ENHANCEMENT OF KERNEL DISCRIMINATIVE ANALYSIS (KDA) IN FACE SPOOFING DETECTION METHOD

S.Menaka, E.P.Prakash, V.Dhinakari

[1]*PG Student, SNS College Of Engineering, Coimbatore*
[2]*Assistant Professor, SNS College Of Engineering, Coimbatore*
[3]*PG Student, ANNA University Regional centre, Coimbatore*

ABSTRACT

In recent years face recognition has been the important factor. So the significant progress has been made in this area currently now. In practical application the problem of spoofing attacks can be threaten to face biometric systems which is used for authentication. This paper proposes a kernel discriminate analysis (KDA).This could be a effective countermeasure against face spoofing attacks. In First this KDA scheme proposed multi scale dynamic texture descriptor based on binary statistical image features on three orthogonal planes (MBSIF-TOP).This scheme should be effective in detecting spoofing attacks, showing promising performance compared to existing alternatives. Next this KDA scheme is combining MBSIF-TOP with a blur-tolerant descriptor. This combined approach should be called as dynamic multi scale local phase quantization representation (MLPQ-TOP).By using the robustness of the spoofing attack detector can be further improved. The kernel fusion approach could be used to realize the information provided by MBSIF-TOP and MLPQ-TOP based on a fast kernel discriminate analysis (KDA) technique .The costly Eigen analysis computations should be avoided by solving the KDA problem using spectral Regression.

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.

INTRODUCTION

Face Recognition

In [1] the authors described about facial matching .In the past couple of days the face recognition technology has been used in many places. The system is operating from small scale industries to real-world solutions. This face recognition technology should be applied with constrained scenarios. The spoofing attack which is the threaten to the operational utility of face recognition system. The spoofing attack should be also called as artificial biometric traits. In a spoofing attack, an attacker tries to gain access to some service of legitimate user by submitting not natural biometric data of original user to the authentication system. In [2] the author's states that face recognition systems are quite susceptible to such type of attacks. The 80% of the spoofing attacks successfully passed the authentication stage.

ISSN: 2278 – 1323

Due to this vulnerability the need for checking the validity of the biometric data increases before proceeding to verification or recognition. Spoofing is not vulnerable to face recognition system only. Other biometrics modalities also suffer from this spoofing attack [4], [5]. The face images or a video clip on the internet has been vulnerable to spoofing attack because these types of attack easily access a person's facial data compared to the other attack. Moreover face spoofing attack take low cost and time which make the face spoofing problem even more common. In face spoofing attack the media used vary from low quality paper prints to high quality photographs is the media used for spoofing as well as video streams played in front of the biometric authentication system sensor is also vulnerable to the spoofing attack. Other types of media like 3D masks are less vulnerable to the face spoofing attacks [6].

This type of spoofing attack performed on a printed photograph or a replayed video by using the sensor. Even though the spoofing attacks are recognized using a variety of different media in a wide range of different applications and imaging conditions, the problem causes serious challenges in practical applications. In the past two years the research into face spoofing attack has become popular increases. The spectrum of spoofing attack detection approach in the literature [9] the spatio-temporal descriptors could be used which applies a group of methods. This method focuses on modeling the dynamic content of image sequences. An example of such methods is described in which employs a LBP-TOP (local binary pattern histograms on three orthogonal planes) in order to detect spoofing attacks.

In [10] author describes the BSIF (Binary Statistical Image Features) descriptor. This BSIF descriptor operates in a similar to the well known local binary pattern (LBP) operator. This descriptor produces a binary coded image instead of an original image. The BSIF descriptor produces filters which provide a better representation of image/image-sequence content based on statistical learning on it. Most significantly the BSIF filters are designed to increase statistical independent outputs. This may enhances their representational capacity compared with a operators producing a dependent outputs. Arguably this scheme also improves their sensitivity in the visual content of an image.

A contribution of the literature [11] is to employ the dynamic multi scale BSIF descriptor (MBSIF-TOP) in conjunction with kernel discriminate analysis (KDA).This combined useful for face aliveness detection. This specific KDA (SR-KDA) method avoids costly Eigen-analysis computations via spectral regression. It produces the orders of magnitude faster than the ordinary KDA [11].

In [8] the author describes the local phase quantization (LPQ) representation .This is a different but closely related dynamic texture descriptor. The local phase quantization and its extension to the time-varying textures (LPQ-TOP) exploit the blur-insensitive property of the Fourier phase

ISSN: 2278 – 1323

spectrum. This could be a promising approach in texture/dynamic-texture modeling, especially when the acquired images suffer from blurring effects. The LPQ descriptor and its invariance to blur may be particularly relevant to spoofing attack detection. In subspace identification using the SR-KDA method the LPQ-TOP representation is very effective in discriminating real-access attempts from a certain type of spoofing attack. The current work follows the same path and presents an effective method for the detection of spoofing attacks using a dynamic texture descriptor that is new to this application domain. The BSIF descriptor and its multi scale dynamic extensions have been successful in a variety of static and dynamic texture representation and recognition problems. These should include face image modeling and recognition, dynamic texture recognition, finger print spoofing detection. Motivated by this, the current work employs the dynamic multi scale BSIF descriptor for face spoofing detection.

EXISTING SYSTEM

[9]In 2006 T. de Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikainen, and S. Marcel ake propose a method called Face liveliness detection using dynamic texture,". In order to differentiate a real access from a duplicate one in a face authentication system uses a variety of different methods have been discussed in this paper. 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.

Disadvantage

- Use characteristics which are exhibited only for live faces not for stored faces.

[13] In 2007 G. Pan, L. Sun, Z. Wu, and S. Lao, proposed Eyeblink-based anti-spoofing in face recognition from a generic webcamera". The method presented here uses eye-blink as a countermeasure to spoofing, formulated as inference in an undirected conditional graphical framework. The method has been evaluated on a publicly available blinking video database.

Disadvantage

- However, eye-blink may not be considered as a reliable countermeasure.
- Spoofing attacks using printed masks with the eye positions cut out can potentially pass such tests.

Dynamic Mode Decomposition[14]

In 2010 S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. Ho, proposed "Detection of face spoofing using visual dynamics". This paper proposed the use of the dynamic mode decomposition (DMD) method for modeling dynamic information of the video content.

ISSN: 2278 – 1323

They are blinking eyes, moving lips, and facial dynamics. The authors propose a combined method called classification pipeline which consisting of DMD, local binary patterns and SVMs. The temporal information of an image sequence should be represented as a single image by using the DMD approach.

Local Binary Pattern[15]

In 2012 T. de Freitas Pereira, A. Anjos, J. M. D. Martino, and S. Marcel, proposed "LBP top based countermeasure against face spoofing attack. In this approach first LBP operators are applied on a single dynamic mode then it should be applied on a SVM for final decision making. 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.

Disadvantage

- Motions in spoofing attacks are rigid whereas a combination of both rigid and non-rigid motions exists in real-access attempts;
- The rigid nature of a face may serve as a complementary cue for spoofing detection.

Spoofing Detection Method for Video Sequences[16]

In 2014 M. D. Marsico, M. Nappi, D. Riccio, and J.-L. Dugelay, proposed "Moving face spoofing detection via 3d projective in variants". This paper propose a Spoofing detection method for video sequences using motion magnification. For this purpose to enhance the facial expressions Eulerian motion magnification is used. From this Two kinds of features are deployed: the first one is based on a configuration of LBP and the second is built upon the motion estimation approach using the HOOF descriptor.

Advantage

- This method achieves good performance on the Print Attack and Replay Attack data sets.
- Presented a method for evaluating liveliness in face image sequences using a set of automatically located facial points.
- Geometric invariants are then used for detecting replay attack.

PROPOSED SYSTEM

This paper combines the MBSIF-TOP and MLPQ-TOP descriptors using the SR-KDA approachin order to take benefit from the complementary properties of both descriptors while detecting the spoofing attack. The SR-KDA (spectral regression kernel discriminate analysis) approach is a computationally efficient approach to implementing KDA. The kernel fusion is also accomplished by SR-KDA. The kernel fusion approach is found to enhance the system

ISSN: 2278 – 1323

performance and it should be measured on the face anti-spoofing database, as well as the Replay-Attack and NUAA databases.This paper proposes the discriminative representation which should be based on the dynamic multi scale binarized statistical image features [16] and kernel discriminate analysis for face anti-spoofing. The combined representation is shown to perform better than similar dynamic texture descriptors such as LBPTOP [24] and LPQ-TOP. The properties of the BSIF descriptor are well suited for spoofing attack detection. On the face anti-spoofing database, the fusion strategy adopted is shown to be particularly effective in real-world scenarios such as low-resolution biometric data or short image sequences. On the Replay-Attack and NUAA databases, the fusion consistently improves the performance.

ADVANTAGES OF PROPOSED SYSTEM

- The proposed kernel fusion combined technique for face spoofing detection improves the performance, compared to either one of the descriptors used individually in most cases.
- The combined scheme is computationally more efficient compared to conventional KDA methods.
- This viable solution is a preliminary step in checking the authenticity of the biometric data captured by a face biometric system.

CONCLUSION

This paper addressed the problem of face biometrics spoofing detection which should be based on dynamic texture analysis of video sequences captured during real time. A novel descriptor namely multi scale binarised statistical image features descriptor (MBSIF-TOP) in the context of the application is proposed. This representation is to be adopted in a spoofing detection system designed using the computationally efficient spectral regression kernel discriminate analysis. The proposed method was comprehensively evaluated on benchmarking datasets using standard protocols which should be a superior to similar dynamic texture analysis schemes. Its superior spoofing detection performance is adhered to the filters producing BSIF, which are designed to enhance statistical individuality of the outputs. The benefit of statistical individuality is improved representational capacity of the texture descriptor and its enhanced sensitivity.

REFERENCES

[1] S. Arashloo, J. Kittler, and W. Christmas, "Facial feature localization using graph matching with higher order statistical shape priors and global optimization," in Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, Sept 2010, pp. 1–8.

[2] S. Rahimzadeh Arashloo and J. Kittler, "Pose-invariant face matching using mrf energy minimization framework," in Energy Minimization Methods in Computer Vision and Pattern Recognition, ser. Lecture Notes

ISSN: 2278 – 1323

in Computer Science, D. Cremers, Y. Boykov, A. Blake, and F. Schmidt, Eds. Springer Berlin Heidelberg, 2009, vol. 5681, pp. 56–69.

[3] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing." in BIOSIG, A. Brmme and C. Busch, Eds. IEEE, 2012, pp. 1–7.

[4] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Securityevaluation of biometric authentication systems under real spoofing attacks," IET Biometrics, vol. 1, pp. 11–24, 2012.

[5] Z. Akhtar, B. Biggio, G. Fumera, and G. L. Marcialis, "Robustness of multi-modal biometric systems under realistic spoof attacks against all traits," in IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BioMS), Milan, Italy, 2011.

[6] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3d masks," Information Forensics and Security, IEEE Transactions on, vol. 9, no. 7, pp. 1084–1097, July 2014.

[7] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, F. Roli, J. Yan, D. Yi, Z. Lei, "Competition on counter measures to 2-d facial spoofing attacks." In IJCB, A. K. Jain, A. Ross, S. Prabhakar, and J. Kim, Eds. IEEE, 2011, pp. 1–6.

[8] I. Chingovska, J. Yang, Z. Lei, D. Yi, S. Li, O. Kahm, C. Glaser, "The 2nd competitionon counter measures to 2d face spoofing attacks," in Biometrics (ICB), 2013 International Conference on, June 2013, pp. 1–6.

[9] T. de Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikainen, and S. Marcel, "Face liveness detection using dynamic texture," EURASIP Journal on Image and Video Processing, vol. 2014:2, Jan. 2014.

[10]"Dynamic texture recognition using multiscale binarized statistical image features," Multimedia, IEEE Transactions on, vol. 16, no. 8, pp. 2099–2109, Dec 2014.

[11] D. Cai, X. He, and J. Han, "Speed up kernel discriminant analysis," The VLDB Journal, vol. 20, no. 1, pp. 21–33, Feb. 2011.

[12] V. Ojansivu and J. Heikkil, "Blur insensitive texture classification using local phase quantization," in Image and Signal Processing, ser.

[13] G. 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.

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

ISSN: 2278 – 1323

[15] T. de Freitas Pereira, A. Anjos, J. M. D. Martino, and S. Marcel, "Lbp - top based countermeasure against face spoofing attacks." in ACCV Workshops (1), ser. Lecture Notes in Computer Science, J.-I. Park and J. Kim, Eds., vol. 7728. Springer, 2012, pp. 121–132.[16] M. D. Marsico, M. Nappi, D. Riccio, and J.-L. Dugelay, "Moving face spoofing detection via 3d projective invariants." in ICB, A. K. Jain, A. Ross, S. Prabhakar, and J. Kim, Eds. IEEE, 2012.

ISSN: 2278 – 1323