The REPLAY-MOBILE Face Presentation-Attack Database

Artur Costa-Pazo*, Sushil Bhattacharjee†, Esteban Vazquez-Fernandez*, and Sebastien Marcel†
*GRADIANT - Galician Research & Development Center in Advanced Telecommunications
CITEXVI, loc. 14 — CUVI, 36310 Vigo (Po.) - Spain
Email: {acosta, evazquez}@gradiant.org
†Idiap Research Institute
Centre du Parc, Rue Marconi 19, PO Box 592, CH-1920 Martigny, Switzerland
Email: {sushil.bhattacharjee, sebastien.marcel}@idiap.ch

***Abstract*—For face authentication to become widespread on mobile devices, robust countermeasures must be developed for face presentation-attack detection (PAD). Existing databases for evaluating face-PAD methods do not capture the specific characteristics of mobile devices. We introduce a new database, REPLAY-MOBILE, for this purpose.[1] This publicly available database includes $1,200$ videos corresponding to 40 clients. Besides the genuine videos, the database contains a variety of presentation-attacks. The database also provides three non-overlapping sets for training, validating and testing classifiers for the face-PAD problem. This will help researchers in comparing new approaches to existing algorithms in a standardized fashion. For this purpose, we also provide baseline results with state-of-the-art approaches based on image quality analysis and face texture analysis[2].**

I. Introduction

Although face recognition is now considered fairly mature technology, in terms of usability and performance [1], [2], it remains a subject of active research. Vazquez-Fernandez *et al.* [3] have published a recent survey of the open problems in facial authentication on mobile devices. One of the most significant road-blocks to wide acceptance of facial authentication technology on mobile devices is the lack of robust countermeasures against spoof attacks. At present, the problem of face *presentation attack detection* (PAD), commonly called face anti-spoofing, is attracting considerable research interest [4].

State of the art face-PAD methods achieve low error performance on current datasets [5], [6]. However, as the high error rates in cross database tests show [7], the performance depends on the use-case. This lack of generalization becomes critical in the space of mobile devices. The quality of presentation attack instruments (PAI) (*i.e.*, mobile devices, printers, monitors, 3D scanners, *etc.*) is also keeping pace with Moore's Law[3]. This implies not only that new methods for PAD need to be developed, but also that new datasets should be generated for realistic testing scenarios.

Well known databases, such as REPLAY-ATTACK [8] or CASIA [9], still extensively used for evaluating new face-PAD methods, are no longer representative of the technology in current mobile devices. Given that the success of a presentation attack (PA) depends strongly on the technology used for face presentation and acquisition, there is a clear need for continuously updating face-PAD databases to keep up with the fast-paced technological advances in the mobile arena. A modern database should consist of high resolution genuine videos and attacks, presented as well as recorded, using mobile devices.

We present here the REPLAY-MOBILE database for face-PAD experiments. The database consists of $1,200$ video clips of photo and video attack attempts, by 40 clients, under various lighting conditions. To create an evaluation benchmark that matches the current requirements and usage of mobile devices, the database has been collected based on three guiding principles.

1) Sequences are captured on representative mobiles devices using the frontal camera. Both, tablets (*iOS*) and smartphones (*Android*) are used to represent the current spectrum of mobile devices.
2) During recording, clients hold the device in the same way as they would do in a real scenario.
3) Attacks are performed using high resolution videos presented on a matte screen (to avoid specular reflections) and high-quality prints on matte paper.

The main contributions of this paper are:

- a new database (REPLAY-MOBILE) which provides realistic test scenarios for the development of new face-PAD algorithms specifically for mobile devices;
- two sets of face-PAD results, one based on image-quality measures (our baseline), and the other based on texture-analysis; and,
- erformance results reported using newly standardized ISO metrics (see the ISO/IEC 30107-3 standard[4]).

[1]This work was partially supported by *GAIN, Axencia Galega de Innovación, Consellería de Economía, Emprego e Industria, Xunta de Galicia* (IN809A. December 30, 2014), EU H2020 project TeSLA, and by the Swiss Center for Biometrics Recognition and Test.

[2]Source-code for experiments reported in this paper are available via the link: https://pypi.python.org/pypi/bob.paper.BioSig2016_ReplayMobile

[3]The quality of digital products – speed, resolution, etc. – is expected to double roughly every 18 months.

[4]https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-1:ed-1:v1:en

Structure of this paper: following a brief summary of related research in Section II, we introduce the REPLAY-MOBILE database, and it associated protocols in Section III. The two face-PAD approaches tested on the new database are described in Section IV, and the corresponding experimental results are presented in Section V. At the end, our conclusions are summarized in Section VI.

II. Related Work

We restrict our context to research in the area of (uni-modal) face-PAD. Several publicly available databases are commonly used to evaluate and compare face-PAD methods. This section provides a brief overview of face-PAD approaches, and the relevant databases.

A. Face-PAD Approaches

Face-PAD methods are usually grouped into three categories, namely, methods based on motion, liveness, and texture [10], [11]. Here we propose a simpler taxonomy, based on two categories: liveness detection based on motion cues, and, image-quality based approaches. Some methods, such as that proposed in [12] and [13] do not fall neatly into one of these two categories, and may be considered as hybrid approaches.

Motion has long been considered an important cue for detecting presentation-attacks. For example, a strong correlation between the estimated optical flow for the face-region and that for the background, is an indicator of a PA [14]. This approach is particularly useful in detecting printed-photos attacks. Clearly, it is not straightforward to extend this idea to video-attacks [12].

Local motion cues, characterizing voluntary or involuntary movements of the face, such as head and lip movements, have been frequently used in face-PAD applications. Several heuristics have been developed for detecting eye-blinks [15]. Pinto *et al.* [12] treat each video as a 3D data-set (instead of a sequence of 2D frames) and compute a number of statistical descriptors over this data. Interestingly, this method can also characterize some image-quality cues (discussed later) such as the presence of Moiré patterns. A recent work [6] attempts to detect involuntary movements using dynamic mode decomposition (DMD) of optical flow to characterize genuine presentations. While not attempting to capture high-level cues directly, this method can detect eye-blinks and lip movements in a face-video [6].

Texture based face-PAD methods characterize the texture information present in the face-region, using, for example, local-binary patterns (LBP), derivatives of Gaussians (DoG), and histograms of oriented gradients (HoG) descriptors [8], [16]. Such methods can produce a decision after processing only one frame of video and are, therefore, favored in systems where fast authentication-response is important. Texture based face-PAD has also been extended to the temporal domain [13], where the LBP-histograms, traditionally computed only in the X-Y plane, have been augmented with LBPs computed in the X-T and the Y-T planes as well (here X and Y are the spatial dimensions, and T is the temporal dimension).

Another approach to face-PAD is the analysis of image-quality. For a face-recognition system, a PA often consists in replaying, to the camera, a video of an enrolled person whose identity is being spoofed. The process of re-capture and playback typically introduces distortions in the video-data that would not be seen in a live data-capture.

Galbally *et al.* have proposed a set of 25 image-quality measures (IQM) [5], well known in the image-compression community, to detect PAs. Wen *et al.* [17] have proposed a different set of image-quality features, that attempt to characterize color-diversity, image-sharpness, and the amount of specularity present in the image. Whereas the IQMs used in [5] are computed on gray-images (the Y component of a color-frame in YCbCr representation), the features proposed in [17] are evaluated on color-images (except for the image-sharpness features).

Videos re-captured from a digital display device often exhibit Moiré patterns. Several researchers have used Moiré pattern detectors [9], [18], [19] for face-PAD. Zhang *et al.* [9] have proposed a Moiré pattern detector based a two-class classifier to detect the presence of high-frequency components in the image. Garcia *et al.* [18] use a set of Mexican-Hat filters to decompose the image. They then assume that a Moiré pattern is present if the energy in any of the filter-responses is stronger than a threshold. Patel *et al.* use multi-scale LBP, to detect Moiré patterns in the spatial domain. Overall, however, these methods have limited success in face-PAD, since Moiré patterns are not guaranteed to be present in all PAs. One efficient way to use a Moiré pattern detector is as a pre-filtering step.

B. Existing Face-PAD Databases

The REPLAY-ATTACK face spoofing database [8] includes $1,300$ videos from 50 subjects. Of these, 100 genuine videos are used for enrollment data for face-verification experiments. The remaining $1,200$ are divided into three non-overlapping subsets. These subsets constitute a protocol for unbiased training, tuning and testing of new algorithms. The genuine-access videos have been captured in two different lighting conditions. Three types of spoofing attacks are included: printed photographs, digital photographs and digital-video replays. The main problem of REPLAY-ATTACK, regarding face authentication on mobile devices, is the presentation and recording technology used. The database was published in 2012 and the videos were recorded by using a $13''$ Macbook at 320×240 resolution, which is very low by current standards of mobile devices.

The CASIA Face Anti-Spoofing Database [9] contains videos of about 10 seconds each, for genuine accesses and attacks from 50 different users. This database has been collected using two different devices: a VGA resolution webcam (640×480) and a high resolution Sony NEX-5 camera (1920×1080). The database does include high resolution videos, but since they were not collected with mobile devices, they are not representative of the mobile scenario: high distortion frontal cameras, video compression, the user holding the

mobile device, changing backgrounds and illumination, and so on.

The public version of the MSU-MFSD database [17] includes real-access and attack videos for 35 subjects. Real-access videos (on average 12 sec. long) have been captured using two devices: a 13″ MacBook Air (using its built-in camera), and a Google Nexus 5 (Android 4.4.2) phone. Videos captured using the laptop camera have a resolution of 640×480, and those captured using the Android camera have a resolution of 720×480. Three kinds of spoof-attacks are included in the database: printed photo attacks, video replays on a smartphone (iPhone 5s), and high-definition (HD) video-replays (captured on a Canon 550D SLR, and played back on an iPad Air). In total, the public version of MSU-MFSD provides 70 real-access videos and 280 attack videos.

Learning-based PAD methods tend to depend strongly on the dataset used for training. The robustness of a PAD method depends on the training and evaluation dataset used, as well as on the technology used for face presentation and acquisition. This leads to the question: can we fairly evaluate the performance face-PAD method designed for use on mobile devices, without mobile-specific databases? This question motivates the REPLAY-MOBILE database presented in this work.

III. The REPLAY-MOBILE Database

The REPLAY-MOBILE database[5] consists of short video recordings of both real-access and attack attempts to 40 different identities. This section presents the details of the data-collection process, as well as an explanation of the evaluation protocols that are provided.

A. Data Collection Set-up

The videos comprising this database have been collected in two sessions separated by an interval of two weeks. In the first session both enrollment videos and media for manufacturing the attacks were collected under two different illumination conditions, namely *lighton* (electric lights in the room are switched on) and *lightoff* (electric lights are turned off). In both scenarios the background of the scene is homogeneous and a tripod is used for the capturing device. (More details are provided in Section III-B.

In the second session each client recorded 10 videos, under the following 5 different scenarios and paying special attention to the lightning conditions:

1) *controlled*: the background of the scene is uniform, the light in the office is switched on and the window blinds are down.
2) *adverse*: the background of the scene is uniform, the light in the office is switched off and the window blinds are halfway up.
3) *direct*: the background of the scene is complex and the user is facing a window with direct sunlight while capturing the video.
4) *lateral*: the background of the scene is complex and the user is near to a window and receiving lateral sunlight while capturing the video.
5) *diffuse*: the video is captured in an open hall with a complex background and diffuse illumination.

When recording the video, the user was asked to stand, to hold the mobile device at the eye level and to center the face on the screen of the video capture application. Each video is approximately 10 seconds long ($\sim$ 300 frames @ 30fps) and HD resolution (720×1280). (Note that the videos in the MSU-MFSD database have relatively lower resolution.) In each lighting condition the user captured two videos, one using an *iPad Mini 2*[6] tablet and another using a *LG-G4*[7] smartphone.

Fig. 1: Examples of real accesses in different scenarios. Top row: samples from real accesses captured on a smartphone. Bottom row: samples captured on a tablet. Columns from left to right show examples of video frames in *controlled*, *adverse*, *direct*, *lateral*, and *diffuse* scenarios, respectively.

B. Generation of Attacks

To create the attacks, a separate set of high resolution photos and videos were first collected, under the same illumination conditions as described above. Each user was asked to sit down in front of two devices while the acquisition operator captured the data under the conditions previously defined (*lighton* and *lightoff*). For photo-based attacks, a *Nikon Coolpix P520* camera was used to capture high resolution images (18 Mpixel). Video-based attacks were recorded by using the back camera of the *LG-G4* smartphone, which records *1080p FullHD* video clips.

The attacks have been created using two different PAIs: *mattescreen*: photos and videos for each client are displayed on a *Philips 227ELH* monitor with a resolution of 1920×1080

[5]The database may be downloaded using the following URL: `https://www.idiap.ch/dataset/replay-mobile`

[6]iPad Mini 2 is an iOS tablet produced and marketed by Apple Inc. This tablet includes a 5 megapixel rear-facing camera and a 1.2 MP FaceTime HD front-facing camera.

[7]LG G4 is an Android smartphone developed by LG Electronics. The rear-facing camera has a 16 megapixel sensor with a f/1.8 aperture lens, infrared active autofocus, three-axis optical image stabilization, and LED flash.

pixels; and *print*: hard-copies of high-resolution digital photographs are printed on plain A4 matte paper (using a *Konica Minolta ineo+ 224e* color laser printer).

Each attack was recorded on each mobile device (tablet and smartphone) for 10 seconds. For recording *mattescreen* attacks the capturing mobile device was supported on a fixed support. Each *print* video, however, was captured in two different attack modes: *hand-held attack*, where the operator holds the capture device; and *fixed-support attack*, where the capture device is fixed on a supportThus, four different PAIs are represented in REPLAY-MOBILE. Figure 2 shows examples of attacks available in the database.

Fig. 2: Samples of the different presentations attack instruments (PAI). Top row: samples from attack accesses captured on a smartphone. Bottom row: samples captured on a tablet. Columns, from left to right, show examples of *mattescreen-lighton*, *mattescreen-lightoff*, *print-lighton*, and *print-lightoff*, respectively.

C. Evaluation Protocols

To simplify its use and adoption, this new database is designed following the structure of REPLAY-ATTACK database [8]. Videos in the REPLAY-MOBILE database are grouped into 3 subsets: *train*, *development* and *test*. The three subsets have no overlap. Identities for each subset have been selected via demographic analysis: each subset has equable distribution for identities based on gender, age and eye-wear.

The REPLAY-MOBILE database also provides an *enroll* set, consisting of 160 videos, corresponding to enrollment data for each of the 40 clients. Specifically, four enrollment videos are available for each client, corresponding to videos recorded in two different illumination conditions (*lighton* and *lightoff*), on each of the two mobile devices.

Table I summarizes the organization of videos in the various protocols for face-PAD experiments. Each row in the table (a specific *Scenario-Type* pair) corresponds to one PAI. The column-labels *Mobile* and *Tablet* indicate the capture-device used. Besides the two protocols (*mattescreen* and *print*), a *Grandtest* protocol is also provided, for global performance evaluation[8].

		mattescreen attack		print attack		Grandtest attack
		real access	photo fixed	print fixed	print hand	
Mobile	Train	60	24	24	24	156
	Devel	80	32	32	32	208
	Test	60	24	24	24	156
Tablet	Train	60	24	24	24	156
	Devel	80	32	32	32	208
	Test	60	24	24	24	156
	Total	400	160	160	160	1040

TABLE I: Number of videos in each database subset.

IV. The Studied Face-PAD Approaches

In this section we describe the two face-PAD methods that we have applied to the REPLAY-MOBILE database. The first method, described in Section IV-A, is based on image-quality measures, and serves as our baseline. In Section IV-B we propose a new method for face-PAD, based on Gabor-jets. Experimental results for these methods are reported in Section V.

A. Face-PAD Based on Image Quality

Our baseline, against which to compare the results of the proposed method, is derived from a set of image-quality measures (IQM), first used for face-PAD by Galbally *et al.* [5]. Some of the IQMs used by Galbally *et al.* [5], have been computed using third-party executables and are not easily reproducible. Our experiments are based a subset of reproducible features. Specifically, from the set of 25 IQMs proposed by Galbally *et al.* [5], we have used a subset of 18 IQMs. The features used in our experiments are listed in Table II. For each frame of video, these features are computed over the entire frame, not just the face-region.

B. Face-PAD Using Gabor-Jets

LBP texture descriptors have been successfully used for face-PAD [20]. Here we propose a new texture-based approach for face-PAD, using Gabor-jets. GRADIANT [21] have previously used Gabor-jets [22], [23] as a feature-extraction step for face-recognition. To our knowledge this texture-descriptor has not previously been applied to the problem of face-PAD.

We compute Gabor-jets over a regular 10×10 grid using 40 Gabor wavelets with default parametrization [22]. After aligning the face images to 85×100 pixels, an adaptation of the retina layer model [24] is used to preprocess them. The computed feature vectors only apply to face region, using bounding boxes computed using a face-detection preprocessor. If the face detector does not detect any face in a given frame of

[8]In Table I, each element in the *Grandtest* column is the sum of the remaining elements in the corresponding row.

F#	Name	Abbrev.
1	Mean Squared Error	MSE
2	Peak Signal to Noise Ratio	PSNR
3	Average difference	AD
4	Structural content	SC
5	Normalized cross-correlation	NK
6	Max. difference	MD
7	Laplacian MSE	LMSE
8	Normalized Abs. error	NAE
9	Signal to noise ratio	SNRv
10	R-averaged Max. difference (r=10)	RAMDv
11	Mean angle similarity	MAS
12	Mean angle magnitude similarity	MAMS
13	Spectral magnitude error	SME
14	Gradient magnitude error	GME
15	Gradient phase error	GPE
16	Structural similarity index	SSIM
17	Visual information fidelity	VIF
18	High-low frequency index	HLFI

TABLE II: List of image-quality measures (IQM) used in the baseline experiments. The use of these measures as features for face-PAD has been proposed by Galbally *et al.* [5]. The feature-names and abbreviations listed here are those used in [5], where full descriptions of the measures, specifically, their mathematical definitions, can be found.

the input video, that frame is discarded from further analysis. For each face-image a 4000-element feature-vector is recorded.

V. Experimental Results

Experimental results for the two face-PAD approaches discussed in Section IV are presented here. To evaluate the PAD performance, we have elected to use standard ISO/IEC 30107-3 metrics, namely, APCER: Attack Presentation Classification Error Rate; and BPCER: *Bona fide* Presentation Classification Error Rate. APCER and BPCER and analogous to the commonly used false (spoof) acceptance rate (FAR), and false (genuine) rejection rate (FRR), respectively. The main difference between the standardized measures and the old measures is that in APCER and BPCER, the attack-potential and the probability of success of each attack type is also taken into account. We also provide the ACER (Average Classification Error Rate), defined as $(APCER + BPCER)/2$, to summarize the overall performance PAD algorithm as a single number. The lower the ACER values the better is the performance. To aid comparison with previously published works, however, we also report the half-total error rates (HTER) for our experiments. In all experiments, the performance has been computed on a 'per-frame basis'.

A. Face-PAD Based on Image Quality

Galbally *et al.* [5] have used linear discriminant analysis (LDA) in their experiments, to achieve a HTER of 15.2% on the REPLAY-ATTACK database (for the *Grandtest* protocol). Our experiments show that a support-vector machine (SVM) with a radial-basis function (RBF) kernel yields better face-PAD results than LDA (using the same features). The results of our experiments are summarized in Table III, which presents the HTER performance of the two classifiers (LDA, and SVM-RBF) on the REPLAY-ATTACK database. The table reports the achieved percent error-rates on the development set (EER, the equal-error rate) and the test set (HTER), for the Grandtest protocol of the REPLAY-ATTACK database[9].

	Galbally *et al.* [5]	LDA	SVM-RBF
Dev. EER (%)		5.06	2.68
Test. HTER (%)	15.20	9.78	5.28

TABLE III: Comparison of different classifiers for the face-PAD Grandtest protocol of the REPLAY-ATTACK database. For SVM, we have used the publicly available, LIBSVM implementation, and have set the kernel parameter $\gamma = 1.5$. (See Table II for the list of features used in our baseline experiments.) The EER and HTER values presented here have been computed on a 'per-frame' basis.

For baseline experiments on the REPLAY-MOBILE database, in Table IV we report results using only the SVM-RBF classifier. The table reports the EER for the development set, and the HTER achieved on the test set, for different combinations of *scenario* and *type* defined in the REPLAY-MOBILE database. The overall performance, as shown for the experiment [Grandtest] in Table IV, is 7.8%[10]. We use this method to set our face-PAD baseline on this database.

	Mattescreen		Print		Grandtest
	photo	video	fixed	hand	
Dev. EER (%)	7.93	11.70	5.31	4.98	7.50
Test. HTER (%)	7.70	13.64	4.22	5.43	7.80

TABLE IV: Baseline results using SVM-RBF classifier ($\gamma = 1.5$) on IQM features (see Table II) computed for the face-PAD protocol of the REPLAY-MOBILE database.

B. Face-PAD Using Gabor-Jets

A two-class classifier is constructed for the 4000-D Gabor-jet feature-vectors using SVM-RBF ($\gamma = \frac{1}{\#features} = 0.00025$). The classification results achieved on REPLAY-MOBILE and the comparison with the IQM baseline are shown in Table V.

From Table V we can also observe the advantage of using the performance measures APCER and BPCER, over HTER. Using HTER one may conclude that both methods (IQM-based and Gabor-based face-PAD) achieve similar results. Using APCER and BPCER, however, we can observe the

[9]Preliminary experiments using principal component analysis (PCA) to reduce the dimensionality of the feature-space showed poorer results than when the 18 IQM features are used directly for classification.

[10]The fact that the classification performance on the REPLAY-MOBILE database is worse than on the REPLAY-ATTACK database, is in line with expectations. We attribute this difference in performance to the fact that attack-videos in the REPLAY-MOBILE database have been constructed using higher quality PAIs than those used for the older, REPLAY-ATTACK database.

	Test. HTER (%)					Test. ACER (%)	Test. APCER (%)	Test. BPCER (%)
	MP	MV	PF	PH	GT			
IQM	7.70	13.64	4.22	5.43	7.80	13.64	19.87	7.40
Gabor	8.64	9.53	9.40	8.99	9.13	**9.53**	7.91	11.15

TABLE V: HTER, ACER, APCER, BPCER (%) of the proposed method compared with the baseline in REPLAY-MOBILE database. The HTER results are reported for each protocol, indicated by the following column-headings: MP – *mattescreen-photo*, MV – *mattescreen-video*, PF – *print-fixed*, PH – *print-hand* and GT – *Grandtest*.

Gabor-based approach seems more consistent among different presentation attack instruments (PAI), which indicates that it is the more robust of the two approaches.

The detection-error tradeoff (DET) curves in Figure 3 show the influence of each attack. These plots illustrate the fact that the Gabor-jet based face-PAD shows consistent performance for the different kinds of attacks, whereas the performance of the image-quality based approach varies significantly among the various attack-types.

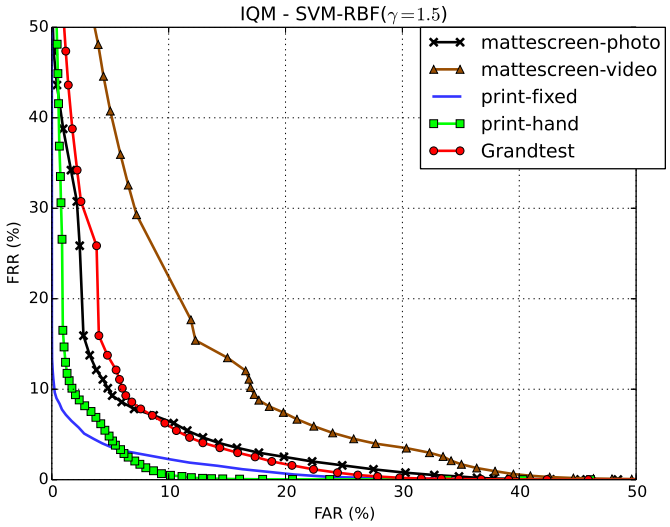
VI. Conclusions

The need for robust countermeasures against presentation attacks remains a significant challenge for the adoption of facial authentication technology on mobile devices. For a effective evaluation of face-PAD methods, new datasets should be generated to reflect realistic testing scenarios. We have reviewed the main limitations of current databases for evaluating face-PAD methods intended to work on mobile devices. Taking into account these requirements, we have proposed REPLAY-MOBILE, a new database for fair evaluation of face-PAD methods on mobile devices. The key characteristics of REPLAY-MOBILE are:

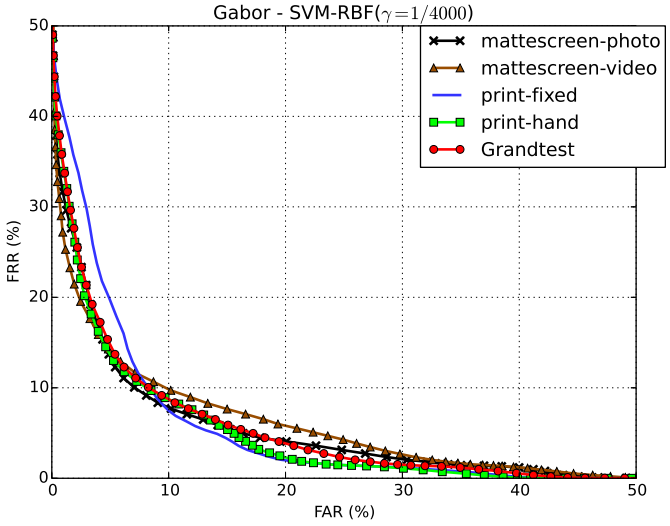
1) high-resolution videos captured under realistic conditions of device-usage, including a variety of illumination conditions;
2) a variety of presentation-attacks, including high quality prints on matte-paper and matte-screen videos;
3) a pre-defined protocol for unbiased training and fair evaluation.

Using REPLAY-MOBILE, we have established a benchmark and baseline for the evaluation of face-PAD by using the newly standardized metrics, APCER and BPCER, defined in the ISO/IEC CD 30107-3 standard. We have also compared the performance of two different face-PAD approaches, one based on image quality assessment and one based on texture analysis (Gabor-jets). The comparison made between the two approaches show the benefits of using these metrics for a more fair evaluation of anti-spoofing algorithms.

The database will be made publicly available in order to help the development and fair evaluation of anti-spoofing algorithms for face authentication on mobile devices.



(a) IQM-based



(b) Gabor-based

Fig. 3: DET curves for the various attack protocols. The performance of the IQM based PAD method varies significantly among the different kinds of attacks. By contrast, the Gabor-jet based approach is more consistent over the range of attack-types.

Acknowledgment

The authors would like to acknowledge the financial support of *GAIN, Axencia Galega de Innovación, Consellería de Economía, Emprego e Industria, Xunta de Galicia* (IN809A. December 30, 2014), as well as the EU H2020 project TeSLA, and the Swiss Center for Biometrics Recognition and Test.

References

[1] S. Z. Li and A. K. Jain, Eds., *Handbook of Face Recognition (2e.)*. Bonn: Springer Verlag, 2011.

[2] T. Bourlai, Ed., *Face Recognition Across The Image Spectrum*. Switzerland: Springer International Publishing, 2016.

[3] E. Vazquez-Fernandez and D. Gonzalez-Jimenez, "Face recognition for authentication on mobile devices," *Image and Vision Computing*, pp. –, 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0262885616300543

[4] "Ieee trans. on information forensics and security: Special issue on biometric spoofing and countermeasures," IEEE, April 2015.

[5] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint and face recognition," *IEEE Trans. on Image Processing*, vol. 23, no. 2, pp. 710–724, February 2014.

[6] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. S. Ho, "Detection of face spoofing using visual dynamics," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 762–777, April 2015.

[7] T. de Freitas Pereira, A. Anjos, J. M. de Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?" in *Proceedings of ICB*, 2013, pp. 1–8.

[8] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG - Proceedings of the International Conference of the*, Sept 2012, pp. 1–7.

[9] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Li, "A face antispoofing database with diverse attacks," in *Biometrics (ICB), 2012 5th IAPR International Conference on*, March 2012, pp. 26–31.

[10] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, F. Roli, J. Yan, D. Yi, Z. Lei, Z. Zhang, S. Z. Li, W. R. Schwartz, A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. Castrilln-Santana, J. Mtt, A. Hadid, and M. Pietikinen, "Competition on counter measures to 2-d facial spoofing attacks," in *Biometrics (IJCB), 2011 International Joint Conference on*, Oct 2011, pp. 1–6.

[11] I. Chingovska and A. R. dos Anjos, "On the use of client identity information for face antispoofing," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 787–796, April 2015.

[12] A. da Silva Pinto, H. Pedrini, W. Schwartz, and A. Rocha, "Video based face spoofing through visual rhythm analysis," in *Proceedings of 25th SIBGRAPI*, August 2012, pp. 221–228.

[13] T. de Freitas Pereira, A. Anjos, J. M. de Martino, and S. Marcel, "Lbp-top based countermeasure against face spoofing attacks." in *Proceedings of ACCV Workshops*, 2012, pp. 121–132.

[14] A. Anjos, M. M. Chakka, and S. Marcel, "Motion-based counter-measures to photo attacks in face recognition," *Institution of Engineering and Technology Journal on Biometrics*, Jul. 2013. [Online]. Available: http://pypi.python.org/pypi/antispoofing.optflow

[15] S. Chakraborty and D. Das, "An overview of face liveness detection," *International Journal on Information Theory (IJIT)*, vol. 3, no. 2, pp. 11–25, April 2014.

[16] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in *(IJCB), Proceedings of IAPR IEEE international joint conference on Biometrics*, 2013, pp. 1–6.

[17] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," *IEEE Trans. on Information Forensics and Security*, vol. 10, no. 4, pp. 746–761, April 2015.

[18] D. C. Garcia and R. L. Queiroz, "Face spoofing 2d-detection based on moiré-pattern analysis," *IEEE Trans. on Information Forensics and Security*, vol. 10, no. 4, pp. 778–786, April 2015.

[19] K. Patel, H. Han, A. K. Jain, and G. Ott, "Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks," in *Proceedings of 8th International Conference on Biometrics (ICB)*, 2015, pp. 98–105.

[20] I. Chingovska, J. Yang, Z. Lei, D. Yi, S. Z. Li, O. Kahm, C. Glaser, N. Darner, A. Kuijper, A. Nouak, J. Komulainen, T. Pereira, S. Gupta, S. Khandel Wa, S. Bansal, A. Rai, T. Krishna, D. Goyal, M. A. Waris, H. Zhang, I. Ahmad, S. Kiranyaz, M. Gabbouj, R. Tronci, M. Pili, N. Sirena, F. Roli, J. Galbally, J. Ficrrcz, A. Pinto, H. Pedrini, W. S. Schwartz, A. Rocha, A. Anjos, and S. Marcel, "The 2nd competition on counter measures to 2D face spoofing attacks," *Proceedings - 2013 International Conference on Biometrics, ICB 2013*, pp. 1–6, 2013.

[21] M. Gunther, A. Costa-Pazo, C. Ding, E. Boutellaa, G. Chiachia, H. Zhang, M. de Assis Angeloni, V. . truc, E. Khoury, E. Vazquez-Fernandez, D. Tao, M. Bengherabi, D. Cox, S. Kiranyaz, T. de Freitas Pereira, J. ganec Gros, E. Argones-Ra, N. Pinto, M. Gabbouj, F. Simes, S. Dobriek, D. Gonzlez-Jimnez, A. Rocha, M. U. Neto, N. Pavei, A. Falco, R. Violato, and S. Marcel, "The 2013 face recognition evaluation in mobile environment," in *2013 International Conference on Biometrics (ICB)*, June 2013, pp. 1–7.

[22] L. Wiskott, J. M. Fellous, N. Kuiger, and C. von der Malsburg, "Face recognition by elastic bunch graph matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 7, pp. 775–779, Jul 1997.

[23] E. Argones Rúa and C. Alba Castro, José Luisand García Mateo, "Quality-based score normalization and frame selection for video-based person authentication," in *BIOID 2008*, 2008, pp. 1–9.

[24] N.-S. Vu and A. Caplier, "Illumination-robust face recognition using retina modeling," in *ICIP 2009*, Nov 2009, pp. 3289–3292.