International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

FACE Spoof Detection and KNN

Sakshi Jha[1], Dr. Neetu Sharma[2]

[1]M.Tech. Scholar, Computer Science & Engineering Ganga Institute of Technology and Management Kablana, Jhajjar, Haryana, India

[2]Associate Professor, Computer Science & Engineering Ganga Institute of Technology and Management Kablana, Jhajjar, Haryana, India

ABSTRACT

Face recognition has been viewed as the best authentication method in today's technological world .Despite of being so safe, it has been noted that it possess vulnerabilities. 3-D masks, video replay attacks and printed photographs plague face recognition. In order to protect the system against these spoof attacks, there is a need to develop face spoof detection system. This paper involves study about these various types of face spoof detection techniques and technology.

Keywords : Spoof, Face spoof, Face spoof detection, Face Recognition, KNN

I. INTRODUCTION

Social Media provides an easy access to someone's biometric features like voice and picture. Intruders have shifted from Password hacking to Spoofing Faces. Innovations in technology have proved to be less rewarding for face recognition. Security has always been a major concern for every individual and every organization. Safeguarding information from intruders is one of the most important tasks.

Organizations have shifted from traditional password protection method to Biometric Technology. It remained a successful method for the time until their hacks were not developed. Availability of one's photos, audios and videos on social media can help an intruder to masquerade as another and breach the authentication system. This attack is called as spoof attack.

Face spoof Attack can be done in two manners. One is the Database Attack and other is the Presentation Attack. In database attack, intruder attempts to insert fake biometrics data into the database [1]. In order to do this an attempt is made to know the communication between the biometric sensor and feature extractor [1]. On the other hand, in Presentation attack, intruder tricks the system to gain access by successfully masquerading itself as another using 3-D masks, video replay or photographs [2]. Replay attacks and printed photograph attacks are the two most common attacks to face recognition system.

In order to address these face spoof attacks, various methods have been developed so far. There is a limitation to every method. These are successful for static backgrounds. In real world environment, these methods and technologies prove to be less accurate. Therefore, a method has been proposed countering this limitation. The approach is to detect face spoof attacks in light controlled environment. Video attacks and photograph attack would be the major spoof attacks taken in consideration. A set of algorithms will be used to develop a system to find out if light reflection patterns can prove to be useful for face spoof detection in facial biometric applications.

This review paper is organized in four sections. Section 1 deals with the introduction part which involves information about face spoofing attacks. Further, Section 2 involves earlier work done in this area. Section 3 describes about the proposed work and the algorithms that will be used. Section 4 describes the conclusion and future scope of this proposed work.

II. RELATED WORK

Earlier researchers have developed and used several techniques for face spoof detection. This section focuses on four different categories of spoof detection techniques. These are characterized on the basis of data, behavioural modelling, external devices and interaction of humans with additional devices [3].

Tan et al . proposed characterization based system which was data driven. He used Lambertian Reflectance to distinguish between a fake face and a real face. Gaussian and variational retinex based system were applied for feature extraction [4] [5]. It came out in the research that the texture of real face differs from the fake face. NUAA database which is public was used for evaluation. Promising results were obtained while detecting fake face and real face [4].

Erdogmus and Marcel used Xbox Kinnect for developing an anti-spoof detection. This involved the use of external devices and Xbox Kinnect.Public spoof face dataset namely 3DMAD was used for research [6]. Classification of uniform features for Local Binary Patterns with Linear Discriminant Analysis yielded best results while detecting masked faces [6].

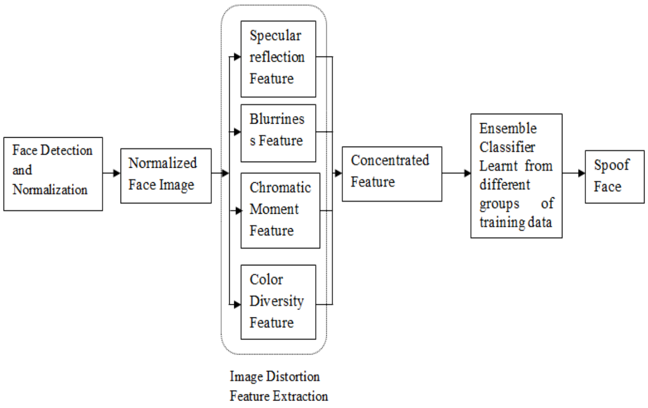
Face Detection and Normalization
Normalized Face Image
Specular reflection Feature
Blurrines s Feature
Chromatic Moment Feature
Color Diversity Feature
Image Distortion Feature Extraction
Concentrated Feature
Ensemble Classifier Learnt from different groups of training data
Spoof Face

Figure 1. Face spoof detection algorithm based on Image Distortion Analysis [7]

Image Distortion Analysis is also one of the best proposed methods by Wen et al for liveness detection of face. Chromatic movements, blurriness, color diversity and specular reflection are the four features on which image distortion analysis is done [7]. SVM classifier was used as an input to image distortion analysis vector. It gave best results in differentiating between a fake face and real face [7].

Eye blinking and lip movement are the two focussed areas in behavioural modelling .Hidden Markov Model is applied for detecting eye blinking [5] [8].Conditional Random field framework was used for considering eye blinking. Context Matching with stationary backgrounds for detecting face spoof was also considered. The proposed system gave promising results in the static background. It was noticed that spoof attacks using Video replay attack, 3D printed mask and pictures failed since the system would easily identify these fake faces. However, it was quickly noticed that the system potentially fails in different image backgrounds. This complication had arisen since most of the developed anti-spoof detection systems are environment dependent.

Therefore, there is a need for much stronger spoof detection system that can withstand successfully with changing backgrounds.

III. PROPOSED METHOD

The proposed system involves the use of KNN classifier for face spoof detection. SVM classifier is used in the existing system as an input to the image distortion vector. Considering large datasets for facial expression recognition, it came out in results that the accuracy id 98.85 % for KNN, 90% for SVM and 98.85% for Random Forests algorithm [9].Studying this measure of accuracy ,we decided to implement a system that uses KNN for spoof detection.

A. Face Detection : Viola and Jones proposed a face detection algorithm which uses HAAR cascade features that identifies a human face [10]. The algorithm searches throughout the entire sections of the image for Haar features. The moment one of the features is found it denotes the position. Features found are then given to the HAAR classifier as input .Further the output obtained is given to the comparator and all the calculations are performed .If the summed output value falls within the stage threshold limit then it is proved that it has passed all the stages. Furthermore, the given input is identified as an image or a face [10].

B. Gabor Filters: Edge detection, Feature Extraction, Text Segmentation and estimation of stereo disparity are the areas in which Gabor filter is used with promising results. In the proposed system, Gabor filter will be used for feature extraction that is noting pattern gradients caused by light reflecting on an image.

C. Blur detection : A probability distribution function Laplacian Variance is used for blur detection. It is also known as double exponential distribution. Laplacian operator uses second order derivative mask. Due to this reason , it is found to be very effective in edge detection and blur detection [11]. High variance of Laplacian results that the image has more edges and less amount of blurriness. If the variance is low it means that there are less edges and high amount of blurriness. Therefore, it is an important task to determine the threshold value set to a heuristic value that comes from empirical studies.

D. Local Binary Pattern: It is a classification algorithm. Its use is found mainly in image texture processing in computer vision. It involves breaking down of image in 16 x 16 pixels .Further the central number between 16 x 16 pixels is used to compare with the neighbours in the surrounding radius. Neighbour's value if found lesser than the middle number, then it is changed to 1 , else to 0 [10] [11]. The value is stored in a LBP mask on the location of middle point initially chosen for the block of image.Futher,when the algorithm has gone through the whole image, weights of blocks are left that represent the whole image. The list of these weights attained from each image block is then concatenated to form a feature vector representing the whole image.

E.

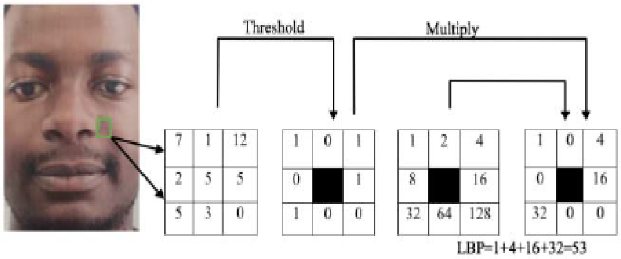

Figure 2. Application of Local Binary Pattern Algorithm

F. Color Moments: Red, Green and Blue are different color channels. Recaptured images have less color than the original ones. There is an observation made that the images captured from video attacks plot distributed histograms. While; histograms of real images are concentrated in one area. This results in higher peaks in histograms of real images than that of spoof images. This helps in distinguishing between a real face and spoofed face.

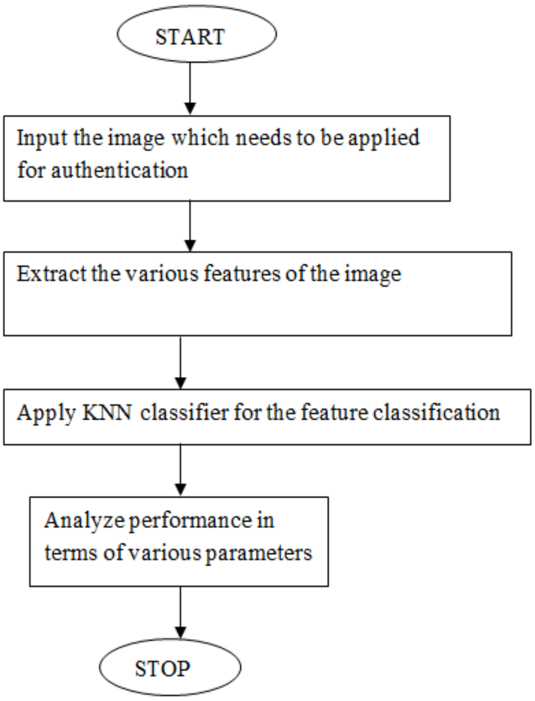
START
Input the image which needs to be applied for authentication
Extract the various features of the image
Apply KNN classifier for the feature classification
Analyze performance in terms of various parameters
STOP

Figure 3. Flowchart of Proposed Technique

IV. CONCLUSION AND FUTURE SCOPE

A model has been proposed to detect spoof faces using KNN classifier on a human face. Future work will involve looking at the angle of reflection together with the shadows produced when capturing a sample to improve detection rates. A model to detect spoof faces using light reflection patterns on a human face using the knowledge that every object reflects light differently has also been proposed.With further research into the use of reflection patterns for spoof detection we believe a robust face spoof detection system can be developed.

V. ACKNOWLEDGEMENT

I would specially like to thanks my worthy guide Dr.Neetu Sharma, who supervised me to complete this review paper. Her technical advice, ideas and constructive criticism contributed to the success of this paper. She suggested me many ideas and solved my puzzles. Her motivation and help has been of great inspiration to me.

VI. REFERENCES

[1]. Z. K. J. a. H. Boulkenafet, "A. Face Spoofing Detection Using Colour Texture Analysis.," IEEE Transactions on Information Forensics and Security 11, 8 (2016), 1818-1830., 2016.

[2]. S. Schuckers, "Spoofing and Anti-Spoofing Measures," Information Security Technical Report 7, 4 (2002), 56-62., 2002.

[3]. S. D. T. V. M. a. S. R. Bharadwaj, "Computationally Efficient Face Spoofing Detection with Motion Magnification," in IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2013.

[4]. A. P. H. R. S. W. a. R. Da Silva Pinto, "A Video-Based Face Spoofing Detection through Visual Rhythm Analysis," in 25th SIBGRAPI Conference on Graphics, Patterns and Images,IEEE Computer Society , 2012.

[5]. G. S. L. a. W. Z. Pan, "Eye blink-based Anti-Spoofing in Face Recognition from a Generic Webcamera," in IEEE 11th International Conference on Computer Vision, 2007.

[6]. N. a. M. S. Erdogmus, "Spoofing Face Recognition with 3D masks," IEEE Transactions on Information Forensics and Security 9, 2014.

[7]. H. H. a. J. Di Wen, "A. Face Spoof Detection with Image Distortion Analysis," IEEE Transactions on Information Forensics and Security 10, 2015.

[8]. S. M. S. A. S. H. M. a. W. A. Parveen, "Face anti-spoofing methods," CURRENT SCIENCE 108, 2015.

[9]. K. M. Ratna Astuti Nugrahaeni, "Comparative Analysis of Machine Learning KNN,SVM and Random Forests algorithm for facial expression classification," in Internation Seminar on Application for Technology of Information and Communication, 2016.

[10]. J. H. A. a. P. M. Maatta, "Face spoofing detection from single images using texture and local shape analysis," IET Biometrics, 2012.

[11]. J. C. G. C.-M. J. a. Pech-Pacheco, "Diatom autofocusing in brightfield microscopy: a comparative study.," in Proceedings 15th Internationa lConference on Pattern Recognition. ICPR-2000, IEEE (2000), 2000.