A Diffusion Speed Model to Detect Face Liveness for a Video Based Anti-Spoofing System

G.Pradeepkumar
Assistant Professor/ECE, Nandha Engineering College, Tamilnadu, India

V.Parameshwari
Assistant Professor/ECE, Nandha Engineering College, Tamilnadu, India

V.Logeswari
Assistant Professor/ECE, Nandha Engineering College, Tamilnadu, India

Abstract – With the increasing demands for high level security in devices and systems several imaging techniques are adopted now days. Along with this threads of video spoofing are also on the rise. Video spoofing detection in security systems is gaining a considerable attention. Image and video spoofing is the common method of attacking verification systems. The proposed approach is based on the diffusion technique, Here the antispoofing features can be accomplished by calculating diffusion speed and total variation flow. Local speed patterns are fed into an appropriate classifier to obtain a decision. The proposed approach does not need any user actions. Preliminary results on datasets shows that proposed approach outperforms the previous approaches mentioned in the literature survey.

Index Terms – List of Keywords that are used in the article should be written. All the keywords should be separated with commas. Minimum of four keywords must be written.

1. INTRODUCTION

A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby 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 video. 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 video is used for identification and verification purposes. In the identification stage the input identity is correlated with the traits that are 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. Usually printed photos, masks or screenshots or playing videos are used by the imposter for the fraudulent attempts. To address the problems in video spoofing detection, this paper proposes a novel idea based on diffusion technique here the anti spoofing features can be estimated by calculating the diffusion speed and total variation flow. The features are fed into an appropriate classifier to obtain a decision. The main objective of this paper is elucidated below, To identify the spoofing attacks in video. Also propose an efficient diffusion technique for the face liveness detection.

In current area of digital world, fanatical enumerations aims to develop smart devices which are automatically identify the persons, depict their actions and react properly. Most of the present biometric security systems rely on accede features from the users, taken from himself/herself and are used for wide variety of applications. If the biometric trait is duplicated or stolen, that creates adverse effects in the security systems. Actually, it is a very challenging task to guard against spoofs based on a static image or video of a face. Most efforts of the current face recognition research has been paid on the image or video matching part of the system without caring whether the matched face is from a live human or not. 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 .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 consists of four steps; (1) locating the components of face; (2) coding the low-level features respectively for all the components; (3) deriving the high-level face representation by pooling the codes with weights derived from Fisher criterion; (4) concatenating the histograms from all components into a classifier for identification. 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.

2.RELATED WORK

A face antispoofing database with diverse attack method, Multiple Difference of Gaussian (DOG) filters are used to extract high frequency information can be treated as a liveness clue. In this method three qualities of the videos are considered mainly low quality, high quality, and normal quality. The baseline algorithm given in Fig. 2 describes the above mentioned technique. In this procedure, Fake face video can be viewed as the genuine face video post processed by the reproduction process. Printing, Imaging or playing videos and displaying process can introduce distortion such as blur and aliasing. Low frequency can be excluded by properly setting Gaussian variance σ.

Face spoofing detection from Single videos using Micro texture Analysis, the face videos are analyzed using Local Binary Patterns. The proposed method encodes the micro texture patterns 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 method; creating a 2D feature space from the input video(video to frame convertion). Reflectance disparity of the images is computed. The Feature vector consists of radiance measurement of forehead region. The main condition for this method is the Facial skin and mask material show linearly separable distribution in feature space.

3.PROPOSED MODELLING

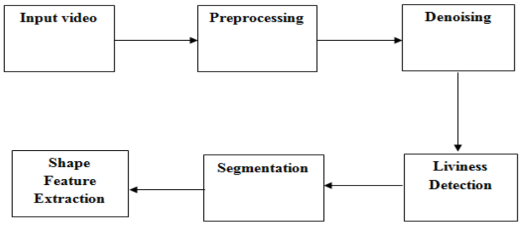


Fig.1 Block diagram of proposed method

3.1. Face Liveness Detection

The hypothesis behind the proposed detection is the significant difference in illumination characteristics. The illumination characteristics on the live face are randomly reflected; but the 2D fake face is relatively uniform. This leads to a difference in the illumination effects of captured video of live and fake faces. In order to estimate this difference in a single vedio, concept of diffusion is proposed. This is because the illumination energies on a 2D surface are evenly distributed and thus are expected to diffuse slowly, whereas those on a live face tend to move faster because of their non-uniformity. Therefore, it is considered that the diffusion speed, e.g., the difference in pixel values between the original and diffused videos, provides useful clues that can be used to discriminate a live faces from a fake one in a single video. In particular, the proposed method attempt to model this diffusion process by allowing for the total variation (TV) flow scheme, and extract anti-spoofing features based on the local patterns of the diffusion speed values computed at each pixel position. Figure2 describe about the illumination characteristics of the input face video.

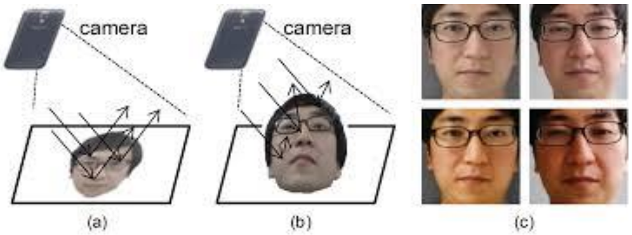


Fig. 2 Illumination Characteristics

3.2 Diffusion Speed

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

$$u^{k+1} = u^k + div\left(d\left({\nabla_u}^k / {\nabla_u}^k \right) \right), \text{u(k=0)=I} \qquad (1)$$

Where K denotes the equation number. The diffusion of an video 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

$$\text{d}(x) = \frac{1}{x+\aleph} \qquad (2)$$

Where $\aleph$ is a positive constant.There are certain rules for estimating the total variation in an image, they areThe two boundary pixel adapt their value with half that speed.Pixels belonging to small region move faster than those belonging to large region.Define the diffusion speed at each pixel position *(x, y)*, which represents the amount of difference on the log space between the diffused video(converting frame) and the original one, given in Eq. 3 given below

Diffusion Speed

$$s(x,y) = |log(u^0(x,y) + 1) - log(u^L(x,y) + 1)| \tag{3}$$

Where $u^0(x,y)$ - Diffused Image, $u^L(x,y)$- Original Image.

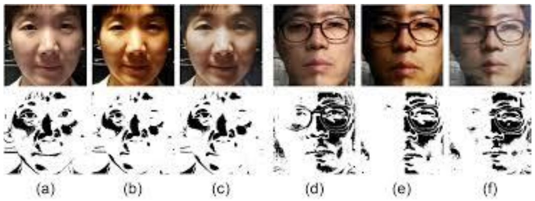


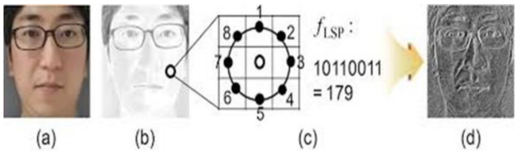
Fig. 3 Diffusion Speed Map

3.3 Feature Extraction

On the basis of the above analysis, antispoofing features are efficiently extracted by utilizing the ability of diffusion speed model. More specifically, straightforwardly employing the value of the diffusion speed itself at each pixel position in baseline features, given as in Eq. 4

$$\mathrm{F_{base}} = \{S(x,y)|0 < x \leq W, 0y \leq H|\} \tag{4}$$

Where W and H denote the width and height of the detected face region respectively.



3.4. Properties of Feature Vector

For each pixel, LSP efficiently encodes not only the illumination characteristics but also the relationships between this information in local regions. The main properties of LSP-based face representation FLSP are summarized as follows.

Focusing on the diffusion speed rather than the diffusion result itself, as in the logarithmic total variation (LTV) model. Based on proposed TV flow-based diffusion speed, which is quite different from the traditional total variation framework used in the LTV model, proposed method can efficiently reveal the difference in the reflectance characteristics according to the 2D plane and3D structure.The LTV model provides only the illumination-invariant face video image, regardless of the liveness of the given face. As compared to the texture patterns widely employed in previous approaches, this LSP-based feature vector captures illumination characteristics on corresponding surfaces. This allows the proposed scheme to be robust to a wide range of spoofing attacks using various media. Moreover, it has a very good ability to discriminate live faces from fake ones, even when the latter are captured in high resolution.Since the diffusion speed model reliably performs under various lighting conditions, the LSP-based feature vector can be applied to images in diverse indoor and outdoor environments.

3.5 Feature Vector Extraction

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

$$f_{LSP(x,y)} = \sum_{1 \leq i \leq n} 2^{i-1} LSP^i(x,y)$$

$$LSP^i(x,y) = \begin{pmatrix} 1 & if\ s(x,y) > s(x_i y_i) \\ 0 & Otherwise \end{pmatrix} \tag{5}$$

where*n* is the number of sampling pixels in the neighborhood of 3 × 3 pixels, $(x_i y_i)$denotes the position of the neighborhood pixels centered at *(x, y)*, where *i* ∈ {1, 2, ・・・, 8}. Thus, the range of $f_{LSP(x,y)}$is [0, 255] and can be represented as a gray-scale image (LSP image).The classification methods can be used to classify the data with data with known labels to partition image feature space. It can be both supervised and unsupervised. Commonly used methods are nearest neighbor and SVM. Nearest neighbor classifier is the simplest classifier is the nearest-neighbor classifier. In this each pixel/voxel is classified in the same class as the training datum with the closest intensity. Generalization of this approach is the *k*-nearest-neighbor (*k*nn) classifier. Pixel/voxel is classified according to the majority vote of the closest training data. *K*nn classifier is considered a nonparametric classifier because it makes no underlying assumption about the statistical structure of the data. Suitable if a large number of training data are available. The limitation of this 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. Support Vector Machines can be defined as the Supervised Learning method which can be used for two or more classification problems, it is more or less based on the concept of decision planes. Decision plane is one that separates b/w a set of items having different class memberships. Use of SVM involves 2 basic steps of training and testing. Basic idea behind SVM is that the optimal hyper plane maximizes the margin between data sets of opposite classes.

4. RESULTS AND DISCUSSIONS

The data set used for the proposed method is NUAA dataset; which is the mostly available bench mark for the evaluation of spoofing detection. This comprises images of 15 subjects who were asked to frontally look at the webcam (capturing faces at 20 fps) with a neutral expression. In addition, none of the faces contains any apparent movement, such as eye blink or head movement. To create fake examples, pictures of each subject are taken using a usual Cannon camera and printed them on photographic paper and normal A4 paper, respectively. All the faces were detected by using a Viola-Jones detector and geometrically normalized based on the eye localizer. Finally, these images were resized to 64 64 pixels with gray-scale representation. Some samples of the NUAA dataset are shown in Figure. For the training set, a total of 3,491 images (live: 1,743 / fake: 1,748) were selected, while the test set was composed of 9,123 images (live: 3,362 / fake: 5,761). It should be noted that there is no overlapping between the training and test sets. NUAA is a widely used database for spoofing detection.

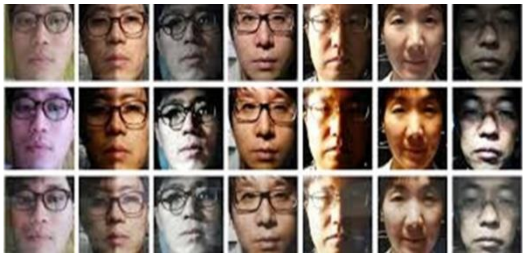
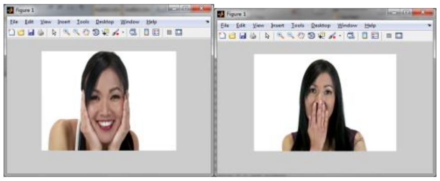


Fig. 4 NUAA Dataset

4.1 Performance Evaluation

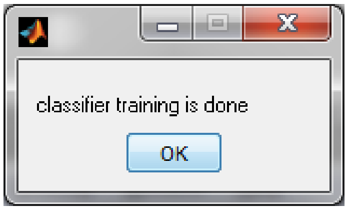
In order to show the performance according to the parameters of our diffusion speed model, we conducted experiments in which the size of the time step and the iteration numbers were varied, as shown in Table I. It should be noted that we use the image block *B* of 32 × 32 pixels in our implementation and thus the dimension of the feature vector is 59 × 9 = 531 and 59 × 49 = 2, 891 for the NUAA datasets. These features are input into the linear SVM classifier [26] for training and testing. In all experiments, we fixed *C* = 100 for SVM, which was shown to give good results when validating the proposed method on a subset of the training set. In Table I, we can see that five iterations are sufficient to yield reliable results in both datasets because of the AOS scheme employed in the proposed method.

4.2Read the input face video.(video to frame conversion)



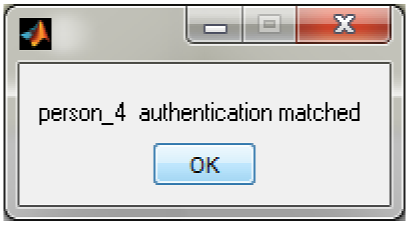
Read the input face video.

4.3Classifier training(comparing training file)



classifier training is done

4.4Testing output(liveness detection)



person_4 authentication matched

The evaluation phase consists of different phases. They are

- Read the input face video.
- Preprocessing face.
- Performing Non Linear Diffusion for the processed video.
- 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.

5. CONCLUSION

The anti-spoofing detection has critical importance in security systems. The pro- posed technique uses diffusion principle which gives higher percentage of detection than existing methods. The proposed method is evaluated using NUAA dataset.At the initial stage performing a nonlinear diffusion of the face video in Matlab. Total variation flow of the image is obtained after adding a positive constant to the diffused video. As a next step Local speed patterns of the video are obtained and feature vectors are generated. At later stages these are fed into a classifier to obtain a decision.A simple and robust method for liveness detection was proposed. The key idea of the proposed method is to adopt diffusion speed for modeling the difference in the illumination characteristics of live and fake faces. Specifically, proposing a technique to exploit the TV flow and then efficiently compute the diffusion speed, which is robust to varying lighting conditions. To capture the difference between live and fake faces more effectively, encoding the local pattern of diffusion speed values, the so-called local speed pattern (LSP).

REFERENCES

[1] 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] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in Proc. IEEE Int. Conf. Image Anal. Signal Process., Apr. 2009, pp. 233–236.

[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, "Faceliveness detection by learning multispectral reflectance distributions," in Proc. IEEE Int. Conf. Autom. Face Gesture Recognit. (FG), Mar. 2011, pp. 436–441.

[9] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," Proc. SPIE, Biometric Technol. Human Identificat., pp. 296–303, Aug. 2004.

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

[11] 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. 11thEur. Conf. Comput. Vis. (ECCV), 2010, pp. 504–517.

[12] 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.

[13] 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.

[14] 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.

[15] P. Perona and J. Malik, "Scale-space and edge detection using anisotropic diffusion," IEEE Trans. Pattern Anal. Mach. Intell., vol. 12, no. 7, pp. 629–639, Jul. 1990.