Face Spoofing Detection Using Local Graph Structure

Housam Khalifa Bashier, Lau Siong Hoe, Pang Ying Han, Liew Yee Ping and Chiang Mee Li

Faculty of Information Science and Technology Multimedia University, 75450 Melaka, Malaysia
me.the.fren@gmail.com, {lau.siong.hoe & yhpang}@mmu.edu.my, {lyping8 & jacalinechiang}@yahoo.com

Abstract - Face spoofing attack is one of the recent security traits that face recognition systems are proven to be vulnerable to. The spoofing occurs when an attacker bypass the authentication scheme by presenting a copy of the face image for a valid user. Therefore, it's very easy to perform face recognition spoofing attack with compare to other biometrics. This paper, addresses the problem of detecting imposter face image from live image. In practically, we address this problem from texture analysis point of view because the printed face usually has less quality defect that can be observed by extracting texture features. We adopt Local graph structure LGS to extract the features. Moreover, LGS is based on applying a dominant graph into the input image and it's proved to be a powerful texture operator. Finally, extensive experimental analysis on NUAA showed an encouraging performance.

Index Terms - Local Graph Structure, image processing, pattern recognition, face recognition, face spoofing.

1. Introduction

Face recognition systems become very popular in recent years. This is because there's a significant improvement in the algorithms with compare to other biometric measures. Face recognition is a straightforward, natural and nonintrusive. In order to achieve a very good performance, researchers suggested that the face needs to be a frontal and normalized [1]. Moreover, pose and illumination have proved to be a very challenging problem for research [1-2].

However, spoofing attack considered to be a security threat for face recognition applications. Authors in [3] define the spoofing attack as outwitting a biometric sensor by presenting a counterfeit biometric evidence of a valid user. This attack is a very straight forward, the attacker just presents the copy of the picture in front of the sensor and it does not needs a previous knowledge about the recognition scheme. Furthermore, most of the face recognition algorithms designed to identify and verify the user who wants to gain access without concerning whether the input data is live or not. Despite the existence of a very sophisticated biometric authentication and verification systems nowadays, implementing anti-spoofing schemes for them is still in its infancy.

At university of Hanoi 2009, researchers in security and vulnerability have has shown that how an attacker can easily spoof a face recognition algorithm at black hat conference. In addition, national institute of standards and technology (NIST) have listed this thread in the national vulnerability database. the On the other hand , face images captured from printed photos look similar to the image where captured directly from the sensor as shown in Fig. 1.

The first row shows real face images where the second row shows fake face image from NUAA database. As we can see, there's no difference between fake face image and real image when we simply look at images. However, if we look from image quality assessment point of view then there's a difference in the texture data.

To cope with these problems, we adopt local graph structure to tackle the problem of detecting fake facial biometric data.

The remaining part of this paper is organised as follow. Section II shows the Literature review. LGS for face spoofing is proposed in III. Experimental and Results are carried out In Section IV. Finally, in IV conclusions are drawn.

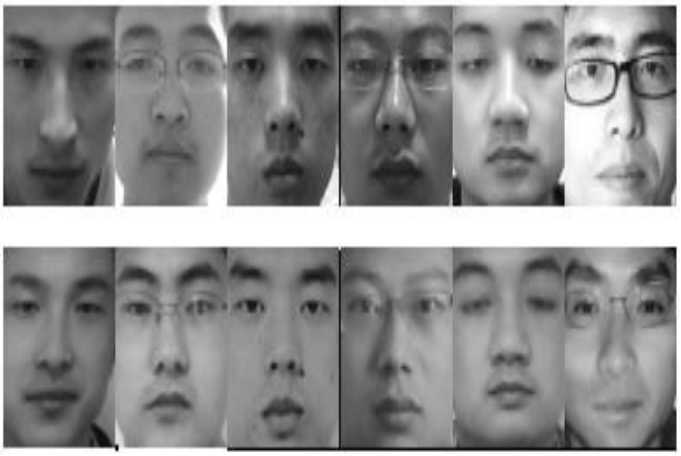

Fig. 1 Live Face vs. Imposter Face (Row1. Live Face, Row2. Imposter Face)

2. Related Work

Most of the state of the art algorithms in face recognition are basically vulnerable to spoofing attack and this is due to the fact that; face algorithms are based on discriminating the face features from each other and furthermore reduce feature dimension. Moreover, using a simple photograph of the enrolled user's face displayed using a cell phone, screen or a hard copy can easily fool the algorithm. Few papers discuss the research against spoofing attack [4, 5].

Furthermore, researcher study detecting facial expression changes, blinking, and mouth movement for face liveness detection. Pan et al [4] proposed an algorithm to detect face liveness by observing the blinking every4-5s. His algorithm counts the number of blink and then makes a decision. Another researchers, proposed a method that uses optical-flow to track the movements of facial face [6, 7].

Face spoofing problem can be solved based on analysing the face skin proprieties for instance skin reflectance and skin texture. As an example, authors in [8] proposed to detect print-attack face spoofing. Their concept is based on the statement

that the printed-face has smaller high frequency component with compare to live face image. Fourier transform is used to analyse the input data. Generally speaking, this algorithm may work for down-sampled picture while on the other hand it fails for high quality images.

Recently, Tan et al proposed a considerable work which utilizes the lambertian reflectance in order to discriminate between printed face and real face (2dimension vs. 3dimension) [9]. Therefore, the algorithm uses variational retinas-based and difference of Gaussian to extract latent reflectance features. The results reported in their research are quite good. The database used for this study is NUAA photograph imposter which is publically available [9]. Therefore, our research is carried out using this database.

On the other hand, Local graph structure is proposed by Eimad et al. [10] for face recognition. Many applications have been considered in the literature such face tracking, recognition, plant identification and others extensions of LGS [11-15] but none of them have paid attention to use LGS for face anti-spoofing. Hence, our target in the study is to implement LGS for face anti-spoofing.

3. Local Graph Structure

The concept of Local Graph Structure is introduced by Eimad et al [10] in 2011. The idea is to form a strong relationship between a given targe pixel I(x,y) and its neighbours. As stated in the paper, having a dominating graph with six pixels forming the graph is sufficient to represent the graph relationship. Moreover, LGS is found to be a very powerful texture operator with compare to the local binary pattern LBP. Further, LGS is robust to montic gray scale changes.

LGS utilize six pixels to form the neighbours of target pixel I(x,y) . Then we start finding the pattern by moving anti-clockwise for the target pixel I(x,y) for the left region of the graph. If a neighbour pixel has a high or equal gray value than the target I(x,y) 0 then assign a binary value equal to 1 on the edge connecting the two vertices, else 0.

Next is to process right region of the dominant graph, the process here is the same as the left region. The only difference here is we have to move first horizontal and then continue in clockwise as shown in Fig. 2.

To produce the LGS for pixel (xd, yd) a binomial weight 2p is assigned to each sign s(gd – gn). These binomial weights are summed:

$$LGS(x_d, y_d) = \sum_{K=0}^{7} s(g_d - g_n)2^p \qquad (1)$$

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

Where $p = 7.\ p = 7,6,...0.$

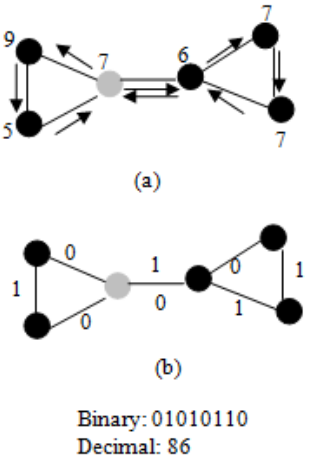

Fig. 2 Local Graph Structure (a. Direction, b. Binary)

Our Proposed solution starts first by converting the input facial image I(x,y) into gray-scale. Next step is to extract the LGS features for I(x,y). Once LGS processed the facial data we need to calculate the histogram in order to reduce the feature dimension. Finally nearest neighbour classifier with cosine measure is used to find the nearest class. Please see Fig. 3.

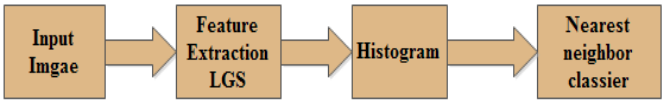

Fig. 3 Proposed algorithm

4. Experiments and Results

In this section, we evaluate our proposed algorithm to detect spoofed faces. The aim of our experiments is to prove that LGS can also be used to detect fake facial data. Fig. 4 shows the initial experiment of face anti-spoofing using LGS and histogram of the LGSs for original image and a new generated one. Moreover, histogram of LGSs image representing the distribution of 256 patterns across the facial image is also shown in Fig. 4.

A. Database

To evaluate the performance of LGS with compare to LBP, NUAA photographer imposter database [9] is used.

The database contains 9000 pictures for real and imposter faces. The high quality photo attacks were recorded using a webcams at 20 fps. The resolution used for the experiments is 252 x 252 pixels. Moreover, the face images of live humans and the photographs were collected in three sessions at intervals of about 2 weeks. In addition, the environmental and illumination condition are changing.

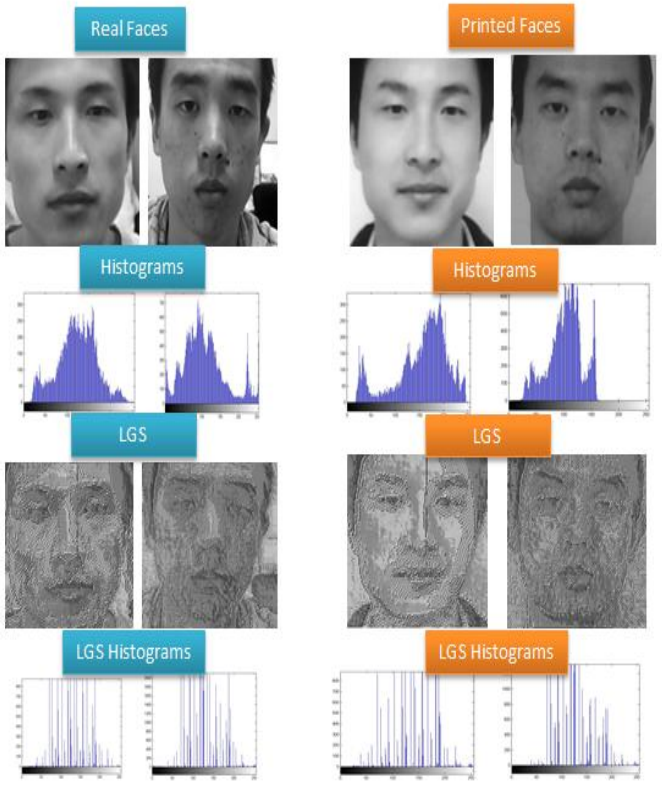

Fig. 4 LGS processing

B. *Experimental Results*

To assess the performance of LGS in detecting spoofed faces, we implemented and compared Local Graph Structure performance with Local Binary Pattern [16]. We have divided the images into training and testing. The experiments results including detection rate and error rate for different training size are tabulated in Table 1 and 2.

TABLE 1 Performance Comparison of Different Training Samples LBP

	Train Real	Train Imposter	Test Real	Test Imposter	Detection Rate	Error Rate
Experiment 1	3250	3250	1500	1500	93.06	6.94
Experiment 2	3400	3400	1500	1500	93.13	6.87
Experiment 3	3500	3500	1500	1500	93.16	6.84

Table 1 shows the first experiment which is to evaluate Local Binary pattern and results reported that LBP performance drops as we decrease the training samples.

Second experiment as shown in Table 2 is to evaluate LGS against detecting spoofed facial picture. The first thing to notice is LGS performance is better than LBP. Second thing is we can observe that as we increase the training samples the detection rate is stable and there's no drop. Furthermore, Table 3 shows the overall performance for both methods.

TABLE 2 Performance Comparison of Different Training Samples LGS

	Train Real	Train Imposter	Test Real	Test Imposter	Detection Rate	Error Rate
Experiment 1	3250	3250	1500	1500	94.53	5.47
Experiment 2	3400	3400	1500	1500	94.53	5.47
Experiment 3	3500	3500	1500	1500	94.53	5.47

TABLE 3 Overall Recognition Rate

Algorithm	Detection Rate
LBP	93.11
LGS	(4.53

The results showed that the Local Graph Structure (LGS) outperforms Local Binary Pattern (LBP) significantly. Even though we cannot keep 100% performance as shown in the Fig. 5.

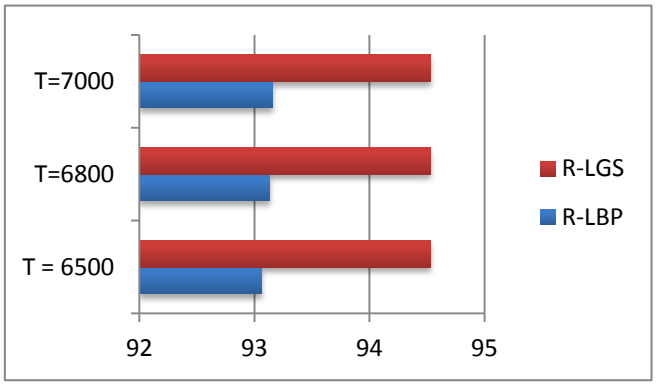

Fig. 5 LGS vs. LBP

5. Conclusions

Face spoofing and anti-spoofing becomes a very important topic for face recognition system. Even though face recognition algorithms are sophisticated; it should be impossible to rely on an algorithm without a protection against spoofing attacks.

The contribution of the research study can be summarized into. Firstly, we study the use of local graph structure against spoofing protection for face recognition. Secondly, performance evaluation against different training size is reported in order to measure the robustness of LGS. Finally LGS is simple, reliable with compare to LBP.

Acknowledgment

The authors acknowledge the financial support of Telekom Research and Development Sdn. Bhd. of Malaysia.

References

[1] P. J. Phillips , P. Grother , R. Michaels , D. Blackburn , E. Tabassi and M. Bone, "Facial Recognition Vendor Test 2002: Evaluation report", 2003.

[2] R. Gross, S. Baker, I. Matthews, T. Kanade, "Face Recognition Across Pose and Illumination, Chapter 9, Handbook of Face Recognition", Stan Z. Li and Anil K. Jain (Eds.), *Springer-Verlag*, 2004.

[3] Chingovska, Ivana, André Anjos, and Sébastien Marcel. "On the effectiveness of local binary patterns in face anti-spoofing." *BIOSIG-Proceedings of the International Conference of the. IEEE*, 2012.

[4] Pan, G., Wu, Z., & Sun, L., "Liveness detection for face recognition",.*Recent advances in face recognition*, 2008, pp. 236-252.

[5] Nixon, K. A., Aimale, V., & Rowe, R. K., "Spoof detection schemes", *InHandbook of biometrics*, *Springer US*, 2008, pp. 403-423.

[6] Kollreider, K., Fronthaler, H., & Bigun, J., "Non-intrusive liveness detection by face images", *Image and Vision Computing*, 2009, 27(3), pp. 233-244.

[7] Bao, W., Li, H., Li, N., & Jiang, W., "A liveness detection method for face recognition based on optical flow field", *In Image Analysis and Signal Processing IEEE, 2009*, 2009, pp. 233-236.

[8] Li, J., Wang, Y., Tan, T., & Jain, A. K., "Live face detection based on the analysis of fourier spectra", *In Defense and Security*, *International Society for Optics and Photonics*, 2004, pp. 296-303.

[9] Xiaoyang Tan, Yi Li, Jun Liu, Lin Jiang, "Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model.ECCV", 2010, pp. 504-517.

[10] Eimad Abusham, Housam Khalifa,"face recognition using local graph structure". *Hcii11 Proceedings of the 14th international conference on Human-computer interaction: interaction techniques and environments*, 2010, pp. 169-175.

[11] Abusham, E. E. A., Bashier, H. K., Khalid, F., Sayeed, S., Hossen, J., & Kalaiarasi, S. M. A, "Illumination Normalization using Eimad-housam Technique", *Trends in Applied Sciences Research*, 2012, 7(8).

[12] HK Bashier, E. Abdu Abusham and F. Khalid, "Face Detection Based on Graph Structure and Neural Networks" *Trends in Applied Sciences Research*, 2012, 7(8), pp. 683-691.

[13] Abusham, E. E. A., & Bashier, H. K, "Face recognition using local graph theory (LGT)", *In Computing, Electrical and Electronics Engineering (ICCEEE), International Conference, IEEE*, 2013, pp. 593-596.

[14] Khalifa Bashier, H., Eldin Abusham, E., Azli Abdullah, M., Liew Tze, H., Yusof, I., & Lau Siong, H., "Real Time Face tracker based on Local Graph Structure Threshold (LGS-TH)", *Australian Journal Of Basic & Applied Sciences*, 2013, 7(2), pp. 632-638.

[15] S. Sayeed, I. Yusof, H.K. Bashier,, E., J. Hossen, 1M. Fikri Azli A. "Real Time Face tracker based on Local Graph Structure Threshold (LGS-TH)", *Australian Journal Of Basic & Applied Sciences*, 2013, 7(2), pp. 632-638.

[16] T. Ojala, M. Pietikäinen, and T. Mäenpää, Multiresolution, "Gray-scale and Rotation Invariant Texture Classification with Local Binary Patterns", *IEEE Trans. Pattern Analysis and Machine Intelligence*, 2002, 24(7): pp. 971-987.