A Noval Approach for Face Spoof Detection using Color-Texture, Distortion and Quality Parameters

Sini K Thomas
Department of Electronics and Communication Engineering
Amal Jyothi College of Engineering
Kanjirapally, Kerala, India
sinikthomas317@gmail.com

Ajai Mathew
Department of Electronics and Communication Engineering
Amal Jyothi College of Engineering
Kanjirapally, Kerala, India
ajaimathew@amaljyothi.ac.in

Abstract— Face spoof detection technique is used in many applications to check whether the given face is spoofed or not. It helps to detect the fake faces from genuine ones. An efficient proposed method for face spoofing detection is based on color-texture, image distortion and image quality parameters. The faces are detected from a compressed format image. The color-texture information from the luminance and chrominance channels extracted using Local Binary Pattern descriptor. The image distortion and image quality parameters are extracted from the same color space. The aim of this method is to bring together the advantages of these methods inorder to improve the accuracy of face spoofing detection. Multiclass SVM classifier is used to train each features of data and detect different face spoof attack. This paper describe a novel and appealing approach for detecting the fake faces from genuine ones using a color-texture combine with image distortion and image quality parameters. More importantly, the proposed method provides more accuracy, other than the method that described in the literature. It helps to separate the original face and fake face clearly and define the type of attack.

Keywords- *Face Recognition, Colour-texture analysis, Image Distortion analysis, Image Quality analysis, Multiclass SVM classifier, Face spoof detection, Printed attack, Mobile Replay attack.*

*****

I. Introduction

In this technological developing world, face spoof detection technique plays an important role to detect the genuine faces from the fake faces. Spoofing attack occurs when someone tries to place spoofed faces such as printed photo or replayed photo (mobile attack) infront of the camera other than the original face [4]. Color spaces are more important to finding the fake faces [1]. Proposed solution uses HSV color space for describing this method. Local Binary Pattern (LBP) is used to extract the texture information from the detected face.

In this method, a new face spoof detection technique is described based on color-texture, image distortion and image quality parameters. The contributions of this paper are summarized as follows:

i) We construct a database consisting of three types of data medium such as original photos, mobile photos and printed photos.

ii) We extracted the color-texture features from the normalized face using Local Binary Patterns (LBP).

iii) Image distortion and image quality parameters are extracted from the same color space.

iv) Multiclass SVM classifier is used to train each features of data. It has an ability to find the type of attack.

We continue this paper as follows: Section II describes the existing works on face spoof detection. Section III provides the proposed method on face spoof detection. Section IV explains the experimental results of proposed method. Section V covers conclusion.

II. Prior Work

A. *Motion Based Method*

In this motion based method, it follows the direction of motion of every pixel in the detected input image. When the object moves, the facial features remain changed [5]. For example, human eye-blink occur once every 2-4seconds. If the background remains non stationary or the video has a low motion activity and poor lighting occurs, it is difficult to identifying the spoofed samples. This motion based method takes long time to detect the given face is spoofed or not.

B. *Texture Based Method*

The texture features of genuine faces and artificial faces are not same. The photographs are normally smaller in size than original and have fewer high frequency components compared to real faces. In this texture based method, skin properties are mainly extracted [1]. But the main drawbacks of texture based method is that high resolution input images are required. And this method has poor generalization ability.

C. *Image Quality Based Method*

In this method, genuine faces are analyzed on the basis of image quality performance. The fake faces have lower quality performance than real faces. In Image quality based method, 25 quality features are extracted from one image [3]. But fake identities always have some different features than original. It always contains different color and luminance levels, quantity of information, quantity of sharpness, structural distortions or natural appearance. But its limitation is different classifiers needed for different spoof attacks.

D. *Cue Based Method*

In this case, additional sensing or processing technique such as IR, audio, 3D is required. But when using audio or 3D cues, its response is very slow (> 3seconds). The main disadvantages of existing methods are, the feature extraction and verification process takes some time and provides less accuracy.

III. Proposed Approach

The spoofed faces are detected on the basis of color-texture, image distortion and image quality parameters. The aim of this work is to bring together the advantages of these methods inorder to improve the accuracy of face spoofing detection technique. The general block diagram for face spoof detection technique is shown in Fig. 1:

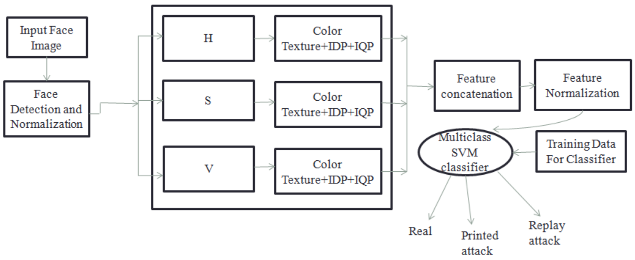

Fig. 1. Proposed block diagram.

A. *Color spaces*

RGB is the most commonly used color space for sensing, representation and displaying of color images. In this case, all luminance and chrominance portions are required. Its application in image analysis is quite limited due to high correlation between the three color components (red, green and blue). But we need only about a specific color variations. So HSV color space is used in this method.

In the HSV color space, H stands for Hue (1) that defines the pure color it resembles. The Hue is described by a number, which specify the position of corresponding pure color as a fraction between 0 and 1. S stands for Saturation (2) that defines how white the color is (white has a saturation of zero). V stands for Value (3) that defines the lightness.

$$H = \cos^{-1} [0.5 [(R-G) + (R-B)] / [(R-G)^2 + (R-B) (G-B)]^{1/2}] \quad (1)$$

$$S = 1- [3/(R+G+B)] [\min(R, G, B)] \quad (2)$$

$$V = [1/3] [R+G+B] \quad (3)$$

Where R, G, B denotes the Red, Green and Blue color intensity. The hue and saturation dimensions define the chrominance of the image while the value dimension corresponds to the luminance. The HSV color space extracts the facial features of the input image. It remains constant, as the face moves or rotate. The genuine face and fake face shows disparities in the color information.

B. *Texture representation*

Local Binary Pattern (LBP) is a method used in texture analysis [5]. The LBP operator is applied on each color band. It tests the relation between pixel and its neighbors (4) and encoding this relation into a binary word is shown in Fig.2. Due to the discriminatory power and computational simplicity, LBP texture operator has become popular.

$$LBP_{P, R} = \sum_p s\,(g_p - g_c) 2^P \quad (4)$$

Where p ranging from 0 to P-1,
P is the total number of involved neighbors,
R is the radius of the neighborhood,
g_p is the gray value of the neighbors,
g_c is the gray value of the central pixel.

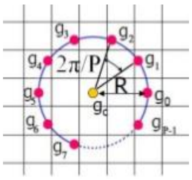

Fig. 2. Example

C. *Distortion parameters*

The distortion is a change, that makes something appear different from the way it is really is. Image distortion means changing the spacial relationship between the parts of the image, usually by printing with paper at an angle to enlarger beam. In this work, the face spoofing attack can be identified on the basis of one distortion parameter. The four distortion features are specular reflection feature, image blurriness, image chromaticity and color diversity. Among these, chromatic moment features can be used in this method. This image chromaticity is due to the imperfect color rendering.

Normalized facial features can be converted from RGB to HSV. Then calculate the mean, standard deviation, skewness, minimal histograms and maximal histograms of each color space. The mean defines the average change of intensity. The skewness defines the probability of distribution of pixels. These features are referred as chromatic moment features. The dimensionality of this feature is 5 X 3 =15. That means 5 types of features with 3 channels.

D. *Quality parameters*

The quality parameters of real face and fake face are somewhat different [3]. Inorder to find the quality features of the given image; we create a Gaussian low pass filter. Gaussian filter has an advantage that their support in time domain is equal to their support in frequency domain and in everywhere, it is nonnegative. This Gaussian filters creating a filtered image from the input image. Both of as compared and extract the quality features such as Mean square error (MSE) (5), Peak signal to noise ratio (PSNR) (6), Signal to noise ratio (SNR) (7), Structural content (SC) (8) and Maximum difference (MD) (9).

$$MSE = sum\ (sum\ (original\ image — filtered\ image)^2\ ) / (rows * columns) \quad (5)$$

$$PSNR = 10 \log [\max (original\ image)^2/MSE] \quad (6)$$

$$SNR = 10 \log [[sum\ (sum\ (original\ image)^2] / [MSE * rows * columns]] \quad (7)$$

$$SC = [sum\ (sum\ (original\ image)^2)]/ [sum\ (sum\ (filtered\ image)^2)] \quad (8)$$

$$MD = \max (original\ image — filtered\ image) \quad (9)$$

E. *Classifier*

For the modification of face spoof detecting method, multiclass SVM (Support Vector Machine) classifier is used. This is a supervised learning method. The Multiclass SVM classifier in normalized feature space is considered for classification by using modified kernel functions. There are 70 images are stored in database. The color-texture information, image distortion features and image quality features are extracted from each image and stored in database feature array. All the features extracted from the input image and the database features of each training data are applied to the multiclass SVM classifier. It check and find the given image is spoofed or not and detect the type of attack.

F. Datasets

To improve the effectiveness of our method, two datasets are created, namely Mobile Replay attack database and Printed attack database (see Fig. 3). The entire database consists of 70 images such as original images, mobile replay attack images and printed images. The genuine face means place the face close to the camera.

Mobile replay attack database contains 23 images. These high resolution images are taken using iPhone. Then these images are placed directly infront of the camera.

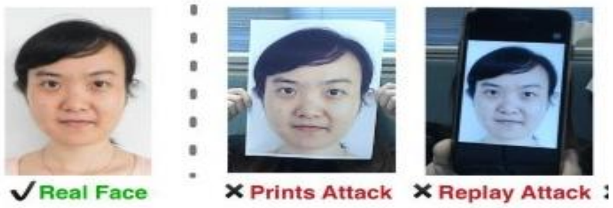

Fig. 3. Example of printed attack and replay attack

Printed attack database contains 17 images. In high resolution printer, corrections of pictures are available. These pictures were printed on A4 size paper and displayed to camera.

IV. EXPERIMENTAL RESULTS

To support the performance analysis, simulations were undertaken using MATLAB. Fig. 4. shows face detection of the given image, and then normalization takes place. In normalization technique, only wanted portions of the image are cropped and then color conversion takes place.

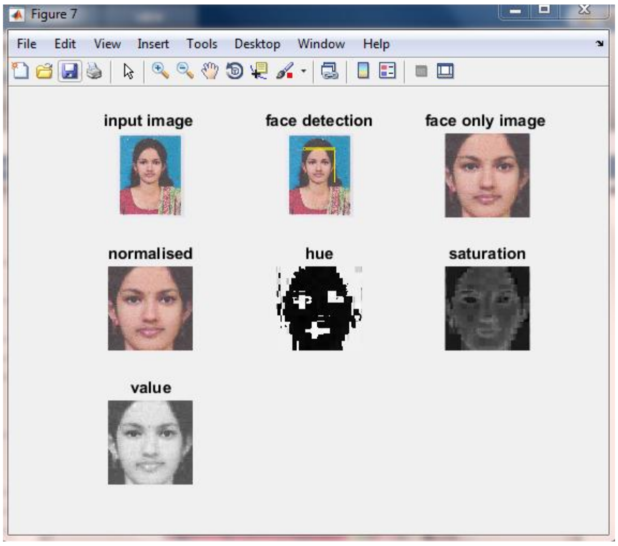

Fig. 4. Face identification, normalization and color conversion

After color conversion, the texture features are extracted using LBP analysis. Then distortion feature as chromatic moment feature and quality features such as MSE, PSNR, SNR, SC and MD are extracted. Finally, these extracted features are concatenated and min-max normalization takes place. It changes the range of pixel intensity values. After that, these features are applied to a multiclass SVM classifier. The database feature of the training data is given to the multiclass SVM classifier. Both features are compared and find the given image is real or not. If the given image is not genuine, then detect the type of attack is shown in Fig. 5.

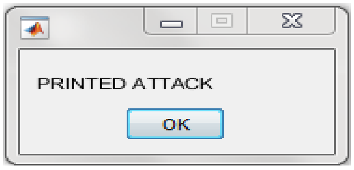
PRINTED ATTACK

Fig. 5. Type of attack

A. Comparison

Inorder to evaluate the performance of proposed method, the face spoof detection technique using color-texture, image distortion and image quality parameters shows very fast response and provide more accurate output with low complexity than the existing methods. The proposed method takes only 8 seconds to detect the given image is spoofed or not and find the type of attack.

V. CONCLUSION

The proposed method is efficient to detect the given image is spoofed or not. It has also found the type of attack such as Replay attack and Printed attack. Based on color-texture analysis with image distortion and image quality parameters, this face spoof detection technique is able to achieve more accuracy with very fast response.

REFERENCES

[1] Zinelabidine Boulkenafet, Jukka Komulainen, and Abdenour Hadid, “Face spoof detection using color texture analysis,” in IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, Aug. 2016.

[2] [6] D. Wen, H. Han, and A. K. Jain, “Face spoof detection with image distortion analysis,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 4, pp. 746-761, Apr. 2015.

[3] J. Galbally, S. Marcel, and J. Fierrez, “ Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition,” IEEE Transactions on Image Processing, vol. 23, no. 2, pp. 710-724, 2014.

[4] Nalinakshi B. G, Sanjeevakumar M. Hatture, Manjunath S. Gabasavalgi, Rashmi P. Karchi, “Liveness Detection Technique for Prevention of Spoof attack in Face Recognition System,” in Proc. IJETAE Int. vol. 3. Dec. 2013, pp. 627-633.

[5] A. Anjos, M. M. Chakka, and S. Marcel, “Motion based countermeasures to photo attacks in face recognition,” IET Biometrics, vol. 3, no. 3, pp. 147-158, 2013.

[6] J. Mtt, A. Hadid, and M. Pietikinen, “Face spoofing detection from single images using micro-texture analysis,” in Proc. Int. Joint Conf. Biometrics (IJCB), Oct. 2011, pp.17.