KNN Classification for the Face Spoof Detection

Samrity Saini, Kiranpreet Kaur

Abstract

Current face spoof detection systems are vulnerable to various spoofing attacks. A spoofing attack occurs when one person tries to façade someone else by misusing and falsifying the data to gain unauthorized access to the system. Face spoof detection has now attracted huge attention with the aim of assuring reliability of face biometrics system. 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. A perfect camera with no defects should be used just to notice the difference between the geometric, the illumination and the texture based disturbances. The face spoof detection techniques are based on two steps; the first step is of feature extraction and second is classification. We present a novel approach based on extracting Eigen features with LBP and using KNN classifier for the classification process as opposed to already existing technique using SVM classier. Experimental analysis showed excellent results compared to existing technique. Comparisons are made to analyze the performance of the proposed algorithm and the existing algorithm in terms of accuracy and time of execution.

KEYWORDS:

Classification, Eigen feature, Feature Extraction, KNN, Local Binary Pattern, SVM,

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 used to perform some operations on the images, which generate an enhanced version of the image or extract some features from it. It is a signal processing in which image acts as the input and characteristic or features acts 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. Face recognition is also one of the very widely used security purpose 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 has been proven 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 implies, 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 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 interfere with the face biometric system by presenting a false face towards the camera, it is termed as Spoof attack. This attack on face recognition systems involves 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 secondly activity characteristics which includes voice signatures or strolling patterns with physical characteristics being the most prominent challenge since it is mostly varied or tampered with in biometric systems. The variations involve chances of fraud which is most commonly known as spoofing attack. The stolen data will effectively run and mimicked by the adversary to have an 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. 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, such that it can be clear and visible. Face spoofing is of two types; 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 masks are easily available in the market.

Figure 1: Different Spoof attacks [16]

The contribution of this paper can be summarized as follows:

i) A face spoof detection algorithm is proposed which is based on extracting Eigen features, which is effective in grasping intrinsic distortions of face spoof images with respect to genuine face images.

ii) For the classification, existing SVM approach is replaced with novel approach utilizing KNN classifier and the results are compared in terms of accuracy and execution time.

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]**designeda 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.

Research Methodology

In this 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 needs to be applied for the features extraction. In the proposed work, the results obtained from the KNN classifier differentiate the test images whether it is spoofed or genuine. The KNN classifier uses the multiple hyper planes due to which the accuracy increases at steady rate.

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 needs to be classified.

In the second phase, the feature extraction process is done with the Eigen vector technique.

In the last phase, the KNN classification algorithm is applied for the classification of spoofed and non-spoofed faces.

The proposed work is implemented as per the following procedure. Following are the various steps of the proposed algorithm:

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

2. Store the input images into the variable.

Calculate Features of the input image:

3.1. Ax= λx says that eigenvectors x keep the same direction when multiplied by A.

3.2. Ay=λyalso says that det(A-λI)=0. This determines n Eigen values

3.3 The eigen values of A^2 and A^{-1} are $\lambda^2$and $\lambda^{-1}$with the same eigenvector

3.4. The sum of the λ's equals the sum down the main diagonal of A (*the trace*).The product of theλ's equals the determinant.

3.5. Projections P, reflections R, 90ı rotations Q have special eigen values 1, 0,-1; I,-i. Singular matrices have $\lambda = 0$. Triangular matrices have λ's on their diagonal.

Classification:

4.1. Calculate "d(x, xi)" i =1, 2, ….., n; where d denotes the Euclidean distance between the points.

4.2. Arrange the calculated n Euclidean distances in non-decreasing order.

4.3. Let k be a +ve integer, take the first k distances from this sorted list.

4.3. Find those k-points corresponding to these k-distances.

4.4 Let k_i denotes the number of points belonging to the i^{th}class among k points i.e. $k \geq 0$

4.5. If $k_i > k_j \; \forall i \neq j$ then put x in class i.

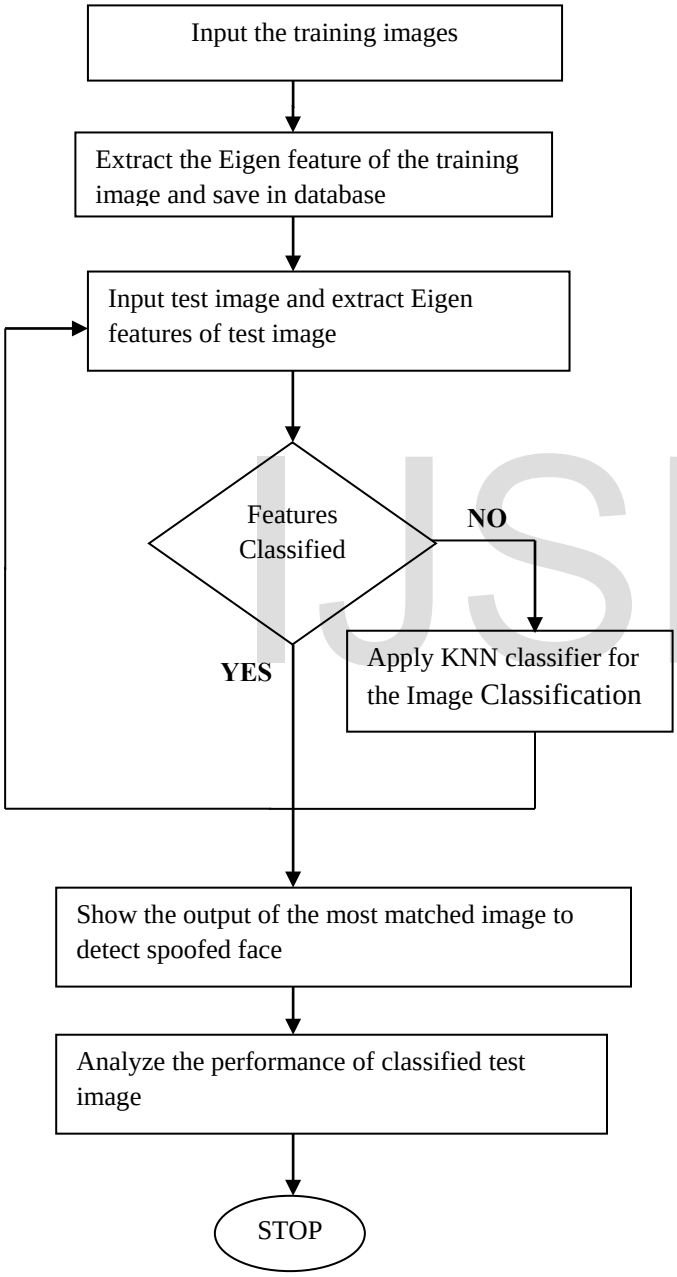

Figure 2: Proposed Flowchart

The proposed technique detects whether the image is spoofed or not. The flowchart is described below:

Input: Test image

Output: Most matched image corresponding to test image along with performance analysis

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

Step 2: LBP for Eigen Feature Calculation/Extraction 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 KNN 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 test and equivalent image is different

NO

Then spoofed

4.3 Otherwise it is non-spoofed.

Experimental Results

The proposed work is implemented in MATLAB and the simulations are performed to evaluate its performance. The dataset of AT & T is used for the simulation. All the images should be captured at different time period having different lighting, facial expressions (open/closed eyes, smiling/ not smiling) and also have all the facial details. The images should be captured in dark homogeneous background with the subject at the upright position, front position (some side movements). This AT&T database most commonly known as The Oral Database of Faces contains images of 10 subjects each having 3-4 different images. All the 40 images are captured between the year 1992 and 1994.

Fig 3: Execution Time

Fig 3 shows the comparisons amongst the proposed KNN classifier as well as the previously existing approach of SVM according to their execution time. The results ensure that the KNN classification approach minimizes the execution time with respect to SVM approach.

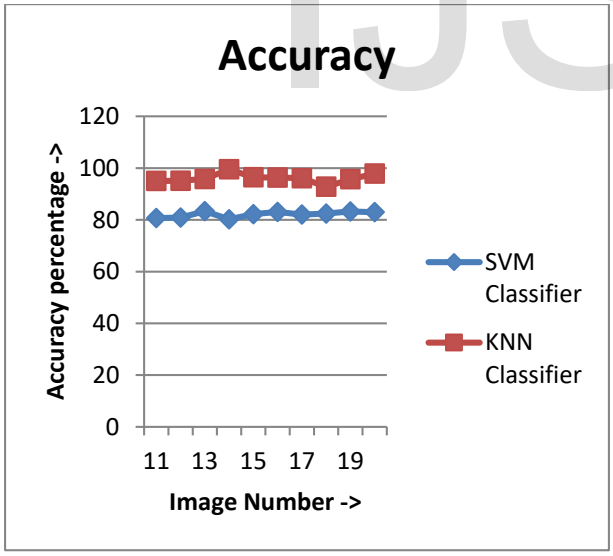

Fig 4: Accuracy Comparison

Figure 4 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.

The average accuracy of existing technique is about 86 percent and execution time is 2.3 seconds. In the proposed technique, the average accuracy of is about 94 percent and average execution time is 1.3 seconds.

Conclusion

Biometric system plays vital role in providing authentication to the users. The face recognition is an efficient type of bio-metric system to provide authentication to authorized parties. While these systems are vulnerable to spoof attacks to gain illegitimate access to the systems, face spoof technique is proposed to identify the spoofed faces added due to the unauthorized access to the data. The existing technique of SVM has less accuracy and high execution in detection of spoofed and non spoofed faces due to the fact that its performance gets degraded in case of noise. Using our novel approach, it has been seen that there is considerable increase in accuracy and decrease in time of execution. The technique of kNN has been found highly effective in case of noisy training data and when the training samples are larger in size.

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] YamanAkbulut, 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, WeihuaOu, Linghui Liu, “Face Liveness Detection with Recaptured Feature Extraction”, 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC)

[15] OlegsNikisins, 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

[16] https://www.google.com/search?tbm=isch&q=Different+Spoof+attacks&chips=q:different+spoof+attacks,online_chips:face+spoofing&usg=AI4_-kQuJ6q8JFpNg4Ws_jHIjqZDWsW8jA&sa=X&ved=0ahUKEwjm6vnDrqvfAhWLfX0KHWWSDeYQ4lYIKygF&biw=1366&bih=657&dpr=1#imgrc=6Be1oO_yiLY78M: