Published in IET Biometrics
Received on 16th December 2011
Revised on 9th February 2012
doi: 10.1049/iet-bmt.2011.0009

ISSN 2047-4938

Face spoofing detection from single images using texture and local shape analysis

J. Määttä A. Hadid M. Pietikäinen

Center for Machine Vision Research, Department of Computer Science and Engineering, University of Oulu, P.O. Box 4500, FI-90014 Oulu, Finland
E-mail: jukmaatt@ee.oulu.fi

Abstract: Current face biometric systems are vulnerable to spoofing attacks. A spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gaining illegitimate access. Inspired by image quality assessment, characterisation of printing artefacts and differences in light reflection, the authors propose to approach the problem of spoofing detection from texture analysis point of view. Indeed, face prints usually contain printing quality defects that can be well detected using texture and local shape features. Hence, the authors present a novel approach based on analysing facial image for detecting whether there is a live person in front of the camera or a face print. The proposed approach analyses the texture and gradient structures of the facial images using a set of low-level feature descriptors, fast linear classification scheme and score level fusion. Compared to many previous works, the authors proposed approach is robust and does not require user-cooperation. In addition, the texture features that are used for spoofing detection can also be used for face recognition. This provides a unique feature space for coupling spoofing detection and face recognition. Extensive experimental analysis on three publicly available databases showed excellent results compared to existing works.

1 Introduction

Despite the great deal of progress during the recent years [1], 2D face biometrics (that is identifying individuals based on their 2D facial biometric characteristic) is still a major area of research. Wide range of viewpoints, occlusions, aging of subjects and complex outdoor lighting are challenges in face recognition. Although there is a significant number of works addressing these issues, the vulnerabilities of face biometric systems to spoofing attacks are mostly overlooked. For instance, the Windows XP and Vista laptops of Lenovo, Asus and Toshiba come with built-in webcams and embedded biometric systems that authenticate users by scanning their faces. However, in 2009, the Security and Vulnerability Research Team of the University of Hanoi (Vietnam) has demonstrated at Black Hat 2009 conference, the world's premier technical security conference, how to easily spoof and bypass these systems (Lenovo's Veriface III, Asus' SmartLogon V1.0.0005, and Toshiba's Face Recognition 2.0.2.32 – each set to its highest security level) using fake facial images of the legitimate user and thus gaining access to the laptops. This vulnerability is now listed in the National Vulnerability Database of the National Institute of Standards and Technology (NIST) in the US. This single example demonstrates the vulnerabilities in current face biometric systems, which suggest an urgent need for addressing spoofing attacks to enhance the security and robustness of face biometric systems, and to bring the technology into practical use.

A spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gaining illegitimate access and advantages. For instance, one can spoof a face recognition system by presenting a photograph, a video, a mask or a 3D model of a targeted person in front of the camera. Although one can also use make-up or plastic surgery as other means of spoofing, photographs are probably the most common sources of spoofing attacks because one can easily download and capture facial images. As illustrated in Fig. 1, face images captured from printed photos can look very similar to face images captured from real faces.

Lately, the vulnerabilities to spoofing attacks have received more attention and a good example of this was the recently organised IJCB 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks [2]. Furthermore, the number of publications in the field is growing steadily and some publicly available databases [3–6] have been released. Still, the field of non-intrusive anti-spoofing methods is rather immature, since there exist no consensus on the best spoofing detection practices and techniques and not that many standard databases to develop and test the algorithms for objective comparison [6].

Typical countermeasure against spoofing is liveness detection that aims at detecting physiological signs of life such as eye blinking, facial expression changes, mouth movements etc. Another existing countermeasure to spoofing attacks consists of combining face recognition with other biometric modalities such as gait and speech. Indeed, multi-modal systems are intrinsically more difficult

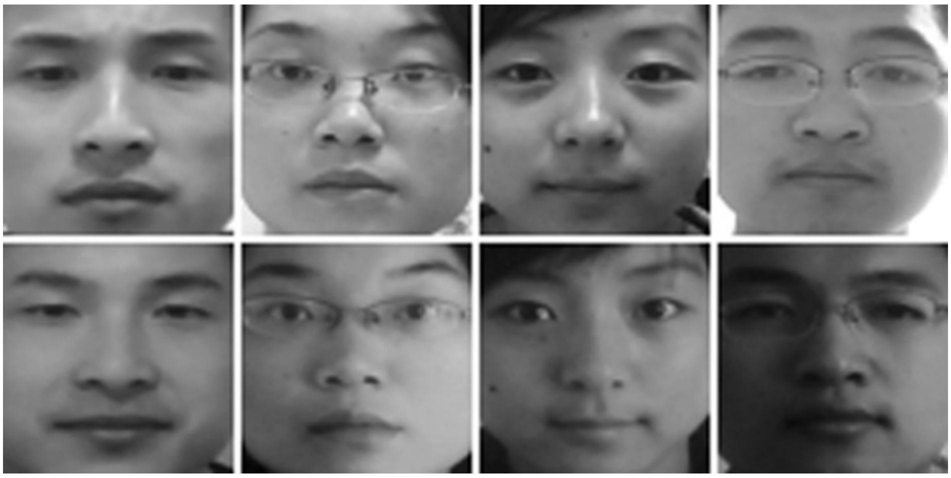

Fig. 1 *Example of images captured from real faces (upper row) and from printed photos (lower row)*
Appearance similarity illustrates the difficulty of spoofing detection from printed photos

to spoof than uni-modal systems. Some other attempts to counter face spoofing are based on structure from motion to calculate the depth information.

Inspired by image quality assessment, characterisation of printing artefacts and by differences in light reflection, we propose to approach the problem of spoofing detection from texture analysis point of view. The differences in surface geometry between human faces and face prints cause distinctive specular reflections and shades as a human face is a complex non-rigid 3D object whereas a photograph can be seen as a planar rigid object. Furthermore printing artefacts and different surface properties, for example, pigments, may cause degradation in image quality which can be assessed using texture and local shape analysis. Hence, we present a novel approach based on analysing facial image textures and gradient structures for detecting whether there is a live person or a face print in front of the camera. Compared to many previous works, our proposed approach is robust and does not require user-cooperation. In addition, the texture features that are used for spoofing detection can also be used for face recognition. This provides a unique feature space for coupling spoofing detection and face recognition.

In this work, we extend our spoofing detection approach using local binary pattern (LBP)-based micro-texture analysis [7] by introducing two low-level features, Gabor wavelet features [8] and histogram of oriented gradients (HOG) [9], to the face description which now consists of three enhanced feature vectors. The proposed method adopts complementary properties of two powerful texture descriptors, since LBP encodes the micro-texture patterns and Gabor filters more macroscopic information. In addition, HOG-based local shape description provides additional information to the face description. A homogeneous kernel map [10] is applied on each resulting feature vector transforming the data into compact linear representation and reproducing an accurate approximation of the desired kernel function. This representation enables then to use fast linear support vector machine (SVM) [11] classifiers. The final decision, whether there is a live person in front of the camera or not, is based on the score level fusion of the individual SVM outputs. Extensive experiments on three publicly available database (NUAA Photograph Imposter Database [4], Yale Recaptured Database [5] and Print-Attack Database [6]) containing several real and fake faces showed excellent results compared to many previous works.

The rest of the paper is organised as follows. Section 2 discusses related works on face spoofing attacks and countermeasures. Our proposed approach, using a set of low-level feature descriptors and linear classification scheme, is then described in Section 3 and evaluated in Section 4, where extensive experiments are conducted. The results are thoroughly analysed and also compared to many previous works. A conclusion is drawn in Section 5.

2 Related work

Without anti-spoofing measures most of the state-of-the-art facial biometric systems are basically vulnerable to attacks, since they try to maximise the discrimination between identities, instead of determining whether the presented trait originates from a real live client. Even a simple photograph of the enrolled person's face, displayed as a hard-copy or on a screen, will fool the system. Short surveys of previous attempts against spoofing attacks can be found in [3, 12]. Typical countermeasure against spoofing is liveness detection that aims at detecting physiological signs of life such as eye blinking, facial expression changes, mouth movements and so on. For instance, Pan *et al.* [3] exploited the observation that humans blink once every 2–4 s and proposed an eye blink-based anti-spoofing method. It uses conditional random field framework to model and detect eye blinking. Another commonly used countermeasure is motion analysis since it can be assumed that the movement of planar objects, for example, video displays and photographs, differs significantly from real human faces which are complex 3D objects. Kollreider *et al.* [13] 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 [14], Bao *et al.* also used optical flow for motion estimation for detecting attacks produced with planar media such as prints or screens. Experiments on a private database showed a 6% false-alarm against about 14% false-acceptance.

Another category of anti-spoofing methods are based on the analysis of skin properties such as skin texture and skin reflectance. For instance, Li *et al.* [15] described a method for detecting print-attack face spoofing. The method is

doi: 10.1049/iet-bmt.2011.0009

based on the analysis of 2D Fourier spectra, assuming that photographs are usually smaller in size and they would contain fewer high-frequency components compared to real faces. Such an approach may work well for down-sampled photos but is likely to fail for higher-quality images. The database used in the experiments is unfortunately not publicly available.

In a recent work, Tan *et al.* [4] considered the Lambertian reflectance to discriminate between the 2D images of face prints and 3D live faces. The method extracts latent reflectance features using a variational retinex-based method and difference-of-Gaussians-based approach. The features are then used for classification. The authors reported promising results on a database composed of real accesses and attacks to 15 subjects using both photo-quality and laser-quality prints. The database, the NUAA Photograph Imposter Database, is made publically available. This provides a valuable resource for fairly comparing the results of different methods. Hence, our current work also considers this database.

Other countermeasures against face spoofing attacks include multi-modal analysis and multi-spectral methods. A system combining face recognition with other biometric modalities such as gait and speech is indeed intrinsically more difficult to spoof than uni-modal systems. Multi-spectral images can also be used for analysing the reflectance of object surfaces and thus discriminating live faces from fake ones [16–18].

In recently organised IJCB 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks [2], a common trend was to use multiple anti-spoofing measures combining motion, liveness and texture and the participants were able to achieve impressive results. However, all best-performing algorithms used also some kind of texture analysis. The main problem of motion analysis and liveness detection-based anti-spoofing measures is that the verification process takes some time or moreover, the user needs to be very cooperative. In addition, these techniques are vulnerable to video replay attacks. The main advantages of spoofing detection schemes based on properties of a single image is that they treat video playback attacks as if they were photo attacks, since only a single frame is considered [19].

Bai *et al.* [19] used micro-textures extracted from the specularity component of a recaptured image and a linear SVM classifier to detect spoofing attacks. 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. Another interesting approach was introduced in [20] by Gao *et al.* who used a set of physical features to discriminate the recaptured images from real ones.

It appears that most of the existing methods for spoofing detection are either very complex (and hence not very practical for real-world face biometric systems requiring fast processing) or using non-conventional imaging systems (e.g. multi-spectral imaging) and devices (e.g. thermal cameras). Therefore we propose an approach based on highly discriminative texture and local shape features, using conventional webcam-quality images and requiring no user cooperation.

3 Spoofing detection using texture and local shape analysis

Face images captured from printed photos may visually look very similar to the images captured from live faces (see Fig. 1). Consequently, all these images would be largely overlapping in the original input space. Therefore a suitable feature space is needed for separating the two classes (live against fake face images). The main issue is how to derive such a feature space. Our method aims at learning the fine differences between the images of real face and those of face prints, and then designing a feature space which emphasises those differences.

A close look at the differences between real faces and face prints reveals that human faces and prints reflect light in different ways, because a human face is a complex non-rigid 3D object whereas a photograph can be seen as a planar rigid object. The surface properties of real faces and prints, for example, pigments, are also different. These two distinctive properties may cause characteristic specular reflections and shades. In addition, face prints often contain printing artefacts, such as jitter and banding [21], that can be detected with texture and local shape analysis on uniform or smooth areas. Furthermore, spoof attacks when executed with face prints tend to engender some overall image blur because of, for example, a low-resolution printing device or rapid motion caused by simulated photo-attacks performed like in [3, 4]. Example images of possible cues used for face print spoofing detection are presented in Fig. 2.

Inspired by the observations above, and particularly by image quality assessment and characterisation of printing artefacts, we derive a facial representation (or a feature space) that is able to capture typical characteristics of real and fake face images. Hence, the key idea of our approach is emphasising the texture and gradient structure differences in the feature space. We extend our spoofing detection approach using LBP-based micro-texture analysis [7] by introducing two complementary low-level features to the face description, Gabor wavelets and HOG. The block diagram of our anti-spoofing approach can be seen in Fig. 3. The proposed method adopts two powerful texture features, LBPs and Gabor wavelets, for describing not only the micro-textures but also more macroscopic information. In addition, local shape description is introduced using HOG. Each low-level descriptor produces its own face representation on which homogeneous kernel map is

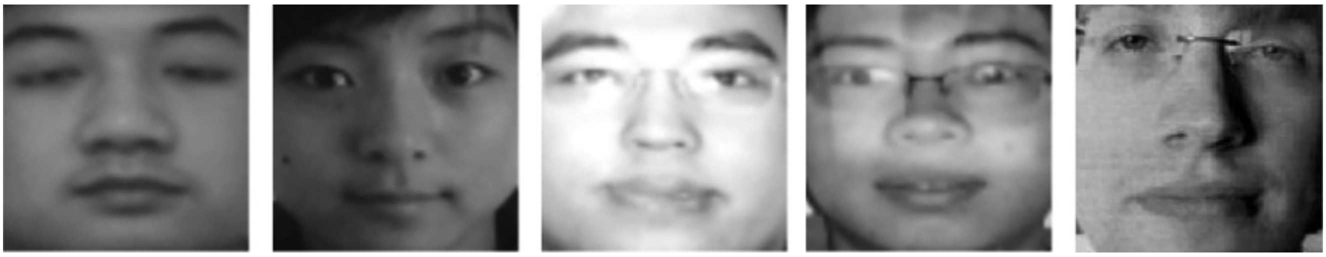

Fig. 2 *Examples of face print properties that could be used for spoofing detection, for example, overall image blur, low contrast, characteristic specular reflections and printing artefacts*

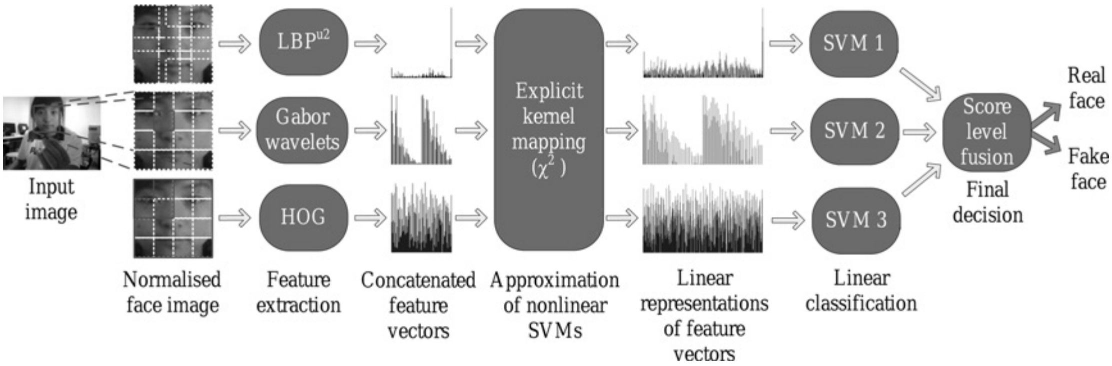

Fig. 3 *Block diagram of the proposed approach*

applied to transform the data into compact linear representation. Each vector in its own transformed feature space is then fed to a linear SVM classifier and score level fusion of the individual SVM outputs determines whether there is a live person or a fake image in front of the camera. We describe below our enhanced spoofing detection method.

3.1 Low-level feature extraction

The texture feature descriptors considered in this paper include LBPs and Gabor wavelets. In addition, shape information is combined to the face representation using HOG. A summary of these descriptors is presented as follows.

The LBP texture analysis operator, introduced by Ojala *et al.* [22], is defined as a grey-scale invariant texture measure, derived from a general definition of texture in a local neighbourhood. It is a powerful means of texture description and among its properties in real-world applications are its discriminative power, computational simplicity and tolerance against monotonic grey-scale changes. We chose uniform LBP patterns in our experiments, because of the more compact feature histogram (see [22] for details).

In addition to the LBP-based texture analysis, we use also Gabor wavelet features to enhance the texture representation of the facial image. The basic idea is to extract features at multiple scales and orientation using a Gabor wavelet decomposition. For classification purposes, a feature vector is constructed using the mean and standard deviation of the magnitude of the transform coefficients at different scales and orientations [8].

The local shape characteristics are introduced to the face representation using HOG which captures the edge or gradient structures of the facial image. HOG representation is invariant to local geometric transformations if translations or rotations are much smaller than the local spatial or orientation bin size [9].

The proposed face description consists of three enhanced feature histograms which encode the texture information and gradient structures of the facial images. First, the face is detected, cropped and normalised into an $M \times M$ pixel image. In order to preserve spatial information, the facial images are spatially partitioned into several local regions, each of which corresponds to a local patch of the face image. Then the descriptors are extracted from each block and the resulting feature vectors are concatenated into an enhanced feature vector.

Our investigations have shown, however, that texture and gradient structure details, that are needed for discriminating a real human face from fake ones, can best be detected when LBP, Gabor wavelet and HOG face representations are computed separately using different block divisions for each feature. Our LBP description [7] computes $\mathrm{LBP}_{8,1}^{u2}$ features from 3 × 3 overlapping regions (with an overlapping size of 14 pixels) to capture the spatial information and enhances the holistic description by including two global LBP histograms computed over the whole face image using $\mathrm{LBP}_{8,2}^{u2}$ and $\mathrm{LBP}_{16,2}^{u2}$ operators. Gabor filter description is determined using 4 × 4 equally spaced non-overlapping regions from which 40 Gabor wavelets of five different scales and eight orientations are extracted. Eight orientations are considered when computing the HOG features and the blocks overlap half of their area but the used block size depends on the size and geometric normalisation of the input face images.

3.2 Classification

In [10] Vedaldi and Zisserman presented a technique to accelerate kernel evaluations using a homogeneous kernel map which enables the use of additive kernels, such as χ^2 and intersection, in large-scale problems. The desired kernel can be approximated to a very good level by linear ones using suitable explicit feature map which transforms the data into a compact linear representation. Very fast linear SVMs can be then used on this representation instead of non-linear SVMs. The approximations stand on a solid theoretical ground and it has been demonstrated that the performance is indistinguishable from the original non-linear SVMs, thus reducing the train and test times notably [10].

In our experiments, we applied homogeneous kernel map on each face description to obtain their corresponding linear approximation of a χ^2 kernel. Each resulting representation is then fed to an SVM classifier and conventional *Z*-score normalisation technique and weighted score level fusion are used for combining the outputs of the individual SVMs to determine whether the input image corresponds to a live face or not.

4 Experimental analysis

In this section, we evaluate the proposed approach on three different databases which consist of single images and videos. First, we perform experiments on the NUAA Photograph Imposter Database and compare the results between LBP-based face representation [7] and the proposed approach using also Gabor wavelets and HOG. In addition, we validate the use of homogeneous kernel map by comparing it to non-linear SVM used in [7]. Then, we compare the proposed method to previously published results using Yale Recaptured Database and Print-Attack Database. Linear SVM implementation of LIBLINEAR [23] and a three-dimensional approximated feature map computed with VLFeat [24] are used in all experiments.

4.1 Evaluation of the extended method

We considered the publicly available NUAA Photograph Imposter Database [4] for comparing the enhanced face representation to our previous work presented in [7] and to validate the use of homogeneous kernel map and linear SVM instead of original non-linear SVM. The data set consists of images of both real client accesses and high-quality photo attacks which were recorded using conventional webcams at 20 fps with resolution of 640 × 480 pixels. The face images of live humans and their photographs were collected in three sessions at intervals of about 2 weeks. In addition, during each session, the environmental and illumination conditions are changing. Examples of images from the database can be seen in Fig. 1.

The database is divided into separate training and test purposes. The training set contains altogether 1743 face images of nine real clients (889 and 854 from the first and the second sessions, respectively) and 1748 imposter images of the same nine clients (855 and 893 images from the first and the second sessions, respectively). The test set is constructed from 3362 client samples and 5761 imposter images taken during the third session. Only three clients who took part in the first two sessions attended the third session. Furthermore, six new clients and their photographs are introduced in the test set to further increase the level of difficulty. In order to achieve fair comparison, we consider the provided greyscale face images which have been geometrically normalised into images of 64 × 64 pixels.

We started by investigating whether linear kernel approximation has indistinguishable performance from the full kernel. The experiments were performed using the LBP feature representation presented in [7] and only the classification scheme differs. The results were surprising since the kernel map approximation was able to produce exactly the same results in terms of equal error rate (EER) as the truly non-linear SVM. However, from the receiver operating characteristic (ROC) curves, which can be seen in Fig. 4, we can notice some minor differences at lower false acceptance rates (FAR) which is a crucial operating point in high security applications. Otherwise, the ROC curves are almost the same, thus the kernel approximation is working also according to our experiments.

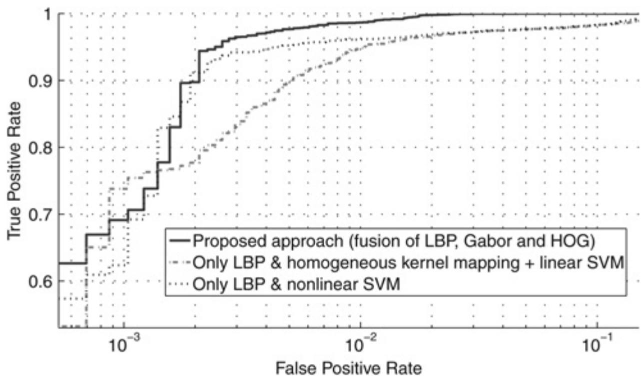

Fig. 4 *Performance (ROC curves) of the proposed approach, the linear LBP face representation using homogeneous kernel map and the non-linear LBP face representation used in [7]*

We performed also experiments to find out whether the combination of different features (LBP, Gabor wavelets and HOG) can improve the spoofing detection performance. Block size of 21 × 21 pixels was used for extracting HOG features and the weight of each individual matcher is inversely proportional to the corresponding EERs [25]. First, we wanted to see whether the LBP, Gabor wavelets and HOG descriptions are able to provide complementary information. The results of these experiments are shown in Fig. 5 and Table 1. From the ROC curves and EER values, it can be seen that the combination of all three features leads to best results. Table 2 presents a performance comparison between our proposed approach and the best results in [4, 5, 7] using the same protocol. The results are compared using EER and area under curve (AUC). The comparative results clearly assess the superiority of our approach (improvement in EER from 2.8 to 1.1% and in AUC from 0.995 to 0.999). The ROC curves of Fig. 4 indicate that the proposed approach is able to improve the performance even at a low FAR.

4.2 Experiments using liquid crystal display (LCD) spoofs

Yale Recaptured Database, proposed by Peixoto *et al.* [5], is composed of 640 real frontal faces from Yale Face Database B [26] (10 test subjects with 64 different illumination conditions) and 1920 LCD spoofs displaying the images from the Yale Face Database B on three LCD monitors, an LG Flatron L196WTQ Wide 19′, a CTL 171Lx 17′ TFT and a DELL Inspiron 1545 notebook. The recaptured images were taken with a Kodak C813 8.2 megapixels and a Samsung Omnia i900, with 5 megapixels. All images were cropped into greyscale images of 64 × 64 pixels. Examples of images from the database can be seen in Fig. 6.

Block size of 8 × 8 pixels was used for extracting HOG features and equal weights were assigned to the feature representations in matcher weighting as the bias of each classifier was not computed. All experiments have been performed using ten-fold cross-validation like in [5] a performance comparison can be seen in Table 3. The LBP representation [7] and the proposed approach outperform the best results reported in [5], the proposed approach yielding to perfect separation.

4.3 Evaluation on the Print-Attack Database

Print-Attack Database [6] was originally introduced within IJCB 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks [2]. The data set consists of 200 real client access and 200 print-attack (50 clients) videos which were captured in controlled and uncontrolled lighting conditions (with homogeneous and more complex background, respectively). The videos were recorded using a built-in webcam of a Macbook laptop at 25fps with resolution of 640 × 480 pixels. The print-attacks were generated by taking high-resolution photographs of each client under the same conditions as in their authentication sessions and the captured images were printed in colour on A4-sized paper. The spoofing attack attempts were performed with fixed or hand-held prints.

The database is divided into three sets, training, development and test data. The EER of development set is used for tuning the threshold which is applied for

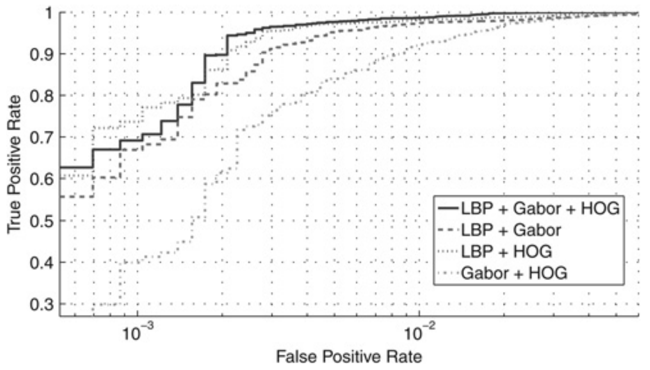

Fig. 5 *Performance (ROC curves) of the proposed approach and the different feature combinations*

Table 1 Performance comparison between the proposed approach and the different feature combinations

Method	AUC	EER, %
LBP + Gabor	0.998	2.0
LBP + HOG	0.999	1.5
Gabor + HOG	0.996	2.4
proposed approach	0.999	1.1

Table 2 Performance comparison between the proposed approach and the best results in [4], [5] and [7] on the NUAA Photograph Imposter Database [4]

Method	AUC	EER, %
Tan *et al.* [4]	0.94	—
Peixoto *et al.* [5]	0.966	8.2
LBP only [7]	0.995	2.8
proposed approach	0.999	1.1

discriminating the test samples. Table 4 summarises how the data set is split into the three separate sets. Clients have been randomly divided for each subset so that the identities do not overlap between the subsets, thus making the problem harder.

The Print-Attack Database differs from the previous two data sets as the provided data consist of videos of the whole authentication scene instead of segmented and normalised face images. Therefore OpenCV library implementation of the Viola–Jones algorithm [27] was used for face detection and the eye locations were retrieved using 2D Cascaded AdaBoost [28]. The face images were geometrically normalised according to the detected eye coordinates and cropped into greyscale images of 80 × 80 pixels. Examples of the geometrically normalised face images can be seen in Fig. 7. The spoofing detection is still performed from single face images because we want to use the same static image analysis-based spoofing detection scheme in all experiments, though the format of the provided data changes. However, the overlapping size of LBP blocks is now 17 pixels and the block size for extracting HOG features is 10 × 10 pixels. Here, we utilise the corresponding EER of each classifier on development set as weights like in [29] to allow each classifier more influence.

Table 5 shows a performance comparison between our proposed approach and the teams who participated in the IJCB 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks [2]. Almost all methods seem to work extremely well on the data set including our approach which is able to obtain perfect results on the test set and only two videos of the development set were incorrectly classified. It is worth mentioning that the proposed anti-spoofing measure is very robust although only a single image of the face area is considered. The other algorithms are either very complex, since multiple cues, for example, motion and texture analysis or even scene information, are fused together, or not too generic because the problem-specific solution works probably only on similar printing artefacts which are present in the provided data set.

5 Conclusions

Current face biometric systems are very vulnerable to spoofing attacks and photographs are probably the most common sources of spoofing attacks. Inspired by image quality assessment, characterisation of printing artefacts and by differences in light reflection, we proposed an approach for spoofing detection based on learning texture features and gradient structures from single images that discriminate live face images from fake ones. Our proposed face description used three enhanced feature histograms which encode the texture and gradient structures of the facial images. A homogeneous kernel map was applied on each resulting feature vector transforming the data into compact linear representation and reproducing an accurate approximation of the desired kernel function. This representation enables then to use fast linear SVM classifiers whose outputs are combined using matcher

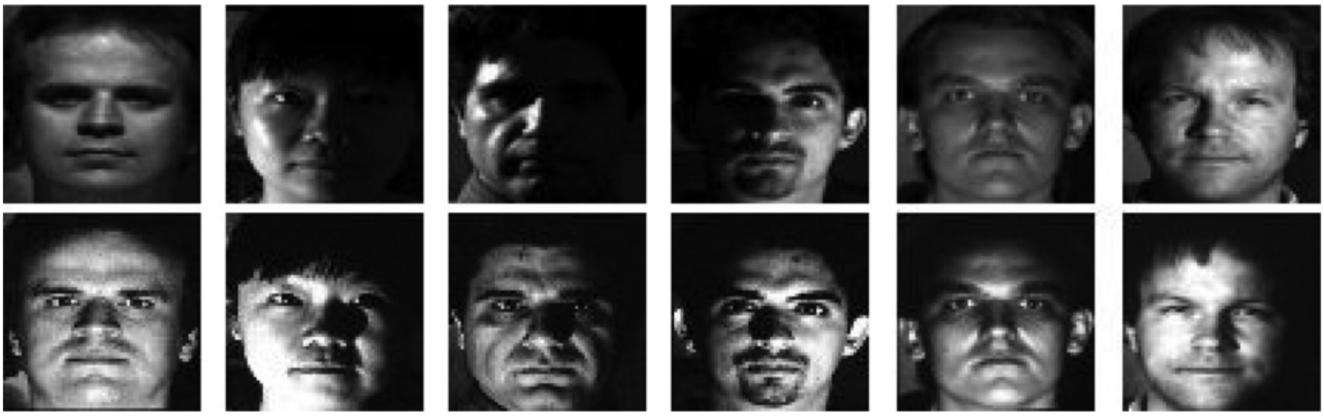

Fig. 6 *Example images from Yale Recaptured Database, real faces (upper row) and printed photos (lower row)*

doi: 10.1049/iet-bmt.2011.0009

Table 3 Performance comparison between the proposed approach and the best results in [5] and only LBP [7] on the Yale Recaptured Database [5]

	Min	Mean	Max	STD
Peixoto et al. [5]				
accuracy, %	89.0	91.7	93.8	1.4
true positive rate, %	83.3	85.8	87.7	1.4
false positive rate, %	0.0	2.5	5.4	1.5
LBP only [7]				
accuracy, %	98.4	99.6	100	0.5
true positive rate, %	98.4	99.2	100	0.8
false positive rate, %	0.0	0.2	1.6	0.5
Proposed approach				
accuracy, %	100	100	100	0.0
positive rate, %	100	100	100	0.0
false positive rate, %	0.0	0.0	0.0	0.0

Table 4 Decomposition of the Print-Attack Database

Type	Train	Development	Test	Total
real	60	60	80	200
attack	30 + 30	30 + 30	40 + 40	100 + 100
total	120	120	160	400

Numbers indicate how many videos are included in each subset (the sums indicate the amount of hand-based and fixed-support attacks)

weighting to give a final decision. Extensive experiments on three publicly available databases containing several real and fake faces showed excellent results. Compared to many previous works, our proposed approach is robust, computationally fast and does not require user cooperation. In addition, the texture features that are used for spoofing detection can also be used for face recognition. This provides a unique feature space for coupling spoofing detection and face recognition.

The current publicly available databases have been an important kick-off for finding out best practices for

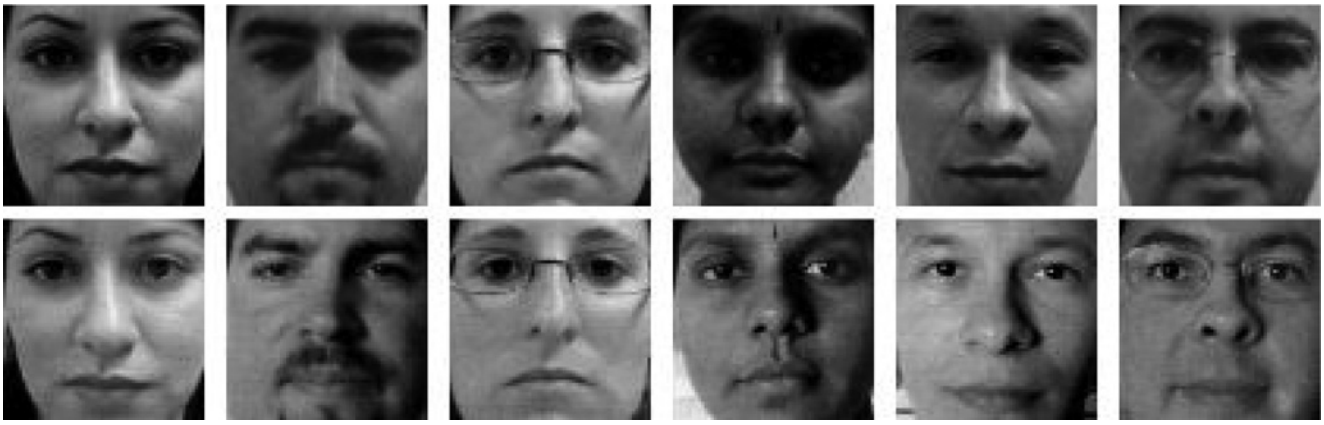

Fig. 7 *Examples of the geometrically normalised face images which were segmented from the videos provided in Print-Attack Database, real faces (upper row) and printed photos (lower row)*

Table 5 Performance comparison between the proposed approach and the teams who participated in the IJCB 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks [2]

Method	Development		Test		
	FAR	FRR	FAR	FRR	HTER
AMILAB	0.00	0.00	0.00	1.25	0.63
CASIA	1.67	1.67	0.00	0.00	0.00
IDIAP	0.00	0.00	0.00	0.00	0.00
SIANI	1.67	1.67	0.00	21.25	10.63
UNICAMP	1.67	1.67	1.25	0.00	0.00
UOULU	0.00	0.00	0.00	0.00	0.00
proposed approach	1.67	1.67	0.00	0.00	0.00

non-intrusive spoofing detection, since common data sets and protocols are provided for objective comparison. However, the excellent results suggest also that more complex databases with various types of high-quality spoofing attacks and proper protocol are needed for future development, since the current publicly available databases have their limitations, thus are not generalising the problem well enough. We believe that our approach can also be extended to detect spoofing attacks using masks or 3D models of the face because skin has a very particular texture with, for example, pores whereas fake faces have seldom such a level of detail.

6 Acknowledgments

This work has been performed within the TABULA RASA project 7th Framework Research Programme of the European Union (EU), grant agreement number 257289. The financial support of the Academy of Finland is also gratefully acknowledged.

7 References

1 Jain, A.K., Li, S.Z.: 'Handbook of face recognition' (Springer-Verlag, New York, Secaucus, NJ, 2011, 2nd edn.)

2 Chakka, M.M., Anjos, A., Marcel, S., *et al.*: 'Competition on counter measures to 2-d facial spoofing attacks'. Proc. IAPR IEEE Int. Joint Conf. on Biometrics (IJCB), Washington, DC, USA, 2011

3 Pan, G., Wu, Z., Sun, L.: 'Liveness detection for face recognition', in Delac, K., Grgic, M., Bartlett, M.S. (Eds.): 'Recent advances in face recognition', (IN-TECH, 2008), Ch. 9

4 Tan, X., Li, Y., Liu, J., Jiang, L.: 'Face liveness detection from a single image with sparse low rank bilinear discriminative model'. Proc. 11th European Conf. on Computer vision: Part VI. ECCV'10, 2010, pp. 504–517, available at http://portal.acm.org/citation.cfm?id=1888212.1888251

5 Peixoto, B., Michelassi, C., Rocha, A.: 'Face liveness detection under bad illumination conditions'. IEE Int. Conf. on Image Processing, 2011

6 Anjos, A., Marcel, S.: 'Counter-measures to photo attacks in face recognition: a public database and a baseline'. Proc. IAPR IEEE Int. Joint Conf. on Biometrics (IJCB), Washington, DC, USA, 2011

7 Määttä, J., Hadid, A., Pietikäinen, M.: 'Face spoofing detection from single images using micro-texture analysis'. Proc. IAPR IEEE Int. Joint Conf. on Biometrics (IJCB), Washington, DC, USA, 2011

8 Manjunath, B.S., Ma, W.Y.: 'Texture features for browsing and retrieval of image Data', *IEEE Trans. Pattern Anal. Mach. Intell.*, 1996, **18**, pp. 837–842, available at http://dx.doi.org/10.1109/34.531803

9 Dalal, N., Triggs, B.: 'Histograms of oriented gradients for human detection'. Int. Conf. on Computer Vision & Pattern Recognition, 2005, vol. 2, pp. 886–893

10 Vedaldi, A., Zisserman, A.: 'Efficient additive kernels via explicit feature maps'. Proc. IEEE Conf. on Computer Vision and Pattern Recognition, 2010

11 Vapnik, V.N.: 'Statistical learning theory' (Wiley-Interscience, 1998)

12 Nixon, K., Aimale, V., Rowe, R.: 'Spoof detection schemes', in 'Handbook of biometrics', (2008), pp. 403–423

13 Kollreider, K., Fronthaler, H., Bigun, J.: 'Non-intrusive liveness detection by face images', *Image Vis. Comput.*, 2009, **27**, pp. 233–244

14 Bao, W., Li, H., Li, N., Jiang, W.: 'A liveness detection method for face recognition based on optical flow field'. IEEE 2009 Int. Conf. on Image Analysis and Signal Processing, 2009, pp. 233–236

15 Li, J., Wang, Y., Tan, T., Jain, A.K.: 'Live face detection based on the analysis of Fourier spectra', in 'Biometric technology for human identification', (2004), pp. 296–303

16 Zhang, Z., Yi, D., Lei, Z., Li, S.Z.: 'Face liveness detection by learning multispectral reflectance distributions'. Int. Conf. on Face and Gesture, 2011, pp. 436–441

17 Pavlidis, I., Symosek, P.: 'The Imaging Issue in an automatic face/disguise detection system'. Proc. IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications (CVBVS 2000), 2000, p. 15, available at http://dl.acm.org/citation.cfm?id=518905.795366

18 Sun, L., Huang, W., Wu, M.: 'TIR/VIS correlation for liveness detection in face recognition'. Proc. 14th Int. Conf. on Computer Analysis of Images and Patterns – Volume Part II. CAIP'11, 2011, pp. 114–121, available at http://dl.acm.org/citation.cfm?id=2044575.2044590

19 Bai, J., Ng, T.T., Gao, X., Shi, Y.Q.: 'Is physics-based liveness detection truly possible with a single image?'. IEEE Int. Symp. on Circuits and Systems (ISCAS), 2010, pp. 3425–3428

20 Gao, X., Ng, T.T., Qiu, B., Chang, S.F.: 'Single-view recaptured image detection based on physics-based features'. IEEE Int. Conf. on Multimedia & Expo (ICME), 2010, pp. 1469–1474

21 Eid, A.H., Ahmed, M.N., Cooper, B.E., Rippetoe, E.E.: 'Characterization of electrophotographic print artifacts: banding, jitter, and ghosting', *IEEE Trans. Image Process.*, 2011, **20**, pp. 1313–1326

22 Ojala, T., Pietikäinen, M., Mäenpää, T.: 'Multiresolution gray-scale and rotation invariant texture classification with local binary patterns', *IEEE Trans. Pattern Anal. Mach. Intell.*, 2002, **24**, pp. 971–987, available at http://portal.acm.org/citation.cfm?id=628329.628808

23 Fan, R.E., Chang, K.W., Hsieh, C.J., Wang, X.R., Lin, C.J.: 'LIBLINEAR: a library for large linear classification', *J. Mach. Learn. Res.*, 2008, **9**, pp. 1871–1874

24 Vedaldi, A., Fulkerson, B.: 'VLFeat: an open and portable library of computer vision algorithms', 2008, http://www.vlfeat.org/

25 Snelick, R., Uludag, U., Mink, A., Indovina, M., Jain, A.: 'Large scale evaluation of multimodal biometric authentication using state-of-the-art systems', *IEEE Trans. Pattern Anal. Mach. Intell.*, 2005, **27**, pp. 450–455

26 Georghiades, A.S., Belhumeur, P.N., Kriegman, D.J.: 'From few to many: illumination cone models for face recognition under variable lighting and pose', *IEEE Trans. Pattern Anal. Mach. Intell.*, 2001, **23**, pp. 643–660

27 Viola, P.A., Jones, M.J.: 'Rapid object detection using a boosted cascade of simple features'. Proc. IEEE Conf. on Computer Vision and Pattern Recognition, 2001, pp. 511–518

28 Niu, Z., Shan, S., Yan, S., Chen, X., Gao, W.: '2D cascaded adaboost for eye localization'. Proc. 18th Int. Conf. on Pattern Recognition, 2006

29 Wang, Y., Tan, T., Jain, A.K.: 'Combining face and iris biometrics for identity verification'. Proc. fourth Int. Conf. on Audio- and Video-Based Biometric Person Authentication. AVBPA'03, 2003, pp. 805–813, available at http://dl.acm.org/citation.cfm?id=1762222.1762327

doi: 10.1049/iet-bmt.2011.0009