ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

Anti-Spoofing of a Face Image Using Diffusion Speed Model

Athira Prem[1], Bineesh. V[2]

P.G. Student, Department of Computer Science and Engineering, MEA Engineering College, Calicut University, Vengoor P.O, Malapuram, India[1]

Associate Professor, Department of Computer Science and Engineering, MEA Engineering College, Calicut University, Vengoor P.O, Malapuram,India[2]

ABSTRACT: In today's e-commerce world the e-business application require a very highlevel of authentication, as the existing traditional authenticating methods such as user name, password, identity card etc can be easily stolen. Face recognition is a widely usedbiometric approach. Face recognition technology has developed rapidly in recent yearsand it is more direct, user friendly and convenient compared to other methods. Butface recognition systems are vulnerable to spoof attacks made by non-real faces. It isan easy way to spoof face recognition systems by using facial pictures such as portraitphotographs, videos etc. A secure system needs Liveness detection in order to guardagainst such spoofing.

Liveness detection is a technique to make sure that the data is being provided by a live user and not from artificial sources. The key idea of this method is that the difference in surface properties between live and fake faces can be efficientlyestimated by using diffusion speed. Computing the diffusion speed by utilizing the total variation (TV) flow scheme and extracting anti-spoofing features based on the local patterns of diffusion speeds, the so-called local speed patterns (LSPs). These featuresare subsequently input into a linear SVM classifier to determine the liveness of the givenface image. As compared to previous approaches, this method performs well regardlessof the image medium and even under varying illuminations. This is quite desirable forachieving robust face recognition and verification in a wide range of environments.

KEYWORDS: Spoofing, diffusion speed, local speed pattern, face liveness detection, eigenface.

I. INTRODUCTION

Biometrics is the technology that establishing the identity of a person based on the physical or behavioural characteristics of an individual. Biometrics is one of the fastest growing segments of security industry. In Biometric technology measuring and analysing the human body characteristics by using different methods such as facial recognition, fingerprint recognition,[1], [2] handwriting verification, hand geometry, DNA verification, retinal and iris scanner. Among all these techniques, the one which has rapidly developed in recent years is face recognition technology, it is more direct, user friendly and very much convenient compared to other methods. Nowadays it is widely applied to various security systems. But, in general, face recognition algorithms are not capable to differentiate original (live) face and fake (non live) face, which is a major security issue. Face recognition systems are highly vulnerable to spoof attacks made by non-real faces. There are many methods to spoof face recognition systems, by using facial pictures such as photographs or videos of a valid user etc. These can be easily obtained from the internet or by captured using a camera. In order to protect against such spoofing, a secure system needs liveness detection technique.

A human can distinguish a live face or a fake face without much effort, because a human can easily recognize the physiological indications of liveness, for example, facial expression changes, mouth movement, head rotation, eye change. But sensing these clues is very difficult for a computer. Spoofing is purely a biometric vulnerability it is not

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

shared with other IT security problems. In these attacks, intruders use some type of artificially produced object (e.g., face mask, gummy nagger or printed iris image) or try to imitate the behaviour of genuine users. To address this limitation, several methods are devoted effort to judicious live faces from fake ones.

II. RELATED WORK

In the face recognition community, numerous recognition approaches have been presented, but the efforts on anti-spoofing are still very limited. The most common faking way is to use a facial photograph of the valid user to spoof the face recognition system, since usually one's facial image is very easily available for the public, for example, downloaded from the web, captured unknowingly by the camera. Photo attack is one of the cheapest and easiest spoofing approaches. The imposter can rotate, shift, and bend the valid user's photo before the camera like a live person to fool the authentication system. It is a challenging task to detect whether the input face image is from a live person or from a photograph. Liveness detection approaches are mainly categorized based on the type of liveness indicator used to assist the liveness detection of faces. There are many different type of indicators are used. Such as spectrum based, depth information, texture, life sign, etc.

Spectrum-based methods clearly expect the inter-class difference between live and fake faces by selecting appropriate working spectrum. In [3], measured the reflectance disparities between live and fake faces based on the computed radiance under different illuminations, and these estimated values were then applied to the Fisher linear discriminant. Also [4], measured the albedo curves of different materials, i.e., skin and non-skin, and selected two discriminative wavelengths. In a user-cooperative environment, the distance between a person to be verified and the camera, and the person's head pose, are roughly fixed. We exploit the fact that reflectance from real facial skin and mask materials (silicon, latex, or skinjell) should be different. These approaches may lead to correct liveness detection.

Texture analysis techniques mainly take the advantage of detectable texture patterns such as print failures [5], [6], [7], and overall image blur to detect attacks. This approach works on the assumption that fake faces are printed on paper, and the printing process and the paper structure that produce texture features can differentiate those printed images from real face images.

Detection of life signs can be of two types. First one assumes certain known interaction from the user. In this situation the user needs to perform a certain task to verify the liveness of his face image. This task can be a certain move that can be considered as a challenge response or a motion password. Users who will perform their task correctly are assumed to be real. The second category does not assume any interaction from the user, but focuses on certain movements of certain parts of the face, such as eye blinking [8], mouth movement [9], head rotation [10] and will consider those movements as a sign of life and therefore a real face. Life sign based liveness detection based approach is very hard to spoof by 2D face images and 3D sculptures.

Most of the current face recognition systems are based on intensity images and equipped with a generic camera. An anti-spoofing method without additional device is more preferable. It could be easily integrated into the existing face recognition systems.

III. SYSTEM STUDY

We propose a simple method for detecting face liveness from a single image. The key idea of this method is that the difference in surface properties between live and fake faces can be efficiently estimated by using diffusion speed [11]. It is easy to detect that the light on a live face is quite randomly reflected because of the 3D structures, while the reflectance of the light on a 2D fake face is relatively uniform as shown in the figure1. This lead a difference in the illumination effects of captured images of live and fake faces. This is because the illumination energies on a 2D surface are evenly distributed and thus are diffuse slowly, whereas those on a live face move faster because of their non-uniformity. Hence, it is considered that the diffusion speed, e.g., the difference in pixel values between the original and diffused images, provides useful clues that can be used to discriminate a live faces from a fake.

In particular, we attempt to model this diffusion process by computing the diffusion speed by utilizing the total variation (TV) flow scheme and extracting anti-spoofing features based on the local patterns of diffusion speeds, the so called local speed patterns (LSPs). Our features are subsequently input into a linear SVM classifier to determine

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

the liveness of the given face image. This method performs well regardless of the image medium and even under varying illuminations. This is quite desirable for achieving robust face recognition and verification in a wide range of environments. The experimental results on various datasets demonstrate that our proposed method provides a reliable performance of face liveness detection.

i. Face Liveness Detection

The illumination characteristics of live and fake faces are significantly different, as shown in the Fig.1. So it is easy to find that the light on a live face is randomly reflected because of its 3D structures, while the reflectance of the light on a 2D fake face is relatively uniform due to it planar structure. This leads to a difference in the illumination effects of live and fake faces. To estimate this difference using a single image, we propose a new concept of diffusion.

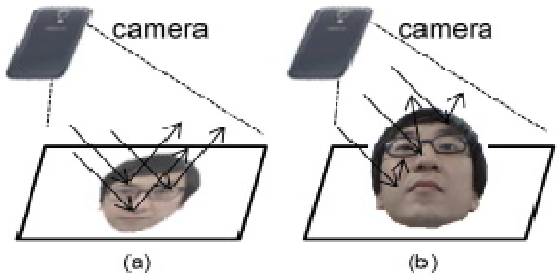

Fig-1: (a) and (b) Different characteristics of illuminations on a fake and a live face, respectively.

Diffusion Speed

To estimate the difference in illumination characteristics of live and fake faces, we propose exploiting the concept of diffusion. Because of the illumination energies on a 2D surface are evenly distributed and thus they are 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, i.e. difference in pixel values between the original and diffused images, provides useful clues that can be used to discriminate a live faces from a fake one in a single image. In particular, we 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.

Efficiently show the diffusion speed in which illumination characteristics are clearly revealed. To this end, at first conduct nonlinear diffusion on the original face image I, given as [12], [13]

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

Where k denotes the iteration number. For the diffusivity function d(•).

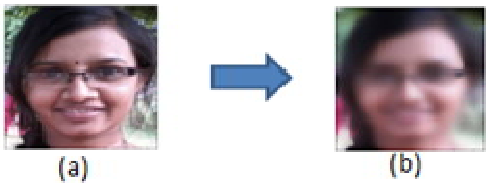

Fig-2: (a) Original image (b) Diffused image

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

In the given image fig.2, the TV flow has been proven to comply with the following rules [14]. 1) Pixels belonging to a small region move faster than those belonging to a large region, e.g., a homogenous region, and 2) the two boundary pixels adapt their value with half that speed. These rules lead to a very useful consequence: by simply computing the difference in pixel values of the original and diffused images generated by the TV flow, we estimate the relative diffusion speed of each pixel (see Fig.2(b)). It is noteworthy that our diffusion space successfully reveals the illumination effects.

In following, define the diffusion speed at each pixel position (x, y), which represents the amount of difference on the log space between the diffused image and the original one, given

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

Where L denotes the total number of iterations, by utilizing the higher order statistics of the diffusion map [15], [16], simply fix the iteration number L in this study to achieve fast computation . Since the positions of the underlying structures of the face of different individuals are similar. It should be emphasized that our diffusion speed is defined on the log space because of its ability to consistently represent the face under varying lighting conditions [17]. The diffusion speed maps of live and fake faces are shown in Fig. 3. To show the results more clearly, it provide a Binarized version of diffusion speed maps according to the predefined value. We can see the difference in the diffusion speeds of fake and live faces, e.g., in the eye and cheek region, although the corresponding original images appear very similar to each other.

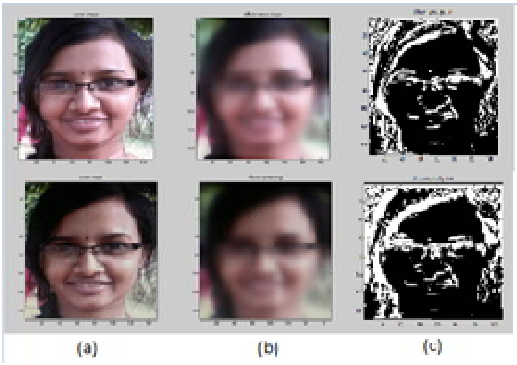

Fig-3: Diffusion speed maps for live (top) and fake faces (bottom). (a) Original image. (b) Diffused image. (c)Binarized diffusion speed values.

Feature Extraction: Local Speed Patterns

On the basis of the above analysis, we can utilize the ability of the diffusion speed model to efficiently extract anti-spoofing features. More specifically, we straightforwardly employ the value of the diffusion speed itself at each pixel position as our baseline features [11]. We propose defining the local speed patterns to efficiently capture even small differences between the diffusion speed maps of live and fake faces as

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

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

The range of features LSP(x,y) is [0, 255] and can be represented as a gray-scale image (LSP image). Then there building the histogram features [18] based on fLSP(x,y) values of the image (LSP image). It should be emphasized

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

that only uniform patterns, which contain at most two transitions between 0 and 1, are utilized, while all the other patterns are accumulated in one additional bin[18], Finally, the LSP histograms generated in each block are subsequently normalized by,

$$h_k = \frac{N_k}{\sqrt{\sum_{q=1}^{59}(Nq)^2 + \varepsilon}}, \qquad N_k = \sum_{\substack{(x,y)\epsilon B \\ f_{LSP}(x,y)\epsilon k}} 1$$

By concatenating all the LSP histograms there can represent the face image as a single vector. Then, our feature vector FLSP is input into the linear SVM classifier for training and tests. The overall procedure of the feature extraction is shown in Fig. 4.

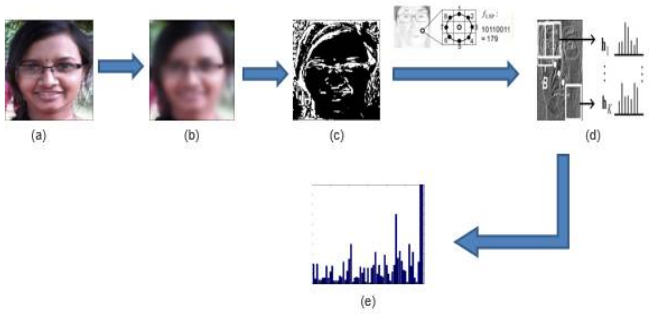

Fig-4: (a) Original face. (b) Diffusion speed map scaled from [0, 255]. (c) Procedure for computing *f*LSP at each pixel position. (d) LSP image. (e) LSP-based feature vector generation for the given face image

ii. Face Recognition

Eigenface:

Eigenfaces is the name given to a set of eigenvectors when they are used in the computer vision problem of human face recognition [19]. These eigenvectors are resultant from the covariance matrix of the probability distribution over the high-dimensional vector space of given face images. The eigenfaces themselves form a basis set of all images used to create the covariance matrix. This produces dimension reduction by allowing the smaller set of basis images to represent the original training images. Classification can be achieved by comparing how faces are represented by the basis of set of images.

A group of eigenfaces can be created by performing a mathematical procedure called principal component analysis (PCA) on a large set of images in our dataset. Casually, eigenfaces can be considered a set of "standardized face ingredients", it is derived from statistical analysis of many pictures of our trained faces on our data set. All human face can be considered to be a combination of these standard faces. For example, one's face might be composed of the average face plus 10% from eigenface 1, 55% from eigenface 2, and even -3% from eigenface 3. Noted that, it does not take the value of many eigenfaces combined together to achieve a fair approximation of most faces. Also, because a person's face is not recorded by a digital photograph, but instead as just a list of values (one single value for each eigenface in the database used), there is much less space is taken for each person's face.

The eigenfaces that are formed will appear as light and dark areas that are arranged in a specific pattern. This pattern is used to calculate how different features of a face are singled out to be evaluated and scored. There will be a pattern to evaluate symmetry of input image, if there is any typical style of facial hair, where the hairline is, or evaluate the size of face parts like nose or mouth. Other eigenfaces have patterns that are less simple to identify, and

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

the image of the eigenface may look very little like the input face. As shown in the fig.5, it find the similarity of input image with eigenface value, only give authentication for the person matching the eigen value with trained faces.

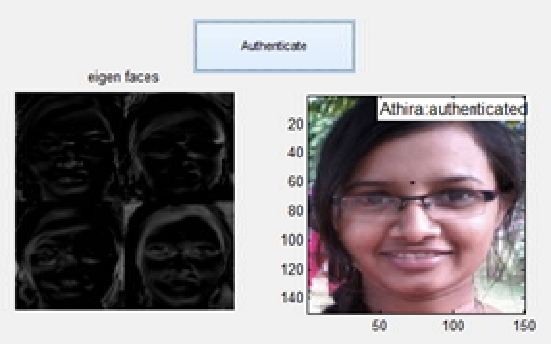

Fig-5: Eigenface matching.

IV. EXPERIMENTAL RESULTS

i. Datasets

There we have available standard benchmark datasets: NUAA dataset [11], which is most widely employed in this field; our liveness (SFL) dataset containing real-world scenarios in indoor and outdoor environments with varying illumination conditions. Here we create a new dataset which include all type face images. Here is a collection of original and fake images at different environments with varying illumination conditions.

ii. Accuracy of the system

To find the accuracy of this method there create a fixed number of fake images. And train the system that these are fake images. Also there is a number of original images are stored in to the database. When we need to check the accuracy of the method system automatically check all images in the database. Through this procedure the system can find original and fake images. Also system count the number of fake images. By comparing the result and input the system can find the accuracy of the system.

Here we already know the accuracy of proposed system. Now we have find the accuracy of one of another existing system, which directly extract features of the face. i.e., In LBP (Local Binary Pattern)[20] we does not calculate the diffusion speed of the image. In LBP method it directly extract features from a Binarized image of face. Here we have to find the accuracy of both system we can find that accuracy of proposed system is higher than LBP method as shown in the figure 6.

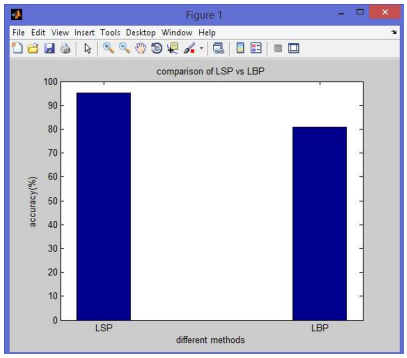

Fig: Comparison between LSP and LBP.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

V. CONCLUSION

A simple and robust method for face liveness detection was discussed in this paper. The key idea of the method is to adopt diffusion speed for modelling the difference in the illumination characteristics of live and fake faces. Specifically, there exploiting the TV flow and AOS scheme to efficiently compute the diffusion speed, which is robust to varying lighting conditions. To capture the difference between live and fake faces more effectively, the method attempted to encode the local pattern of diffusion speed values, the so-called local speed pattern (LSP), and define it as our feature. And to make the system more secured we find the authentication of each person. Only authenticated person can use the system further. Based on diverse experimental results, here confirmed that this method successfully performs when the images are captured in a wide range of indoor and outdoor environments, and when they include persons with varying poses and expressions and under different illuminations. Moreover, our LSP-based scheme is effective in real-time and can thus be deployed in various mobile devices. Therefore, conclude that the method for face liveness detection will lead to high-level security for mobile 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.Criminisi, P. Perez, and K. Toyama, "Region filling and object removal by exemplar-based image inpainting.", IEEE Transactions on Image Processing, vol. 13, no.9, pp. 1200–1212, 2004.

[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] 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.

[4] 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.

[5] 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.

[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] 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.

[8] 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.

[9] 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.

[10] 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.

[11] Wonjun Kim, Member, IEEE, SungjooSuh, Member, IEEE, and Jae-Joon Han, Member, IEEE, "Face Liveness Detection From a Single Image via Diffusion Speed Model," IEEE Transactions On Image Processing, Vol. 24, No. 8, August 2015.

[12] 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.

[13] M. Rousson, T. Brox, and R. Deriche, "Active unsupervised texture segmentation on a diffusion based feature space," in Proc. IEEE Comput. Soc. Comput. Vis. Pattern Recognit. (CVPR), vol. 2. Jun. 2003, pp. II-699–II-704.

[14] T. Brox and J. Weickert, "A TV flow based local scale measure for texture discrimination," in Proc. 8th Eur. Conf. Comput. Vis. (ECCV), May 2004, pp. 578–590.

[15] W. Kim and C. Kim, "A texture-aware salient edge model for image retargeting," IEEE Signal Process. Lett., vol. 18, no. 11, pp. 631–634, Nov. 2011.

[16] W. Kim and C. Kim, "Active contours driven by the salient edge energy model," IEEE Trans. Image Process., vol. 22, no. 4, pp. 1667–1673, Apr. 2013.

[17] E. H. Land and J. J. McCann, "Lightness and retinex theory," J. Opt. Soc. Amer., vol. 61, no. 1, pp. 1–11, 1971.

[18] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE Trans. Pattern Anal. Mach. Intell., vol. 24, no. 7, pp. 971–987, Jul. 2002.

[19] Ruiz-del-Solar, J and Navarrete, P.Eigenspace-based face recognition: a comparative study of different approaches, 2005.

[20] A. H. J. Maatta and M. Pietikainen, \Face spoofing detection from single imagesusing micro-texture analysis," in Proc. IEEE Int. Joint Conf. Biometrics (IJCB),pp. 1{7, Oct 2011.