AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

An Efficient Mechanism For Detection Of Face Spoofing Using Support Vector Machine

S. Dhivya

Assistant Professor, Dept. of CSE, Kongunadu College of Engineering and Technology, Trichy

Address For Correspondence:
S. Dhivya, Assistant Professor, Dept. of CSE, Kongunadu College of Engineering and Technology, Trichy
E-mail: sdhivya005@gmail. Com

ARTICLE INFO

Article history:
Received 3 April 2016
Accepted 21 May 2016
Published 2 June 2016

Keywords:
SVM; Face Spoof; MSU; DMD.

ABSTRACT

The most developments of face recognition systems in applications from the de-duplication to the mobile devices unlocking, securities against the face spoofing attacks required to an increased attention; such attacks can been easily launched by a via printed photos, video replays 3D masks of a faces. In their existing systems, pipelining of DMD + LBP + SVM is introduced it's which works based on their visual dynamics of the system. This existing works will divided to the videos into multiples of visual dynamics frame and which the phase angle values would be calculated. Finally the image with 0 phase angle values would be selected for their further processing. This exiting works might to than lacks from performance, in terms of accurate detections of face spoofing where it's considered only one image for LBP calculation. We address the problem of facial spoof detections against print (photo) and replay attacks based on their analysis of image aliasing (e.g., surface reflection, more patterns, colour distortion, and shape deformations) in spoof face images (or video frames). The application domain interesting is the mobile phone unlock, given that to growing the number of phones having face unlock and mobile payment capabilities. The mobile spoof face build to database (MSU MSF) containing more than 1; 1000 subjects, which is our knowledge, the largest spoof of face database in terms of the number of subjects.

INTRODUCTION

As convenient user's authentication techniques, automatic face recognition system has been attracted to an increasing attention in their various access control applications, especially for mobile unlocking. Within the release of face unlocking functions in their android mobile operating systems, face recognition function becomes a biometric authentication technique for mobile phones, similar to finger print authentication (Touch ID) in the ios system. Unlike a fingerprint authentication a, faces recognition does not add requires any additional sensors since all smart phones come to an equipped with front facing camera (Li, X.H., *et al*., 2015).

However similar methods to other than biometric modalities, it need to an address concerns about face spoof attacks on face recognition systems, particularly in an unconstrained sensing and uncooperative subject scenarios. It is relatively easier to an acquire a person's face image or video (e.g., A digital camera or from social media) than it is to acquire other biometrics trait such as fingerprint, palm print, and iris (Roberts, C., 2014). Furthermore, the costs of launching a face spoof attack, such as a printed photo, is played photo.

A genuine face image of a subject in the ideal databases and three examples of spoofs of the same subjects using a (a) printed photo, (b) displayed photo (on a tablet screen), and (c) 3 Dimensional face masks. Re played video is relatively low. State of art Commercial Off-the-Shelf (COTS) face recognition systems, is not sufficient to design with differentiate the spoof faces from genuine live faces (Ratha, N.K., *et al*., 2011). The face identifications performance is COTS face recognition systems, when the spoof faces as probably with matched

To Cite This Article: S. Dhivya., An Efficient Mechanism For Detection Of Face Spoofing Using Support Vector Machine. ***Aust. J. Basic & Appl. Sci.,*** *10(9): 255-259, 2016*

to genuine image in the gallery. In this experiments more than 70% of probe videos were successfully matched to then gallery mates by COTS1 at rank-1 indicates that COTS1 can't effectively distinguish between the genuine and spoof face (Kollreider, K., *et al*., 2005).

In this paper does not address in 3D face masks attack, which is more expensive to launch. Instead of focused on a printed photo and replayed with video attack. The fragility of face recognition systems to face spoof attacks has been motivated in a number of studies on face spoof detection (da Silva Pinto, A., *et al*., 2012). However published studies are limited in their scopes of the training and testing images or videos are used in were captured the under same imaging conditions. It is very essential to develop robust and efficient of face spoofing detections or anti spoofing algorithms that generalized well to new imaging conditions and environments. In this paper the cross database face spoof detection problem and proposed a face spoof detection approach based on Image Distortion Analysis (IDA) (Lazarick, R., 2012).

Existing System:

Detection of face Antispoofing is very important safe guarding the information's against the face spoofing attacks in their videos. Dynamic mode decompositions (DMD) pipeline classification methods consisting of DMD, local binary patterns (LBPs), and support vector machines (SVMs) has been used in their previously to detecting the face spoofing attacks. The performance of the face anti spoofing can be furthered in improved by an using Improved DMD pipeline classifications. The proposed approach, instead of selecting a single dynamic mode images, concatenates the all different mode images into a single image (Meyer, H., 2008). Then the LBP codes are computed and then classified in using SVM with higher performance. This approach also helps in detecting more sophisticated attacks in the videos.

In their existing works presenting the pipelined of our old methods which consists of DMD, Local Binary Pattern histograms and a kernel based Support Vector Machines (SVM) classifiers. First a video processed in using the DMD algorithms in order to output dynamic mode images. From which, it select a single dynamic mode images corresponding into the Eigen values whose phase angle is 0 or closest to it. Second, LBP histogram features are computed in this dynamic mode images. Finally, the produced LBP code is fed into a trained SVM classifier's in order to classify whether the processed video is a valid access or spoof. Half Total Error Rate (HTER) is used to evaluate the performance measure. To validate our DMD pipeline have used principle component analysis (PCA) based on snapshot approach as a baseline method (Matsumoto, T., *et al*., 2012).

Flow Chart:

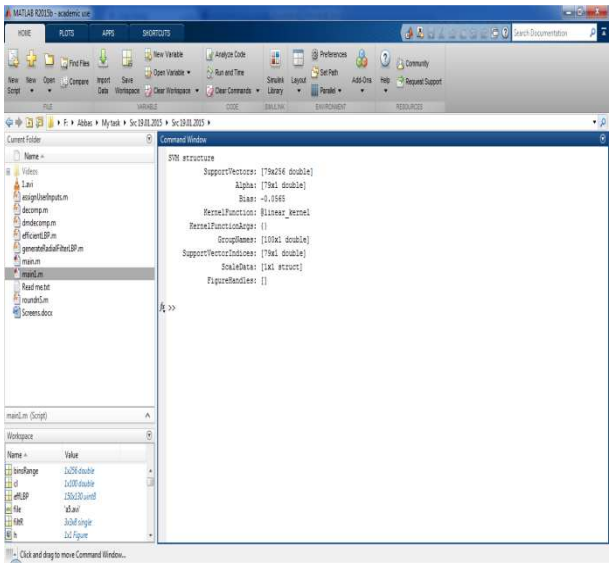

Fig. 1: Programming

SVM classifiers Histogram Intersection Kernel based on Support Vector Machine (SVM) is a widely used in pattern classification methods and its well known for its high classification accuracy. A kernel method transforms data from a low dimensional space to a high dimensional space using non-linear maps. By non linearly mapping the data onto the high dimensional space, it is theoretically shown in that any linearly non-separable data can become linearly separable. Since only the inner product's between a pair of observations is required in the SVM formulation, the non-linear mapping does not need to been explicitly defined as for an individual observations in the training set (Thalheim, L., *et al*., 2010). Instead, the non-linear kernel functions

are also defined for a pair of observation. These maintain the efficiency of the SVM. Therefore, a kernel based SVM in general has a better performance over an original SVM for linearly non-separable classification tasks.

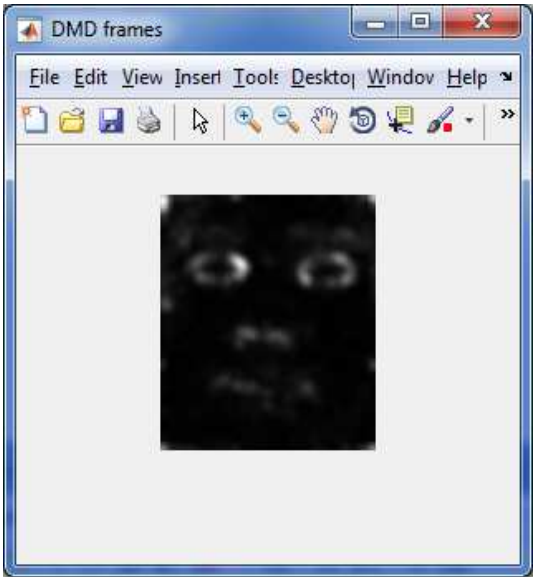

Fig. 2: DMD Frames

Selection of DMD modes:

Form N number of frames, we obtained in N_1 DMD modes. We calculates the phase angles based on the complex eigen values and select the eigen vector which has the eigen value phase angle = 0 (or the closest value = 0) and compute the dynamic mode. Figure 5 shows the eigen values of upper Hessen berg matrix H, which represents the mapping between video frames. Unstable eigen values are located outside the circle and stable eigen values can be found on the circle. For the selection of modes, we calculate the phase angle for each of the eigen values, i.e, the eigen value at (1; 0) has phase angle = 0 and captures the overall dynamics from the video sequence (Duc, N. and B. Minh, 2012).

The phase angles above the axis [(0; 1); (1; 0)] corresponding to positive phase and negative phase angles respectively. Each of these dynamic modes captured in various dynamic information's pertaining to the video sequences, from large scale to small scale.

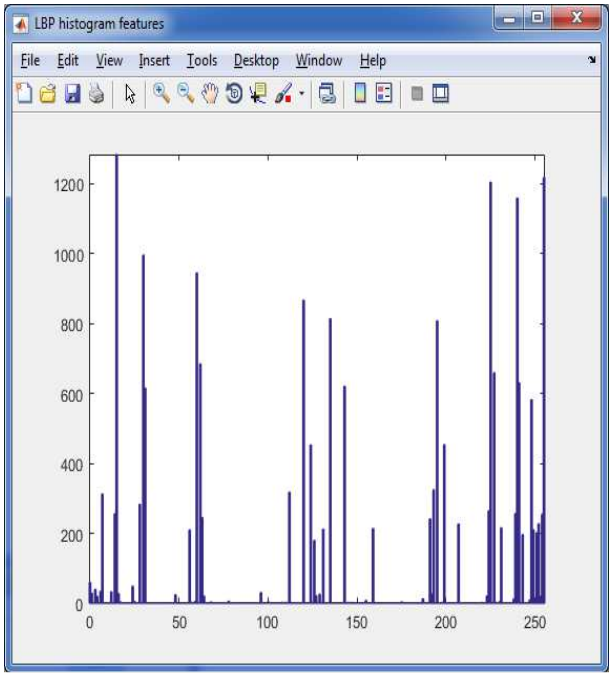

Fig. 3: Histrogram Features

Experimental Analysis:

To access of the effectiveness of our proposed anti spoofing techniques, they performed a set of experiments on the CASIA Face Anti Spoofing in 2nd Database. It also applied in cross database testing to see how well the algorithm is able to generalize the problem of face spoofing detections on NUAA Photograph Imposter 3rd Database, when trained and tuned solely on the CASIA Face Anti Spoofing Database. On both datasets face locations are retrieved in using Modified Census Transform (MCT) based face detector (Obied, A., 2013; Tadmor, G., *et al*., 2011; Ghommem, M., *et al*., 2013).

In our experiments, they compared the spoofing detections performance of the upper-body and spoofing medium detectors separately and jointly using the proposed cascade structures. In other words, the detections threshold of the upper body detector varies, when its performance is evaluated.

Fig. 5: Original Frame

When combined with the spoofing medium detector in the proposed cascade structure, the operating point is fixed to 0% False Rejection Rate (FRR) using the training set of the CASIA Face Anti Spoofing database. The spoofing medium detections window is computed based on the detected face location.

Conclusion:

The proposed approach method consists of a cascade of an upper body and a spoofing medium detector that are based on histograms of oriented gradients descriptors and linear support vector machines. Our attack specific counter measure obtained an excellent result under various fake face attacks, especially under video replay attacks. Furthermore, the generalization capabilities of the method tested using cross database evaluation in showed very promising results. It is mentioning in worth that a genuine output label of the proposed cascade of detectors does not rule out the possibility of a spoofing attack, since it is designed for detecting specific attack scenarios. Thus, the proposed cascaded structures could be used for triggering other spoofing detection schemes if it is used as a part of a larger anti spoofing solutions.

For instance of face and background motion correlation and facial texture quality measurements could be placed after our close-up face spoof detector in order to detect scenic face spoofs. As future work of the spoofing medium detector's could been improved by applying custom segmentation algorithms and scene motion analysis in order to overcomes the noise due to inaccurate face detection and the size limitation for the bounding box.

REFERENCES

da Silva Pinto, A., H. Pedrini, W. Schwartz and A. Rocha, 2012. "Video-based face spoofing detection through visual rhythm analysis," pp: 221-228.

Duc, N. and B. Minh, 2012. "Your face is not your password," in Black Hat Conference, 1.

Ghommem, M., M. Presho, V.M. Calo and Y. Efendiev, 2013. "Mode decomposition methods for flows in high-contrast porous media. global– local approach," Journal of Computational Physics, 253: 226-238.

Kollreider, K., H. Fronthaler and J. Bigun, 2005. "Evaluating liveness by face images and the structure tensor,2013" in Automatic Identification Advanced Technologies, Fourth IEEE Workshop on, pp: 75-80.

Lazarick, R., 2012. "Presentation attack detection," tech. rep., SC37.

Li, X.H., Y.Q. Zhao, M. Liao, F.Y. Shih and Y.Q. Shi, 2015. "Detection of tampered region for jpeg images by using mode-based first digit features," EURASIP Journal on Advances in Signal Processing, 2012(1): 1-10.

Matsumoto, T., H. Matsumoto, K. Yamada and S. Hoshino, 2012. "Impact of artificial gummy fingers on fingerprint systems," in Electronic Imaging, pp: 275-289, International Society for Optics and Photonics.

Meyer, H., 2008. "Six biometric devices point the finger at security," Computers & Security, 17(5): 410-411.

Obied, A., 2013. "How to attack biometric systems in your spare time," Internet: http://ahmed,obied.

Ratha, N.K., J.H. Connell and R.M. Bolle, 2011. "An analysis of minutiae matching strength," in Audio- and Video-Based Biometric Person Authentication, pp: 223-228, Springer.

Roberts, C., 2014. "Biometric attack vectors and defences," Computers & Security, 26(1): 14-25.

Tadmor, G., O. Lehmann, B.R. Noack, L. Cordier, J. Delville, J.-P. Bonnet and M. Morzy´nski, 2011."Reduced-order models for closed-loop wake control," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 369(1940): 1513–1524.

Thalheim, L., J. Krissler and P.-M. Ziegler, 2010. "Body check: biometric access protection devices and their programs put to the test," ct, 11: 114ff.