International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 09, September-2018

NOVEL APPROACH FOR FACE SPOOF DETECTION IN IMAGE PROCESSING

Deepika , Rachhpal Singh

M .Tech (Scholar) , Assistant Professor
Department of Computer Science and Engineering , PURCITM ,Punjabi University,(Punjab)India

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 of presence of exceptional disturbances like geometric disturbances and the artificial texture disturbances. The time which is required for the classification is very long and it is difficult to evaluate optimal value of k . According to the data, the value of k is evaluated. By increasing the value of k, noise is reduced. The distinct boundary value is very less as compared to the other generated classes. By using several k-values of different classes KNN methodology is increased in order to overcome such limitations. Comparisons are being made to analyze the proposed approach performance according to the accuracy of the proposed algorithm and the existed algorithm in terms of accuracy and time of execution.

KEYWORDS: Face Spoof Detection, SVM, KNN

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. 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. 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 [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. Though all these face recognition methods solves the face recognition problem, there are some factors that affect or degrade the performance of face recognition. The reason behind these factors is in real life situation where the person's face is not always neutral (expression full). The factors affecting face recognition include expressions, occlusion, pose, illumination, facial ageing, and others. 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 [5]. It aims at detection of physiological signs of life. Biometric technologies are used to measure and analyze human body characteristics. 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. It gives better performance when the dimension of the input space is very high. The main purpose of this classifier is to assign the objects to the class when the assets of objects are provided to every class. The future objects can be described as vector of variables only [6]. This problem is commonly called problem of supervised classification and different methods are introduced for the development a rules for them. Pone is one of the very significant naive bayes methods being proposed by scientist and researchers and is called idiot's bayes or simply Bayes and sometimes independence Bayes. It 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. It is used for the approximation of discrete-valued target functions in which the learner's capacity is judged by decision tree.

Literature Review

Yaman Akbulut, et.al (2017) studied that the identity as well as liveness of the input of face can be known through a reliable face-based access system [7]. 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. 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.

M. Killioglu, et.al (2017) presented a study to detect the liveness of spoofing of facial recognition system with the help of mobility of a fake face [8]. 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. High success ratio is achieved as per the experiments conducted using this proposed approach.

Keyurkumar Patel, et.al (2016) presented a study on the smart phone 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 [9]. 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.

Aziz Alotaibi, et.al (2016) proposed an efficient mechanism using static frame of sequenced frames in order to solve the face spoofing attack issues [10]. For creating a speed-diffused image, an AOS-based scheme was applied along with a large time step size. 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. 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 Rahimzadeh Arashloo, et.al (2017) presented a study related to the issues faced when detecting the face spoof [11]. 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. From the training set, the samples that were of similar to that of a test sample were excluded as per the novel 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 Phuong Nguyen, et.al (2016) 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 [12]. 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.

Research Methodology

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 DWT algorithm was used to analyze the textual features of the test images for the identification of the face spoofing in the previously existed techniques. 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 samples are used to represent the n-dimensional numeric attributes in the KNN classifier. The point in n-dimensional space is denoted by a sample. If there is any unknown sample present then the k-nearest neighbor classifier match the k-training samples and select the pattern space which is nearest to the unknown sample. Closeness is defined by the Euclidean distance. Nearest neighbor classifier breaks with the weight to every attribute unlike any other machine learning technique. These conditions give rise to huge amount of confusion when infinite amount of unnecessary data are present within the network. The nearest neighbor classifier is used for the prediction purpose in order to verify whether the image is genuine or spoofed. In this way, the average value of the genuine valued associated with the KNN classifier is given back to the classifier. The KNN classifier is considered as the simplest method amongst all the other machined learning methods. The DWT method is used to analyze the features related with the test images. The KNN classifier is applied where we want to detect whether the image is genuine or spoofed.

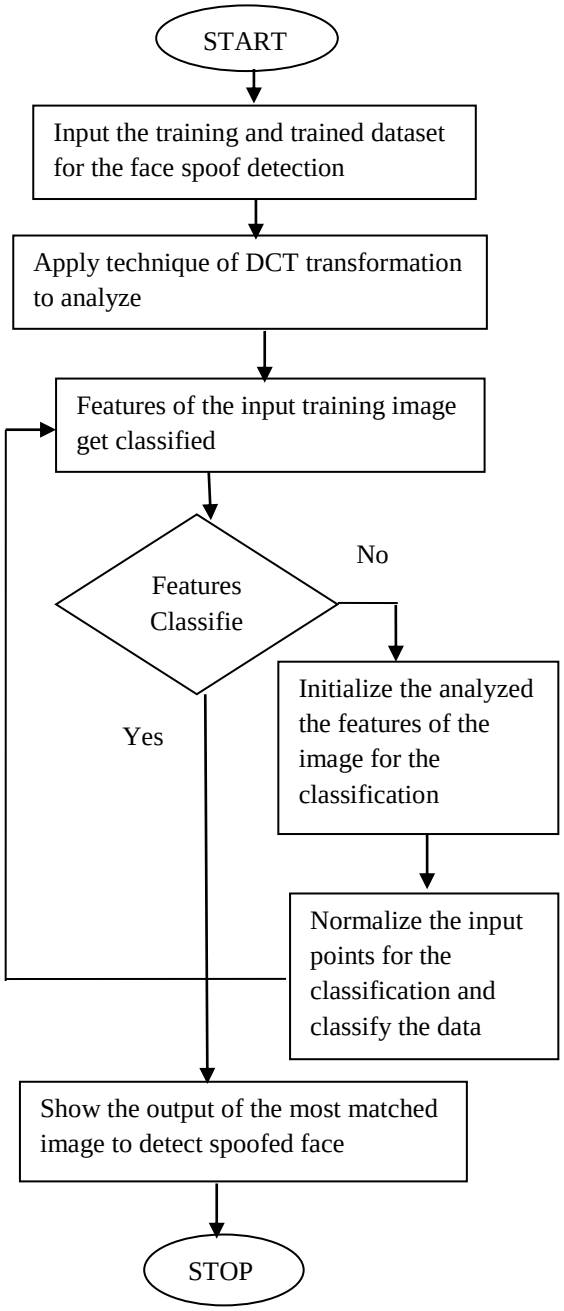

Figure 1: Proposed Flowchart

Experimental Results

The proposed work has been implemented in MATLAB and the results have been evaluated through comparisons made in terms of several parameters.

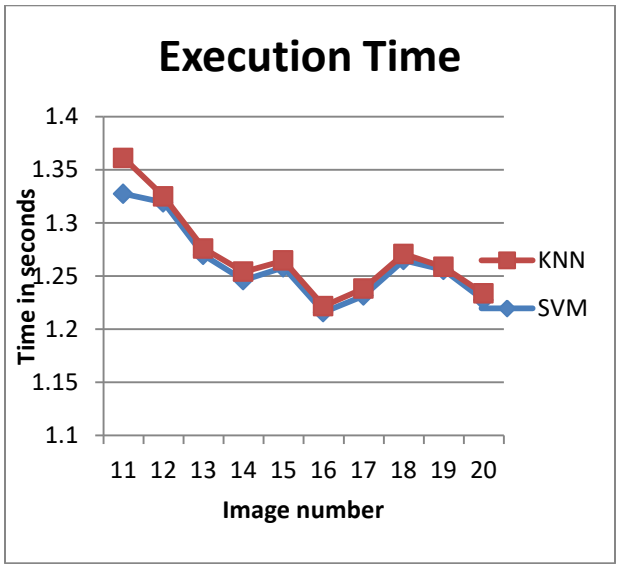

Fig 2: Execution Time

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 SVM classification approach minimizes the execution time with respect to KNN approach.

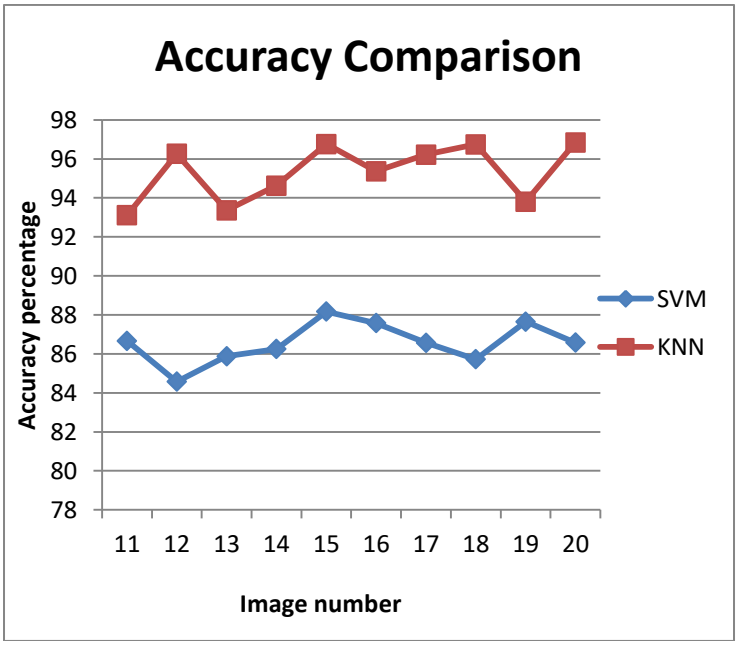

Fig 3: Accuracy Comparison

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 approach.

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.

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] Yaman Akbulut, Abdulkadir Sengur, Ümit Budak, Sami Ekici, "Deep Learning based Face Liveness Detection in Videos", 2017, IEEE
[8] 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
[9] Keyurkumar Patel, Hu Han, and Anil K. Jain, "Secure Face Unlock: Spoof Detection on Smartphones", 2016, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY
[10] 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
[11] Shervin Rahimzadeh Arashloo, Josef Kittler, and William Christmas, "An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol", 2017 IEEE
[12] Hoai Phuong Nguyen, Florent Retraint, Frederic Morain-Nicolier, Agnes Delahaies, "FACE SPOOFING ATTACK DETECTION BASED ON THE BEHAVIOR OF NOISES", 2016, IEEE