Face Spoofing Detection From Single Images Using Micro-Texture Analysis

Jukka Määttä, Abdenour Hadid, Matti Pietikäinen
Machine Vision Group, University of Oulu, Finland
{jukmaatt,hadid,mkp}@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, characterization of printing artifacts, and differences in light reflection, we 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 features. Hence, we present a novel approach based on analyzing facial image textures for detecting whether there is a live person in front of the camera or a face print. The proposed approach analyzes the texture of the facial images using multi-scale local binary patterns (LBP). 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. Extensive experimental analysis on a publicly available database showed excellent results compared to existing works.

1. Introduction

Despite the great deal of progress during the recent years [4], 2D face biometrics (that is identifying individuals based on their 2D face information) is still a major area of research. Wide range of viewpoints, occlusions, aging of subjects and complex outdoor lighting are challenges in face recognition. While 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.

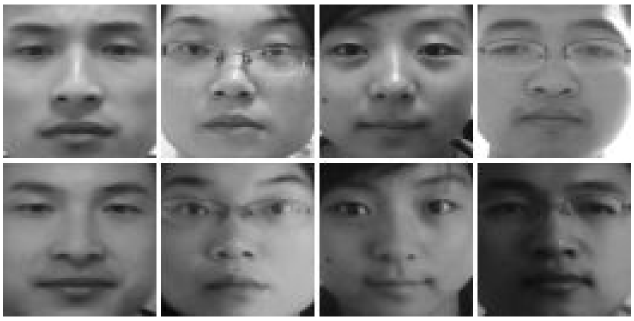

Figure 1. Example of images captured from real faces (upper row) and from printed photos (lower row). The appearance similarity illustrates the difficulty of spoofing detection from printed photos.

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. While 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.

Typical countermeasure against spoofing is liveness de-

978-1-4577-1359-0/11/$26.00 ©2011 IEEE

tection 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, multimodal systems are intrinsically more difficult 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, characterization of printing artifacts and by differences in light reflection, we 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 micro-texture patterns. Furthermore, 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. This may cause different specular reflections and shades. The surface properties of real faces and prints, e.g. pigments, are also different. Hence, we present a novel approach based on analyzing facial image textures 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, 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 proposed approach analyzes the texture of the facial images using multi-scale local binary patterns (LBP) [9] and encodes the micro-texture patterns into an enhanced feature histogram [1]. The results are then fed to a support vector machine (SVM) [13] classifier which determines whether there is a live person in front of the camera or not. Extensive experiments on a publicly available database (NUAA Photograph Imposter Database [12]) containing several real and fake faces showed excellent results compared to previous works.

The rest of the paper is organized as follows. Section 2 discusses related works on face spoofing attacks and countermeasures. Our proposed approach, using multi-scale local binary patterns and SVM, is then described in Section 3 and evaluated in Section 4, where extensive experiments are conducted. The results are thoroughly analyzed and also compared to 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. 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 [11, 8]. 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. For instance, Pan *et al.* [11] exploited the observation that humans blink once every 2-4 seconds and proposed an eye blink-based anti-spoofing method. It uses Conditional Random Field framework to model and detect eye-blinking. Kollreider *et al.* [5] 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 [2], 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.* [6] described a method for detecting print-attack face spoofing. The method is 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.* [12] 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 (DoG) 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 [14].

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). We therefore propose in this work a computationally very fast approach based on highly discriminative micro-texture features, using conventional images and requiring no user-cooperation.

3. Spoofing Detection using Micro-Texture 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 vs. 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 emphasizes 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. This may cause different specular reflections and shades. The surface properties of real faces and prints, e.g. pigments, are also different. In addition, face prints usually contain printing quality defects that can be detected with micro-texture patterns. Furthermore, spoof attacks when executed with face prints tend to engender some overall image blur.

Inspired by the observations above, and particularly by image quality assessment and characterization of printing artifacts, 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 approch is emphasizing the micro-texture differences in the feature space.

Our method adopts the local binary patterns [9], a powerful texture operator, for describing not only the micro-textures but also their spatial information. The vectors in the feature space are then fed to an SVM classifier which determines whether the micro-texture patterns characterize a live person or a fake image. Fig. 2 shows examples of two images (a live face and a face print) in the original space and the corresponding LBP images (using basic LBP as feature space). We can notice that the printed photo looks quite similar to the image of the live face whereas the LBP images depict some differences. We describe below our enhanced LBP feature space.

3.1. Discriminative Feature Space Using LBP

The LBP texture analysis operator, introduced by Ojala et al. [9], is defined as a gray-scale invariant texture measure, derived from a general definition of texture in a local neighborhood. 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 gray-scale changes.

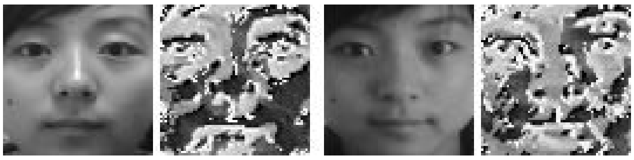

Figure 2. Examples of two images (a live face and a face print) in the original space and the corresponding LBP images using basic LBP as a feature space.

The original LBP operator forms labels for the image pixels by thresholding the 3×3 neighborhood of each pixel with the center value and considering the result as a binary number. Fig. 3 shows an example of an LBP calculation. The histogram of these $2^8 = 256$ different labels can then be used as a texture descriptor.

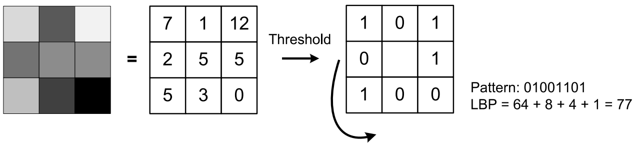

Figure 3. The basic LBP operator.

The operator has been extended to use neighborhoods of different sizes. Using a circular neighborhood and bilinearly interpolating values at non-integer pixel coordinates allow any radius and number of pixels in the neighborhood. The notation (P, R) is generally used for pixel neighborhoods to refer to P sampling points on a circle of radius R. The calculation of the LBP codes can be easily done in a single scan through the image. The value of the LBP code of a pixel (x_c, y_c) is given by:

$$\mathrm{LBP}_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p, \tag{1}$$

where g_c corresponds to the gray value of the center pixel (x_c, y_c), g_p refers to gray values of P equally spaced pixels on a circle of radius R, and s defines a thresholding function as follows:

$$s(x) = \begin{cases} 1, & \text{if } x \geq 0; \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

Another extension to the original operator is the definition of so called **uniform patterns**. This extension was inspired by the fact that some binary patterns occur more commonly in texture images than others. A local binary pattern is called uniform if the binary pattern contains at most two bitwise transitions from 0 to 1 or vice versa when the bit

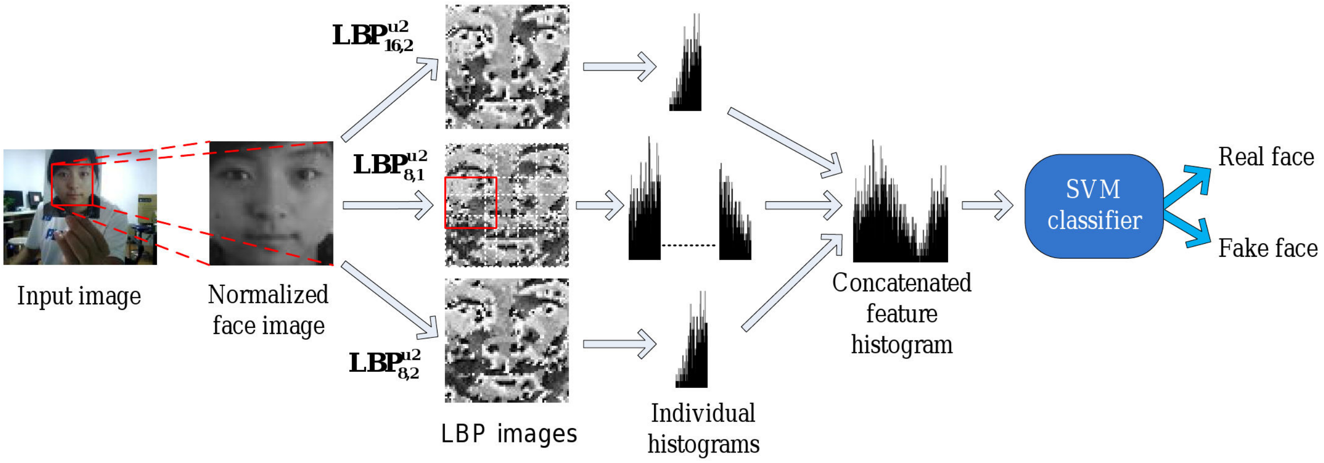
$\mathbf{LBP}^{u2}_{16,2}$
$\mathbf{LBP}^{u2}_{8,1}$
$\mathbf{LBP}^{u2}_{8,2}$
Input image
Normalized face image
LBP images
Individual histograms
Concatenated feature histogram
SVM classifier
Real face
Fake face

Figure 4. The proposed approach. The face is first detected, cropped and normalized into a 64×64 pixel image. Then, we apply $LBP^{u2}_{8,1}$ operator on the normalized face image and divide the resulting LBP face image into 3×3 overlapping regions. The local 59-bin histograms from each region are computed and collected into a single 531-bin histogram. Then, we compute two other histograms from the whole face image using $LBP^{u2}_{8,2}$ and $LBP^{u2}_{16,2}$ operators, yielding 59-bin and 243-bin histograms that are added to the 531-bin histogram previously computed. Finally, we use a nonlinear SVM classifier with radial basis function kernel for determining whether the input image corresponds to a live face or not.

pattern is traversed circularly. In the computation of the LBP labels, uniform patterns are used so that there is a separate label for each uniform pattern and all the non-uniform patterns are labeled with a single label. This yields to the following notation for the LBP operator: $\text{LBP}^{u2}_{P,R}$. The subscript represents using the operator in a (P, R) neighborhood. Superscript $u2$ stands for using only uniform patterns and labeling all remaining patterns with a single label (see [9] for details).

Each LBP label (or code) can be regarded as a micro-texton. Local primitives which are codified by these labels include different types of curved edges, spots, flat areas etc. The occurrences of the LBP codes in the image are usually collected into a histogram. The classification can be then performed by computing histogram similarities. For an efficient representation, facial images are first divided into several local regions from which LBP histograms are extracted and concatenated into an enhanced feature histogram. Such a representation is shown to be very adequate for face recognition [1]. Our investigations have shown, however, that micro-texture details that are needed for discriminating a real human face from fake ones, can best be detected using a combination of different LBP operators. Therefore, to better capture the differences between real human faces and fake ones, we derive an enhanced facial representation using multi-scale LBP operators. The proposed representation is depicted in Fig. 4.

As illustrated in Fig. 4, our proposed representation computes LBP features from 3×3 overlapping regions to capture the spatial information and enhances the holistic description by including global LBP histograms computed over the whole face image. This is done as follows: the face is first detected, cropped and normalized into a 64×64 pixel image. Then, we apply $LBP^{u2}_{8,1}$ operator on the normalized face image and divide the resulting LBP face image into 3×3 overlapping regions (with an overlapping size of 14 pixels). The local 59-bin histograms from each region are computed and collected into a single 531-bin histogram. Then, we compute two other histograms from the whole face image using $LBP^{u2}_{8,2}$ and $LBP^{u2}_{16,2}$ operators, yielding 59-bin and 243-bin histograms that are added to the 531-bin histogram previously computed. Hence, the length of the final enhanced feature histogram is 833 (i.e. 531+59+243).

3.2. Classification

Once the enhanced histograms are computed, we use a nonlinear SVM classifier with radial basis function kernel [13] for determining whether the input image corresponds to a live face or not. The SVM classifier is first trained using a set of positive (real faces) and negative (fake faces) samples.

4. Experimental Analysis

4.1. Experimental Data

For performance evaluation, we considered the publicly available NUAA Photograph Imposter Database [12] which contains images of both real client accesses and photo attacks. The face images of live humans and their photographs were collected in three sessions at intervals of about two 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 client accesses and spoofing attacks were recorded using a video camera at 20fps. There are 500 images for each subject's recording. When capturing the data, the main idea was to make the live subjects look like a static as much as possible by minimizing the movements and the eye-blinking. In contrast, five different vivid photo-attacks were simulated using 2D facial prints with varying motions. The database is composed of real-accesses and attacks to 15 subjects using both photo-quality and laser-quality prints. The images are captured using conventional webcams with resolution of 640 × 480 pixels.

Performing the experimental evaluation on this publically available database will not only allow us to fairly compare our results against those of *Tan et al.* [12] but will also allow other researchers to compare their results against ours.

4.2. Setup

The images of the 15 subjects (in three sessions for most of the subjects) in the database are divided into two separate sets for training and test purposes. The training set consists of images from the first two sessions only. The test set consists of the images from the remaining third session. The training set contains altogether 1743 face images of 9 real clients (889 and 854 from the first and the second sessions, respectively) and 1748 imposter images of the same 9 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. The considered face images were geometrically normalized into images of 64 × 64 pixels.

4.3. Experimental Results

We started by evaluating the performance of three powerful texture operators, namely LBP, Local Phase Quantization (LPQ) [10] and Gabor wavelets [7] in discriminating real faces from fake ones (i.e. faces captured from prints). The three operators are applied to the whole facial area (i.e. without block division). The computed features are fed to SVM classifiers. For fair comparison, optimal SVM parameters are determined and used for each texture descriptor. LibSVM Library [3] is used for SVM implementation in all experiments. The performance of the three texture operators in terms of Receiver Operating Characteristic (ROC) curves are shown in Fig. 5. From the results, we can notice that the three descriptors performed quite well. The equal error rates (EER), shown in Table 1, indicate that LBP (EER= 2.9%) and LPQ (EER= 4.6%) performed almost equally well, outperforming Gabor wavelets (EER= 9.5%). The good performance of LPQ can be explained by the fact that many images (especially those captured from prints) contain some amount of blur whereas the LPQ operator is blur-tolerant [10].

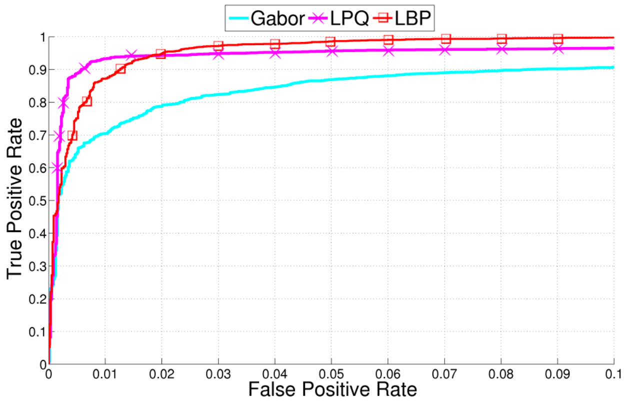

Figure 5. Performance (ROC curves) of three texture operators (LBP, LPQ and Gabor) in discriminating live face images from fake ones.

Descriptor	LBP	LPQ	Gabor
Error Equal Rate (EER)	**2.9 %**	**4.6 %**	**9.5 %**

Table 1. Performance (Error Equal Rates) of three texture operators (LBP, LPQ and Gabor) in discriminating live face images from fake ones.

Although the basic LBP operator applied to the whole image performs relatively well, our investigations have however shown that fine details that are needed for discriminating real human face images from fake ones are best detected using a combination of LBP operators as described in our proposed approach depicted in Fig. 4. One major difference between real faces and the fake ones is that the 2D prints can possibly contain specular reflections which are typical on planar objects but not on 3D faces. In addition, the print defects can be more easily found locally, e.g. on uniform surfaces like cheeks. Some examples of typical characteristics of real faces and face prints can be seen in Fig. 6. These fine details that can be used for detecting facial prints might be lost if only a single LBP histogram of the face is used.

Table 2 presents a performance comparison between our proposed approach and the best results from Tan et al. [12] on the same database and using the same protocol. For fair comparison, we also report our results in terms of Area under Curve (AUC) as Tan et al. did in their paper [12]. The comparative results clearly assess the superiority of our approach (0.99 versus 0.94). Our method was able to achieve almost perfect spoofing detection, yielding total classification accuracy of 98.0%, false acceptance rate of 0.6% and

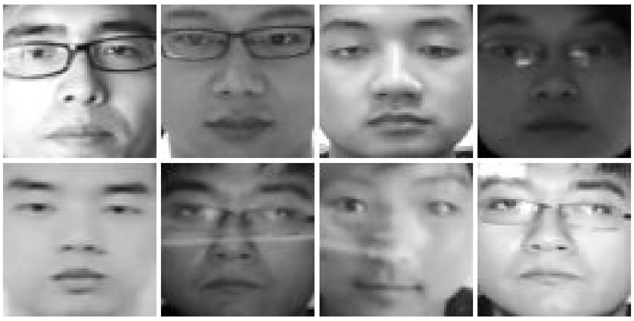

Figure 6. Typical characteristics of real client images (upper row) and 2D facial prints (lower row), showing examples of details that can be exploited for discriminating real human face from fake ones.

Method	Tan et al. [12]	Our approach
AUC	**0.94**	**0.99**

Table 2. Performance comparison between our proposed approach and the best results in [12] on the same database and using the same protocol.

false rejection rate of 4.4%. A closer look at the samples that were misclassified revealed that the misclassified samples mainly consist of over-exposed and very blurry images of client faces that are labeled by our approach as 2D prints. Fig. 7 shows some of such misclassified cases.

Our proposed representation considers multi-scale LBP and computes features from 3 × 3 overlapping regions to capture the spatial information and enhances the holistic description by including global LBP histograms computed over the whole face image. To gain insight into the importance of using multi-scale LBP, overlapping blocks, and combination of local and holistic descriptions, we performed a set of experiments evaluating the impact of these choices. The results are shown in Fig. 8. It can be seen that the block processing methodology significantly improves the performance at lower false acceptance rates, e.g. from 54.0% to 89.0% at 0.2% FAR using overlapping regions. Furthermore, the combination of global and local representations achieves even better results, e.g. 91.2% at 0.2% FAR using the fusion of overlapping regions and multiscale LBP on the whole face area. In addition, we performed experiments on overlapping and non-overlapping block divisions using different block sizes. We noticed that larger block sizes lead to better results with both spatial division strategies. Furthermore, as shown in Fig. 8, the use of overlapping regions yields significantly better performance at lower false acceptance rates.

We have also evaluated our proposed anti-spoofing solution in a real world-environment by incorporating the anti-spoofing module into an access control system based on face recognition. We performed various 2D face spoofing attacks using good quality face prints and also high resolution displays. The system detected most of the spoofing attempts. The spoofing detection module takes only about 16.5ms in average to process an image on a 2.4 GHz Intel Core 2 Duo CPU with 3 GB of RAM using un-optimized C++ code.

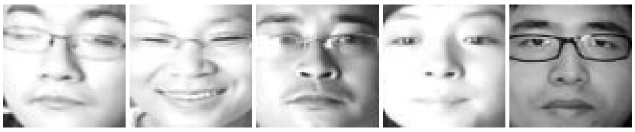

Figure 7. Examples of misclassified images. The first four images from the left are from rejected clients and one on the right is a photograph.

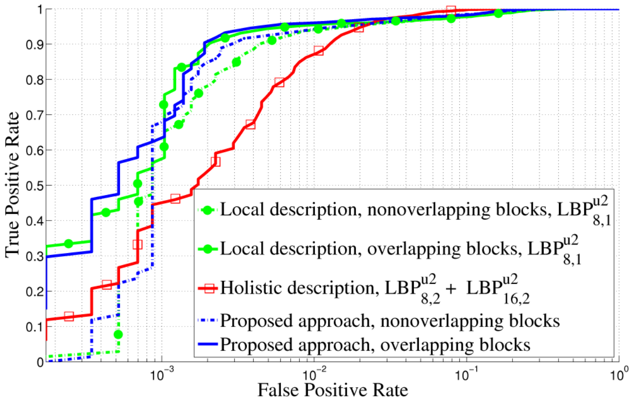

Figure 8. Performance analysis on the importance of using multi-scale LBP, overlapping blocks, and feature computation from the whole images.

5. Conclusion

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, characterization of printing artifacts and by differences in light reflection, we proposed an approach for spoofing detection based on learning the micro-texture patterns that discriminate live face images from fake ones. Indeed, face prints usually contain printing quality defects that can be well detected using micro-texture patterns. Furthermore, 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. This may cause different specular reflections and shades. The surface properties of real faces and prints, e.g. pigments, are also different. Our proposed approach used multi-scale local binary patterns (LBP) to encode the micro-texture patterns into an enhanced feature histogram. The results are then fed to a support vector machine classifier which determines whether there is a live person in front of the camera or not. Extensive experiments on a publicly available database 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.

We have also evaluated our approach in a real world application (face based access control) by performing various 2D face spoofing attacks using good quality face prints and also high resolution displays. The results were promising. 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.

Acknowledgment

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.

References

[1] T. Ahonen, A. Hadid, and M. Pietikäinen. Face description with local binary patterns: Application to face recognition. *IEEE Trans. Pattern Anal. Mach. Intell.*, 28:2037–2041, December 2006. 2, 4

[2] 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. 2

[3] C.-C. Chang and C.-J. Lin. LIBSVM: A library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, 2:27:1–27:27, 2011. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm. 5

[4] A. K. Jain and S. Z. Li. *Handbook of Face Recognition*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2005. 1

[5] K. Kollreider, H. Fronthaler, and J. Bigun. Non-intrusive liveness detection by face images. *Image and Vision Computing*, 27:233–244, 2009. 2

[6] 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. 2

[7] B. S. Manjunath and W. Y. Ma. Texture features for browsing and retrieval of image data. *IEEE Trans. Pattern Anal. Mach. Intell.*, 18:837–842, August 1996. 5

[8] K. Nixon, V. Aimale, and R. Rowe. Spoof detection schemes. In *Handbook of Biometrics*, pages 403–4239. 2008. 2

[9] T. Ojala, M. Pietikäinen, and T. Mäenpää. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Trans. Pattern Anal. Mach. Intell.*, 24:971–987, July 2002. 2, 3, 4

[10] V. Ojansivu and J. Heikkilä. Blur insensitive texture classification using local phase quantization. In *Proceedings of the 3rd international conference on Image and Signal Processing*, ICISP '08, pages 236–243, Berlin, Heidelberg, 2008. Springer-Verlag. 5

[11] 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. 2

[12] X. Tan, Y. Li, J. Liu, and L. Jiang. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In *Proceedings of the 11th European conference on Computer vision: Part VI*, ECCV'10, pages 504–517, Berlin, Heidelberg, 2010. Springer-Verlag. 2, 4, 5, 6

[13] V. N. Vapnik. *Statistical Learning Theory*. Wiley-Interscience, 1998. 2, 4

[14] 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. 2