OPEN ACCESS
ISSN 2460-9056
socj.telkomuniversity.ac.id/indojc

Intl. Journal on ICT
Vol. 4, Issue. 2, December 2018. pp. 11-18
doi:10.21108/indojc.2018.42.134

Image Spoofing Detection Using Local Binary Pattern and Local Binary Pattern Variance

Arida Kartika [#1], Indra Bayu Kusuma [*2], Tjokorda Agung Budi Wirayuda [#3], Kurniawan Nur Ramadhani [#4], Febryanti Sthevanie [#5]

 # School of Computing, Telkom University
Bandung, Indonesia

[1] aridakartika@students.telkomuniversity.ac.id
[3] cokagung@telkomuniversity.ac.id
[4] andiess2006@gmail.com
[5] febryantisthevanie@gmail.com
[*]Telkom University
Bandung, Indonesia

[2] indrabay@students.telkomuniversity.ac.id

Abstract

Particularly in the field of biometric security using human face has been widely implemented in the real world. Currently the human face is one of the guidelines in the security system. Nowadays the challenge is how to detect data falsification; such an attack is called spoofing. Spoofing occurs when someone is trying to pretend to be someone else by falsifying the original data and then that person may gain illegal access and benefit him. For example one can falsify the face recognition system using photographs, video, masks or 3D models. In this paper image spoofing human face detection using texture analysis on input image is proposed. Texture analysis used in this paper is the Local Binary Pattern (LBP) and Local Binary Pattern Variance (LBPV). To classified input as original or spoof K-Nearest Neighbor (KNN) used. Experiment used 5761 spoofs and 3362 original from NUAA Imposter dataset. The experimental result yielded a best success rate of 87.22% in term of accuracy with configuration of the system using LBPV and histogram equalization with ratio $R = 7$ and $P = 8$. In term of retrieved measurement, we achieve precision level at 0.8406 that indicate the correct classify of the system is high with the accuracy 87.22%.

Keywords: K-Nearest Neighbor, Local Binary Pattern, Local Biner Pattern Variance, NUAA Imposter dataset, Spoofing

Received on Nov 2018. Accepted on Dec 2018

I. Introduction

FACE detection has been widely implemented in real life and generally used for security purposes. The reason lies in the uniqueness of every human face that can be used to identify one person to another. The existing face detection has shortcomings, such as weak against falsification of data using images of faces that have been printed. Such attacks are called spoofing. Spoofing attacks occur when there are people trying to impersonate someone by falsifying data and take advantage of the restricted access area [1]. Without any measurements on spoofing detection, most face detection systems are vulnerable to spoofing attack. System can be fooled only by using a printed face photograph. The real face and the photograph certainly reflect light in different ways, this is caused by the human face which is a complex 3D object, whereas a printed face photograph can only be seen as a rigid planar object.

From previous studies, human face detection spoofing performed using texture analysis. Texture analysis used is based upon several algorithms such as Local Binary Pattern, Local Binary Pattern Variance, Gabor Wavelet, Wavelet Haboor, Histogram of Gradient, Spatiotemporal Local Binary Patterns [3-6]. LBP and LBPV has the ability to extract the characteristics of a texture and contrast images that can distinguish human faces of the original image with the result of a spoof. According to the vulnerability of spoofing attacks, the authors built a system that can detect human face spoofing using printed photograph. Therefore, in this research proposed methods Local Binary Pattern and Local Binary Pattern Variance as feature extraction method based texture. For the next feature extraction results obtained will be classified into two classes, namely classes and class spoof non-spoof.

II. Literature Review

A. Image Spoofing

An attack to biometrical sensor could be divided into several scenarios. The biometrical characteristics of each individual must be different, not even in the case of identical twins. So many people were tried to manipulated this difference by doing an attack. The attack could be in the form of a compulsion to a user who has been registered, a registration by using dead bodies or parts of the dead bodies which has been genetically cloned, and showing fake biometrical data (spoofing)[10].

One of the attacks toward biometrical sensor is spoofing. We can see the anti-spoofing measurement by liveness detection. In this measurement, we will see several signs showing that there is a life in it. The difference between the original face and its photograph is shown by the non-rigid 3D complex of the shadow or the color of the live face, while the result of the face photograph could be seen as a stiff planar object. Thus, to detect spoofing attack on a human face using a face photograph could be done by doing a texture analysis. The scheme of common face recognition is shows in Fig. 1 and the spoofing attack by using face photograph is shows Fig. 2.

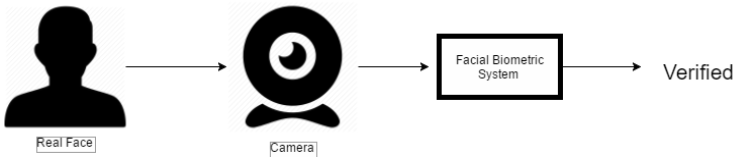

Fig. 1. Facial Biometric Scheme

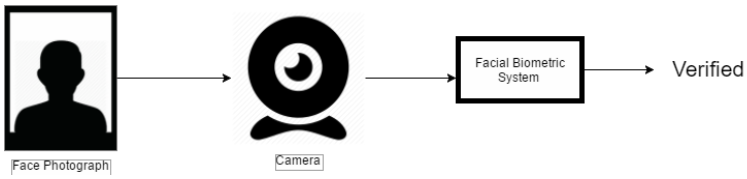

Fig. 2. Spoofing Attack Scheme

B. Related Work

Nowadays, face recognition has been implemented in the real world as a security issue. Facial biometric systems are vulnerable to attack, thus anti spoofing detection system is needed. On the other hand, spoofing image can be detected by extracting its textual feature. Hence, Määttä and the other authors was purpose the anti-spoofing detection using textual features. On previously work on face spoofing detection from single images using micro-texture analysis [2] written by Määttä, J, purpose of the study was to analyze the texture of facial images using multi-scale Local Binary Pattern (LBP) and the changing patterns of micro-texture into a histogram feature. The result will be classified using Support Vector Machine (SVM) to determine whether the input image is an image of a spoof or not. LBP used in these studies using LBP16,2, LBP8,1, and LBP8,2 where an input image will be cutting into 64 x 64 pixels then those images has been normalized. Results from these studies resulted in the value of an EER of 2.9% and compared to other methods such as Local Phase Quantization (LPQ) and Gabor that produce value EER and Gabor respectively 4.6% and 9.5% in the same database.

In another study, namely face spoofing detection using dynamic texture [1], the previous study developed a method that uses only LBP by adding features from Gabor Wavelett and Histogram of Gradient (HOG). Also in another study, the results of performance measured by a parameter that is for LBP EER + 2.0% Gabor, LBP + 1.5% HOG, HOG Gabor + 2.4% and a combination of all methods of LBP + Gabor HOG + 1.1%. In studies image spoofing other method used is Histogram Of Oriented Gradients (HOG), Color Frequency (CF), Gray Level Co-Occurrence Matrix (GLCM) and Histogram Of Shearlet Coefficients (HSC) with a weighting scheme Partial Least Squares (PLS). The purpose of these studies is to obtain a solution that can extract low-level features to distinguish ideals and video are 'live' and 'spoof'. The results of this research is EER values as low as 1.67% by using HOG + CF + GLSM + HSC. While the value of EER for each method range between 4.30% to 11.67%. On the previous study by using DoG filter to remove frequency noise and implemented Local Binary Pattern Variance (LBPV) as the feature extraction and using exhausted search for distinguish between spoof and real face image. The result of that study is 11.97% as an ERR.

II. Research Method

Fig. (3) and Fig. (4) shows the system implemented to detect image spoofing, that consist of two part; first is model building, second is testing. Testing step consist of these steps, input image, preprocessing, feature extraction (LBP and LBPV), classification (KNN), output class.

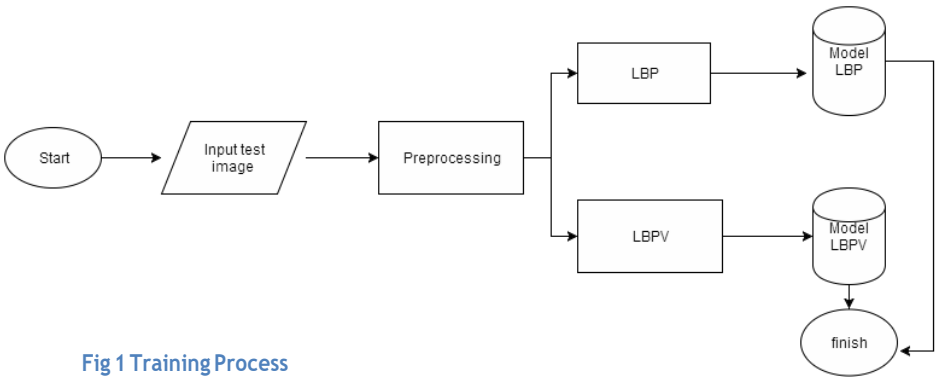

Fig. 3. Training Process

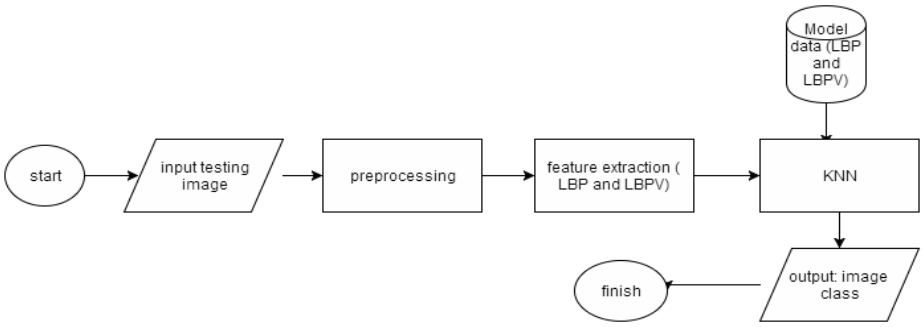

Fig. 4. Testing Process

A. *Dataset*

This research selected NUAA Imposter database [2] as the dataset in this paper. There are 15 subjects in the dataset, every one of them consist of real face of the subject, and photograph of them. Real face is taken from webcam with natural expression and frontally face the camera, there is no movement such as eyeblink, this is used to make the real face is similar like the photograph.

Photograph of the subject is taken with Canon camera that appear 2/3 of the photograph is subject's face. Next stage is being done in two step, the first is printed on photograph paper with normal size 6.8cm x 10.2cm (small) and 8.9cm x 12.7cm (medium). The second is be printed on normal paper A4 70g with HP printer.

Fig. 5. Live Faces (Non Spoof)

Fig. 6. Fake Faces (Spoof)

B. *Local Binary Pattern*

Local Binary Pattern (LBP) method was initially proposed as texture descriptor, then used in several areas in computer vision such as face recognition, facial expression recognition, modelling motion and action, and medical image analysis. The value of LBP on the central pixel ***C*** of an image can be calculated from comparing the centre value with its neighbouring pixels in radius of ***P***. The comparison of centre ***C*** and ***P*** is defined by binary number which are 1 and 0. The value is 1 when a neighbour is bigger than its ***C***, otherwise the value is 0. The common parameter for ***P*** and ***R*** is 8 and 1 respectively [9]. Thus, LBP value for pixel (xc, yc) is computed by this equation (1)

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

Where gc is the intensity value of centre (xc,yc) and gp is the intensity value of its neighbours ***P*** on radius ***R***. S is defined as a thresholding function as in equation (2)

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

The result vector of LBP value is represented by histogram. For example, the size of the image is $\times Y$, after calculated LBP value of pixels (i,j) then histogram is calculate by equation (3)

$$H(k) = \sum_{i=1}^{X} \sum_{j=1}^{Y} f\big(LBP_{P,R}(i,j), k\big), k \in [0, K] \quad (3)$$

C. Local Binary Pattern Variance

Local Binary Pattern Variance (LBPV) is a simple method yet eficient to learn LBP and other contrast distribution method [8]. It can be seen in equation (3) that variance is not included in histogram H, therefore there is no variance included in local area as the histogram gave the same weight. Actually, variance is related to texture because a high frequency texture area should also has high variance. LBPV can be calculated using equation (4) and (5)

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

$$w\big(LBP_{P,R}(i,j), k\big) = \begin{cases} \big(VAR_{P,R}(i,j)\big) & (LBP_{P,R}(i,j) = k) \\ 0 & x \leq 0 \end{cases} \quad (5)$$

Where k is the value of LBP in pixel (i, j), w is weight and VAR stand as the variance.

D. K-Nearest Neighbor

K-Nearest Neighbor (KNN) is one of classification method most used, because it can be modified in the stage of its system. KNN has two step [7]; the first is determine the nearest neighbor, and the second is determine the class of tested data. Visualization of KNN using the value of k=3 in Fig. 1, the first step, tested data was compared to the model data, then k data is chosen to be the neighbor of the tested data. The second step is to determine the class, many methods used to do this step, simply count the majority class of neighbors then used it to label the data testing.

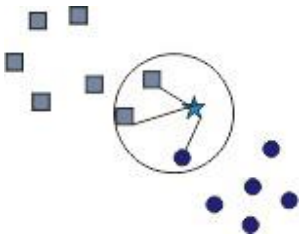

Fig. 7. KNN Classify

Neighbour is derived by calculated the distance between data test and model data using Euclidean distance, also other distance method such as Minkowski, Manhattan, etc. can be used as the distance calculation.

E. Performance Measurement

This paper used confusion matrix as the method to differentiated spoof and non-spoof data from training data and testing data. The accuracy, precise and recall of this system was measured, because of the imbalance between classes. The equation of accuracy, precise and recall is shown below:

$$Accuracy = \frac{\sum True_{positive} + \sum True_{negative}}{Total\ Data} \quad (6)$$

$$Precision = \frac{\sum True_{positive}}{\sum True_{positive} + \sum False_{positive}} \quad (7)$$

$$Recall = \frac{\sum True_{positive}}{\sum True_{positive} + \sum False_{positive}} \quad (8)$$

III. RESULTS AND DISCUSSION

A. Dataset Description

In this paper dataset used for testing derived from database NUAA with a human face images come from 16 different individuals. The dataset used have different lighting conditions vary for each individual. The number of spoof images used in the test was 5,761 images while for non-spoof images used in the test was 3,362 images. The number of images every individual is different it is because in this study only differentiate the original image of a human face or not. In other words, this study did not differentiate between individuals.

TABLE 1
NUMBER OF IMAGE IN DATASET

Training Set	Total	Test Set	Total
Spoof	1748	Spoof	5761
Non Spoof	1743	Non Spoof	3362

B. The Result of Different Extraction Method

In this part, we are applying with or without pre-processing method. The pre-processing used are Histogram Equalization and Adaptive Histogram Equalization. These pre-processing is used to enhance the contrast of the image. In this part of test 6 different parameters used. The result is shown in Fig. 8.

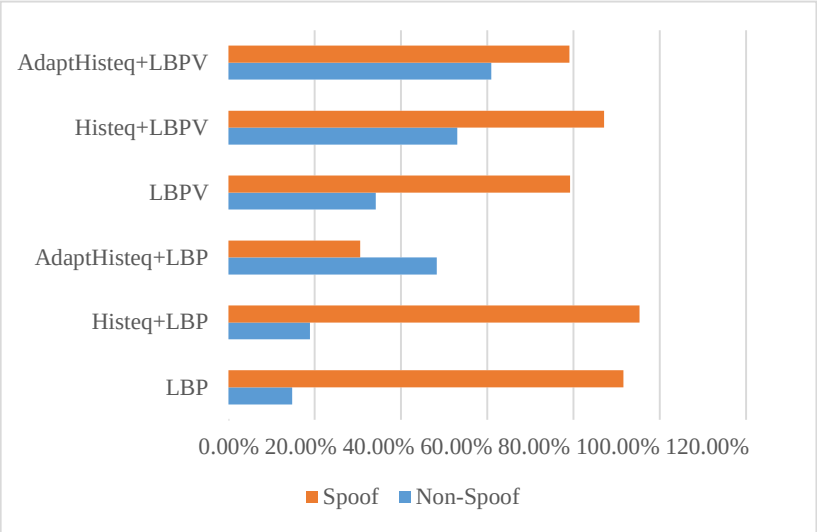

Fig. 8. Accuracy of Each Class in Different Feature Extraction Method

C. *The Result of Different Radius R*

On the second part the experiment focus in the parameter radius R and using Histogram Equalization as preprocessing method and LBPV as feature extraction. R parameter used are $R = 2$, $R = 4$, $R = 5$, $R = 7$, the result on this experiment shows in Table 2.

TABLE 2
PRECISION AND RECALL RESULT

Feature Extraction Method	Recall	Precision
$LBPV_{8,2}$+Histeq	0.9479	0.8319
$LBPV_{8,4}$+Histeq	0.9523	0.8554
$LBPV_{8,5}$+Histeq	0.9849	0.8168
$LBPV_{8,6}$+Histeq	0.9842	0.8406

Based on the Table 2 the experiment shows that with a different radius R each result not so different in detect spoof image but it can increase detection of non-spoof image. The accuracy system with different Radius R is shows in Fig. 8

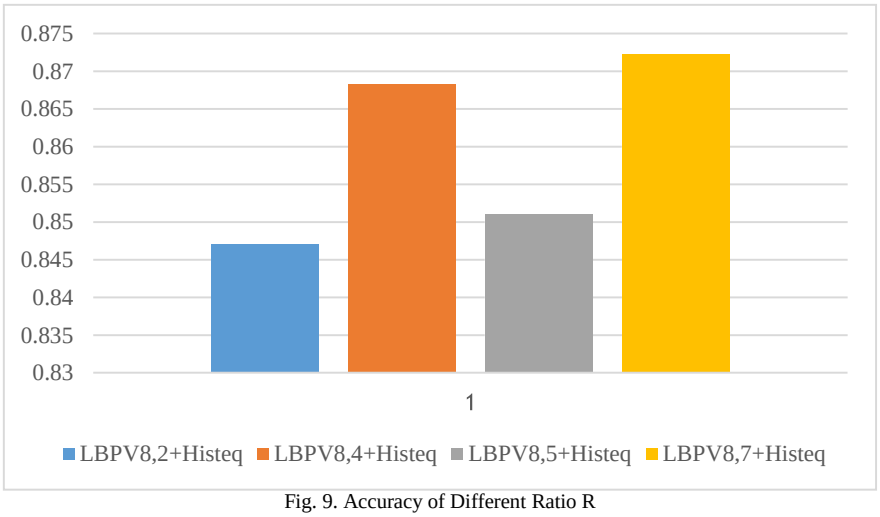

Fig. 9. Accuracy of Different Ratio R

The best result is computed by using $R = 7$ because with $R = 1$ (shows in Fig. 8) it can not distinguish feature that taken neighbour pixel equal to 1. The variance is increasing by using R=7 but still did not affect the original feature. The result shows that the exact radius R determine the accuracy of the system.

IV. Conclusion

Most of state-of-the-art facial biometric systems are vulnerable to attack. Such an attack called spoofing. Therefore, facial biometrics system is need preventive measures to overcome spoofing attack. LBP and LBPV can be used to detect image spoofing by using NUAA imposter database. In this paper stated the variance of the experiment, using preprocessing and different feature extraction. The combination which is better was LBPV and using histogram equalization as preprocessing, that can distinguish spoof image with the true positive point is 87.10% and non spoof image 53.03% that is the best of other combination. Then to improve the accuracy of the system, this paper was tried to change the parameters of the radius *R*, and got the accuracy 87.22% with the precision value is 84.06%.

The improvement that can be done in the future work is to find better preprocessing method to help the system improve the ability to distinguish the different of real face and face photograph. Classification method used in this paper is still took a lot of time to execute, maybe can use clustering or other method to reduce the complexity of the algorithm.

Acknowledgment

The authors would like to thank to our supervisor, Artificial Intelligence Laboratory, School of Computing, Telkom University and those who has helping us.

References

[1] Maatta, J., Hadid, A., & Pietikainen, M. (2012). Face spoofing detection from single images using texture and local shape analysis. *Biometrics, IET*, *1*(1), 3-10.

[2] X. Tan, Y. Li, J. Liu, L. Jiang, "Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Mode," in *Proc. Of the 11th European conference on Computer vision*,2010,pp. 504-517.

[3] Komulainen, J., Hadid, A., & Pietikäinen, M. (2012, November). Face spoofing detection using dynamic texture. In *Computer Vision-ACCV 2012 Workshops*(pp. 146-157). Springer Berlin Heidelberg.

[4] Määttä, J., Hadid, A., & Pietikainen, M. (2011, October). Face spoofing detection from single images using micro-texture analysis. In *Biometrics (IJCB), 2011 international joint conference on* (pp. 1-7). IEEE.

[5] Wen, D., Han, H., & Jain, A. K. (2015). Face spoof detection with image distortion analysis. *Information Forensics and Security, IEEE Transactions on*,*10*(4), 746-761.

[6] de Freitas Pereira, T., Anjos, A., De Martino, J. M., & Marcel, S. (2012, November). LBP− TOP based countermeasure against face spoofing attacks. In *Computer Vision-ACCV 2012 Workshops* (pp. 121-132). Springer Berlin Heidelberg.

[7] C., Padraig, S.J., Delany. (2007, March). k-Nearest Neighbour Classifier. Technical Report UCD-CSI-2007-4.

[8] Kose, N., & Dugelay, J.,-L. Classification of Captured and Recaptured Images to Detect Photograph Spoofing.*Multi Media Department, EURECOM 2229*.

[9] Lahdenoja, O., Poikonen, J., & Laiho, M. (2013). Towards understanding the formation of uniform local binary patterns. *ISRN Machine Vision*, *2013*.

[10] Schuckers, S. A. (2002). Spoofing and anti-spoofing measures. *Information Security technical report*, *7*(4), 56-62.