2014 22nd International Conference on Pattern Recognition

Face Anti-Spoofing Based on General Image Quality Assessment

Javier Galbally
Joint Research Centre, European Commission, Ispra, Italy
Email: javier.galbally@jrc.ec.europa.eu

Sébastien Marcel
IDIAP Research Institute, Martigny, Switzerland
Email: sebastien.marcel@idiap.ch

***Abstract*—A new face anti-spoofing method based on general image quality assessment is presented. The proposed approach presents a very low degree of complexity which makes it suitable for real-time applications, using 14 image quality features extracted from one image (i.e., the same acquired for face recognition purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on two publicly available datasets, show very competitive results compared to other state-of-the-art methods tested on the same benchmarks. The findings presented in the work clearly suggest that the analysis of the general image quality of real face samples reveals highly valuable information that may be very efficiently used to discriminate them from fake images.**

I. Introduction

The study of the vulnerabilities of biometric systems against spoofing has been a very active field of research in recent years [1]. Biometric *spoofing*, also referred to as biometric *direct attacks*, is widely understood in the specialised literature as the ability to fool a biometric system into recognizing an illegitimate user as the genuine one, by means of presenting to the sensor a synthetic forged version (i.e., artefact) of the original biometric trait.

In 2D-face recognition spoofing attacks are generally carried out in one of three ways: i) *Photo Attacks*: These fraudulent access attempts are performed presenting to the recognition system a photograph of the genuine user. This image may be printed on a paper or displayed on the screen of a digital device such as a mobile phone or a tablet. ii) *Video Attacks*: In this case, the attacker does not use a still image, but replays a video of the genuine client using a digital device (e.g., mobile phone, tablet or laptop). iii) *Mask Attacks*: In these cases the spoofing artefact is a 3D mask of the genuine client's face, increasing the difficulty to find accurate countermeasures. In addition, all the previous types of attacks have a number of variants depending on the resolution of the attack device, the type of support used to present the fake copy, or the type of external variability allowed (e.g., illumination or background conditions).

All these attacks have been shown in different works to pose a real security threat to 2-D face recognition systems [2], [3], [4]. Therefore, in order to enhance the robustness of this technology, the biometric community has proposed a number of anti-spoofing approaches that attempt to prevent direct attacks. Among the different proposed techniques we may highlight: the detection over a video sequence of face motion (e.g., eye blinking or face gestures) [5], [6]; the analysis of the face texture using different tools such as multiple Difference of Gaussian (DoG) filters [3], the Fourier Spectrum [7], or a more recent trend based on Local Binary Patterns [8], [2]; the combination of the face with another related and easily measurable biometric such as the voice [9]; Or the use of specific sensors to acquire near-infrared or multispectral images [10], [11].

The previous efforts, and other similar works, have led to big advances in the field of security-enhancing technologies for face-based applications. However, in spite of this noticeable improvement, the development of efficient protection methods against known direct attacks has proven to be a challenging task that still requires novel algorithms. The big diversity of spoofing attacks described above makes it very difficult to design a protection method with a high performance in all possible scenarios [12].

In the present research work we explore the potential of general Image Quality Assessment (IQA) as a protection method against face spoofing attacks. In the current state-of-the-art, the rationale behind the use of IQA features for liveness detection is supported by three factors:

- Image quality has been successfully used in previous works for image manipulation detection [13] and steganalysis [14] in the forensic field. To a certain extent, many face spoofing attacks, especially those which involve taking a picture of a facial image displayed in a 2D device (e.g., spoofing attacks with printed face images), may be regarded as a type of image manipulation which can be effectively detected, as shown in the present research work, by the use of different quality features.
- In addition to the previous studies in the forensic area, different features measuring trait-specific quality properties have already been used for liveness detection purposes in fingerprint and iris applications [15], [16].
- Human observers very often refer to the "different appearance" of real and fake samples to distinguish between them. The different metrics and methods designed for IQA intend to estimate in an objective and reliable way the perceived appearance of images by humans.

The proposed anti-spoofing approach is evaluated on the two largest public face-spoofing databases currently available, which contain both photo and video attacks captured under different conditions and with several acquisition devices. Thanks to the use of a public benchmark (i.e., databases and protocols),

1051-4651/14 $31.00 © 2014 IEEE
DOI 10.1109/ICPR.2014.211

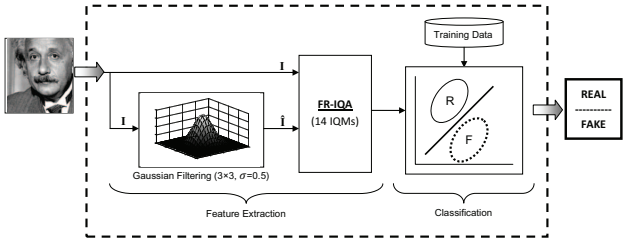

Fig. 1. General diagram of the biometric protection method based on Image Quality Assessment (IQA) proposed in the present work. See Table I for the complete list and formal definitions of the 14 full-reference Image Quality Measures (FR-IQM). See Sect. II for a more detailed description of each IQM.

the new method can be fairly compared to other state-of-the-art algorithms, showing a remarkable performance and a great adaptation capability to detect different types of direct attacks. Furthermore, the proposed solution only requires one input image acquired with a regular sensor (i.e., the same sample used later for authentication purposes) and therefore presents some other very desirable characteristics in a practical biometric protection system such as: simplicity, speed, non-intrusive, user-friendly and cheap.

The rest of the paper is structured as follows. The proposed anti-spoofing method is presented in Sect. II. The databases and experimental protocol are described in Sect. III. Evaluation and comparative results are given in Sect IV. Conclusions are finally drawn in Sect. V.

II. The Proposed Anti-spoofing 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 14 general full-reference image quality measures.

The goal of an objective full-reference image quality measure (IQM) is to provide a quantitative score that describes the degree of fidelity or, conversely, the level of distortion of a given test image according to an original distortion-free image.

A general diagram of the protection approach proposed in this work is shown in Fig. 1. 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 face 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., face detection) 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 a simple Linear Discriminant Analysis (LDA) classifier.

The final 14 selected image quality measures are summarized in Table I. Details about each of these 14 IQMs are given in the Sect. II-A.

A. Image Quality Measures

As described above, full-reference 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. In order to circumvent this limitation, the same strategy already successfully used for image manipulation detection in [13] and for steganalysis in [14], is implemented here.

As shown in Fig. 1, the input grey-scale image $\mathbf{I}$ (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 distorted version $\hat{\mathbf{I}}$. Then, the quality between both images ($\mathbf{I}$ and $\hat{\mathbf{I}}$) 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. Assumption which is confirmed by the experimental results given in Sect. IV.

The 14 full-reference IQM considered in the present work may be classified into three different groups according to the type of image information measured, namely:

- **Pixel Difference measures** [20], [17]. These features compute 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.
  In the RAMD entry in Table I, $\max_r$ is defined as the r-highest pixel difference between two images. For the present implementation, $R = 10$.
  In the LMSE entry in Table I, $h(\mathbf{I}_{i,j}) = \mathbf{I}_{i+1,j} + \mathbf{I}_{i-1,j} + \mathbf{I}_{i,j+1} + \mathbf{I}_{i,j-1} - 4\mathbf{I}_{i,j}$.
- **Correlation-based measures** [20], [17]. 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 (also defined in Table I): Normalized Cross-Correlation (**NXC**), Mean Angle Similarity (**MAS**) and Mean Angle-Magnitude Similarity (**MAMS**).
  In the MAMS entry in Table I, $\alpha_{i,j} = \frac{2}{\pi} \cos^{-1} \frac{\langle \mathbf{I}_{i,j}, \hat{\mathbf{I}}_{i,j} \rangle}{||\mathbf{I}_{i,j}|| ||\hat{\mathbf{I}}_{i,j}||}$
- **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 [21].

#	Acronym	Name	Ref.	Description
1	MSE	Mean Squared Error	[17]	$MSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})^2$
2	PSNR	Peak Signal to Noise Ratio	[18]	$PSNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\max(\mathbf{I}^2)}{MSE(\mathbf{I},\hat{\mathbf{I}})})$
3	SNR	Signal to Noise Ratio	[19]	$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N\cdot M\cdot MSE(\mathbf{I},\hat{\mathbf{I}})})$
4	SC	Structural Content	[20]	$SC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{\mathbf{I}}_{i,j})^2}$
5	MD	Maximum Difference	[20]	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|$
6	AD	Average Difference	[20]	$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})$
7	NAE	Normalized Absolute Error	[20]	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|}{\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{I}_{i,j}\|}$
8	RAMD	R-Averaged MD	[17]	$RAMD(\mathbf{I},\hat{\mathbf{I}},R) = \frac{1}{R}\sum_{r=1}^{R}\max_r\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|$
9	LMSE	Laplacian MSE	[20]	$LMSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}(h(\mathbf{I}_{i,j})-h(\hat{\mathbf{I}}_{i,j}))^2}{\sum_{i=1}^{N-1}\sum_{j=2}^{M-1}h(\mathbf{I}_{i,j})^2}$
10	NXC	Normalized Cross-Correlation	[20]	$NXC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}\cdot\hat{\mathbf{I}}_{i,j})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}$
11	MAS	Mean Angle Similarity	[17]	$MAS(\mathbf{I},\hat{\mathbf{I}}) = 1-\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\frac{2}{\pi}\cos^{-1}\frac{\langle\mathbf{I}_{i,j},\hat{\mathbf{I}}_{i,j}\rangle}{\|\mathbf{I}_{i,j}\|\|\hat{\mathbf{I}}_{i,j}\|})$
12	MAMS	Mean Angle Magnitude Similarity	[17]	$MAMS(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(1-[1-\alpha_{i,j}][1-\frac{\|\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\|}{255}])$
13	TED	Total Edge Difference	[21]	$TED(\mathbf{I}_\mathbf{E},\hat{\mathbf{I}}_\mathbf{E}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\|\mathbf{I}_{\mathbf{E}i,j}-\hat{\mathbf{I}}_{\mathbf{E}i,j}\|$
14	TCD	Total Corner Difference	[21]	$TCD(N_{cr},\hat{N}_{cr}) = \frac{\|N_{cr}-\hat{N}_{cr}\|}{\max(N_{cr},\hat{N}_{cr})}$

TABLE I. LIST OF THE 14 IMAGE QUALITY MEASURES (IQMS) IMPLEMENTED IN THE PRESENT WORK AND USED FOR LIVENESS DETECTION. ALL THE FEATURES WERE EITHER DIRECTLY TAKEN OR ADAPTED FROM THE REFERENCES GIVEN. IN THE TABLE: $\mathbf{I}$ DENOTES THE REFERENCE CLEAN IMAGE (OF SIZE $N \times M$) AND $\hat{\mathbf{I}}$ THE DISTORTED VERSION OF THE REFERENCE IMAGE. FOR OTHER NOTATION SPECIFICATIONS AND UNDEFINED VARIABLES OR FUNCTIONS WE REFER THE READER TO THE DESCRIPTION OF EACH PARTICULAR FEATURE IN SECT. II.

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 are computed according to the corresponding expressions given in Table I, we use: (i) the Sobel operator to build the binary edge maps $\mathbf{I}_\mathbf{E}$ and $\hat{\mathbf{I}}_\mathbf{E}$; (ii) the Harris corner detector to compute the number of corners N_{cr} and $\hat{N}_{cr}$ found in $\mathbf{I}$ and $\hat{\mathbf{I}}$.

III. DATABASES AND EXPERIMENTAL PROTOCOL

In order to achieve reproducible results, two publicly available databases with well described evaluation protocols are used in the experimental validation. This has allowed us to compare, in an objective and fair way, the performance of the proposed system with other existing state-of-the-art liveness detection solutions.

In addition, the two databases have complimentary characteristics that permit to analyze in depth the behaviour of face anti-spoofing approaches: on the one hand, the REPLAY-ATTACK DB [2] contains attacks with an increasing level of resolution, captured with a fixed acquisition device; on the other hand, the CASIA-FAS DB [3], considers similar quality attacks, captured with three different resolution devices.

- **REPLAY-ATTACK DB** [2]. It is publicly available from the IDIAP Research Institute[1].
  The database contains short videos (around 10 seconds in mov format) of both real-access and spoofing attack attempts of 50 different subjects, acquired with a 320×240 resolution webcam of a 13-inch MacBook Laptop. The recordings were carried out under two different conditions: i) *controlled*, with a uniform background and artificial lighting; and ii) *adverse*, with natural illumination and non-uniform background.
  Three different types of attacks were considered with an increasing level of resolution: i) *mobile*, the attacks are performed using photos and videos taken with the iPhone using the iPhone screen; ii) *print*, illegal access attempts are carried out with hard copies of high-resolution digital photographs of the genuine users; iii) *highdef*, similar to the mobile subset but in this case the photos and videos are displayed using an iPad screen with resolution 1024×768.
  In addition, access attempts in the three attack subsets (mobile, print and highdef) were recorded in two different modes depending on the strategy followed to hold the attack replay device (mobile phone, paper or tablet): i) *hand*-based and ii) *fixed*-support.
  Some typical images (frames extracted from the videos) from real and fake (mobile, print and highdef) access attempts that may be found in the REPLAY-ATTACK DB are shown in Fig. 3.
- **CASIA FAS-DB** [3]. It is publicly available from the Chinese Academy of Sciences (CASIA) Center for Biomerics and Security Research (CASIA-CBSR) [2].
  The CASIA Face Anti-Spoofing DB contains short videos (around 10 seconds in avi format) of both real-access and spoofing attack attempts of 50 subjects, acquired with three devices with different resolutions: i) *low resolution*, with an old 640×480 USB web camera (model is not specified); ii) *normal resolution*, with a modern 480×640 USB web camera (model is not specified); and iii) *high resolution*, using the

[1] https://www.idiap.ch/dataset/replayattack

[2] http://www.cbsr.ia.ac.cn/english/index.asp

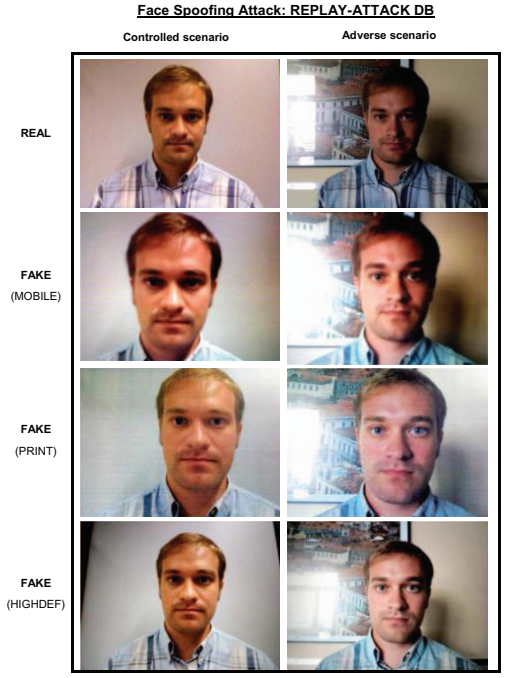

Fig. 2. Typical examples of real and fake (mobile, print and highdef) face images that can be found in the public REPLAY-ATTACK DB. Images were extracted from videos acquired in the two considered scenarios: controlled and adverse.

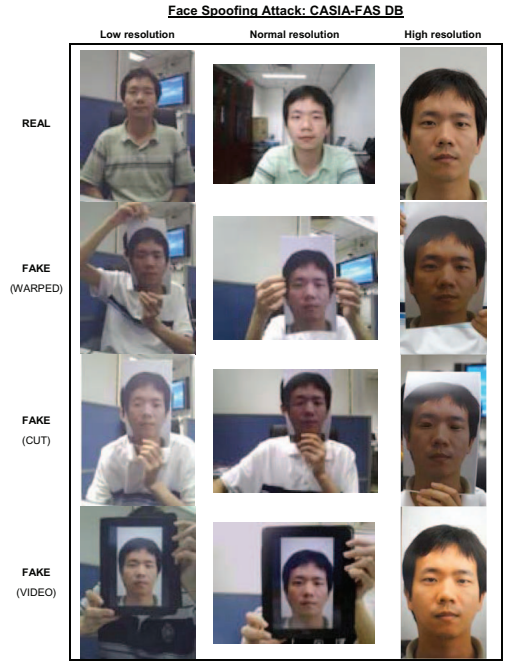

Fig. 3. Typical examples of real and fake (warped, cut and video) face images that can be found in the public CASIA-FAS DB. Images were extracted from videos acquired with the three capturing devices used: low, normal and high resolution.

1920×1080 Sony NEX-5 high definition camera.
Three different types of attacks were considered: i) *warped*, illegal access attempts are carried out with slightly curved hard copies of high-resolution digital photographs of the genuine users; ii) *cut*, the attacks are performed using hard copies of high-resolution digital photographs of the genuine users, where the eyes have been cut out and the face of the attacker is placed behind (i.e., so that eye blinking is forged); iii) *video*, in this case the high resolution videos of the genuine users are replayed in front of the acquisition device using an iPad.
Some typical images (frames extracted from the videos) from real and fake (warped, cut and video) access attempts that may be found in the CASIA-FAS DB are shown in Fig. 3.

The task in *all* the scenarios and experiments described in the results section is to automatically distinguish between real and fake samples. 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 considered as fake. The Half Total Error Rate (HTER) is computed as $\mathrm{HTER} = (\mathrm{FGR} + \mathrm{FFR})/2$.

IV. Results

The experimental protocol takes advantage of the complimentary characteristics of the two considered databases with three objectives: i) determine the performance of the proposed method under increasing-resolution attacks; ii) study the behaviour of the anti-spoofing approach for acquisition devices with different resolutions; iii) establish a comparison with previously presented state-of-the-art liveness detection techniques.

The 14 image quality measures have been implemented in MATLAB, while experimental results have been obtained with the free machine learning toolbox BOB[3] [22].

A. Results: REPLAY ATTACK DB

The database has a perfectly defined associated evaluation protocol which considers three totally independent datasets (in terms of users): train, used to tune the parameters of the method; development, to fix the decision threshold; and test, where final results are computed. The protocol is released with the database and has been strictly followed in the present 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 unbiased and not dependent on contextual-specific artifacts such as: unwanted changes in the background; different sizes of the heads (we can see in Fig. 3 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.

[3]http://idiap.github.com/bob/

	Results: REPLAY-ATTACK DB			
	Mobile	Print	Highdef	Grandtest
	HTER	HTER	HTER	HTER
Hand	2.8	9.3	13.1	15.4
Fixed	3.5	8.4	9.1	12.7
All	3.2	7.9	12.1	15.2

TABLE II. RESULTS OBTAINED ON THE REPLAY-ATTACK DB BY THE PROPOSED FACE ANTI-SPOOFING METHOD FOR THE DIFFERENT SCENARIOS CONSIDERED IN THE REPLAY-ATTACK DB AND FOLLOWING THE ASSOCIATED EVALUATION PROTOCOL.

	Results: REPLAY-ATTACK DB		
	FFR	FGR	HTER
IQA-based	17.9	12.5	15.2
LBP-based [2]	-	-	15.2
LBP-based [2], [8]	-	-	13.9

TABLE III. COMPARISON OF THE RESULTS OBTAINED BY THE IQA-BASED ANTI-SPOOFING METHOD PROPOSED IN THE PRESENT WORK, AND THE LBP-BASED ANTI-SPOOFING TECHNIQUES DESCRIBED IN [2] (PARTIALLY BASED ON THE RESULTS REPORTED ON [8]). RESULTS ARE OBTAINED FOLLOWING THE GRANDTEST PROTOCOL OF THE REPLAY-ATTACK DB (CONSIDERING BOTH HAND AND FIXED SUPPORTS).

	Results: CASIA-FAS DB			
	Warped	Cut	Video	All
	HTER	HTER	HTER	HTER
Low	25.0	23.3	21.7	31.7 (a)
Normal	23.3	16.7	23.3	22.2 (b)
High	10.0	11.7	6.7	5.6 (c)
All	26.1 (d)	18.3 (e)	34.4 (f)	32.4 (g)

TABLE IV. RESULTS OBTAINED ON THE CASIA-FAS DB BY THE PROPOSED FACE ANTI-SPOOFING METHOD FOR THE DIFFERENT SCENARIOS CONSIDERED IN THE DATASET AND FOLLOWING THE ASSOCIATED EVALUATION PROTOCOL. INDICES (A), (B), ...(G) CORRESPOND TO THE SEVEN ATTACKING SCENARIOS DEFINED IN [3]. COMPARATIVE RESULTS ARE GIVEN IN TABLE V.

	Results: CASIA-FAS DB						
	(a)	(b)	(c)	(d)	(e)	(f)	(g)
IQA-based	31.7	22.2	5.6	26.1	18.3	34.4	32.4
DoG-based [3]	13.0	13.0	26.0	16.0	6.0	24.0	17.0

TABLE V. COMPARISON OF THE RESULTS (HTER IN %) OBTAINED BY THE IQA-BASED PROTECTION METHOD PROPOSED IN THE PRESENT WORK, AND THE DOG-BASED ANTI-SPOOFING TECHNIQUE DESCRIBED IN [3]. RESULTS ARE PRESENTED FOR THE SEVEN SCENARIOS DEFINED IN [3], HIGHLIGHTED WITH AN INDEX (A), (B), ...(G) IN TABLE IV.

As the proposed IQA-based method is a single-image technique (i.e., it just needs one input image and not a sequence of them), each frame of the videos in the REPLAY-ATTACK DB has been considered as an independent sample. Therefore, classification (real or fake) is done on a frame-by-frame basis and not per video.

In Table II we show the results obtained on the test set. In the *grandtest* experiments (also defined in the associated protocol) the protection method is trained using data from the mobile, print and highdef scenarios, and tested also on samples from the three type of attacks.

The performance exhibited by the proposed IQA-based algorithm follows the expected pattern: although the low error rates are for all the considered scenarios show the high potential of IQA for anti-spoofing purposes, the general performance of the technique degrades when the quality of the attacking devices increases.

In [2] different LBP-based anti-spoofing techniques (partially based on the study presented in [8]) were tested following the exact same protocol used in the present work. Results were only reported on the grandtest scenario considering all types of supports (hand and fixed). A comparison between both protection approaches (IQA-based and LBP-based) appears in Table III. The error rates of all methods are almost identical, however, the IQA-based approach presents certain advantages such as: i) simplicity, it does not rely on the accuracy of any preprocessing step (e.g., face detection) to distinguish between real and fake samples; ii) speed, the absence of image processing steps coupled with the very reduced computation time of the 14 IQMs implemented makes the proposed method extremely fast (i.e., non-intrusive and user-friendly) and especially suited for real-time applications.

B. Results: CASIA-FAS DB

The database is released with an associated evaluation protocol which considers two totally independent datasets (in terms of users): train, used to tune the parameters of the anti-spoofing method and to fix the decision threshold of the classifier; and test, where final results are computed.

In order to be able to compare the results presented here with those reported in [3], the error rates given in this case are computed *per-video* and not on a frame-by-frame basis. Following the protocol used in [3], the final score of a video is computed averaging the scores of 30 randomly selected frames. Then, according to that final global score, the video is classified as real or fake.

The results of the IQA-based method proposed in the present work for the CASIA-FAS DB are given in Table IV. The indices (a), (b), ...(g) that appear in some of the table cells correspond to the seven attacking scenarios considered in [3] for the evaluation of their liveness detection system based on Difference of Gaussians (DoG) filters. Comparative results of the two approaches for these seven scenarios are presented in Table V.

From the results given in Tables IV and V we can see that, opposed to what happened with the liveness detection technique described in [3], the IQA-based method has lower error rates as the resolution of the acquisition device increases (from (a) to (c)), clearly outperforming the DoG-based approach for the high resolution scenario (c).

In general, most face recognition algorithms present lower error rates the higher the resolution of the acquisition sensor is. Therefore, the IQA-based anti-spoofing method permits to maximize both critical performance measures in a complete face biometric system: recognition and protection.

V. CONCLUSIONS

Simple visual inspection of a real and a fake face image of the same person shows that the two samples 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 the present work we have considered a feature space of 14 general image quality measures which we have combined with a simple LDA classifier to detect real and fake access attempts. The novel protection method has been evaluated on two publicly available face databases with well defined associated protocols. This way, the results are reproducible and may be fairly compared with other future analogue solutions.

Several conclusions may be extracted from the evaluation results presented in the article. As expected, being a quality-based method, the performance of the proposed anti-spoofing method degrades when the quality of the spoofing attempts increases (assuming a fixed acquisition device).

On the other hand, just as most face recognition algorithms, the performance of the anti-spoofing method clearly increases for a higher quality (i.e., resolution) of the acquisition device. Therefore, the proposed protection scheme permits to optimize at the same time two critical performance measures of face biometric systems: recognition and anti-spoofing detection.

Comparative results using the same databases and protocols have shown that the proposed method is highly competitive with respect to previously presented approaches from the state-of-the-art. In addition, the proposed method presents some other very attractive features such as: simplicity, speed, non-intrusiveness, user-friendliness and low complexity, each of which is very desirable in a practical protection system.

The present research also opens new possibilities for future work, including: i) extension of the considered 14-feature set with new image quality measures (including no-reference metrics); ii) as the proposed method does not require any preprocessing steps and relies on general IQMs it may be used for antispoofing purposes also on different biometric image-based modalities (e.g., iris, fingerprint or palmprint); iii) use of video quality measures for video replay attacks (e.g., illegal access attempts considered in the REPLAY-ATTACK DB and the CASIA-FAS DB).

VI. Acknowledgements

This work has been partially supported by projects TABULA RASA (FP7-ICT-257289) and BEAT (FP7-SEC-284989) from EC.

References

[1] S. Prabhakar *et al.*, "Biometric recognition: security and privacy concerns," *IEEE Security and Privacy*, vol. 1, pp. 33–42, 2003.

[2] I. Chingovska *et al.*, "On the effectiveness of local binary patterns in face anti-spoofing," in *Proc. Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, 2012.

[3] Z. Zhiwei *et al.*, "A face antispoofing database with diverse attacks," in *Proc. Int. Conf. on Biometrics (ICB)*, 2012, pp. 26–31.

[4] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with kinect," in *Proc. IEEE Biometrics: Theory, Applications and Systems (BTAS)*, 2013.

[5] K. Kollreider *et al.*, "Non-intrusive liveness detection by face images," *Image and Vision Computing*, vol. 27, pp. 233–244, 2009.

[6] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: a public database and a baseline," in *Proc. Int. Joint Conf. on Biometrics (IJCB)*, 2011.

[7] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in *Proc. SPIE Biometric Technology for Human Identification (BTHI)*, 2004, pp. 296–303.

[8] J. Maatta *et al.*, "Face spoofing detection from single images using micro-texture analysis," in *Proc. Int. Joint Conf. on Biometrics (IJCB)*, 2011.

[9] M.-I. Faraj and J. Bigun, "Audio-visual authentication using lip-motion from orientation maps," *Pattern Recognition Letters*, vol. 28, pp. 1368–1382, 2007.

[10] I. Pavlidis and P. Symosek, "The imaging issue in an automatic face/disguise detection system," in *Proc. IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications*, 2000, pp. 15–24.

[11] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in *Proc. IEEE Int. Conf. on Automatic Face and Gesture Recognition (AFGR)*, 2011, pp. 436–441.

[12] T. de Freitas Pereira, A. Anjos, J. M. D. Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?" in *Proc. IEEE Int. Conf. on Biometrics (ICB)*, 2013.

[13] S. Bayram *et al.*, "Image manipulation detection," *Journal of Electronic Imaging*, vol. 15, p. 041102, 2006.

[14] I. Avcibas *et al.*, "Steganalysis using image quality metrics," *IEEE Trans. on Image Processing*, vol. 12, pp. 221–229, 2003.

[15] J. Galbally *et al.*, "A high performance fingerprint liveness detection method based on quality related features," *Future Generation Computer Systems*, vol. 28, pp. 311–321, 2012.

[16] ——, "Iris liveness detection based on quality related features," in *Proc. Int. Conf. on Biometrics (ICB)*, 2012, pp. 271–276.

[17] I. Avcibas *et al.*, "Statistical evaluation of image quality measures," *Journal of Electronic Imaging*, vol. 11, pp. 206–223, 2002.

[18] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," *Electronics Letters*, vol. 44, pp. 800–801, 2008.

[19] S. Yao *et al.*, "Contrast signal-to-noise ratio for image quality assessment," in *Proc. Int. Conf. on Image Processing*, 2005, pp. 397–400.

[20] A. M. Eskicioglu and P. S. Fisher, "Image quality measures and their performance," *IEEE Trans. on Communications*, vol. 43, pp. 2959–2965, 1995.

[21] M. G. Martini *et al.*, "Image quality assessment based on edge preservation," *Signal Processing: Image Communication*, vol. 27, pp. 875–882, 2012.

[22] A. Anjos *et al.*, "Bob: a free signal processing and machine learning toolbox for researchers," in *Proc. ACM Int. Conf. on Multimedia (ACMMM)*, 2012.