Open access • Proceedings Article • DOI:10.1109/ICB.2013.6612968

Complementary countermeasures for detecting scenic face spoofing attacks — Source link

Jukka Komulainen, Abdenour Hadid, Matti Pietikäinen, André Anjos ...+1 more authors

Institutions: University of Oulu, Idiap Research Institute

Published on: 04 Jun 2013 - International Conference on Biometrics

Topics: Spoofing attack and Replay attack

Complementary Countermeasures for Detecting Scenic Face Spoofing Attacks

Jukka Komulainen, Abdenour Hadid, Matti Pietikäinen
Center for Machine Vision Research, University of Oulu
P.O. Box 4500
FI-90014 University of Oulu, Finland
{jukmaatt,hadid,mkp}@ee.oulu.fi

André Anjos, Sébastien Marcel
Idiap Research Institute
Centre du Parc - rue Marconi 19
CH-1920 Martigny, Suisse
{andre.anjos,marcel}@idiap.ch

Abstract

The face recognition community has finally started paying more attention to the long-neglected problem of spoofing attacks. The number of countermeasures is gradually increasing and fairly good results have been reported on the publicly available databases. There exists no superior anti-spoofing technique due to the varying nature of attack scenarios and acquisition conditions. Therefore, it is important to find out complementary countermeasures and study how they should be combined in order to construct an easily extensible anti-spoofing framework. In this paper, we address this issue by studying fusion of motion and texture based countermeasures under several types of scenic face attacks. We provide an intuitive way to explore the fusion potential of different visual cues and show that the performance of the individual methods can be vastly improved by performing fusion at score level. The Half-Total Error Rate (HTER) of the best individual countermeasure was decreased from 11.2% to 5.1% on the Replay Attack Database. More importantly, we question the idea of using complex classification schemes in individual countermeasures, since nearly same fusion performance is obtained by replacing them with a simple linear one. In this manner, the computational efficiency and also probably the generalization ability of the resulting anti-spoofing framework are increased.

1. Introduction

Face recognition has been an active research area in computer vision research because facial information provides means for non-intrusive and natural interaction, identity verification and recognition. Although wide range of viewpoints, ageing of subjects and complex outdoor lighting are still research challenges, face recognition is beginning to be mature enough for biometric-enabled applications. However, vulnerability to direct attacks is the most crucial problem for companies willing to market 2D face based biometric identity management solutions.

A spoofing attack occurs when a biometric authentication system is bypassed by falsifying biometric data of a valid user and presenting the forged trait to the sensor. Compared to other modalities, falsifying face biometric data is straightforward because no special skills are required. Hiding your face in public is extremely difficult, thus facial information can be captured even from long distance. Furthermore, a great deal of multimedia content, i.e. photographs and videos, is openly available in the Internet due to the increasing popularity of social network websites (facebook, flickr, youtube, instagram and others). While photo-realistic masks and plastic surgery remain still rather expensive, spoofing attacks are usually perpetrated using photographs and videos of the targeted person because printers and high definition display devices are very affordable.

Recently, face recognition community has begun to focus more on the vulnerabilities of face authentication systems that can be attested in the gradually increasing number of publicly available databases and developed countermeasures. Although impressive results have been reported on individual databases, the varying nature of spoofing attacks and environmental conditions makes it impossible to predict how single anti-spoofing techniques can generalize the problem in real-world applications. Moreover, we cannot foresee all possible attack scenarios and cover them in databases because the imagination of the human mind always finds out new tricks to fool existing systems. Thus, we must constantly keep developing novel countermeasures.

Nevertheless, the security of the current face authentication systems can be already improved by utilizing existing countermeasures. A good example of this was the eye blink detection based liveness check that was introduced to the Face Unlock feature on Android phones. Although this simple security update is not capable of dealing with cut-photo or animated face attacks, it still manages to boost the robustness to the plain photo-attacks. It is reasonable to assume that no single superior technique is able to detect all known, let alone unseen, spoofing attacks. However, an anti-spoofing solution consisting of several complemen-

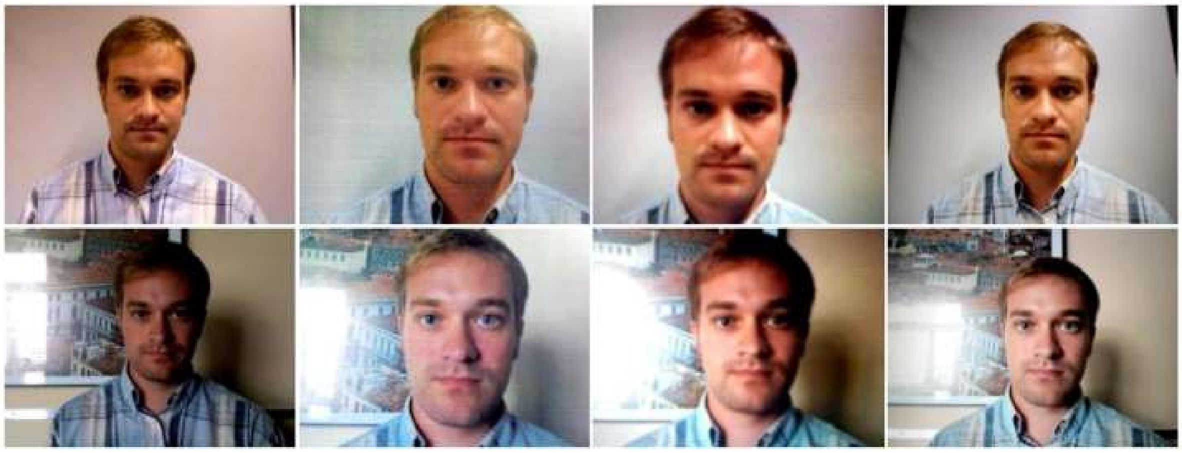

Figure 1. Examples of real accesses attempts (leftmost column) and corresponding scenic fake face attacks, i.e. face spoof with both face and background scene, from the Replay-Attack Database [6].

tary countermeasures probably performs more robustly under various fake face attacks. Therefore, it is also important to find out which countermeasures are complementary and how the different techniques should be combined. This would provide insight on how to construct a flexible anti-spoofing framework in which new techniques can be easily integrated. In this manner, the discovered vulnerabilities could be patched in no time when new countermeasures appear.

Fusion of multiple visual cues for spoofing detection is its own research topic but unfortunately it has not been studied much apart from the methods [20, 23, 24] proposed within the context of the recently organized IJCB 2011 competition on counter measures to 2D facial spoofing attacks [5]. In this work, we address this issue by analysing the fusion potential of motion [1] and micro-texture analysis [6, 15] based methods under various scenic face spoofing attacks on the Replay-Attack Database [6] (see Fig. 1). We show that the two countermeasures are indeed complementary and that their moderate performance can be vastly improved by performing fusion at score level. More importantly, we find out that the computational efficiency and probably also generalization ability of the anti-spoofing framework can be increased by reducing the complexity of the individual countermeasures without nearly any trade-off in the fusion performance.

The remainder of the paper is organized as follows: Section 2 gives on overview of the state-of-the-art countermeasures to 2D face spoofing attacks. In Section 3, we introduce the studied countermeasures and the fusion strategy used in our experiments. In Section 4, we provide the results of our complementarity analysis and report the resulting fusion performance of the countermeasures. Finally, we conclude the paper and discuss directions for future research in Section 5.

2. Related work

While challenge-response approach [9, 12, 7], multi-modal analysis [8, 12] and multi-spectral imaging [25, 18, 21] provide efficient means for discriminating real faces from fake ones, they are also rather impractical due to interaction or unconventional imaging requirements. In this section, we review only anti-spoofing techniques requiring no user-cooperation and using conventional imaging systems because these properties make them appealing to use within the existing face authentication systems. Another advantage is that usually it is not known which visual cues are used when the system is harder to deceive.

Typical non-intrusive 2D face anti-spoofing technique is liveness detection that aims at detecting physiological signs of life, such as eye blinking, facial expression changes and mouth movements. For instance Pan *et al.* [17] exploited the observation that humans blink once every 2-4 seconds and used Conditional Random Field (CRF) framework to model and detect eye blinking. In general, motion analysis is a commonly used countermeasure since it can be assumed that the movement of planar objects, e.g. video displays and photographs, differs significantly from real human faces which are complex 3D objects. Kollreider *et al.* [11] presented an optical-flow based method to capture and track the subtle movements of different facial parts, assuming that facial parts in real faces move differently than on photographs. In another work [4], Bao *et al.* also used optical flow based motion estimation for describing the movement of planar objects such as prints or screens. Anjos *et al.* [1] presented a countermeasure to scenic face attacks by measuring the motion correlation between the face and the background regions through simple frame differences. Even though motion is an important visual cue, vitality and non-rigid motion detectors are powerless under video-replay attacks if interaction is not employed.

Another category of anti-spoofing methods are based on the analysis of skin properties such as reflectance and texture. Assuming that photographs are usually smaller in size and they would contain fewer high frequency components compared to real faces, Li *et al.* [14] described a method based on the analysis of 2D Fourier spectra. In a recent work, Tan *et al.* [22] considered the Lambertian reflectance model and extracted two types of latent reflectance features using a variational retinex-based approach and difference-of-Gaussians (DoG) filtering to discriminate between the 2D images of face prints and 3D live faces. The aforementioned approaches may work well for down-sampled photos but are likely to fail for higher-quality images. Bai *et al.* [3] extracted micro-textures from the specularity component of an image to detect recaptured images. The major drawback of this method is that it requires high resolution input images in order to discriminate the fine micro-texture of the used spoofing medium. Määttä *et al.* [15] and Chingovska *et al.* [6] addressed this issue by exploring the structure of facial micro-textures using local binary patterns (LBP) [16] on conventional webcam-quality images. However, the nature of texture patterns varies a lot due to different acquisition conditions and spoofing media, thus diverse datasets are needed for training the micro-texture based methods.

Recently, Komulainen *et al.* [13] extended the micro-texture analysis based spoofing detection into spatiotemporal domain. In addition to analysing the structure of facial micro-textures, local binary patterns from three orthogonal planes (LBP-TOP) [26] were applied for describing specific dynamic events, e.g. facial motion and sudden characteristic reflections of planar spoofing media, and scenic cues which might differentiate real faces from fake ones. Similar visual cue was considered in the work by Pinto *et al.* [19] as the dynamic artefacts of display devices were exploited for detecting video-replay attacks. More specifically, visual rhythms were computed from the Fourier spectrum of the extracted video noise signatures and the resulting textural information was compressed with gray level co-occurrence matrices (GLCM).

Fusion of anti-spoofing measures has not been studied much and mainly combination of highly correlated motion cues [10] has been considered. The algorithms [20, 23, 24] proposed within the context of the recently organized IJCB 2011 competition on counter measures to 2D facial spoofing attacks [5] were an exception and presented interesting visual cues and fusion strategies. Tronci *et al.* [23] and Schwartz *et al.* [20] were able to obtain impressive performance using motion and texture information but at the cost of complexity. In [23], many visual features and support vector machines (SVM) were needed for detecting simple print-attacks, whereas in [20] temporal information from videos was accumulated by concatenating descriptions of individual frames which results in very high-dimensional feature vectors. Conversely, Yan *et al.* [24] wanted to achieve better generalization capabilities and proposed novel liveness clues with clear semantic definitions in order to avoid just extracting specific feature and training a "black box" classifier. However, the algorithm utilized mainly two uncorrelated motion cues, non-rigid motion and face-background consistency analysis, while the only spatial cue, banding analysis, was discarded unless uniform background was observed, since both face and background regions were used for image quality assessment.

Indeed, many directions for non-intrusive spoofing detection have been already explored but none of them is alone able to capture the nature of every face spoofing scenario. Therefore, the problem of spoofing attacks should be broken down into attack-specific subproblems that can be solved efficiently with a proper combination of countermeasures. To follow this principle, we propose fusion of motion and texture based methods for detecting various scenic face attacks. Furthermore, as computational efficiency is very important criterion when multiple anti-spoofing measures are used in parallel, we question the use of complex classifications schemes on individual countermeasures.

3. Detecting scenic fake face attacks

In addition to the used spoofing medium type, such as photograph and video display, 2D fake face attacks can be categorized into two groups, close-up and scenic attacks, based on how the fake face is represented with the spoofing medium. Both types of 2D face spoofs have common and, more importantly, their own distinctive visual cues that can be exploited in spoofing detection schemes.

A close-up spoof describes only the facial area which is presented to the sensor. The main weakness with the tightly cropped fake spoofs is that the boundaries of the spoofing medium, e.g. a video screen frame, photograph edges, or the attacker's hands are usually visible during the attack, thus can be detected in the scene [13]. However, these visual cues can be hidden by incorporating background scene in the face spoof and placing the resulting scenic face spoof very near to the sensor. Fortunately, the proximity between the spoofing medium and the camera might cause the recaptured face image to be out-of-focus and reveal also other facial texture quality issues, like degradation due to the used spoofing medium. Furthermore, for stationary systems, it should be possible to observe high correlation between the overall motion of the face and the background regions.

In this work, we concentrate on detecting scenic spoofing attacks by exploiting the aforementioned two visual cues. More specifically, we study more closely the fusion of two recently proposed countermeasures based on motion [1] and

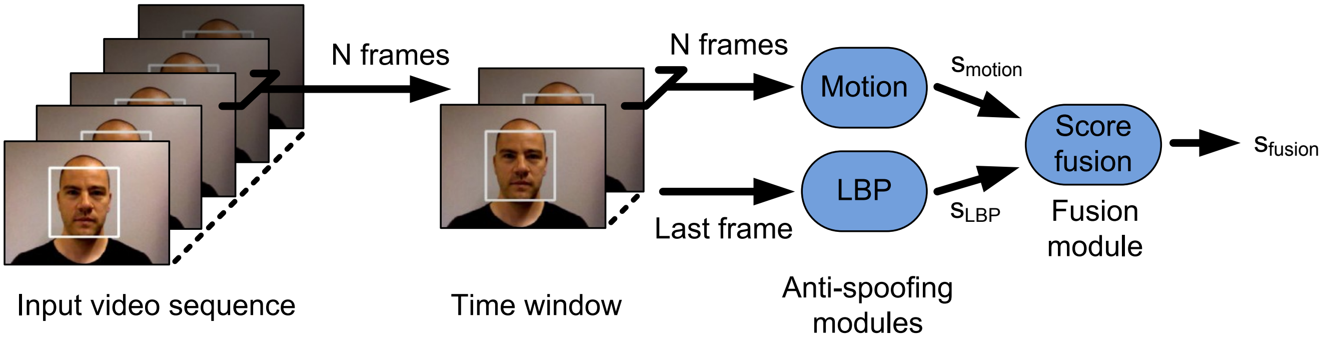

Figure 2. Block diagram of the used fusion strategy.

micro-texture analysis [6, 15] that have individually shown moderate discriminative power.

3.1. Motion correlation analysis

Anjos and Marcel [1] proposed a straightforward motion-based anti-spoofing technique to measure the correlations between the client head movements and the background scene. The main idea of the algorithm is to ignore the direction of the movements and focus only on intensity information. Thus, an area-normalized sum of the frame-difference is computed separately for both regions to form two signal patterns that describe the total motion within the regions. The resulting motion signals are divided into time windows of N frames from which five quantities are extracted to form a compact motion representation. A multi-layer perceptron (MLP) classifier is then used for evaluating whether excessive motion (hand-held attack) or no movement (fixed support photo-attack) is observed during the time window of N frames.

3.2. Facial texture analysis

Määttä *et al.* [15] and Chingovska *et al.* [6] found that degradation in facial skin texture quality and disparities in reflectance properties can be captured by analysing facial micro-textures using local binary patterns (LBP) [16]. More specifically, uniform patterns (LBP^{u2}) were considered when only the labels which contain at most two 0-1 or 1-0 transitions are utilized instead of all possible LBP codes. Like in [6, 15], we describe the facial texture properties by computing LBP over normalized face of 64 × 64 pixels. However, we extract only the global description of the facial texture using $LBP^{u2}_{8,1}$ operator instead of dividing the face into several blocks. The resulting 59-bin feature histogram is then fed to a support vector machine (SVM) classifier that decides whether the texture description corresponds to the properties of genuine face or not.

3.3. Fusion strategies

The motion correlation analysis based technique is efficient for measuring synchronized shaking of hand-held attacks within the scene. However, a drawback is that it can get confused between a fixed support photo-attack and a motionless person while being recognized [1]. Moreover, the method was originally proposed for detecting photo-attacks, while the assumption of decorrelated movement between face and background is unfortunately true also in case of video replay-attacks. On the other hand, the performance of LBP based countermeasures is not dependent on the spoofing attack scenario if disparities in the facial texture properties exist. More importantly, the two countermeasures exploit independent visual cues, motion and texture, thus intuitively they should be able to provide complementary information about the nature of the observed access attempt.

The environmental conditions and possible spoofing scenarios are unpredictable in real world applications. It can be assumed that the generalization ability and stability of the individual countermeasures could be improved by reducing the complexity of individual countermeasures. Thus, we also considered to utilize linear discriminant analysis (LDA) instead of the complex classifiers (MLP and SVM) used in the original methods to avoid overfitting and possibly increasing robustness in real-world applications.

The block diagram of the proposed fusion strategy is illustrated in Fig 2. In order to combine the motion and micro-texture analysis based techniques, the video sequences are divided into overlapping windows of N frames with an overlap of N-1 frames and each observation generates an independent score of the rest of the video sequence. For the sake of simplicity, the LBP based face description is computed only for the last frame, whereas the five quantities are extracted over the whole time window for evaluating the motion correlation as in [1]. The fusion of the two visual cues is then performed at score level using linear logistic regression (LLR).

	Motion	LBP	Mutual
Devel	11.13	14.72	**2.25**
Test	12.22	12.51	**1.37**

Table 1. Overall error rates (%) of time windows for individual methods with complex classifiers (MLP for motion and SVM for LBP) compared to the percentage of mutual errors over all samples.

	Motion	LBP	Mutual
Devel	15.16	19.07	**2.27**
Test	16.89	15.69	**1.76**

Table 2. Overall error rates (%) of time windows for individual methods with LDA classifier compared to the percentage of mutual errors over all samples.

The proposed anti-spoofing framework was implemented using the free signal processing and machine learning toolbox Bob [2]. The source code of the fusion algorithm[1] as well as the individual countermeasures (motion[2] and texture[3]) are available as add-on packages to this framework. After installation, it is possible to reproduce all reported experiments.

4. Experimental analysis

In this section, we provide an in-depth analysis on combining the motion and micro-texture analysis based countermeasures. The experiments are conducted on the Replay-Attack database[4] consisting of several types of scenic spoofing attacks. The database is divided into three non-overlapping subsets for training, development and testing the countermeasures. The training set is used for training the countermeasure, whereas the development set operates as a separate validation set for estimating a threshold value to be used on the test set. The database protocol defines the Equal Error Rate (EER) as a decision threshold. The actual test set is used only to report results. As performance measure, the protocol suggests to report the Half-Total Error Rate (HTER) on the test data.

The purpose of our experimental analysis is to first determine if the two countermeasures have fusion potential and then see what is the actual fusion performance under scenic spoofing attacks. More importantly, we study how the reduced complexity of the individual methods affects the performance of the anti-spoofing framework. To be consistent with the experiments in [1], we fixed the window size N at 20 frames which represents roughly a second in video time.

4.1. Fusion potential analysis

The complementarity of different countermeasures should be determined before blindly trying fusion. Therefore, we considered a set of total errors for each individual anti-spoofing technique and applied mutual error analysis on the two error sets in order to determine the number of samples that both countermeasures fail to recognize.

Table 1 and Table 2 present the total error rates for time windows of 20 frames using the original and simplified classification schemes of the individual countermeasures and the portion of their mutual mistakes. As we can see, the percentage of common errors is extremely low compared to the moderate accuracy of the individual methods. Furthermore, the LDA outputs of the two techniques with a LLR decision boundary are visualized in Fig. 3. The scatter plot depicts that an increased linear separability can be obtained by combining the two visual cues. These observations indicate that the motion and LBP based countermeasures are indeed complementary, thus the fusion of these anti-spoofing approaches should improve robustness to scenic attacks.

It is also important to notice that only a minor increase from 1.37% to 1.76% in the number of mutual errors is observed when LDA is used on individual countermeasures to reduce complexity even if the individual performances degrade substantially. Since the fusion potential is unaffected by the proposed simplification, the use of LDA is considered also in the following experiments.

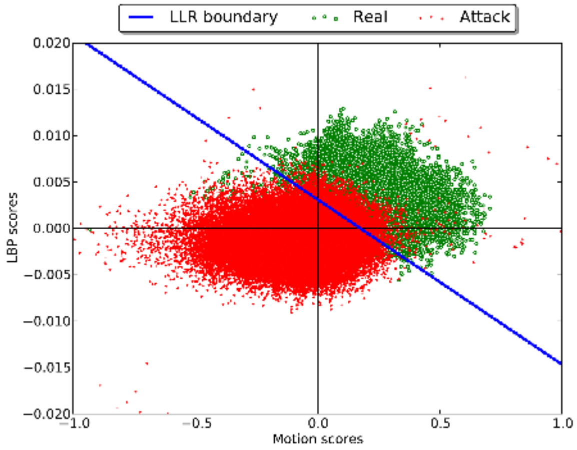

Figure 3. Scatter plot of the two countermeasures with LLR decision boundary.

4.2. Fusion results using independent observations

Now, we perform fusion at score level in order to find out the actual benefit that we gain by combining motion correlation and LBP based countermeasures. The overall accuracy for time windows is shown in Table 3. The results sup-

[1] http://pypi.python.org/pypi/antispoofing.fusion
[2] http://pypi.python.org/pypi/antispoofing.motion
[3] http://pypi.python.org/pypi/antispoofing.lbp
[4] http://www.idiap.ch/dataset/replayattack

	Devel		Test	
Method	Complex	LDA	Complex	LDA
Motion	11.13	15.16	11.2	16.05
LBP	14.72	19.08	15.06	17.12
LLR	**4.57**	**5.48**	**5.11**	**5.47**

Table 3. Overall performance (HTER in %) for time windows. Complex classifiers means that MLP is used for motion correlation and SVM for LBP based method.

port our complementary hypotheses as significant performance enhancement is obtained when both techniques are used together. For example, the HTER of motion correlation based approach can be improved from 11.20% to 5.1% by utilizing also the LBP based face description. Moreover, the simplification of classification schemes reduces the performance of the individual methods whereas the fusion performance remains nearly the same. This observation is also consistent with our mutual error analysis, thus suggesting that the complementarity of countermeasures is somewhat independent of the complexity of the individual classification techniques.

4.3. Access attempt based analysis

So far, we classified the individual time windows of 20 frames without exploiting the temporal dimension of the video sequences. In this section, we determine the video-based performance of the proposed spoofing detection scheme by accumulating the fused scores of classified time windows as time passes.

Fig 4 describes the HTER evolution of access attempt based performance on the test set using the same threshold as in Section 4.2. As expected, LBP based countermeasure does not benefit much from the temporal processing because it is not able to exploit the available motion information. On the other hand, the motion based technique gains a huge performance boost because people tend to start moving more in front of the camera as time passes, thus reducing the false rejection rate as the amount of decorrelated movement increases in the scene.

Fusion always outperforms the individual countermeasures. However, it is interesting to notice that the HTER of combination of LDA-based classifiers drops much faster and saturates within 75 frames (three seconds in video time), whereas it takes more than 100 frames (four seconds in video time) when the outputs of more complex classification schemes are combined. Furthermore, the simplified anti-spoofing framework actually works significantly better when spoofing decision is made within 100 frames. This gives another good reason to consider the use of less complex classification schemes in addition to their computational simplicity.

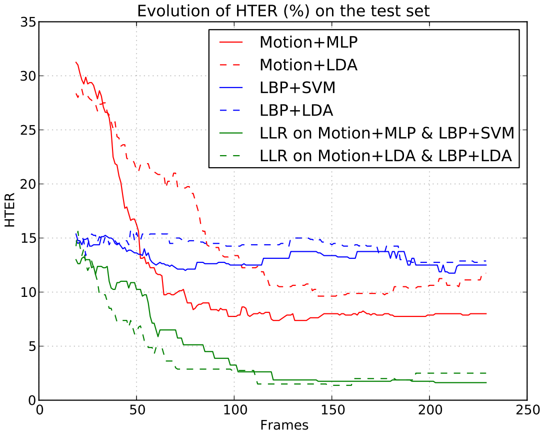

Figure 4. HTER (%) evolution of the individual countermeasures and their fusion (video based analysis).

5. Conclusion

No existing anti-spoofing technique is able to detect all types of attacks, thus it is important to find out complementary countermeasures and study how they should be combined in order to construct an easily extensible anti-spoofing framework. In this work, we addressed this issue by studying fusion of motion and texture based countermeasures under several types of scenic fake face attacks. We explored the fusion potential of different anti-spoofing techniques by performing mutual error analysis. The total error rates of the individual methods were over 12% whereas the percentage of mutual errors was below 2% suggesting that the countermeasures are indeed complementary. The actual fusion results were coherent with our mutual errors analysis since the unsatisfying performance of the two individual techniques was significantly improved (from 11.2% to 5.1% in terms of HTER) when performing fusion at score level.

The use of simpler linear classification scheme on individual countermeasures was also studied. When the original complex classifiers were replaced with LDA, the performance of individual methods degraded substantially. However, the number of mutual errors increased only from 1.4% to 1.8% and the HTER of the fusion performance from 5.1% to 5.5%, thus indicating that the complementarity of countermeasures is somewhat independent of the complexity of the individual classification techniques. Furthermore, the access attempt based analysis revealed that the performance of the simplified anti-spoofing framework actually converged faster when temporal information was accumulated. Since the generalization ability of very complex classification schemes can be questioned and the gain in fusion performance on databases is very small, the use of simple and computationally efficient classifiers should be indeed considered when constructing real-world anti-spoofing solutions.

In future, we plan to increase the number of countermeasures and fusion techniques in the anti-spoofing framework because interesting approaches have been introduced very recently. For instance the use of dynamic texture has shown to be effective in describing the differences between real faces and fake ones. In addition, we will focus on studying the generalization capabilities of the individual countermeasures and their fusion using cross-database testing. Especially the effectiveness of different classification schemes on individual countermeasures and fusion strategies will be evaluated more closely.

6. Acknowledgments

The research leading to these results has received funding from the European Community's FP7 under grant agreements 257289 (TABULA RASA) and 284989 (BEAT). The financial support of Academy of Finland and Infotech Oulu Graduate School is also gratefully acknowledged.

References

[1] A. Anjos and S. Marcel. Counter-measures to photo attacks in face recognition: a public database and a baseline. In *Proceedings of IAPR IEEE International Joint Conference on Biometrics (IJCB), Washington DC, USA*, 2011.

[2] A. Anjos, L. E. Shafey, R. Wallace, M. Günther, C. McCool, and S. Marcel. Bob: a free signal processing and machine learning toolbox for researchers. In *20th ACM Conference on Multimedia Systems (ACMMM), Nara, Japan*. ACM Press, Oct. 2012.

[3] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi. Is physics-based liveness detection truly possible with a single image? In *IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 3425–3428, 2010.

[4] W. Bao, H. Li, N. Li, and W. Jiang. A liveness detection method for face recognition based on optical flow field. In *2009 International Conference on Image Analysis and Signal Processing*, pages 233–236. IEEE, 2009.

[5] 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. Castrillón-Santana, J. Määttä, A. Hadid, and M. Pietikäinen. Competition on counter measures to 2-d facial spoofing attacks. In *Proceedings of IAPR IEEE International Joint Conference on Biometrics (IJCB), Washington DC, USA*, 2011.

[6] I. Chingovska, A. Anjos, and S. Marcel. On the effectiveness of local binary patterns in face anti-spoofing. In *IEEE BIOSIG 2012*, Sept. 2012.

[7] M. De Marsico, M. Nappi, D. Riccio, and J.-L. Dugelay. Moving face spoofing detection via 3D projective invariants. In *ICB 2012, 5th IAPR International Conference on Biometrics, 29 March-1 April 2012, New Delhi, India*, New Delhi, INDIA, 03 2012.

[8] R. W. Frischholz and U. Dieckmann. Bioid: A multimodal biometric identification system. *Computer*, 33(2):64–68, Feb. 2000.

[9] R. W. Frischholz and A. Werner. Avoiding replay-attacks in a face recognition systenm using head-pose estimation. In *Proceedings of the IEEE International Workshop on Analysis and Modeling of Faces and Gestures*, 2003.

[10] K. Kollreider, H. Fronthaler, and J. Bigun. Verifying liveness by multiple experts in face biometrics. In *IEEE Conference on Computer Vision and Pattern Recognition Workshops : CVPR 2008*, pages 1200–1205, 2008.

[11] K. Kollreider, H. Fronthaler, and J. Bigun. Non-intrusive liveness detection by face images. *Image and Vision Computing*, 27:233–244, 2009.

[12] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun. Real-time face detection and motion analysis with application in liveness assessment. *Trans. Info. For. Sec.*, 2(3):548–558, Sept. 2007.

[13] J. Komulainen, A. Hadid, and M. Pietikäinen. Face spoofing detection using dynamic texture. In *International Workshop on Computer Vision With Local Binary Pattern Variants - ACCV*, 2012.

[14] J. Li, Y. Wang, T. Tan, and A. K. Jain. Live face detection based on the analysis of fourier spectra. In *In Biometric Technology for Human Identification*, pages 296–303, 2004.

[15] J. Määttä, A. Hadid, and M. Pietikäinen. Face spoofing detection from single images using micro-texture analysis. In *Proceedings of IAPR IEEE International Joint Conference on Biometrics (IJCB), Washington DC, USA*, 2011.

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

[17] G. Pan, Z. Wu, and L. Sun. Liveness detection for face recognition. In K. Delac, M. Grgic, and M. S. Bartlett, editors, *Recent Advances in Face Recognition*, page Chapter 9. IN-TECH, 2008.

[18] I. Pavlidis and P. Symosek. The imaging issue in an automatic face/disguise detection system. In *Proceedings of the IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications (CVBVS 2000)*, pages 15–, Washington, DC, USA, 2000. IEEE Computer Society.

[19] A. d. S. Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha. Video-based face spoofing detection through visual rhythm analysis. In *Conference on Graphics, Patterns and Images (Sibgrapi)*, 2012.

[20] W. R. Schwartz, A. Rocha, and H. Pedrini. Face Spoofing Detection through Partial Least Squares and Low-Level Descriptors. In *International Joint Conference on Biometrics*, 2011.

[21] L. Sun, W. Huang, and M. Wu. Tir/vis correlation for liveness detection in face recognition. In *Proceedings of the 14th international conference on Computer analysis of images and patterns - Volume Part II*, CAIP'11, pages 114–121, Berlin, Heidelberg, 2011. Springer-Verlag.

[22] X. Tan, Y. Li, J. Liu, and L. Jiang. Face liveness detection from a single image with sparse low rank bilinear discrimi-

native model. In *Proceedings of the 11th European conference on Computer vision: Part VI*, ECCV'10, pages 504–517, 2010.

[23] R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, and F. Roli. Fusion of multiple clues for photo-attack detection in face recognition systems. In *Proceedings of IAPR IEEE International Joint Conference on Biometrics (IJCB), Washington DC, USA*, 2011.

[24] J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Z. Li. Face liveness detection by exploring multiple scenic clues. In *12th International Conference on Control, Automation, Robotics and Vision, (ICARCV2012)*, 2012.

[25] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li. Face liveness detection by learning multispectral reflectance distributions. In *International Conference on Face and Gesture*, pages 436–441, 2011.

[26] 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.