Classification of Captured and Recaptured Images to Detect Photograph Spoofing

Neslihan Kose¹, Jean-Luc Dugelay ²

Multi Media Department, EURECOM 2229 Route des Cretes, 06560, Sophia-Antipolis, France

¹ Neslihan.Kose@eurecom.fr, ² Jean-Luc.Dugelay@eurecom.fr

Abstract—In this paper, a new face anti-spoofing approach, which is based on analysis of contrast and texture characteristics of captured and recaptured images, is proposed to detect photograph spoofing. Since photo image is a recaptured image, it may show quite different contrast and texture characteristics when compared to a real face image. In a spoofing attempt, image rotation is quite possible. Therefore, in this paper, a rotation invariant local binary pattern variance (LBPV) based method is selected to be used. The approach is tested on the publicly available NUAA photo-impostor database, which is constructed under illumination and place change. The results show that the approach is competitive with other existing methods tested on the same database. It is especially useful for conditions when photos are held by hand to spoof the system. Since an LBPV based method is used, it is robust to illumination changes. It is non-intrusive and simple.

I. INTRODUCTION

It has been shown that face recognition techniques are vulnerable to spoofing attacks. In a spoofing attempt, a person tries to masquerade as another person and thereby, tries to gain an access to the system. Numerous recognition approaches have been presented in face recognition topic, however the studies on face anti-spoofing methods are still very limited. Therefore, nowadays anti-spoofing is a popular topic for researchers to fill this gap. Aim is to develop non-intrusive methods without extra devices and human involvement. In this way they can be integrated into existing face recognition systems. Also, methods which are robust to pose and illumination changes are preferable.

A. Related Work

Various approaches have been developed on face photo spoofing detection. The existing techniques mainly concentrate on depth analysis and motion detection in case analyses are not restricted to a single image. Depth map analysis approaches rely on the fact that even when there is motion, depth map is plane for photos; whereas it varies in case of live faces. In [1], spoofing is detected by analyzing this depth map. Spoofing can also be detected by analyzing the frequency spectrum of a live face [2, 3]. In [3], it is assumed that the high frequency components of photos are less than those of live face images. However, this method gives good results when photo images have low definition and small size as it is stated in [2]. Eye-blinking as anti-spoofing measure against presented photos is also another approach. There are various methods for eye-blink detection. In [4], statistical models are used for this detection. However, since liveness is detected by recognizing spontaneous eye blinks, again analysis requires several images among time.

In this paper, an approach, which is based on contrast and texture analysis of captured and recaptured images, is proposed to detect face photograph spoofing. A good survey of approaches against photograph spoof can be found in [5]. Each face anti-spoofing technique differs from each other in terms of the need for data quality, additional hardware, and user collaboration. In our approach, a rotation invariant LBP variance (LBPV) based method together with a pre-processing step of Difference of Gaussian (DoG) filtering is used to detect photograph spoofing. This method relies on a single image. Only a generic webcam is used, hence there is also no need for extra hardware and user collaboration.

LBP algorithm is a popular approach especially in texture classification. LBP has been used in various types of studies. Spoofing detection is also one of them. There are studies which use different types of LBP for iris and fingerprint spoofing detection [6-9]. In this study, a LBPV based method is used for face spoofing detection. To the best of our knowledge, it is the first time that an LBPV based approach, is used for face spoofing detection. In this paper, it is verified that the proposed approach provides satisfactory results for photograph spoofing detection. It is known that there are also other types of face spoofing attacks such as video and mask attacks. Since the proposed approach relies on different texture and contrast characteristics of real face and fake face, and video and mask attacks have also different texture and contrast characteristics when compared to a real face; the proposed method can even be used for detection of video and mask attacks by analyzing texture and contrast characteristics of real and fake faces.

The paper is organized as follows: Section II describes the proposed approach, in which the specifications of DoG filter are presented first. Next, the classification problem of captured and recaptured images using a LBPV based algorithm is explained. Finally, the specifications of the selected NUAA photograph database [2] are given. Section III gives the experimental results. Conclusions are provided in Section IV.

II. PROPOSED APPROACH

The proposed approach relies on different contrast and texture characteristics of captured images and recaptured images to detect photograph spoofing.

In the proposed approach, initially a DoG filter is used to obtain a special frequency band which gives considerable information to discriminate between real and photo images. In [2], DoG features are used for
liveness detection and satisfactory results are reported. In this study, DoG filtering is used as the pre-processing step, and LBPV based method is used for feature extraction in the main part. As it is shown in ‘Experimental Results’ of this paper, the results are improved when compared to the method in [2] where only DoG features are used. Fig. 1 shows the flow chart of the approach. In this study, the problem is simply a classification problem with two classes. First class is the real image class, which are in fact captured face images, and second class is the class of photograph images of real faces. Since the image of a photo is an image of a real face which passes through the camera system twice and the printing system once, it is in fact a recaptured image which has lower image quality compared to a real face image taken under same imaging conditions.

A rotation invariant LBPV based method [10] is used for feature extraction in our approach. LBP [11] is one of the most popular texture analysis approaches, which characterizes the spatial structure of the local image texture. Texture can be characterized by a spatial structure (e.g. LBP), which varies with rotation, and the contrast (e.g variance of local image texture), which does not vary with rotation [10]. The LBPV is a combination of the spatial structure and the contrast. LBP and LBPV can also provide local rotation invariant classification, but they have the drawback of losing global spatial information. However, when LBPV is used with global matching as it is proposed in [10], global spatial information is not lost, and hence more accurate results are obtained. This claim is verified in [10] by testing the method on different textures. In our approach, initially rotation variant LBPV histograms are obtained. Then distances from each test image to images in the client and impostor model sets are computed applying matching by exhaustive search. For each test image, quadratic means of distances are computed for both client set and impostor set, consecutively. Finally, images are classified in the nearest class by comparing client and impostor quadratic mean results.

A. Pre-Processing Part of the Proposed Approach

Recaptured face image has less sharpness (lower image quality) when compared to captured face image; therefore recaptured image contains less high frequency components [2, 3]. This fact can be observed by analysing the 2D Fourier spectra of real face and photo face images.

DoG filtering is used to remove noise while preserving the high frequency components, which are especially the image edges. In this approach, instead of analysing all high frequency bands, the high-middle band frequency spectrum is analysed. For the DoG filter, a quite narrow Gaussian (σ₀ = 0.5) is formed without introducing noise. To filter out misleading low spatial frequency information, σ₁ = 2 is selected for the outer Gaussian. This pre-processing technique helps to remove misleading information and noise; hence we can focus on the part of the spectrum which provides fundamental information to discriminate between captured and recaptured face images.

The effect of applying DoG filtering as the pre-processing step in the proposed approach is also verified in the ‘Experimental Results’ of Section III. The results show that applying DoG filtering as the pre-processing step improves the recaptured image detection rate.

\[ LBP_{p,r} = \sum_{p=0}^{P-1} s(g_p - g_c)2^p, \]  
\[ s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \]  

\[ LBP_{p,r} \] is computed such that for a given central pixel in an image, a pattern number is computed by comparing its value with those of its neighbours. In Equation (1), \( g_c \) is the gray value of the central pixel, \( g_p \) is the value of its neighbours, \( P \) is the number of neighbours around a circle of radius \( R \).

To obtain LBPV histogram of an \( X \times Y \) image, the LBP pattern of each pixel \((i,j)\) is used in calculation.

\[ H(k) = \sum_{i,j} f(LBP_{p,r}(i,j), k), \quad k = [0 \ K] \]  
\[ f(x, y) = \begin{cases} 1 & x = y \\ 0 & \text{else} \end{cases} \]  

\( K \) is the maximal LBP pattern value in (3). In this histogram, each LBP pattern has weighting factor of 1. LBPV algorithm is used to add contrast information to this histogram. Variance is computed for the P sampling points around a circle of radius \( R \) using Eqs. (5) and (6).

\[ Var_{p,r} = \frac{1}{P} \sum_{p=0}^{P-1} (g_p - w)^2 \]
The LBPV computes the variance from a local region and accumulates it into the LBP bin as the weighting factors [10]. LBPV histogram is calculated using Eqs. (7) and (8).

\[
LBPV_{p,r}(k) = \sum_{i} \sum_{j} w(LBP_{p,r}(i,j), k), \quad k = [0 \ K]
\]  

(7)

\[
w(LBP_{p,r}(i,j), k) = \begin{cases} \text{var}_{p,r}(i,j) & \text{if } LBP_{p,r}(i,j) = k \\ 0 & \text{else} \end{cases}
\]  

(8)

The representations of two different selections for P and R values are shown in Fig. 2. When P and R values are increased, even better results are obtained; however with a cost of increasing computational complexity as stated in [10]. In the proposed approach, P and R values are selected as P = 8, R = 1, due to this computational complexity.

\[
u = 1/P \sum_{p=0}^{P} g_{p}
\]  

(6)

In our study, this global matching is implemented using exhaustive search scheme [10] to find the minimal distance in all candidate orientations, which is a simple method. The LBPV histogram is reorganized and represented by a rotation variant histogram $H^v$, and a rotation invariant histogram $H^i$. Then for two texture images, the matching distance is calculated as shown in Eq (10).

\[
D_{ri}(H^i_s, H^i_u) = D_{ri}(H^v_s, H^v_u) + D_{min}(H^v_s, H^v_u)
\]

\[
D_{ri}(H^v_s, H^v_u) = D(O_s, O_u)
\]

(10)

In (10), $D(X,Y)$ represents chi-square distance defined in (11). $H_s$ is the test sample image and $H_u$ is the model image histograms. $\overrightarrow{H^v(j)}$ is the new matrix which is obtained by shifting j columns of original $H^v$ matrix. From equation (10), it is clear that distance between two histograms is composed of two parts. $D_{ri}(H^v_s, H^v_u)$, is derived from rotation invariant part and the other one, $D_{min}(H^v_s, H^v_u)$, is obtained by searching minimal distance within rotation variant part. Matching by exhaustive search is explained in [10, 12] with more details.

In the proposed approach, chi-square distance is selected to be used as the dissimilarity metric, since for LBP based algorithms, it is recommended as dissimilarity metric in various studies [10, 13, 14].

Fig. 3. Different photo-attacks are shown from column (1) to column (5): (1) move the photo horizontally, vertically, back and front; (2) rotate the photo in depth along the vertical axis; (3) the same as (2) but along the horizontal axis; (4) bend the photo inward and outward along the vertical axis; (5) the same as (4) but along the horizontal axis. Fig. is taken from [2].
Chi-square distance between sample and model histograms is computed as

$$D(S, M) = \sum_{i=1}^{N} \frac{(S_i - M_i)^2}{S_i + M_i}$$

(11)

N is the number of bins and $S_i$ and $M_i$ are, respectively, the values of the sample and model histograms at the $i^{th}$ bin. For each test image, matching by exhaustive search is applied using chi-square distance metric, and distances from each test sample to all samples ($x_i$) in the client and impostor model sets are obtained. Then, quadratic means of distances are computed for client and impostor model sets, consecutively, using (12). In (12), N is the number of images in the model set and $x_i$ is the distance between test sample and model sample as shown in Fig. 4.

$$QMSD = \sqrt[2]{\frac{1}{N} \sum_{i=1}^{N} (x_i)^2}$$

(12)

Finally, each test image is classified in the nearest class by comparing the two quadratic mean values, which are obtained for client and impostor sets.

C. Selected Database

This part provides the basic specifications of the selected NUAA impostor database [2]. There are only a few number of publicly available photo impostor databases. NUAA is one of them. It is constructed by using a generic webcam. Fig. 5 shows the live and photo images in different sessions. Place and illumination condition of each session is different. Test and training sets are constructed from different sessions. The database involves 15 subjects. In each session, the images of both live subjects and their photos are captured with frame rate 20 fps. 500 images are collected for each subject. Images are all frontal with neutral expression. There are no apparent movements like eye blink and head movements. Therefore, captured and recaptured images have more similarities, which makes the spoofing detection problem more difficult.

A high definition photo of each subject is taken using a Canon camera for the NUAA photo database. Photographs are developed in two ways. First way is to print them on a photographic paper with the common size of 6.8cm×10.2cm (small) and 8.9cm×12.7cm (bigger), respectively. Second way is to print them on a 70g A4 paper using a usual color HP printer. To make an exact comparison with the existing methods in [2], the same database is selected. In our study, test images are selected from the test sets of NUAA database; whereas the client and impostor training sets of NUAA database are used as client and impostor model sets in this paper as shown in Fig. 4. Table 1 gives statistics of the number of images involved in NUAA database for each train and test sets.

III. EXPERIMENTAL RESULTS

To test the effectiveness of the proposed approach, three types of experiments are done. The first experiment includes exact comparison results between the proposed approach and the methods published in [2]. The second experiment is done to show the effect of DoG filtering in the proposed approach. Finally, the last test is done to show the superiority of using LBPV with global matching method over using LBP with global matching method in the proposed approach. The aim of this test is to show that LBPV based method is more appropriate for the classification problem of this study since contrast provides also significant information in discrimination of captured and recaptured images.

A. Test 1: Results under Illumination Change

For this test, initially DoG filtering is applied to obtain the high frequency regions of the images which provide considerable spoofing detection information. Next, LBPV with global matching method is applied and images are classified either in client set or impostor set using the chi-square distance metric as shown in the flow chart of the proposed approach in Fig. 1.
The results of the approach using all LBPV patterns are given in Table 2 and the results of the approach using only the uniform LBPV patterns are given in Table 3.

The total error using all LBPV patterns is computed as 11.97% in Table 2; on the other hand, when only uniform patterns are used, it is computed as 13.05% in Table 3. This fact shows that instead of using all LBPV patterns, if only uniform LBPV patterns are used, the result is 8.28% worse. Out of 9123 test images, 99 more images are detected as true in case all LBPV patterns are used in classification.

Fig. 6 shows the comparison of classification accuracies (%) using three classification methods and various input features which are explained in [2] with details. The database which is proposed by Tan et al. [2] is used in this paper to make an exact comparison with the other existing methods in [2]. Sparse Linear Logistic Regression (SLR), Sparse Nonlinear Logistic Regression (SNLR) and Support Vector Machine (SVM) classifiers are used as classifiers; illuminance component of image estimated with Logarithmic Total Variation (LTVu), reflectance component of image estimated with Logarithmic Total Variation (LTVp), DoG filtered image (DoG), and high frequency component of image (HF) are used as input features in the study of Tan et al. [2]. The illuminance and reflectance components of images are also fused (LTVfused) and it is used as another input feature in [2], which gives the best results as it is shown in Fig. 6.

According to the results in Fig. 6, it is clear that the proposed approach is quite competitive with the existing techniques in face photograph spoofing detection, even better when compared to most of the results in this figure.

The remarks extracted from Fig. 6 are; initially, the proposed approach gives better results when compared to the results obtained with SLR classifier for all input feature cases. It is also clear that SLR, SNLR and SVM classifiers give worse results compared to our result (88.03%) in case DoG, HF, and LTVp are used as input features. Best results are obtained for the cases where LTVu and LTVfused are used as input features and SNLR and SVM are used as the classifiers as shown in Fig. 6. However, the result of proposed approach (88.03%) is also quite similar to these results; even has some advantages compared to these best cases shown in this figure. For example, for these best performance cases, the image has to be decomposed into illuminance and reflectance components; whereas in the proposed approach, the method is applied directly on the image. Furthermore, in our approach, classification method is very simple. Quadratic means of distances are computed for client and impostor sets and then images are classified in the nearest class comparing two quadratic mean values. Therefore, we can say that the approach provides less computational complexity compared to the best performance cases in [2].

In fact, since the proposed approach is applied directly on the image, (i.e. no decomposition of image into separate components), it is more reasonable to make the comparison with the cases where DoG and HF are used as input features. It is obvious that the proposed approach result is quite better than the results obtained for HF case. For the DoG feature case, DoG filtered image is also obtained at the first step of our approach. However, the components of this image (DoG features) are not used as input features in our study. After this step, the only thing we do is to apply a rotation invariant LBPV based method to obtain LBPV patterns to be used as input features. According to Fig. 6, for the case where DoG features are used as input features, the best results are obtained using SNLR and SVM classifiers, which give accuracies around 85%. For an exact comparison, SNLR and SVM classifiers, which give the best performances in the study of Tan et al. [2], may be considered to be used also in our study. However, in case LBP patterns are used as input features, the classifiers which use chi-square dissimilarity metric are recommended in various studies [10, 14]. This is why, in this study, a very simple classifier which uses chi-square dissimilarity metric is selected to be used for the classification.

As a result, the proposed method can be considered to provide sufficient detection accuracy of 88.03% with advantages of less computational complexity and robustness to illumination and rotation changes.

### B. Test 2: Effect of DoG Filtering in the Proposed Approach

In Test 1, approximately 88% success is achieved under illumination change in recaptured face image detection. For this test, as pre-processing step, DoG filter is used to extract the regions from which considerable spoofing information can be obtained. In this test, the aim is to show the effect of DoG filtering

#### Table 2. Proposed Approach Results Using All LBPV Patterns

<table>
<thead>
<tr>
<th>Test Set</th>
<th>Total # of Images</th>
<th># of Wrong Detection</th>
<th>FRR (%)</th>
<th>FAR (%)</th>
<th>Total Error (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>3362</td>
<td>308</td>
<td>9.16%</td>
<td>-</td>
<td>11.97%</td>
</tr>
<tr>
<td>Impostor</td>
<td>5761</td>
<td>784</td>
<td>-</td>
<td>13.61%</td>
<td></td>
</tr>
</tbody>
</table>

#### Table 3. Proposed Approach Results Using only Uniform LBPV Patterns

<table>
<thead>
<tr>
<th>Test Set</th>
<th>Total # of Images</th>
<th># of Wrong Detection</th>
<th>FRR (%)</th>
<th>FAR (%)</th>
<th>Total Error (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>3362</td>
<td>399</td>
<td>11.83%</td>
<td>-</td>
<td>13.05%</td>
</tr>
<tr>
<td>Impostor</td>
<td>5761</td>
<td>792</td>
<td>-</td>
<td>13.75%</td>
<td></td>
</tr>
</tbody>
</table>

![Fig. 6. Comparison of detection rates using SLR, SNLR, SVM as classifiers and LTVp, LTVu, LTVfused, DoG and HF as input features. This fig. is taken from [2].](image-url)
in the proposed approach. Table 4 shows the results of the approach, which is applied both with and without DoG filtering.

The effect of using DoG filtering can easily be observed from Table 4. With DoG filtering, there is a significant improvement compared to the case where DoG filtering is not applied as the pre-processing step. The effect of DoG filtering is due to the fact that DoG filtering helps to remove misleading information and noise, and thereby it provides a frequency spectrum which gives significant information for detection of recaptured images.

Table 4. Proposed Approach Results with DoG Filtering and without DoG Filtering as Pre-Processing Step

<table>
<thead>
<tr>
<th>Proposed Approach</th>
<th>Total # of Images</th>
<th>Total # of Wrong Detection</th>
<th>Error (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>with DoG Filtering</td>
<td>9123</td>
<td>1092</td>
<td>11.97%</td>
</tr>
<tr>
<td>without DoG Filtering</td>
<td>9123</td>
<td>2140</td>
<td>23.46%</td>
</tr>
</tbody>
</table>

C. Test 3: Comparison of LBP with Global Matching Method and LBPV with Global Matching Method in Recaptured Face Image Detection

For this test, instead of LBPV with global matching, LBP with global matching algorithm is applied in the proposed approach to prove that LBPV based method is more appropriate for our study. The superiority of LBPV over LBP algorithm is also verified in [10] by showing both LBP and LBPV histograms of two images. These LBP and LBPV histograms of two images in [10] show that although LBP histograms of the images are similar, LBPV histograms of the two textures can be quite different.

In this test, we applied LBP with global matching in the proposed approach. However almost random results are obtained for this specific problem of our study, this is why the results are not reported here. Therefore, we conclude that basic LBP with global matching is not appropriate to classify captured and recaptured images, and this proves that significant information is obtained from variance characteristics (contrast) of real and photo images in spoofing detection. Since LBPV algorithm analyses not only texture characteristics of images but also contrast characteristics of images, it is more appropriate for classification problem of captured and recaptured images.

IV. CONCLUSION

In this paper, a recaptured face image detection method, which is based on the analysis of different contrast and texture characteristics of captured and recaptured images, is proposed. The proposed approach gives quite satisfactory results when compared to the results obtained in [2] which use the same NUAA database in their experiments.

LBP based methods are very popular and it has been used in many different areas. However to the best of our knowledge, it has not been yet used for face photo spoofing detection. In the proposed approach, a LBPV with global matching method, which analyses both LBP (texture) and variance (contrast) characteristics of images, is used. In this study, it is also proved that LBPV with global matching method gives better results than LBP with global matching method in spoofing detection problem since LBPV also uses contrast information in classification of captured and recaptured images. The proposed approach is also rotation invariant. This property provides significant advantages in photo spoofing detection, since it is quite possible to make movements when photos are used for spoofing.

ACKNOWLEDGMENT

This work has been performed by the TABULA RASA project 7th Framework Research Programme of the European Union (EU), grant agreement number: 257289. The authors would like to thank the EU for the financial support and the partners within the consortium for a fruitful collaboration. For more information about the TABULA RASA consortium please visit http://www.tabularasa-euproject.org.

REFERENCES