Detection of Face Spoofing using Color Texture and Edge Features

Neenu Daniel, A. Anitha

Abstract*: The wide scale use of facial recognition systems has caused concerns about spoofing attacks. Security is essential requirement for a face recognition system to provide reliable protection against spoofing attacks. Spoofing happens in situations where someone tries to behave as an authorized user to obtain illicitly access the protected system to gain advantage over it. In order to identify spoofing attacks, face spoofing detection approaches have been used. Traditional face spoofing detection techniques are not good enough as most of them focus only on the gray scale information and discarding the color information. Here a face spoofing detection approach with color texture and edge analysis is presented. The approach for investigating the texture of input images, Local binary pattern and Edge Histogram descriptor are proposed. Experiments on a publicly available dataset, Replay attack, showed excellent results compared to existing works.

Keywords*: Face Recognition, Color texture analysis, Spoofing attacks, Spoofing detection

I. INTRODUCTION

Biometric authentication systems promise a secure alternative for traditional authentication systems such as username, password etc. It has great diversity of applications such as criminal investigation, access control, etc. Biometric offers the recognition of an individual identity. Face Recognition, iris, fingerprint are some of the commonly used biometric authentication systems. Face is one of the widely used biometric as it is easy to use and non-intrusive in nature. But spoofing attacks are one of the main threats to the face recognition systems [1]. Spoofing is a kind of attack where, when an attacker tries to gain authorized user's privileges by using video, photo of the user. Spoofing attacks are easy to launch using video replays, photo attacks, and using 3D face masks. The Availability of images and videos on the social media and recent advances in technology such as 3D face mask, plastic surgery help the attackers to spoof the system. When an attacker try to spoof the system with the help of printed photograph, then it is called printed photo attack. Attackers will display the photo of an authorized person in a tablet or mobile phone in front of the camera, and then it is called digital photo attack. In video replay attack, Attackers capture video of genuine users using digital cameras, mobile, and tablet. This video is played at the time of face recognition and access the biometric modality. Attackers build a mask or clay face to spoof the system. The mask has similar 3D face shape features of the real face. The role of face spoofing detection in face recognition system is intended to safeguard the user from unlawful access through the face recognition systems. Face spoofing detection checks whether the user is fake before the face recognition start. Several face spoofing detection methods have been suggested to defend from face spoofing attacks. However, a powerful solution is required which works well under new imaging conditions and environments.

Spoofing causes degradation of image quality. Texture quality differs for real and fake faces. We propose a new technique which exploits the texture and edge based features for uncovering face spoofing in this paper. In particular we utilize Local binary pattern (LBP) and Edge histogram descriptor (EHD) for face spoofing detection. To evaluate our method we utilize the publicly available database, replay attack database.

The structure of the paper is as follows. Section II represents few previous studies on the detection of face spoofing. Section III elaborates our proposed methodologies in detail. Section IV demonstrates the results of the experiments conducted. Finally, conclusion is presented in Section V.

II. RELATED WORKS

Here we discuss few methods proposed recently in the field of detecting face spoofing. Existing approaches can be categorized based on texture analysis, frequency, image quality analysis, hybrid methods, motion analysis, person specific, and other cues. It is based on the assumption that there is a difference in the texture of real faces and fake face. Texture analysis is widely used approach in the area of face spoofing detection. Quality based techniques are based on an assumption that, there will be a reasonable difference between the quality of real and fake faces. The movement of 2D faces varies significantly from real human faces (3D objects). Frequency based approaches analyzes recaptured video to detect noise signals for real and fake face access. It is found that while recapturing the printed photos, the low-frequency components decreases and the high -frequency components increases. Person specific method makes use of client enrolled samples for face spoofing detection. Hybrid methods combine more than one face spoofing technique for example texture with motion etc.

A color texture analysis based face spoofing detection method was introduced by Z. Boulkenafet et al. [1]. The RGB image is given as input in this approach and it is converted in to suitable color space and from each color channel. Features extracted are LBP features and these are concatenated and

Revised Manuscript Received on January 30, 2020..
***** Correspondence Author
Neenu Daniel*, Department of CSE, Noorul Islam Centre for Higher Education. Nagercoil, India. Email: neenudaniel@gmail.com
A.Anitha, Department of CSE, Noorul Islam Centre for Higher Education, Nagercoil, India. Email: anithadathi@yahoo.co.in

classified by SVM. The experiments were performed popular data sets like MSU Face spoof database, Replay attack database, and CASIA FASD database and this technique revealed progress in generalization ability.

Wen et. Al [2] presented an approach based on analyzing image distortions. When real face images and videos in screens are recaptured to generate spoof face images and videos, there will be a degradation of reflection, color and blurriness while comparing the real images and videos. This method showed comparatively good generalization ability while considering different scenarios.

Li et al. [3] presented a hybrid method which incorporates flash light to capture texture and structure information to differentiate between fake face and real face. This technique combines both hardware and software method. Flash can improve the differentiation between real and fake users. With flash and without flash images of each subject were considered as input in this work. Texture and structure descriptors were used to capture information for discriminating live faces and fake faces.

Recently deep learning methods are becoming popular. De Souza et al. [4] addressed a face spoofing detection technique with great results on NUAA dataset, based on modified CNN with LBP. Here texture features using deep learning are used in face spoofing detection. In this technique LBP is integrated in the first layer of CNN and the deep texture features are extracted. Here NUAA dataset is used in this work. Accuracy is the merit of CNN based technique. But the problem is that, to train CNN a large number of samples are needed.

Recently Zhao et.al [5] described a dynamic texture face spoofing detection technique. Dynamic texture patterns are motion patterns. In this work, spatiotemporal descriptor called volume local binary count (VLBC) was proposed to represent dynamic texture. VLBC is adopted to capture neighboring pixel information. A completed version of VLBC was proposed to extract dynamic textures by considering local difference and central pixel intensities. CVLBC descriptor is utilized for face spoofing detection. CVLBC can describe the difference between motion and appearance in facial videos genuine faces and fake faces. The experiment was performed on print Attack, CAS Anti spoofing database and Replay Attack database which show good performance on three databases.

III. PROPOSED SYSTEM

A.Proposed Scheme framework

In this section framework of our proposed approach is presented. The proposed approach combines liveness features from two aspects. Texture and Edge based features. Face spoofing attacks are carried out by wearing mask on the face, displaying videos or photos in front of an input sensor. Gray scale images were considered in most of the existing solutions, and they try to detect the attacks by analyzing the texture and quality of the images. But color reproduction of photographs, mask and video displays is limited compared to real faces. Naked human eye is less sensitive to Chroma than luminance. That is the reason why human eyes fail to find the differences between original image and fake image. The recaptured image contains texture differences such as

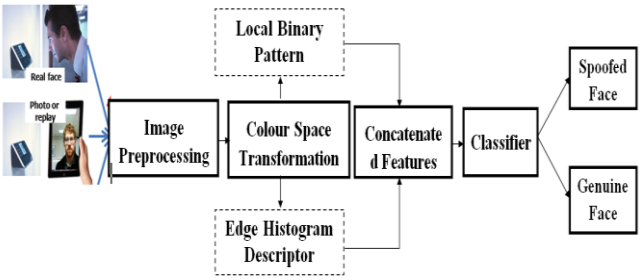


Fig. 1. Illustration of face spoofing detection approach.

printing defects, video artifacts etc. It is important to consider the luminance and chroma components to detect face spoofing. The structural diagram of the face spoofing detection using color texture and edge analysis is shown in Fig. 1.

In the proposed framework a single frame is randomly selected from a given face video. Then the face is identified, cropped and normalized in to 64X64 pixel image. Then the image is converted in to HSV color space. The proposed approach uses texture and edge features for face spoofing detection. Then the edge features and texture features are obtained from each color channel. Finally the extracted features are given to a SVM classifier which classifies the fake face and the real face. The proposed approach can be broken down in the following steps.

B. Preprocessing

In our work, face detection is implemented using the popular Viola Jones algorithm. This algorithm uses Haar cascade features to detect a face. This detection technique is very fast. The facial image is normalized to 64X64 pixels to reduce the effect of sizes variations in the input images, the facial image and its background.

C. Color Space

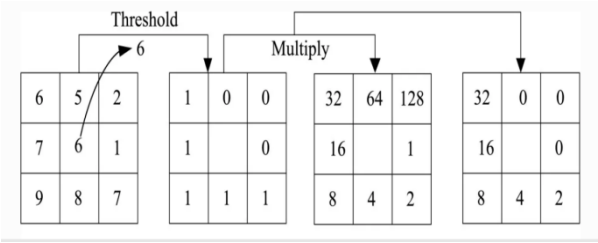
RGB is the most normally used color space which is used by computers, graphics cards, monitors etc. Because of high correlation between the color components, image analysis is difficult in terms of red, green and blue. In this work we considered HSV color space. HSV color space separates the luminance and chroma components. Hue and saturation is used to represent the chrominance of the image, and value denotes the luminance. In the proposed system, HSV color space is used for extracting color information.

D. Feature descriptors.

In the area of face spoofing detection, texture plays an important role. Inspired from face spoofing texture descriptors, LBP is the most efficient one. We explore the use of LBP[6] in our approach. For extracting edge features, edge histogram descriptor is considered. As structural distorion of an image is closely related to edge degradation. We decided to explore both the features using LBP and edge Histogram descriptor. Finally these two features are fused to form the final feature vector.

Local Binary Pattern (LBP) is a robust discriminative texture discriminator. This approach is used in several areas of computer vision such as, analysis

of medical image, recognize facial expression,



LBP = 2+4+8+16+32 = 64

Fig. 2. LBP operation[6]

modeling of motion and action etc.

Fig. 2 shows the LBP operation. LBP methodology works by calculating the local differences between the neighboring pixels and center pixel. It considers the comparison result in terms of 1 and 0. At first examined window is split into cells. For every pixel in a cell, it is compared to the nearest neignbours. Center pixel value is used as the threshold. If the intensity of the neighboring pixel is more than the center pixel intensity, the value is encoded as 1. If the intensity of the neighboring pixels are less than the center pixel intensity, the value is encoded as 0. P = 8 with the circle radius R = 1 is the most commonly used sample in LBP. In this sample LBP is performed on 8 neighboring pixel around the center pixel. The distance between the center pixel and neighboring pixel is assigned a value one if R = 1. After that, concatenate the binary value of the neighboring pixel. Then convert the binary value to a decimal value. For every pixel in the image conduct the same process.

The other powerful Edge Histogram descriptor (EHD)[7] is used for extracting edge feature. EHD falls under the family of MPEG7 descriptors. Human eyes are more subtle to edges for image perception. Edge information can also be evaluated for textural representation for finding the shape. Edge in faces offers an effective way to represent the information and the content. The frequency and the directionality of the brightness variations in an image can be represented by edge histogram in the images. Most of indicative information and the relevant features are pertained by edges. Five types of edges are defined by Edge Histogram descriptor in a local area, and are known as sub image. To extract EHD features, image is divided into 4×4 sub images. Now every sub image is again divided in to non-overlapping blocks. Edge histogram is calculated for each block evaluating the strength of five types of edges. Fig. 3 defines the five types of edges. Relative frequency of five types of edges represents histogram of sub image.

E. Classifier

Choosing the classifier is important to classify the spoofed and real faces. Support vector machine (SVM) is the widely used classification method in face spoofing detection. We adopt the SVM classifier to determine the correct class for features extracted from both real and spoofing face images. SVM classifier is best suited for classification as it takes lesser execution and accuracy. It is one of the simplest of classification algorithms. It is a method for classifying objects based on finding hyper plane that separates the real and fake faces. In the First step, the SVM training is performed using real and attack samples. The LBP and edge

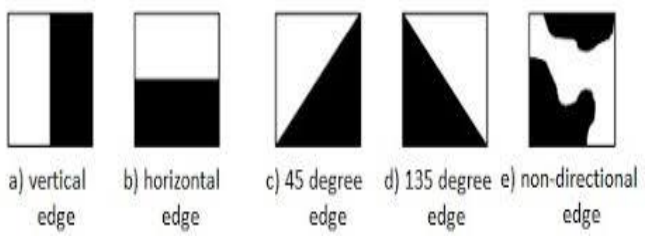


Fig. 3. Type of Edges [7]

Fig. 4. Real faces and corresponding high definition, mobile and print attacks are shown from left to right[8]

features of input image are concatenated from to form a feature vector. The concatenated edge and LBP features are fed to SVM classifier. SVM classifier decides the real and fake face.

IV. EXPERIMENTS

Spoofing detection technique is expected to be powerful across various types of attacks. The effectiveness of our proposed method is evaluated using replay attack dataset [8]. It is one of the challenging databases which contain video recordings of different types of attacks and real samples.

This database holds videos of real and spoofed attack attempts recorded using 1300 MacBook at 320×240 resolution. Attack samples are acquired under controlled and adverse lighting conditions. Fig 4 shows the real faces and attack samples from the replay attack database. Three spoofing attack types considered including video attack, print attack, and digital video attack. The experiments were performed using the images in replay attack dataset database, selecting 80 % of the images are used in the training phase and the remaining 20 % used for testing phase. The main objective of the work is to detect various types of attack such as High definition attacks, replay and print attack.

A.Discussions

The metric used to evaluate the performance of the proposed face spoofing detection system was using half total error rate (HTER). HTER is computed using the equation;

Table- I: Experimental Results

Sl. NO	PARAMETERS	VALUE
1	Accuracy	97 %
2	Sensitivity	97 %
3	FPR	0.83%
4	HTER	0.3

Table-II. Performance comparison with existing techniques

Sl. NO	METHOD USED	EER (%)	HTER (%)
1	Image distortion analysis(IDA)[2]	-	7.41
2	Dynamic mode decomposition (DMD)[9]	5.3	3.75
3	Visual code book (VCB)[10]	-	2.8
4	Color Texture Analysis (CTA)[1]	0.4	2.8
5	Volume local Binary Count (VLBC)[5]	1.7	0.8
6	Proposed Method	-	0.3

$$HTER = (FAR+FRR)/2 \qquad (1)$$

In which, FAR and FRR stands for False Rejection Rate and False Acceptance Rate. The metric, False Acceptance Rate (FAR) is the ratio of malicious acceptance that was not correctly recognized by the system. False Rejection Rate (FRR), called as False Positive Rate (FPR), represents the ratio of real accesses that were wrongfully classified as spoofing attacks. The metric Sensitivity is called True Positive Rate (TPR) or recall which is the percentage of number of spoof images getting correctly classified as spoof. Overall accuracy rate is the number of images correctly classified as spoof or original.

The proposed approach was implemented using MATLAB. We started by evaluating the performance of two powerful texture descriptors namely LBP and Edge Histogram descriptor to distinguish between real and fake faces. These computed features are fed to SVM Classifier. In Table-I we can see the results, where descriptors performed well to capture the discriminative information between real and fake faces.

Our method was able to achieve classification accuracy of 97%, sensitivity of 97%, false positive rate of 0.83%.Typically lower the HTER, better the method is. For replay attack database, it is clearly evident that the results obtained using color texture features using LBP and EHD on HSV color space significantly improves the performance. The proposed scheme is compared with some existing face spoofing detection techniques and the results are listed in Table-II. Quality based methods not performing well when compared to texture features. This is because wide variety of camera models affects the distortion information of spoofing objects. Texture based methods is showing average performance. But using color texture features, better performance can be achieved in some situations mainly different scenarios.

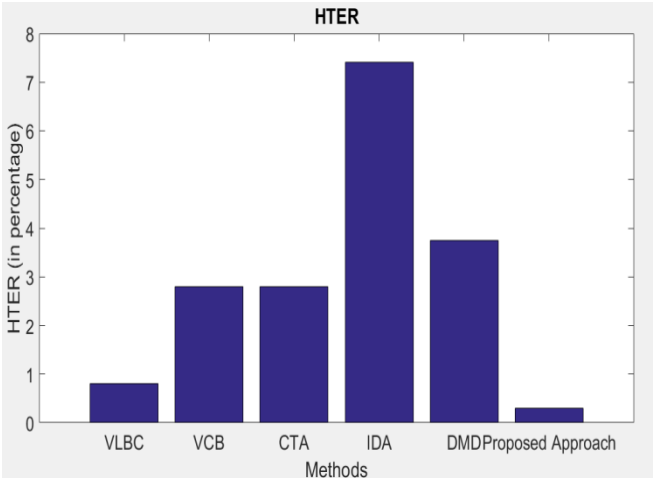


Fig. 5. Experimental Results

The results of existing approaches in terms of HTER are represented as a bar graph in Fig 5. By comparing with the existing similar methodologies, the proposed system performs more efficiently and achieved a much lower error rate.

V. CONCLUSION

Face spoofing is a substantial challenge in face recognition systems. Here we examined the problem of face spoofing detection using color texture and edge analysis. For this we propose the use of LBP and Edge histogram descriptor for texture analysis. The proposed system is systematically evaluated on publicly available datasets and proved to be excellent when compared to other texture analysis schemes. In this study we observe that color texture analysis provide more information to detect spoofing attacks when compared to other techniques. It is found that the objective of most of the research works were to reduce the error rate. But their generalization ability was not properly addressed. So a robust design is required for the face spoofing detection system with generalization capabilities to all the attacks. In the future we will deal with cross database testing.

REFERENCES

1. Z.Boulkenafet, J. Komulainen, A. Hadid, "Face spoofing detection using color texture analysis", IEEE Transactions on. Information. Forensics Security, Vol. 11, No. 8,(2016), pp: 1818-1830.
2. D. Wen , H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," *IEEE Transactions on. Information and. Forensics Security*, Vol. 10, No. 4,(2014),pp: 746–761.
3. P. P. K. Chan et al., "Face liveness detection using a flash against 2D spoofing attack," *IEEE Trans. Inf. Forensics Security*, Vol. 13, No. 2, (2017), pp: 521–534B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.
4. De Souza, G.B.; Da Silva Santos, D.F.; Pires, R.G.; Marana, A.N.; Papa, J.P.," Deep texture features for robust face spoofing detection*." IEEE Transactions on Circuits and Syst. II Exp.ress Briefs* ,Vol.64,No.2,(2017), pp: 1397 – 1401.
5. X. Zhao, Y. Lin, and J. Heikkila, "Dynamic texture recognition using ¨ volume local binary count patterns with an application to 2d face spoofing detection," IEEE Transactions on Multimedia,Vol20,No.3(2018).
6. T. Ahonen, A. Hadid and M. Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 2037-2041, Dec. 2006.
7. C. S. Won, D. K. Park, and S. J. Park, Efficient use of MPEG-7 edgehistogram descriptor, ETRI J., vol.

24, no. 1, pp. 23-30, 2002C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

8. I. Chingovska, A. Anjos, S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing", Proc. IEEE Int. Conf. Biometrics. Special Interest Group, pp. 1-7, 2012-Sep
9. S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. Ho,"Detection of face spoofing using visual dynamics," IEEE Transactions on Information Forensics Security, Vol. 10, No. 4, (2015), pp: 762–777.
10. A. Pinto, H. Pedrini, W. R. Schwartz, A. Rocha, "Face spoofing detection through visual codebooks of spectral temporal cubes", IEEE Trans. Image Process., vol. 24, no. 12, pp. 4726-4740, Dec. 2015 .

AUTHORS PROFILE

Neenu Daniel is pursuing her PhD from Department of Computer Science and Engineering at Noorul Islam Centre for Higher Education, Tamil Nadu, India. She completed her M.Tech in Computer Science and Engineering from VIT University, Vellore in the year of 2007. She completed her B.E from CSI College of Engineering in the year of 2005. She has published 7 papers in international journals. Her area of interest include Image processing, Mobile Computing and Web Technologies**.**

A.Anitha is working as an Assistant professor in the Department of Computer Science and Engineering at Noorul Islam centre for Higher Education, Tamil Nadu, India. She obtained her PhD degree in A Novel approach for improving QoS in WLAN from Noorul Islam centre for Higher Education, Tamil Nadu, India and Master degree in computer Science and Engineering from Dr. Sivanthi Adithanar College of Engineering in the year of 2008. She did her B.E degree from Noorul Islam College of Engineering in the year of 2004. Her research interest includes Wireless Sensor Networks, Wireless Networks and Image Processing.