**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 6.017**

***IJCSMC, Vol. 8, Issue. 3, March 2019, pg.166 – 171***

# Analysis of Face Spoof Detection Technique

**Nidhi Sharma**
Research Scholar, Bhagwant Institute of Technology, Muzaffarnagar, UP, India
95nidhisharma06@gmail.com

**Mrs. Shivani Chauhan**
Assistant Professor, Bhagwant Institute of Technology, Muzaffarnagar, UP, India
shivanichauhanbit@gmail.com

***Abstract: The face spoof technique was proposed to identify and detect the spoofed and non-spoofed images. The DWT technique is used to analyze the textual features present within the test images. There is a possibility that some exceptional disturbances are available like geometric disturbances and the artificial texture disturbances. The camera and the illumination subordinates are mostly responsible for such disturbances. A perfect camera with no defects should be used just to notice the difference between the geometric, the illumination and the texture based disturbances. To detect the whether the image is spoofed or non-spoofed already existed technique SVM classifier is used. The SVM based technique is proposed in the previous work for the detection of face spoof. The face spoof detection techniques are based on two steps; the first step is of feature extraction and second is of classification. The Eigen based technique is applied for the feature extraction and SVM classifier is applied for the classification. To improve accuracy of the face spoof detection SVM classifier will be replaced with the KNN classifier.***
***KEYWORDS: SVM, KNN, Machine learning, DIP***

## Introduction

Image processing is defined as the process use to perform some operation on the images, which generate an enhanced version of the images or extract some features from it. It signal processing in which image act as the input and characteristic or features act as the output of that image. Image processing is very widely used and growing technology and plays a core role in the research field, as lot of research is still going on in this field. There are two methods available for the image processing mechanism that is analogue and digital image processing. Analogue image processing is the technique which is used for hard copies like printouts and photographs. Image analysts require different types of fundamental during the use of visual techniques. Digital image processing is the techniques which help in the manipulation of the digital images with the help of computers [1]. All the data have to pass through the three types of phases that is pre-processing, enhancement and information extraction. Face recognition is also one of the very widely used security purpose used technique. As the numbers of crimes are increasing day by day, so to maintain the proper check on the people such type of methods are employed on various fields like banks, hospitals, industries and so on. There is huge success in this area, by applying them on several

 

applications like human-computer interaction (HCI), biometric analysis, content-based coding of images and videos, and surveillance. Face recognition is proved to be very difficult to imitate artificially, although there are certain similarities in some faces most probably due their age, gender, color. The biggest problem this method is facing is image quality, expressions, background and other climatic conditions [2]. Face detection as the name suggests, it suggests where the face is located in an image. As it seems to be very easy task but in reality it is very difficult to detect images. We have to consider all the possible constraints like single face or multiple faces, image rotation, pose etc. this give rise to some false detection of an image, or it sometimes does not contain any image. There are various types of techniques available for face detection. Face detection as the name suggests, it suggests where the face is located in an image. It seems to be very easy task but in reality it is very difficult to detect images [3]. We have to consider all the possible constraints like single face or multiple faces, image rotation, pose etc. this give rise to some false detection of an image, or it sometimes does not contain any image. There are various types of techniques available for face detection. When someone tries to interferes in the face biometric system by presenting a false face towards the camera. It attacks on face recognition systems which involve all the artificial faces of authorized users to cleverly go inside the biometric security systems. These attacks are very easy to carry by just having printed photographs or digitalized images being displayed on the screen. If we want to differentiate between the real face features from fake faces, the face liveness technique is used. It aims at detection of physiological signs of life. Biometric technologies are used to measure and analyze human body characteristics. It can be categorized into two parts, physical characteristics in which fingerprints, faces or iris patterns are used and then activity characteristics which includes voice signatures or strolling patterns [4]. It is the most prominent challenge being varied in biometric systems. The variations involve chances of fraud which is most commonly known as spoofing attack. The stolen data will effectively ruin and mimicked by the adversary to have a unauthorized access to the systems. This technique is based on facial statistics in the light weighing physiological properties detection. Moreover, the false faces are of two types i.e. positive and the negative one. The positive faces are real faces and having restricted variation and negative includes spoof faces on images, dummy and so on. Spoofing attack is type of attack in which the attacker submits the fake identity and evidence to the biometric system in order to get access to the network. It is very easy for the attacker to generate attack in the face recognition system because the images and videos are easily available on the social networking sites [5]. The attacker can store images from the social networking sites or the attacker can capture the image of any person from a distance, so that it can be clear and visible. Face spoofing is of two types that is 2D spoofing and 3D spoofing. These are further divided in various attacks like photo attack, video attack and mask attack, as shown the figure. It is very easy for the attacker to get the photos and video of any individual due to the advanced internet technology. 3D mask attack is easily available in the market [6]. This attack requires face modality. Photo Attack is the type of 2D spoof attack and the attacker shows the photo of the person to the biometric modality in order to get an access to the mobile phone screen, laptop, tablets etc. Video Attack is the advanced version of the photo attack. The attacker captures the video of the genuine individual by using mobile phone, tablet and digital camera, then during face recognition the attacker play that video and get access to the biometric system modality just have the proper movement of the facial part. Therefore, it is very difficult to detect. 3D Mask Attack is the updated version of both the photo attack and the video attack. In this the attacker creates 3D mask of the genuine person which is quite similar to the genuine individual [7]. It is very time consuming task and provides better solutions against identity of the authentic person. It is less common and not that much used as compared to other two attacks. The 3D mask is generally made up of different materials like paper, plastic, plaster or silicon.

# Literature Review

**Yaman, et al. [8]** studied that the identity as well as liveness of the input of face can be known through a reliable face-based access system. Thus, several feature-based spoof face detection techniques have been proposed by different researchers. For detecting the liveness of a face, a series of processes are applied on the input image. A deep-learning based face spoof detection approach is proposed in this paper by using two various deep learning methods. The local receptive fields (LRF)-ELM and CNN are known to be these two methods. NUAA and CASIA are the two common face spoof detection databases on which the experiments were conducted to evaluate the performance of proposed approach. The performance of LFR-ELM approach was known to be better within both the databases as per the comparisons made towards the end.

 

**Killioglu, et.al [9]** presented a study to detect the liveness of spoofing of facial recognition system with the help of mobility of a fake face. Common hardware equipment was used to develop a pupil direction observing system such that the anti-spoofing systems could be benefitted. The Haar-Cascade Classifier was used initially to extract the eye area from the real time camera. To detect the eye region, a trained classifier was used. To reduce the head movements of an individual, the extraction and tracking of feature points was done. From a real time camera frame, the eye area is cropped and for providing a stable eye region, the rotation is performed. A new improved algorithm is used to extract the pupils from the eye region. To check whether the direction of pupil and the position of LED match, the direction of eye is observed once the selected LED is activated. The data that includes liveness information is given as output by the algorithm in case if the compliance's needs are satisfactory. High success ratio is achieved as per the experiments conducted using this proposed approach.

**Keyurkumar, et.al [10]** presented a study on the smartphone unlock systems that are today very popular within several mobile phones and also within the systems that include mobile payments. An unconstrained smartphone spoof attack database (MSU USSA) that includes not less than 1000 subjects is generated here. Using the front as well as rear camera of a smartphone, the images of print and replay attacks are gathered. Various intensity channels, image areas, as well as feature descriptors are used for analyzing the image distortion of print and replay attacks. The Android smartphone is used to develop an efficient face spoof detection approach. As per the experiments conducted it is seen that to detect the face spoofs of both, cross-database and intra-database testing environments, the proposed approach provided effective results. There were around 20 participants included within the evaluations which showed that the performance of proposed approach within real applications was very good.

**Alotaibi and Mahmood, [11]** proposed an efficient mechanism using static frame of sequenced frames in order to solve the face spoofing attack issues. For creating a speed-diffused image, an AOS-based scheme was applied along with a large time step size. The sharp edges and texture features present within the input image are extracted by applying large time step parameter. When the input video was recaptured twice, it was seen that around the eyes, nose, lips and cheek areas, there were few sharp edges and flattened regions present within the fake face images. Thus, the sharp edges were destructed and the locations of pixels were changed due to this. The edges were destroyed using a large time step. The sparse auto-encoder was to be explored such that a diffused frame could be achieved in the future work. Therefore, the diffused frame would be generated to be given to the deep CNN network by generating an auto-encoder within the overall architecture within the future work.

**Shervin, et.al [12]** presented a study related to the issues faced when detecting the face spoof. It is possible to include new means of spoofing attackers as per the various observations made. The image sensor inter-operability issue and the minimal size of a sample are few of the issues that have come forward within this work. This paper initially proposed a new evaluation protocol through which the effects of unseen attack types could be known on the basis of certain existing factors. This paper proposed a novel and highly realistic formulation of the spoofing detection issue with respect to the conceptual innovations. To train the systems, only the positive samples were needed by the new formulation. Towards the end, the experiments conducted showed that there was still the need to improve the detection rates since the performance of both the schemes was not up to the mark.

**Hoai, et.al [13]** presented a study related to the facial recognition systems in which the issues of spoofing attacks were solved. The surfaces of real faces and falsified faces showed differences of micro-textures when placed in front of a security system. Thus, for discriminating the face spoof images, these differences were highlighted. The distribution of local variances of noise had a static behavior that was exploited by this method. It was seen that in case of real and face faces, this method performed differently. The two various databases that were constructed by the authors were used to test the proposed approach by using a classification technique known as SVM. The performance of proposed approach was seen to be much better as per the experimental results achieved.

**Xiao, et.al [14]** presented a novel mechanism for addressing the issue of face liveness detection in which the various recaptured features were extracted. In the form of discriminative features, the reflection ratio, Hue channel distribution and blurriness were considered here. Further, for classifying the live subjects and impostors, SVM was applied. The

 

differentiation of genuine user's face and spoof faces was very important for a safe face recognition system. Mostly, for addressing the face spoofing issues, the unreliable and less robust face liveness approaches were applied that included the involvement of only single image feature. In terms of efficacy and detection rate, the proposed approach was known to provide better results. Also, the performance of all approaches was affected negatively due to the illumination changes occurring in the images.

**Olegs, et.al [15]** presented a study related to the face anti-spoofing mechanisms. Through the huge diversity of spoofing attacks within the realistic applications as well as the generalization issues that are relevant to the PA detectors present within the tests that result in causing the unseen spoofs, the proposed work is motivated. A new evaluation protocol was designed for highlighting the mentioned generalization issues. Thus, during the presence of unseen attacks, the PAD algorithms were studied through this proposed protocol. For the proposed aggregated database, these protocols are proposed that included Replay-Attack, Replay-Mobile and MSU MFSD which are the three different sets available publically. To introduce a challenging set as compared to any individual components, the data collection efforts of several institutions were combined to generate an aggregated database. Moving towards the more realistic evaluation environments, huge varieties of photo and replay attacks were included in the proposed approach.

| Authors Names | Year | Description | Outcomes |
|---|---|---|---|
| Yaman, Abdulkadir Sengur, Ümit Budak, Sami Ekici | 2017 | A deep-learning based face spoof detection approach is proposed in this paper by using two various deep learning methods. The local receptive fields (LRF)-ELM and CNN are known to be these two methods. | The performance of LFR-ELM approach was known to be better within both the databases as per the comparisons made towards the end. |
| Killioglu, M. Taskiran, N. Kahraman | 2017 | A new improved algorithm is used to extract the pupils from the eye region. A random direction is chosen by the proposed spoofing algorithm once the few stable numbers of frames that include pupils were identified. | High success ratio is achieved as per the experiments conducted using this proposed approach. |
| Keyurkumar, Hu Han, and Anil K. Jain | 2016 | An unconstrained smartphone spoof attack database (MSU USSA) that includes not less than 1000 subjects is generated here. Using the front as well as rear camera of a smartphone, the images of print and replay attacks are gathered. | There were around 20 participants included within the evaluations which showed that the performance of proposed approach within real applications was very good. |
| Alotaibi and Mahmood, | 2016 | An efficient mechanism was proposed using static frame of sequenced frames in order to solve the face spoofing attack issues. For creating a speed-diffused image, an AOS-based scheme was applied along with a large time step size. | In case when a time step of $\tau = 100$ and number of iterations, $L = 5$ were applied, around 10% of HTER was achieved which was the best classification results achieved by the proposed approach. |
| Shervin, Arashloo, Josef Kittler, and William Christmas | 2017 | This paper initially proposed a new evaluation protocol through which the effects of unseen attack types could be known on the basis of certain existing factors. | The experiments conducted showed that there was still the need to improve the detection rates since the performance of both the schemes was not up to the mark. |
| Hoai Phuong Nguyen, Florent Retraint, Frederic Morain-Nicolier, Agnes Delahaies | 2016 | The surfaces of real faces and falsified faces showed differences of micro-textures when placed in front of a security system. Thus, for discriminating the face spoof images, these differences were highlighted. | The performance of proposed approach was seen to be much better as per the experimental results achieved. |
| | | | |

 

| | | | |
|---|---|---|---|
| Xiao, Huaming Wang, Weihua Ou, Linghui Liu | 2017 | A novel mechanism was proposed for addressing the issue of face liveness detection in which the various recaptured features were extracted. In the form of discriminative features, the reflection ratio, Hue channel distribution and blurriness were considered here. | In terms of efficacy and detection rate, the proposed approach was known to provide better results. Also, the performance of all approaches was affected negatively due to the illumination changes occurring in the images. |
| Olegs Nikisins, Amir Mohammadi, Andre Anjos, Sebastien Marcel | 2018 | A new evaluation protocol was designed for highlighting the mentioned generalization issues. For the proposed aggregated database, these protocols are proposed that included Replay-Attack, Replay-Mobile and MSU MFSD which are the three different sets available publically. | Moving towards the more realistic evaluation environments, huge varieties of photo and replay attacks were included in the proposed approach. |

## Conclusion

Face spoof technique is proposed to identify the spoofed faces added due to the unauthorized access to the data. The face spoof detection methods have the two steps which are feature extraction and classification. The techniques of Eigen vector are applied for the feature extraction and SVM is applied for the classification in the existing technique. It is analyzed that accuracy is reduced for the face spoof detection when SVM classifier is applied. In this research work, the technique of SVM is replaced with KNN which increase accuracy of face spoof detection. The simulation of proposed and existing method is done in MATLAB by considering AT & T dataset. The performance analysis is done in terms of two parameters which are accuracy and execution time.

# References

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

[2] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in Proc. ECCV, Sep. 2010, pp. 504– 517.

[3] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in Proc. ICB, Mar./Apr. 2012, pp. 26–31.

[4] L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live face detection using conditional random fields," in Proc. AIB, 2007, pp. 252–260.

[5] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in Proc. IASP, Apr. 2009, pp. 233–236.

[6] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2013, pp. 105–110.

[7] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," Proc. SPIE, vol. 5404, pp. 296–303, Aug. 2004.

[8] Yaman Akbulut, Abdulkadir Sengur, Ümit Budak, Sami Ekici, "Deep Learning based Face Liveness Detection in Videos", 2017, IEEE

[9] M. Killioglu, M. Taskiran, N. Kahraman, "Anti-Spoofing In Face Recognition with Liveness Detection Using Pupil Tracking", SAMI 2017, IEEE 15th International Symposium on Applied Machine Intelligence and Informatics

 

[10] Keyurkumar Patel, Hu Han, and Anil K. Jain, "Secure Face Unlock: Spoof Detection on Smartphones", 2016, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY

[11] Aziz Alotaibi, Ausif Mahmood, "Enhancing Computer Vision to Detect Face Spoofing Attack Utilizing a Single Frame from a Replay Video Attack Using Deep Learning", 2016 International Conference on Optoelectronics and Image Processing

[12] Shervin Rahimzadeh, Arashloo, Josef Kittler, and William Christmas, "An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol", 2017 IEEE

[13] Hoai Phuong Nguyen, Florent Retraint, Frederic Morain-Nicolier, Agnes Delahaies, "FACE SPOOFING ATTACK DETECTION BASED ON THE BEHAVIOR OF NOISES", 2016, IEEE

[14] Xiao Luan, Huaming Wang, Weihua Ou, Linghui Liu, "Face Liveness Detection with Recaptured Feature Extraction", 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)

[15] Olegs Nikisins, Amir Mohammadi, Andre Anjos, Sebastien Marcel, "On Effectiveness of Anomaly Detection Approaches against Unseen Presentation Attacks in Face Anti-Spoofing", 2018 International Conference on Biometrics

 