ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 6, June 2016

AN EFFICIENT DEVELOPMENT OF FACE SPOOFING DETECTION METHOD USING IMAGE DISTORTION ANALYSIS

Dr.B.CHELLAPRABHA[1], S. MENAKA[2]

[1]Professor &Head, SNS College of Engineering, Coimbatore, India.

[2]ME Scholar, SNS College of Engineering, Coimbatore, India

ABSTRACT

In recent years face recognition has been the important factor in biometric authentication. Significant progress has been made in the area of face spoofing detection. In practical application, the problem of spoofing attacks can be threatened to face biometric systems which is used for authentication. Kernel Discriminate Analysis(KDA) is effective in detecting the face spoofing detection. Kernel Discriminate Analysis uses two techniques, MultiScale Binarized Statistical Image Features on Three Orthogonal Planes (MBSIF-TOP) and MultiScale Local Phase Quantization on Three Orthogonal Planes(MLPQ-TOP).MBSIF-TOP is effective in detecting spoofing attacks, showing promising performance compared to existing alternatives. Next, by combining MBSIF-TOP with a blur-tolerant descriptor, namely Multiscale Local Phase Quantization representation (MLPQ-TOP), the robustness of the spoofing attack improved. The fusion of the information provided by MBSIF-TOP and MLPQ-TOP is realized via a kernel fusion approach based on a kernel Discriminant Analysis technique. But it avoids the costly eigen analysis computations by solving the KDA problem, So it fails to detect the low quality images. The proposed work use a technique called Image Distortion Analysis (IDA) which is effective in detecting spoofing in the low quality images. It is very efficient texture operator which labels the pixels of an image by thresholding the neighbourhood of each pixel and if the threshold value below the setting pixels then it detected as low quality images. Spoofing has done in low quality images. Then IDA compares the original image with the spoofed image and find the percentage of spoofing has done in that image.

Key Words: - Face Spoofing, Multi scale Binarized Statistical Image Features on Three Orthogonal Planes (MBSIF-TOP), Multi scale Local Phase Quantization on Three Orthogonal Planes, Kernel Discriminate Analysis, Kernel Fusion, Image Distortion Analysis.

1. INTRODUCTION

Although face recognition technology has witnessed significant progress in the past couple of decades, from systems operating in well-controlled laboratory settings to real-world solutions for unconstrained scenarios, the operational utility of these systems can be challenged by artificial biometric traits, i.e.

spoofing attack [2]. In a recent study, it has been observed that face recognition systems are quite vulnerable to such attacks, as nearly 80% of the spoofing attempts successfully passed the authentication stage [8].

Spoofing attacks are one of the security traits that biometric recognition systems are proven to be vulnerable to. Spoofing attack or copy attack is still a fatal threat for biometric authentication systems. When spoofed, a biometric recognition system is by passed by presenting a copy of the biometric evidence of a valid user. While it is possible to spoof a face authentication system using plastic surgery or forged masks, photographs and videos are probably the most common threats.

2 EXISTING SYSTEM

2.1 FACE LIVELINESS DETECTION

Face liveliness detection uses dynamic texture, in order to differentiate a real access from a duplicate one in a face authentication system. The various approaches to face liveliness detection have been categorized and reviewed according to the cues employed. These categories include methods for detecting signs of vitality (liveliness) and gauging differences in motion patterns and those based on image quality differences [4]. This method also exploit several dynamic visual cues that are based on either the motion patterns of a genuine human face or the used display medium. Unlike photographs and display devices, real faces are indeed non-rigid objects with contractions of facial muscles which result in temporally deformed facial features such as eye lids and lips. Therefore, it can be assumed that the specific facial motion patterns such as including eye blinking, mouth movements and facial expression changes should be detected when a live human being is observed in front of the camera.

2.2 LOCAL BINARY PATTERN

In this approach first LBP operators are applied on a single dynamic mode then it should be applied on a SVM for decision making[10].The LBP method uses motion cues which should be considered as the second class in a categorization of anti-spoofing methods. It should provide the methods which assume the motion patterns between different components of a real face differ from those of a fake face. This assumption is based on the truth that the spoofing attack should done on flat 2D planes compared to the 3D structure of a real face. The LBP operator extracts information which is invariant to local monotonic grey-scale variations of the image. During the LBP operation, the value of current pixel is applied as a threshold to each of the neighbors, to obtain a binary number. A local binary pattern is obtained by concatenating these binary bits and then converting the sequence into the decimal number.

2.3KERNELDISCRIMINANTANALYSIS

Linear Discriminate Analysis has been a popular method for extracting features which preserve class separability. The projection vectors are commonly obtained by maximizing the between class covariance and simultaneously minimizing within class covariance. LDA can be performed either in the original input space

or in the reproducing kernel Hilbert space into which data points are mapped, which leads to Kernel Discriminate Analysis (KDA). When the data are highly nonlinear distributed, KDA can achieve better performance than LDA. However, computing the projective functions in KDA involves Eigen-decomposition of kernel matrix, which is very expensive when a large number of training samples exist. The Kernel Discriminant Analysis model is very effective in classification. Since the Eigen-decomposition of the kernel matrix is involved, the ordinary KDA is computationally expensive in training [3].Moreover, it is difficult to develop incremental algorithm based on the ordinary KDA formulation.

3. PROPOSED SYSTEM

3.1 IMAGE DISTORTION ANALYSIS

Number of face spoofing detection techniques have been proposed, their generalization ability has not been adequately addressed. Image Distortion Analysis (IDA), which is effective in grasping the intrinsic distortions of spoof face images with respect to the genuine face images. Four types of IDA features such as specular reflection, blurriness, color moments, and color diversity have been designed to capture the image distortion in the spoof face images. The four different features are concatenated together, resulting in a 121-dimensional IDA feature vector.SVM classifiers trained for different spoof attacks is used for the classification of genuine and spoof faces.Compared to the existing methods, the proposed method try to extract features that capture the facial details, and also the face image quality differences due to the different reflection properties of different materials such as facial skin, paper and screen. Image Distortion Analysis yields better performance when compare to existing methods.

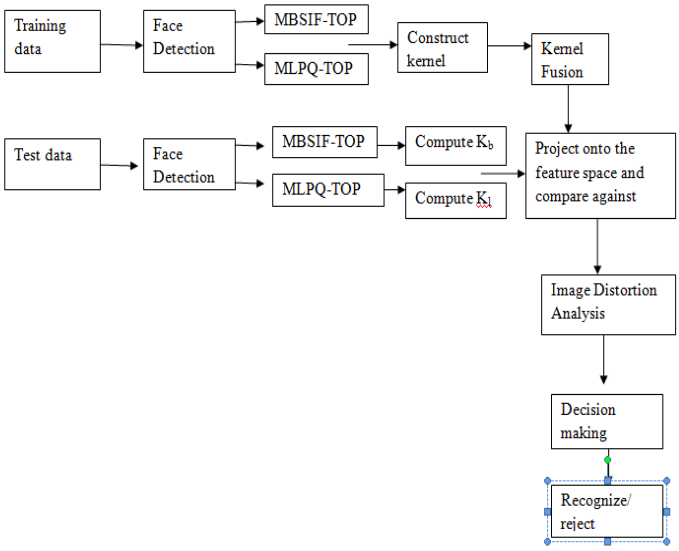


Fig 3.1 Architecture Design

In this system architecture, first data should be collected from the training data set. Then the Face should be detected. Kernels associated with different representations such as MBSIF-TOP and MLPQ-TOP. Multiscale Binarized Statistical Image Features on Three Orthogonal Planes (MBSIF-TOP) is effective in detecting spoofing attacks. Next,by combining MBSIF-TOP with a blur-tolerant descriptor, namely the dynamic Multiscale Local Phase Quantization representation (MLPQ-TOP), the robustness of the spoofing attack can be further improved. The fusion of the information provided by MBSIF-TOP and MLPQ-TOP is realized via a kernel fusion approach based on a fast Kernel Discriminant Analysis (KDA) technique. Test the data by using the same features. In the present work Image Distortion Analysis (IDA) is used which divide the images into blocks and assign the values to each of the neighbour to obtain the binary number. IDA

is a method based on texture analysis. It is a simple yet very efficient texture operator which labels the pixels of an image by thresholding the neighbourhood of each pixel It is very efficient texture operator which labels the pixels of an image by thresholding the neighbourhood of each pixel and if the threshold value below the setting pixels then it detected as low quality images. Spoofing has done in low quality images. Then IDA compares the original image with the spoofed image and find the percentage of spoofing has done in that image.

3.3 IMPLEMENTATION

3.3.1 TRAINING DATA

3.3.1.1FACE DETECTION

The data was collected from the training data set and used for the face detection.

3.3.1.2 KERNEL FUSION

Kernels associated with different representations such as MBSIF-TOP and MLPQ-TOP. Multiscale Binarized Statistical Image Features on Three Orthogonal Planes(MBSIF-TOP) is effective in detecting spoofing attacks. Next, by combining MBSIF-TOP with a blur-tolerant descriptor, namely the dynamic Multiscale Local Phase Quantization representation (MLPQ-TOP), the robustness of the spoofing attack can be further improved. The fusion of the information provided by MBSIF-TOP and MLPQ-TOP is realized via a kernel fusion approach based on a fast kernel discriminant analysis (KDA) technique.

3.3.1.3 ESTIMATION OF α and ω

Spoofing detection is posed as a two-class classification problem. As a result, only a single transformation vector for the KDA projection would be obtained, i.e. only a single vector α. After computing the inner product of the test vector and the unique α satisfying the equation $KWK\alpha = \lambda KK\alpha$ the projection is compared against the projection of the mean of the positive training samples in the induced feature space ω.

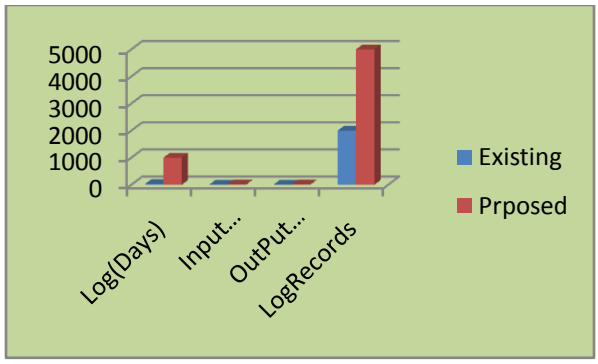
3.3.2 TESTING MODULE

3.3.2.1 FACE DETECTION

The original test data used for the face detection.

3.3.2.2 KERNEL FUSION

Kernels associated with different representations such as MBSIF TOP and MLPQ-TOP. MBSIF-TOP is effective in detecting spoofing attacks. Next, by combining MBSIF-TOP with a blur-tolerant descriptor, namely the dynamic multiscale local phase quantization representation (MLPQ-TOP), the robustness of the spoofing attack can be further improved. The fusion of the information provided by MBSIF-TOP and MLPQ-TOP is realized via a kernel fusion approach based on a fast Kernel Discriminant Analysis (KDA) technique. This is accomplished by solving the problem with the kernel matrix replaced by Kc given as Kc = KB + KL, where KB and KL correspond to the kernel matrices constructed using the MBSIF-TOP and MLPQ-TOP descriptors, respectively.



CONCLUSION

Image Distortion Analysis (IDA), which is effective in grasping the intrinsic distortions of spoof face images with respect to the genuine face images. Image Distortion Analysis capture face image quality differences due to the different reflection properties of different materials such as facial skin, paper and screen. Image Distortion Analysis yields better performance when compare to existing methods.

REFERENCES

1. Arashloo and J. Kittler, (2014)"Class-specific kernel fusion of multiple descriptors for face verification using multiscale binarised statistical image features," Information Forensics and Security, IEEE Transactions on, vol. 9, no. 12, pp. 2100–2109.

2. Bharadwaj, T. I.Dhamecha, M.Vatsa, and R. Singh,(2013) "Computationally efficient face spoofing detection with motion magnification," in The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops.

3. Cai, X. He, and J. Han, (2011) "Speed up kernel discriminant analysis," VLDB Journal, vol. 20, no. 1, pp. 21–33.

4. De Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikainen, and S. Marcel,(2014) "Face liveness detection using dynamic texture," EURASIP Journal on Image and Video Processing, vol. 2014:2.

5. Jianwei, L. Zhen, L. Shengcai, and S. Z. Li,(2013) "Face liveness detection with component dependent descriptor," in Proceedings of the 6th IAPR International Conference on Biometrics, (ICB).

6. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera." in ICCV. IEEE, 2007, pp. 1–8

7. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model." in ECCV (6), ser. Lecture Notes in Computer Science, K. Daniilidis, P. Maragos, and N. Paragios, Eds., vol. 6316. Springer, 2010, pp. 504–517

8. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. Ho,(2015)"Detection of face spoofing using visual dynamics," Information Forensics and Security, IEEE Transactions on, vol. 10, no. 4, pp. 762–777.

9. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks." in ICB, A. K. Jain, A. Ross, S. Prabhakar, and J. Kim, Eds. IEEE, 2012, pp. 26–31.

10. Zhen, D. Huang, Y. Wang, and L. Chen, "Lpq based static anddynamic modeling of facial expressions in 3d videos," in Biometric Recognition, ser. Lecture Notes in Computer Science, Z. Sun, S. Shan, G. Yang, J. Zhou, Y. Wang, and Y. Yin, Eds. Springer International Publishing, 2013, vol. 8232, pp. 122–129.

11. ShervinRahimzadehArashloo, Josef Kittler and William Christmas "Face Spoofing Detection Based on MultipleDescriptor Fusion Using Multiscale Dynamic Binarizedstatistical image features" IEEE transactions on information forensics and security.