International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Face Spoofing Detection based on Texture Analysis and Color Space Conversion

Irshad PP[1], Vinila Jinny S[2]

[1]*PG Scholar, CSE Department, Noorul Islam Centre for Higher Education, Kumaracoil, TamilNadu, India*
[2]*Associate Professor, CSE Department, Noorul Islam Centre for Higher Education, Kumaracoil, TamilNadu, India*

Abstract - *Biometrics offers a powerful solution to authentication purposes. Biometrics refers to the identity of an individual. In biometrics, Face is widely used in identification of individual's identity. Biometric recognition is leading technology for identification and security systems. Face has unique identification among all other biometric modalities. Face spoofing detection attributes to the investigation of the facial characteristics to ensure whether the face is spoofed or live. This paper introduces a novel and appealing approach for detecting face spoofing using a colour texture analysis. This work is simulated using MATLab.*

Key Words: **Biometrics, Spoofing, Texture, Color space, SVM**

1. INTRODUCTION

Biometric applications are increasing day by day and it is more secure than any other username, password etc. Fingerprint, face, and iris are the biometric traits most frequently used in present authentication systems. Biometrics may use physical or behavioural characteristics for identification purposes. Face is the important biometric as its natural, ease to use and non-intrusiveness. A biometric authentication is realized in two steps: the enrolment and the verification phases. The first one consists in generating the biometric reference template of one user and to store it for further comparison. During verification, a query biometric template is compared to the reference one for decision .Face is more popular as it doesn't require any additional hardware and almost all mobile phones are equipped with front facing camera. However, the problem of spoofing attacks can challenge face biometric systems in practical applications. Spoofing attacks can easily launch by photo attacks, video replays and 3 D masks of the face. Recent advancements such as plastic surgery, 3D face mask and easily availability of images and videos in the social network help the attackers to spoof the system. Though several face spoofing detection techniques have been proposed, the issue is still unsolved due to sensitive constraints and limitations.

1.1 Face Spoofing Attacks

Spoofing attack occurs when attackers submit fake evidence to the biometric system to gain evidence. Face spoofing detection is used to identify an attacker try to masquerade himself /herself as genuine user in facial recognition systems. Face Spoofing can be categorized in to two: 2 D and 3D face Spoofing. 2 D face spoofing could be printed photo attack and reply attack .3 D face spoofing could be 3 D mask attack and plastic surgery.

1.2 Face Spoofing Detection

Face spoofing detection module is a countermeasure of face spoofing. The purpose of face spoofing detection module is to prevent the users from illegal access of face recognition systems. Most of the FR system doesn't include this module or it doesn't function effectively.

2. Literature Survey

Texture based face anti-spoofing has been widely adopted in face anti-spoofing research. Texture analysis techniques mainly compare the texture pattern of the face which is captured by the sensor in the system with the texture pattern of the real face which is present in the database. These techniques take the advantage of detectable texture patterns such as print failures, and overall image blur to detect attacks. Texture analysis based approach is easy to implement and it does not need user cooperation.

Boulkenafet described face spoofing detection based on colour texture analysis. In this approach authors used the joint colour texture information between luminance and chrominance channels. This technique was performed on Replay attack database, CASIA FASD database and MSU mobile Face Spoof Database and technique showed an improvement in generalization ability.

De souza proposed a face spoofing detection based on modified CNN with LBP which presented great results on NUAA dataset. These method make use of deep texture features for face spoofing. This technique integrates LBP with CNN in its first layer in order to extract deep texture features. The experiment was performed on NUAA dataset. The main advantage of this approach is accuracy

Anjos presented a detection technique based on foreground/background motion correlation using optical flow. It tries to detect motion correlations between the head of the user trying to authenticate and the background of the scene. This technique uses a video as input and converts the input video to gray scale, and then optical flow is computed. All experiments are conducted on Photo-Attack Database.

Arashloo proposed improved dynamic texture based to promote the detection performance, such as binarized statistical image features on three orthogonal planes (BSIF-TOP), local phase quantization on three orthogonal planes

(MLPQ-TOP)and local derivative pattern from three orthogonal planes (LDP-TOP) . Spatiotemporal analysis can explore the information of the whole video sequence, but the computational complexity is high.

A novel and appealing approach for detecting face spoofing using a colour texture analysis was proposed. This method exploited the joint colour texture information from the luminance and the chrominance channels by extracting complementary low-level feature descriptions from different colour spaces. More specifically, the feature histograms are computed over each image band separately. Extensive experiments on the three most challenging benchmark data sets, namely, the CASIA face anti-spoofing database, the replay-attack database, and the MSU mobile face spoof database, showed excellent results compared with the state of the art. This method is able to achieve stable performance across all the three benchmark data sets. The facial colour texture representation is more stable in unknown conditions compared with its gray-scale counterparts.

2. Proposed System

The proposed system uses a color texture analysis based face anti – spoofing. Face spoofing attacks are most likely performed by displaying the targeted faces using prints, video displays or masks to the input sensor. The most crude attack attempts performed, e.g. using small mobile phone displays or prints with strong artifacts, can be detected by analysing the texture and the quality of the captured gray-scale face images. It is reasonable to assume that fake faces of higher quality are harder or nearly impossible to detect using only luminance information of webcam-quality images. This system uses two phases the testing phase and the training phase. The features used are the texture and quality based features. Texture based descriptors are HOG that deal with shape information, mLBP, deals with local information and Gabour Wavelet to enhance the texture Representation . The quality method extracting image quality features to find the difference between real and fake faces. Distortion features can capture the quality differences between the different reflection properties of different materials. Quality features are color distortion, colour diversity, specular reflection and blurriness. Fig -1 portraits the system architecture.

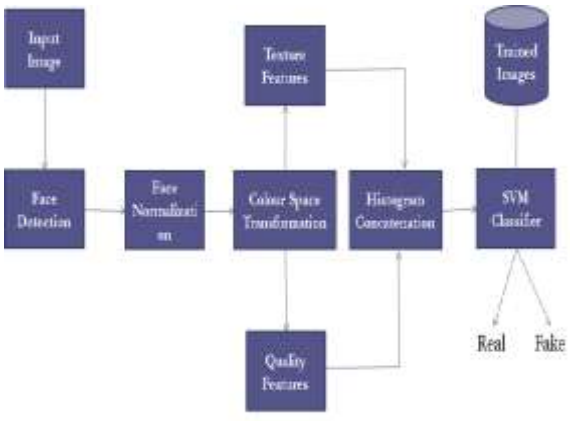

Fig -1: Architecture of the proposed system

2.1. Face Detection

Face detection can be regarded as a specific case of object-class detection. In object-class detection, the task is to find the locations and sizes of all objects in an image that belong to a given class. A reliable face-detection approach based on the genetic algorithm and the eigen-face technique. Firstly, the possible human eye regions are detected by testing all the valley regions in the gray-level image. Then the genetic algorithm is used to generate all the possible face regions which include the eyebrows, the iris, the nostril and the mouth corners.

Each possible face candidate is normalized to reduce both the lightning effect, which is caused by uneven illumination; and the shirring effect, which is due to head movement. The fitness value of each candidate is measured based on its projection on the eigen-faces. After a number of iterations, all the face candidates with a high fitness value are selected for further verification. At this stage, the face symmetry is measured and the existence of the different facial features is verified for each face candidate.

2.2. Face Normalization

An individual's identity, however, is captured by these small variations alone and is not specified by the variance due to the large rigid body motion and illumination of the face. Thus, it is necessary to compensate or normalize a face for position and illumination so that the variance due to these is minimized. Consequently, the small variations in the image due to identity, muscle actuation and so on will become the dominant source of intensity variance in an image and can thus be analyzed for recognition purposes.

2.3. Color-Space Transformation

A color space transformation matrix calculating system is provided that optimizes a color space transformation matrix. The matrix is obtained as a product of a first and a second matrix and transforms colors in a first color space to colors in a second color space. The system comprises first and second optimizers that calculate elements of the first matrix and second matrix by multiple linear regression analysis. The input colors which correspond to color patches and hue corrected colors obtained by using the first matrix and the input colors are set as explanatory variables. First and second goal colors respectively relating to hue and saturation in a second color space, and which correspond to the color patches, are set as criterion variables. The elements of matrices are set as partial regression coefficients.

2.3. SVM Classifier

The invention discloses an SAR image classification method for an SVM classifier by using a hybrid kernel function based on wavelet properties, belonging to the technical field of image processing and mainly solving the problem that effectiveness in image characteristic extraction is not sufficient. The method comprises the following steps: firstly, imputing training and testing sample images, and

normalizing and marking the sample images; secondly, decomposing the normalized sample images, respectively extracting a plurality of characteristics from various decomposed sub-zones, and storing the characteristics in terms of a structural body of T1 x r; thirdly, according to the characteristics of the sub-zones, constructing the hybrid kernel function based on wavelet properties for the SVM classifier (see the formula on the lower right side, wherein, in the formula, Xi and Xj respectively indicate an ith sample image and a jth sample image, i and j are both less than or equal to 1, xik and xjk respectively indicate the kth chacteristics of the first sample image and the second sample, and third is a convex combination coefficient; and fourthly, finishing the classification of the image characteristics by optimizing the convex combination coefficient in the hybrid kernel function. The method has the advantage of high image classification recognition rate and can be used for machine learning and mode identification.

2.4. Texture Features

Spatial features of an object are characterized by its gray level, amplitude and spatial distribution. Amplitude is one of the simplest and most important features of the object. In X-ray images, the amplitude represents the absorption characteristics of the body masses and enables discrimination of bones from tissues. The histogram of an image refers to intensity values of pixels. The histogram shows the number of pixels in an image at each intensity value.

Generally the transformation of an image provides the frequency domain information of the data. The transform features of an image are extracted using zonal filtering. This is also called as feature mask, feature mask being a slit or an aperture. The high frequency components are commonly used for boundary and edge detection. The angular slits can be used for orientation detection. Transform feature extraction is also important when the input data originates in the transform coordinate.

Asner and Heidebrecht (2002) discussed edge detection is one of the most difficult tasks hence it is a fundamental problem in image processing. Edges in images are areas with strong intensity contrast and a jump in intensity from one pixel to the next can create major variation in the picture quality. Edge detection of an image significantly reduces the amount of data and filters out unimportant information, while preserving the important properties of an image. Edges are scale-dependent and an edge may contain other edges, but at a certain scale, an edge still has no width. If the edges in an image are identified accurately, all the objects are located and their basic properties such as area, perimeter and shape can be measured easily. Therefore edges are used for boundary estimation and segmentation in the scene.

3. Results and Discussion

3.1. Image Preprocessing

The input images are taken from video recordings. Face images are preprocessed to normalize the illumination. For example, gamma correction, logarithmic transforms histogram equalization few of the methods are used here. Then using invariant features extraction facial features are extracted invariant to illumination variations. For example, edge maps, derivatives of the gray-level, Gabor-like filters and Fisher-face etc are few of the methods applicable here. Then face modelling is done. Illumination variations are mainly due to the 3D shape of human faces under lighting in different directions. There are researchers trying to construct a generative 3D face model that can be used to render face image with different pose and under varying lighting conditions.

3.2. Color Space Conversion

This new color space for face detection is based on the application of colorimetry to television systems. Looking from the analog television systems, such as NTSC or PAL, to the current digital systems, different color spaces (YIQ, YUV and YCbCr) have been proposed for processing luminance and chrominance signals separately. As they are transmission oriented, the chrominance components were chosen trying to minimize the encoding decoding errors, and the biggest differences were selected: (R-Y) and (B-Y). Here, a novel color space, YCgCr, using the smallest color difference (G-Y) instead of (B-Y) is defined exclusively for analysis applications, mainly for face segmentation. Considering the YCbCr color space, a human skin color model can be considered practically independent on the luminance and concentrated in a small region of the Cb-Cr plane. So, the simplest model used for the classification between skin and nonskin pixels is based only in the definition of a chrominance bounding box. Considering only color information, a pixel will be classified as skin if both of its color components are within each of these ranges. So, the technique used for the face segmentation consists of defining maximum and minimum thresholds for each of the two chrominance components (Cb and Cr).

Facial regions need to be manually segmented in an RGB image to determine the above mentioned maximum and minimum decision thresholds for each of the two chrominance components (Cg and Cr). If both color components of a pixel are within the boundary box, it will be classified as a skin pixel. These decision thresholds must be precisely determined, so that all the face pixels are detected and the pixels in the background are excluded from the detection area. Not only human skin color must be taken into account, as the elements on the background can be taken as face pixels. Therefore, the selection of the segmentation decision values will achieve the detection of either nothing or the whole image.

Two other colour spaces are considered, HSV and YCbCr, to explore the colour texture information in addition to RGB. Both of these colour spaces are based on the separation of

the luminance and the chrominance components. In the HSV colour space, hue and saturation dimensions define the chrominance of the image while the value dimension corresponds to the luminance. The YCbCr space separates the RGB components into luminance (Y), chrominance blue (Cb) and chrominance red (Cr). It is worth noting that the representation of chroma components in HSV and YCbCr spaces is different, thus they can provide complementary facial colour texture descriptions for spoofing detection.

3.3. Feature Extraction

The texture features are extracted. Texture descriptors originally designed for grayscale images can be applied on colour images by combining the features extracted from different colour channels. The colour texture of the face images is analysed using five descriptors Local Binary Patterns (LBP). The LBP descriptor proposed by Ojala et al. is a highly discriminative grayscale texture descriptor. For each pixel in an image, a binary code is computed by thresholding a circularly symmetric neighbourhood with the value of the central pixel. The occurrences of the different binary patterns are collected into histogram to represent the image texture information. LBP pattern is defined as uniform if its binary code contains at most two transitions from 0 to 1 or from 1 to 0.

3.4. Classification

The invention discloses an SAR image classification method for an SVM classifier by using a hybrid kernel function based on wavelet properties, belonging to the technical field of image processing and mainly solving the problem that effectiveness in image characteristic extraction is not sufficient. The method comprises the following steps: firstly, imputing training and testing sample images, and normalizing and marking the sample images; secondly, decomposing the normalized sample images, respectively extracting a plurality of characteristics from various decomposed sub-zones, and storing the characteristics in terms of a structural body of T1 x r; thirdly, according to the characteristics of the sub-zones, constructing the hybrid kernel function based on wavelet properties for the SVM classifier (see the formula on the lower right side, wherein, in the formula, Xi and Xj respectively indicate an ith sample image and a jth sample image, i and j are both less than or equal to 1, xik and xjk respectively indicate the kth chacteristics of the first sample image and the second sample, and third is a convex combination coefficient; and fourthly, finishing the classification of the image characteristics by optimizing the convex combination coefficient in the hybrid kernel function. The method has the advantage of high image classification recognition rate and can be used for machine learning and mode identification.

The input data is given into an input space which cannot be separated with a linear hyper plane. So, we map all the points to feature space using specific type of kernel, in order to separate the non-linear data on a linear plane. After separating the points in the feature space we can map the points back to the input space with a curvy hyper plane. The algorithm proposed by Osuna, Freund and Girosi detects faces by exhaustively scanning an image for face-like patterns at many possible scales, by dividing the original image into overlapping sub-images and classifying them using a SVM to determine the appropriate class. Multiple scales are handled by examining windows taken from scaled versions of the original. Before storing the image some pre-processing steps like masking, illumination and histogram equalization are performed. In the masking process unnecessary noise like the background pattern is reduced from the objects of interest. And then histogram equalization is used that manages the distribution of colors in images. The images of class face and class non face are used to train the SVM using the kernel and upper bound margin values. Once a decision surface has been obtained through training, the run-time system is used over images that do not contain faces, and misclassifications are stored so they can be used as negative examples in subsequent training phases. In order to increase the precision of detecting face we can use negative examples for training misclassification class. There are ample non-face images available which can be trained in SVM. Non face images are richer and broader than face images.

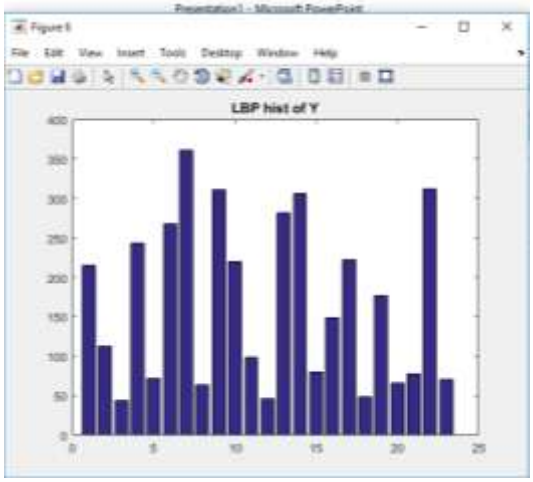

Fig -2: LBP Histogram of Y Component

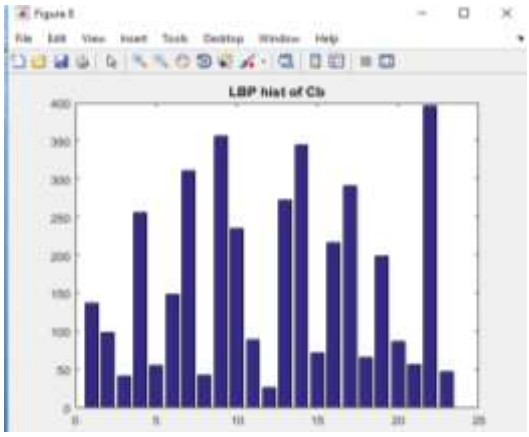

Fig -3: LBP Histogram of Cb Component

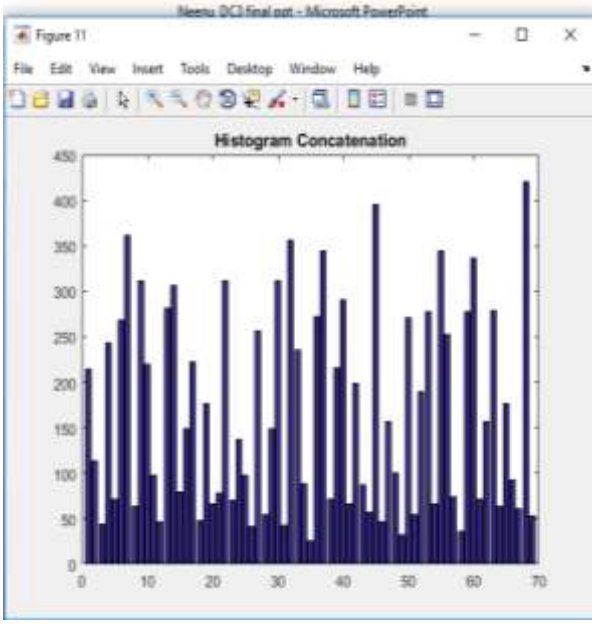

Fig -4: Histogram Concatenation

The simulation is done in MATLab. Fig-2 shows the LBP Histogram of Y Component. Fig-3 shows the LBP Histogram of Cb Component and Fig-4 shows the histogram concatenation.

4. CONCLUSION

Face Recognition systems are vulnerable to spoofing attacks. Photo attacks and video attacks are the most common attack occurs in face recognition systems. This paper describes the overview of existing techniques including various types of face artifacts. Databases and performance metrics used to evaluate the efficiency of these countermeasures were also discussed .Although several methods have been proposed, their generalization ability has not been adequately addressed. So there is a need to design a robust face spoofing detection system which can be generalized well to all the attacks. In this paper we proposed to approach the problem of face anti-spoofing from the color texture analysis point of view. Here the texture features are extracted and the color space conversion is performed using Y component and Cb component and histogram concatenation is done.

REFERENCES

[1] . J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," IEEE Access, vol. 2, pp. 1530–1552, 2014

[2] Sandeep Kumar, Sukhwinder Singh, and Jagdish Kumar, "A Comparative Study on Face Spoofing Attacks", In IEEE International Conference on Computing, Communication and Automation (ICCCA), 5 th -6 th May 2017

[3] Boulkenafet,Z., Komulainen,J .,Hadid,A.:'"Face spoofing detection using colour texture analysis', IEEE Trans. Inf. Forensics Sec., 2016, 11, (8), pp.1818–1830.

[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 Trans. Circuits Syst. II Exp.ress Briefs ,vol.64,issue12,pp 1397 - 1401 ,Dec 2017.

[5] Javier Galbally, Sébastien Marcel Julian Fierrez, "Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition", IEEE Transactions on Image Processing, vol: 23, issue: 2, Feb. 2014,pp710-724.

[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.

[7] A. Anjos, M. M. Chakka, and S. Marcel, "Motion-based counter- measures to photo attacks in face recognition," IET Biometrics, vol.3, no. 3, pp. 147–158, Sep. 2014.

[8] S. R. Arashloo, J. Kittler, and W. Christmas, "Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features," IEEE Trans. Inf. Forensics Security, vol. 10,no. 11, pp. 2396–2407, Nov. 2015.

[9] A. Pinto, W. Robson Schwartz, H. Pedrini, and A. de Rezende Rocha,"Using visual rhythms for detecting video-based facial spoof attacks, "IEEE Trans. Inf. Forensics Security, vol. 10, no. 5, pp. 1025–1038, May 2015.

[10] Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, "Face spoofing detection through visual codebooks of spectral temporal cubes," IEEETransactions on Image Processing, vol. 24, no. 12, pp. 4726–4740, Dec. 2015.