Feature Extraction and Classification Method for Face Spoof Detection

Jyoti Thakur, Er. Poonam Chaudhary
Mtech Scholar, Assistant Professor
Sirda Institute of Engineering Technology, Sunder Nagar

Abstract- Nowadays, face biometric based access control systems are being used in our daily life while they are still vulnerable to spoofing attacks. So developing robust and reliable methods to prevent such frauds is unavoidable. As deep learning techniques have achieved satisfactory performances in computer vision, they have also been applied to face spoofing detection. 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. 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 hybrid 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- Face spoof, classification, SVM, Hybrid Classifier

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 [1]. 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 [2]. It consists of human cognition abilities in order to make decisions according to the information provided. The processing is not confined to the area which is needed to be studied but also to the knowledge analysis. Association is one of the important tools being used in image processing which use visual techniques [3]. The analysts apply a mixture of personal data and collateral data to image processing. It is very strongly correlated with computer vision and graphics. 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 [4]. 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 [5]. When someone tries to interfere 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 [6]. 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 [7]. 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. The classifications of documents are already defined categories, the documents are classified in three categories: unsupervised, supervised and semi supervised methods [8]. The automatic text classification has been widely studied and huge success is also seen in this area, it also includes machine

learning approaches. SVM classifier is proposed for regression, classification and pattern recognition of the data. Because of its highly generalized results without getting any prior knowledge to add, this respective classifier is one of the best classifier proposed by the researchers. The main purpose of Naïve Bayes Classifier is to assign the objects to the class when the assets of objects are provided to every class [9]. Decision Tree Classifier is non-parametric supervised learning technique used for the classification and regression of data. The objective is to create a model which can predict the value of a targeted variable by just learning simple decision making rules. K-Nearest neighbor 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.

II. LITERATURE REVIEW

Yaman, et al. [10] proposed deep-learning based face spoof detection approach by using two various deep learning methods. The local receptive fields (LRF)-ELM and CNN are known to be these two methods. For increasing the speed of processing of a model, LRF-ELM was introduced lately in which a convolution and pooling layer was included. There are a series of convolution and pooling layers, however, present within CNN. Higher number of completely connected layers might also be available within the CNN model. 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 [11] presented that 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. The Kanade-Lucas-Tomasi (KLT) algorithm was used to achieve a stable eye region. 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. A random direction is chosen by the proposed spoofing algorithm once the few stable numbers of frames that include pupils were identified. 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 [12] 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. 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, [13] 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. Thus, the sharp edges were destructed and the locations of pixels were changed due to this. However, mainly around the nose and lips, sharp edges and rounded surfaces were seen within the real face frame. From the diffused image, the local and complex features were extracted with the help of proposed CNN architecture. 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, et.al [14] proposed a new evaluation protocol through which the effects of unseen attack types could be known on the basis of certain existing factors. From the training set, the samples that were of similar to that of a test sample were excluded as per the novel mechanism. For accounting the variability of imaging conditions, both inter and intra database experiments were performed by applied the proposed mechanism. 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 [15] 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.

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 SVM classifier method. The Eigen feature extracted algorithm need to be applied for the features extraction. The result obtained from the SVM classifier differentiates the test images whether the image is spoofed or genuine. The accuracy of SVM 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.

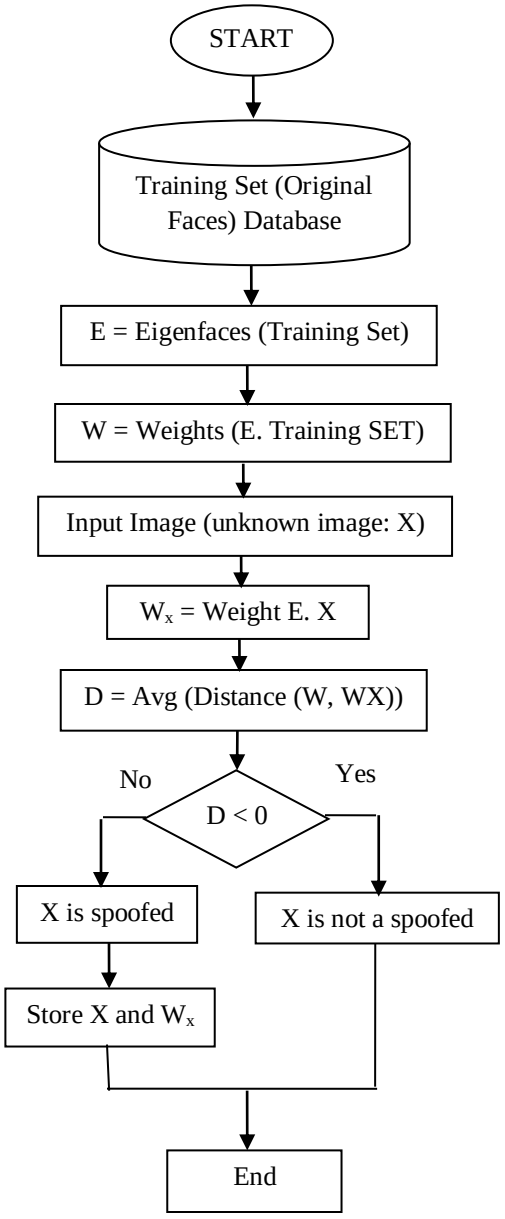

Fig.1: Flowchart of Proposed Work

Following are the various steps of the flowchart

Step 1: Input the number of images to prepare the training set for the spoof and non spoofed faces

Step 2: Eigen Feature Calculation of input training image

2.1. Calculate the eigen feature of each image

2.2. Store the calculated feature in the database with image label

Step 3: Input the test image which is the unknown image

3.1. Calculate the eigen feature of the unknown image

Step 4: Apply hybrid classifier for the detection of spoofed and non spoofed unknown image

4.1. Calculate distance between the features of the unknown image and all the images stored in the data base

4.2. if distance between the image is above zero than it is non spoofed

4.3 Otherwise it is spoofed

IV. EXPERIMENTAL RESULTS

The proposed work is implemented in MATLAB and the results are evaluated based on the execution time and accuracy as shown below.

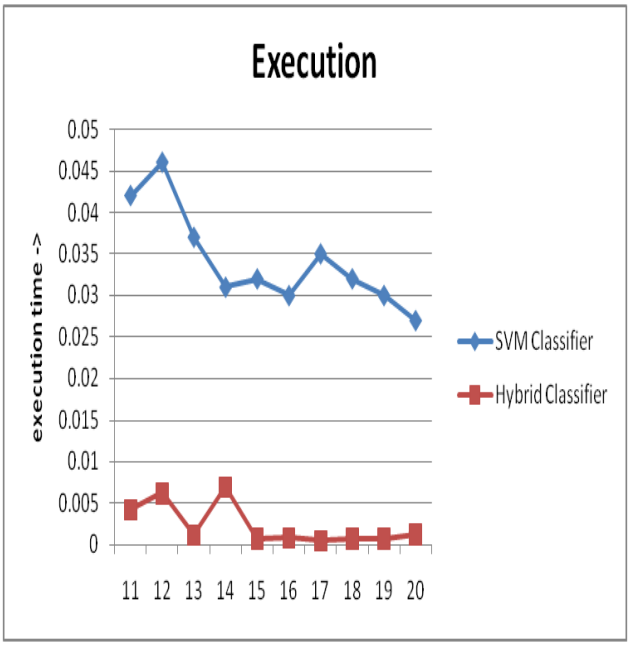

Fig.2: Execution Time

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

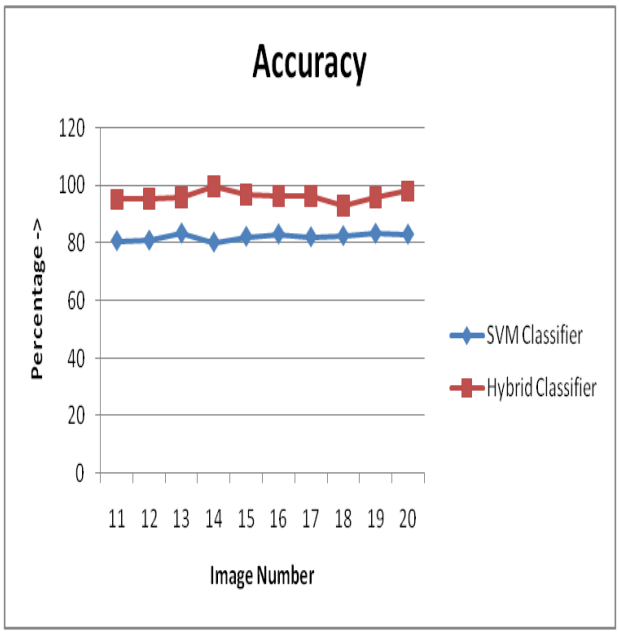

Fig.3: Accuracy Comparison

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

V. CONCLUSION

In this research work, the technique of SVM is replaced with hybrid which increases 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. 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.

VI. 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]. K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in „liveness" assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, Sep. 2007
[9]. J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proc. IJCB, Jun. 2013, pp. 1–6.
[10]. Yaman Akbulut, Abdulkadir Sengur, Ümit Budak, Sami Ekici, "Deep Learning based Face Liveness Detection in Videos", 2017, IEEE
[11]. 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
[12]. Keyurkumar Patel, Hu Han, and Anil K. Jain, "Secure Face Unlock: Spoof Detection on Smartphones", 2016, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
[13]. 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
[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
[15]. Hoai Phuong Nguyen, Florent Retraint, Frederic Morain-Nicolier, Agnes Delahaies, "FACE SPOOFING ATTACK DETECTION BASED ON THE BEHAVIOR OF NOISES", 2016, IEEE