# The 2nd Competition on Counter Measures to 2D Face Spoofing Attacks

I. Chingovska[1,*], J. Yang[2], Z. Lei[2], D. Yi[2], S. Z. Li[2], O. Kähm[3], C. Glaser[3], N. Damer[3], A. Kuijper[3], A. Nouak[3],
J. Komulainen[4], T. Pereira[5,6], S. Gupta[7], S. Khandelwal[7], S. Bansal[7], A. Rai[7], T. Krishna[7], D. Goyal[7],
M.-A. Waris[8], H. Zhang[8], I. Ahmad[8], S. Kiranyaz[8], M. Gabbouj[8], R. Tronci[9], M. Pili[9], N. Sirena[9], F. Roli[9],
J. Galbally[10], J. Fierrez[10], A. Pinto[5], H. Pedrini[5], W. S. Schwartz[11], A. Rocha[5], A. Anjos[1], S. Marcel[1]

[1]Idiap Research Institute (CH), [2]Chinese Academy of Sciences (CN),
[3]Fraunhofer Institute for Computer Graphics Research IGD (DE), [4] University of Oulu (FI), [5]University of Campinas (BR),
[6]CPqD Telecom & IT Solutions (BR), [7]The LNM Institute of Information Technology (IN), [8]Tampere University of Technology (FI),
[9]University of Cagliari (IT), [10]Universidad Autonoma de Madrid (ES), [11]Universidade Federal de Minas Gerais (BR)

## Abstract

*As a crucial security problem, anti-spoofing in biometrics, and particularly for the face modality, has achieved great progress in the recent years. Still, new threats arrive in form of better, more realistic and more sophisticated spoofing attacks. The objective of the 2nd Competition on Counter Measures to 2D Face Spoofing Attacks is to challenge researchers to create counter measures effectively detecting a variety of attacks. The submitted propositions are evaluated on the Replay-Attack database and the achieved results are presented in this paper.*

## 1. Introduction

As a result of the great advancement of biometrics in the past years, systems secured by the paradigm to present *"who you are"* instead of *"what you possess"* or *"what you remember"* [12] have reached great popularity. Biometric systems have become robust, efficient and accurate even in challenging conditions. A recent problem that is questioning the application of biometrics when high security is required are spoofing attacks. Also referred to as presentation attacks, spoofing attacks are performed when an invalid user tries to gain access to the system by presenting a copy of the biometric traits of a valid user.

Many widely used biometric modalities can be a subject to spoofing. In the domain of face modality, an attacker has a variety of options: from a simple print of the valid user's face to video replays or even more complex 3D masks. Obtaining face images of a valid user is nowadays nearly a trivial task: they are present in abundance on the Internet or can be easily taken cooperatively or at distance.

*Corresponding author: ivana.chingovska@idiap.ch

Until recently, face anti-spoofing researchers were confronted with the lack of publicly available databases containing different types of attacks. Many of the state-of-the-art algorithms have been evaluated on databases which are not publicly released. The pioneer publicly available face spoofing database is NUAA [20], followed by Print-Attack [3], both containing only printed attacks. CASIA-FASD [26] is the first database containing three types of attacks: printed photographs, printed photographs with perforated eyes regions and video replay attacks. An important limitation of some of these databases is the absence of a precise protocol containing training, development and test sets. The consequence is a difficulty in fair evaluation and comparison of face anti-spoofing methods.

The first attempt to benchmark face anti-spoofing algorithms was the Competition on Counter Measures to 2D Facial Spoofing Attacks [4], where the participants' algorithms were evaluated on the Print-Attack database. The possibility for fair evaluation on this database is provided by its protocol, which precisely defines training, development and test sets. In the meantime, an amendment of this database with 2 additional types of attacks (photo attacks and video replay attacks) has led to the creation of Replay-Attack database [5], which inherits its unbiased protocol. This has motivated the 2nd Competition on Counter Measures to 2D Face Spoofing Attacks: an effort to probe the current trends in face anti-spoofing and to compare and evaluate novel face anti-spoofing algorithms on a variety of spoofing attacks.

The existing state-of-the-art face spoofing countermeasures can be categorized in three broad categories [4]. The *texture-based* methods explore the texture artifacts and the quality deterioration that appear when an image is recaptured. The *motion-based* methods explore the unnatural movements on the scene in the case of spoofing attacks,



978-1-4799-0310-8/13/$31.00 ©2013 IEEE

Table 1. Participating teams' names and institutions

| Team | Institution |
|---|---|
| **CASIA** | Center for Biometrics and Security Research & National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences |
| **IGD** | Fraunhofer Institute for Computer Graphics Research IGD |
| **MaskDown** | joint team from Idiap Research Institute, University of Oulu, University of Campinas and CPqD Telecom & IT Solutions |
| **LNMIIT** | The LNM Institute Of Information Technology, Jaipur |
| **MUVIS** | Tampere University of Technology |
| **PRA Lab** | University of Cagliari |
| **ATVS** | Universidad Autonoma de Madrid |
| **Unicamp** | joint team from University of Campinas and Universidade Federal de Minas Gerais |

while the *liveness-based* methods try to detect any evidence of liveness on the scene as an indicator of the presence of a real person.

Unique spoofing counter-measures, some of which go beyond the boundaries of the mentioned categories, have been proposed by 8 teams participating in this competition. In this paper they are thoroughly explained and their spoofing detection capabilities are compared using the Replay-Attack database. The teams' details are provided in Table 1.

The remainder of the paper is organized as follows: a short description of Replay-Attack database follows in Section 2. Each team's face spoofing counter-measure is described in Section 3, followed by a report on its performance and a comparative analysis in Section 4. Conclusions are given in Section 5.

## 2. Replay-Attack database

The Replay-Attack face spoofing database[1] [5] consists of short video recordings of both real-access and attack attempts to 50 different identities. The database contains three types of attacks: printed photographs, photographs displayed on the screen of a device and videos replayed on the screen of a device. The attacks are divided into two groups with regards to the support the attack media is attached to when they are presented to the system: *fixed* (the attack media is attached on a fixed stall) and *hand* (the attacker holds the attack media with her hands). Furthermore, the photo and video replay attacks can be of lower quality (taken with an iPhone and displayed on an iPhone screen) and of high quality (displayed on an iPad screen). These variations introduce even larger diversity in the spoofing attacks present in the database.

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

Besides the different attack types, this database has several other advantages over the previous face spoofing databases. Firstly, it defines a precise protocol consisting of training, development and test sets. For fair and unbiased algorithm evaluation, it is recommended that the training set is used to train counter-measures, development set to estimate specific parameters to maximize the performance, while the test set should be solely used to report results. Secondly, the database provides a separate set of enrollment videos, which can be used to train and evaluate a face recognition system. Such an approach is of high importance, as it enables to assess how effective the attacks are in deceiving a face recognition system and whether an anti-spoofing scheme is necessary in that setup. As claimed by [5], more than 80% of the attacks in this database successfully bypass a baseline face verification system.

The total number of videos in the database is 1200 (360 in the training set, 360 in the development set and 480 in the test set). In the course of the competition, the participants had access to all the protocol sets of the data. However, in the test stage, they received an anonymized test set that consists of clipped versions of the original test set videos, containing 100 frames with a random starting frame.

## 3. Summaries of the anti-spoofing algorithms

**CASIA** The team takes advantage of the differences between the real accesses and spoofing attacks from two aspects: motion and texture. In terms of motion, the algorithm is motivated by the observation that the spoofing attacks have either global motion or no motion, whereas the real accesses have motion localized at the human body regions. The team proposes feature-level fusion of motion and texture characteristics.

For the motion features, the team implemented Gunnar Farneback's algorithm [8] to extract dense optical flows between two frames, with an interval of five frames. To characterize the global and local distribution of motion, each frame is divided into three regions: head, torso and background. The regions are further divided into 6, 3 and 2 subregions, respectively. For each of the obtained 11 regions, 2 temporal sequences are computed: one for the angles and one for the magnitudes of the optical flow. Three types of features are extracted from these temporal sequences: *frequency coefficients* computed using 1D Fast Fourier Transform (FFT), *histogram of magnitudes of optical flows* and *correlation coefficients* for each pair of two magnitude and two angle sequences of a video. For the texture features, the team exploits multi-scale Local Binary Patterns (LBP) as in [14] to analyze the quality degradation of the attack samples. The features are extracted only from the head region of one random frame of the video.

The extracted motion and texture features are concatenated into the final feature vector. Then, the features are fed

into a linear Support Vector Machine (SVM).

**IGD** The implemented approach exploits subtle changes in the faces of the subjects in the videos that are characteristic for real accesses. In particular, the team implemented an algorithm which magnifies the small changes of color and movement which appear on the face due to the blood flow. After magnifying, these changes are expected to have different nature in the real access videos compared to spoofing attacks.

In order to magnify the changes happening with a set of given frequencies, Eulerian magnification [23] is applied on the video sequences as a preprocessing step. The selected frequencies represent the frequency range of human pulse. The algorithm uses two main approaches for spatial decomposition: Laplacian and Gaussian pyramids. Both approaches are implemented to magnify changes of different nature.

From the Gaussian filter output, among 30 frames, the frame whose output has the largest average magnitude was picked to represent the video. The Laplacian filter outputs of the frames in the video are averaged over 30 frames. The obtained results are processed with PCA for dimensionality reduction. The two final feature vectors are fed into separate AdaBoost [9] classifiers. The obtained scores for the two approaches are then normalized and combined using a weighted sum fusion rule.

**MaskDown** The team creates a composite system by joining different categories of counter-measures together, each of which may be effective against a single type of attack. After fusing the systems at score-level, the final system should be effective against all types of attacks.

For describing static texture, the team extracts two types of features: uniform Local Binary Patterns (LBP) [16] and texture features from Gray-Level Co-occurrence Matrix (GLCM) [11]. The both types of features are classified using Linear Discriminant Analysis (LDA). In addition, the different texture patterns in spatio-temporal domain are explored using Local Binary Patterns from Three Orthogonal Planes (LBP-TOP) [25] operator. More specifically, the team analyzes dynamic texture content within two different time windows by combining the temporal processing strategies proposed in [6] and [13]. The motion based counter measure exploits the high correlation between the movements in the background and in the face region in the case of spoofing attacks [3].

The texture features are computed for each frame separately on normalized face bounding box. The scores of the three visual cues for each time window are fused using Linear Logistic Regression (LLR). The scores for the videos are obtained by averaging the scores over all time windows.

The proposed algorithm is easily reproducible because the source code, programmed using the free signal-processing and machine-learning toolbox Bob[2] [2], is freely available[3].

**LNMIIT** The method proposed by this team performs both texture and motion analysis on a video and combines the information on feature level. The algorithm utilizes three types of intuitive visual features. Firstly, to capture textural information, the team uses LBP features calculated on the face region, similarly to [14]. Secondly, as a complementary non-rigid motion analysis approach, the team extracts face background consistency features [24]. Gaussian Mixture Model (GMM) [19] is used for background modeling. The third type of features combines motion and texture analysis and consists of 2D FFT on the GMM modeled background.

Each of the three feature types aims at detecting different types of attacks. The first type of features is effective against printed and low-quality attacks. The second type aims at detecting video replay attacks, while the third one is able to cope with high-definition video attacks.

All the three types of feature vectors are computed on per-frame basis and averaged over the full video. The three features vectors are concatenated in a single feature vector. The classifier used for discrimination between real accesses and spoofing attacks is Hidden Markov Support Vector Machines (SVM$^{hmm}$) [1].

**MUVIS** The team adopts a texture-based approach by extracting two types of texture features: LBP and Gabor. Unlike many previously proposed solutions which are computing the texture features only on the face region of the frame [6], [5], this approach takes whole scene into account because the authors believe that the surrounding region of face also contains dominant cues for detection of spoofing attacks.

For the LBP features, a Rotation-Invariant Uniform LBP ($LBP^{riu2}_{P,R}$) histogram [16] is computed individually for every frame of the video, where the number of neighboring pixels $P = 16$ and the radius $R = 2$. The Gabor features require computation of Gabor wavelet transform in 4 scales and 6 orientations. The feature vector on per-frame basis is constructed using mean and standard deviation of the magnitude of the transform coefficients [15].

In both cases, the feature vector on video-level is computed as average of the feature vectors on frame-level. The result of the concatenation of the two feature vectors is fed into Partial Least Square regression [7] classifier.

[2] http://www.idiap.ch/software/bob

[3] Code available at: https://pypi.python.org/pypi/antispoofing.competition_icb2013

**PRA Lab** The team's choice is to use only static image analysis to detect spoofing attacks. The aim of static analysis is to discover some peculiarities related to the visual structure of the input samples.

To detect the differences in the visual information between data captured from a real scene and from an attack, the team explored several different types of visual features (e.g. color features, edges, textures etc.) . For detailed reference of the used features, please refer to the team's algorithm in [4].The features are extracted from each frame and they are used to train several SVMs (for each feature separately). Based on the training results, a subset of features is selected by taking into account both the performance and the classification time.

The final spoofing score of a video is obtained by using a two stage combination of the scores. The first stage of combination is performed at frame level: the scores obtained for different features are fused to create a single confidence score for a given frame. The second stage combines the scores for the frames to calculate the final score for the video. This is done in an incremental way in order to simulate a "live" tool: the final score is recalculated with every new frame in the video as the time passes.

For the both stages the team used Dynamic Score Combination [22] as a score-level fusion rule that allows dynamically choosing the best scores and weights to be combined. It requires computation of a weight parameter via majority voting [21]. In the second combination stage the team introduced a heuristic to exclude single frames with outlier scores.

**ATVS** The method proposed by this team is based on the expectation that a recaptured image has different quality than a real sample acquired in the normal operation scenario for which the sensor was designed. Motivated by this different quality hypothesis, the system uses a novel parameterization of 25 objective Image Quality Measures (IQM) which provide a quantitative score that describes the level of distortion of the input image. Two types of IQMs are present in the feature set: *full-reference* and *no-reference*. To compute full-reference IQM, an original distortion-free reference image is needed [18]. Since in the case of spoofing attack detection there is no access to such a sample, the team simulates it by filtering the input image with a low-pass Gaussian kernel ($\sigma = 0.5$ and size $3 \times 3$). To compute no-reference IQM (also referred as *blind*), a pre-trained statistical model is required [17].

Among 25 IQM in the feature vector, 21 are full-reference and 4 are no-reference. They are classified using LDA classifier. The system works on a frame-by-frame basis. The final score for a video is produced as an average of the scores of its frames.

**Unicamp** The team explores artifacts which appear in recaptured videos, such as distortion, moiring and band effect. For that, the team designed a feature characterization process to extract a noise signature of biometric samples. The algorithm takes advantage of global information over time and is invariant to the video content.

The algorithm consists of 4 steps. The first step isolates the noise signature information contained in the video. This process consists of subtracting the frames of the original video from a filtered version of the frames (with Gaussian filter with size $3 \times 3$, $\mu = 0$, and $\sigma = 0.5$) and results in a new *noise residual video*. The second step performs a spectral analysis of the noise patterns of the noise residual video using 2D discrete Fourier transform on each frame. The new video of spectra is referred to as *Fourier spectrum video*. In the third step, to capture temporal information contained in the Fourier spectrum video, the team uses the visual rhythm technique [10]. It summarizes the content of the video in a 2D image by sampling particular regions of interests. The algorithm considers three regions of interest and creates three types of visual rhythms: horizontal, vertical and zig-zag. Finally, the visual rhythms are concatenated in order to form a single visual rhythm.

From the image representing the visual rhythm, the team extracts a set of features using its Gray Level Co-occurrence Matrices (GLCM) [11]. In the classification stage, the team uses Support Vector Machine (SVM) considering radial basis function as kernel.

## 4. Discussion and results

The algorithms proposed in this competition approach the problem from different aspects, as listed in Table 2. The analysis of the textural differences is the most popular approach adopted by 7 out of 8 teams. Three teams use motion-based approach, but in combination with texture-based, while one team relies solely on liveness detection.

A common approach for many teams is combining several different concepts together. In particular, the fusion is performed either at score-level or decision-level. An interesting observation is that the category of used features does not influence the choice of level of fusion. For example, two teams (CASIA and LNMIIT ) perform feature-level fusion on different categories of features (texture and motion-based), while MUVIS and IGD adopt the same level of fusion for features belonging to the same category (texture-based and liveness-based, respectively). On the other hand, MaskDown combines different categories of techniques at score-level. PRA Lab utilizes a specific type of fusion scheme to combine techniques belonging to the same category. The fusion approaches of the teams are listed in the right-most column of Table 2.

The ranking of the participating anti-spoofing algorithms is based on Half Total Error Rate (HTER). It is defined as

Table 2. Usage of categories of counter-measures and fusion techniques. F stands for feature-level, S for score-level fusion.

| Team | Texture-based | Motion-based | Liveness-based | Fusion |
|---|---|---|---|---|
| **CASIA** | ✓ | ✓ | · | F |
| **IGD** | · | · | ✓ | S |
| **MaskDown** | ✓ | ✓ | · | S |
| **LNMIIT** | ✓ | ✓ | · | F |
| **MUVIS** | ✓ | · | · | F |
| **PRA Lab** | ✓ | · | · | S |
| **ATVS** | ✓ | · | · | · |
| **Unicamp** | ✓ | · | · | · |

Table 3. Performance results for the proposed anti-spoofing algorithms (in %)

| | Development | | | Test | | |
|---|---|---|---|---|---|---|
| **Team** | FAR | FRR | HTER | FAR | FRR | HTER |
| **CASIA** | 0.00 | 0.00 | **0.00** | 0.00 | 0.00 | **0.00** |
| **IGD** | 5.00 | 8.33 | 6.67 | 17.00 | 1.25 | 9.13 |
| **MaskDown** | 1.00 | 0.00 | 0.50 | 0.00 | 5.00 | 2.50 |
| **LNMIIT** | 0.00 | 0.00 | **0.00** | 0.00 | 0.00 | **0.00** |
| **MUVIS** | 0.00 | 0.00 | 0.00 | 0.00 | 2.50 | 1.25 |
| **PRA Lab** | 0.00 | 0.00 | 0.00 | 0.00 | 2.50 | 1.25 |
| **ATVS** | 1.67 | 0.00 | 0.83 | 2.75 | 21.25 | 12.00 |
| **Unicamp** | 13.00 | 6.67 | 9.83 | 12.50 | 18.75 | 15.62 |

a mean of False Acceptance Rate (FAR) and False Rejection Rate (FRR). In the case of anti-spoofing, FAR refers to the ratio of spoofing attacks which are not correctly detected, while FRR refers to the ratio of real accesses which are incorrectly classified as spoofing attacks. The HTER is measured on the anonymized test set using a threshold calculated 'a priori' on the development set. The threshold, chosen using the Equal Error Rate (EER) criterion, is the value equalizing FAR and FRR.

Table 3 summarizes the performance of the proposed algorithms. The performance figures are given for both development and anonymized test set. The algorithms are trained and evaluated considering all the types of attacks in the Replay-Attack database.

Considering the results on the test set, two teams have achieved perfect discrimination between the real accesses and the spoofing attacks of the Replay-Attack database: CASIA and LNMIIT . Several other teams have achieved perfect separability of the two classes on the development set, but their algorithms do not generalize as well on the anonymized test set. Still, they are outperforming state-of-the-art algorithms evaluated on Replay-Attack [5], [6].

It is interesting to notice that the winning algorithms fuse two categories of features: texture- and motion-based. The rest of the algorithms which achieve very low HTER also combine several approaches together: PRA Lab and MUVIS fuse only texture based methods, while MaskDown combines different categories of methods, but at score-level. On the contrary, the algorithms which rely only on a single cue are less successful in discriminating real accesses and spoofing attacks.

Considering the diversity of attacks in Replay-Attack, it seems that an approach relying on a single cue is not able to detect all types of attacks. Different types and different qualities of spoofing attacks need to be tackled in a different way. Perhaps that is the reason why algorithms that are combining complementary counter-measures achieve better results and even manage to solve the spoofing problem for the Replay-Attack database.

One of the goals of the competition was to support reproducible research by encouraging the participants to provide the source code of their algorithms as a free software. This will allow easy reproduction of results and a reliable reference for comparison with future anti-spoofing algorithms. One team, MaskDown , responded to this invitation.

## 5. Conclusion

As a challenging problem critical for the security of the biometric recognition system, spoofing attacks are drawing more and more attention from the biometric community. The face modality is a widely used biometric trait, but exceptionally easy to spoof due to the wide availability and easy accessibility to the face data of the users. Starting with naive spoofing attacks created by printing a face image on a paper, the face anti-spoofing field achieved great progress in the past several years. Not only the anti-spoofing algorithms have become complex and sophisticated, but the spoofing attacks themselves have evolved to be more realistic and very successful in bypassing a baseline face recognition system.

The appearance of Replay-Attack has inspired a competition to challenge researchers to develop novel spoofing counter-measures able to detect several different types of face spoofing attacks. This paper presents the face anti-spoofing algorithms developed in the course of the competition. All 8 participating teams have developed highly-sophisticated methods, approaching the problem from different aspects. Some of them extend the boundaries of the established categories of face spoofing counter-measures. For example, IGD explores a new evidence of liveness: the human pulse. ATVS introduces a novel cue, which is the degradation of the quality of images when being recaptured. Unicamp and MaskDown extend the definition of texture in temporal dimension.

Several participating teams achieve impressive results in detecting spoofing attacks in the Replay-Attack database. A new developing trend that most of them follow is fusion of

different categories of cues. Such an approach seems to be effective in tackling diverse set of spoofing attacks. As the quality and sophistication of spoofing attacks is expected to increase in the future, this observation gives indication on the directions for future research in face anti-spoofing.

Although refined and effective in deceiving face recognition systems, the attacks in the Replay-Attack database have been defeated by the anti-spoofing algorithms proposed in this competition. One of the main objectives for future work should be assembling a database with even more realistic spoofing attacks, for example 3D masks. That database should inherit the advantages of Replay-Attack, like the unbiased protocol and the provision of enrollment data.

Given the novel ideas, the achieved results and the drawn conclusions, the 2nd Competition on Counter Measures to 2D Face Spoofing Attacks has achieved the goals to consolidate a set of state-of-the-art face spoofing counter-measures and to establish a new level of quality for the research in face anti-spoofing in general.

**Acknowledgments** The authors would like to thank the Swiss Innovation Agency (CTI Project Replay) and the FP7 European TABULA RASA Project[4] (257289) for their financial support.

## References

[1] Y. Altun, I. Tsochantaridis, and T. Hofmann. Hidden markov support vector machines. In *International Conference on Machine Learning*, 2003.

[2] A. Anjos et al. Bob: a free signal processing and machine learning toolbox for researchers. In *20th ACM Conference on Multimedia Systems (ACMMM)*. ACM Press, Oct. 2012.

[3] A. Anjos and S. Marcel. Counter-measures to photo attacks in face recognition: a public database and a baseline. In *International Joint Conference on Biometrics 2011*, 2011.

[4] M. M. Chakka et al. Competition on counter measures to 2-d facial spoofing attacks. In *IJCB*, pages 1–6, 2011.

[5] 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*, pages 1–7, 2012.

[6] T. de Freitas Pereira et al. LBP-TOP based countermeasure against face spoofing attacks. In *International Workshop on Computer Vision With Local Binary Pattern Variants - ACCV*, page 12, 2012.

[7] S. de Jong. SIMPLS: an alternative approach to partial least squares regression. *Chemometrics and Intelligent Laboratory Systems*, 18(3):251–263, 1993.

[8] G. Farnebäck. Two-frame motion estimation based on polynomial expansion. In *SCIA*, pages 363–370, 2003.

[9] J. Friedman, T. Hastie, and R. Tibshirani. Additive logistic regression: a statistical view of boosting. *Annals of Statistics*, 28:2000, 1998.

[4] http://www.tabularasa-euproject.org

[10] S. Guimaraes et al. A Method for Cut Detection Based on Visual Rhythm. In *SIBGRAPI*, pages 297–304, 2001.

[11] R. Haralick, K. Shanmugam, and I. Dinstein. Textural Features for Image Classification. *IEEE TSMC*, SMC-3(6):610 –621, nov. 1973.

[12] A. K. Jain and A. Ross. *Handbook of Biometrics*, chapter Introduction to Biometrics. Springer-Verlag, 2008.

[13] J. Komulainen, A. Hadid, and M. Pietikäinen. Face spoofing detection using dynamic texture. In *ACCV 2012 Workshops, Part I (LBP 2012), LNCS*, volume 7728, pages 146–157, 2013.

[14] J. Määttä, A. Hadid, and M. Pietikäinen. Face spoofing detection from single images using micro-texture analysis. In *International Joint Conference on Biometrics*, pages 1–7, 2011.

[15] B. Manjunath and W. Ma. Texture features for browsing and retrieval of image data. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(8):837–842, 1996.

[16] T. Ojala, M. Pietikainen, and T. Maenpaa. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(7):971 –987, July 2002.

[17] M. A. Saad, A. C. Bovik, and C. Charrier. Blind image quality assessment: A natural scene statatistics approach in the DCT domain. *IEEE Trans. on Image Processing*, 21:3339–3352, 2012.

[18] H. R. S. Sheikh, M. F. Sabir, and A. C. Bovik. A statistical evaluation of recent full reference image quality assessment algorithms. *IEEE Trans. on Image Processing*, 15:3440–3451, 2006.

[19] Stauffer and W. Grimson. Adaptive background mixture models for real-time tracking. In *Computer Vision and Pattern Recognition*, 1999.

[20] X. Tan et al. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In *ECCV (6)*, pages 504–517, 2010.

[21] R. Tronci et al. Fusion of multiple clues for photo-attack detection in face recognition systems. In *IJCB*, pages 1–6, 2011.

[22] R. Tronci, G. Giacinto, and F. Roli. Dynamic score combination: A supervised and unsupervised score combination method. In *Machine Learning and Data Mining in Pattern Recognition*, volume 5632, pages 163–177. 2009.

[23] H.-Y. Wu et al. Eulerian video magnification for revealing subtle changes in the world. *ACM Trans. Graph. (Proceedings SIGGRAPH 2012)*, 31(4), 2012.

[24] J. Yan et al. Face liveness detection by exploring multiple scenic clues. In *12th International Conference on Control, Automation, Robotics and Vision*, 2012.

[25] G. Zhao and M. Pietikäinen. Dynamic texture recognition using local binary patterns with an application to facial expressions. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(6):915–928, 2007.

[26] Z. Zhiwei et al. A face antispoofing database with diverse attacks. In *Proceedings of the 5th IAPR International Conference on Biometrics (ICB'12), New Delhi, India*, 2012.