Face spoofing detection based on improved local graph structure

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

Faculty of Information Science & Technology, Multimedia University, Jalan Ayer Keroh Lama,75450,Melaka Malaysia
me.the.fren@gmail.com

***Abstract*— Face spoofing attack is one of the recent security problems 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 a face recognition spoofing attack with compare to other biometrics. This paper, presents a novel and efficient facial image representation for face spoofing called improved local graph structure (ILGS). We divide the input facial image into several regions and then we calculate local graph structure (LGS) codes for each region. On the other hand, the histograms are concatenated into an enhanced feature vector to detect spoofed facial image. Finally, performance of the proposed method is evaluated on the NUAA database.**

***Index Terms*— local graph structure, texture analysis, pattern recognition, liveness detection, face recognition, face spoofing.**

I. Introduction

Nowadays, there's a significant improvement in developing face recognition algorithms with compare to other biometrics measures. The reason behind this development is because the process of developing face recognition algorithm is nature, nonintrusive and straightforward. On the other hand, studies reported that faces need to be frontal and normalized in order to achieve an acceptable performance [1]. Furthermore, pose and illumination have proved to be very challenging problems for research [1-2].

However, there's an unpaid attention to spoofing attack which is considered to be a security threat for face recognition schemes. The spoofing attack can be defined as outwitting a biometric sensor by presenting a counterfeit biometric evidence of a legitimate user [3]. Therefore, the spoofing attack is very straightforward; this is means that the attacker just needs to present a copy of a valid facial data for a legitimate user in front of the sensor without a prior knowledge about the recognition algorithm. On the other hand, the method simply accepts the input facial data and then pass the data to the pre-processing, feature extraction and classification methods.

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 lab have 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 issue in the national vulnerability database.

On the other hand , face images captured from printed photos look similar to the images where captured directly from the sensor as shown in the below figure.

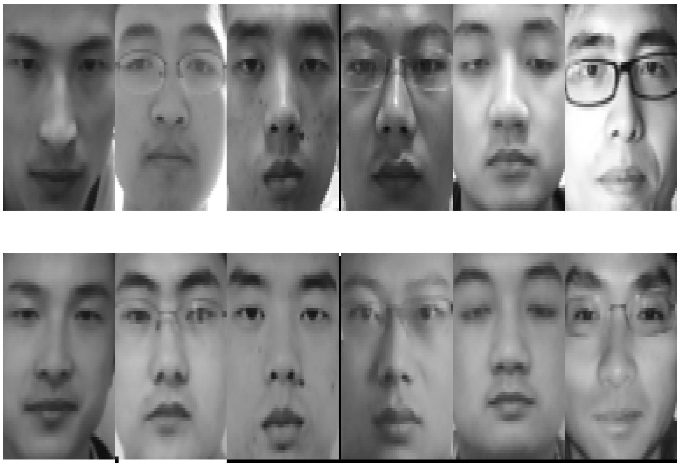


Figure 1: Live Face vs. Imposter Face (Row1. Live Face, Row2. Imposter Face)

The first row shows real face images where the second row shows fake face image from NUAA database. There's no a clear difference between real face pictures and imposter face pictures. However, there's a difference between the two rows when we look at the images from textures point of view.

To cope with this problem, we present a novel descriptor for facial image spoofing based on local graph structure; the features are extracted from the local facial image regions in order to tackle the problem of detecting fake facial biometric data. Our goal is to detect the spoofed face image from texture analysis point of view.

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

II. Related Work

In general, the state of the art schemes for face recognition applications are vulnerable to spoofing attack. This is because of two facts; 1) algorithms are developed for discriminating features and 2) dimensionality reductions and classifications.

Therefore, using a copy of the legitimate user facial data obtained from a photograph, mobile phone or picture displayed on a screen can easily fool the face recognition

978-1-4799-4441-5/14/$31.00 ©2014 IEEE

algorithm. Researchers carried out studies to solve this issue in [4, 5].

The problem of face spoofing detection can be solved by analysing facial expression changes, blinking and mouth movement. In addition, Pan et al [4] proposed a method to identify liveness by observing the blinking every4-5s. His algorithm counts the number of blinks 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. For instance, authors in [8] proposed to detect print-attack face spoofing. Their concept is based on the statement that the printed-face has a 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 pictures 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. In addition the database used for this study is NUAA photograph imposter which is publically available [9].

Moreover, it's very important to find a good descriptor for the appearance of local facial image regions. Ideally, we need to find facial descriptors that are easy to compute and a descriptor that is robust to changes in illuminations and others factors.

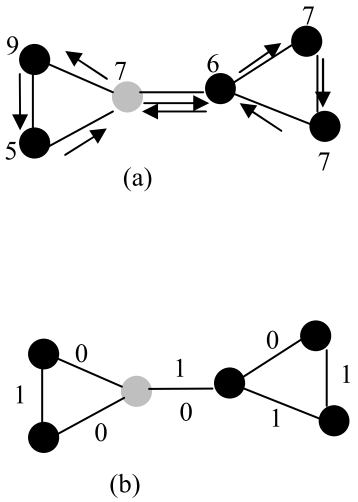
On the other hand, Local graph structure is proposed by Eimad et al [10] for face recognition. Many applications have been considered in the literature such as face tracking, recognition, plant identification, face spoofing and others extensions of LGS [11-16].

III. Improved Local Graph Structure

LGS is introduced by eimad et al in [10], the idea is to form a strong relationship between a given target 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 utilizes six pixels to form the neighbours of target pixel I(x, y) in gray color as shown in the below figure. 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) then assign a binary value equal to 1 on the edge connecting the two vertices, else 0.

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



Binary: 01010110
Decimal: 86

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

In this work, the LGS presented in the above section is used as a facial descriptor for liveness detection. The goal of our method is to calculate several local descriptors for the facial image and then combining them into a global descriptor. The reason is that local features are better than the holistic representation.

In general, the input facial image is divided into several local regions followed by applying LGS in each region to extract the texture information. Then concatenate the result from each region to form one feature vector.

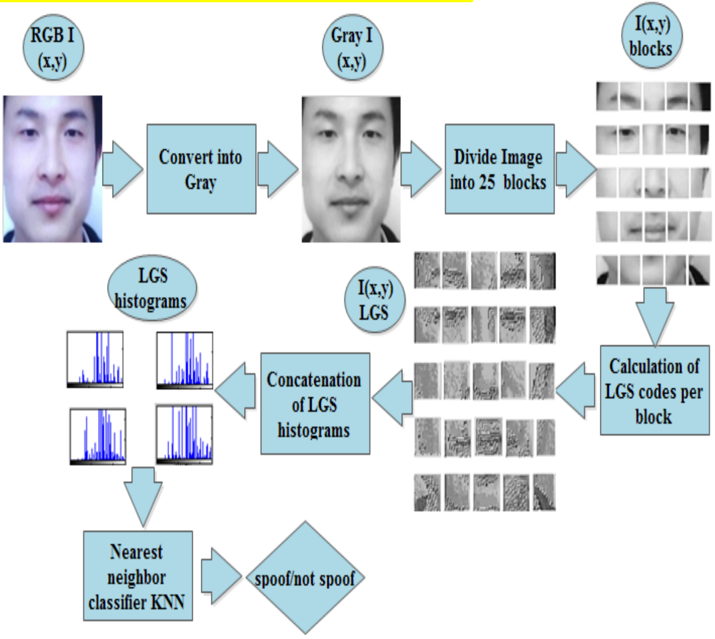

RGB I (x,y)
Convert into Gray
Gray I (x,y)
Divide Image into 25 blocks
I(x,y) blocks
Calculation of LGS codes per block
I(x,y) LGS
Concatenation of LGS histograms
LGS histograms
Nearest neighbor classifier KNN
spoof/not spoof

Figure 3: Proposed ILGS.

The method starts first by converting the input image I(x,y) into gray. Next is to divide the image into 25x25 blocks; we have found that this number is sufficient to represent the local description for each region. ILGS codes for each region are calculated as shown in figure 3. The histogram for each region encodes both the appearance and the spatial relation is computed. Moreover, the histograms for k facial region R0, R1… Rm-1are concatenated into one histogram yielding ILGS. Finally nearest neighbour classifier with cosine measure is used to classify the input facial data. Therefore, the texture description of a single region describes the appearance of the region and the combination of all region descriptions encodes the global geometry of the face.

IV. Experiments And Results

In this section, we compare ILGS performance with LGS and LBP.

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 130 x 130 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.

B. Experimental Results

To assess the performance of ILGS, The training sets are divided into real facial data and imposter facial data. The rest of the samples we used for testing and evaluation. The experiments results including detection rate and error rate for different training size for LBP [17] are shown in table 1.

TABLE 1
PERFORMANCE COMPARISONS OF DIFFERENT TRAINING SAMPLES (LBP)

	Train real	*Train Imposter*	*Test Real*	*Test Imposter*	*Detection Rate*	*Error Rate*
Experiment1	3250	3250	1500	1500	93.06	6.94
Experiment2	3400	3400	1500	1500	93.13	6.87
Experiment3	3500	3500	1500	1500	93.16	6.84

Table 1 shows the first experiment which is to evaluate Local Binary pattern and the results reported that LBP performance drops as we decrease the training samples.
Next experiment is to evaluate LGS [16] against detecting spoofed facial pictures as shown in table2. 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 is stable. On the other hand ILGS performs quite better with compare to LGS and LBP as shown in table 3. This means that 25x25 is sufficient to detect spoofed faces from the real ones. Therefore, ILGS using local regions works well and produces better detection rate. In this way we can easily encodes the global geometry of the facial data and use it for face recognition also. In addition, the over detection rate is shown in table 3.

TABLE 2
PERFORMANCE COMPARISONS OF DIFFERENT TRAINING SAMPLES (LGS)

	Train real	*Train Imposter*	*Test Real*	*Test Imposter*	*Detection Rate*	*Error Rate*
Experiment1	3250	3250	1500	1500	94.53	5.47
Experiment2	3400	3400	1500	1500	94.53	5.47
Experiment3	3500	3500	1500	1500	94.53	5.47

TABLE 3
PERFORMANCE COMPARISONS OF DIFFERENT TRAINING SAMPLES (ILGS)

	Train real	*Train Imposter*	*Test Real*	*Test Imposter*	*Detection Rate*	*Error Rate*
Experiment1	3250	3250	1500	1500	99.36	0.64
Experiment2	3400	3400	1500	1500	99.40	0.60
Experiment3	3500	3500	1500	1500	99.33	0.67

TABLE 3
OVERALL DETECTION RATE

Algorithm	***Detection Rate***
LBP	**93.11**
LGS	**94.53**
ILGS	**99.36**

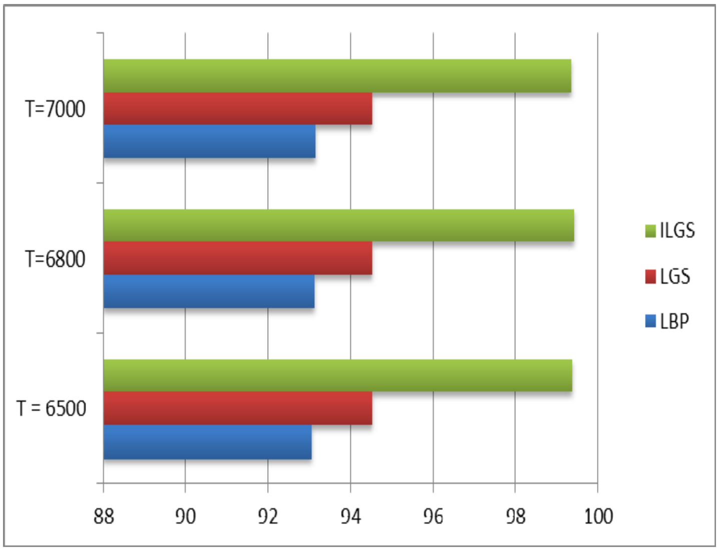


Figure 4: Performance

The results showed that the ILGS outperforms LBP [17] and LGS [16] significantly as shown in the above figure. Furthermore, T represents the number of training samples.

V. Conclusions

Face spoofing is 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 this research can be summarized into. Firstly, we studied the problem from texture analysis point of view and then we presented a new method based on dividing the input facial data into small regions. Next is to compute a description of region using local graph structure. The results of LGS are then combined into a spatially enhanced feature vector. Secondly, performance evaluation against different training size is reported in order to measure the robustness of ILGS.

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." Biometrics Special Interest Group (BIOSIG), 2012 BIOSIG-Proceedings of the International Conference of the. IEEE, 2012.

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

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

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

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

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

[9] Xiaoyang Tan, Yi Li, Jun Liu, Lin Jiang: Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model.ECCV (6) 2010: 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 environments2010- Volume Part II Pages 169-175

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

[12] Bashier, H. K., Abusham, E. A., & Khalid, F. (2012). Face Detection Based on Graph Structure and Neural Networks. Trends in Applied Sciences Research, 7(8).

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

[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, 7(2), 632-638 (2013)..

[15] Sayeed, S., Yusof, I., Bashier, H. K., Hossen, J., & Azli, M. A. (2013). Plant Identification Based on Leaf Shape and Texture Pattern Using Local Graph Structure (LGS). Australian Journal of Basic & Applied Sciences, 7(11).

[16] Bashier, H. K., Lau, S. H., Han, P. Y., Ping, L. Y., & Li, C. M. (2014, January). Face Spoofing Detection Using Local Graph Structure. In 2014 International Conference on Computer, Communications and Information Technology (CCIT 2014). Atlantis Press.

[17] 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* 24(7): pp. 971-987, 2002.