International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 9, September 2014)

Liveness Detection& Image Quality Assessment for Fake Biometric Detection

Chetlapalli Deepika Goud
PG Research Scholar
VNR Vignana Jyothi Institute Of Engineering & Technology
Hyderabad, India

Mr. C. V. RamBabu
Sr. Assistant professor, Electronics and Instrumentation
VNR Vignana Jyothi Institute Of Engineering & Technology
Hyderabad, India

Abstract: **To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this project, 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 liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. 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**

Keywords: **Image Quality Assesment, Liveness Detection, Lab View**

1. INTRODUCTION

Biometric technology has developed rapidly in recent years and it is more direct, user friendly and convenient. But biometric systems are vulnerable to spoof attacksand it is an easy way to spoof biometric system. A secure system needs Liveness detection in order to guard against such spoofing. To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. In this project, 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 liveness 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 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. The entire project is simulated using Laboratory Virtual Instrument Engineering Workbench (Lab View) platform.

2. LITERATURE REVIEW

According to Javier Galbally,C.MSebastien Marcel, Julian Fierrez (2010), the general image quality features extracted from a image to distinguish between the legitimate and imposter samples. Considering that the fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario. Following this quality difference the authors explored the potential of general image quality assessment as a protection method against different biometric attacks with special attention towards spoofing. As the implemented features do not evaluate any specific property of a given biometric modality or of a specific attack, they may be computed on any image. According to SaptarshiChakraborty, Dhrubajyoti Das(2014), the face liveness detection approaches are categorized based on the various types of techniques used for liveness detection. This categorization helps understanding different spoof attacks scenarios and their relation to the developed solutions. A review of the face liveness detection works is presented. The difference between the live face from not live face ,which is a major security issue is presented. According to S.Z. Li, J. Galbally, A. Anjos·S. Marcel (2011), the different types of spoofing attacks related to face, iris and fingerprint are mentioned and also about the anti-spoofing methods are explained. The sites of the available data bases is given for the reference and the values are compared with the trained set. Through the difference in the obtained values the real and fake images can be distinguished and the spoofing attacks can be controlled. According to Zhou Wang, Alan Conrad Bovik , Hamid Rahim Sheikh (2004), methods for assessing perceptual image quality traditionally attempted to quantify the visibility of errors (differences) between a distorted image and a reference image using a variety of known properties of the human visual system. Under the assumption that human visual perception is highly adapted for extracting structural information from a scene, we introduce an alternative complementary framework for quality assessment based on the degradation of structural information. As a specific example of this concept, we develop a Structural Similarity Index and demonstrate its promise through a set of intuitive examples, as well as comparison to both subjective ratings and state-of-the-art objective methods on a database of images compressed are explained.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 9, September 2014)

3. RESEARCH METHODOLOGY

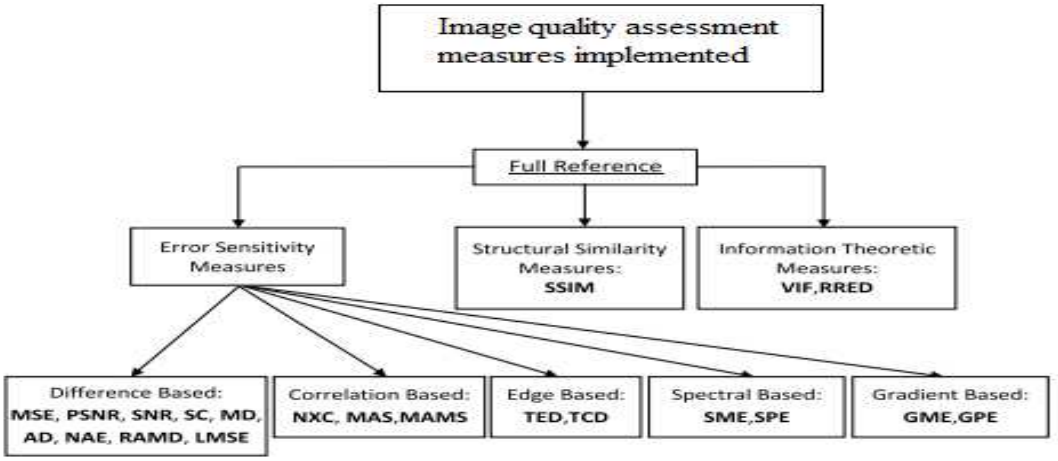

Figure 1: Classification of the 25 image quality measures

Full-reference IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. The input grey-scale image I (of size N×M) is filtered with a low-pass Gaussian kernel (σ=0.5 and size 3×3) in order to generate a smoothed version ˆI. 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.

In this project, we use a novel software-based multi-biometric and multi-attack protection method which use the image quality assessment. It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario.Many spoofing attacks, especially those which involve taking a picture of a facial image displayed in a 2D device (e.g., spoofing attacks with printed iris or face images), may be regarded as a type of image manipulation which can be effectively detected, as shown in the present work, by the use of different quality features.Different features measuring trait-specific quality properties have already been used for liveness detection purposes in fingerprint and iris applications. However, even though these two works give a solid basis to the use of image quality as a protection method in biometric systems, none of them is general. For instance, measuring the ridge and valley frequency may be a good parameter to detect certain fingerprint spoofs, but it cannot be used in iris liveness detection. On the other hand, the amount of occlusion of the eye is valid as an iris anti-spoofing mechanism, but will have little use in fake fingerprint detection. This same reasoning can be applied to the vast majority of the liveness detection methods found in the state-of-theart. Although all of them represent very valuable works which bring insight into the difficult problem of spoofing detection, they fail to generalize to different problems as they are usually designed to work on one specific modality and in many cases, also to detect one specific type of spoofing attack. 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 project we propose a novel parameterization using19 general image quality measures. All the 19 features of the full reference image quality measures are explained below.

3.1 FR-IQMs: 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. The error sensitivity measures are classified into five different categories according to the image property measures.

3.2 Pixel Difference Measures:These features compute the distortion between two images on the basis of their pixel wise differences. Here we include: 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).

3.3 Correlation-Based Measures: The similarity between two digital images can also be quantified in terms of the correlation function. A variant of correlation based measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and distorted images. These features include Normalized Cross-Correlation (NXC), Mean Angle Similarity (MAS) and Mean Angle Magnitude Similarity (MAMS). In the MAS and MAMS entries in Table I, $\alpha_{i,j}$ denotes the angle between two vectors, defined as, $\alpha_{i,j}$

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 9, September 2014)

=2πarccosIi,jIi,j————————————————||Ii,j||·||Ii,j||, whereIi,j,ˆIi,j———————————————— denotes the scalar product. As we are dealing with positive matrices I andˆ I, we are constrained to the first quadrant of the Cartesian space so that the maximum difference attained will be π/2, therefore the coefficient 2/π is included for normalization.

***3.4 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. Since the structural distortion of an image is tightly linked with its edge degradation, here we have considered two edge-related quality measures: Total Edge Difference (TED) and Total Corner Difference (TCD). In order to implement both features, which, we use:(i)the Sobel operator to build the binary edge maps IE andˆ IE; (ii)the Harris corner detector to compute the number of corners Ncr and ˆ Ncr found in I and ˆI.

3.5 Spectral Distance Measures:The Fourier transform is another traditional image processing tool which has been applied to the field of image quality assessment. In this project we will consider as IQ spectral-related features: the Spectral Magnitude Error (SME)and the Spectral Phase Error (SPE).

3.6 Gradient Based Measures:Gradients convey important visual information which can be of great use for quality assessment. Many of the distortions that can affect an image are reflected by a change in its gradient. Therefore, using such information, structural and contrast changes can be effectively captured. Two simple gradient-based features are included in the biometric protection system proposed in this project, Gradient Magnitude Error (GME) and Gradient Phase Error (GPE).

3.7 Structural Similarity Measures:Although being very convenient and widely used, the aforementioned image quality metrics based on error sensitivity present several problems which are evidenced by their mismatch (in many cases) with subjective human-based quality scoring systems. In this scenario, a recent new paradigm for image quality assessment based on structural similarity is used following the hypothesis that the human visual system is highly adapted for extracting structural information from the viewing field. Therefore, distortions in an image that come from variations in lighting, such as contrast or brightness changes (nonstructural distortions), should be treated differently from structural ones. Among these recent objective perceptual measures, the Structural Similarity Index Measure (SSIM), has the simplest formulation and has gained widespread popularity in a broad range of practical applications. In view of its very attractive properties, the SSIM has been included in the 25-feature parameterization.

3.8 Information Theoretic Measures:The quality assessment problem may also be understood, from an information theory perspective, as an information-fidelity problem (rather than a signal-fidelity problem). The core idea behind these approaches is that an image source communicates to a receiver through a channel that limits the amount of information that could flow through it, thereby introducing distortions. The goal is to relate the visual quality of the test image to the amount of information shared between the test and the reference signals, or more precisely, the mutual information between them. Under this general framework, image quality measures based on information fidelity exploit the (in some cases imprecise) relationship between statistical image information and visual quality. In this project we consider two of these information theoretic features they are the Visual Information Fidelity (VIF) and the Reduced Reference Entropic Difference index (RRED). Both metrics are based on the information theoretic perspective of IQA but each of them take either a global or a local approximation to the problem, as is explained below. The VIF metric measures the quality fidelity as the ratio between the total information (measured in terms of entropy) ideally extracted by the brain from the whole distorted image and the total information conveyed within the complete reference image. This metric relies on the assumption that natural images of perfect quality, in the absence of any distortions, pass through the human visual system (HVS) of an observer before entering the brain, which extracts cognitive information from it. For distorted images, it is hypothesized that the reference signal has passed through another “distortion channel” before entering the HVS. The VIF measure is derived from the ratio of two mutual information quantities: the mutual information between the input and the output of the HVS channel when no distortion channel is present (i.e., reference image information) and the mutual information between the input of the distortion channel and the output of the HVS channel for the test image. Therefore, to compute the VIF metric, the entire reference image is required as quality is assessed on a global basis.

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 sub band 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. This way, contrary to the VIF feature, for the RRED it is not necessary to have access the entire reference image but only to a reduced part of its information (i.e., quality is computed locally). This required information can even be reduced to only one single scalar in case all the scaled entropy terms in the selected wavelet sub band are considered in one single block.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 9, September 2014)

#	Type	Acronym	Name	Description
1	FR	MSE	Mean Squared Error	$MSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})^2$
2	FR	PSNR	Peak Signal to Noise Ratio	$PSNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\max(\mathbf{I}^2)}{MSE(\mathbf{I},\hat{\mathbf{I}})})$
3	FR	SNR	Signal to Noise Ratio	$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N\cdot M\cdot MSE(\mathbf{I},\hat{\mathbf{I}})})$
4	FR	SC	Structural Content	$SC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{\mathbf{I}}_{i,j})^2}$
5	FR	MD	Maximum Difference	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert$
6	FR	AD	Average Difference	$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})$
7	FR	NAE	Normalized Absolute Error	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}\rvert}$
8	FR	RAMD	R-Averaged MD	$RAMD(\mathbf{I},\hat{\mathbf{I}},R) = \frac{1}{R}\sum_{r=1}^{R}\max_r\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert$
9	FR	LMSE	Laplacian MSE	$LMSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(\mathbf{I}_{i,j})-h(\hat{\mathbf{I}}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}h(\mathbf{I}_{i,j})^2}$
10	FR	NXC	Normalized Cross-Correlation	$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\cdot\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$
11	FR	MAS	Mean Angle Similarity	$MAS(\mathbf{I},\hat{\mathbf{I}}) = 1-\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\alpha_{i,j})$
12	FR	MAMS	Mean Angle Magnitude Similarity	$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1-[1-\alpha_{i,j}][1-\frac{\lvert\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert\rvert}{255}])$
13	FR	TED	Total Edge Difference	$TED(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{\mathbf{E}i,j}-\hat{\mathbf{I}}_{\mathbf{E}i,j}\rvert$
14	FR	TCD	Total Corner Difference	$TCD(I,\hat{I}) = \frac{\lvert N_{cr}-\hat{N}_{cr}\rvert}{\max(N_{cr},\hat{N}_{cr})}$
15	FR	SME	Spectral Magnitude Error	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{F}_{i,j}\rvert-\lvert\hat{\mathbf{F}}_{i,j}\rvert)^2$
16	FR	SPE	Spectral Phase Error	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(\mathbf{F}_{i,j})-\arg(\hat{\mathbf{F}}_{i,j})\rvert^2$
17	FR	GME	Gradient Magnitude Error	$SME(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\lvert\mathbf{G}_{i,j}\rvert-\lvert\hat{\mathbf{G}}_{i,j}\rvert)^2$
18	FR	GPE	Gradient Phase Error	$SPE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\arg(\mathbf{G}_{i,j})-\arg(\hat{\mathbf{G}}_{i,j})\rvert^2$
19	FR	SSIM	Structural Similarity Index	See [36] and practical implementation available in [37]

Table 1: list of the 19 image quality measures used for biometric protection

4. RESULT & ANALYSIS

The algorithm which was developed on LabView extracts 19 Image Quality Measurements in to front panel display as well as fin an excel sheet. ATVS-flrDB is a publicly available database which consists of 800 image files of real and fake each. Out of 800 we have extracted 19 IQM's for 50 real and 50 fake images as a classifier set, thus saving them all into an excel sheet to find out properties of each IQM and compared respective results of real and fake images to classify whether real value is less than fake or vice versa.

Name of IQM	Classification	No of Images satisfies Condition out of 50	Property Classified
MSE	R < F	36	R<F
	R > F	14	
PSNR	R < F	14	R > F
	R > F	36	
SNR	R < F	14	R > F
	R > F	36	
SC	R < F	36	R<F

	R > F	14	
MD	R < F	18	R > F
	R > F	32	
AD	R < F	14	R > F
	R > F	36	
NAE	R < F	28	R<F
	R > F	22	
RAMD	R < F	16	R > F
	R > F	34	
LMSE	R < F	34	R<F
	R > F	16	
NXC	R < F	15	R > F
	R > F	35	
MAS	R = F	50	R > F
MAMS	R < F	35	R<F
	R > F	15	
TED	R < F	27	R<F
	R > F	23	
TCD	R < F	30	R<F
	R > F	20	
SME	R < F	34	R<F
	R > F	16	
SPE	R < F	15	R > F
	R > F	35	
GME	R < F	35	R<F
	R > F	15	
GPE	R < F	14	R > F
	R > F	36	
SSIM	R < F	37	R<F
	R > F	13	

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 9, September 2014)

5. CONCLUSION & FUTURE SCOPE

In summary, the main theme of this work is to find the difference between a real and the fake image using the 19 image quality measures to ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample, this increases the protection of a biometric system. The algorithm was developed on LabVIEW extracts 19 Image Quality Measures in to front panel. ATVS-flrDB is a publicly available database which consists of 800 image files of real and fakeeach. Out of 800 we have extracted 19 IQM's for 50 real and 50 fake images as a classifier set, thus saving them all into an excel sheet to find out properties of each IQM and compared respective results of real and fake images to classify whether real value is less than fake or vice versa. Based on the property classified from table, we have applied these properties to another set of 50 real and fake images to classify no of real images satisfies the condition. Out of which we were able to satisfy 75% of real images to be real wherein we were able to get false genuine report as 25%.The proposed method is able to consistently perform at a high level for different biometric traits ("multi-biometric").The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection ("multi-attack"). The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios. The error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions. In addition to its very competitive performance, and to its "multi-biometric" and "multi-attack" characteristics, the proposed method presents some other very attractive features such as: it is simple, fast, non-intrusive, user-friendly and cheap, all of them very desirable properties in a practical protection system.The liveness detection method is classified into two types online process and offline process, the 19 IQM's work is offline process when this is combined with the online process it will be the most desirable protection approach to increase the security of biometric systems. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate, while software-based techniques are in general less expensive (as no extra device is needed), and less intrusive since their implementation is transparent to the user. Hence when both combined together it can be a effective biometric protection system.The present project also opens new possibilities for future work, including:

i) extension of the considered 19 feature set with new image quality measures.

iv) use of video quality measures for video attacks (e.g., illegal access attempts).

.

REFERENCES

[1]. A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.

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

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

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

[6]. J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez,et al., "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates,"PatternRecognit. Lett., vol. 31, no. 8, pp. 725–732, 2010.

[7]. 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.

[8]. 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.

[9]. 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.

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

[11]. 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.