International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 6, May 2016

ISSN: 2394-4404

Face Spoofing Detection In Biometric System

Niranjan Gowda S.R
M. Tech, Student,
Computer Networking and Engineering,
Cambridge Institute of Technology, Bangalore

Shivakumar Dalali
Associate Professor,
Computer Science and Engineering,
Cambridge Institute of Technology

Abstract: Biometric frameworks have more precision when compared to with conventional strategies (watchword, key and so on). It recognizes and confirms the identity of a man based one or more physiological and behavioral attributes. That is Human body as secret key. The most well-known physical biometric characteristics incorporate unique finger impression, face, ear, iris, retina, hand geometry, palm print, DNA and so forth. Behavioral biometric qualities incorporate signature, gait, key strokes, speech patterns etc and so on. Each biometric has its own quality and restrictions and as needs be each biometric is utilized as a part of distinguishing proof (confirmation) application. This paper focuses on spoof attack against face recognition system, i.e. in this sort of assault a fake biometric can be displayed to sensor. This paper examines about Introduction to The Face biometric framework Spoofing attack in Face recognition system.

Keywords: SVM, Viola and jones, Gabor feature, CSLBP.

I. INTRODUCTION

Face recognition frameworks are a part of facial image processing applications. [1] It has been a active research topic in the last two decades and its methods are presently sent in access control frameworks. It is the most common method for biometric distinguishing proof and has the advantage of non intrusiveness over the other biometric strategies, for example, irises and fingerprints. So these frameworks can be utilized for crime counteractive action, video reconnaissance, individual check, and similar security activities. Yet, despite the fact that the biometric frameworks add an extra layer of security than customary techniques by secure identification and authentication, they are still defenseless against assaults. Spoofing attack is common in behavioral traits (voice, signature) but physical traits such as fingerprint face, iris are also susceptible to spoof.

In practice, biometric technologies employ a standard process across different types. A sample of the biological trait is collected using a sensor of some kind, such as a camera for faces or a recorder for voices. Through the use of an algorithm that extracts information from the biometric sample, the trait is then converted into a digital representation called a template, which can be stored in a database.

The larger the database, the more templates there are to verify or identify subjects. The key component is the algorithm used to construct the template; this is the feature that distinguishes a biometric recognition system from (and makes it better or worse than) others. *Visual biometric* system analysis the facial features or patterns for the authentication or recognition of an individual’s identity. There are many pros in using biometrics for Big Data security, the first of which is the elimination of unauthorized access.

Big data system is characterised by Volume, variety, veracity and a velocity. Volume parameter is referred to an extremely large quantity of enrolment and verification data in some modern biometrics systems. In turn, you are making better decisions when it comes to acquiring, retaining, growing and managing those customer relationships. The term velocity refers to the speed at which data arrives. This becomes an important concern when large civilian and enterprise systems such as online face detection,[6] recognition, surveillance camera image on fly analysis use of face recognition for authentication for all of their daily transaction. Face snooping detection is an important parameter in biometric systems which concerned to the parameter veracity. Face recognition algorithm have been constructed to operate on a wide variety of data types such as 2D-gray scale images, colour images, different poses, different intensities, in addition fusion of different modalities.

II. RELATED WORK

Motivated by picture quality evaluation, portrayal of printing artifacts, and contrasts in light reflection, we propose to approach the issue of spoofing detection from texture analysis point of view. In reality, face prints more often contain printing quality deformities that can be very much identified utilizing texture features. Consequently, [2] Jukka present a novel methodology taking into account investigating facial image texture for distinguishing whether there is a live individual in front of the camera or a face print. The proposed approach breaks down the composition of the facial pictures utilizing multi-scale nearby parallel examples (LBP). Contrasted with numerous past works, our proposed methodology is robust, computationally quick and does not require user collaboration. Moreover, the texture feature that are utilized for spoofing detection can likewise be utilized for face acknowledgment. This gives a special component space for coupling parodying identification and face acknowledgment.

Neslihan Kose[3] proposed another new face anti-spoofing approach, which depends on examination of contrast and texture characteristics of caught and recaptured pictures, is proposed to identify photo spoofing. Since photograph picture is a recaptured picture, it might indicate very diverse in contrast and texture characteristic when contrasted with a genuine face picture. In a spoofing image, picture rotation is very common. so, in this paper, a rotation invariant local binary pattern variance (LBPV) based strategy is chosen to be utilized. The methodology is tested on the freely accessible NUAA photograph impostor database, which is built under brightening. The outcomes demonstrate that the methodology is aggressive with other existing techniques tried on the same database. It is particularly helpful for conditions when photographs are held by hand to spoof the framework.

In this work, Allan [4] introduce an answer for video-based face spoofing to biometric frameworks. To catch the nose and get a minimized representation, we utilize the Fourier range took after by the calculation of the visual rhythm and extraction of the gray level co-occurrence matrices, utilized as highlight descriptors. Results demonstrate the viability of the proposed way to deal with recognize genuine and fake clients.

Samarth Bharadwaj [5] presents another methodology for spoofing recognition in face recordings utilizing movement magnification. Eulerian motion magnification methodology is utilized to upgrade the facial appearances Next, two sorts of highlight extraction calculations are proposed: (i) a design of LBP that gives enhanced execution compared with other methods (ii) motion estimation approach utilizing HOOF descriptor. Particularly HOOF descriptor yielding a close flawless half aggregate blunder rate of 0% and 1.25% individually.

III. PROPOSED SYSTEM

To make face recognition as a successful biometric innovation, it is need to solve the spoofing assault issue. In this manner to overcome spoofing issues, a strategy that can be utilized for accepting whether the information is really from a genuine user or not. Our proposed system gives a strong guarantee for high performance rate.

In our approach, we divide the work in 2 phases. In the first phase, that is training phase read the image from the database folder as per the query image. Perform image pre-processing methods on the image. Using viola and Jones face detection is achieved. And then features of the image will be extracted followed by feature selection. Save those trained images in the database. In testing phase images are taken as input and pre-processed. After pre-processing a features are extracted. These features are matched with knowledge base for classification using SVM Classifier.

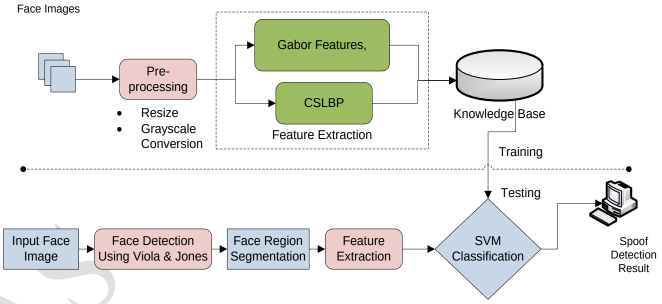

Figure 1: Architecture of Proposed System

A. GABOR FEATURE

The Gabor filter is generally utilized as a part of the image features. The Gabor filter wavelet is the type of sine wave adjusted by the Gaussian coefficient. The Gabor filter is helpful for extracting local and global data. The Gabor filter are tunable band pass channel, multiscale and multi resolution filter [5].

The Gabor filter eq. (1) is utilized as a part of texture segmentation, image representation. It offers ideal resolution in space and time domain. It gives better visual representation in the involved composition pictures. Be that as it may, the current gabor parameter requires additional time utilization for feature extraction. The Gabor filter works on the frequency, orientation and Gaussian kernel.

$$\text{Gabor}(x, y, \theta, \varphi) = X.Y \qquad (1)$$

$$X = \exp\left(-(x^2 + y^2) \div \sigma^2\right) \qquad (2)$$

$$Y = \exp\left(2\pi\theta(x\cos\theta + y\sin\theta)\right) \qquad (3)$$

The terms x and y (eq. 2 and eq. 3) is the position of the filter relative to the input signal [5]. The angular representation of the filter is represented as ‘θ’. The angular orientation of the filter is represented as ‘∅’.

B. CSLBP

Instead of comparing each pixel with the center pixel, we compare center-symmetric pairs of pixels as illustrated in Fig. 1. This halves the number of comparisons for the same number of neighbours. We can see that for 8 neighbours, LBP produces 256 different binary patterns, whereas for CS-LBP this number is only 16. (Equation 4 and 5) Furthermore, robustness on flat image regions is obtained by thresholding the gray level differences with a small value T.

$$\mathrm{CS}-\mathrm{LBP}_{R,N,T}(x,y)=\sum_{i=0}^{\left(\frac{N}{2}\right)-1} S(n_i - n_i + (N/2)2^i) \qquad (4)$$

$$S(x) = \begin{cases} 1 & x > T \\ 0 & otherwise \end{cases} \qquad (5)$$

where n_i and $n_i + (N/2)$ correspond to the gray values of center-symmetric pairs of pixels of N equally spaced pixels on a circle of radius R. The value of the threshold T is 1% of the pixel value range in our experiments. Since the region data lies between 0 and 1, T is set to 0.01. The radius is set to 2 and the size of the neighborhood is 8.which gave the best overall performance for the given test data. It should be noted that the gain of CS-LBP over LBP is not only due to the dimensionality reduction, but also to the fact that the CS-LBP captures better the gradient information than the basic LBP.

C. VIOLA AND JONES

The basic principle of the Viola-Jones algorithm is to scan a sub-window capable of detecting faces across a given input image. Viola-Jones rescale the detector instead of the input image and run the detector many times through the image – each time with a different size. At first one might suspect both approaches to be equally time consuming, but Viola-Jones have devised a scale invariant detector that requires the same number of calculations whatever the size. This detector is constructed using a so-called integral image and some simple rectangular features reminiscent of Haar wavelets.

The first step of the Viola-Jones face detection algorithm is to turn the input image into an integral image. This is done by making each pixel equal to the entire sum of all pixels above and to the left of the concerned pixel. This allows for the calculation of the sum of all pixels inside any given rectangle using only four values. These values are the pixels in the integral image that coincide with the corners of the rectangle in the input image. The Viola-Jones face detector analyzes a given sub-window using features consisting of two or more rectangles. The different types of features are shown in Figure 2.

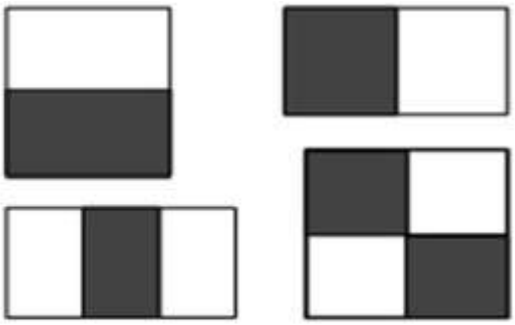

Figure 2: Different Haar Features

D. SVM CLASSIFIER

SVM is suitable to characterize the Color and shape includes precisely and effectively. [8] It is superintend learning process which break down and perceive examples, for example, surface, color, shape and it is utilized for classification and regression methods. The grouping is associated by hyper plane which has outsized separation to nearest separation training data of any class (shading, surface, shape). In this manner the perception is bigger the margin, bring down the generalization error of classifier. The arrangement isolates information into preparing tests and testing tests. The goal of SVM is to foresee the objective estimations of test information by giving just the test information qualities.

II. RESULT AND DISCUSSION

Below Figure 3 is input spoof image which is preprocessed and face is detected using viola and jones algorithm. When image (figure 3) whose features are extracted and stored in a knowledge base. SVM classifier identifies query image is spoof detected or not.

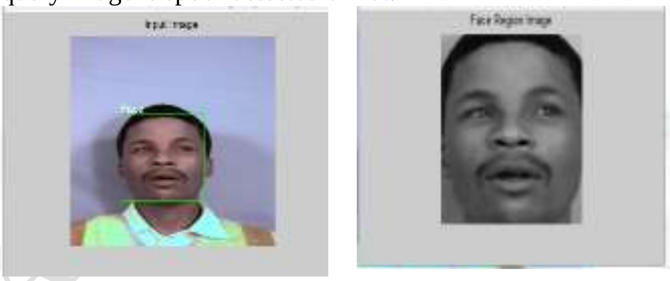

Figure 3: Input spoof image and Face detected Output.

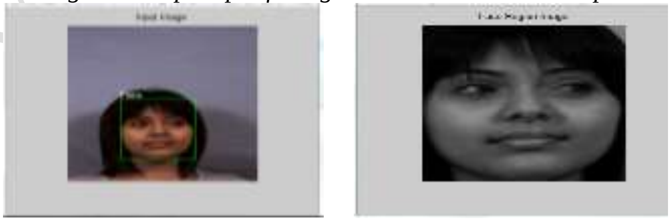

Figure 4: Original input image and face detected Output

III. CONCLUSION

In this paper, we address the problem of face spoof detection, for particular database. While most of the published methods use proposed approach performs better than the state-of-the-art methods in database motion or texture based features, we propose to perform face spoof detection based on CSLBP and Gabor feature. An ensemble classifier consisting of two constituent SVM classifiers trained for different spoof attacks is used for the classification of genuine and spoof faces.

REFERENCES

[1] S.Hemalatha, Amitabh Wahi, "A Study of Liveness Detection in Face Biometric Systems" International Journal of Computer Applications (0975 – 8887) Volume 91 – No 1, April 2014.

[2] Jukka M¨a¨att¨a, Abdenour Hadid, Matti Pietik¨ainenMachine Vision Group, University of Oulu, Finland Face Spoofing Detection From Single Images Using Micro-Texture Analysis.

[3] Neslihan Kose, Jean-Luc Dugelay “Classification of Captured and Recaptured Images to Detect Photograph Spoofing” Multi Media Department, EURECOM 2229, France.

[4] Allan da Silva Pinto1, Helio Pedrini1, William Robson Schwartz2, Anderson Rocha” Video-Based Face Spoofing Detection through Visual Rhythm Analysis”.

[5] Samarth Bharadwaj, Tejas I. Dhamecha, Mayank Vatsa and Richa Singh,” Computationally Efficient Face Spoofing Detection with Motion Magnification” IIIT-Delhi, India.

[6] Hanane. Rami, Mohammed. Hamri, Lhoucine. Masmoudi.” Objects Tracking in Images Sequence Using Center-Symmetric Local Binary Pattern (CS-LBP)”, International Journal of Computer Applications Technology and Research Volume 2– Issue 5, 504 - 508, 2013, ISSN: 2319–8656.