International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 2, Mar-Apr-2019,ISSN (Online): 2395-566X

A Review on Different Face Spoof Detection Techniques in Biometric Systems

M. Tech. Scholar Kanika kalihal Asst. Prof. Jaspreet Kaur
Dept. of Electronics and Communication
Rayat & Bahra Institute of Engineering & Bio-Technology
Mohali, India

Abstract **- Biometric systems are increasingly used in different security systems for the last few years. Fingerprints, Iris recognition, face recognition systems have grabbed attention from academicians and researchers all over the world. But there are certain issues associated with these systems that make them vulnerable. One such issue is the spoof attack in which an impostor attacks the system by presenting a printed photograph of the genuine user to the system. These attacks compromise the security of the system and therefore need to be addressed. This paper presents an overview of different techniques that are used in face spoof detection and discussed parameters that are used to evaluate the performance of different face spoof detection techniques.**

Keywords- **Spoof attack, Local binary pattern, Histogram of gradient**

I. INTRODUCTION

Passwords, pins and ID cards have been traditionally used in authentication for identifying an individual. But these systems suffer some drawbacks like the IDs can be easily stolen and password and pins can be hacked. An alternative for this is biometric systems which recognise an individual based upon his/her behavioural or physiological traits that include facial features, fingerprints and voice [1]. These traits are unique therefore provide a better level of security .But these systems are susceptible to spoof attacks.

With high resolutions digital media devices and social media it is very easy to acquire face images of a target person. The attacker can easily download photos or videos of the authorized user, print it and then present it to the biometric system to gain illegitimate access to the system. To ensure reliability of the face recognition system various face spoofing methods have been developed. This paper evaluates different methods and techniques that are being used in face spoof detection. A typical biometric system broadly contains database, feature extractor and classifier.

1. Feature extractor

Important features are extracted from the training and test images in the feature extractor. These features help in determining real images from fake images.

2. Database

The extracted features from the training and test data are stored in the database. Input image are stored in the test dataset and the training images are stored in the training dataset.

3. Classifier

Classifiers categorize the input data into distinct number of classes and decide whether it is real or fake.

The rest of the paper is summarised as follows: Section 2 discuss various types of spoof attacks. Section 3 describes methods use for face spoof detection.
And discuss various parameters used to evaluate face spoof detection system. Finally there is conclusion at section 4

II. DIFFERENT TYPES OF SPOOF ATTACKS

Research is going on in the field of face spoof detection from the last few years. This section discuss various spoof attacks and the methods use for face spoof detection. There is a growing popularity of face recognition system in access control. Not only industries but mobile phones companies are also integrating these systems in their devices for locking and unlocking the phones. Several research articles, journals and conferences came with innovative ideas for providing security to face spoof detection system. Figure A represents spoofing attacks on a face recgnition system which is broadly classified into two types 2D and 3D spoofing.

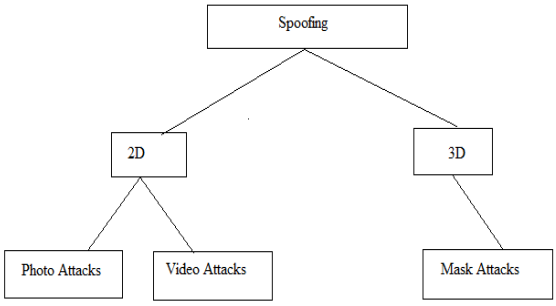

Fig.1 Spoofing Attacks.

© 2019 IJSRET

1. Photo attack
In this attack a fraudulent attempts to attack the system by presenting a photograph of the authorised user. Attackers can either capture the pictures from a digital device such as a camera or a mobile from a distance without taking permission from the genuine user or can acquire pictures from social media platform. The attacker either prints the image or displayed it on a digital device for deceiving the face recognition system.

2. Video attack
Replay attack or video attack is a sophisticated way to trick a biometric system. In this attack irrespective of still images, the attacker uses the video of the user which contains the behaviour traits of an individual like eye blinking and facial expressions. Video attack looks more natural to the face recognition as compare to a print photo.

3. Mask attack
Masks attacks are broadly classified into two type paper cut mask and life size wearable mask. These attacks are more sophisticated then the video attack as they can deceive several layers of security provided to face recognition system. For detecting 3D mask attacks expensive 3D printers and other special devices are used.

III. DIFFERENT METHODS FOR FACE SPOOF DETECTION

Face spoof detection techniques counter measure spoof attack in which an impostor tries to deceive the system. Face spoof detection techniques are classified into one of the two groups depending upon in which biometric module they are used

1. Hardware based techniques
In these techniques specific devices are added to the sensor which can detect traits of an individual like blood pressure, thermo gram or specific eye properties. Hardware based or sensor based techniques generally measure one of the three properties which include physical properties such as elasticity and density, electrical properties like resistivity or permittivity, spectral properties, visual properties such as colour of the eye.

These techniques also include behaviour or reflex actions of the body in response to an external signal which require user cooperation. This can be done by instructing the user to perform a specific movement of the hand, shoulder or eye or by asking some challenging question. The hardware based techniques are effective as they provide the depth of the samples which are being observed. But they are hard to implement on mobile phones and tablets. However in the near future mobile phones companies can integrate multiple sensors in their device.

2. Feature based techniques
Features based techniques are usually referred as software based techniques in which fake images are detected by extracting features from the biometric samples. They are used after the sensor in the feature extraction modules. Broadly they are classified into frequency, texture and motion anti spoofing methods.

2.1 Frequency based
Jiangwei Li [8] implemented face liveliness detection by analysing high frequency descriptors. The authors calculate the ratio of high energy components to all the frequency components in the image and finally the standard deviation of the frequency components are computed to represent the temporal changes of the face.

2.2 Texture based
Texture provides detectable information between the real and fake images. This method extracts image artifacts from the fake images and countermeasure photo and replay video attack. In [11] authors implemented two feature extraction algorithms Local binary pattern (LBP) and GLCM (Gray level Co-Occurrence matrix).

The proposed work shows that the LBP performed better than GLCM in terms of accuracy, with LBP giving 99.07% accuracy and GLCM giving 92.82%. Using the combination of LBP and GLCM the proposed system achieved an accuracy of 99.26. The authors of [12] proposed a face anti spoof detection system which implements texture features descriptors Gabor wavelength, HOG and LBP. While LBP provides powerful means for texture description, gabor wavelength enhance the textural representation of the image. The histogram of gradient (HOG) features is further used to capture edges in the face image.

2.3 Motion based
In motion based methods the subconscious motion of an organ or a muscle is captured such as eye movement, head rotation. These methods has more generalised approach than the texture methods. Optical flow algorithm [6] finds the correlation between the head of the user and background which helps in determining the possible spoof attack. OFC estimates precise motion parameters from two region of interest and compare their value to obtain a correlation score. However there are some limitations to motion based methods, they take a relatively long time to obtain stable features for face spoof detection.

IV. DETECTION EVALUATION PARAMETERS

Five common parameters used for the evaluation of face spoof detection system are: FAR(False acceptance rate), FRR(false rejection rate with corresponds to minimum or zero false attempt accepted by the system), HTER(Half total error rate), accuracy(Determines how accurate the system is) and EER (equal error rate). These parameters help in determining real threats that

© 2019 IJSRET

affects any face recognition system by a spoofing database.

V. CONCLUSION

In this paper various spoof attacks that can harm any biometric system are discussed. And different methods used to counter measure these attacks are described. The paper broadly classified two level approaches hardware level and feature level. Specific devices are integrated on hardware level approaches which results in additional cost to the system. Feature approach however discussed the discriminative features in an image. We have found that there is no single method that can achieve all the requirements of an ideal biometric system. Therefore research is still required in this field to develop a reliable security technique.

REFERENCES

1. J. Galbally, S. Marcel, and J. Fierrez, 2014."Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," IEEE Trans. Image Process. vol. 23, no. 2, pp. 710– 724.
2. T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, 2012." LBP-TOP based countermeasure against face spoofing attacks," in Proc. ACCV Workshops.
3. Hoai Phuong Nguyen, Florent Retraint, Frederic Morain-Nicolier, Agnes Delahaies, "Face Spoofing Attack Detection Based On The Behavior Of Noises", 2016, Ieee
4. Xiao Luan, Huaming Wang, Weihua Ou, Linghui Liu, "Face Liveness Detection with Recaptured Feature Extraction", 2017 in International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)
5. Wang, Tao, Jianwei Yang, Zhen Lei, Shengcai Liao, and Stan Z. Li. "Face liveness detection using 3D structure recovered from a single camera." in Biometrics (ICB), 2013 International Conference on, pp. 1-6. IEEE, 2013.
6. A. Anjos, M. M. Chakka, and S. Marcel, "Motion-based countermeasures to photo attacks in face recognition," IET Biometrics, vol. 3, no. 3, pp. 147–158, Sep. 2014
7. Nayar, Shree K., and Yasuo Nakagawa. "Shape from focus." Pattern analysis and machine intelligence, IEEE Transactions on 16, no. 8 (1994): 824-831
8. J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," Proc. SPIE, Biometric Technol. Human Identificat., pp. 296–303, Aug. 2004.
9. Okereafor, Kenneth, and Clement Onime. "Enhancing Biometric Liveness Detection Using Trait Randomization Technique."
10. S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh,2013. "Computationally efficient face spoofing detection with motion magnification," Proc.CVPR Workshops. IEEE Trans. Image Process. vol. 23, no. 2, pp. 710–724.
11. F Sthevanie, K N Ramadhani. "Spoofing detection on facial images recognition using LBP and GLCM combination" in International Conference on Data and Information Science.
12. Taha J. Alhindi1,2,3 , Shivam Kalra∗1,3 , Ka Hin Ng3 , Anika Afrin4 , Hamid R. Tizhoosh1. "Comparing LBP, HOG and Deep Features for Classification of Histopathology Images".
13. Patrick P. K. Chan, Weiwen Liu, Danni Chen, Daniel S. Yeung, Fei Zhang , Xizhao Wang, and Chien-Chang Hsu, "Face Liveness Detection Using a Flash Against 2D Spoofing Attack" 2017 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
14. Shervin Rahimzadeh Arashloo, Josef Kittler and William Christmas, "An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol" 2017 IEEE. Translations and content mining

© 2019 IJSRET