ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 3, March 2016

Modified Boosting Algorithm For Face Liveness Detection Using Diffusion Speed Values

D.Thamarai Selvi
Research scholor, Dep. Of ECE
IFET College of Engineering
Villupuran, India

K.Sureshkumar
Assistant Proffessor, Dep. Of ECE
IFET College of Engineering
Villupuram, India

***Abstract*- In today's world there is an increasing need for high level security for devices like mobile , laptops ,etc,. There are various kinds of spoofing attacks like usage fake finger prints and faces to access secured devices. This propose method is a real time application to discriminate between fake and real face depending on diffusion speed values. Modified boosting algorithm is one of the best classifier that make this application suitable for various illumination and environmental conditions. Main advantage is removing noise and enhancing the image before comparison . User action is not needed for the discrimination process. So, it can be used in any situation. Experimental results using the proposed method gives more effective outcome for face liveness detection as compared with other previous approaches .**

Keywords: Spoofing, diffusion speed, modified boosting algorithm, face liveness detection.

I. Introduction

A spoofing attack is a situation in which a person or program is used to successfully to forge by falsifying data and and gaining an illegitimate advantage. Existing security systems are fragile to spoofing attacks .Spoofing attacks in image has a radical inclination intending to reassure the authenticity of input images. Recurrently face can be used as a peculiar feature to recognize individuals. Antispoofing detection methods used in the past few decades avail geometric models, but current methods uses more sophisticated models which boomed the recognition technology.

Spoofing detection in images is used mainly for identification and verification purposes. In the former stage the input identity is correlated with the traits that aer stored in the database. The obtained output is then compared with a score which is then relate to a decision threshold by pointing the score in an appropriate classifier. If the score is above the decision threshold the input can be evaluated as a live face otherwise a fake one. Fingerprint and iris recognition systems are actively researched and deployed in various security systems [1], [2]. Usually printed photos, masks or screenshots are used by the imposter for the fraudulent attempts.

To address the problems in image spoofing detection, this novel proposed idea is based on diffusion technique here the antispoofing features can be estimated by calculating the diffusion speed and total variation flow. The features are then fed as input into an appropriate classifier to obtain a decision

Fig.1 Spoofing image

. The main objective of this paper is elucidated below,

(a) To identify the spoofing attacks in images
(b) Also propose an efficient diffusion technique for the face liveness detection.

Most of the current methods face recognition has used the image matching part of the system without considering whether the matched face is a live human face or not [3]. Based on the kinds of biometric notions used the antispoofing detection of a valid user can be categorized. The most commonly used technique is the motion based counter measures to the photo attacks in face recognition [4]. This method solely based on foreground/background motion of the pixel correlation using optical flow. In this method direction of motion of every pixel is formulated. In component based face recognition method [5] consists of four steps; (1) components of face considered is located; (2) low-level features of the located components is coded ; (3) codes is represented with weights derived from Fisher criterion; (4) histogram is drawn for the located components. Micro difference between live face and fake face can be effectively correlated in this method. Here not only the canonical regions, but also the informative regions are considered for the face discrimination.

Spoofing can be detected from Single Images using Micro texture Analysis [6], the face images are analyzed using Local Binary Patterns. The proposed method then uses the micro texture patterns as the input and is feed into an enhanced feature histogram. The results obtained are fed into an appropriate classifier which determines the liveness of the subject. In Masked Fake Face Detection using Radiance Measurements [7] method; creating a 2D feature space from the input images.

Reflectance disparity of the images are computed. The radiance measured is used along with the feature vector obtained from the forehead region of the face. The main idea is that the skin and the material of the mask show separate linear distribution .

II. Proposed system

The proposed method uses a single image as the input for face liveness detection . It uses the modified boosting algorithm for the purpose of classification.

A. Face Liveness Detection

The main idea of this proposed method is the significant difference in illumination characteristics. The illumination characteristics of an object is obtained when light falls on it. Depending on the structure of the object the characteristics vary. On a live face because of it is 3D structure the light is quite randomly reflected whereas the light on a 2D fake face is reflected relatively uniform. Hence their illumination characteristics vary and it helps us in discrimination of the faces. This difference in the illumination characteristics effects of input images of live and fake faces. To find the difference in the nature of face we use the concept of diffusion speed along with the modified boosting algorithm. This idea because possible because the light get reflected evenly on a 2d surface and gets reflected unevenly on a 3D surface. So this idea can be used successfully.

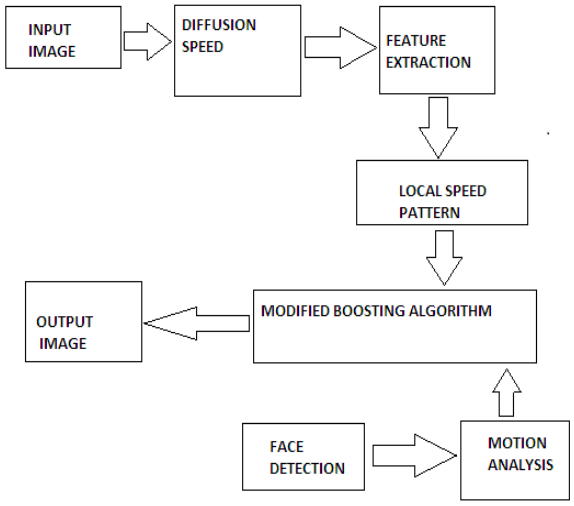

Fig.2 Block Diagram

B. Diffusion Speed

The section aims to estimate the diffusion speed of the face image; so that the illumination characteristics are clearly revealed. For estimating the diffusion speed nonlinear diffusion speed of the original image can be performed which is given in Eq. 1

$$X^{a+1} = X^{a} + \mathrm{div}(d(|\nabla X^{a}|\nabla X^{a}) \rightarrow (1)$$

. The diffusion of an image mainly smooth the textures in an image. A threshold function is set to preserve the edges in an image. Proposing another method called total variation flow which can be defined as in Eq. 2

$$d(\nabla X^{)} = 1/(\nabla X^{a} + \alpha) \quad \text{-}\rightarrow(2)$$

Where α is a positive constant. The rules for estimating the total variation in an image, (I) The pixels in the boundary adapt their value with half that of the speed of diffusion. (II) Movement of small pixels is faster compared to the movement of fast pixels.

C. Feature Extraction

On the basis of the above analysis, antispoofing features are efficiently extracted by utilizing the ability of diffusion speed model. Straightforwardly value of the diffusion speed is used at each pixel position in baseline features, given as in Eq. 3

$$F=\{S(M,N)|0<M\leq a,0<N\leq B \rightarrow (3)$$

Where A and B denote the width and height of the input region considered

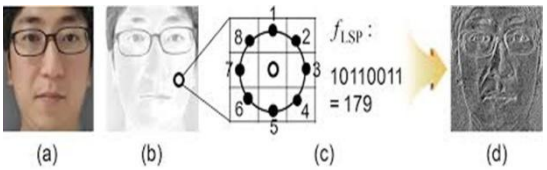

Fig. 3 Feature Extraction of Diffused Image

D. Feature Vector Extraction

The local speed patterns are used to efficiently capture the difference between the nature of live and fake face is given in Eq.5 given below.

$$F_{lsp}(a,b) = \sum_{1\leq u\leq v} 2^{u-1} lsp^{v}(a,b) \quad \text{-}\rightarrow(4)$$

$$F_{lsp} = 1,\ s(a,b)>s(a_i,b_i) \quad \rightarrow(5)$$
$$0, \text{otherwise}$$

where *u* is the number of sampling pixels in the neighborhood The classification methods can classify the input with the help of the already store data. The data in the database are obtained by doing the process with various original images with different background , various gesture, various climatic conditions , etc. All kinds of classifier us this kind of methods for their classification method, but they vary only in performance. The limitation of this existing method can be defined as due to the manual interaction in the training phase, the method is not fully automatic and the results depend on particular choice of the training set.

III. Modified boosting algorithm

Adaptive Boost algorithm is easy to implement and a best out of box classifier. Color and texture are the widely used features that are given as input for classifying objects in indoor scenes. The main reason is because they allow good

discrimination of several image. It is used to reduce the noise, distortion in a given image. The preprocessing time is mainly highly reduced because this algorithm does not need any pre-processing steps and hence the real-time performance can be reached to the higher needed extent. To improve any kind of inputs like photo and videos under different lighting conditions used in attack can be detected. It is a best out of box classifier. Modified Boosting is a particular method of training a boosted classifier.

$F_T(x)=\sum_{t=1}^{T} f_t(x) \rightarrow (6)$

where each f_t is a weak training set learner that takes an input x and returns values that can be used to indicate the class of the object. This week learner helps in the comparison process. Each weak training set learner produces an output, $h(x_i)$. This hypothesis is the output that helps in discriminating the faces.

$h(x_i)=\text{sign}(\sum_{t=1}^{T} \alpha_t h_t(x)) \rightarrow (7)$

IV. Experimental Results

A. Dataset

NUAA database is used in this method. This database consist of three types of images and is used for spoofing detection. The kinds of image present in this data base are webcam images with neutral expression , fake printed images [9] and 64x64 normalized face images. There are about 15 images in the database. The fake images are obtained by printing the face images in the A4 sheet. The webcam images does not contain any expression and gestures. All faces in the data base are detected with the help of Viola-Jones detector and it is normalized to grey scale image. In this method about 3,491 total images are used from the dataset. One of the important factor to be considered is that there should be no overlapping of images in the training set and the test set.

B. Performance Evaluation

The performance of the considered parameter like the diffusion speed values are obtained by conducting the experiments. In this experiment the time step , iteration numbers are varied accordingly in each steps. The image input used in the method is 32x32 pixel and the feature vector extracted from the corresponding images 531 , 2891 for the considered NUAA dataset. These features are then given as input to the classifier. The fixed threshold value considered for the evaluation is c=100. This value is found to provide good performance for the training set. Hence the discrimination of live face from a fake face using the proposed method is found to give high accurate results.

Table 1

Method	**Accuracy**
LTv	68.44
Proposed	98

The evaluation phase consists of different phases. They are

- Read the input face Image.
- Preprocessing face.
- Performing Non Linear Diffusion for the processed Image.
- Computing Diffusion Speed and Total Variation Flow.
- Obtain Local Speed patterns.
- Generate Feature Vector from the Local Speed Patterns.
- Concatenate Feature Vectors into a histogram.
- The histograms are fed into an appropriate Classifier.

Fig. 4 Top faces detected as fake, bottom face detected as live

V. Conclusions

A simple and easy method to discriminate between a fake face and a real face has been proposed. The main ides of this proposed method is the removal of the unwanted noise and features in the image taken at the first time. By doing so before the comparison we can achieve a high accuracy of detection of face. This method provides a easy and simple method of high level security **.** This method is suitable for both the indoor environment and outdoor environment. It is also suitable for all kinds of illumination and lightings conditions. This method process all the sides of the object placed before the camera. So the various spoofing attacks using technologies can be easily detected and thus it provides an easy way of providing high level security for devices. It can be used as a real time application in devices like mobiles, laptops ,etc,. Thus this proposed liveness detection method provides a better high level of security to the devices,

References

[1] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, “Filterbank-based fingerprint matching,” IEEE Trans. Image Process., vol. 9, no. 5, pp. 846–859, May 2000.

[2] Y. Wang, J. Hu, and D. Phillips, “A fingerprint orientation model based on 2D Fourier expansion (FOMFE) and its application to singular-point detection and fingerprint indexing,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 573–585, Apr. 2007.

[3] G. Pan, L. Sun, Z. Wu, and S. Lao, “Eyeblink-based anti-spoofing in face recognition from a generic webcamera,” in Proc. IEEE 11th Int. Conf. Comput. Vis. (ICCV), Oct. 2007, pp. 1–8.

[4] L. Sun, G. Pan, Z. Wu, and S. Lao, "Blinking-based live face detection using conditional random fields," in Proc. Adv. Biometrics, Oct. 2007, pp. 252–260.

[5] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in 'liveness' assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558, Sep. 2007.

[6] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in Proc. IEEE Int. Joint Conf. Biometrics (IJCB), Oct. 2011, pp. 1–7.

[7] Y. Kim, J. Na, S. Yoon, and J. Yi, "Masked fake face detection using radiance measurements," J. Opt. Soc. Amer. A, vol. 26, no. 4, pp. 760–766, Apr. 2009.

[8] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in Proc. IEEE Int. Conf. Autom. Face Gesture Recognit. (FG), Mar. 2011, pp. 436–441.

[9] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in *Proc. 11th Eur. Conf. Comput. Vis. (ECCV)*, 2010, pp. 504–517.

[9] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in Proc. IEEE 5th IAPR Int. Conf. Biometrics (ICB), Mar./Apr. 2012, pp. 26–31.

[10] B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions," in Proc. 18th IEEE Int. Conf. Image Process. (ICIP), Sep. 2011, pp. 3557–3560.

[11] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proc. IEEE Int. Conf. Biometrics (ICB), Jun. 2013, pp. 1–6.