OPEN ACCESS
ISSN: 2249-6645

International
Journal
Of Modern Engineering Research (IJMER)

Detection of Fake Biometric: Application to Face Recognition, IRIS and FINGERPRINT

G.Naidu Babu[1], B.Doss[2]
*(Department of ECE, Kodada Institute of Technology & Science for Women, India)
Email: naidu_nrt@yahoo.co.in)
** (Department of ECE,JNTUACollege of Engineering(Autonomous)Ananthapuramu , India
Email: dasalways4u@gmail.com)

ABSTRACT : Spoofing is one of the most problem in developing security world. . In future world security is the important to every person. . So we need to develop new method to find and rectifies the spoofing datas. 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 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 11 general image quality features extracted from one image 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. In this process done by mat lab image processing.

Keywords : attacks, biometrics, countermeasures, Image quality assessment, security

I. INTRODUCTION

IN RECENT years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research [1]: the publication of many research works disclosing and evaluating different biometric vulnerabilities [2], [3], the proposal of new protection methods [4][5],related book chapters [6], the publication of several standards in the area [7], [8], the dedication of specific tracks sessions and workshops in biometric-specific and general signal processing conferences [9], the organization of competitions focused on vulnerability assessment [10], [11], the acquisition of specific datasets [12], [13], the creation of groups and laboratories specialized in the evaluation of biometric security [14], or the existence of several European Projects with the biometric security topic as main research interest[15], [16].

All these initiatives clearly highlight the importance given by all parties involved in the development of biometrics (i.e., researchers, developers and industry) to the improvement of the systems security to bring this rapidly emerging technology into practical use.Among the different threats analyzed, the so-called *direct* or *spoofing* attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris [2], the fingerprint [17], the face [13], the signature [18], or even the gait [19] and multimodal approaches [20]. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., gummy finger, printed iris image or face mask), or tries to mimic the behaviour of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As this type of attacks are performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective.

The aforementioned works and other analogue studies, have clearly shown the necessity to propose and develop specific protection methods against this threat. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them, improving this way the robustness and security level of the systems .Besides other anti-spoofing approaches such as the use of multi biometrics or challenge-response methods, special attention has been paid by researchers and industry to the *liveness detection* techniques, which use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain

demanding requirements : *(i)* non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user; *(i i)* user friendly, people should not be reluctant to use it; *(i i i)* 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 (i.e., false rejection) of the biometric system. Liveness detection methods are usually classified into one of two groups (see Fig. 1):

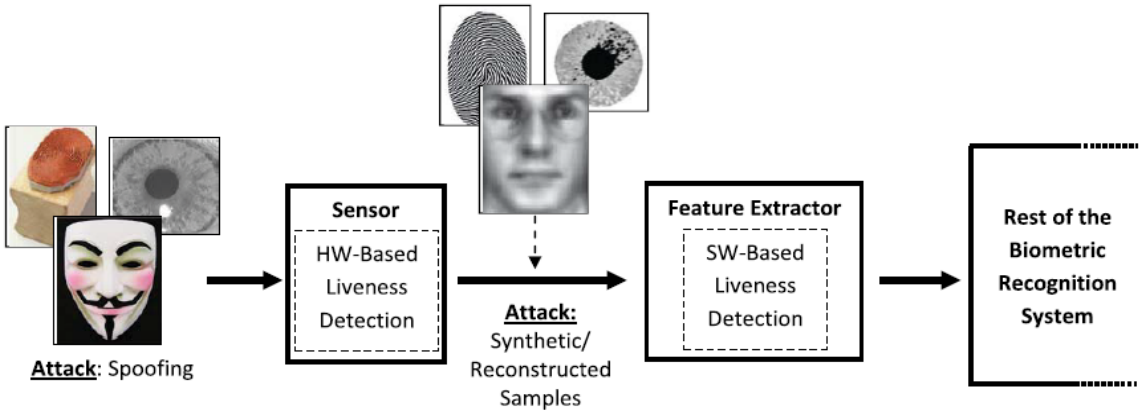

Fig.1.Types of attacks detected by hardware based and software-based liveness detection techniques

(i) Hardware-based techniques, which add some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye);
(i i) Software-based techniques, in this case the fake trait is detected once the sample has been acquired with a standard sensor The 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. As a coarse comparison, hardware-based schemes usually present a higherfake 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. Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module which makes them potentially capable of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks. For instance, software-based methods can protect the system against the injection of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor

II. IMAGE QUALITY ASSESSMENT FORLIVENESS DETECTION

The use of image quality assessment for liveness detection is motivated by the assumption that: "*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 for which the sensor was designed.*" Human observers very often refer to the "different appearance" of real and fake samples to distinguish between them. As stated above, the different metrics and methods designed for IQA intend to estimate in an objective and reliable way the perceived appearance of images by humans.

.

III. THE SECURITY PROTECTION METHOD

The problem of fake biometric detection can be seen as a two-class classification problem where an input biometric sample has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image "realism" given the extracted set of features. In the present work we propose a novel parameterization using 25 general image quality measures. A general diagram of the protection approach proposed in this work is shown in Fig. 2.

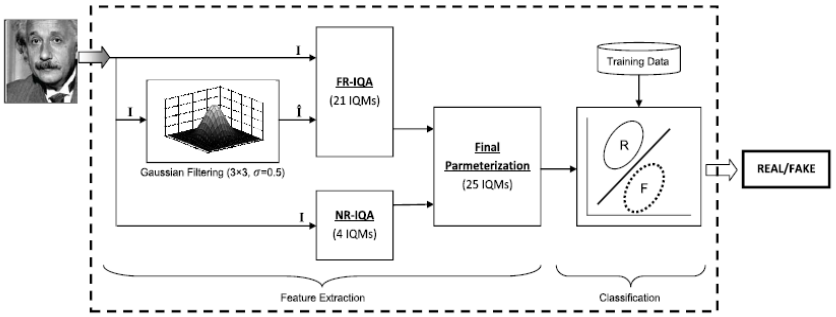

Fig.2.General diagram for the biometric protection method based on Image Quality Assessment

In order to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake (i.e., the same image acquired for biometric recognition purposes). Furthermore, as the method operates on the whole image without searching for any trait-specific properties, it does not require any preprocessing steps (e.g., fingerprint segmentation, iris detection or face extraction) prior to the computation of the IQ features. This characteristic minimizes its computational load. Once the feature vector has been generated the sample is classified as real (generated by a genuine trait) or fake (synthetically produced), using some simple classifiers. In particular, for our experiments we have considered standard implementations in Matlab of the Linear DiscriminantAnalysis (LDA) and Quadratic Discriminant Analysis (QDA)classifiers . The final 25 selected image quality measures are highlighted in bold in the text and in Fig. 3.

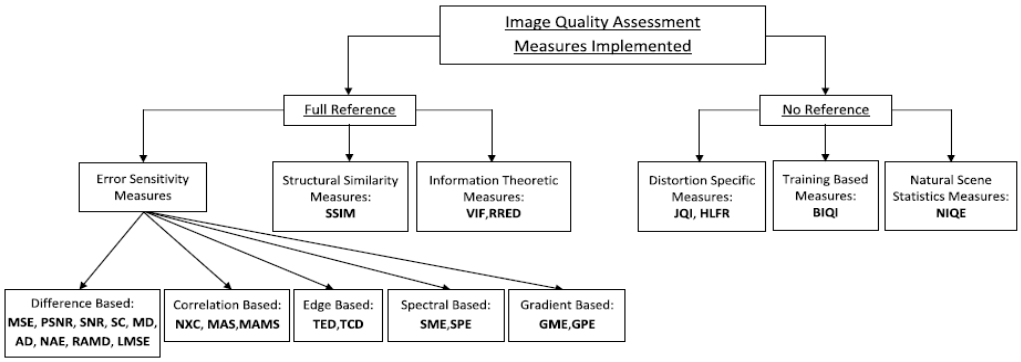

Fig.3.Classification f the 25 image quality measures implemented in the work.

A. Full-Reference IQ Measures

Full-reference (FR) IQA methods rely on the availability ofa clean undistorted reference image to estimate the quality ofthe 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. In order to circumvent this limitation, the same strategy already successfully used for image manipulation detection in and for steganalysis is implemented here. As shown in Fig. 2, the input grey-scale image **I** (of size $N \times M$) is filtered with a low-pass Gaussian kernel ($\sigma = 0.5$ and size 3×3) in order to generate a smoothed version $\hat{\mathbf{I}}$. Then, the quality between both images (**I** and $\hat{\mathbf{I}}$) is computed according to the corresponding full-reference IQA metric. Submit your manuscript electronically for review. prepare it in two-column format, including figures and tables(untill it don't fit properly and data is not visible).

pixel Difference measures . These featurescompute the distortion between two images on the basis of their pixelwise 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**). The formal definitions for each of these features are given in Table I.

Correlation-based measures . The similarity between two digital images can also be quantified interms of the correlation function. A variant of correlationbased measures can be obtained by considering the statistics of the angles between the pixel vectors of the original and distorted images. These features include (also defined in Table I): Normalized Cross-Correlation (**NXC**), Mean Angle Similarity (**MAS**) and Mean Angle- Magnitude Similarity (**MAMS**).**Spectral distance measures**. The Fourier transform is another traditional image processing tool which has been applied to the field of image quality assessment [29]. In this work we will consider as IQ

spectral-related features: the Spectral Magnitude Error (**SME**) and the Spectral Phase Error (**SPE**), defined in Table I (where **F** and ˆ**F** are the respective Fourier transforms of **I** and ˆ**I**), and arg*(***F***)* denotes phase.

TABLE-I : List of the image quality measures implementation for biometric method

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

B. No-Reference IQ Measures

Unlike the objective reference IQA methods, in general the human visual system does not require of a reference sample to determine the quality level of an image. Depending on the images used to train this model and on the *a priori* knowledge required, the methods are coarsely divided into one of three trends :The JPEG Quality Index (**JQI**), The High-Low Frequency Index (**HLFI**), Natural Image Quality Evaluator (**NIQE**)

IV. EXPERIMENTS AND RESULTS

The evaluation experimental protocol has been designed with a two-fold objective:

• First, evaluate the "multi-biometric" dimension of the protection method. That is, its ability to achieve a good performance, compared to other trait-specific approaches, under different biometric modalities. For this purpose three of the most extended image-based biometric modalities have been considered in the experiments: iris, fingerprints and 2D face.

• Second, evaluate the "multi-attack" dimension of the protection method. That is, its ability to detect not only spoofing attacks (such as other liveness detectionspecific approaches) but also fraudulent access attempts carried out with synthetic or reconstructed samples (see Fig. 1).

The task in *all* the scenarios and experiments described in the next sections is to automatically distinguish between real and fake samples. As explained in Section III, for this purpose we build a 25-dimensional simple classifier based on general IQMs (see Fig. 2). Therefore, in all cases, results are reported in terms of: the False Genuine Rate (FGR), which accounts for the number of false samples that were classified as real; and the False Fake Rate (FFR), which gives the probability of an image coming from a genuine sample being consider as fake. The Half Total Error Rate (HTER) is computed as HTER = *(*FGR + FFR*)*/2

Fig.4.Typical real iris images and coressponding fake samples.

A. Results: Iris

For the iris modality the protection method is tested under two different attack scenarios, namely: *i*) spoofing attack and *i i*) attack with synthetic samples. *1) Results: Iris-Spoofing:* The database used in this spoofing scenario is the ATVS-FIr DB which may be obtained from the Biometric Recognition Group-ATVS.1 .*2) Results: Iris-Synthetic:* In this scenario attacks are performed with synthetically generated iris samples which are injected in the communication channel between the sensor and the feature extraction module (see Fig. 1).

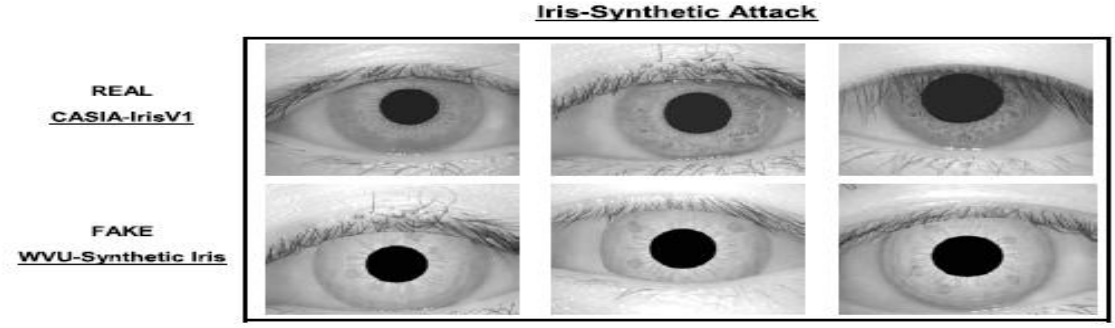

Fig.5.Typical real iris images from CASIA-Iris and fake samples from WVU-Synthetic Iris DB.

In Fig. 5 we show some typical real and fake iris images that may be found in the CASIA-IrisV1 DB and in the WVU-Synthetic Iris DB

TABLE-II Results obtained by the proposed Biometric protection based on IQA

	Results: Iris			
	FFR	FGR	HTER	Av. Exec. (s)
Iris-Spoof.	4.2	0.25	2.2	0.238
Iris-Spoof. [28]	1.3	4.9	3.1	2.563
Iris-Synthetic	3.4	0.8	2.1	0.156

The results achieved by the proposed protection method based on IQA on this attacking scenario are shown in the bottom row of Table II. In spite of the similarity of real and fake images, the global error of the algorithm in this scenario is 2.1%.

B. Results: Fingerprints

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

C. Results: 2D Face

The performance of the IQA-based protection method has also been assessed on a face spoofing database: the REPLAY-ATTACK DB which is publicly available from the IDIAP Research Institute. Three different types of attacks were considered: *i*) *print*, illegal access attempts are carried out with hard copies of high-resolution digital photographs of the genuine users; *i i*) *mobile*, the attacks are performed using photos and videos taken

with the iPhone using the iPhone screen; *i i i*) *highdef*, similar to the mobile subset but in this case the photos and videos are displayed using an iPad screen with resolution 10 × 768. Some typical images (frames extracted from the videos) from real and fake (print, mobile and highdef) access attempts that may be found in the REPLAY-ATTACK DB are shownin Fig. 7.

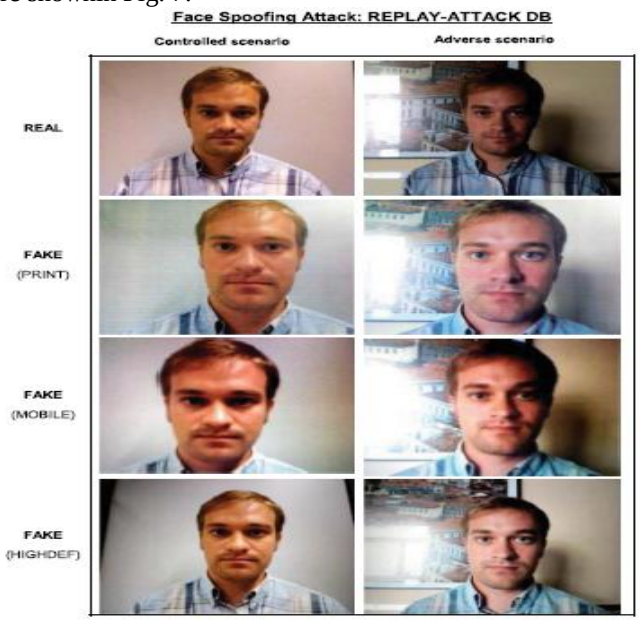

Fig.6.Typical examples of real and fake face images that can be found in public REPLY-ATTACK DB used in the face anti-spoofing experiments

The database is also released with face detection data. These data was used to crop and normalize all the faces to a 64×64 bounding box prior to the anti-spoofing experiments. This way the final classification results are ensured to be totally unbiasedand not dependent on contextual-specific artifacts such as: unwanted changes in the background; different sizes of the heads (we can see in Fig. 6 that fake faces are in general slightly bigger than the ones in real images); a black frame due to an imperfect fitting of the attack media on the capturing device screen, etc.

V. CONCLUSION

Simple visual inspection of an image of a real biometric trait and a fake sample of the same trait shows thatthe 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. These differences come from the fact that biometric traits, as 3D objects, have their own optical qualities (absorption, reflection, scattering, refraction), which other materials (paper, gelatin, electronic display) or synthetically produced samples do not possess. Furthermore, biometric sensors are designed to provide good quality samples when they interact, in a normal operation environment, with a real 3D trait. If this scenario is changed, or if the trait presented to the scanner is an unexpected fake artifact (2D, different material, etc.),the characteristics of the captured image may significantly vary.

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 IEEE Int. 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 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.

[12] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," J. Telecommun. Syst., vol. 47, nos. 3–4, pp. 3–254, 2011.

[13] 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.

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

[15] (2012). BEAT: Biometrices Evaluation and Testing [Online]. Available: http://www.beat-eu.org/

[16] (2010). Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available: http://www.tabularasa-euproject.org/

[17] 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," Pattern Recognit. Lett., vol. 31, no. 8, pp. 725–732, 2010.

[18] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366–375.

[19] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, "Can gait biometrics be spoofed?" in Proc. IAPR ICPR, 2012, pp. 3280–3283.

[20] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in Proc. IEEE 5th Int. Conf. BTAS, Sep. 2012, pp. 283–288