensitivity features.

a. Pixel Difference Measures

$$PSNR(I,I') = 10\log(\frac{\max(I^2)}{mse(I,I')}) \qquad \text{MSE}(\text{I},\text{I}') = \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{i,j} - I'_{i,j})^2$$

It Computes the distortion between two images on the basis of their pixel wise differences. It includes: 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). E.g.

$$MD(I,I') = \max|I_{i,j}\text{-}I'_{i,j}| \qquad NAE(I,I') = (\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}|I_{i,j} - I'_{i,j}|}{\sum_{i=1}^{N}\sum_{j=1}^{M}|I_{i,j}|})$$

b. Correlation-Based Measures

The similarity between two digital images can also be quantified in terms of the correlation. It includes: Normalized Cross-Correlation(NXC), Mean Angle Similarity (MAS) and Mean Angle-Magnitude Similarity (MAMS). E.g.

$$\text{NXC}(I,I') = (\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}|I_{i,j}.I'_{i,j}|}{\sum_{i=1}^{N}\sum_{j=1}^{M}(I'_{i,j})^2}) \qquad \text{MAS}(\text{I},\text{I}') = 1 - \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}(\alpha_{i,j})$$

Table 1 Full-Reference Image Quality Measures Summary

#	Name	Acronym
1	Mean Square Error	MSE
2	Peak Signal To Noise Ratio	PSNR
3	Signal To Noise Ratio	SNR
4	Structural Content	SC
5	Maximum Difference	MD
6	Average Difference	AD
7	Normalized Absolute Error	NAE
8	R-Averaged Maximum Difference	RAMD
9	Laplacian Mean Squared Error	LMSE
10	Normalized Cross-Correlation	NXC
11	Mean Angle Similarity	MAS
12	Mean Angle-Magnitude Similarity	MAMS
13	Total Edge Difference	TED
14	Spectral Magnitude Error	SME
14	Total Corner Difference	TCD
15	Spectral Phase Error	SPE
17	Gradient Magnitude Error	GME
18	Gradient Phase Error	GPE
19	Structural Similarity Index Measure	SSIM
20	Visual Information Fidelity	VIF
21	Reduced Reference Entropic Difference Index	RREDI

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 the human visual system and in many computer vision algorithms including quality assessment applications. It includes: Total Edge Difference(TED) and Total Corner Difference (TCD). E.g.

$$\text{TED}(\text{I},\text{I}') = \frac{1}{MN}\sum_{i=1}^{N}\sum_{j=1}^{M}(I_{\boldsymbol{E}i,j} - I_{\boldsymbol{E}'i,j})$$

d. Spectral Distance Measures

The Fourier transform is another traditional image processing tool which has been applied to the field of image quality assessment. It includes Spectral Magnitude Error (SME) and the Spectral Phase Error (SPE).E.g.

$$\text{SME}(\text{I},\text{I}') = \tfrac{1}{MN}\textstyle\sum_{i=1}^{N}\sum_{j=1}^{M}\left(|\boldsymbol{F}_{i,j}| - |\boldsymbol{F}'_{i,j}|\right)^2$$

e. Gradient-Based Measures.

Many of the distortions that can affect an image are reflected by a change in its gradient. It Includes: Gradient Magnitude Error (GME) and Gradient Phase Error (GPE).

B. Structural Similarity Measures:

It is Based on error sensitivity. Structural similarity was proposed following the hypothesis that the human visual system is highly adapted for extracting structural information from the viewing field .Here includes:

Structural Similarity Index Measure (SSIM).

C. Information Theoretic Measures

The quality assessment problem may also be understood, from an information theory perspective, as an information-fidelity problem .Here include: Visual Information Fidelity (VIF) and Reduced Reference Entropic Difference index (RRED).

No-Reference IQ Measures

Automatic no-reference image quality assessment (NR-IQA) algorithms try to handle the very complex and challenging problem of assessing the visual quality of images, in the absence of a reference.

a. Distortion-Specific Approaches

These techniques rely on previously acquired knowledge about the type of visual quality loss caused by a specific distortion

Here include: JPEG Quality Index (JQI) ,High-Low Frequency Index (HLFI).

b. Training-Based Approaches

A model is trained using clean and distorted images. Then, the quality score is computed based on a number of features extracted from the test image and related to the general model. Here we include: Blind Image Quality Index (BIQI).

c. Natural Scene Statistic Approaches

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. Here we include: Natural Image Quality Evaluator (NIQE)

Table 2 No-Reference Image Quality Measures Summary

#	Name	Acronym
22	JPEG Quality Index (JQI)	JQI
23	High-Low Frequency Index (HLFI)	HLFI
24	Blind Image Quality Index (BIQI)	BIQI
25	Natural Image Quality Evaluator (NIQE)	NIQE

III. PROPOSED WORK

Existing work has made several contributions to the state-of-the-art in the field of biometric security, in particular: it has shown the high potential of image quality assessment for securing biometric systems against a variety of attacks, proposal and validation of a new biometric protection method, reproducible evaluation on multiple biometric traits based on publicly available databases, comparative results with other previously proposed protection solutions. However, this research also opens new possibilities for future work, including : Extension of the considered 25-feature set with new image quality measures and further evaluation on biometric multimodalities such as face, fingerprint, iris and palm print biometric.

In the proposed research work we present novel software based fake biometric trait detection method which involves extension of previously considered 25 image quality feature set and evaluation of this method on multimodalities i.e. Iris, Fingerprint, Face and Palm print. Following section Summarizes newly selected image quality feature set which will be extension for the aforementioned 25 image quality set.

Table 3 New Image Quality Measures to be added Summary

#	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

It consist both Full reference and No reference image quality measures, which are selected using four general criteria : performance, complementarity, complexity, speed. After adding these features to aforementioned 25 image quality set, performance of the new system will be evaluated. Image quality assessment task is implemented using the MATLAB Tool . In which simple classifier is used to classify the input biometric sample into one of two classes i.e. Real or Fake. Firstly, the newly build Classifier is trained with the parameterization of extended image quality feature set then applied to the iris, face, fingerprint and palm print image database samples for fakeness detection task.

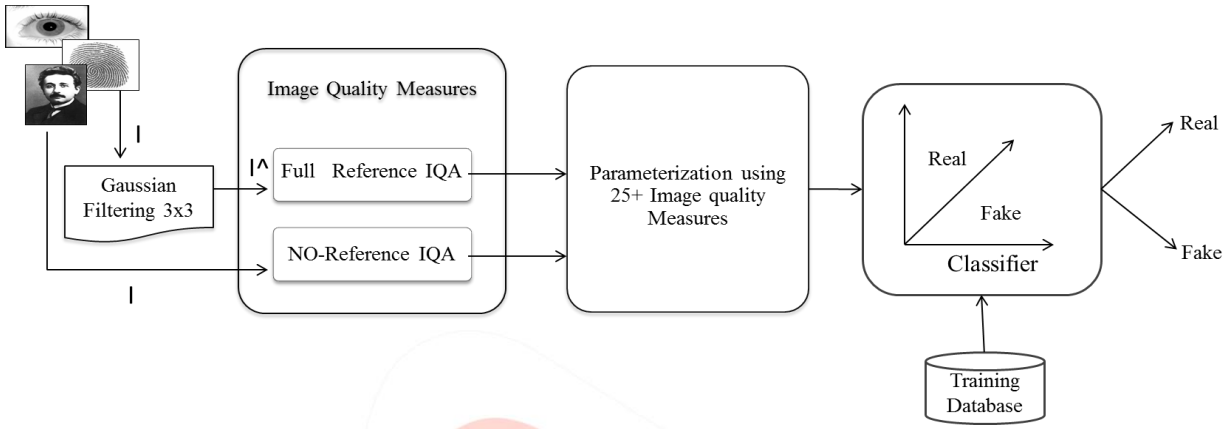

Figure 2 Operational flow of Proposed Image quality assessment based biometric Security protection Method

Lastly, research results are reported in terms of: False Genuine Rate (FGR), which accounts for the number of false samples that were classified as real; False Fake Rate (FFR), which gives the probability of an image coming from a genuine sample being considered as fake. The Half Total Error Rate (HTER) is computed as HTER = (FGR + FFR)/2.

IV. Conclusion

To protect biometric systems from vulnerabilities like spoofing attack. Live ness assessment can be applied to the biometric systems in order to guard them against such harmful attacks. In this paper, we proposed novel software based protection measure against fraudulent biometric system access attempt. Legitimate biometric sample comprises of efficient quality features that can be analyzed to discriminate it from self-manufactured, synthetic or reconstructed fake biometric trait used in fraudulent system access. This novel software based method computes more than 25 Reference and No-Reference image quality features of biometric sample to verify its legitimacy. These extracted features are efficient to judge between legitimate and imposter sample. Proposed approach suggests utilization of high potential of image quality assessment for securing biometric systems against a variety of attacks.

This new biometric protection approach contributes to security of biometric system at fast, less complex design than the hardware based system. It also makes the biometric system more user friendly, more suitable for real time applications. Future enhancement for this work could be, 1)Assessment of video quality measures for video attacks , 2)Extension of the aforementioned image quality feature set with new image quality measures, 3) Hand geometry, Vein based biometric systems can be implemented and evaluated for the present work.

V. Acknowledgment

I am thankful to Prof. Mrs. S.D. Sapkal Department of Master of Computer Application. Aurangabad, India. My guide for her valuable guidance that she provided me at various stages throughout this research work. She has been a source of motivation enabling me to give my best efforts in this work.

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] 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.

[3] 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.

[4] M. Eskicioglu and P. S. Fisher, “Image quality measures and their performance,” IEEE Trans. Commun., vol. 43, no. 12, pp. 2959–2965, Dec. 1995.

[5] 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.

[6] 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.

[7] 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.
[8] 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.
[9] http://live.ece.utexas.edu/research/Quality/index.html 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.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] H.R. Sheikh, M.F. Sabir, and A.C. Bovik, "A statistical evaluation of recent full reference image quality assessment algorithms", IEEE Trans. on Image Processing, vol. 15, no. 11, pp. 3440-3451, 2006.
[16] Ismail Avcıbas , Bulent Sankur, Khalid Sayood ,"Statistical evaluation of image quality measures ",Journal of Electronic Imaging 11(2), 206–223 (April 2002).
[17] Hamid Rahim Sheikh, Muhammad Farooq Sabir, Alan C. Bovik, "A Statistical Evaluation of Recent Full Reference Image Quality Assessment Algorithms", IEEE TRANS. IMAGE PROCESSING.
[18] Hamid Rahim Sheikh, Alan Conrad Bovik, and Gustavo de Veciana ,"An Information Fidelity Criterion for Image Quality Assessment Using Natural Scene Statistics", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 14, NO. 12, DECEMBER 2005.
[19] Lin Zhang, Lei Zhang, Xuanqin Mou, and David Zhang," A COMPREHENSIVE EVALUATION OF FULL REFERENCE IMAGE QUALITY ASSESSMENT ALGORITHMS".
[20] Lin Zhang and Hongyu Li, "SR-SIM: A FAST AND HIGH PERFORMANCE IQA INDEX BASED ON SPECTRAL RESIDUAL".
[21] Zhou Wang, Eero P. Simoncelli and Alan C. Bovik, "MULTI-SCALE STRUCTURAL SIMILARITY FOR IMAGE QUALITY ASSESSMENT".
[22] Lin Zhanga, Lei Zhanga1, and Xuanqin Moub,"RFSIM: A FEATURE BASED IMAGE QUALITY ASSESSMENT METRIC USING RIESZ TRANSFORMS", Proceedings of 2010 IEEE 17th International Conference on Image Processing September 26-29, 2010, Hong Kong .
[23] 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 .
[24] Jieying Zhu and Nengchao Wang," Image Quality Assessment by Visual Gradient Similarity", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 3, MARCH 2012.
[25] Alphy George, S. John Livingston, "A SURVEY ON FULL REFERENCE IMAGE QUALITY ASSESSMENT ALGORITHMS", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 ISSN: 2321-7308.
[26] I. Avcibas, B. Sankur, and K. Sayood, "Statistical valuation of image quality measures," J. Electron. Imag., vol. 11, no. 2, pp. 206–223, 2002.