Machine Learning Approach for Face Spoof Detection in Image Processing

Nidhi Sharma[1], Mrs Shivani Chauhan[2], Ajay Singh[3]
[1] Research Scholar, [2,3]Assistant professor,
Bhagwant Institute of Technology, Muzaffarnagar, UP, India.

Abstract **-** For the identification and detection of spoofed and non-spoofed images, face spoof approach was proposed. The textual features occurring inside the test images were analyzed with the help of DWT scheme. It is possible that some exceptional turbulence such as geometric turbulences and the artificial texture turbulences will remain present. Generally, these kinds of turbulences occur due to camera and light subsidiaries. The dissimilarity among the arithmetical, the lighting and the texture based turbulences can be noticed using an ultimate camera without faults. Earlier presented support vector machine classification model is utilized for the detection of spoofed or non-spoofed images. In the proposed approach, the KNN classifier is used in place of SVM classifier for improving the accuracy of the face spoof discovery. The performance of the proposed algorithm and the earlier algorithm is analyzed through some comparisons among them in terms of precision and execution time.

Keywords - SVM, KNN, DWT, Face Spoof

I. INTRODUCTION

Image Processing is also known as digital image processing. Imaging is the name given to the production of images in a particular place. It comprises a metric and topological boundary. This edge or boundary is utilized for image scrutiny and crack edge is used for the creation of configuration among the pixels. It is analyzed that the intensity or brightness varies from small locality of pixel edge. In image processing, pixel edge is one more important factor. Using sinkhole, the image is visible in computer. The processing absolutely depends on understanding and implementation [1]. It comprises human cognition potentials for making decisions on the basis of given data. The percentage of deterioration is evaluated through picture quality. The technique which is used for performing some procedures on the pictures is called image processing. This technique generates a modified variant of pictures or retrieves several features from the image. The picture behaves as input in signal processing while features act as the output. Image processing is an extensively utilized and rising technology. This technology plays an important role in the research area, since various researches are currently happening in this domain [2]. Mainly two types of methods are available for image processing. One is analogue image processing and the other is digital image processing. The techniques used for hard copies like photographs and printouts is called analogue image processing while the technique used for the handling of the digital images using computers is called digital image processing. In digital image processing, whole data passes through three phases. These phases are pre-processing, improvement and data extraction. Face detection is one of the most widely used techniques which are mainly used to serve the security purpose. In these days, crimes are increasing at a very high rate, so these types of methods are very useful to keep a check on the people in various fields such as industries, banks hospitals and much more. These methods can also be used in a number of applications like biometric study; content based coding of images and videos, surveillance and human computer interaction (HCI) [3]. Due to the presence of similarity among some faces because of their color, age, gender, the implementation of face detection technique proved very complex. The problems which occur during the implementation of this method are image quality, background, expressions and the environmental changes. Face detection as the name indicates, depicts the position of face in an image. It is very difficult to detect the image while it seems very easy from far. During the implementation of this technique, all the possible options should be considered like image rotation, single or multiple faces, poses and so on. If this technique is not applied properly this can give rise to fake detection of image or sometimes no image exists there [4]. A number of methodologies are present for face detection. By presenting a false face towards the camera when someone tries to interfere in the face biometric system, it is called an attack on the face recognition system. Due to this, all the artificial faces of the authorized users go to the biometric security systems. Only by using printed photographs and digitalized images being displayed on the screen, these attacks can be carried out. A technique named face liveliness is used to distinguish the real faces from fake faces. This technique mainly focuses on the identification of physiological signs of life. In order to measure and analyze the human body individuality, biometric characteristics are used [5]. These characteristics can be divided into two parts, physical characteristics and activity characteristics. In physical characteristics fingerprints, faces or iris patterns are used while the activity characteristics use strolling patterns or voice signatures. Being varied in biometric systems is a very important test. Because of the variations, chances of fraud occur and this is known as spoofing attack. By unauthorized access in the system, the stolen data can be destroyed and imitate by the intruder. The technique of face scooping detection is mainly based on the facial characteristics in the light weighing physiological properties recognition. The

false faces identifies as positive and negative false faces. Real faces having restricted variation are called positive faces while negative face involves dummy, spoof faces on images and much more [6]. The documents are classified in three types: unsupervised, supervised and semi supervised methods. The automatic text classification has been analyzed extensively and demonstrates excessive success in this region. This classification approach involves machine learning algorithms. Support vector machine classification model is proposed for regression, classification and pattern identification of information. This classifier is identified as one of the best classifier proposed by the researchers due to of its extremely comprehensive outcomes without having any previous knowledge to add. The major aim of Naïve Bayes classifier is to allocate the objects to the class when the resources of objects are given to each class. The prospect objects can be explained just as vector of variables. This issue is generally identified as issue of supervised classification and several techniques are commenced for creating rules for them. Decision tree classifier is non-parametric supervised learning method utilized for the classification and regression of information [7]. The purpose is the creation of a model which can forecast the value of a targeted variable through the learning of simple decision making rules. K-nearest neighbor approach depends on analogy learning. The samples are generated by n-dimensional attributes. Every pattern shows a point in any dimension. The maximum part of the training samples is stored in n-dimensional pattern with all these lines.

II. LITERATURE REVIEW

Yaman, et al. [8] presented a study which highlighted that a reliable face-based access system needs to be designed for detecting the identity and liveness of the facial data given as input. Different researchers designed different feature-based techniques for detecting face spoof. On the input image, a series of processes are applied such that the liveness of face could be detected. This paper used two different deep learning techniques for designing a deep-learning based face spoof detection technique which were called local receptive fields (LRF)-ELM and CNN. The CNN model might include higher numbers of completely connected layers. For evaluating the performance of proposed approach, the two most commonly found databases NUAA and CASIA were used. Based on the comparisons, improvement in the performance of LFR-ELM approach was achieved through this research.

Killioglu, et.al [9] proposed a novel approach in which by using the mobility of a fake face, the liveliness of the face spoofing used in face identification system could be find out. For obtaining a stable eye area, the Kanade-Lucas-Tomasi(KTL) algorithm was used. The eye region was cropped by using a real time camera frame and rotation was done to obtain a stable eye region. For the extraction of pupil from the eye area, a new better algorithm was used. A square frame was used that carried eight LEADs, one for each direction. After activating the selected LED, the direction of the eye was checked. This was done to confirm whether the position of LED and direction of pupil were same or not. After matching the direction of pupil and position of LED, liveness information was given as output by the algorithm. The tested results made clear that the given approach was very successful.

Keyurkumar, et.al [10] proposed an approach based on the Smartphone unlock systems. These systems were in great demand and used within various mobile phones. Some systems that involve mobile payments also used these systems. A database named Smartphone spoof attack database (MSU USSA) that included almost 1000 subjects was made. For achieving capable face spoof detection, Android smart phones were used. The presented approach proved very beneficial for detecting the spoofs of cross-database and intra-database testing environments and gave good results. The evaluation involved almost 20 participants which proved that the given approach was very successful when applied on the real time applications.

Alotaibi and Mahmood, [11] presented a useful system for solving the face spoofing attack issues by using static frame of sequenced frames. An AOS-based scheme along with a large time step size was implemented to develop a speed – diffused image. Some sharp edges and flattened areas were found around the lips, nose, cheek areas and eyes within the fake images, when the input video was recaptured again. As a result of this, pixels location changed and the sharp edges were destroyed. By using the CNN approach, the local and complex facial characteristics were extracted from the diffused image. Large time step was used for destroying the boundaries. For getting a diffused frame for future work, the sparse auto-encoder was developed. Hence a diffused frame will be generated by an auto-encoder within the architecture of the given structure in future.

Shervin, et.al [12] proposed a novel evaluation protocol by the use of which the effects of hidden attack types could be identified on the base of some accessible factors. During face spoof detection, researchers faced a number of problems. A number of issues like minimum sample size and the image sensor inter-operability were arose before the researchers during this work. By using the given approach, both intra and inter database experiments were conducted for calculating the inconsistency of imaging conditions. For solving the face spoofing recognition problem, a new and highly reliable solution was proposed by the researchers. According to the new approach, only positive samples were needed for training the systems. The outcomes of the performed experiments indicated that more improvement in the detection rates was needed because obtained results were unsatisfactory.

Hoai, et.al [13] suggested a study for solving the problem of spoofing attacks occurring in face detection systems. While real faces and falsified faces were placed in front of a security system, differences of micro-textures were found between the surfaces of both the faces. These differences were highlighted to distinguish both the face spoof images. This method showed that the division of the local variances

of nose had a fixed behavior. This method acted differently for both real and fake faces. The two different databases developed by researchers were used for testing the presented mechanism with the help of a classification technique named as SVM. The tested results clearly showed that the given mechanism performed well.

III. RESEARCH METHODOLOGY

Following is the flowchart describing the implement of proposed work:

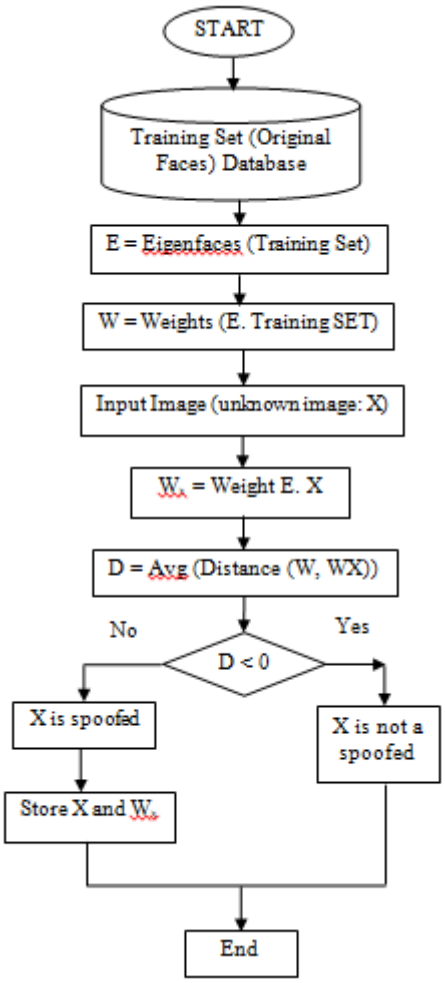

Figure 1: Proposed Flowchart

The spoofed and non spoofed images are categorized to propose the face spoof detection technique. Eigen face detection technique is applied in the initial phase. For performing classification, the output of previous step is given as input. The n-dimensional numeric attributes present in KNN classifier are represented using samples. The k-nearest neighbor classifier matches the k-training samples in case when there is any unknown sample available. Then, the pattern space that is closest to the unknown sample is chosen. Euclidean distance is calculated for defining closeness. Unlike any other machine learning technique, the weight is divided to every attribute by the nearest neighbor classifier. Thus, in the presence of infinite amount of unnecessary data in the network, huge amount of confusion arises.

To verify is the image is spoof or genuine, prediction is performed using nearest neighbor classifier. As a result, the classifier is given back the average value of genuine values associated KNN classifier. In comparison to all other machine learning algorithms, the KNN classifier is known to be the simplest. The features relevant to the test images are analyzed using Eigen method. For detecting if the image is genuine or spoof, the KNN classifier is applied.

IV. EXPERIMENTAL RESULTS

The proposed research is implemented in MATLAB and the results are evaluated by comparing proposed and existing techniques in terms of various parameters.

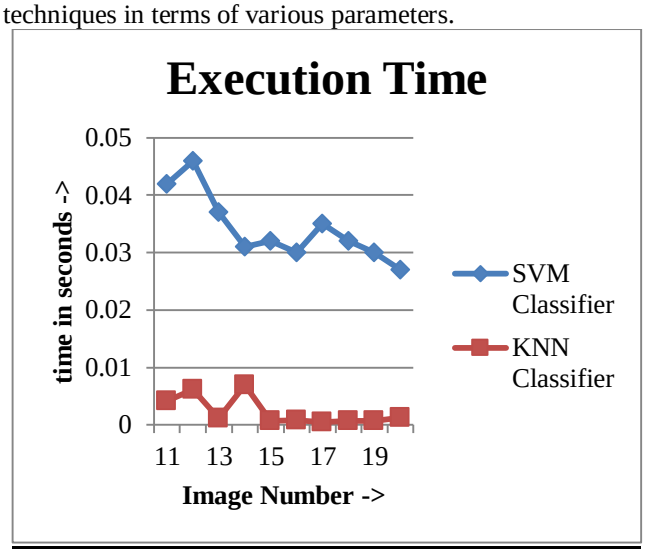

Figure 2: Execution Time

The comparisons against proposed and existing approaches in terms of the execution time consumed by each of them are shown in figure 2. It is seen that the execution time of proposed algorithm is reduced in comparison to the time consumed by existing approach.

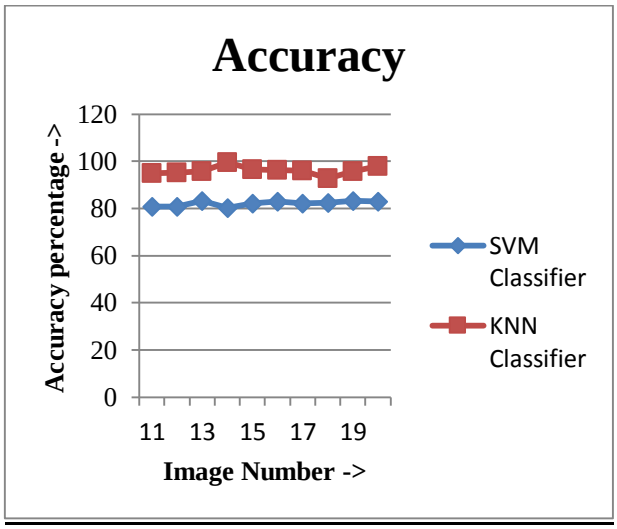

Figure 3: Accuracy Comparison

The comparisons of proposed and existing techniques on the basis of accuracy of their results are shown in figure 3. It is seen that the accuracy of proposed technique is higher as compared to the existing technique.

V. CONCLUSION

The spoofed faces which are added because of the presence of unauthorized users are identified using face spoof detection techniques. Feature extraction and classification are the two steps performed in these techniques. Feature extraction is performed using Eigen vector and classification is performed using SVM in case of previously proposed technique. The presence of SVM classifier however, resulted in reducing the accuracy of face spoof detection. The proposed work uses KNN classifier to increase the accuracy of face spoof detection technique. AT and T dataset is used to perform simulations for proposed and existing techniques in MATLAB. Accuracy and execution time are calculated to analyze the performance of both these algorithms. It is concluded through the results that the proposed approach increases the accuracy and reduces the execution time.

VI. REFERENCES

[1]. 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