IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 06, Issue 07 (July 2016), ||V2|| PP 35-40

Anti Facial Spoof By Using Lytro's LFC

[1]T. Silpasree, [2]N.DilipKumar
[1]*M.Tech (DECS), t.silpasree@gmail.com, AITS, India*
[2]*Assistant professor, ECE, dilipkumar.aits@gmail.com, AITS, India*

Abstract:- The liability of the face recognition systems in the biometrics is a growing concern today, as still it remains vulnerable to the various sophisticated attacks that in determined the reliability of biometric systems. In this paper, we present a novel approach which accurately detects and mitigates the spoof attacks on the face by introducing a new Lytro called light field camera (LFC), also known as Plenoptic camera. LFC can records the multi dimensional data and also capture information about the light field emanating from the scene: i.e., the intensity of the light as well as the direction that the light rays were traveling in the space. In addition to these, it also exhibits an unique characteristic of exhibiting multiple depth (focus) images in a single capture, also known as Refocussing, which provides the high quality artefact face features. To this extent, we first collect a new face artefact database using LFC comprises of 80 subjects, then generate the face artefacts by simulating two different kinds of spoof effects including photo print and electronic screen attacks. Extensive experiments has been carried on these LFC artefact database have revealed the outstanding performance of proposed anti spoofing scheme when benchmarked with the various well established state-of-the-art schemes.

Keywords:- *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 many reliable biometric traits, face is a very popular one and it owes this reputation mainly to its accessibility. But unfortunately, this gift can also be a curse in malicious circumstances, enabling attackers to easily create copies and spoof a face recognition systems. Spoofing is an attempt to gain authentication through a biometric system by presenting a counterfeit evidence of a valid user Most of the existing biometric modalities are not resistant to spoof attacks: the biometric systems are usually designed to only recognize identities without concern whether the identity is live or not. Direct attack or presentation attack has gained a much attention at sensor level and is defined as in which the unauthorized person will presents the biometric artefact of the genuine user to the sensor.

Due to their convenience and low-cost, the most common types of spoofing methods being focused are photo and video attacks. Proposed anti-spoofing approaches against these attacks can be broadly classified into three groups: liveness detection, motion analysis and texture analysis. The first group aims to detect liveness of face, based on live-face specific movements such as eye blinking [13] or lip movements. The second group of approaches analyze the motion in the scene and expose spoofing attacks by examining the way the objects move in front of the sensor. The movements of planar objects like papers or screens differ greatly from those of a real face. For this reason, the trajectories of small regions in face images are analyzed and classified as real or fake. Similarly in a set of facial points are located automatically and their geometric invariants are utilized to detect attacks. Finally, in the third group of methods, the texture of the face image is examined to find spoofing clues like printing artefact and/or blurring.

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 motion based approach 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 and estimating the optical flow from the recorded videos. Further the motion magnification scheme based on Eulerian Video Motion Magnification (EVM) was explored 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. Further, the use of different LBP variants are investigated in [4]. The Difference of Gaussian (DoG) technique 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. Recently, Binarized Statistical Image Features (BSIF) for robust face PAD was introduced in [1] 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 spoof 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 called Refocussing. This property of LFC was effectively analyzed to reconstruct the both super resolution and high dynamic range images for both face [3] and iris recognition, which have demonstrated the increased biometric performance of the LFC based systems over conventional biometric sensors.

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 a new 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 describes the PAD for face and iris biometrics, Section IV describes the light field camera and its imaging performance, Section V includes simulation results and Section VI draws the conclusion.

II. RELATED WORKS

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, we introduces REPLAY-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-spoofing 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. PAD FOR FACE AND IRIS BIOMETRICS

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 spoof 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). The efficiency of the existing systems with an ACER=10.21% on face and ACER=0% on the iris biometrics.

IV. LIGHT FIELD CAMERA TO DETECT THE FACE

Light field camera: It 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 is not affected by changes in background lighting and it does not need any special light for imaging, and also identifies face from different viewing angles.

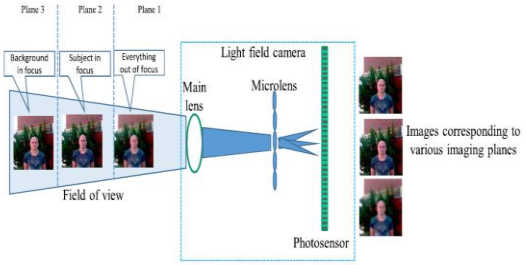

Fig 1. Light field imaging device configurations

In this work, we employed light Field Camera is used to capture the set of images which are slightly differ from one each other and each of them correspond to different view and angles i.e., LFC can able to obtain images from different imaging planes in the field of view. These are termed ad *Depth images*. Thus LFC can be used to obtain depth of scene imaged and multiple images with different regions in focus and to combine these images to create a single image.

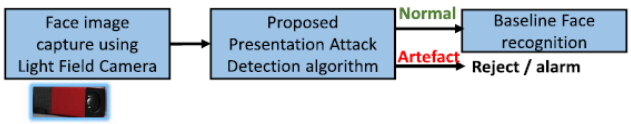

Fig 2.Overview of the proposed face recognition system

The main objective of proposed face recognition system is to explore the variation between different depth or focus images rendered by LFC. In this work ,we are analyzing the issue of detecting the face artefacts that are generated using three attacks i.e., inkjet printer, laser and an electronic display.

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.

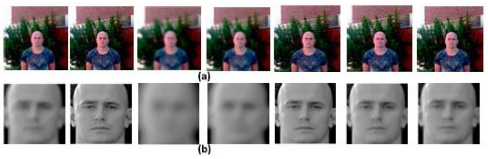

Fig 3. Example of light field samples captured using Lytro LFC
(a) Different depth images corresponding to single capture, (b) Face region from each of the depth image.

V. SIMULATION RESULTS

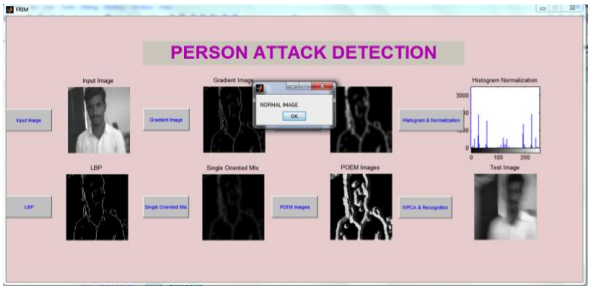

Fig 4. illustrates the different stages in detecting a normal image

It performs 8 operations on the captured face and also performs several focus operations on the background and foreground scene and calculate its depth images and finally detect whether the captured face matches with any of the face in its database or not i.e., normal image or artefact attack image.

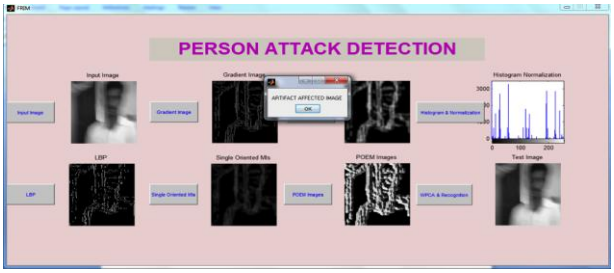

Fig 5 .illustrates in detecting the artefact affected image

TABLE 1 QUANTITATIVE ANALYSIS OF FOUR DIFFERENT CLASSIFIERS ON THE PROPOSED SCHEMES

scheme with different classifiers	Attack using Laser jet	Attack using Inkjet	Attack using I-Pad
	ACER	ACER	ACER
LDA	7.36	6.11	4.16
Polynomial SVM	6.8	8.05	3.47
RBF SVM	6.52	6.52	5.55
Linear SVM	***5.27***	***4.94***	***4.01***

The above table shows the extensive comparison with different schemes and shows the outstanding performance of the proposed scheme (a)with Laserjet is ACER=5.27% (b) with Ink jet is ACER=4.97% and(c)with I-Pad is ACER=4.01%.

VI. 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 artefact databases that comprises of 80 subjects and is collected by a presenting three different types of artefacts 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 Tenengrad 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

[12] Images to detect photograph spoofing," in *Proc. Int. Conf. Informat.,Electron. Vis. (ICIEV)*, May 2012, pp. 1027–1032.

[13] 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.

[14] M. M. Chakka *et al.*, "Competition on counter measures to 2D facial

[15] spoofing attacks," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011,pp. 1–6.

[16] M.-A. Waris *et al.*, "The 2nd competition on counter measures to 2D

[17] face spoofing attacks," in *Proc. Int. Conf. Biometrics*, Jun. 2013, pp. 1–6.

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

[19] 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.

[20] R. Raghavendra, Kiran B. Raja, B. Yang, and C. Busch, "Combining

[21] iris and periocular recognition using light field camera," in *Proc. 2ndIAPR Asian Conf. Pattern Recognit. (ACPR)*, Nov. 2013, pp. 155–159.

[22] Kiran B. Raja, R. Raghavendra, F. A. Cheikh, B. Yang, and C. Busch,

[23] "Robust iris recognition using light-field camera," in *Proc. Colour Vis. Comput. Symp.*, Sep. 2013 pp. 16.

[24] 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.

[25] *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 Technology in Digital Electronics 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 ,vidyanagar in 2010 and Master degree from SRM University, Chennai in 2014 and his area of interest is testing of VLSI Circuits. He is 3 years of teaching experience. He is currently working as Assistant Professor, in Annamacharya Institute of Technology and Sciences, Tirupathi..He has been active in research and published 2 international journals& attended 2 National conferences.