TEXTURE AND QUALITY ANALYSIS FOR FACE SPOOFING DETECTION USING MACHINE LEARNING AND DEEP LEARNING TECHNIQUES

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

SUBMITTED BY

G.Indhumathi (20PIT004)

Under the Guidance of

Mrs.S.Karthika M.C.A.,M.Phil,NET.

Assistant Professor

Department of Information Technology

AVINASHILINGAM INSTITUTE FOR HOME SCIENCE AND HIGHER EDUCATION FOR WOMEN

SCHOOL OF PHYSICAL SCIENCES AND COMPUTATIONAL SCIENCES

DEPARTMENT OF INFORMATION TECHNOLOGY

COIMBATORE-641043

MAY-2022

1. INTRODUCTION

The majority of the existing face recognition is now known to be susceptible to spoofing attempts Spoofing occurs when someone attempts to fool facial expression facial recognition software by having to put on a false smile in front of a camera. As an example, in [1,] research examines the threat of internet community web facial disclosing against the most recent editions of six production faces authentication systems. Whereas only half of the images posted on social media could be successfully spoofing, this same limited fraction of useable images was sufficient to fool 77 percent of a 74 clients' face authentication software.

A female intruder trying to wear such makeup also was effective in fooling face recognition in a video concert at the Conference on Biometric Authentication (ICB 2013). Among many others, these two examples illustrate how vulnerable face recognition systems can be to spoofing efforts there have been innumerable anti-spoofing techniques proposed. that conduct an investigation static (and dynamic) facial feature properties, assuming that there are lots of different kinds between genuine faces and fabricated content and is visible in image data.

The main reason is that a picture of a phoney face will be managed to capture by 2 distinct video cameras as well as a publishing or display device, results in a recaptured image. Due to problems such as a large amount of quality original signal, the identified fake facial recognition system is more probable to have poor picture quality than a legitimate something captured in the circumstances. [1].

Other quality issues the with captured images involve content-independent printing objects as well as video noise signatures. Because the above said characteristics can be thought of as variations in facial image characteristics as well as picture quality, face mask features analyzing techniques are also known as composition or picture quality analysis-based techniques in the literature.

Above - Picture discrepancies between such a genuine human face and a freed face image are introduced during the retaking process. This is due to the dependent gamut of the spoofing medium (physical copy pictures, gadget, or mask) as well as other factors. Color reproduction flaws, including publishing flaws and noise signatures.

2. ABSTRACT

Existing face bio - metric systems are susceptible to spoofing attacks. A spoofing attack happens when someone attempts to impersonate someone by falsifying information and gaining unauthorized access. We suggested approaching the Spoofing identification from the standpoint of texture classification, engendered by contrast enhancement, characteristics of printing artifacts, and variations in light reflection In fact, face prints frequently have able to print top notch faults that can be discovered using surface as well as local texture. The human body of studies on pro software-based face attacker uses classification methods has focused on gray – level documentation in face images, disregarding a same Chromo component, that can be very important in differentiating between fake and honest faces This article explains a novel as well as appealing texture analysis analysis technique for identifying face spoofing. We use complement low in fat and high explanations from different color spaces to manipulate the joint image feature extraction from the chrominance and luminance channels.

Keywords — Color texture analysis, Deep Learning, Face recognition, Machine Learning, spoofing detection, presentation attack.

3. METHODOLOGY

The proposed framework has been divided into four stages. The dataset has been illustrated throughout Phase I. The pre-processing techniques for reducing image over-brightness using gamma correction are explained in Phase II. In phase III, feature extraction is being used to detect faces using HOG and LBP. Machine learning and deep learning detection were also implemented in phase IV to detect spoofed humans.

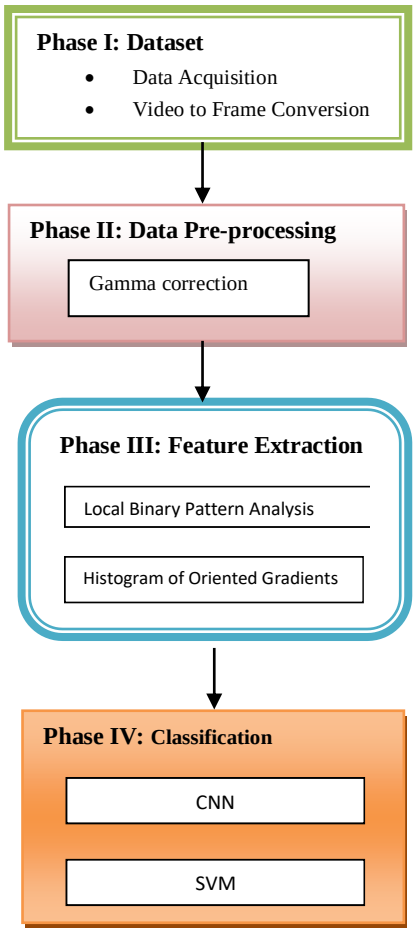

Figure 1: shows the proposed methodology using supervised Learning-based spoof detection.

4. RESULTS AND DISCUSSION

Phase I: Dataset

Convolutional neural networks Anti-spoofing Face -As a classification of two-class issues, this paper are opposed to face spoofing. The two types of face n To handle the above-mentioned framework, the "Reply Mobile Attack" set of data (Texture as well as Quality Assessment for Face Spoofing Detection-2021) [3] is used. Replay-Mobile is a face recognition dataset that detects introduction known attacks (anti-spoofing) [3]. The dataset includes 1190 short videos of video and photo presentation (spoofing) attacks on 40 customers in various lighting conditions. The front-facing camera wishes to record colour clips in the ".mov" format file at a resolving of 720 pixel resolution (width) besides 1280 pixel resolution (height) (height). The legitimate user already had performed real-accesses (revealing one's true face to the device). Incursions have indeed been decided to carry out by displaying for the at least 10 seconds a photo or recorded video of the attacked client.

Phase II: Data pre-processing

The input images in the selected dataset are taken from video recordings. To normalize the illumination, face images are preprocessed. Gamma correction is used in this scenario. Different camera or video recorder devices do not capture luminance correctly. Different display devices, such as a monitor, phone screen, as well as television, do not display luminance correctly. As a outcome, they must always be corrected, which is where the gamma correction functions finally came in. A gamma correction function is used to correct the luminance of the image.

Output luminance = gamma Correction Function

[Input luminance]

Gamma Correction is one of the techniques which can be used to control the brightness and quality of image data. Figure 2 shows the training set instance before and after the gamma correction technique has been applied.

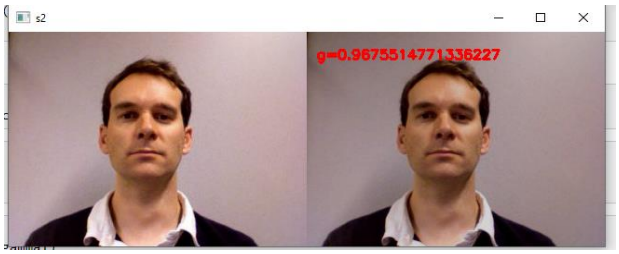

Figure 2: Before and after applying the Gamma Correction.

The Power Law Transform is another term for gamma correction. To start, humans must scale our image pixel intensities from [0, 255] to [0, 1.0]. Next we apply the following equation to get our output gamma corrected image:

$$O = I \wedge (1 / G)$$

Our input image is I, and our gamma value is G. The scale of such output image O is then restored to [0, 255].

Gamma values almost one will make the image appear darker, while gamma values greater than one will make it appear lighter. The input image will be unchanged by the gamma value of G=1.

Phase III: Feature Extraction

LBP (Local Binary Pattern Analysis) is a grayscale texture descriptor really is highly discriminative. By quantizing the other's normalised environment with benefit of the centre pixel, A binary code is aimed at each pixel of an image. A histogram is eventually created to track these same occurrences of different patterns.

Ojala et al introduced the LBP, which is shown in the literature being an effective gray - level invariant texture descriptor. These same An LBP operator's functional and statistical local texture characteristics have been combined. The LBP depicts texture by utilising micro primitive people and about their statistical placement rules. The LBP operates pixel perfect, displaying the 8 pixels in binary code. The LBP then combines all the rules into a graph, which is displayed. it much easier to extract a texture feature. As a result, a 256-texture pattern for a two-half neighboring would be generated.LBP was built to handle grayscale images, but it was later extended to include colour information well as. A simple and direct yet effective colour LBP descriptor was proposed. On each colour band, the LBP operator is

being used. The LBP pattern of an image band I pixel (x, y) can be written as follows:

$$\mathbf{LBP}(x_c, y_c) = \sum_{i=0}^{7} s(g_i - g_c)2^i$$

$$s(x) = \begin{cases} 1 & x \geq 0 \\ 0 & x < 0 \end{cases}$$

The LBP assumed that texture has parallel elements: pattern and strength. A specified threshold is being used to annotate the pixels of an image by evaluating influence the process to the middle. A binary number would be used to represent the result. This value will be used to create a texture descriptor.

Divide the window under examination into molecules (e.g. 16x16 pixels for each cell). Compare each pixel in a cell to its eight neighbours (just on left-top, left-middle, left-bottom, and right-bottom). Follow the pixels around a circle in a clockwise direction. The neighbors considered in the previous stage can be altered by altering the radius containing the data point, R, and the loss compression of the angle space P.

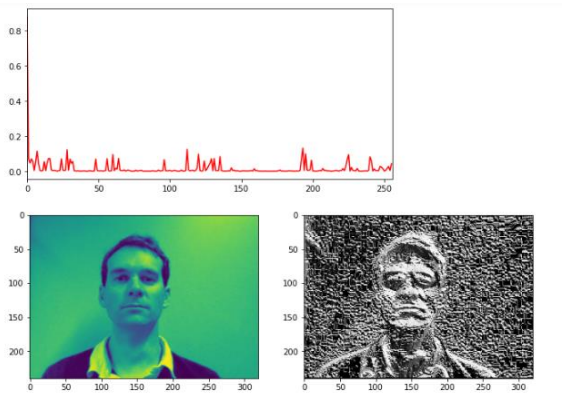

Figure 3: Facial features from the face using LBP texture descriptor.

Write "0" in which the value of a center pixel is higher than the price of its neighbor. Alternatively, write "1." This yields an 8-digit binary code (which is usually converted to decimal for simplicity of the use). Calculate the frequency distribution of each "number" that occurs inside the cell (i.e., each combination of pixels that are barely larger).

To detect spoofing attacks, color LBP extracting features from face images are fed into a Vector

Support Machine (SVM) classifier.

The Histogram of Oriented Gradients (HOG) is an identical descriptor to the Based on edges Detection Algorithm and SIFTS (Feature Transform and Scale Invariant) it is used to detect objects in image and video processing. The method counts the amount of times a chrominance direction appears in a small area of an image. This method is similar to Edge Direction Graphs and Scale-Invariant Invariant Functionality Transformations (SIFT). The HOG classier emphasizes an object's structure or shape. It outperforms all other edge descriptive terms, so it bases the content of the matrix both on the magnitude and angle of a gradient. It creates histograms for the illustration region's magnitude and gradient orientation.The 361 vectors are concatenated into one giant vector to calculate the final feature vector for the entire image patch.

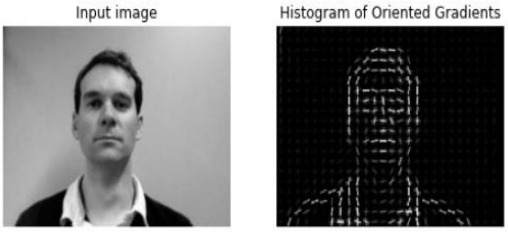

Figure 4: It will detect the Edges of a face.

So, if the input picture is 6464 pixels, the 1616 block has 7 horizontal values and 7 vertical positions. We have 4 histograms in one 1616 block, which after normalizing join to produce a 361 vector. This block spans 7 positions horizontal and vertical, accounting for 77 percent of the total. As nothing more than a byproduct, when we multiply them all together, we have a 3649 = 1764 linear vector. This variable is now being used to train Classifier model, which could be used to recognize items. Where the valuation of the key point is larger than the cost of its neighbor, write "0." Otherwise, write "1."

The image's gradient is calculated. The gradient is calculated by adding up the image's magnitude and angle. For each pixel in a 3x3 pixel block, the very first Gx and Gy elements are calculated. For each pixel the formulae below have been used to calculate value, Gx, and Gy first.

$$G_x(r,c) = I(r,c+1) - I(r,c-1) \quad G_y(r,c) = I(r-1,c) - I(r+1,c)$$

Phase IV: Classification

Convolutional neural networks Face Anti-spoofing -As a categorization of two-class issues, this paper are opposed to face spoofing. Real characteristics and mocked face images are the two types of face images. During the preparation stage, the CNN model class is predicted for preparing images, the unchecked pass misfortune is predicted, and finally, the system loads are updated using the inclination drop like a rock strategy by back-engineering of gradient for misfortune work.

Congratulations on the improved very good results while spoofing thanks to the use of a colour image blending technique. These loads will be used in all range age to generate output values and categorization precision over authorization pictures by using preparing pictures. Following completion of work, these same educated loads with the highest accuracy are delivered.

SVM based Face Anti-spoofing Convolutional neural networks Face Anti-spoofing -As a classification of two-class issues, this paper is opposed to face spoofing. Face Detection That Used Supervised learning Anti-spoofing in Approved Machine Learning Problems, multiclass phrase that really can refer to activities in which labels are designated to cases in which the classifications are collected from the a finite group of components.

For various spoof attacks, classification methods can be used in the present structure, which is premised on image distortion analysis. Each classifiers are trained on all genuine samples as well as a single set of spoof samples.To obtain final result, the output from each of these classifiers should be fused. Moreover, fusion is a time-consuming process, and if the output of any of the classifiers is invalid, the entire result will cause. To solve this, the proposed system employs a unique multiclass SVM.

SVM and CNN based Face Anti-spoofing

S.NO	METHODS	Accuracy
1.	Convolutional Neural Network	97.92%
2.	Support Vector Machine	100%

Figure 5: Performance Evaluation

5. CONCLUSION

The human body of studies on pro software-based face attacker uses classification methods has focused on gray – level documentation in face images, disregarding a same Chromo component, that can be very important in differentiating between fake and honest faces This article explains a novel as well as appealing texture analysis analysis technique for identifying face spoofing. We use complement low in fat and high explanations from different color spaces to manipulate the joint image feature extraction from the chrominance and luminance channels.

The Proposed methodology using SVM provides greater accuracy.CNN provides 97% accuracy with minimum loss. It is concluded that the SVM in machine learning and CNN in deep learning works better for Face spoofing identification based on image texture and quality.

6. REFERENCES

[1] Jukka Ma¨att ¨ a, Abdenour Hadid, Matti Pietik ¨ ainen Texture and quality analysis for face spoofing detection (29 January 2021)

[2] Balamurali K 1 , Chandru S 2 , Muhammed Sohail Razvi 3 and V. Sathiesh Kumar, Face Spoof Detection Using VGG-Face Architecture(2021).

[3] Kamlesh Kumar[1], Asif Ali Wagan[1*], Mansoor Ahmed Khuhro[1], Aamir Umrani[1], Ameen Chhajro[1], Abdul Hafeez[1], Asif Ali Laghari[1] Texture based Face recognition using GLCM and LBP schemes(2020)

[4] Chaorong Li, Huang Wei, Huafu Chen , LGLG-WPCA: An Effective Texture-based Method for Face Recognition (7 Jun 2019)

[5] Chaorong Li, Huang Wei, Huafu Chen, LGLG-WPCA: An Effective Texture-based Method for Face Recognition (2019).

[6] Md Rezwan Hasan[1], S M Hasan Mahmud[2] and Xiang Yu Li[1] , FACE ANTI-SPOOFING Using Texture-Based Techniques and Filtering Methods(2019).

[7] Yaojie Liu, Jeol Stehouwer, Amin Jourabloo, Yousef Atoum, Xiaoming Liu, Face Anti-spoofing, Face Presentation Attack Detection(2018).

[8] Zinelabidine Boulkenafet, Jukka Komulainen, Abdenour Hadid Center for Machine Vision Research, University of Oulu, Finland: FACE ANTI-SPOOFING BASED ON COLOR TEXTURE ANALYSIS (2018)

[9] Jukka Määttä; Abdenour Hadid; Matti Pietikäinen, Face spoofing detection from single images using micro-texture analysis(2011).

[10] Noor Al-Huda Taha a , Taha Mohammed Hassan b , Mohammed Akram Younis c, Face Spoofing Detection Using Deep CNN.