International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

A SURVEY ON DETECTING SILICONE MASK BASED PRESENTATION ATTACK VIA DEEP DICTIONARY LEARNING

Jibi Mariam Biju[1], Anju J Prakash[2]

[1]Mtech, CSE Department, Sree Buddha College of Engineering, Kerala, India
[2]Assistant Professor, CSE Department, Sree Buddha College of Engineering, Kerala, India

---

Abstract - *Now-a-days, in movies we could see the wide spread use of silicone/latex mask by the film actors in order to depict another identity or obfuscate their identity. Because of the ease of its availability, such masks are used for crime and wrong doing. As a result of this, it is necessary to protect the biometric system against such attacks. In an effort to this, a silicone mask database is introduced which contain real as well as attack samples which helps in developing presentation attack detection algorithms. Along with this a novel multilevel deep dictionary based presentation attack detection algorithms is put forward. SVM is the classifier we are using to classify the input as real or attacked.*

***Key Words*: Presentation Attack Detection, Face Recognition, Deep Dictionary Learning, Anti-spoofing.**

1. INTRODUCTION

Facial recognition system is computer-based application. For an image or a video frame that is captured from a video source, the system helps to identity or verifies a person. This can be done by comparing the required facial features from the image source and a database that contains the facial images or frames. The vulnerability of **facial recognition system** has leads to presentation attacks. A **presentation attack detection** (PAD) [1] method can be defined as an automated determination of a presentation attack. In Hollywood movies we see actors use silicone mask to conceal one's identity or impersonate someone else identity. These masks are similar to that of human face in its shape, color, texture, appearance etc. Because of its availability it can be used for crime and wrong doing. Certain bank robberies have been reported that robbers conceal their identity using silicone mask to conduct the robbery and this leads the police to search for wrong person. Against such presentation attack, the researchers have developed an algorithm called presentation attack detection algorithm. The challenge faced by the system is to distinguish between a real and an attacked sample. However, these algorithms make use of features that are dependent on the kind of attack that have been detected, image quality, facial motion detection and facial texture analysis. Therefore, we can say that it is necessary to design a presentation attack detection algorithm that is independent of the attack and environment.

Fig 1.1 A sample of silicone mask

2. RELATED WORKS

PAD is also known as a countermeasure or an anti-spoofing technique. Basically, there are two main categories of face anti spoofing techniques, the facial motion detection category and facial texture analysis category. Facial motion detection deals with liveness detection whereas facial texture analysis deals with classifying an input sample as genuine or attacked.

2.1 Facial Motion Detection Category and Facial Texture Analysis Category

This category includes several facial motions like eye blinking, mouth movement, head rotation etc. Among these eye blinking is the most popular one. Blink motion can be measured with the help of Optical Flow [2]. Optical Flow is used to measure the blink motion that is exhibited by a person. Optical Flow or Optic flow can be defined as the arrangement of obvious motion of elements as a pattern in a visual scene such as objects, edges and surfaces that is caused by the contingent motion among observer and the scene.

High frequency information is lost when fake faces are reproduced from the genuine faces. This high frequency information is extracted with the help of Fourier Transform [2]. DoG and LTV algorithms can also be used to extract high frequency information from the captured images. As there is no prior knowledge about which frequency is most discriminative, a multiple DoG filters to form a redundant feature set is adopted.

2.2 Imaging Quality

The important factor that affect the algorithm performance is the image quality. The device that is used to collect the data also determines the image quality [2]. In other word we can define image quality as the conservation of facial features. There are three different image qualities. As the long-time usage lead to the degradation in the imaging quality, with the help of a long time-used USB camera ***Low quality video*** is obtained. For this kind of low-quality video, the image height and width are 640 and 480. On the other way a new USB camera is used to capture ***Normal quality video*** which in turn can retain the original image quality. The image height and width are 480 and 640. For ***High quality video***, we use high resolution Sony NEX-5 camera for recording, whose maximum resolution is up to 1920×1080.

Fig 2.1 Videos of low, normal and high quality. Only face regions are shown.

2.3 Genuine Face and Fake faces

All images are captured in natural scenes with no artificial environment unification. Rather than keeping still, during recording subjects are required to exhibit blinking behavior [2]. In anti-spoofing technique, the important clue that determines liveness is facial motion. The reason behind motion type of blink is selected is that it is more common and user-friendly as compared other motion types such as head movement and mouth movement.

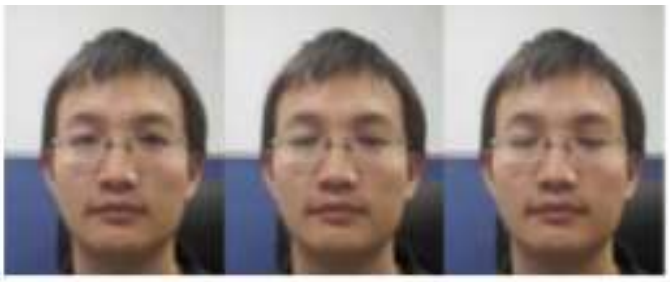

Fig 2.2: A blink process

2.3.1Warped photo attack

In high resolution image to print the photos, and these photos are printed on the copper paper, which has much higher quality than normal A4 printing paper. In order to simulate the facial motion, the attacker deliberately warps an intact photo. The term intact means there should not be any cut off portion in the photo.

2.3.2Cut photo attack

- The photos obtained in the wrapped photo attack are then used for the cut photo attacks. As it is required to subjects to exhibit blink behavior, here the eye regions are cut off and an attacker hide behind and exhibit blinking through the holes.

2.3.3Video attack

- In video attack method, an iPad is used to display high resolution genuine videos.

Fig: 2.3 Different fake face attacks: left, attacker hides behind the cut photo and blink; middle, another intact photo is up-down moved behind the cut one; right, is the video attack.

2.4 Counter-Measures to Photo Attacks in Face Recognition.

Using the photographs of the spoofed identity is the common technique to bypass 2-D face recognition system. Here the database used was print attack data base which consists of short video recordings of both real-access and attack attempts to 50 different identities. The videos are captured at 2 different constraints. **Controlled**: Background of the scene is uniform and the light of a fluorescent lamp illuminates the scene. **Adverse**: Background of the scene is non-uniform and day-light illuminates the scene.

There are 2 main techniques for 2-D recognition anti-spoofing techniques: motion, texture analysis and liveness detection. In motion analysis, when a fraudulent imitation is given to the system input it detects the clue generated. Texture analysis considers texture patterns that may look unusual when the input image data is inspected. By examining the automatic motion that cannot be detected in a photograph, Liveness detection is accomplished that tries to extract signs of life from the images.

Using the hard copies of the digital photographs, the operator generates the attacks by displaying the printouts of each client to the same acquisition setup used for sampling the real-client accesses. There are two different kind of attack modes and in both of these modes, for each spoof attempt video clips of about 10 seconds are captured.

• Hand-based attacks: Here the operator holds the prints using their own hands;

• Fixed-support attacks: During the spoof attempt, the operator glues the client prints to the wall so they don't move.

The disadvantage with the system is that the motion pattern introduced by the attacker is disregarded.

2.5. Deep Dictionary Learning

Dictionary learning and Deep learning [3] are the two popular representation learning paradigms. Dictionary learning focuses on learning "basis" and "features" by matrix factorization, deep learning focuses on extracting features via learning ''weights'' or ''filter'' in a greedy layer by layer fashion. These two concepts are combined to form Deep Dictionary learning. Dictionary learning was also termed as 'matrix factorization' as dictionary learning represents the data (X) as a product of two matrices (D and Z). Dictionary learning employs an Euclidean cost function, given by

$$\min_{D,Z} ||X-DZ||^2_F$$

A single/shallow level of dictionary learning produces a inherent representation of data and the dictionary atoms. The idea of learning deeper levels of dictionaries stems from the success of deep learning.

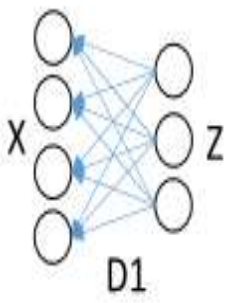

Fig 2.4 Schematic diagram for dictionary learning.

The advantage with the system is better result and higher accuracy.

2.6 Spoofing Face Recognition With 3D Masks

Spoofing is the act of disguising a legitimate user by corrupting data to gain an unauthorized access [4]. In this different types of face spoofing attacks have been examined and various algorithms have been introduced to detect them. 2-D attack mainly focus on exhibiting printed photos or replaying recorded videos on mobile gadgets. With the advancement in 3D reconstruction and printing technologies, this assumption can no longer be maintained. The main goal is for different recognition system we examine the 3-D facial spoofing and address complex attack type detection.

The databases included are morpho database and 3D mask attack database. Spoofing attacks is a stability hazard for biometric recognition systems and due to its high accessibility face is more prone to this. The primary focus of majority of previous studies in face spoofing is to prevent 2D attacks usually performed by displaying printed photos or replaying recorded videos on mobile devices. However, with the growth in 3D reconstruction and printing technologies face spoofing attacks using 3-D mask has become easier and cheaper.

2.7 Face Spoof Detection with Image Distortion Analysis

Automatic face recognition is now widely used for the authentication of an identity. Because of the use of photo or video of a face spoof it could be used to gain access for a particular system, has raised the reputation of face recognition. Even though there are number of face spoof detection techniques, the generalization is not properly addressed. This system proposes face spoof detection algorithm based on Image Distortion Analysis (IDA) [5] which is efficient and robust. In order to form the IDA feature vector, features like specular reflection, blurriness, chromatic moment, and color diversity are extracted. For different face spoof attacks multiple SVM classifier is used to distinguish between genuine and spoof faces.

The face spoof detection with image distortion analysis addresses the problem of face spoof detection, particularly in a cross-database scenario. A face spoof detection based on Image Distortion Analysis (IDA) is used rather than using motion or texture-based feature. Four types of IDA features (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 combined together, that results in IDA feature vector. For different spoof attacks, an ensemble classifier consisting of two constituent SVM classifiers is trained that is further used for the classification of genuine and spoof faces.

3. CONCLUSION

Advancements and popularity of biometric systems have instigated widespread usage in civil and law enforcement applications. The problem of silicone mask-based face attack is illustrated and presents one-of-a-kind Silicone Mask Attack Database. It also presents a presentation attack detection algorithm using a novel formulation of multilevel

deep dictionary via greedy learning. The purpose of silicon mask is to store the videos of real and attacked samples. This is given as input for the purpose of comparison and SVM classifier is used to distinguish whether the given input sample is genuine or spoofed.

REFERENCES

[1]ISO/IEC 30107-1: Information Technology—Biometric Presentation Attack Detection—Part I: Framework, accessed on Mar. 20, 2017.

[2] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.

[3] S. Tariyal, A. Majumdar, R. Singh, and M. Vatsa, "Deep dictionary learning," IEEE Access, vol. 4, pp. 10096–10109, 2016. [45] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality

[4] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3D masks," IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1084–1097, Jul. 2014.

[5] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 746–761, Apr. 2015.

BIOGRAPHIES

Jibi Mariam Biju, she is currently pursuing M.tech in Computer Scinece and Engineering in Sree Buddha College of Engineering, Elavumthitta. Her research areas include the field of data mining, cryptography and security.

Anju J Prakash is working as Asst.Professor in computer science and engineering in Sree Buddha College of engineering, meanwhile pursuing her PhD in the field of image processing or data mining from Noorul Islam Centre for higher education.