ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Fake Detection of IRIS, Fingerprint and 2D Face Images by Using Image Quality Parameters

D.Gireesh Babu
PG Scholar,
Dept of VLSI & ES,
Gates Institute of Technology,
Gooty, Anantapuramu, AP, India.

G.Nagesham
Assistant Professor,
Dept of VLSI & ES,
Gates Institute of Technology,
Gooty, Anantapuramu, AP, India.

ABSTRACT:

Image and biometric details of man is design artificial by using some software it is called scooping. Scooping is one of the most problem in developing security world. In scooping process is done by so many software and skilled person. In future world security is the important one every person. The biometric data will help in all fields to identification process. So we need to develop new method to find and rectifies the scooping data's. In this paper, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding aliveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 11 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits. This process is done by mat lab image processing.

Index Terms:

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

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 counter measure 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 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 is more complex than the unimodal systems.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

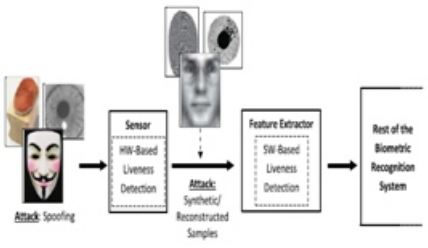

Fig. 1. Types of attacks potentially detected by hardware-based (spoofing) and software-based (spoofing + reconstructed/synthetic samples) liveness detection techniques.

III PROPOSED 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.

A. Full-Reference IQ Measures:

Full-reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. In the problem of fake detection addressed in this work such a reference image is unknown, as the detection system only has access to the input sample. Then, the quality between both images (I and ˆI) is computed according to the corresponding full-reference IQA metric. This approach assumes that the loss of quality produced by Gaussian filtering differs between real and fake biometric samples. 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 quantifythese errors in a way that simulates human visual error sensitivity features. Although their efficiency as signal fidelity measures is somewhat controversial, up to date, these are probably the most widely used methods for IQA as they conveniently make use of many known psychophysical features of the human visual system, they are easy to calculate and usually have very low computational complexity. Several of these metrics have been included in the 25-feature parameterization proposed in the present work. For clarity, these features have been classified here into five different categories

A.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).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 1 Full-Reference Image Quality Measures Summary

#	Type	Acronym	Name	Ref.	Description
1	FR	MSE	Mean Squared Error	[29]	$MSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})^2$
2	FR	PSNR	Peak Signal to Noise Ratio	[30]	$PSNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\max[\mathbf{I}^2]}{MSE(\mathbf{I},\hat{\mathbf{I}})})$
3	FR	SNR	Signal to Noise Ratio	[31]	$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N\cdot M\cdot MSE(\mathbf{I},\hat{\mathbf{I}})})$
4	FR	SC	Structural Content	[32]	$SC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{\mathbf{I}}_{i,j})^2}$
5	FR	MD	Maximum Difference	[32]	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})$
6	FR	AD	Average Difference	[32]	$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})$
7	FR	NAE	Normalized Absolute Error	[32]	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}\rvert}$
8	FR	RAMD	R-Averaged MD	[29]	$RAMD(\mathbf{I},\hat{\mathbf{I}},R) = \frac{1}{R}\sum_{i=1}^{R}\max_i\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert$
9	FR	LMSE	Laplacian MSE	[32]	$LMSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(\Lambda(\mathbf{I}_{i,j})-\Lambda(\hat{\mathbf{I}}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}\Lambda(\mathbf{I}_{i,j})^2}$
10	FR	NXC	Normalized Cross-Correlation	[32]	$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\cdot\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$
11	FR	MAS	Mean Angle Similarity	[29]	$MAS(\mathbf{I},\hat{\mathbf{I}}) = 1-\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\alpha_{i,j})$
12	FR	MAMS	Mean Angle Magnitude Similarity	[29]	$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1-\lvert 1-\alpha_{i,j}\rvert)(1-\lvert\frac{\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert}{2^{bpp}}\rvert)$
13	FR	TED	Total Edge Difference	[33]	$TED(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{\mathbf{E},i,j}-\hat{\mathbf{I}}_{\mathbf{E},i,j}\rvert$
14	FR	TCD	Total Corner Difference	[33]	$TCD(I,\hat{I}) = \frac{\lvert N_{cc}-\hat{N}_{cc}\rvert}{\max[N_{cc},\hat{N}_{cc}]}$
15	FR	SME	Spectral Magnitude Error	[34]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{F}_{i,j}\rvert-\lvert\hat{\mathbf{F}}_{i,j}\rvert)^2$
16	FR	SPE	Spectral Phase Error	[34]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(\mathbf{F}_{i,j})-\arg(\hat{\mathbf{F}}_{i,j})\rvert^2$
17	FR	GME	Gradient Magnitude Error	[35]	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{G}_{i,j}\rvert-\lvert\hat{\mathbf{G}}_{i,j}\rvert)^2$
18	FR	GPE	Gradient Phase Error	[35]	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(\mathbf{G}_{i,j})-\arg(\hat{\mathbf{G}}_{i,j})\rvert^2$
19	FR	SSIM	Structural Similarity Index	[36]	See [36] and practical implementation available in [37]
20	FR	VIF	Visual Information Fidelity	[38]	See [38] and practical implementation available in [37]
21	FR	RRED	Reduced Ref. Entropic Difference	[39]	See [39] and practical implementation available in [37]
22	NR	JQI	JPEG Quality Index	[40]	See [40] and practical implementation available in [37]
23	NR	HLFI	High-Low Frequency Index	[41]	$SME(\mathbf{I}) = \frac{\sum_{i=1}^{N_1}\sum_{j=1}^{M_1}\lvert\mathbf{F}_{i,j}\rvert-\sum_{i=N_1+1}^{N}\sum_{j=M_1+1}^{M}\lvert\mathbf{F}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{F}_{i,j}\rvert}$
24	NR	BIQI	Blind Image Quality Index	[42]	See [42] and practical implementation available in [37]
25	NR	NIQE	Naturalness Image Quality Estimator	[43]	See [43] and practical implementation available in [37]

IV.RESULTS:

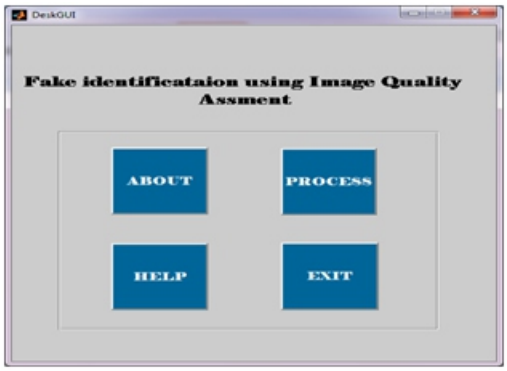

Fig 2 Shows The Fake Identification using Image Quality assment

Fig 3 shows the Image quality values measured

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

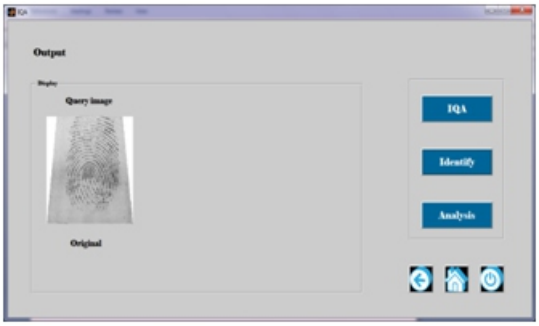

Fig 4 Shows The Original or fake Images

V CONCLUSION:

The study of the biometric systems against different types of attacks has been a very active field in feture. This is enchanced the field of security technologies for biometric-based applications. However, in spite of tis noticeable improvement, the development of efficient protection methods against known threats has proven to be a challenging task.

Simple visual inspection of an image of a real biometric trait and a fake sample of the same trait shows that the two images can be very similar and even the human eye may find it difficult to make a distinction between them after a short inspection. Yet, some disparities between the real and fake images may become evident once the images are translated into a proper feature space.

In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. Following this "quality-difference" hypothesis, in the present research work we have explored the potential of general image quality assessment as a protection tool against different biometric attacks (with special attention to spoofing). For this purpose we have considered a feature space of 11 complementary image quality measures which we have combined with simple classifiers to detect real and fake access attempts.

The novel protection method has been evaluated on three largely deployed biometric modalities such as the iris, the fingerprint and 2D face, using publicly available databaseswith well defined associated protocols. This way, the results in proposed system contain some conclusions. It adabt the different biometric details by high performance method, It able to analysis multi biometric details, and it is simplest, accure and less complexity method.

VI FEATURE ENCHANCEMENT:

In our proposed we use software based sooping attack system. In this process get several advantages over the exisiting system but in feature some enchancement is there for good security in biometric authendication. In that characters we use hybrid the hardware and software based biometric system to increase the accuracy of authentication.

REFERENCES:

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

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

[3] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," Pattern Recognit., vol. 43, no. 3, pp. 1027–1038, 2010.

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

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

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

[7] ISO/IEC 19792:2009, Information Technology—Security Techniques—Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.[8] Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.

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

[10] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu,et al., "First international fingerprint

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

liveness detection competition—LivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716. 2009,pp. 12–23.

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

AUTHOR'S DETAILS:

D.Gireesh Babu

pursuing his M.Tech (VLSI &Embedded Systems Design) Stream From Gates Institute of Technology, Gooty, Anantapuramu, Andhra Pradesh. His areas of interest are VLSI and Embedded system designing Fields.

G.Nagesham

M.Tech,(cne) working as a Assistant professor For ECE Department in Gates Institute of Technology, Gooty, Anantapuramu, Andhra Pradesh, His areas of interest Mobile communication, wireless communication ,cryptography .