COMPLETE LOCAL BINARY PATTERN AND SPATIAL STRUCTURE OF LIVE FACES

Sajida Parveen[1, 2], Sharifah Mumtazah[1, 3], Nadeem Naeem[1,4] ,Intesab Hussain[2], and Pardeep Kumar[2]
[1]Department of Computer and Communication Systems Engineering, Universiti Putra Malaysia (UPM), Serdang, Malaysia.
[2]Department of Computer Systems Engineering, Quaid-e-Awam Univertersity of Engineering, Science and Technology, Nawabshah, Pakistan.
[3]Wireless and Photonic Networks Research Centre of Excellence, Universiti Putra, Malaysia
[4]Department of Electronic Engineering, Quaid-e-Awam Univertersity of Engineering, Science and Technology, Nawabshah, Pakistan.
[*]Corresponding author: engr_sajida@hotmail.com

ABSTRACT: *The security of face biometric based systems should be resistance to presentation attacks. In these attacks the appearance of a face biometric sample is physically changed or replaced with a fake face. To overcome this security issue a robust method of complete modeling of local binary pattern operator for checking the face liveness is proposed in this paper. The research is based on analyzing the spatial structure of presented face in front of face biometric systems. The proposed method is evaluated on a publicly available NUAA face imposter database. And the comparison is conducted on a traditional Local texture descriptor known as Local Binary Pattern. The achieved results shows that the classification accuracy rate of our proposed method is outperform as compared to the local binary pattern.*

Keywords—Liveness checking; Texture analysis; Face biometrics; Local Binary Pattern LBP**.**

INTRODUCTION

Nowadays, personal identification by using biometrics has become more important in modern society. The main reason behind the popularity of such security measure is the use of more and more biometric based applications for personal computers. However, in spite of the significant development in recent research, biometric systems are still open and vulnerable to attacks such as face, fingerprint, iris and soft biometrics, which can be replaced with stolen or copied using physical characteristics of an individual person for personal identification. The security threat of face biometric occurs when someone presents a fake face of authorized person in front of their systems in order to get unauthorized access and advantages [1]. Currently there are a number of companies in the market which are providing security solutions based on face biometric authentication technologies. For instance, Lenovo, Asus and Toshiba Laptops launched in the market with an embedded face recognition system with built-in webcams. The presentation attacks such as photographs, video, 3D mask and makeup, or plastic surgery is being a major problem for the deployment of face biometric based systems at commercial and government sectors.

Thus, there is a need for efficient and reliable solutions for checking the face liveness against these attacks. To identify the liveness of a face from pattern characteristics of a facial skin is currently being under research. This research work is motivated by the increasing demand of reliable technique based on spatial structure analysis for checking liveness of the faces.

In this research work, the potential of Complete Local Binary Pattern (CLBP) [2] is explored in the field of spatial structure for checking the liveness of a human face. We carried out the experiments on a publicly available database known as NUAA dataset. Moreover, the evaluation of the proposed method and the comparison with Local Binary Pattern (LBP) [3] is also presented for benchmarking.

The rest of the paper is organized as follows. Section 2 provides a short review of texture based face liveness detection techniques. The proposed texture descriptor for calculating the feature vector is discussed in section 3. Experimental setup is discussed in Section 4. The evaluation and performance comparison of CLBP is carried out in Section 5. Concluding remarks are summarized in the last Section 6.

LITRATURE REVIEW

There are many approaches implemented in face liveness checking. In this section we discuss some of the most recent work in spatial structure analysis or pattern analysis.

The liveness detection method [4] was proposed based on the Fourier spectra. The research has been conducted on the idea that, the high frequency component of real face skin is greater than printed photos. The method differentiated fake faces from real faces by using Fourier spectra and demonstrated that the high frequency component was used to identify the structural information and the temporal changes that were calculated by an energy value of frequency domain of the attacked identity. The performance of this technique is limited due to the changing effects of illumination.

The surface properties of live human and imitated faces were analyzed in Lambtertian model [5], in which two extensions of the sparse logistic regression model for classification were developed. NUAA face imposter database was employed for research experiments. That database can be accessed on the internet for research purpose. This technique also found to be lacking in defending the attacks under different illumination conditions.

Furthermore, the identification of liveness from recaptured images on LCD display has been proposed in [6]. This method was designed to deal with lighting effects and contrast of the displayed image. Difference of Gaussian (DoG) filter and adaptive histogram equalization (CLAHE) was used respectively. Spatio-temporal information method is used on human face to distinguish live face from non-live face was developed [7]. A low level feature descriptor along with partial least squares regression is utilized in this research. The shape of the human face, its skin color and texture were considered during the experiments.

Recently, in face liveness detection, an efficient face detection method called Local binary Pattern (LBP) is introduced. This detection method serves as the basis and is now widely being used in liveness detection strategy.

Face liveness detection method based on LBP feature descriptor [8, 9] presented the approach that employed multiple resolution scheme in which a single descriptor from three orthogonal planes of Local Binary Pattern (LBP-TOP) were used to combine the space and time information. Another variation of LBP that is known as Local Binary Pattern Variance (LBPV) [10] was proposed for liveness detection of captured and recaptured images. The characteristics of texture and contrast were considered in this feature descriptor. Later on, the extension of LBP known as Local Graph Structure (LGS) [11] was introduced. Local graph structure has a slightly different way as compared to the other LBP extensions. In LGS, six pixels are utilized to form the neighbors of the target pixel while in the LBP eight pixels that are used in clockwise direction.

Moreover, a recent scheme based on image distortion analysis (IDA) [12] for face liveness detection was proposed in which four different features were extracted i.e. spatial reflection, blurriness, chromatic moment and color diversity. The authors adopted LBP operator to make the IDA feature vector. Similarly, a multiscale directional transform has been demonstrated [13] for feature extraction. Another weber's law based extended version was introduced for discriminating the spoof and liveness features in face images [14].

Review of literature shows that Local Binary Pattern and its variants are mostly used in numerous skin texture analysis based schemes for face liveness checking [15]. LBP operator can be defined as a rotation invariant grayscale measure. This method is known to be a simple and efficient texture operator. The operation of LBP works on 3 × 3 pixel block consisted of eight neighborhood pixels and converting their values into the binary 0 or 1 by comparing with the value of their center pixel of the pattern. The achieved binary numbers are encoded and converted into decimal numbers as shown in the Figure 1. As the neighborhood, which is consisting of 8 pixels, a total of $2^8 = 256$ different labels can be obtained depending on the relative gray values of the center and the pixels in the neighborhood.

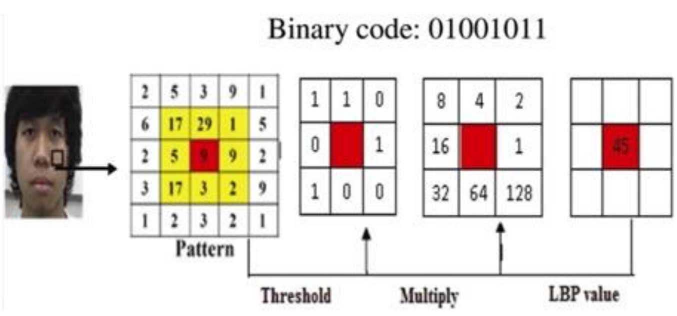

Fig 1. Image sample with Local Binary Pattern (LBP) operator calculation [15]

MATERIAL AND METHODS

The Complete model of Local binary Pattern [2] was proposed to improve the performance of LBP. It is clearly observed in *equation 2* that LBP only considers the sign of the difference of two pixels. This means some of the information is loss by means of magnitude. To consider maximum information from the micro texture patch authors developed a method that was based on two components: the sign component and the magnitude component. This can be defined as:

$$s_x = (a_p - a_c), \quad m_x = (a_p - a_c) \qquad (1)$$

Where s_x is used to calculate CLBP sign component and m_x is used to calculate CLBP magnitude component. The CLBP sign component is the same as of LBP, whereas the CLBP magnitude measures the local variance of magnitude. Both components can be used to build final feature map for the original image. This can be shown in below expression:

$$I_x = s_x \times m_x \qquad (2)$$

$$\begin{cases} s_x = sign(I_x) \\ m_x = |I_x| \end{cases} \qquad (3)$$

In this paper, we have introduced the Complete Local Binary Pattern (CLBP) operator for face liveness checking. CLBP sign component and CLBP magnitude component produce binary strings for feature calculation. Therefore, both of the components can be used together for spatial structure or pattern classification. After getting sign and magnitude feature vector separately on the single image, the histogram is calculated by concatenates both in a single histogram. Then for classification linear Support Vector Machine (SVM) classifier is used to classify the original faces from fake faces.

EXPERIMETNAL SETUP

In this section, the experiment is performed to evaluate the proposed CLBP on NUAA dataset [5]. The NUAA frontal face test set is among the most commonly used datasets for assessment of liveness testing performance. This dataset is composed of 500 images of 15 subjects in three sessions. Some variations in terms of lighting, environmental and rotations of photographs are introduced in this dataset. The dataset contains 12614 images of original client accesses and photo attacks. Some of the images from the dataset are shown in Figure 2. These images have been pre-classified into two separate sets of training and testing purposes of real and imposter images. Two independent datasets were further derived from these two datasets. Each one is used for training and testing purpose.

For performing numbers of experiments in this research work, the different sizes for training and testing sets is derived from two basic datasets of imposter and original sets. These are chosen randomly in all our conducted experiments. These datasets are summarized in table 1. The number of experiments is classified into three type of methods named as: *Method (a), Method (b) and Method (c)*

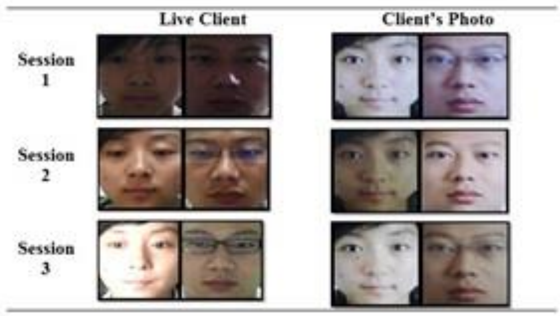

Fig. 2. Examples from NUAA dataset [5]

Table 1. Datasets for Different Experiments

Method	Test Methods	Real Train datasets	Imposter Train datasets	Real Test datasets	Imposter Test datasets
a	*xperiment 1*	1743	1748	3362	5761
b	*xperiment 2*	1000	1000	1000	1000
	xperiment 3	1500	1500	1500	1500
	xperiment 4	2000	2000	2000	2000
c	*xperiment 5*	1000	1000	1500	1500
	xperiment 6	1000	1000	2000	2000
	xperiment 7	1000	1000	2500	2500
	xperiment 8	1000	1000	3000	3000

Method (a): only consist on *Experiment 1*, in which the training set consists of images from the first two sessions only. The test set consists of the images from the remaining third session. Three different values of neighbors (*P)* and radius (*R)* are adopted for *Experiment 1* to calculate the feature vector.

To increase the level of difficulty, the database is further split for remaining two test methods, by developing equal and increased test datasets.

Method (b): is consisted on *Experiment 2*, *Experiment 3 and Experiment 4*, the equal size of dataset is used for training and testing with different three values of 1000, 1500 and 2000 respectively. Moreover, in *Method (c)*, the experiments are performed by using constant training set that is 1000 and increasing the testing data set from 1500 to 3000 by adding 500 in each from *Experiment 5 to Experiment 8.*

RESULTS AND DISCUSSION

Method (a)

According to calculated results of *Experiment 1* on NUAA database, it is confirmed that our proposed face liveness testing method is more resistance to the challenges in terms of illumination in photograph based attack. The obtained results are summarized in Table 2. Complete Local Binary Pattern (CLBP) gives the very good classification rate in contrast with the traditional LBP scheme at the number of neighbors 24 and radius 3 as shown in Table 2. We can see that CLBP outperforms in all cases in terms of all radiuses 1, 2 and 3 as shown in Fig 3.

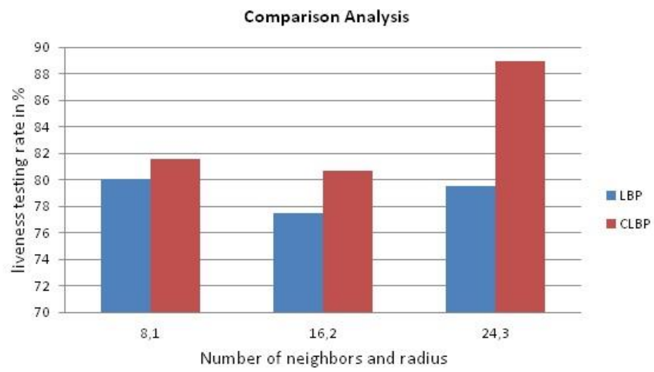

Fig. 3. Performance comparison of CLBP and LBP operator

Table 2. Liveness Checking accuracy on NUAA dataset.

Techniques	P=8,R =1	P=16.R=2	P=24, R=3
Accuracy with LBP	80.1	77.4382	79.5040
Accuracy with CLBP	81.6	80.6908	88.9684

Method (b)

The equal train and test datasets are used for Experiment 2, Experiment 3 and Experiment 4 in this test method. Table 3 shows the accuracy rate of the three experiments with LBP and CLBP by using the SVM classifier. Again, when compared with LBP, one can observe the clear increases of performances, i.e. over 14% increase in average, on all three experimental datasets.

Table 3. Achieved results on Equal datasets

Techniques		Experiment 2	Experiment 3	Experiment 4
Train data		1000	1500	2000
Set data		1000	1500	2000
Accuracy rate (%)	LBP	84.6	76.96	78.25
	CLBP	96	94.89	90.95

Method (c)

The calculated results in method (c), form the Table 4 it is shown that our proposed method improves the accuracy rate on average by 12.33% over LBP.

Table 4. Achieved results on increasing test datasets

Techniques		Experiment 5	Experiment 6	Experiment 7	Experiment 8
Train data		1000	1000	1000	1000
Test data		1500	2000	2500	3000
Accuracy rate (%)	LBP	91.13	88.76	75.09	68.39
	CLBP	93.72	89.43	95.22	94.35

Using CLBP texture descriptor, we obtain a clear margin of the performance superiority over traditional method. The best performance of 96% is obtained with the equal size data set in the second experiment, superior to 84.6% with LBP. The comparative performance shows that how various datasets affect the performance of features calculated by LBP and CLBP. In general, the CLBP surprisingly performed well for face liveness checking and show its effect in increasing accuracy rates for the entire number of experimental results in Fig 4.

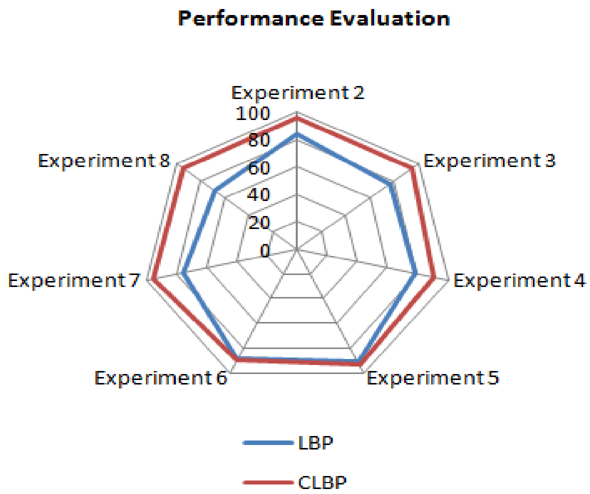

Fig. 4. Comparative performance analysis of Complete Local Ternary pattern with Local binary pattern by using different datasets in different experiments

CONCLUSION

A robust face anti spoofing method based on Complete Local Binary Pattern (CLBP) for face liveness checking was presented in this research paper. In which the image feature vector is decomposed and calculated through sign and magnitude components. An experimental support is given on a most popular publicly available NUAA test dataset in order to calculate the best spatial structure information about fake faces. The final feature vector is achieved by joining both components into the one histogram. The achieved result shows that our proposed method has high classification rate for testing live and non-live faces.

REFERENCES

1. K. A. Nixon, V. Aimale, and R. K. Rowe, "*Spoof detection schemes",* In *Handbook of biometrics*, pp. 403-423. Springer US, 2008.
2. Z. Guo, L. Zhang, and D. Zhang, "A completed modeling of local binary pattern operator for texture classification", *Image Processing, IEEE Transactions on* 19, no. 6, pp. 1657-1663, 2010.
3. T. Ojala, M. Pietikäinen, and T. Mäenpää, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 24, no. 7, pp.971-987, 2002.
4. J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra", In *Defense and Security*, pp. 296-303. International Society for Optics and Photonics, 2004.
5. X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model", In *Computer Vision–ECCV 2010*, pp. 504-517. Springer Berlin Heidelberg, 2010.
6. B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions", In *Image Processing (ICIP), 2011 18th IEEE International Conference on*, pp. 3557-3560. IEEE, 2011.
7. W. R. Schwartz, A. Rocha, and H. P. Edrini, "Face spoofing detection through partial least squares and low-level descriptors", In *Biometrics (IJCB), 2011 International Joint Conference on*, pp. 1-8. IEEE, 2011.
8. J. Määttä, A. Hadid, and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis", In *Biometrics (IJCB), 2011 international joint conference on*, pp. 1-7. IEEE, 2011.
9. T. D. F. Pereira, A. Anjos, J. M. D. Martino, and S. Marcel, "LBP-TOP based countermeasure against face spoofing attacks", In *Computer Vision-ACCV 2012 Workshops*, pp. 121-132. Springer Berlin Heidelberg, 2013.
10. N. Kose, and J. L. Dugelay, "Classification of captured and recaptured images to detect photograph spoofing", In *Informatics, Electronics & Vision (ICIEV), 2012 International Conference on*, pp. 1027-1032. IEEE, 2012.
11. K. B. Housam, S. H. Lau, Y. H. Pang, Y. P. Liew, and M. L. Chiang, "Face spoofing detection based on improved local graph structure", In *Information Science and Applications (ICISA), 2014 International Conference on*, pp. 1-4. IEEE, 2014.
12. D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis." *Information Forensics and Security, IEEE Transactions on* 10, no.4, pp. 746-761, 2015.
13. Feng, L., Po, L.M., Li, Y. and Yuan, F., 2016. Face liveness detection using shearlet-based feature descriptors. *Journal of Electronic Imaging*, *25*(4), pp.043014-043014.
14. Parveen, S., Ahmad, S.M.S., Abbas, N.H., Adnan, W.A.W., Hanafi, M. and Naeem, N., 2016. Face Liveness Detection Using Dynamic Local Ternary Pattern (DLTP). *Computers*, *5*(2), p.10.
15. S. Parveen, S. M. S. Ahmad, M. Hanafi and W. A. W. Azizun, "Face anti-spoofing methods", *Current Science (00113891)*, vol. *108, no.* 8, pp.1491-1500, 2015.