International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 3, March 2016

A Review on Anti Spoofing For Face by Using Light Field Camera

[1]T. Silpasree, [2]N.DilipKumar, [3]N.Pushpalatha
[1]M.Tech Student (DECS), [2][3]Assistant professor,
[1][2][3] Department of ECE, Annamacharya Institute of Technology and Science (AITS) Tirupathi.
[1]t.silpasree@gmail.com [2]dilipkumar.aits@gmail.com [3] pusphalatha_ nainaru@rediffmail.com

Abstract: **The liability of face recognition systems in biometrics is a growing concern today, as still it remains vulnerable to various sophisticated attacks that undetermined the reliability of biometric systems. In this paper, we present a novel approach to accurately detect and mitigate the Spoofy attacks on the face by introducing light field camera (LFC), also known as plenoptic camera. Since the use of a LFC can record the direction of each incoming ray in addition to the intensity, it also exhibits an unique characteristic of rendering multiple depth (or focus) images in a single capture, also known as refocusing, which provides the high quality artefact face features. Introducing a novel idea of exploring the inherent characteristics of Light Field Camera to detect spoof attacks by estimating the variation of the focus between multiple depth images. To this extent, we first collect a new biometric face artefact database using LFC. We then generate the face artefacts samples by simulating three different kinds of spoof effects including photo print and electronic screen attacks. Extensive experiments carried out on the light field face artifact database have revealed the outstanding performance of the proposed anti spoofing scheme when benchmarked with various well established state-of-the-art schemes.**

***Index Terms*—Biometrics, face-recognition, spoofing, security, refocussing, light field camera.**

I. INTRODUCTION

Biometric systems are widely used in numerous large- scale security and access control applications in real-life scenario. Despite their widespread use, these systems still remains vulnerable to the various sophisticated attacks that undermine the reliability of a biometric system. Among the different forms of attacks that can be performed on the biometric system, the presentation of the biometric artefacts at sensor level has received much attention from the research community. This type of attack is termed as direct attack or presentation attack, in which the unauthorized person will presents the biometric artefact of the genuine user to the sensor to gain access to restricted data, resources or premises. The spoof attack is a serious threat as it can be easily performed without any prior knowledge about the internal operation of the biometric systems. Among the available biometric modalities, face recognition is one of the most promising and widely adopted modern technologies.

With the evolving knowledge in creating an biometric artifact, it is possible to generate a high quality attack artifact in a cost effective manner that can be used to subvert the face recognition system. Among the several ways to perform spoof attacks against face recognition system, the easy way is by presenting an image of a particular enrollee either by printing a photo or by displaying photo using electronic screens such as tablets or SGIPAD screens. The feasibility of these attacks on a face recognition systems are acknowledged by the number of recent publications in this field [1]–[13], the organization of competitions [14], [15] and the evolution of standards [16] that show the strong importance to develop a technique which successfully detect and mitigates the spoof attacks in real-life scenarios.

Thus in this work, we consider the spoof attacks at a sensor level using cost effective methods such as a photo print attack and electronic screen (or display) attack. Most of the available techniques for face Presentation Attack Detection (PAD) are either based on exploring texture or the motion information that can be further processed to detect these face artefacts. The idea of the motion based approaches is based on the assumption that, normal (or real/live) face produces different motion which is largely centered on the nose when compared to the artefact samples. Most of the existing motion based spoof schemes [1], [7], [13] are based on estimating the optical flow from the recorded videos which is further analyzed to detect the spoof attacks.

Further the motion magnification scheme based on Eulerian Video Motion Magnification (EVM) [17] was explored in [12] to identify the small motion encountered in normal face video samples. The texture based face PAD

schemes are based on analyzing the texture variation using Local Binary Patterns (LBP) and its variants. Extensive analysis on adopting LBP for face PAD is presented in [5] that shows the superiority of the using LBP for this precise application. Further, the use of different LBP variants are investigated in [6], [8], and [10]. The Difference of Gaussian (DoG) technique was explored in [3] that also demonstrated the same level of the performance when compared with LBP based PAD schemes.

In addition to these schemes, frequency analysis based schemes also exist the use of 2D Fast Fourier Transform (FFT) to identify the face presentation attacks [2]. The use of image face presentation attacks by estimating the variation of focus from multiple depth images. Quality analysis for face spoof attacks are presented in [4] that shows the superior performance when compared with texture based PAD schemes. Recently, Binarized Statistical Image Features (BSIF) for robust face PAD was introduced in [11] shows the superior performance when compared with both texture, quality and the frequency analysis techniques.

In this work, we present a new approach for the face PAD using a Light Field Camera (LFC). Then we addresses these presentation attacks on 2D face recognition system by exploring the inherent characteristics of the light field camera (LFC) also known as plenoptic camera. Unlike the existing face recognition sensors, the light field camera will capture not only the intensity, but also the direction of all possible incident rays on each photo sensor pixel. As a consequences, the LFC can provides a multiple depth (or focus) images in a single capture. This property of LFC was effectively analyzed to reconstruct the both super resolution and high dynamic range images for both face [18] and iris recognition [19], which have demonstrated the increased biometric performance of the LFC based systems over conventional biometric sensors.

In this work, we explore an innovative way of exploiting the variation of focus among the multiple depth images rendered by LFC to extract the information about the presence of an artefact (or spoof). To the best of our knowledge, no work has been reported in the literature on employing LFC for biometric PAD applications.

With this backdrop, in our recent works we presented a preliminary study on face spoof attack detection on visible spectrum iris recognition. Our preliminary results carried out on adopting LFC for PAD on visible iris recognition motivated us to extend this work in many directions. More particularly, we are interested in exploring in different kinds of focus measures as well as different methods of focus variation analysis that can constitute as the building blocks of our proposed schemes.

Therefore, in this paper, we aim to answer two of the questions: (1) what is the role of the focus measure operator and its impact on calculating the variation of focus from the multiple depth images to achieve the robust face presentation attack detection algorithm? (2) How much improvements in performance can be achieved by exploring the variation of focus, when compared to the state-of-the-art spoof schemes? In the course of answering these questions, the main contributions of this work can be listed as follows: Introducing anew idea of exploring the inherent characteristics of the light field camera to detect the face spoof attacks by estimating the focus variations from multiple depth images.

- Analysing extensively 26 different focus measure operators and their impact on the face spoof methods.
- Introducing three different methods to calculate the focus variations from the multiple depth face image that in turn can be explored to detect the presence of face spoof attacks.
- Introducing a new light field face artefact database comprising of 80 subjects. We then generate a face artefact samples by simulating three different kinds of presentation attacks, including a photo print and electronic screen attacks. This is the first of its kind database collected using LFC so far.
- Presenting an extensive analysis on newly constructed light field face artefact database to study the vulnerability of the baseline face recognition systems on three different presentation attacks.
- Benchmarking the proposed scheme with 10 different well adopted state-of-the-art schemes. Obtained results have demonstrated the efficiency of the proposed scheme for the robust face PAD using light field camera.
- The rest of the paper is organized as follows: Section II presents the related works on different spoof attacks, Section III presents the existing systems, Section IV describes the light field camera and its imaging performance, Section V draws the conclusion.

II.RELATED WORKS

R.Raghavendra, Christoph Busch proposed Presentation attack detection algorithm for face and iris biometrics. Biometric systems are vulnerable to diverse attacks that emerged as a challenge to assure the reliability in adopting these systems in real-life scenario. It will extract the statistical features that can capture the micro-

texture variation using the Binarized Statistical Image Features (BSIF) and the Cepstral features that can reflect the micro changes in frequency using 2D Cepstrum analysis. Extensive experiments has carried out on a publicly available face and iris spoof database show the efficiency of the proposed PAD algorithm with a Average Classification Error Rate (ACER) = 10.21% on face and ACER = 0% on the iris biometrics.

IvanaChingovska, Andre Anjos and Sebastien Marcel proposed on the effectiveness of local binary patterns in face Anti-Spoofing. Spoofing attacks are one of the security traits that the biometric recognition systems are proven to be vulnerable to. Here, we inspect the potential of texture features based on Local Binary Patterns (LBP) and their variations on three types of attacks: printed photographs, and photos and videos displays on electronic screens of different sizes. For this purpose,weintroducesREPLAY-ATTACK, a new publicly available face spoofing database which contains all the mentioned types of attacks. Depending on the biometric modality being attacked, fabricating a fake biometric data can have different levels of difficulty.

Nesli Erdogmus proposed spoofing in 2D face recognition with 3D masks and Anti-spoofying with kinect. The problem of detecting face spoofing attacks has recently gained the well-deserved popularity. Mainly focusing on 2D attacks forged by displaying a printed photos or replaying a recorded videos on mobile devices, a significant portion of these studies ground their arguments on the flatness of the spoofing material in front of the sensor.

Pradnya M.Shende proposed a survey based on fingerprint, face and iris biometric recognition systems, image quality assessment and fakes biometric. A biometric system is a computerized system, which identifies the person on their behavioral and a physiological characteristic (for example fingerprint, face, iris, key-stroke, signature, voice, etc. This approach introduces three biometric techniques which are face recognition, fingerprint recognition, and the iris recognition and also introduces the attacks on the system and by using Image Quality Assessment For face Liveness Detection how to protect system from fake biometrics and and the different spoof attacks.

I. Chingovska, J. Yang, Z. Lei Proposed the II competition on the counter measures to 2d face spoofing attacks. As a crucial security problem, anti-spoofing in biometrics, and particularly for face modality, has achieved great progress in the recent years. Still, new threats arrives in the form of better, more realistic and more sophisticated spoofing attacks.

Samarth Bharadwaj proposed a face anti-spoofing via motion magnification and a multi-feature videolet aggregation. For robust face biometrics, the reliability in anti-spoofing approach has becoming an essential and pre-requisite against attacks. While spoofing attacks are possible with any biometric modality, face spoofing attacks are relatively easy which makes facial biometrics especially vulnerable.

III EXISTING SYSTEM

Biometric systems are vulnerable to the diverse attacks that emerged as challenge to assure the reliability in adopting these systems in real-life scenaries. In this approach, we are proposing a new solution which is used to detect the spoofy attacks based on the exploring both statistical and the Cepstral features. The existing Presentation Attack Detection (PAD) algorithm will extract statistical features that can capture the micro-texture variations using Binarized Statistical Image Features (BSIF) and Cepstral features that can reflect these micro changes in the frequency using 2D Cepstrum analysis.

We then fuse these features to form a single feature vector before making the decision on whether an capture attempt is a normal presentation or an artefact presentation using a linear Support Vector Machine (SVM).

Training set	Performance on Testing Set in ACER (%)								
	Low Resolution(LR)			Middle Resolution(MR)			High Resolution(HR)		
	Photo	Mask	RA	Photo	Mask	RA	Photo	Mask	RA
LR	6.75	7.94	2.10	0.07	0.25	2.18	0.00	0.03	0.22
MR	3.95	3.58	2.75	4.40	7.05	4.62	0.07	0.03	0.10
HR	0.02	0.27	0.01	0.05	0.02	0.02	8.16	10.55	2.14

Table I
Performance of existing pad with varying resolution on cassia face spoof database

Extensive experiments has been carried out on a publicly available face and iris spoof database show the efficiency of a proposed PAD algorithm with an Average Classification Error Rate (ACER) = 10.21% on face and ACER=0% on the iris biometrics.

FACE		IRIS	
Algorithms	**ACER(%)**	**Algorithms**	**ACER(%)**
LBP-LDA[5]	21.01	IQA[9]	2.20
LBP-SVM[5]	18.21	Quality Feature[13]	3.10
DoG-SVM[8]	26.72	GLCM[10]	5.60
Proposed Scheme	10.21	Proposed Scheme	0.00

Table II
Comparative Performance of the Existing Scheme on Cassia Face and ATVS Iris Fake Databases

IV. LIGHT FIELD CAMERA TO DETECT THE FACE

Introducing an novel idea of exploring the inherent characteristics of the light field camera to detect the face spoof attacks by estimating the focus variations from multiple depth images.

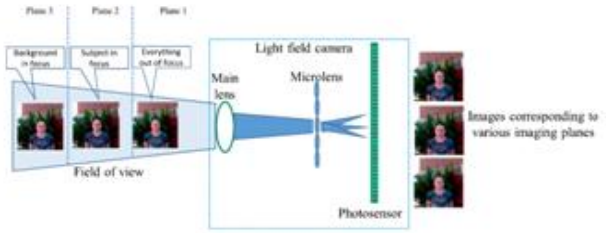

Fig 1. Light field imaging device configurations

Analyzing extensively26 different focus measure operators and their impact on the proposed face PAD method. Introducing three different methods to calculate the focus variations from the multiple depth face image that in turn can be explored to detect the presence of face spoof attacks. Introducing a new light field face artefact database comprising of 80subjects. We then generate a face artefact samples by simulating three different kinds of spoof attacks, including photo print and electronic screen attacks. It is the first of its kind of database collected using LFC so far. Presenting an extensive analysis on the newly constructed light field face artefact database to study the vulnerability of the baseline face recognition system on a three different presentation attacks.

Fig.2. Example of light field sample captured using LYTRO LFC

(a) Different depth images corresponding to single capture, (b) Face region from each of the depth image.

Biometrics: Generally this term is used alternatively to describe a characteristics or a process

1. As a process it encompasses on automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

2. As a characteristics it is a measurable biological (anatomical and physiological) and behavioral characteristics that can be used for the automated recognitions.

Face recognition*:* Face recognition has long been a goal of computer vision, but only in the recent years reliable automated face recognition has become the realistic target of biometrics research. New methods, and developments spurred by falling costs of cameras and by an increasing availability processing power have led to practical face recognition systems. These systems are increasingly being deployed in the wide range of practical applications, and future improvements promise to spread the use of face recognition further still. In this approach, we review the field of face recognition, analyzing its strengths and weaknesses and describe the applications where a technology is currently being deployed and where it shows future potential. We describe the IBM face recognition system and the some of its application domains.

Spoofing: Spoofing is the action of making something looks like that it is not in an order to gain the unauthorized access to the user's private information. This idea of spoofing originated in the 1980s with its discovery of an security hole in the TCP protocol. Today spoofing exists in various forms namely IP, URL and Email spoofing.

Light field camera: It is also known as Plenoptic camera captures information about the intensity of light in the scene, and also captures information about the direction that the light rays traveling in a space. It captures the information about shape of a face ,it is not affected by changes in background of a image, and also identifies face

from different viewing angles and able to detect upto 180 degrees of image. It is capable of reproducing old results in an Integral Photography, as well as generating new ones. Furthermore, our aim is out to finding a equivalence between a radiance density in optical phase space and the light field.The light field (radiance) density is constant along each ray. The integral of this density over any volume in a 4D phase space (light field space) is preserved during its transformations in any optical device.

V. CONCLUSION

In this paper, we proposed a novel approach to accurately detect and mitigate the spoof attacks on the face recognition system which employs the light field camera as a sensor. This method will explore the variation of the depth and focus from multiple depth images rendered in a single capture using lytro or light field camera. We also introduced a new and the relatively large scale light field face artifact databases that comprises of 80 subjects and is collected by a presenting three different types of artifacts generated using an photo print and electronic display.

This method based on measuring the relative variation of the focus shows the better performance when compared with the proposed method which is based on measuring absolute variation of the focus..•Extensive evaluation of 26 different focus measure operations revealed the best performance of the gradient based focus measure operators. In particular, the Leningrad variance showed the best performance among the different gradient based focus measure operators evaluated in this work.

REFERENCES

[1] R. Raghavendra and C. Busch, "Presentation attack detection algorithm for face and iris biometrics," in *Proc. 22nd Eur. Signal Process. Conf. (EUSIPCO)*, sep. 2014, pp. 1387–1391.

[2] 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 (BIOSIG)*, Sep. 2012, pp. 1–7.

[3] R. Raghavendra, B. Yang, Kiran B. Raja, and C. Busch, "A new perspective—Face recognition with light-field camera," in proc. *Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–8.

[4] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," in *Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep./Oct. 2013, pp. 1–6.

[5] S.Chakraborthy and Dhrubajyothi Das "Overview of face liveliness detection" in proc. *IEEE* IJIT vol.3 no.2, Apr 2014

[6] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, " face spoofing via motion magnification and multi feature videolet aggregation" in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2013, pp. 105–110.

[7] Pradnya M. Shende ,"A survey based on finger print,,face and iris biometric recognition system,image quality assessment and fake biometric" in Proc.*IEEE IJCSET*, vol. 4 issue 4 129-132, Apr.2014.

[8] I.Chingovska, J.Yang ,Z.Lei., "The 2nd competition on counter measures to 2D face spoofing attacks," in *Proc. Int. Conf. Biometrics*, Jun. 2013, pp. 1–6.

[9] Sooyeon Kim ,Yuseok Ban and Sooyeon Lee"Face liveliness detection" *in Proc. IEEE ICB*, Jun 2013,pp.1-6..

[10] A. Anjos, M. M. Chakka, and S. Marcel, "Motion-based countermeasures to photo attacks in face recognition," *IET Biometrics*, vol. 3, no. 3, pp. 147–158, Sep. 2013.

[11] N. Kose and J. Dugelay, "Classification of captured and recaptured images to detect photograph spoofing," in *Proc. Int. Conf. Informat.,Electron. Vis. (ICIEV)*, May 2012, pp. 1027–1032.

[12] K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," *Image Vis. Comput.*, vol. 27, no. 3, pp. 233–244,Feb. 2009.

[13] M. M. Chakka *et al.*, "Competition on counter measures to 2D facialspoofing attacks," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011,pp. 1–6.

[14] M.-A. Waris *et al.*, "The 2nd competition on counter measures to 2D face spoofing attacks," in *Proc. Int. Conf. Biometrics*, Jun. 2013, pp. 1–6.

[15] *Information Technology—Presentation Attack Detection—Part 3: Testing, Reporting and Classification of Attacks*, ISO/IEC JTC1 SC37Biometrics, ISO/IEC Standard WD 30107-3, 2014.

[16] H.-Y. Wu, M. Rubinstein, E. Shih, J. V. Guttag, F. Durand, and W. T. Freeman, "Eulerian video

magnification for revealing subtle changes in the world," *ACM Trans. Graph.*, vol. 31, no. 4, p. 65, 2012.

[17] R. Raghavendra, Kiran B. Raja, B. Yang, and C. Busch, "Combiningiris and periocular recognition using light field camera," in *Proc. 2ndIAPR Asian Conf. Pattern Recognit. (ACPR)*, Nov. 2013, pp. 155–159.

[18] Kiran B. Raja, R. Raghavendra, F. A. Cheikh, B. Yang, and C. Busch,"Robust iris recognition using light-field camera," in *Proc. Colour Vis. Comput. Symp.*, Sep. 2013, pp. 1–6.

[19] E. H. Adelson and J. R. Bergen, "The plenoptic function and the elements of early vision," in *Computational Models of Visual Processing*. Cambridge, MA, USA: MIT Press, 1991, pp. 3–20.

[20] *Lytro*. [Online]. Available: http://www.lytro.com, accessed Aug. 26, 2014.

[1]**T.Silpasree** did her B.Tech in Electronics and Communication Engineering at Shree Institute of technical education and doing Master of TechnologyinDigitalElectronics and Communication systems at Annamacharya Institute of Technology& Science, Tirupati, Andhra Pradesh, India.

[2]**Mr.N.Dilipkumar** obtain his B.Tech(ECE) at N.B.K.R I.S.T ,vidya nagar in 2010 and Master degree from SRM University, Chennai in 2014 and his area of interest is testing of VLSI Circuits.He is 2 years of teaching experience..He is currently working asAssistant Professor,in Annamacharya institute of technology and sciences, tirupathi. He has been active in research and published 2 international journals& attended 2 National conferences.

[3]**N. Pushpalatha** completed her B.Tech at JNTU, Hyderabad in 2004 and M.Tech at A.I.T.S., Rajampet in 2007. Presently she is working as Assistant Professor of ECE, Annamacharya Institute of Technology and Sciences, Tirupati since 2006. She has guided many B. Tech projects. Her Research area includes Data Communications and Ad-hoc Wireless Sensor Networks.