Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 24 (2016) 1285 – 1291

Procedia Technology

International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST - 2015)

Spoof Face Recognition in Video Using KSVM

Faseela T[a,] * , Jayasree M[a]

[a]*Government Engineering College Thrissur, Kerala, 680009, India.*

Abstract

With the advancement of video and its transmission technologies, video has found its use extensively in surveillance, security, especially in detecting forgery. Unlike still images, video provide large amount of intra-personal variations, making face recognition a significant concept in the field of biometric security. Automatic face recognition is a widely used concept in implementing security, which is also prone to various spoof attacks. Spoof attacks accounts to reproducing a person's face using printed photos or by replaying a video. A large number of face recognition and spoof detection algorithms have been developed for still images, but those concerning videos are less in number. Face recognition from videos and related spoof detections are less explored. This paper deals with countering such spoof attacks in facial recognition using videos, where KSVM (K-Means and SVM) is used to identify the recognized images to be real or spoof. KSVM, a combined concept of K-Means and SVM outperforms simple SVM.

Peer-review under responsibility of the organizing committee of ICETEST – 2015

Keywords: Face Recognition ; K-Means; SVM ;Spoof Detection; KSVM

1. Introduction

The widespread use of camera technology in various surveillance systems urges the requirement for facial recognition from videos. The surveillance cameras and fingerprint identification technologies are also used to identify or authenticate individuals as legal/public safety procedures. Unlike still images, videos provide large amount of intra-personal variations making face recognition a significant concept. Video based facial recognition is

* Corresponding author. Tel.: +91-949-548-8091.
E-mail address: fslfars@gmail.com.

Peer-review under responsibility of the organizing committee of ICETEST – 2015
doi:10.1016/j.protcy.2016.05.118

prone to spoofing attack to a greater extent than other biometric authentication/security systems. Spoofing attacks are easy to develop which makes countering such attacks and extracting the spoofed face, a necessity. Videos are susceptible to replayed video attacks where a previously recorded video is being displayed in front of a computer camera.

Extensive researches have been done on face detection from video since it is easy to produce videos which can pack large amount of information. This also necessitates the need to develop anti-spoofing methods to prevent forgery and building robust security/safety systems.

2. Related Works

The research contribution by Vishal M Patel et al. [18] in dictionary based face recognition under variable lighting and pose took a set of training samples and a dictionary learning algorithm called K-SVD algorithm , a generalization of K-Means, was run to learn face specific dictionaries. Approximation errors were computed for the test image, based on which the individual present in the image was identified.

Yet another contribution in video recognition was by Lior Wolf et al. [2] focusing on matched background similarity where a set to set similarity approach was adopted. Using this approach, both the videos were represented as feature vectors and locating each member of the video, its nearest neighbour in a set of background samples. Finally all the matched frames were aggregated into a set which was used to compare with one of the original video. This was performed using SVM.

Video based recognition on real world data by Johannes Stallkamp et al. [3] was also a notable work. Face images extracted by Johannes [8] from training sequences are classified by a local appearance based face recognition algorithm. Individual frames scores obtained from each classification are progressively combined to identify the real subject.

A spoof face detection algorithm was introduced by Keyurkumar Patel et al. [20] in which moiré pattern was analyzed that occurs due to the recapturing and replaying of video or photos on digital screen.

Another work on video spoof attack detection was using visual rhythms proposed by Allan Pinto et al. [4] where the content independent noise signatures of the video are analyzed to distinguish between fake and valid access videos.

Spoof detection on consumer devices to tackle the replay attacks proposed by Smith Daniel et al. [5] is also a major contribution in spoof attack detection. The reflections onto the screen are analysed over here and the sequence of screen images and their corresponding reflections digitally watermarks the video.

Another work on authentication was authenticating the face with make-up. The work was put forwarded by Guodong Guo et al. [19] were for a given set of images ,after extracting its features, patch selection, discriminative mapping, makeup selection and correlation mapping was done to recognize faces .

A new algorithm called K-Means-SVM (K-SVM) by Yao Yukai et al. [7]and Wang Jiaqi et al. [9] which is a joint concept of K-Means and SVM is a recent development to be added up to the group of clustering algorithms .Here a small subset is selected from the original training set to act as the final training set. This is to sift the important samples with massive information.

3. Spoof Attacks

The technological advancements in today's scenario are having heavy threats from the hackers and attackers who mainly concentrate on the authentication spoofing. The two major type of spoof attacks are: (1) Printed Photo attacks and (2) Replay Video Attacks. The paper is mainly focusing on replay video attacks.

Printed Photo Attack: In printed photo attack, the image of a person is acquired using a camera and is then reproduced on a paper .This is then used for spoof attacks by the attacker as shown in figure below (*Courtesy*: *1080plus.com/BfAu66HcbQE.video*).

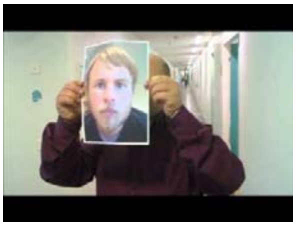


Fig. 1. Printed Photo Attack

Replay Video Attack: As shown in figure below (*Courtesy*: *www.bittree.it/portfolio/92*)**,** in replay video attack, the recorded video of an individual is displayed to another camera for spoof attacks in authentication.

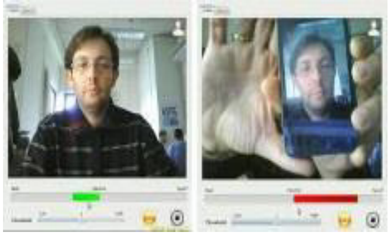


Fig. 2. Replay Video Attack

4. Video recognition using K-SVM

The paper presents the idea of identifying a video to be spoof or genuine based on the combined algorithm of K-SVM (K-Means and SVM) introduced by Yao Yukai et al. [7]. The advantage of using K-SVM is that it helps in reducing the support vectors. The framework of the proposed system presented in Fig. 3. is carried out through four steps. So, when we have a video to test if it is genuine or not, first the video is divided into different frames. For each frame the Image Distortion Analysis (IDA) features are extracted and they are compared to the samples of a spoof database. Based on the comparison, a ranked list is created. The ranked list is then fed as an input to a K-SVM algorithm. The K-Means algorithm of K-SVM clusters the data in the ranked list and the SVM then trains the misclassified data present in it. Finally the SVM classifier classifies the frame to be genuine or spoof. At last all such results of every frame are fused to get the final decision whether the video is genuine or spoof.

The following lists the different steps:

- Extracting the IDA features.
- Ranking the input image or frame based on the database.
- Running the K-SVM on the ranked list to create clusters and training the SVM.

- Fusing all the frame outputs and applying a majority voting method to identify the whole video to be genuine or spoof.

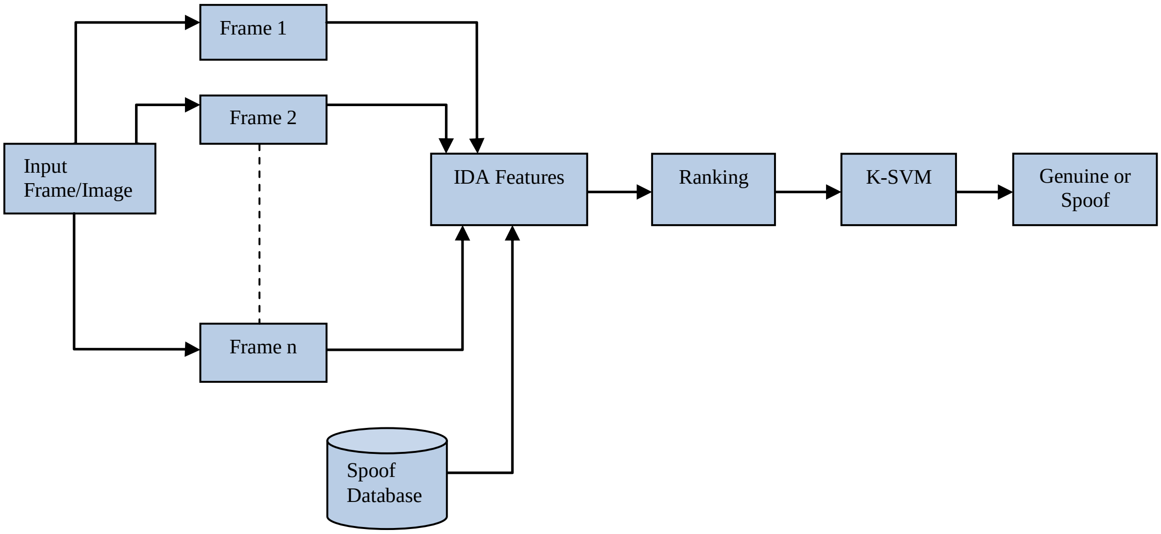


Fig. 3. Framework of Proposed Method

4.1. Extracting the IDA Features

The input video is first divided into various frames which is similar to a set of images. Since the paper focuses on finding out a video to be genuine or spoof, here the IDA features of the input are extracted. The IDA features are those that distinguish the spoof image characteristics from the real image. As introduced by Wen et al. [6], the various IDA features are (1) Specular reflection, (2) Color diversity, (3) Chromatic Moment features and (4) Blurriness features. Out of these those concerning videos are:

- Specular Reflections

  This type of features are obtained when light falls on a spoof image, that is, there is certain difference observed in the reflections obtained when light falls on a real image and a spoof image. Robby T Tan et al. [10] introduced this feature.

- Colour Diversity

  The recaptured face images concept introduced by Chen et al. [11] show a different colour distribution compared to the genuine face images. Genuine images/frames have richer colours compared to spoof faces. This is how the colour diversity features are identified.

- Blurriness Features

  F Crete et al. [12] brought the concept that spoof images are often more defocussed compared to the real images. This is because, the spoofing medium has limited size and so the attacker tends to place the camera close to the medium to cover its boundaries. Finally, the image gets blurred.

4.2. Ranking

In order to generate a ranked list, each IDA extracted image is now compared with the database and a ranked list is created using Linear Discriminant Analysis, a method introduced by P. N. Belhumeur [13].The input frame and the images in the database are projected onto a subspace and the Euclidean distance is calculated between the input frames and the images in the database. The ranked list finally contains the most similar image on top of the list, a concept by Himanshu Bhatt et al. [1].

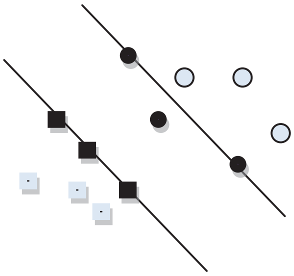
$$Y = W^T X \tag{1}$$

Here Y is the subspace representation and X is the input image and W is the projection matrix.

4.3. Clustering Using K-SVM

Finally, each frame will be having a ranked list. Hence, now for each frame the K-SVM algorithm is run. The goal of the algorithm is to sift the most important samples with massive information. In order to search a decision boundary for learning algorithm, the points close to or on the boundary of the clusters are searched.

The points may get to the misclassified points set if distance of one of the points is close enough to the opposite cluster. In the figure below, the lines represent the decision boundary and the points lying on the hyper plane are the support vectors or the misclassified points.



Based on the information of the misclassified points, training and the prediction model can be designed. For this purpose, the neighbouring points of the misclassified points are taken into consideration. As the first step, each data point of the original training set are first assigned a cluster label and the true label of each data point is compared with the obtained cluster label. If they come out as different, then those points may lie towards the edge region of the two clusters. These are the misclassified points. As a second step, for each of these misclassified points their neighbours are selected whose true labels are different to those misclassified points or the number of the points with the same label is equal to that with the different label. Those chosen neighbours are the candidate training set.

So for a given training set $X = \{x_1, x_2, ...x_n\}$ and a label set $Y = \{y_1, y_2, ...y_n\}$ and a sample $\{x_i, y_i\}$, K-Means clustering is performed on training set and each sample in it gets a cluster label. If this cluster label is different from the true label, then those samples are added to the misclassified points set MIS such that,

$$MIS = \{x_i \mid y_{ik} \neq y_i\} \tag{2}$$

where y_{ik} the cluster label of sample x_i with true label y_i. From MIS, N-nearest neighbors are found out. The selected informative samples from the set are mapped to a new training set. Finally the SVM of K-SVM technique produces the result as the frame to be genuine or spoof.

4.4. Multi Frame Fusion

Since each video is composed of several frames, all the above steps need to be carried out for all the frames. The outputs of all the frames now need to be fused. Various fusion techniques, by J Zhang et al. [14], and Ross et al. [15, 16] are available out of which majority voting technique comes out the best over here. Referred to the concept by Liu Nan et al. [17] the classification result from each frame will be fused by a voting technique for the whole video. So a face video could be classified to be genuine if 50% of the frames have a classification result to be genuine.

5. Face Spoof databases

Most of the spoof face recognition algorithms adopt the publicly available spoof databases. The various spoof databases are (1) NUAA Photograph Imposter Database, (2)Idiap REPLAY-ATTACK database,(3)CASIA Face Anti-spoofing Database and (4)MSU MFSD Database.

NUAA Photo Imposter Database: This database is mainly composed of 12614 images of genuine and attack samples of just 15 subjects. The database is mainly built up for printed photo attacks.

Idiap REPLAY-ATTACK Database: The database consists of 1300 video recordings of genuine samples and attack attempts of 50 subjects. This database mainly focuses printed photo attacks, displayed photo/videos on mobile phone's screen and those on an HD screen.

CASIA Face Anti-spoofing Database: This database consists of 600 video recordings of genuine and 50 subjects of spoof samples. This database supports both printed photo attack and replayed video attack.

MSU MFSD Database: This database consists of 440 video clips of photo and video attack samples of 55 individuals. All the other three databases consist of images captured by web cameras or high quality digital cameras. This database supports images captured via mobile phones.

6. Conclusion

Various face recognition approaches have been developed, but some of them are prone to various spoof attacks. So the paper here presents a frame work to identify a video to be genuine or spoof. The paper uses K-SVM technique to identify the video frame to be genuine or spoof. By using the K-SVM technique the support vectors needed to train the SVM get reduced i.e.; the size of the training set gets reduced and the time for establishing the prediction model also gets reduced. Using this method, the efficiency in finding out the spoof face is improved.

Acknowledgements

We the authors are thankful to the Head of the Department, the faculty members and the staff of the Computer Science and Engineering Department of Government Engineering College ,Thrissur for providing the necessary facilities and support for fulfilling the work. We are also thankful to the database developers of ‘Replay Attack’ database published in the paper “On the Effectiveness of Local Binary Patterns in Face Anti-spoofing” by Ivana Chingovska and André Anjos And Sébastien Marcel in the IEEE BIOSIG 2012 proceedings and the database ‘MSU MFSD’ published by Di Wen and Hu Han and A K Jain, in the paper titled “Face Spoof Detection with Image Distortion Analysis” in April 2015 IEEE Transactions in Information Forensic and Security.

References

[1] Himanshu S Bhatt,Richa Singh,Mayank Vatsa “ On Recognizing Faces in Videos using Clustering Based Re-Ranking and Fusion”, IEEE Transactions in Information Forensics and Security,Vol 9,No.7,July 2014 pp. 1056-1068.

[2] Wolf, Lior, Tal Hassner, and Itay Maoz. "Face recognition in unconstrained videos with matched background similarity." Computer Vision and Pattern Recognition (CVPR), 2011 IEEE Conference on. IEEE, 2011.

[3] Stallkamp, Johannes, Hazim K. Ekenel, and Rainer Stiefelhagen. "Video-based face recognition on real-world data." In Computer Vision, 2007. ICCV 2007. IEEE 11th International Conference on, pp. 1-8. IEEE, 2007.

[4] Pinto, Allan da Silva, Helio Pedrini, William Robson Schwartz, and Anderson Rocha. "Video-based face spoofing detection through visual rhythm analysis." In *Graphics, Patterns and Images (SIBGRAPI), 2012 25th SIBGRAPI Conference on*, pp. 221-228. IEEE, 2012.

[5] Smith, Daniel F., Arnold Wiliem, and Brian C. Lovell. "Face Recognition on Consumer Devices: Reflections on Replay Attacks." *Information Forensics and Security, IEEE Transactions on* 10, no. 4 (2015): 736-745.

[6] Wen, Di, Hu Han, and Anil K. Jain. "Face spoof detection with image distortion analysis." *Information Forensics and Security, IEEE*

Transactions on 10, no. 4 (2015): 746-761

[7] Yao, Yukai, Yang Liu, Yongqing Yu, Hong Xu, Weiming Lv, Zhao Li, and Xiaoyun Chen. "K-SVM: An effective SVM algorithm based on K-means clustering." *Journal of computers* 8, no. 10 (2013): 2632-2639.

[8] Stallkamp, Johannes. "Video-based face recognition using local appearance-based models." *Thesisreport, Universitat Karlsruhe (TH)* (2006).

[9] Wang, Jiaqi, Xindong Wu, and Chengqi Zhang. "Support vector machines based on K-means clustering for real-time business intelligence systems." *International Journal of Business Intelligence and Data Mining* 1, no. 1 (2005): 54-64.

[10] Tan, Robby T., and Katsushi Ikeuchi. "Separating reflection components of textured surfaces using a single image." *Pattern Analysis and Machine Intelligence, IEEE Transactions on* 27, no. 2 (2005): 178-193.

[11] Y. Chen, Z. Li, M. Li, and W.-Y. Ma, “Automatic classification of photographs and graphics,” in Proc. ICME, 2006, pp. 973–976.

[12] F. Crete, T. Dolmiere, P. Ladret, and M. Nicolas, “The blur effect:perception and estimation with a new no-reference perceptual blur metric,” in Proc. SPIE: Human Vision and Electronic Imaging XII, 2007.

[13] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, “Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 7, pp. 711–720, Jul. 1997.

[14] J. Zhang, J. Gao, M. Zhou, and J. Wang,” Improving the effectiveness of information retrieval with clustering and fusion Computational Linguistics and Chinese Language Processing”, vol. 6, no. 1, pp. 109-125, Feb 2001.

[15] Ross, Arun, and Anil Jain. "Information fusion in biometrics." *Pattern recognition letters* 24, no. 13 (2003): 2115-2125.

[16] Jain, Anil, Karthik Nandakumar, and Arun Ross. "Score normalization in multimodal biometric systems." *Pattern recognition* 38, no. 12 (2005): 2270-2285.

[17] Liu, Nan, and Han Wang. "Classification of transformed face images with majority voting." In *Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference on*, pp. 2860-2864. IEEE, 2007

[18] Patel, Vishal M., Tao Wu, Soma Biswas, P. Jonathon Phillips, and Rama Chellappa. "Dictionary-based face recognition under variable lighting and pose." *Information Forensics and Security, IEEE Transactions on* 7, no. 3 (2012): 954-965.

[19] Guo, Guodong, Lingyun Wen, and Shuicheng Yan. "Face Authentication with makeup changes." *Circuits and Systems for Video Technology, IEEE Transactions on* 24, no. 5 (2014): 814-825.

[20] Patel, Keyurkumar, Hu Han, Anil K. Jain, and Greg Ott. "Live Face Video vs. Spoof Face Video: Use of Moiré Patterns to Detect Replay Video attacks."