KNN Classification for the Face Spoof Detection

Anu Priya[1], Dr. Hardayal Singh Shekhawat[2], Mr. Maninder Singh Nehra[3]
[1]*Student*, [2]*Assistant Professor, IT*, [3]*HOD, CSE*
[123]*Engineering College, Bikaner*

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 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. The Comparisons are made to analyze the performance of the proposed algorithm and the existing algorithm in terms of accuracy and time of execution.

Keywords- Feature Extraction, SVM, KNN

I. INTRODUCTION

The process of producing input images in a particular place is called imaging. It contains a metric and topological edge which is used for image analysis and crack edge for creating structure between the pixels. Analysis shows that the intensity is varied from small neighborhood of pixel boundary. The pixel boundary is another significant topic used in image processing. The image is visible to computer through sinkhole. The processing is completely based on knowledge and execution [1]. It consists of human cognition abilities in order to make decisions according to the information provided. The image quality is used to assess the percentage of degradation. 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. The image similarities are significant as they are used to assist retrieval from image database. The original images are often degraded by errors called noises [2]. This happens at the time of image capture, transmission of images contents. The perception of human color adds another subjective layer on the top highlighting the physical properties of electromagnetic radiations. The object will be transferred between client and the server. It is responsible for graph storage analysis from resource images. Every node of graph works as the processing unit of the application. 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 [3]. 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. 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 [4]. 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 [5]. 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. 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 [6]. 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

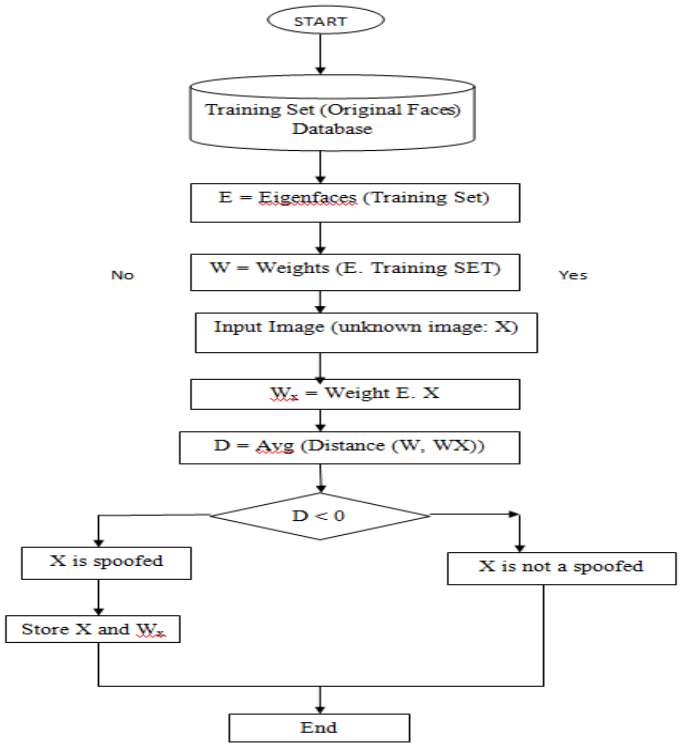
spoofing is of two types that is 2D spoofing and 3D spoofing. These are further divided in various attacks like photo attack, video attack and mask attack, as shown the figure. It is very easy for the attacker to get the photos and video of any individual due to the advanced internet technology. 3D mask attack is easily available in the market. This attack requires face modality. K-Nearest neighbor (KNN) depends on analogy learning. The samples are created by n-dimensional attributes. Each sample shows a point in any dimension. With all these lines the maximum part of the training samples are stored in n-dimensional pattern [7]. When an unknown sample is given then KNN looks the pattern space for training samples which are closest to that unknown sample. This closeness is defined in Euclidean space. The entire like tree have the tree induction and back propagation, the classifier which is closest breaks even with the weight of every attributes.

II. 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. A deep-learning based face spoof detection approach is proposed in this paper by using two various deep learning 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, et.al [9]** used a new improved algorithm 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, 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. 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 diffused frame was 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]** 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, et.al [13]** presented a study related to the facial recognition systems in which the issues of spoofing attacks were solved. 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 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]** designed a new evaluation protocol for highlighting the mentioned generalization issues. Thus, during the presence of unseen attacks, the PAD algorithms were studied through this proposed protocol. 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.

III. RESEARCH METHODOLOGY

In this research work, the face spoof detection is most widely used for the detection of face spoofing data due to which the unauthorized users are prevented in the bio-matrix system. Traditionally the detection of the spoofing is performed using KNN classifier method. The Eigen feature extracted algorithm need to be applied for the features extraction. The result obtained from the KNN classifier differentiates the test images whether the image is spoofed or genuine. The accuracy of KNN classifier is decreased during the detection process as there are certain similarities between the textual characteristics of the spoofed images. The proposed approach is implemented in MATLAB and research methodology process is shown in figure 3.1.



Phase 1: In the first phase algorithms of face spoof detection will be studied.

Phase 2: In this phase, the algorithm is proposed for the face spoof detection. The proposed algorithm will be based on the features extraction and classification. The eigen vector technique is applied for the feature extraction and KNN classifier is applied for the classification

Phase 3: In this phase, the algorithm which is proposed in the phase 2 will be implemented in the MATLAB. In the MATLAB the computer vision toolbox will be used for the implementation. In the eigen features of the input image will extracted which later classified with the classification algorithm

Phase 4: In the fourth phase, the performance of the proposed algorithm will be compared with the existing algorithm. The performance of the algorithms will be compared in terms of certain parameters like accuracy, execution time

Experimental Results

The proposed work is implemented in MATLAB and the simulations are performed to evaluate its performance.

Fig.2: Execution Time

Fig 2 shows the comparisons amongst the proposed KNN classifier as well as the previously existed approaches of SVM according to their execution time. The results ensure that the KNN classification approach minimizes the execution time with respect to SVM approach.

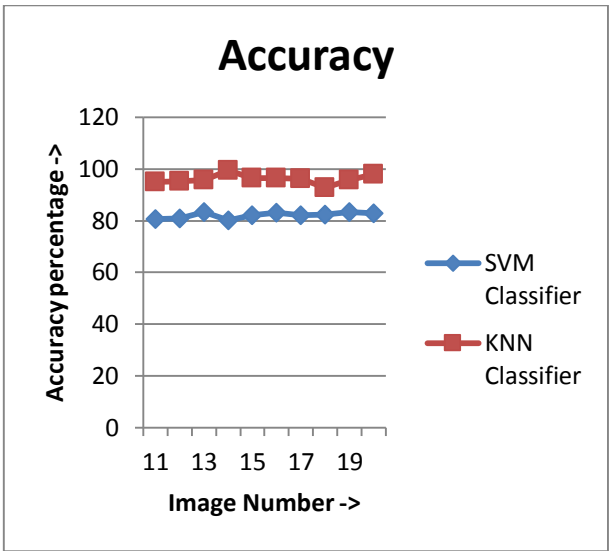


Fig.3: Accuracy Comparison

Figure 3 shows the comparison between proposed KNN approach and SVM based face spoof detection method based on their accuracy. According to the performed analysis, the accuracy of KNN approach is more than the accuracy of face spoof detection as compared to the previous SVM approach.

IV. CONCLUSION

Face spoof technique is proposed to identify the spoofed faces added due to the unauthorized access to the data. DWT is another technique which is used to identify the textual characteristics from the input dat. The traditional methods like SVM classifiers are used for the classification of spoofed and non-spoofed faces. According to the results, the approximate equal classifiers are classified by implementing KNN classifier for classification performance in this work. The analysis is done with the help of accuracy and execution. On the basis of the result obtained there is increase in accuracy and the decrease in time of execution by using this novel approach proposed in this work.

V. 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