Random Forest Classifier for Face Spoof Detection

Sheikh Irfan Ul Haq
Research Scholar
Chandigarh Engineering College,
Landran, Mohali, Punjab, India
irfanahmed189@gmail.com

Ms. Rashmi Karkra
Assistant Professor
Chandigarh Engineering College,
Landran Mohali, Punjab, India
rashmi.4048@cgc.edu.in

Mr. Gurbaj Singh
Assistant professor
Chandigarh Engineering College,
Landran Mohali, Punjab, India
gurbaj.3534@cgc.edu.in

Abstract - The face spoof technique was proposed to identify and detect the spoofed and non-spoofed images. Discrete wavelet transform (DWT) technique is used to analyze the textual features present within the test images. Some exceptional disturbances may available such as geometric disturbances and the artificial texture disturbances. The Eigen based technique is applied for the feature extraction. Support Vector Machine classifier is applied for the classification purpose. To improve the accuracy of the face spoof detection, support vector machine classifier will be replaced with the Random Forest Classifier. Comparisons are performed to analyze the performance of the proposed algorithm and the existing algorithm in terms of accuracy and execution time. It is analyzed that accuracy will be optimized up to 10 percent as compared to existing method.

Keywords **-** Random Forest, Face Spoof, Machine Learning

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. Analog techniques are used by image processing to have hard copies like Photostat and printout. The analysts use wide range of fundamental interpreted data using visual techniques. 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 [2]. The analysts apply a mixture of personal data and collateral data to image processing. It is very strongly correlated with computer vision and graphics. Information can be perceived, processed and interpreted by using visual information. Almost half of the brain processing is dependent on the visual information processing. Digital image processing is the computer based type of processing in automatic processing takes place [3]. Manipulation, interpretation of visual information plays a very significant role in our daily routine and widely in the variety of disciples and in the scientific as well as in the technical field having various applications like television, photography, robotic, remote sensing, medical diagnosis and industrial inspection. 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. 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 [6]. 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 [7]. 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.

II. LITERATURE REVIEW

Lei Li, et.al [8] proposed a new end-to-end learnable LBP network to detect face spoofing. During the designing of proposed network, the similarities between LBP extraction and convolutional neural network (CNN) were considered. The proposed network was able to decrease the amount of network parameters in significant manner. These layers were made up of sparse binary filters and derivable simulated gate functions. Compared with existing deep leaning based detection methods, the parameters in the completely linked layers were equal to 64*x* savings in contrast to available detection techniques based on deep leaning. Several tests were performed on two average spoofing databases. These databases were called Relay-Attack and CASIA-FA. The proposed network significantly showed better performance as compared to the state-of-the-art techniques.

Yaman, et al. [9] proposed deep-learning based face spoof detection approach 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. 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 [10] used the Kanade-Lucas-Tomasi (KLT) algorithm 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. For activating the chosen direction's LED on a square frame that includes eight LEADs for every direction, a signal was sent to Arduino. 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 [11] 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, [12] 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. 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 [13] 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.

III. RESEARCH METHODOLOGY

The face spoof detection technique is proposed for the classification of spoofed and non spoofed image. In the first phase, the technique of Eigen face detection is applied which later given as input for the classification. First, Random Forest algorithm is a supervised classification algorithm. As per its name, this algorithm creates a forest and makes it random. There is a direct relationship between the number of trees in the forest and the results it can get: the larger the number of trees, the more accurate the result. But one thing to note is that creating the forest is not the same as constructing the decision with information gain or gain index approach. The author provides four links to help people who are working with decision trees for the first time to improve learning and understanding. The decision tree is a decision support tool. It uses a tree-like graph to show the possible consequences. If you input a training dataset with targets and features into the decision tree, it will formulate some set of rules. These rules can be used to perform predictions. The author uses one example to illustrate this point: suppose you want to predict whether your daughter will like an animated movie, you should collect the past animated movies she likes, and take some features as the input. Then, through the decision tree algorithm, you can generate the rules. You can then input the features of this movie and see whether it will be liked by your daughter. The process of calculating these nodes and forming the rules is using information gain and Gini index calculations.

The algorithm and flowchart used for the implementation of proposed work is given below:-

Algorithm

The proposed algorithm detects the spoofed and non spoofed image. The proposed algorithm is divided into three phase, in the phase 1 the images are taken as input which need to classify .In the second phase, the feature extraction process is done which the Eigen vector technique. In the last phase, the random forest classification algorithm is applied for the classification of spoofed and non spoofed faces

The algorithm is given below:-

1. Input the images of the training set and test set for the classification.

2. Store the input images into the variable A

Calculate Features of the input image with following steps:

- Ax=λX says that eigenvectors x keep the same direction when multiplied by A.
- Ay=λY also says that det(A- λI)=0. This determines n Eigen values
- The Eigen values of A^2 and A^{-1} are $\lambda^2$and $\lambda^{-1}$with the same eigenvector
- The sum of the λ s equals the sum down the main diagonal of A (*the trace*). The product of the λ's equals the determinant.
- Projections P, reflections R, 90ı rotations Q have special eigenvalues 1, 0,-1; I,-i .
- Singular matrices have $\lambda = 0$. Triangular matrices have λ's on their diagonal.

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 performance parameters.

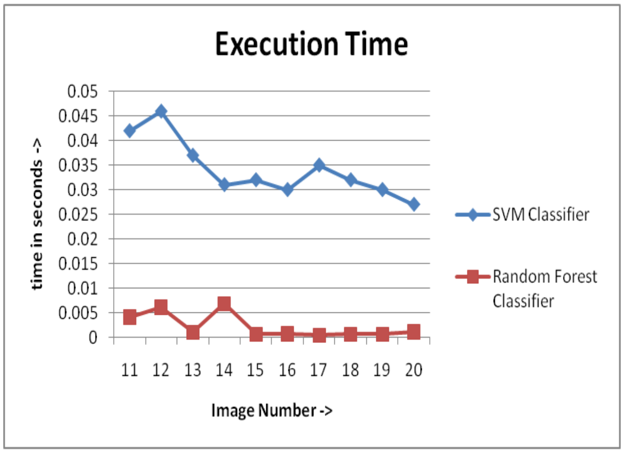
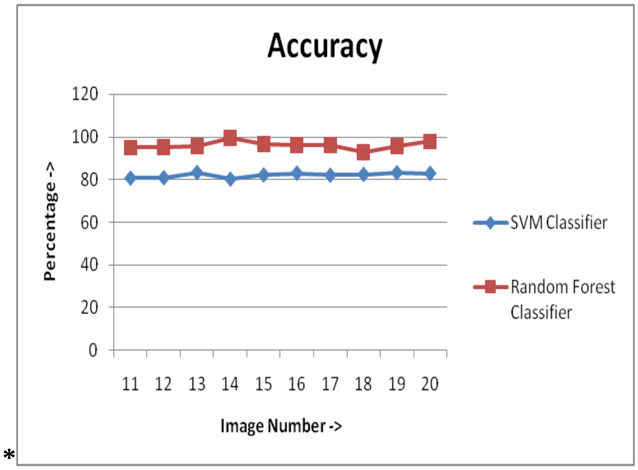


Figure 1: Execution Time

Fig 1 shows the comparison amongst the proposed random forest classifier as well as the previously existed approaches of SVM according to their execution time. The results ensure that the random forest classification approach minimizes the execution time with respect to SVM approach.



*

Figure 2: Accuracy Comparison

Figure 2 shows the comparison between proposed random forest approach and SVM based face spoof detection method based on their accuracy. According to the performed analysis, the accuracy of random forest approach is more than the accuracy of face spoof detection as compared to the previous SVM approach.

V. 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 random forest 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. The proposed method increases the accuracy for the face spoof detection upto 10 percent as compared to existing method.

VI. REFERENCES

[1]. A. Anjos and S. Marcel, “Counter-measures to photo attacks in face recognition: A public database and a baseline,” International Joint Conference on Biometrics (IJCB), vol. 16, issue no.30, pp. 1–7, 2011.

[2]. X. Tan, Y. Li, J. Liu, and L. Jiang, “Face liveness detection from a single image with sparse low rank bilinear discriminative model,” European Conference on Computer Vision, vol. 18, issue no.34, pp. 504– 517, 2010.

[3]. Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, “A face antispoofing database with diverse attacks,” IAPR International Conference on Biometrics (ICB), vol. 2, issue no.27, pp. 26–31, 2012.

[4]. L. Sun, G. Pan, Z. Wu, and S. Lao, “Blinking-based live face detection using conditional random fields,” Advances in Biometrics, vol. 5, issue no.23, pp. 252–260, 2007.

[5]. W. Bao, H. Li, N. Li, and W. Jiang, “A liveness detection method for face recognition based on optical flow field,” International Conference on Image Analysis and Signal Processing, vol. 7, issue no.24, pp. 233–236, 2009.

[6]. S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, “Computationally efficient face spoofing detection with motion magnification,” IEEE Conference on Computer Vision and Pattern Recognition Workshops, vol. 9, issue no.24, pp. 105–110, 2013.

[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] Lei Li, Xiaoyi Feng, Zhaoqiang Xia, Xiaoyue Jiang, Abdenour Hadid, “Face Spoofing Detection with Local Binary Pattern Network”,2018, Journal of Visual Communication and Image Representation

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

[10] 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

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

[12] 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

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