SPOOFING FACE RECOGNITION USING DIFFUSION SPEED METHOD

T.Inithakaran
M.E Scholar
Department of Computer Science & Engineering
Manonmaniam Sundaranar University
Tirunelveli-627012, India
inithakaran@gmail.com

Dr.R.S.Rajesh
Professor
Department of Computer Science & Engineering
Manonmaniam Sundaranar University
Tirunelveli-627012, India
rs_rajesh@yahoo.co.in

P.Sivananaintha Perumal
Research Scholar
Department of Computer Science & Engineering
Manonmaniam Sundaranar University
Tirunelveli-627012, India
sivanpaul@gmail.com

ABSTRACT - A spoofing attack is a situation in which one individual or program successfully masquerades as another by falsifying data thereby gaining an illegitimate point of preference. Spoofing is the act of masquerading as a valid user by falsifying data to gain an illegitimate access. In this paper, we expect to inspect the spoofing potential for different recognition systems and location the detection problem of this more complex attack type. In this a technique the dispersion velocity of picture is taken to address the false face acknowledgment issue. In particular, the difference in surface properties between an original face and a mask one is efficiently revealed in the diffusion speed,, the anti spoofing features are exploited by utilizing the total variation flow scheme. More specifically, this paper defines the local patterns of the diffusion speed, the so-called local speed patterns, are the features, which are input into the linear SVM classifier to figure out if the given face is fake or not. One important advantage of the proposed method is that, in contrast to previous approaches, it accurately identifies the false input.

***Keywords**:* Spoofing, presentation attacks face recognition, mask attack.

1. INTRODUCTION

Being the most usually utilized biometric quality by people, face acknowledgment has turned into a dynamic examination theme now and it has discovered many unbelievable applications in customer electronics and programming. Face owes its disrepute basically to being effectively and non-rudely available contrasted with other biometric attributes like thumb impression or iris. Caricaturing attack is the demonstration of outsmarting a biometric framework by displaying fake confirmation keeping in mind the end goal to pick up verification [1]. It is generally easy to fashion such an attack for facial acknowledgment frameworks, because of the way that the photos or recordings of a legitimate client can be effortlessly caught from a separation or acquired by means of web, e.g. through informal communities. Legitimate clients (just clients or customers) can be characterized as the persons that are selected in a face acknowledgment framework. For the most part as an aftereffect of their straightforwardness and minimal effort, the already said photograph print and video replay attacks [2] constitute the center of examination exercises in face acknowledgment. Existing adverse to satirizing approaches against these sorts of attacks can be generally arranged into three gatherings: composition investigation, movement examination and live discovery. Accepting the nearness of theory like printing antiquities [3] and/or obscuring [4], numerous against mocking systems analyze the composition of the caught face picture. Likewise, in a late study [5], smaller scale surface examination utilizing multi-scale nearby paired examples is proposed. It is satisfied that this kind of methodologies exceedingly relies upon the nature of the printed picture or video show. The second gathering of strategies expects to distinguish caricaturing assaults by investigating the movement in the scene taking into account the way that planar items like a sheet of paper or a cellular telephone screen move in an altogether diverse manner contrasted with genuine appearances. For instance, in [6], the directions of little locales of face pictures are examined to be named genuine or fake. In a comparable way, by figuring geometric invariants of an arrangement of consequently found facial focuses, Marico et al. [7] abuse the same miracle. At last in the last gathering of strategies, liveness of the face is resolved taking into account live-confront particular motions, for example, eye squinting [8] or lip developments [9]. Be that as it may, methodologies of this kind will undoubtedly come up short on account of video replay assaults or much all the more basically, with photographic covers which are entirely determination facial prints worn on face after the eyes and mouth districts are removed, as guaranteed in [10]. Correspondingly in [11], it is again demonstrated that with eyes cut out from the photographs, conventional noticeable live identification technique still identifies flickering, at the end of the day, can't recognize a photograph assault. As of late, a few studies have been distributed that present systematic and reproducible examinations of a few of these and some different techniques, with a common reason for giving practically similar results on open databases [12]–[14]. Chip away at misrepresentation discovery capacities for face is still restricted and a significant piece of it depends on the levelness of the caught surface before the sensor amid an assault. This is likewise valid for methodologies that look at the 3D way of the face by utilizing extra gadgets, which is substantially more practical now with the presentation of moderate shopper profundity cameras. For example, in [15], 3D information procured with an ease sensor is used to confine face and in the meantime to test its genuineness to condense their framework's powerlessness to parodying assaults. Sadly, techniques that depend upon the supposition of a planar surface for a fake face are rendered useless if there should be an occurrence of 3D facial cover assaults [16]. To the best of our knowledge, there have been very few studies published addressing this issue and they are detailed in the next section.

I. RELATED WORK

The earliest studies in mask detection aim to distinguish between facial skins and mask materials by exploiting the difference in their reflectance characteristics. This thought can be traced 30 years back to [17], which claims that a face thermo gram is not vulnerable to disguises and even plastic surgery can be detected, since it reduces the thermal signature of face. Later, stating that disguises can be detected even better in near-infrared, Pavli is and Symosek propose to utilize the 1.3-1.7 μm sub-band of the upper band [18]. Simple thresholding is suggested for classification, without reporting any experimental results, but only illustrations. Two more studies that follow the same way of thinking are published with systematic experiments and results [11], [19]. A multi-spectral analysis is proposed in both, claiming that fake, by its definition, is indistinguishable for human eyes and therefore, using only visual images is not sufficient to detect the attacks.

On the other hand, they both handle the mask attack problem in an evasion/disguise scenario rather than spoofing since they don’t examine masks that are replicas of valid users to be impersonated. In [19], the authors conduct experiments on different mask materials such as silicon, latex or skin-jell to see how different they behave in reflectance when compared to facial skin that is sampled from the forehead region.

The technique is accounted for to identify fake countenances with 97.78% arrangement rate. Be that as it may, the likelihood of impediment in the temple district and the forced reach constraint limits handy application. Also, in this study, veils don't exist subsequent to the examinations are done specifically on cover materials. So also in [11], two discriminative wavelengths (850 and 1450 nm) are chosen in the wake of looking at the albino bends of facial skin and veil materials with shifting separations. A SVM classifier is prepared to separate in the middle of authentic and fake endeavors and tried on a database of 20 veils of various materials: 4 plastic, 6 silica gel, 4 paper mash, 4 mortars and 2 wipes. The outcomes demonstrate that the strategy can accomplish an arrangement rate of 89.18%. This work enhances the cutting edge by eliminating the range limitation.

II.FACE LIVENESS DETECTION

A. Motivation

The rationale behind the proposed method is that the illumination characteristics of live and fake faces are significantly different. It is easy to see that the light on a live face is quite randomly reflected because of the face image structures (e.g., nose, lip, etc.), whereas the reflectance of the light on 2D fake face is relatively uniform. This leads to a difference in the illumination effects of captured images of live and fake faces. In order to estimate this difference in a single image, we propose the concept of diffusion. 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 no uniformity. Therefore, 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 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.

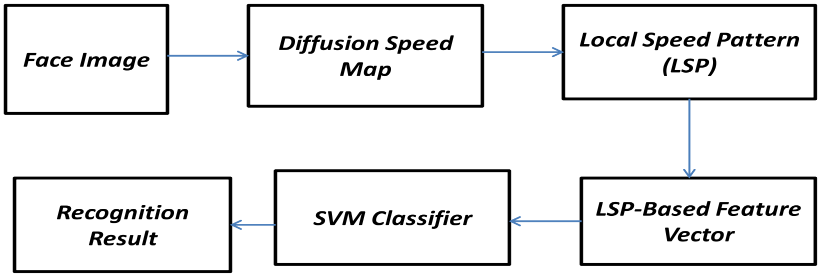


Fig 1.1 Block Diagram Of Proposed System

B. Diffusion Speed

In this subsection, we aim to efficiently show the diffusion speed in which texture based illumination characteristics are clearly described. To this end, we first conduct nonlinear diffusion on the original face image *I,* given as [15]:

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

Where *k* denotes the iteration number. For the diffusivity function *d (·)*, we propose adopting the total variation (TV) flow, defined as [16]

$$d(x) = \frac{1}{x+\xi}, \qquad (2)$$

Where ξ is a small positive constant. In a given image, the TV flow has been proven to comply with the following rules [17]. 1) Pixels belonging to a small region move quicker than those belonging to a large region, e.g., a homogenous region, and the two boundary pixels adapt their value with half that speed. These rules lead to useful significant by simply computing the dissimilar in pixel values of the original and diffused images generated by the TV flow, we can easily estimate the relative diffusion speed of each pixel.

An important issue is to solve the diffusion equation defined in (1). To this termination, we use an efficient method, called the additive operator splitting (AOS) scheme [18] defined as

$$u^{k+1} = \frac{1}{2}((I - 2\tau A_x(u^k))^{-1} + (I - 2\tau A_y(u^k))^{-1})u^k, \quad (3)$$

Where *Ax* and *Ay* denote the diffusion matrices computed in the horizontal and vertical directions, individually.

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

$$s(x, y) = |\log(u^0(x, y) + 1) - \log(u^L(x, y) + 1)|, \quad (4)$$

Where *L* denotes the total number of iterations, which is set experimentally in our implementation. Although the optimal iteration for *L* can be adaptively determined, e.g., by utilizing the higher order statistics of the diffusion map [20], [21], we 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 highlight that our diffusion speed is defined on the log space because of its ability to consistently represent the face under varying lighting conditions.

C. Feature Extraction: Local Speed Patterns

On the basis of the above analysis, we can use 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, given as

$$\mathbf{F}_{\text{base}} = \{s(x, y) | 0 < x \leq W, 0 < y \leq H\}, \quad (5)$$

Where and *H* denote the width and height of the detected face region, respectively. Defining the local speed patterns to methodical capture even small differences between the diffusion speed maps of live and fake faces.

D. Properties of the LSP-Based Feature Vector

We discuss here the advantages of our proposed features for face live detection. 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 **F**LSP are outline as follows.

1) Focus on the diffusion speed rather than the diffusion result itself, as in the logarithmic total variation (LTV) model [22]. Based on our TV flow-based diffusion speed, which is quite different from the traditional total variation framework used in the LTV model, our 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 live of the given face.

2) As compared to the texture patterns widely employed in previous approaches, our LSP-based feature vector captures texture based characteristics on corresponding surfaces. This allows the proposed scheme to be 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.

3) Since our diffusion speed model reliably works under various lighting conditions, the LSP-based feature vector can be applied to low light environments.

4) Because of the AOS-based diffusion scheme, the proposed method can perform sufficiently well in real-time to be applied in the systems. These properties allow our LSP-based features to convey reliable information about the given face image to determine whether it is fake or not in real-time system.

IV. RESULT & DISCUSSION

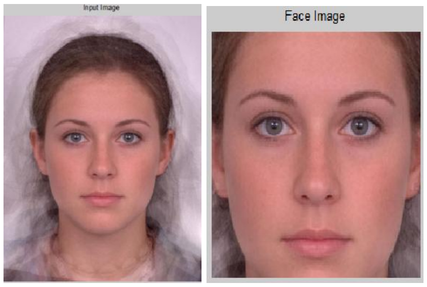


Fig 4.1 Input Image and Extracted Face Image

The first part in the above figure is the original image of the person and the second part is the extracted image to look the face closer. The figure show that the input image which get read from the mat lab path. The input image may be original face of the person or the impostor with mask to make spoofing. It leads to spoofing attack.

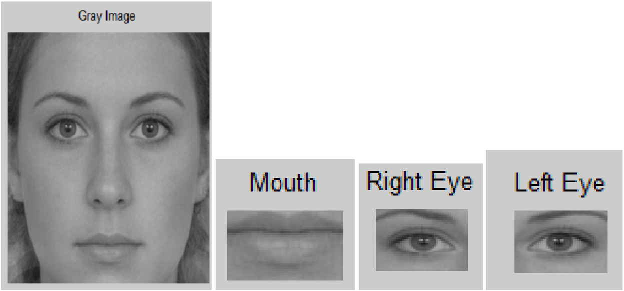


Fig 4.2 Gray-Level Face Components

The figure shows the extracted face components such as mouth, right eye and the left eye. Extraction of the edge, texture features from the face components helps to recognize the face correctly.

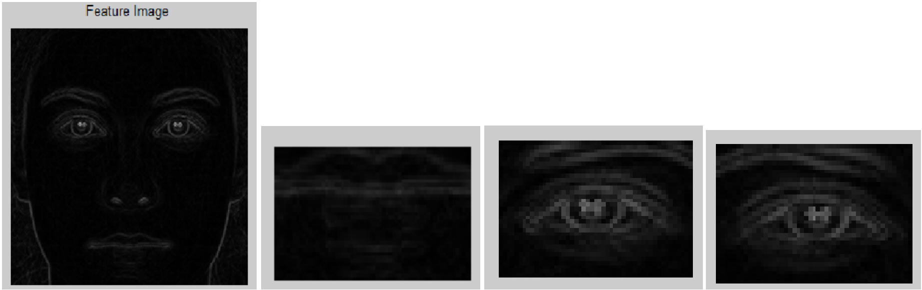
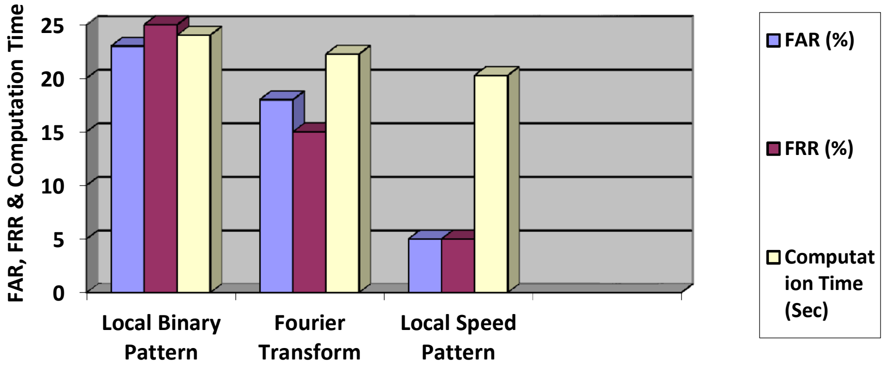


Fig 1.4 Features -Level Face Components

The figure 1.4 shows that the Feature -Level components of the face input image. Extraction of edges and texture features helps to recognize the face. The Diffusion speed method for face mask recognition leads to recognize the original and fake faces with high recognition rate.

Local Binary Pattern (LBP)	***Image1***	***Image2***	***Image3***	***Image4***	***Image5***	***Measures***
	23	24	22	23	25	FAR (%)
	25	24	23	23	24	FRR (%)
	24.8712	25.0121	24.0276	24.6201	26.7340	Computation Time (Sec)
Fourier Transform	18	17	16	15	14	FAR (%)
	15	18	15	18	15	FRR (%)
	22.2506	23.1723	21.7604	22.7289	22.9142	Computation Time (Sec)
Local Speed Pattern (LSP)	5	6	5	5	4	FAR (%)
	5	4	5	4	5	FRR (%)
	20.2605	20.0217	21.7432	20.1232	21.0987	Computation Time (Sec)

Comparison Graph



Graph 4.1 Recognition Rate Comparisons

V. CONCLUSION

A simple method for face live detection was proposed in this paper. The key idea of the proposed method is to diffusion speed for modeling the difference in the texture based characteristics of live and fake faces. Specifically, we proposed exploiting the TV flow and AOS scheme to efficiently compute the diffusion speed, which is system to varying lighting conditions. To capture the difference between live and fake faces more effectively, we attempted to encode the local pattern of diffusion speed values, so-called local speed pattern (LSP), and define it as our feature. We confirmed that the proposed method successfully performs when the images are captured in a wide range of low light and highlighting environments, and when they include persons with varying poses and expressions and under different illumination. Moreover, our LSP-based scheme is effective in real-time and can thus be deployed in various systems. Therefore, we conclude that the proposed method for face live detection will lead to high-level security for systems.

REFERENCES

[1] K. Nixon, V. Aimale, and R. Rowe, “Spoof detection schemes,” in *Handbook of Biometrics*, A. Jain, P. Flynn, and A. Ross, Eds.New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.

[2] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, “Security evaluation of biometric authentication systems under real spoofing attacks,” *IET Biometrics*, vol. 1, no. 1, pp. 11–24, Mar. 2012.

[3] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, “Is physics-based liveness detection truly possible with a single image?” in *Proc. IEEE ISCAS*,May/Jun. 2010, pp. 3425–3428.

[4] J. Li, Y. Wang, T. Tan, and A. K. Jain, “Live face detection based on the analysis of fourier spectra,” *Proc. SPIE*, vol. 5404, pp. 296–303, Aug. 2004.

[5] J. Maatta, A. Hadid, and M. Pietikainen, “Face spoofing detection from single images using micro-texture analysis,” in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–7.

[6] K. Kollreider, H. Fronthaler, and J. Bigun, “Evaluating liveness by face images and the structure tensor,” in *Proc. IEEE Workshop Autom.Identificat. Adv. Technol.*, Oct. 2005, pp. 75–80.

[7] M. De Marsico, M. Nappi, D. Riccio, and J. Dugelay, “Moving face spoofing detection via 3D projective invariants,” in *Proc. 5th IAPR ICB*, Mar./Apr. 2012, pp. 73–78.

[8] G. Pan, L. Sun, Z.Wu, and S. Lao, “Eyeblink-based anti-spoofing in face recognition from a generic webcamera,” in *Proc. IEEE ICCV*, Oct. 2007, pp. 1–8.

[9] G. Chetty and M. Wagner, “Multi-level liveness verification for face-voice biometric authentication,” in *Proc. Biometrics Symp., Special Session Res. Biometric Consortium Conf.*, Sep./Aug. 2006, pp. 1–6.

[10] K. Kollreider, H. Fronthaler, and J. Bigun, “Verifying liveness by multiple experts in face biometrics,” in *Proc. IEEE CVPRW*, Jun. 2008, pp. 1–6.

[11] 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. Workshops*, Mar. 2011, pp. 436–441.

[12] M. M. Chakka*et al.*, “Competition on counter measures to 2-D facial spoofing attacks,” in *Proc. IJCB*, Oct. 2011, pp. 1–6.

[13] A. Anjos and S. Marcel, “Counter-measures to photo attacks in face recognition: A public database and a baseline,” in *Proc. IJCB*, Oct. 2011, pp. 1–7.

[14] I. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing,” in *Proc. Int. Conf. Biometrics Special Interest Group*, Sep. 2012, pp. 1–7.

[15] F. Tsalakanidou, C. Dimitriadis, and S. Malassiotis, “A secure and privacy friendly 2D+3D face authentication system robust under
pose and illumation variation,” in *Proc. Int. WIAMIS*, Jun. 2007, p. 40.

[16] N. Erdogmus and S. Marcel, “Spoofing 2D face recognition systemswith 3D masks,” in *Proc. Int. Conf. Biometrics Special Interest Group*,2013.

[17] F. J. Prokoski, “Disguise detection and identification using infrared imagery,” *Proc. SPIE*, vol. 0339, pp. 27–31, Jun. 1983.

[18] I. Pavlidis and P. Symosek, “The imaging issue in an automatic face/disguise detection system,” in *Proc. Workshop Comput. Vis. Beyond Vis. Spectr., Methods Appl.*, 2000, pp. 15–24.

[19] 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, 2009.

[20] J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Z. Li, “Face liveness detection by exploring multiple scenic clues,” in *Proc. 12th ICARCV*, Dec. 2012, pp. 188–193.

[21] 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.

[22] 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.

[23] 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.