© 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Face Spoofing Detection from a Single Image using Diffusion Speed Model

K. Sreenivasulu[1], V. Annapurna[2]

[1]JNTUA College of Engineering, Anantapuram, Andhra Pradesh, India

[2] Lecturer, JNTUA College of Engineering, Anantapuram, Andhra Pradesh, India

ABSTRACT

Face spoofing using photographs is one of the most well-known strategies of attacking face recognition and verification frameworks. This paper proposes a spoofing detection method based on the diffusion speed of the input image. The diffusion speed is nothing but the difference of pixel value between original image and diffused image. The implementing method is based on the diffusion speed, and there is no user involvement, and works with a single input image. Diffusion speed is calculated by using total variation (TV) method, and to solve the nonlinear scalar valued equation additive operator (AOS) algorithm is applied. The local speed patterns are calculated from diffused speed image at each pixel position. And these pattern are input into the SVM classifier.

Keywords : Total Variation, SVM, LSP, Additive Operation Splitting, LSP, NUAA

I. INTRODUCTION

In the advanced technology, the systems require high security. In this security systems biometric authentication is the most advanced and highly secure. Fingerprint recognition, hand geometry, retinal and iris scanner are some of the well-known biometric techniques used for security purpose. In these systems accuracy is more but the user need direct contact with the biometric system. But the face recognition system is the alternative method, which gains more popularity in recent times. Face recognition systems are user friendly more convenient when compare to other systems, and therefore every security system adopting face recognition. Though this is more advanced, the face recognition systems facing some spoofing attacks. Spoofing means creation of non-faces, fake face pictures. If the face is spoofed the recognition system may not differentiate the fake face and real face. When the face is spoofed the system bypasses the valid user.

To overcome this problem, the recognition systems must contains the face liveness detection system, it can differentiate live face and fake face. The fallowing figure depicts the overall system of liveness detection.

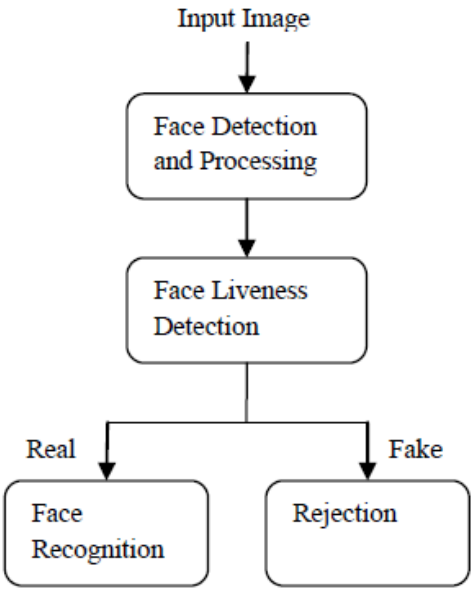

Figure 1 : Face liveness detection

II. Related Work

Several researchers has contributed different techniques to detect the face liveness, based on the textures or motion.

Texture based techniques are relatively easy to use as they work on a single image and does not require anti-spoofing databases. Such techniques aim to differentiate the fake and live using micro texture present in the printed paper.

The physics-based method [1] detects works with a single image recaptured from printed material. When light incident on image surface, some amount of light is reflected off by the surface. This reflection is referred as the specular component of image which is being used for differentiating live and recaptured / fake faces.

Face spoofing detection based on micro-texture analysis [3] detects whether a print image is produced in front of the camera or a live person is present. The key idea behind this approach is that printing quality defects are present in the face prints on paper which can be are easily detected using micro-texture patterns. These approaches have considered a human face as a non-rigid, complex 3D object and a photograph as a 2D planar object. Therefore; there both objects (human faces and photograph prints) reflect light in different ways which result in different specular reflections and shades.

In particular, Tan *et al.* [11] combined texture information with the response of the DoG filter to improve the performance of face liveness detection. Inspired by this work, Peixoto *et al.* [12] applied a similar scheme, defined as a combination of DoG filters and a standard sparse logistic regression model, to bad illumination conditions. Maatta *et al.* [13] attempted to extract micro textures by using the multi scale local binary patterns (LBP), which are frequently treated as a liveness clue.

Above methods are effective when used with a single input image but vulnerable to high resolution-based spoofing attacks using a large display. In order to counter this problem Kim et. al. [11] suggested diffusion based method to differentiate a live and fake face in a single image. The whole idea was based on the fact that the illumination energies diffuse slowly on a uniform 2D surface, whereas these energies move faster on a 3D live face because of its non-uniformity. Diffusion speed is calculated using Local Speed Patterns (LSPs) - local patterns of diffusion speeds and by utilizing the Total Variation flow scheme. The anti-spoofing features are extracted and fed into a linear Support Vector Machine to detect the liveness of the given face input.

III. Methodology

3.1. Motivation:

The implementing process is based on the surface properties of the input image, due to this the illumination characteristics of live and fake faces are significantly different, and these differences are clearly seen in diffusion process. Figure-2 shows illumination characteristics of fake and live face respectively.

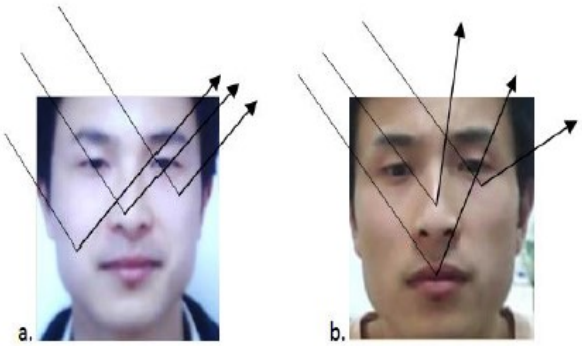

Figure 2 : illumination characteristics fake (a) and live (b) faces

The following figure shows the block diagram of implementing process, firstly computing the diffused image using the AOS (Additive Operation Splitting) algorithm. After that compute the diffusion speed image or delta image is obtained by finding the difference of the original image and diffused image. And extracting the local speed patterns of diffusion speed image at each pixel position. Extracted features are fed to Support Vector Machine to classify whether input image is live image or fake image.

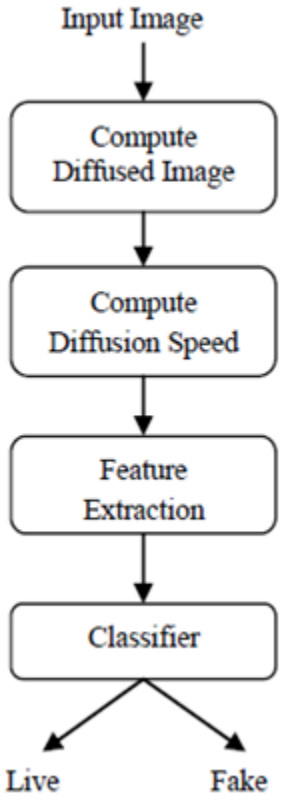

Figure 3 : over all process of implementing system

3.2. Computing diffusion speed:

Firstly, compute the diffusion image, for the input image (I), by using the nonlinear diffusion equation as follows.

$$u^{k+1} = u^k + div(d(|\nabla u^k|\nabla u^k), u(k=0) = I \quad (1)$$

Where k denotes the number of iterations

The additive operation splitting algorithm is used to solve above equation, it is defined in the equation (2),

$$u^{k+1} = \frac{1}{2}((I - 2\tau A_x(u^k))^{-1} + (I - 2\tau A_y(u^k))^{-1})u^k \quad (2)$$

3.3. Computing diffusion speed image:

It represents the amount of difference between original image and diffused image at each pixel position of *I(x, y),* it is applied on the log scale as shown in the equation (3),

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

Where L denotes the number of iteration for which the diffused image is calculated.

3.4. Feature Extraction:

Local speed pattern (LSP) are calculated from the diffused speed image, these acts as the base line features,

$$F_{base} = \{s(x,y) \mid 0 < x \leq W, 0 < y \leq H\} \quad (4)$$

Here, W and H are width and height of the identified face region, respectively.

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

$$LSP^i(x, y) = \begin{cases} 1, & \text{if } s(x, y) > s(x_i, y_i), \\ 0, & \text{otherwise,} \end{cases} \quad (5)$$

Where n is the number of sampling pixels in the neighborhood of 3 × 3 pixels,

Here (x, y) is the center pixel, n is the number of neighboring pixels in the 3 x 3 (here n=8) and (x_i, y_i) indicates the position of the neighboring pixels for I ranging from 1 to 8. Therefore; calculated *LSP* (x, y) is in the range of [0, 255] as shown in Figure-4, a gray-scale representation of the image.

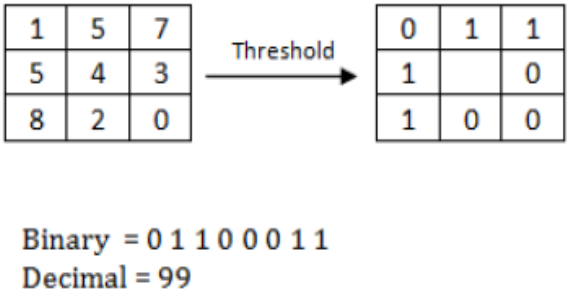

Figure 4 : Local Speed Patterns

3.4. Classification

Support Vector Machine (SVM) is a supervised machine learning algorithm which can be used for both classification and regression challenges. However, it is mostly used in classification problems. In this algorithm, we plot each data item as a point in n-dimensional space (where n is number of features you have) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiates the two classes very well.

IV. Experimental Result

4.1. NUAA datasets:

The dataset provided by NUAA [2] is used is most widely adopted dataset for face liveness detection. It consists of 15 subjects looking at the webcam with a neutral expression. Images are captured at 20 fps. For creating the fake images, pictures of the subjects have taken using the Cannon camera, and printed on the photographic paper as well as a normal A4 sheet. These printed photographs are then shown to the webcam to create the fake images.

Figure 5 : Sample images from NUAA dataset, real (top row) and fake (bottom row)

4.2. Results:

For given input image diffusion speed is calculated, features extracted from the diffusion speed image. Extracted features by LSP are sent to the SVM classifier. For training purpose 100 images are randomly selected from NUAA datasets, in that 50 fake images and 50 real images. For classification purpose 42 real images and 58 fake images fake images are taken.

	Real	Fake	Total
Training	50	50	100
classification	42	58	100

Table 1: dataset summary

The proposed method shows 90% accuracy, for testing the 100 images (42 real, 58 fake).
In that 37 are correctly detected for 42 real images and 53 are correctly detected for 58 fake faces.

Input images	Input images	Correctly detected	Percentage (%)
Real	42	30	71.42%
Fake	58	43	74.13%
Total	100	73	73%

Table 2: Classification Details (LBP)

Table3: Classification Details (Proposed Method (AOS & LSP))

	Input images	Correctly detected	Percentage (%)
Real	42	37	88.09%
Fake	58	53	91.37%
Total	100	90	90%

Intermediate images for some input images is shown below

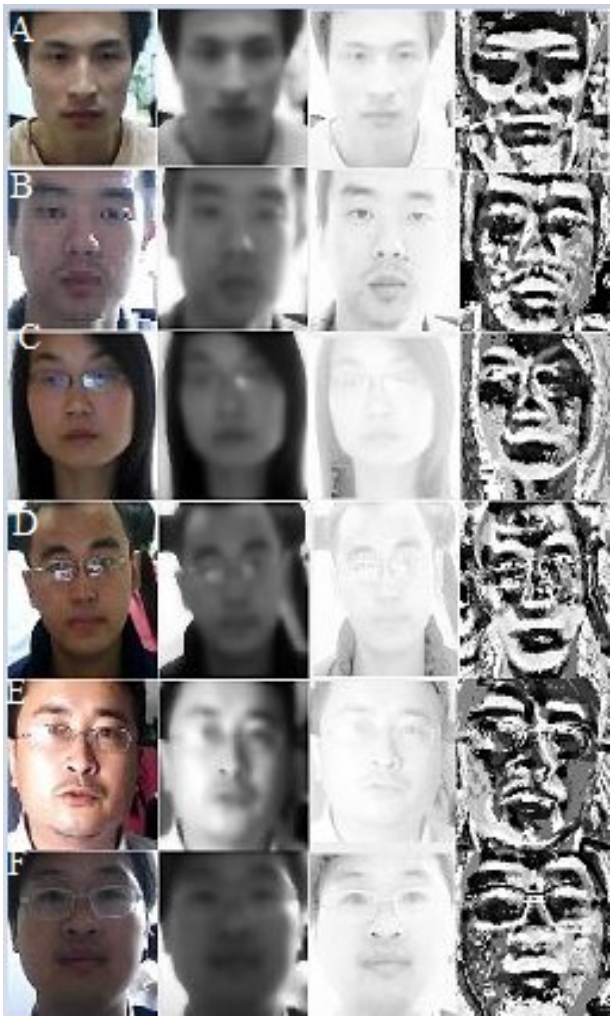

Figure 6 : (A), (C), (E) are the real images and (B), (D), (F) are fake images. The first column shows the images taken from the NUAA dataset. Diffusion images, diffusion speed, LSP are shown in second, third, fourth column respectively.

V. Conclusion

For detecting face liveness this depends on the diffusion speed rather than the diffusion result itself, as in the logarithmic total variation (LTV) model. Based on our TV flow-based diffusion speed, which is quite different from the traditional total variational framework used in the LTV model, this method can efficiently reveal the difference in the reflectance characteristics according to the 2D plane and 3D structure, whereas the LTV model provides only the illumination-invariant face image, regardless of the liveness of the given face. As compared to the texture patterns widely employed in previous approaches, 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. Based on the observational result it is observed that the implemented system gives 90% accuracy.

VI. REFERENCES

[1]. J. Bai, T. Ng, X. Gao, and Y. Shi, "Is physics-basedliveness detection truly possible with a single image?", IEEE International Symposium on Circuits and Systems, 2010, pp. 3425-3428.

[2]. X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model", Computer Vision ECCV 2010, vol. 6316, pp. 504-517, 2010.

[3]. J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single image using micro-textureanalysis," International Joint Conference on Biometrics (IJCB), 2011.

[4]. G. Pan, L. Sun, Z. Wu, and S. Lao, "Eye blink-based anti- Spoofing in face recognition from a generic web camera," IEEE 11thInternational

Conference on Computer Vision, 2007, pp. 1-8.

[5]. G. Pan, Z. Wu, and L. Sun, "Liveness detection for face recognition," Recent Advances in Face Recognition, December 2008, pp. 109-124.

[6]. G. Pan, L. Sun, Z. Wu, and Y. Wang, "Monocularcamera-based face liveness detection by combining eyeblink and scene context" Journal of Telecommunication Systems, 2009.

[7]. W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," IEEE International Conference on Image Analysis and Signal Processing, 2009, pp. 233-236.

[8]. K. Kollreider, H. Fronthaler, J. Bigun, "Non-intrusiveliveness detection by face images" Image and Vision Computing, 2009, vol. 27, no. 3, pp. 233-244.

[9]. A. Anjos, M. M. Chakka, and S. Marcel, "Motion-basedcounter measures to photo attacks in face recognition" IET Biometrics, vol. 3, no. 3, pp. 147-158, September 2014.

[10]. Santosh Tirunagari, Norman Poh, David Windridge, Aamo Iorliam, Nick Suki, Anthony T. S. Ho, "Detection of face spoofing using visual dynamics" IEEE Transaction on Information Forensics and Security", vol. 10, No. 4, April 2015.

[11]. Won Jun Kim, Sungjoo Suh, Jae Joon Han, "face liveness detection from single image via diffusion speed model" IEEE Transaction on Image Processing, vol. 24, No. 8, August 2015.

[12]. R.Raghavendra, Kiran. B. Raju, Christoph Bush, "Presentation attack detection for face recognition using Light field camera", IEEE Transaction on Image Processing, vol. 24, No. 3, March 2015

[13]. J. Ralli "PDE Based Image Diffusion and AOS", PhD thesis, 2014.

[14]. P. Perona and J. Malik, "Scale-space and edge dtection using anisotropic diffusion" IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 12, no. 7, pp. 629-639, July 1990.

[15]. J. Weickert, B.M.T.H. Romeny, and M.A. Viergever, "Efficient and reliable schemes for nonlinear diffusion filtering" Transaction on Image Processing, vol. 7, no. 3, pp. 398-410, Mar. 1998.

About Authors:

Mr. K Sreenivasulu completed B.Tech in ECE from RGUKT RK VALLEY in 2014. He is pursuing M.Tech in JNTUA College of Engineering, Anantapuramu.

Mrs. B Annapurna Lecturer, Dept. of ECE, JNTUA College of Engineering, Anantapuramu.