Face Spoof Detection Using Naive Bayes Classifier

Kanika kalihal[1], Jaspreet kaur[2]
[1]*Student, M. Tech, Department of Electronics and Communication, Rayat & Bahra Institute of Engineering & Bio-Technology, Mohali, India*
[2]*Assistant Professor, Department of Electronics and Communication, Rayat & Bahra Institute of Engineering & Bio-Technology, Mohali, India*

***Abstract*- Face recognition systems are widely used in applications ranging from identification to authentication. Certain concerns however are raised along with their popularity such as face spoof attacks where an impostor could use the photo or video of the authorised user and get access to the facilities. This paper proposes a classification based face anti spoof detection technique using HOG and Gabor features. Images are input to the system and feature extraction techniques are implemented. Finally naive bayes classifier is used to classify images on faces 94 database and results are compared with state of art methods.**

Index Terms- Face spoof attacks, Histogram of gradients, Gabor filter

INTRODUCTION

Providing security to a face recognition system is a challenging job. Attackers can easily acquire face images of the authorized person (with digital devices or social media) prints it on the paper, spoof the system and then gain the access. Therefore an efficient face recognition system not only requires good face recognising capabilities but must be able to distinguish genuine images from the fake images.

Many papers have been published recently on face anti spoofing [1-7]. But competition increases with the rapid development in this field [8-10]. Various frameworks for verification system has been designed and compared with state of the art methods. In [11] an algorithm based on image distortion analysis investigates the difference between real and fake images. SVM classifier is trained for face spoof attacks. Individual person specific anti spoofing approach overcomes the challenges of a generic anti spoofing system. A classifier helps in extracting face spoof attacks for each subject [12]

In this framework we have developed a face anti spoof detection system by first extracting discriminative textual features from the test images(Spoof images) and training images(Real images) by using Hog and Gabor feature descriptors And then we have classified the genuine and fake images with the help of simple probabilistic naive bayes classifiers

LITERATURE SURVEY

Significant developments have been made in past few years for treating face spoof attacks. But due to the varying nature of these attacks it is very difficult to develop a universal face anti spoofing technique. Image features helps in enhancing the stability of face spoofing classifier. Fake faces and real faces have different micro textures, spoof images are highlighted by these discriminative features. Texture based technique is used to prevent the system for face spoof attacks. [13]

Spoofing attacks are a major concern for biometric systems, software and hardware based face spoof detection methods have been proposed for reducing the threat of an impostor gaining someone access rights. The biometric traits of enrolled client are stored in the system database. The claimed biometric traits of a person are then verified by comparing it with the stored biometric traits. A matching score is obtained after the verification process which is then compared with the threshold. The systems allows user only when the score is more than the threshold otherwise he/she is rejected and considered as an impostor [14]

Certain details differentiate real images from fake ones, flash is one of them. Flash highlights some details in 3D images which are not present in printed 2D images used by impostors. Local features from the flash images are extracted by Local binary Pattern (LBP). Light intensity varies in the flash images and standard deviation is use to measure intensity.

Method applies SVM classifier to distinguish genuine user from the attackers [15]

Real images behave normally whereas fake images are considered to exhibit abnormal behaviour. Using class modelling anomalies in the data are detected. Data which is labelled as anomaly considered as spoofed and does not belong to the class of real images. Dynamic textual descriptors are used to model temporal and spectral features in the sample images. This paper investigates new samples by extracting anomalies and setting boundaries for the target data. Minimisation approach is employed in SVDD classifier for detecting new samples [16]

Unsupervised domain adaption helps in learning discriminative features from labelled and unlabelled data. In [17] Labelled samples are provided to source domain and unlabelled samples to the target domain. Classifier learns from both of the samples and its results are compared with the supervised domain adaption.

Generally texture, motion and liveliness is used for detecting spoof attack in a biometric system. Texture based methods examines the textural differences between the real and spoof images. Motion based techniques finds the distinctive features in a 3D human face and uses it as cue for detecting the 2d printed spoof attacks. Eye blinking, lip movement and some involuntary body movements are used as a sign to detect liveliness in the image. The proposed method use client based information rather than complex strategies to find the spoof attacks for biometric systems [18]

Due to certain factors partition of feature space become extremely complicated. Xiao, et.al proposed two novel features to reduce complexity in the face recognition system. Template face depth binocular and spatial pyramid micro text feature are used along with a spatial coding algorithm for this purpose. These two features implemented multi model face anti spoofing on widely used dataset and the experiments are compared with the existing methods [19]

Liveliness features from three facets, optical flow based scene motion, shearlet based image quality and optical flow based face motion features are proposed in [20]. All these features employed altogether provide a better image quality feature descriptor. No scenic or motion model is assumed in the proposed work. Higher accuracy is achieved as compared with the state of the art methods.

David Menott et.al [21] proposed a face spoof detection system employing two deep learning models. Architecture optimisation finds the best architecture of convolution neural network and filter optimisation implemented in the proposed work on the other hand learns the filter weights. Both of these optimisation techniques are applied separately as well as together. These approaches are implemented on nine widely available datasets and the results outperform all the existing methods.

PROPOSED WORK

In this work we present a face spoof detection technique in which the spoof attacks by an impostor are detected by naive bayes classification approach. Real Images are fed to the training database and spoofed images are presented to the target database. Features are extracted from the images fed to the training and test database. The extracted features from both datasets help in differentiating real images from the fake images. We have implemented Hog and Gabor feature descriptors to analyse the textual differences in the genuine and fake images. The naive bayes classifier finally applies simple probabilistic approach to classify images.

HOG FEATURES

Hog features helps in calculating local shape features from the region of interest of an image. Hog features basically divides the windows into small regions called cell and then accumulates local gradient orientations over the cell pixels. In the first step of hog feature extraction gradients values are calculated both in the horizontal and the vertical positions. In the second step cell histograms are derived from the orientations and finally normalisation is done. Each cell histograms has certain bins which represent the gradient orientation that should be equally spaced between 0 to 180 or 0 to 360. Each cell histograms are calculated by adding its magnitude values to the corresponding orientation bin, this value is called vote.

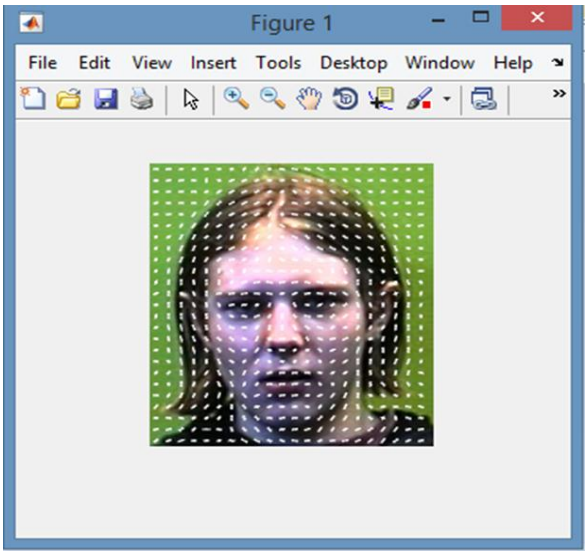

Figure 1 Hog features of a training image

GABOR FEATURE

Gabor transformation is implemented in Gabor feature extraction techniques. In gabor transformation 2D gabor filter is multiplied with the guassian function. Convolution theorem is implemented and filters are convolved with the signal. As textual information in the real and the fake images are different, the output of the gabor filter helps in detecting this dissimilarity.

Mathematically the input image v(x,y) is multiplied/Convolved with the guassian function g(x,y) as represented in the equation 1

$$u(x,y) = \int\int v(\alpha,\beta)g(x-\alpha,y-\beta)d\alpha d\beta$$

Where α and β are integral values and g(x,y) is the guassian function and can be represented as

$G(x,y,\psi,\lambda,\theta,\sigma,\gamma) = \exp(\frac{-x^2+\gamma y^2}{2\sigma^2}) \cos(\frac{x'}{\lambda}2\pi + \psi)$

X'=xcos(θ)+ysin(θ)

Y'=xsin(θ)+ycos(θ)

Where θ – orientation of the gabor function

λ – Wavelength of the sinusoidal function

σ – Standard deviation of Gaussian factor

φ - Phase offset of the gabor function

The parameter θ has real values which range from 0 and λ and phase offset parameter is used to decide the symmetry of the filter.

NAIVE BAYES CLASSIFIER

Naive bayes classifiers are popular in image processing applications this is because they provide simple yet effective methods for image classification. In naive bayes model each attribute is independent of each other and every one of them contributes for the final decision. This classifier is based on Bayesian a network which is a probabilistic model. When the input data is provided to the classifier which are the extracted features of the real and the spoofed images, the classifier created the probabilistic values for each data sequence and compared them to obtain the classified result.

The classified algorithm obtained results in two categories real of fake. The probability of data is obtained using the standard bayessian equation:

$$P(H|E) = \frac{P(E|H)}{P(E)} P(H)$$

FEATURE EXTRACTION

The proposed scheme has been represented in the figure 2 and its corresponding steps are described below:

1. Real images are fed to the training database for training classifier and spoofed images are fed to the test database.
2. Mean of all images are calculated and the images are subtracted from it one by one.
3. To take the average of both hog and Gabor feature extraction schemes eigen values are calculated.
4. The features extracted from the train images and test images are then classified with the help of naive bayes classifier.
5. And finally classifier obtains the results in two categories genuine or fake.

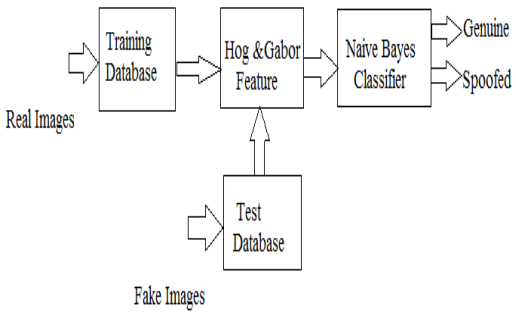

Fig 2 Flow Diagram of Proposed Scheme

RESULTS AND DISCUSSIONS

In this section image database and results are discussed, the experiments are conducted on faces 94 database and the coding is done in Matlab. In the proposed work total half rate, accuracy, false acceptance rate and execution time is calculated and compared with state of art. Out of the most prominent techniques of face spoof detection such as Mutiscale local binary patterns, dynamic local ternary patterns and LBPnet our systems achieves highest HTER and outperforms other schemes except LBP net and n-LBP net in terms of accuracy.

Method	EER	AUC	Acc	HTER	FAR	FRR
Hog,Gabor +Naive	0.2611	0.971	0.973	0.016	0.0182	0.0176
MLBP	-	0.990	0.98	0.025	0.006	0.044
DLTP	-	0.952	0.945	0.035	0.032	0.038
LBPnet	0.021	0.0993	0.976	0.022	0.028	0.016
n-LBPnet	0.018	0.996	0.982	0.017	0.019	0.015
LBP+SVM	0.029	-	-	0.0132	-	-
NUAA best	-	0.950	0.977	-	-	-
LLD	-	0.96	-	-	-	-

An additional parameter called execution time is also calculated that comes out to be 0.00327 seconds in our research work.

CONCLUSIONS AND DISCUSSIONS

The proposed work is concerned with the recent face spoof attacks experienced by people all over the world. The face spoof detection schemes implemented here utilizes the feature extraction schemes to detect the fake images. The results are compared with the recent face spoof detection techniques and the conventional ones.

Hog and gabor feature extraction schemes are introduced in the work along with naive bayes classifier. Parameters such as half total error rate, accuracy are calculated and compared with the existing methods. We have finally found that our system outperforms other systems in terms of HTER and therefore give better results.

REFERENCES

[1] A. Rocha, W. Scheirer, T. Boult, and S. Goldenstein, "Vision of the unseen: Current trends and challenges in digital image and video forensics," ACM vol. 43, no. 4, pp. 26:1–26:42, Oct. 2011.

[2] 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.

[3] Z. Boulkenafet, J. Komulainen, and A. Hadid, ''Face spoofing detection using colour texture analysis,''IEEETrans.Inf.ForensicsSecurity,vol.11, no. 8, pp. 1818–1830, Aug. 2016.

[4] W. Schwartz, A. Kembhavi, D. Harwood, and L. Davis, "Human Detection Using Partial Least Squares Analysis," in IEEE Conference on Computer Vision, 2009.

[5] Pan G, Sun L, Wu Z, et al., 2007. Eyeblink-based AntiSpoofing in Face Recognition from a Generic Webcamera, IEEE, International Conference on Computer Vision.

[6] Galbally J, Marcel S, Fierrez J. "Image Quality Assessment for Fake Biometric Detection". IEEE Transactions on Image Processing 2014. IEEE vol 24 2002

[7] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE 2002

[8] R.Raghavendra, K.B.Raja, andC.Busch, "Presentation attack detection for face recognition using light field camera," IEEE TransactionsonImageProcessing,vol.24,no.3,pp.1060–1075, 2015.

[9] A. Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, "Video-based face spoofing detection through visual rhythm analysis," in Conference on Graphics, Patterns and Images, Ouro Preto, MG, Brazil, august 2012, pp. 221–228.

[10] C. Riess, "Illumination analysis in physics-based image forensics: A joint discussion of illumination direction and colour," Computer and information science vol 766, 2017.

[11] Di Wen et.al "Face Spoof Detection with Image Distortion Analysis". IEEE Transactions on Information Forensics and Security, 2015

[12] Jianwei Yang et.al "Person-Specific Face Antispoofing With Subject Domain Adaptation" IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, April 2015.
[13] Hoai, et.al "Face Spoofing Attack Detection Based on the Behavior of Noises", 2016, IEEE
[14] Allan Pinto, Helio Pedrini, William Robson Schwartz and Anderson Rocha, "Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes" IEEE Transactions ON Image Processing. Volume 24,No 12,PP 4726-4740, December 2015
[15] Patrick P. K. Chan, Weiwen Liu, Danni Chen, Daniel S. Yeung, Fei Zhang, Xizhao Wang, and Chien-Chang Hsu, "Face Liveness Detection Using a Flash Against 2D Spoofing Attack" 2017 IEEE Transactions on Information Forensics and Security.
[16] Shervin Rahimzadeh Arashloo, Josef Kittler and William Christmas, "An Anomaly Detection Approach to Face Spoofing Detection: A New Formulation and Evaluation Protocol" IEEE Translations and content mining 2017
[17] Haoliang Li, Wen Li Hong Cao Shiqi Wang, "Unsupervised Domain Adaptation for Face Anti-Spoofing". IEEE Transactions on Information Forensics and Security 2018.
[18] Ivana Chingovska and André Rabello dos Anjos, "On the Use of Client Identity Information for Face Antispoofing". IEEE Transactions on Information Forensics and Security. Volume 10, Issue No 4 , PP 787-796 April 2015
[19] Xiao Song, Xu Zhao, Tianwei Lin, "Face Spoofing Detection by Fusing Binocular Depth and Spatial pyramid coding Micro-Texture Features", IEEE 2017
[20] Litong Feng, et. al, "Integration of image quality and motion cues for face anti-spoofing" ElsevierApril 2016.
[21] David Menott William Robson Schwartz, Alexandre Xavier Falc˜ao, "Deep Representations for Iris, Face, and Fingerprint Spoofing Detection" 2014 IEEE Transactions on Information Forensics and Security