

Kent Academic Repository

Full text document (pdf)

Citation for published version

Hasan, Md Rezwan and Hasan Mahmud, S M and Li, Xiang Yu (2019) Face Anti-Spoofing Using Texture-Based Techniques and Filtering Methods. In: Journal of Physics: Conference Series. Journal of Physics: Conference Series. Journal of Physics: Conference Series , 1229 (012044). 012044. IOP Publishing

DOI

<https://doi.org/10.1088/1742-6596/1229/1/012044>

Link to record in KAR

<https://kar.kent.ac.uk/87135/>

Document Version

Publisher pdf

Copyright & reuse

Content in the Kent Academic Repository is made available for research purposes. Unless otherwise stated all content is protected by copyright and in the absence of an open licence (eg Creative Commons), permissions for further reuse of content should be sought from the publisher, author or other copyright holder.

Versions of research

The version in the Kent Academic Repository may differ from the final published version.

Users are advised to check <http://kar.kent.ac.uk> for the status of the paper. **Users should always cite the published version of record.**

Enquiries

For any further enquiries regarding the licence status of this document, please contact:

researchsupport@kent.ac.uk

If you believe this document infringes copyright then please contact the KAR admin team with the take-down information provided at <http://kar.kent.ac.uk/contact.html>

Journal of Physics: Conference Series

2019 3rd International Conference on
Machine Vision and Information Technology
(CMVIT 2019)

Edited by
Qingbo He

IOP Conference Series
Proceedings services for science



1742-6596



IOP Publishing

- 012033 A Method of License Plate Recognition Based on BP Neural Network with Median Filtering**
Miaomiao Li, Zhenjiang Miao, Jiaji Wang, Shengbo Wang and Yuanhao Zhang
- 012034 DCRN: Densely Connected Refinement Network for Object Detection**
Shihui Gao, Zhenjiang Miao, Qiang Zhang and Qingyu Li
- 012035 Action Keyframe Connection Network for Temporal Action Proposal Generation**
Shengbo Wang, Zhenjiang Miao, Tianyu Zhou, Miaomiao Li and Ruyi Zhang
- 012036 Feature Extraction Method for EEG based Biometrics**
Sukun Li and Sung-Hyuk Cha
- 012037 Metric Learning Based Rolling Bearing Faults Diagnosis with Curvelet Transform**
Ziming Lu, Jiang-Wen Xiao and Zhengyi Huang
- 012038 Cerebral Microbleed Detection by Extracting Area and Number from Susceptibility Weighted Imagery Using Convolutional Neural Network**
S Sa-ngiem, K Dittakan, K Temkiatvises, S Yaisoongnern and K Kespechara
- 012039 Video Object Detection by Aggregating Features across Adjacent Frames**
Ruyi Zhang, Zhenjiang Miao, Qiang Zhang, Shanshan Hao and Shengbo Wang
- 012040 Light Corner Based Object Detector with Stacked-ENet Backbones**
Qingyu Li and Zhenjiang Miao
- 012041 Iterative Relation Reasoning for Multiple Object Recognition**
Tianyu Zhou and Zhenjiang Miao
- 012042 Mobile Object Detection Using 2D and 3D Basic Geometric Figures in Colour and Grayscale**
Ari Ernesto Ortiz Castellanos
- 012043 Control Method Based on Deep Reinforcement Learning for Robotic Follower with Monocular Vision**
Dongdong Wang, Feng Qiu and Xiaobo Liu
- 012044 Face Anti-Spoofing Using Texture-Based Techniques and Filtering Methods**
Md Rezwan Hasan, S M Hasan Mahmud and Xiang Yu Li

Information Technology

- 012045 Weight Loss for Point Clouds Classification**
FangYuan Huang, Cheng Xu, XiaoHan Tu and SiQi Li
- 012046 The Frontier of SGD and Its Variants in Machine Learning**
Juan Du
- 012047 TDMA Device Identification Using Continuity of Carrier Phase**
Y Pan, H Peng, T Li and W Wang
- 012048 Application of Sparse Dictionary Adaptive Compression Algorithm in Transient Signals**
Zhang Ailun and Tailin Han
- 012049 Feature Points Matching Algorithm based on Homography Constraint and Gray Scale Truncation Number**
Ruo Wu, Kun Wang and Jiquan Ma
- 012050 Design of Wideband Signal Decimation Based on Polyphase Filtering**
Yue Qu and Yunqing Liu

PAPER • OPEN ACCESS

Face Anti-Spoofing Using Texture-Based Techniques and Filtering Methods

To cite this article: Md Rezwan Hasan *et al* 2019 *J. Phys.: Conf. Ser.* **1229** 012044

View the [article online](#) for updates and enhancements.



IOP | ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

Face Anti-Spoofing Using Texture-Based Techniques and Filtering Methods

Md Rezwan Hasan¹, S M Hasan Mahmud² and Xiang Yu Li^{*,1}

¹ School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing, China

² School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), China

* Correspondence: wl@njust.edu.cn

Abstract: User authentication for an accurate biometric system is the demand of the hour in today's world. When somebody attempts to take on the appearance of another person by introducing a phony face or video before the face detection camera and gets illegitimate access, a face presentation attack usually happens. To effectively protect the privacy of a person, it is very critical to build a face authentication and anti-spoofing system. This paper introduces a novel and appealing face spoof detection technique, which is primarily based on the study of contrast and dynamic texture features of both seized and spoofed photos. Valid identification of photo spoofing is anticipated here. A modified version of the DoG filtering method, and local binary pattern variance (LBPV) based technique, which is invariant to rotation, are designated to be used in this paper. Support vector machine (SVM) is used when feature vectors are extracted for further analysis. The publicly available NUAA photo-imposter database is adapted to test the system, which includes facial images with different illumination and area. The accuracy of the method can be assessed using the false acceptance rate (FAR) and false rejection rate (FRR). The results express that our method performs better on key indices compared to other state-of-the-art techniques following the provided evaluation protocols tested on a similar dataset.

1. Introduction

The performance of face detection and recognition systems have improved drastically in the last few years. Therefore, this innovation is currently considered as a developed system and is used in numerous real-world applications from banking security to smart house systems and device authentication. However, several studies show that this kind of systems suffers from vulnerabilities to fake face spoofing attacks, a disadvantage that may restrict their use in many real-time scenarios. Indeed, it is a very tough task to protect against spoofs based on a static photo of a face, while the most effort of the present face recognition study has been focused on the "image matching" part of the system without noticing whether the corresponding face is live or fake [1]. Many face liveness detection techniques have been proposed to restrain the face recognition systems against this kind of occurrences. These techniques have shown good performances on the existing face presentation attack databases. Besides, their performances deteriorate radically under real-world variations (e.g., illumination and camera device variations).



These days, the requirement for reliable identification and authentication methods is a prime necessity in numerous applications from banking security to smart house systems and device authentication. Moreover, in our real-world applications, face detection, and recognition systems are getting increasing attention in the last few years, specifically with the growing use of smartphone devices. Thereafter, almost most of the smartphones are equipped with a suitable front-facing camera and their computing power has grown remarkably in the recent few years, and face recognition systems have been easily integrated into these devices. For example, Apple and Android have already mobilized face recognition systems into their smartphone operating systems to permit users to unlock their smartphones securely. The outlook of a human face can transform rapidly due to different lighting conditions, and there are also many camera-related factors that may control the nature of images, which makes it difficult to distinguish images from a fake photo and live person. Utilizing different image processing methods to extract features that reflect the variance between images from photographs and live human faces, can be another technique.

Work on spoofing face detection capabilities is still inadequate, and a significant part of it is based on the planeness of the captured surface in front of the sensor during an attack. It is also correct for methods that observe the 3D nature of the face by engaging supplementary strategies, which is further accurate now with the overview of reasonable user depth cameras. With the help of the improvements in 3D manufacturing technologies, readily available facial masks take the spoofing attacks one step ahead and present new demands for countermeasure studies. The lack of defense against biometric spoofing attacks is not exclusive to face biometrics systems [2].

Basically, among many face liveness detection techniques, the facial motion detection category, and the facial texture analysis category, are the two major categories. Approaches which are based on facial motion detection, assume subjects to display certain facial gesture, and the liveness is determined by the detection. Throughout the imitation procedure, facial texture analysis methods believe that forged faces perhaps lack about high-frequency data, and real & phony faces can be appropriately classified by scrutinizing and learning the facial texture data. Here the term “texture” signifies the high-frequency specifics in face images, and without uncertainty, the study treats “texture” equally with “high-frequency information.” Moreover, representing the face images in various scales, the multi-scale filtering techniques also work as pre-processing against variables such as noise and illumination. Throughout this work, we present an in-depth analysis of the existing face liveness detection methods and propose solutions mainly for improving the texture-based methods and multi-scale filtering methods concerning classification accuracy and error rate.

This paper is organized as follows: In section 2 we discuss related works on face spoofing attacks and countermeasures. The structure of the proposed approach is given in section 3. Section 4 describes the methodology, in which the specifications of the DoG filter are presented first. Next, the feature extraction using LBPV based algorithm is explained, and classification using SVM classifier is described. Finally, the selected NUAA photograph dataset is specified. Extensive experiments are conducted in Section V, consisting of analysis of results and comparison. Conclusions are provided in Section VI.

2. Related work

Although it is not impossible to spoof a face verification system using make-up, plastic surgery or forged masks; photographs and videos are undoubtedly the most common intimidations. Furthermore, due to the growing acceptance of social network websites, a great deal of hypermedia content, especially videos and photos, is accessible on the web that can be castoff to spoof a face authentication system. Many studies (e.g.,[3]) have shown that most of the present biometric systems are vulnerable to face presentation attacks. In [4], after downloading images from social media websites, six commercial face authentication systems were successfully attacked. In comparison to other systems, face recognition systems are more susceptible to spoofing attacks. To mitigate this kind of vulnerabilities, effective countermeasures against face spoofing must be needed to deploy.

The methods which are based on advanced senses and processing systems are most likely the most potent face liveness detection methods because the intrinsic gap among the live and fake faces in 3D structure [5] and (multi-spectral) reflectance [6] properties are directly adopted by the dedicated sensors. For example, planar spoofing detection becomes rather inconsequential if we can get the depth information [5], while near-infrared or thermal cameras are well-organized in face anti-spoofing as most of the displays in consumer electronics discharge only clear light. On the other hand, these kinds of special sensors are usually costly and not compact, thus not (yet) accessible in mobile devices, which prevents their full arrangement.

It would be relatively tempting to conduct face spoofing detection by analyzing only the same data that is used for the actual bio-metric tenacities or additional data captured with the standard acquisition device. This kind of software-based systems can be largely divided into active (requiring user association) and passive methods. Further user interaction can be very effectively used for face liveness detection because humans can be actively collaborative, whereas a photo or video-replay attack cannot respond to randomly specified action requirements. Approaches based on a challenge-response object at performing face spoofing detection based on whether the necessary action (challenge), e.g., facial appearance [7], aperture movement [7] or head alternation (3D structure) [8], was noticed within a predefined time window (reaction). Meanwhile, practical methods, which are based on software can be generalized well across diverse acquisition conditions and attack circumstances, at the cost of usability due to increased authentication time and system complexity.

Preferably, unreceptive approaches based on software would be superior to face spoofing detection since they are quicker and less invasive than their active complements. Due to the growing number of public standard datasets, several passive methods based on software have been proposed for face liveness detection. Overall, passive approaches based on evaluating diverse facial properties, like occurrence content [9], texture-based ones [10] and excellence [11], or signal cues, alike eye blinking [12], facial expression variations [13], mouth actions [13], or even color disparity because of blood flow (pulse) [14], to distinguish fake objects from original ones. Reflexive systems based on software have revealed encouraging results on the widely available databases but the initial cross-database assessments, corresponding [15], exposed that the performance is likely to worsen radically when functioning in unknown circumstances.

Of late, the study focusses on face anti-spoofing based on software has been progressively stirring into evaluating and refining the generalization proficiencies of the proposed and current approaches in a cross-dataset setup rather than operating merely on single datasets. Between hand-crafted methods based on features, image distortion analysis [16], mixture of texture and image quality analysis through interpupillary distance (IPD) based reject selection [17], active spectral domain analysis [18] and pulse recognition [14] have been applied in the situation of comprehensive face liveness detection but with solitary reasonable outcomes.

In our study, we have mainly focused on recognized and effective texture operator termed Local Binary Pattern (LBP) [19] and its improved varieties. And to further enhance the discriminate power of the scheme, the Difference of Gaussian (DoG) filter methods are adopted. For data classification, multi-SVM classifiers were utilized to calculate the results.

3. Proposed System

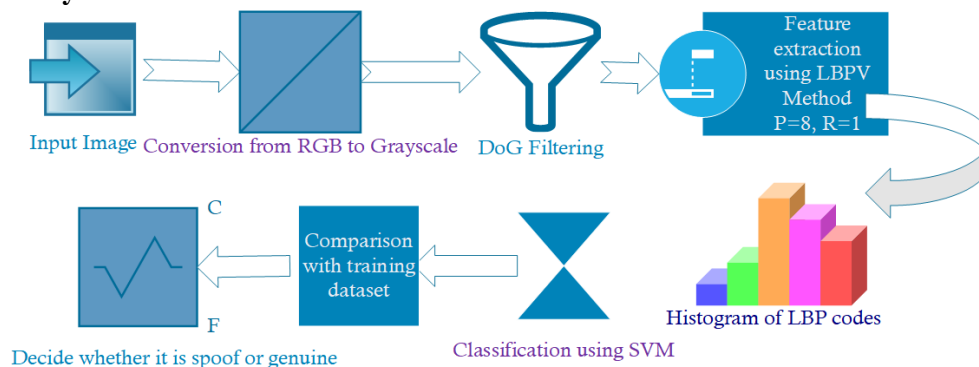


Figure 1. Block diagram of the proposed countermeasure.

Figure 1 is the block diagram of our proposed system which shows the entire flow of this paper. In this paper, the proposed method uses DoG filtering as the pre-processing step, and in the later part, LBPV based technique is used for feature extraction. Subsequently associating the input image through all images in the dataset, it will distinguish whether it is an original face or fake face by separately passing all the features via SVM classifier.

4. Methodology & Algorithm

4.1. Pre-Processing Step of the Proposed Method

A captured photo of a face has better image quality than a recaptured face photo; consequently, recaptured picture comprises less high-frequency materials [20]. This circumstance can be detected by evaluating the 2D Fourier spectra of the original face and fake ones.

DoG filtering is applied to eradicate noise while conserving the high-frequency mechanisms, which are notably the image edges. In this method, rather than evaluating all high-frequency bands, the high-middle band frequency spectrum is examined. For the DoG filter, a quite narrow Gaussian is built without presenting noise. To filter out false low spatial frequency information, little more outer Gaussian can be selected. This pre-processing procedure benefits to eradicate false info and noise; hereafter we can see the emphasis on the portion of the range which delivers essential information to differentiate among captured and fake face pictures. The consequence of applying DoG filtering as the pre-processing phase in the proposed method is also tested in the experimental analysis segment. Thus, the DoG filter is considered as a band-pass filter. This band-pass filter also uses two Gaussian filters with standard deviations as limits. Our purpose is to maintain the high-middle-frequencies to distinguish the boundaries, but not much, to eliminate the noise (which is also a high-frequency). In this paper, a relatively fine Gaussian ($\sigma_i = 0.6$) is formed without presenting noise. To filter out misleading low spatial frequency information, $\sigma_j = 1$ is selected for the outer Gaussian. This DoG filter is also proposed to improve the sturdiness of LBP features. Given an image I , the DoG image at the scale s defined by the two parameters σ_i and σ_j is given by:

$$I(x, y, \sigma_i, \sigma_j) = \left(G(x, y, \sigma_i) - G(x, y, \sigma_j) \right) * I(x, y). \quad (1)$$

4.2. Feature Extraction Step of the Proposed Approach

LBPV is an abridged and competent joint LBP and contrast rotation technique [21]. There is no data associated with variance in LBP calculation. The variance is also referred to as the texture feature, and usually, the high-frequency texture areas have higher variations and contribute more to the discrimination of images [21]. Since initially, DoG filtering is applied, the high-frequency areas are all removed after this step. Thus, it is easier to distinguish captured and spoofed pictures by utilizing the LBPV procedure on these areas which are derived by DoG filtering. The contrast and pattern of

texture are corresponding features. For the pattern histogram, LBPV adds extra contrast measures, and this delivers expressively better outcomes than LBP. Both LBP and LBPV are tested using diverse textures in [21], to establish the prerogative. In our study, these algorithms are used.

LBPV calculation is entirely based on LBP calculation. $LBP_{P,R}$ is calculated as follows:

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c) 2^p, \quad (2)$$

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases} \quad (3)$$

$LBP_{P,R}$ is computed such that for a specified central pixel in a photo, a pattern number is calculated by relating its value with those of its neighbors'. The gray value of the central pixel is g_c , the neighbors' value is g_p , in radius R of a circle, the number of neighbors' is P in equation (1).

In the calculation, the LBP pattern of each pixel (i, j) is used to attain LBP histogram of an $X \times Y$ image.

$$H(k) = \sum_{i=1}^X \sum_{j=1}^Y f(LBP_{P,R}(i, j), k), \quad k = [0 K] \quad (4)$$

$$f(x, y) = \begin{cases} 1 & x = y \\ 0 & \text{else} \end{cases} \quad (5)$$

K is the absolute LBP pattern value in (3). Each LBP pattern has a weighting aspect of 1 in this histogram. To complement contrast information LBPV procedure is used here. In Eqs. (5) and (6), the variance is calculated for the P sample points around a circle of radius R.

$$Var_{P,R} = \frac{1}{P} \sum_{p=0}^{P-1} (g_p - u)^2 \quad (6)$$

$$u = \frac{1}{P} \sum_{p=0}^{P-1} g_p \quad (7)$$

The LBPV gathers it into the LBP bin as the weighting factors [21] and calculates the variance from a local region. In Eqs. (7) and (8), LBPV histogram is computed.

$$LBPV_{P,R}(k) = \sum_{i=1}^X \sum_{j=1}^Y W(LBP_{P,R}(i, j), k), \quad k = [0 K] \quad (8)$$

$$W(LBP_{P,R}(i, j), k) = \begin{cases} Var_{P,R}(i, j) & LBP_{P,R}(i, j) = k \\ 0 & \text{else} \end{cases} \quad (9)$$

Uniform patterns can be used, instead of applying all LBPV patterns as features in the classification step. Uniform patterns are nominated according to the U value which is defined as

$$U(LBPV_{P,R}) = |s(g_{p-1} - g_c)| - |s(g_0 - g_c)| + \sum_{p=1}^{P-1} |s(g_p - g_c)| - |s(g_{p-1} - g_c)| \quad (10)$$

In the pattern, U value is the number of spatial conversions (bitwise 0/1 changes). In the globular binary presentation [21], the uniform LBPV pattern has limited development or disjointedness. The patterns which satisfy $U \leq 2$ are selected as uniform patterns. The purpose of choosing uniform patterns is that 'uniform' patterns are verified to be underlying patterns of local image texture. Sufficient information can be attained by using only uniform patterns, instead of using all patterns.

In the proposed approach, a method which is robust to the rotation is ideal to detect recaptured images. It is entirely possible to make movements while holding photos. They can even be fixed to make them visually closer to a 3D face or to move horizontally or vertically to act as a live face. It means that a rotation-invariant system is essential for the case in this study.

There are both local and universal rotation invariant systems in texture classification. In the proposed approach, a fusion method, which is based on globally rotation invariant matching with locally variant LBPV texture features [21], is applied to extract features for classification. In that way, both global spatial information and local texture information is well-maintained in classification.

4.3. Classification using Support Vector Machine (SVM)

Given that we aim to design an efficient face anti-spoofing system with good generalization ability and swift response, it is required to have a suitable classifier for the extracted features. In signal processing [22], pattern recognition, classification applications [23], and in many more areas SVM [24] is successfully applied. That's why we prefer to adopt SVM through the Lib-SVM Library [25]. There are also many discrepancies of SVM for handling large-scale classification problems, such as LIBLINEAR and ALM-SVM; though most of the publicly available face anti-spoofing datasets (as

well as the dataset which is used in our research) are of an inadequate size regarding the size of still imageries, and subjects. An SVM classifier with RBF kernel will be trained for each group of training data. Here, the final LBP feature vectors will be fed into linear SVM (LIBLINEAR) classifier. An SVM is defined by creating high margin hyperplane for the dataset which is linearly separable and belongs to one of two classes. The primary purpose of the support vector machine is to generate a hyperplane in between data sets to specify which category it belongs to. The primary test of SVM is to train the device to understand the data structure and mapping the right class label. The selected hyperplane's distance is most significant to the adjacent training data points of any class [24].

4.4. Brief Database Description

This section provides the basic specifications of the selected NUAA imposter database [20]. There are only a few numbers of widely available photo impostor databases. NUAA is one of them. It is created by using a generic webcam. Location and illumination condition of each session are varied. Test and training sets are constructed from distinct sessions. The dataset consists of 15 subjects. In each session, the photos of both live subjects and their photos are captured with a frame rate of 20 fps. Five hundred images are collected for each item. Pictures are all frontal with a neutral expression. There are no deceptive movements like eye blink and head movements. Therefore, captured and recaptured images have more correspondences, which makes the spoofing detection problem more critical.

A high definition photograph of each subject is captured using a Canon camera for the NUAA photo dataset. Photos are taken in two ways. 1st way is to print them on a photographic paper with the general size of 6.8cm×10.2cm (trivial) and 8.9cm×12.7cm (more prominent), respectively. The other way is to print them on a 70g A4 size paper using a standard color HP printer. To make a thorough evaluation with the existing methods in [20], the same dataset is selected. In this approach, test images are selected from the test sets of NUAA dataset; whereas the client and imposter training sets of NUAA dataset are used as client and impostor model sets in this.

5. Experimental analysis

To test the effectiveness of our proposed approach, we evaluated two different types of spoof detection methods: LTP (Local Ternary Pattern) features (as used in [26]), and modified DoG-LBPV features (as proposed). We describe our performance evaluation on the NUAA dataset [20], which is designed specifically for face spoofing studies and contains various spoofing attacks as well. First, we calculate the classification accuracy of the proposed method on the test samples. The corresponding results are shown in Table 1. In the following, we describe the comparison of our method with previous approaches to this dataset. Precisely, we computed the half total error rate (HTER), which is half of the sum of the false rejection rate (FRR) and false acceptance rate (FAR) formulated as:

$$HTER(\tau) = \frac{FAR(\tau) + FRR(\tau)}{2} \quad (11)$$

Where τ denotes the threshold value, which makes the ROC curve. The HTER results based on this value are shown in Table 1. The HTER values of the proposed method and LTP based method for test on the whole set are 0.39% and 7.50%, respectively.

Table 1. Performance of LTP at the threshold value ($\tau = 5$) and modified DoG-LBP on the dataset

Methods	Accuracy	HTER	FAR	FRR	AUC
LTP	91.1	7.4	5.1	9.7	0.886
Mod. DoG- LBPV	99.22	0.39	0.35	0.43	0.990

The rate of face liveness detection on test sets in the dataset is displayed in Table 1. in terms of Half Total Error Rate (HTER), Accuracy, and Area Under the Curve (AUC) along with False Rejection Rate (FRR) and False Acceptance Rate (FAR) at fixed threshold value of ($\tau = 5$) for the LTP method.

The receiver operating characteristic (ROC) curve is presented in Figure 2 that displays the error graph of False Positive Rate against True Positive Rates. ROC curves are best for equating the

performance analysis of any two systems. In Figure 2, the ROC curve of modified DoG-LBPV compared with LTP tested on NUAA database is shown.

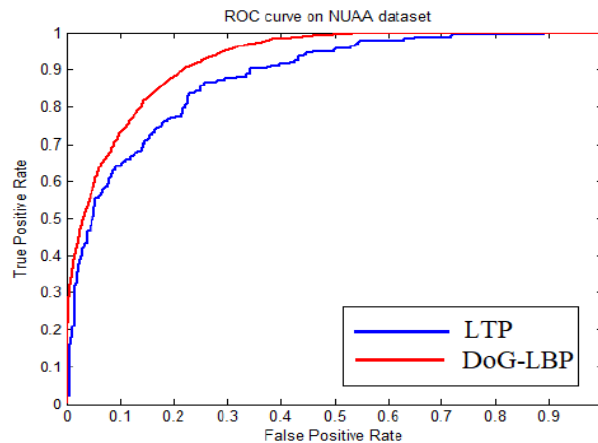


Figure 2. ROC curve of LTP and DoG-LBPV on NUAA dataset

The modified version of DoG-LBPV features is more strong across several illuminations, situations, and multiple textures than the features of LTP, which is indicated by the constant advanced performance in the test dataset of the ROC curve.

According to the consequences, our proposed method achieves higher accuracy and lower error rate. This texture descriptor-based method outclasses in comparison to the general LTP descriptor-based method, which is also specified by all the results. It can be detected that the proposed method of modified DoG-LBPV is more robust to noise with a uniform pattern.

The outcome of higher accuracy and lower value of error rates shows that the modified DoG-LBPV texture descriptor computes more useful features, and also has stability in unlike scenarios and lighting effects. It is found to be more robust for several textures.

Furthermore, a relative assessment of modified DoG-LBPV and LTP with other prevailing state-of-the-art methods to texture-based analysis using NUAA dataset by implementing comparable experimental procedures to benchmark the consequences is presented in **Table 2**.

Table 2. Performance comparison on NUAA dataset

Techniques	HTER (%)
Local Binary Pattern (LBP) [19]	18.32, 19.03 and 13.17
Local Binary Pattern Variance (LBPV) [27]	11.97 and 13.0
Local Ternary Pattern (LTP)	7.4
Dynamic Local Ternary Pattern (DLTP)	3.5
Modified DoG-LBPV	0.39

The results specify that the combination and variations in LBP extend to good performance for face anti-spoofing. As compared to the conventional and simple LBP, LTP progresses the results in face pattern analysis because of its noise resistance stuff by quantization of 3 levels. For making quantization levels further stable and reliable, the modified DoG-LBPV is introduced. As per expectations, from the achieved results, modified DoG-LBPV provides a better outcome for face liveness detection in the key indices in contrast to the state-of-the-art systems.

6. Conclusion

In this paper, we have proposed a presentation attack detection method, which is based on the analysis of various contrast and texture characteristics of original and spoofed photos and modified DoG filtering technique. When we compared the results with the other well-known methods using the same NUAA database, our proposed technique has shown excellent performance. LBP based techniques are

very famous, and they have been used in many unique areas. In our proposed extension method, an LBPV method with modified DoG filtering, which analyzes both LBP (texture) and variance (contrast) characteristics of photos has been applied. In this approach, it is also seen that LBPV with SVM classifier method gives better results than LBP with SVM classifier in presentation attack detection case because LBPV also uses contrast information in the classification of original and spoofed photos. Invariant rotation is one of the critical features of this approach. There's an absolute possibility of making movements when the fake faces are used for spoofing so that this feature provides significant benefits.

As a future work, we can try to improve the test results for other well-known face spoof datasets, especially the face data taken from high-quality cell-phone display. Moreover, the performance of cross-database testing needs more development. The overall cross-database performance is relatively weak on almost all the face spoofing detection systems.

Acknowledgment

I want to acknowledge my appreciation and sincere gratitude to my supervisor Dr. LI Xiang Yu for his invaluable guidance, and kind co-operation during my research. This work was supported in part by Natural Science Foundation of Jiangsu Province of China under Grant No. BK20160850.

References

- [1] R.N. Rodrigues, "Face Modeling and Biometric Anti-Spoofing Using Probability Distribution Transfer Learning," *BiblioBazaar*, 2012.
- [2] S. Lina, R. Latha, "Detecting Masquerade in Face Recognition System – A Literature survey," *IOSR Journal of Computer Engineering*, Vol.16, Iss.1, Ver. IV, pp.01-05, 2014.
- [3] I. Chingovska, N. Erdogmus & S Anjos André and Marcel (2016), "Face Recognition Systems Under Spoofing Attacks," pp. 165–194.
- [4] Y. Li, K. Xu, Q. Yan, Y. Li & RH. Deng (2014), "Understanding OSN-based facial disclosure against face authentication systems," In *ACM Symposium on Information, Computer, and Communications Security*, pp. 413–424.
- [5] N. Erdogmus, S. Marcel, "Spoofing attacks to 2D face recognition systems with 3d masks," In *IEEE International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2013.
- [6] R. Raghavendra, K. B. Raja, C. Busch, Presentation attack detection for face recognition using light field camera, *IEEE Transactions on Image Processing* 24 (2015) 1060–1075.
- [7] K. Kollreider, H. Fronthaler, J. Bigun, "Real-time face detection and motion analysis with application in liveness assessment," *IEEE Transactions on Information Forensics and Security* (2007).
- [8] T. Wang, J. Yang, Z. Lei, S. Liao, S. Z. Li, Face liveness detection using 3D structure recovered from a single camera, In *International Conference on Biometrics (ICB)*, 2013.
- [9] J. Li, Y. Wang, T. Tan, A. K. Jain, "Live face detection based on the analysis of Fourier spectra, In *Biometric Technology for Human Identification*," 2004, pp. 296–303.
- [10] I. Chingovska, A. Anjos, S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," In *IEEE International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2012.
- [11] J. Galbally, S. Marcel, Face anti-spoofing based on general image quality assessment, In: *International Conference on Pattern Recognition (ICPR)*, 2014, pp. 1173–1178.
- [12] G. Pan, Z. Wu, L. Sun, "Liveness detection for face recognition," In: *Recent Advances in Face Recognition*, In-Teh, 2008, pp. 109–124.
- [13] K. Kollreider, H. Fronthaler, J. Bigun, "Real-time face detection and motion analysis with application in liveness assessment," *IEEE Transactions on Information Forensics and Security* (2007).

- [14] X. Li, J. Komulainen, G. Zhao, P.-C. Yuen, M. Pietikainen, "Generalized face anti-spoofing by detecting pulse from face videos, In: International Conference on Pattern Recognition (ICPR), 2016.
- [15] T. de Freitas Pereira, A. Anjos, J. De Martino, S. Marcel, "Can face anti-spoofing countermeasures work in a real-world scenario?", In: International Conference on Biometrics, 2013.
- [16] D. Wen, H. Han, A. Jain, Face spoof detection with image distortion analysis, *IEEE Transactions on Information Forensics and Security* 10 (2015) 746–761.
- [17] K. Patel, H. Han, A. K. Jain, "Secure face unlock: Spoof detection on smartphones," *IEEE Transactions on Information Forensics and Security* 11 (2016) 2268–2283.
- [18] A. Pinto, H. Pedrini, W. Robson Schwartz, A. Rocha, Face spoofing detection through visual codebooks of spectral-temporal cubes, *IEEE Transactions on Image Processing* 24 (2015) 4726–4740.
- [19] A. Hadid, "The local binary pattern approach and its application to face analysis." In *Proceedings of the Image processing theory, tools and application*, Sousse, Tunisia, 2008; pp. 1–9.
- [20] X. Tan, Y. Li, J. Liu, L. Jiang, "Face Liveness Detection from a Single Image with Sparse Low-Rank Bilinear Discriminative Model," In: 11th European conference on Computer vision, 2010.
- [21] Z. Guo, L. Zhang, D. Zhang, "Rotation Invariant Texture Classification Using LBP Variance (LBPV) with Global Matching," *Elsevier Pattern Recognition*, vol. 43, no. 3, 2010, pp. 706-719.
- [22] A. Bashashati, M. Fatourechi, R. K. Ward, and G. E. Birch, "A survey of signal processing algorithms in brain-computer interfaces based on electrical brain signals," *Journal of Neural Engineering*, vol. 4, no. 2, pp. R32–R57, 2007.
- [23] Y. Lin, F. Li, S. Zhu, M. Yang, T. Cour, K. Yu, L. Cao, and T. Huang, "Large-scale image classification: Fast feature extraction and SVM training," in *Proc. IEEE CVPR*, 2011, pp. 1689–1696.
- [24] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A training algorithm for optimal margin classifiers," in *Proc. 5th ACM Workshop on Computational Learning Theory*, (1992), pp. 144–152.
- [25] C.C. Chang and C.J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intel. Syst. Technol.*, vol. 2, no. 3, pp. 27:1–27, May 2011.
- [26] X. Tan; B. Triggs, "Enhanced local texture feature sets for face recognition under difficult lighting condition," *IEEE Trans. Image Proc.* 2010, 19, 1635–1650.
- [27] N. Kose, J.L. Dugelay, "Classification of captured and recaptured images to detect photograph spoofing," In *Proceedings of the International Conference on Informatics, Electronics and Vision (ICIEV)*, Dhaka, Bangladesh, May 2012.