Ear Presentation Attack Detection: Benchmarking Study with First Lenslet Light Field Database

Alireza Sepas-Moghaddam, Fernando Pereira, Paulo Lobato Correia
Instituto de Telecomunicações, Instituto Superior Técnico – Universidade de Lisboa, Lisbon, Portugal
{alireza, fp, plc}@lx.it.pt

Abstract— **Ear recognition has received broad attention from the biometric community and its emerging usage in multiple applications is raising new security concerns, with robustness against presentation attacks being a very active field of research. This paper addresses for the first time the ear presentation attack detection problem by developing an exhaustive benchmarking study on the performance of state-of-the-art light field and non-light field based ear presentation attack detection solutions. In this context, this paper also proposes an appropriate ear artefact database captured with a Lytro ILLUM lenslet light field camera, including both 2D and light field contents, using several types of presentation attack instruments, including laptop, tablet and two different mobile phones. Results show very promising performance for two recent light field based presentation attack detection solutions originally proposed for face presentation attack detection.**

Keywords—Ear Presentation Attack Detection; Light Field Imaging; Artefact Database; Feature Extraction.

I. INTRODUCTION

Ear recognition is emerging as a reliable biometric modality in image-based biometrics for human identification [1]. It can also be used as a complement to facial profile-based recognition [2], and fused with other biometric modalities, notably palmprint and gait [3][4]. As for other biometric modalities, there are challenges for ear recognition systems. The presentation of ear artefacts in front of the acquisition sensors, using Presentation Attack Instruments (PAI), is known as a spoofing or presentation attack, raising new security concerns for ear recognition systems. Presentation Attack Detection (PAD) solutions, also known as anti-spoofing solutions, have been proposed to automatically detect presentation attacks [5]. Despite the fact that PAD solutions have been widely used for face [6] [7] [8] [9], fingerprint [10], or iris recognition [11] [12], so far there is no research activity addressing ear PAD. This paper is the first attempt to address ear PAD.

Recent advances in imaging sensor technologies offer new possibilities for biometric recognition and PAD. Among the emerging sensors, light field imaging technologies have recently come into prominence, allowing to consider light variations both in terms of position and direction [13] [14] [15]. Thanks to the richer scene representation, light field imaging brings new capabilities, including *a posteriori* refocusing, disparity exploitation and depth map computation which can be very useful for biometric recognition [16] [17] [18] [19] [20] [19] and PAD [21] [22] [23] [24] [25] systems.

In this context, this paper proposes the first ear PAD database, the Lenslet Light Field Ear Artefact Database (LLFEADB), including both 2D and light field ear artefact images. The database contains two sets: The first set, named *baseline LLFEADB*, includes 268 *bona fide* ear samples derived from the publicly available IST-EURECOM LLFEDB ear database [19], which includes ears from 67 subjects, with 4 shots per person, captured with a Lytro ILLUM lenslet light field camera [26]. The *extended LLFEADB* includes an additional set of high resolution *bona fide* samples, captured with the same camera from 15 subjects, with 4 image shots per person. For both sets, four types of PAIs were used to create the artefact samples: a laptop, a tablet and two different mobile phones. Since LLFEADB is the first database to consider ear presentation attacks, there are naturally no previous benchmarking results on ear PAD. To overcome this limitation, this paper exhaustively evaluates the performance of state-of-the-art light field and non-light field based available PAD solutions, in terms of accuracy, generalization and complexity, using a common evaluation framework.

This paper is organized as follows: Section 2 reviews recent PAD solutions in the literature. Section 3 describes the proposed LLFEADB database. Section 4 presents the benchmarking assessment methodology and performance evaluation results. Finally, Section 5 concludes the paper.

II. SOLUTIONS FOR EAR PAD: A REVIEW

This section overviews the available light field and non-light field based PAD solutions. According to [25], PAD solutions can be categorized based on their feature extraction approaches, notably considering cues derived from texture, quality, depth/focus or learning methods. It is also not uncommon to find PAD methods combining two or more feature extraction approaches [9]. Again, since ear PAD was not previously addressed in the literature, the examples below were originally proposed for PAD using other biometric modalities.

It is expected that reproducing an artefact using PAIs will include textures that are somehow different from the *bona fide* samples. Texture based methods can exploit the local textural patterns to distinguish artefacts from *bona fide* samples. Examples of non-light field PAD solutions include: i) using multi-scale Local Binary Patterns (LBP) to form a feature vector by concatenating local histograms extracted from overlapping micro-textures, classified using a Support Vector Machine (SVM) classifier [27]; ii) adding Gabor wavelet (GW) features and Histogram of Oriented Gradient (HOG) to the multi-scale

ISBN 978-90-827970-1-5 © EURASIP 2018

LBP descriptor, using score level fusion to combine individual SVM outputs [28]; iii) analysing facial image textures using LBP and Gray-Level Co-Occurrence Matrix (GLCM), using logistic regression classifiers and score-level fusion [29]; and iv) exploiting the joint colour texture information extracted by Local Phase Quantization (LPQ) and the co-occurrence of adjacent local binary patterns, to conclude that additionally using colour is beneficial for PAD [30].

Texture-based PAD methods exploiting the additional information available in light field images include: i) exploiting edge and ray difference features to distinguish *bona fide* from artefact samples [22], where the edge feature expresses the different light distributions for different focal planes, and the ray difference feature explores the different incident rays' information available in the sub-aperture images; ii) using a compact descriptor, named Light Field Angular Local Binary Patterns (LFALBP), exploiting the colour and angular variations captured in light field images [24], which is computed for each colour channel in the HSV and YC_bC_r colour spaces and then concatenated to be fed to a SVM classifier; and iii) using a descriptor named Histogram of Disparity Gradients (HDG), expressing the variations associated to the multiple light capturing directions available in light field images [25], which is computed for each colour HSV channel, concatenating the three histogram components and fed to a SVM classifier.

Quality based methods typically explore changes in the attack images' quality to distinguish *bona fide* samples from those captured from PAI; examples include the loss of sharpness and detail, blurriness, and differences in light distribution. For instance, an image distortion analysis based solution has been proposed, exploiting specular reflection, blurriness, chromatic moments, and colour diversity, together with multiple SVM classifiers, and trained for different presentation attacks [31].

Focus/depth based methods explore changes either in depth or focus information between the images captured/rendered at different focus planes. A light field solution relying on *a posteriori* refocusing has been proposed, exploiting the variation of focus between images rendered at different depths to detect spoofing attacks [21]. Another solution relying on a light field histogram of gradients (LFHoG) descriptor has been proposed, considering both spatial and depth information. The rendered image texture and the distribution of the scene depth are combined, providing a more comprehensive description, which is exploited by a linear SVM classifier.

Learning based methods derive features by modelling and learning relationships from images in view of distinguishing *bona fide* samples from artefact attempts. In particular, the usage of convolutional neural networks (CNN) has been growing very fast for PAD since 2014 [32]. CNNs can support both feature extraction and classification [33] [34], or they can be used only for feature extraction and combined with different classifiers, such as SVM [35] [36].

III. Lenslet Light Field Ear Artefact Database

This section describes the Lenslet Light Field Ear Artefact Database (LLFEADB) being proposed and made publicly available. LLFEADB consists of a baseline and an extended sets, with the difference between the two sets being related to the settings used for *bona fide* image acquisition.

- **Baseline set**: The *bona fide* samples in the baseline LLFEADB have been derived from the IST-EURECOM LLFEDB [24], consisting of 268 ear samples from 67 subjects, with 4 image shots per person, notably the right and left half and full profile images, captured with a Lytro ILLUM lenslet light field camera. They include ear images partly occluded by ear piercing, earing, hair and combinations of multiple occlusions. A 2D central view image (see Figure 1), rendered by the Lytro Desktop Software [37], corresponding to each *bona fide* light field, was used to generate the artefacts. The size of the rendered ear images varies, with an average size of 213×143 pixels and aspect ratio of 1.49. All *bona fide* images in the baseline set were first rescaled to 192×128 pixels, with an aspect ratio of 1.5, to have the same size while displaying using PAIs.
- **Extended high resolution set:** The ear samples derived from the IST-EURECOM LLFEDB were extracted from full facial images, and thus are representative of the type of material an attacker might be able to access online. However, resulting from cropping, they typically do not have a very high resolution, which can affect the quality of the samples displayed on PAIs, thus facilitating distinguishing them from bona fide samples. To consider a more challenging condition, additional high resolution bona fide images have been captured with the same camera, from 15 subjects, with 4 image shots per person. The size of the rendered ear images varies, with an average size of 1162×760 pixels and aspect ratio of 1.53. All the bona fide images were rescaled to 1152×768 pixels, with an aspect ratio of 1.5, to have the same size while displaying using PAIs.

A. LLFEADB: Artefact Acquisition

The artefact acquisition pipeline is illustrated in Figure 1; this acquisition of images from PAIs was performed using the Lytro ILLUM lenslet light field camera, thus creating one Light Field Raw (LFR) file per sample.

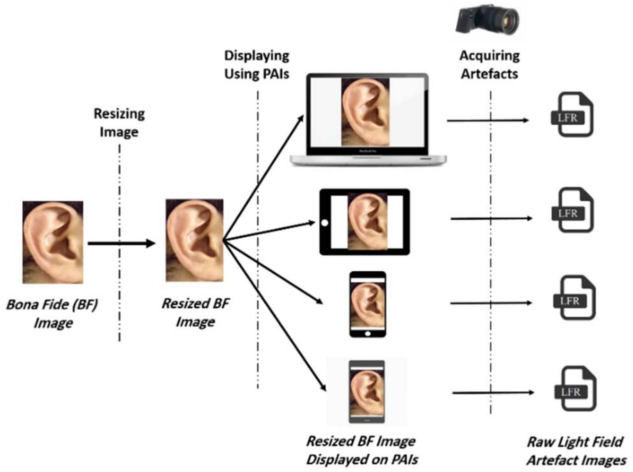
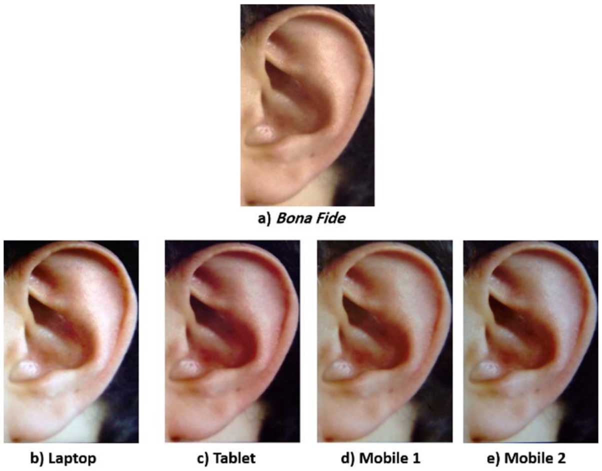


Figure 1: Artefact acquisition pipeline.

Four types of PAIs were considered for the LLFEADB:

1. **Laptop attack:** A 2D *bona fide* rendered image is displayed using a MacBook Pro 13'' – see Figure 2.b.

2. **Tablet attack:** A 2D *bona fide* rendered image is displayed using an iPad Air2, 9,7'' – see Figure 2.c.
3. **Mobile attack 1:** A 2D *bona fide* rendered image is displayed using an iPhone 6S – see Figure 2.d.
4. **Mobile attack 2:** A 2D *bona fide* rendered image is displayed using a Sony Xperia z2 – see Figure 2.e.


a) *Bona Fide*

b) Laptop c) Tablet d) Mobile 1 e) Mobile 2

Figure 2: Illustration of LLFEADB images for a *bona fide* sample and corresponding artefact samples for four different PAIs.

B. *LLFEADB: Database Elements*

The LLFEADB is the first ear artefact database for PAD, including both 2D and light field images. It is composed by the following elements:

1. **Raw Light Field Images**: Light field images in the Lytro ILLUM native file format, Light Field Raw (LFR). LFR files can be processed using the Lytro Desktop Software [37], or any other processing library/toolbox, such as the Matlab Light Field Toolbox v.0.4 [38].
2. **2D Rendered Images**: 2D rendered images for the light field central view, containing only the ear region, and created using the Matlab Light Field Toolbox V0.4 [38] – see Figure 1.
3. **Multi-view Sub-aperture Image Array**: Sub-aperture images corresponding to different viewpoints, forming a multi-view array, and created using the Matlab Light Field Toolbox V0.4 [38] – see Figure 3; these multi-view arrays contain only the ear region.
4. **Camera Calibration File**: Calibration data is provided, as this information is essential to compensate for the specific properties of each camera sensor.

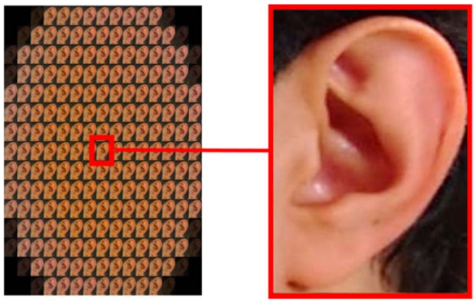


Figure 3: Multi-view sub-aperture image array for an ear image.

In summary, the LLFEADB is expected to offer a new resource that can be used for PAD research and performance benchmarking. The database will be made freely available for research purposes, together with the final version of this paper.

IV. Assessment Methodology and Benchmarking Results

This section presents the assessment metrics and the benchmarking solutions, followed by the obtained performance results.

A. *Performance Metrics*

A PAD system can be subject to two types of errors: either the *bona fide* access is rejected, known as Bona Fide Presentation Classification Error Rate (BPCER), or an access attempt using an artefact is accepted, known as Attack Presentation Classification Error Rate (APCER). To summarize the overall performance of a PAD solution, ACER (Average Classification Error Rate) is defined as half of the sum of the BPCER and APCER [6].

B. *Benchmarking Solutions*

As the LLFEADB proposed in this paper is the first database to consider ear presentation attacks, there are no relevant PAD performance results available in the literature. For the benchmarking study, the more promising solutions available in the literature have been implemented by the authors of this paper and performance results were obtained according to the best parameter settings reported in the literature. The state-of-the-art PAD solutions considered for benchmarking have been grouped into:

1. *Conventional 2D solutions*, notably those proposed in [27], [29], and [30];
2. *Light field based solutions*, notably those proposed in [23], [24], and [25].

The size of the ear images considered for all the experiments is 192×128 pixels. The central view 2D rendered sub-aperture images and the full light field images are used to test the conventional 2D and light field based PAD methods, respectively.

C. *PAD Performance*

The protocol considered for testing used 4-fold cross-validation, for each experiment the PAD system being trained with ¾ of the database and tested with the remaining ¼. The training set contains ¾ of the *Bona Fide* samples and the same number of artefact samples which are randomly selected from all PAI types. The average ACER results, obtained after 50 runs, are reported.

Benchmarking results obtained for the LLFEADB baseline set (see Table I) show that two recent light field based solutions [24] ,[25] as well as a conventional 2D solution [30] achieve perfect or near perfect classification accuracy for all PAIs considered. Concerning the LLFEADB extended set (see Table II), [24] still achieves perfect classification accuracy, while [25] and [30] show a slight reduction in PAD performance in comparison to the baseline set. In practice, the LLFEADB extended set provides a more challenging condition than the baseline for ear PAD due to two main reasons: i) the higher resolution of the images captured from the PAI makes distinguishing artefacts from *bona fide* samples more difficult for the extended set, as expected; ii) as the detection performance decreases when training uses less samples, a slight performance degradation may be also justified by the smaller size of the extended set.

Table I: ACER for the LLFEADB baseline set.

Detection solution			Presentation Attack Instrument				
Ref.	Year	Type	Laptop	Tablet	Mobile 1	Mobile 2	Average
[27]	2011	2D	7.93 %	4.94 %	5.95 %	2.11 %	5.23 %
[29]	2015	2D	5.12 %	9.29 %	5.34 %	4.80 %	6.13 %
[30]	2016	2D	**0 %**	0.15 %	**0 %**	**0 %**	0.04 %
[23]	2016	LF	3.11 %	2.09 %	1.66 %	0.57 %	1.85 %
[24]	2018	LF	0.01 %	0.02 %	**0 %**	**0 %**	0.01 %
[25]	2018	LF	**0 %**	**0 %**	**0 %**	**0 %**	**0 %**

Table II: ACER for the LLFEADB extended set.

Detection solution			Presentation Attack Instrument				
Ref.	Year	Type	Laptop	Tablet	Mobile 1	Mobile 2	Average
[27]	2011	2D	12.49 %	21.45 %	16.54 %	17.70 %	17.04 %
[29]	2015	2D	5.84 %	6.77 %	4.62 %	5.62 %	5.71 %
[30]	2016	2D	1.05 %	2.42 %	0.65 %	0.29 %	1.10 %
[23]	2016	LF	0.45 %	5.75 %	4.55 %	5.92 %	2.74 %
[24]	2018	LF	0.20 %	0.39 %	0.18 %	1.22 %	0.49 %
[25]	2018	LF	**0 %**	**0 %**	**0 %**	**0 %**	**0 %**

D. *Generalization to Unknown Attacks*

When deploying a PAD solution, there is naturally no way to know with absolute certainty what type of attacks will be performed. This paper investigates ear PAD generalization to consider an unforeseen artefact type, by training the solutions with all attack types available in LLFEADB excluding one, which is then used for testing, thus performing the role on an unknown attack. Table III and Table IV report the ACER generalization performance results obtained with 50 runs, respectively for the LLFEADB baseline and extended sets.

Table III: ACER generalization results for the LLFEADB baseline set.

Detection solution			Presentation Attack Instrument				
Ref.	Year	Type	Laptop	Tablet	Mobile 1	Mobile 2	Average
[27]	2011	2D	10.08 %	6.35 %	7.12 %	2.28 %	6.45 %
[29]	2015	2D	7.98 %	10.67 %	10.64 %	7.93 %	9.30 %
[30]	2016	2D	**0 %**	1.23 %	**0 %**	**0 %**	0.31 %
[23]	2016	LF	16.85 %	4.26 %	8.03 %	2.09 %	7.80 %
[24]	2018	LF	0.01 %	0.16 %	**0 %**	**0 %**	0.04 %
[25]	2018	LF	**0 %**	**0 %**	**0 %**	**0 %**	**0 %**

Table IV: ACER generalization results for the LLFEADB extended.

Detection solution			Presentation Attack Instrument				
Ref.	Year	Type	Laptop	Tablet	Mobile 1	Mobile 2	Average
[27]	2011	2D	16.01 %	18.75 %	16.83 %	14.59 %	16.54 %
[29]	2015	2D	7.88 %	13.49 %	4.15 %	10.11 %	10.03 %
[30]	2016	2D	1.84 %	6.25 %	0.67 %	0.53 %	2.32 %
[23]	2016	LF	0.28 %	6.72 %	5.84 %	6.15 %	4.74 %
[24]	2018	LF	0.27 %	0.43 %	0.21 %	2.22 %	0.78 %
[25]	2018	LF	**0 %**	**0 %**	**0 %**	**0 %**	**0 %**

The results show that [25] generalizes perfectly to unforeseen PAIs for both the LLFEADB baseline and extended sets. Concerning [24] and [30], even though their performance decreases compared to the performance reported in Section IV.C, their generalization abilities are superior regarding the other solutions for most considered PAIs. It should be noted that, in the absence of artefact samples captured from 3D PAIs, for instance wrapped paper or silicon ears, it is not expected to experience a significant performance degradation when considering this generalization scenario. This highlights the need for a more complete ear artefact database, notably including artefacts samples captured from 3D PAIs, to more exhaustively study ear PAD technology.

E. *Complexity Assessment*

As PAD performance comes at the cost of computational complexity, it is important to assess this trade-off. Table V shows the average extraction and classification times per image (in seconds) for the selected PAD benchmarking solutions. This Table also summarizes the descriptor sizes for the various solutions. Time measurements were performed on a standard 64-bit Intel PC with a 3.40 GHz processor and 16 GB RAM, running MATLAB R2015b. The total processing time for [24] and [25], the best performing solutions, are around 49 and 217 milliseconds per image, respectively, exhibiting the lowest computational complexity over all tested solutions. This shows that light field based solutions not only achieve very effective and stable PAD performance, but are also very fast, thus representing one step forward in biometric and forensic applications regarding regular 2D imaging solutions.

Table V: Average extraction, classification and total times, and descriptor size.

Solution			Feat. extrac. time (s)	Class. time	Total proc. time (s)	No. of vector elements/bins	Descriptor size (bytes)
Ref.	Year	Type					
[27]	2011	2D	0.9820	0.0026	0.9846	833	695
[29]	2015	2D	0.4188	0.1188	0.5376	369	339
[30]	2016	2D	0.3598	0.0095	0.3693	7,680	12,173
[23]	2016	LF	19.0351	0.0640	19.0991	12,420	93,494
[24]	2018	LF	**0.0489**	**0.0002**	**0.0492**	**96**	**158**
[25]	2018	LF	0.1016	0.1162	0.2178	37,260	274,475

V. Summary and Future Work

This paper provides the first content database, labeled LLFEADB, and benchmarking study on light field based and non-light field based solutions for ear presentation attack detection. The proposed ear artefact database includes two sets, the baseline and extended sets, adopting a different resolution for the *bona fide* artefacts acquisition. LLFEADB is captured with a Lytro ILLUM lenslet light field camera, simulating different types of presentation attacks, notably laptop, tablet and mobile phones. The state-of-the-art PAD solutions are benchmarked in terms of accuracy, generalization and complexity, using a common, meaningful representative evaluation framework. The results show very promising performance for two recent light field based solutions proposed for face PAD, also exhibiting a very low computational complexity. The LLFEADB covers artefact types captured from digital display PAIs. In the future, the creation of a more complete database, notably including artefact samples captured from 3D PAIs, and its assessment, will be considered.

VI. Acknowledgment

This work has been partially supported by Instituto de Telecomunicações under Fundação para a Ciência e Tecnologia, Grant UID/EEA/ 50008/2013.

VII. References

[1] Z. Emeršic, V. Štruc and P. Peer, "Ear recognition: More than a survey," *Neurocomputing,* vol. 255, no. 1, pp. 26-39, Sep. 2017.

[2] S. Lei and M. Qi, "Multimodal recognition method based on ear and profile face feature fusion," *International Journal of Signal Processing, Image Processing and Pattern Recognition,* vol. 9, no. 1, pp. 33-42, Jan. 2016.

[3] K. Annapurani, M. Sadiq and C. Malathy, "Fusion of shape of the ear and tragus – A unique feature extraction method for ear authentication system," *Expert Systems with Applications,* vol. 42, no. 1, p. 649–656, Jan. 2015.

[4] N. Hezil and A. Boukrouche, "Multimodal biometric recognition using human ear and palmprint," *IET Biometrics,* vol. 6, no. 5, pp. 351-359, Aug. 2017.

[5] ISO/IEC 30107-1, "Information technology—Presentation attack detection—Part 1: Framework," International Organization for Standardization, Jan. 2016.

[6] J. Galbally, S. Marcel and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," *IEEE Access,* vol. 2, no. 1, pp. 1530-1552, Dec. 2014.

[7] A. Hadid, "Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions," *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, Columbus, OH, USA, Jun. 2014.

[8] L. Li, P. Correia and A. Hadid, "Face recognition under spoofing attacks: Countermeasures and research directions," *IET Biometrics,* vol. 7, no. 1, pp. 3-14, Jan. 2018.

[9] R. Ramachandra and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," *ACM Computing Surveys,* vol. 50, no. 1, pp. 801-837, Apr. 2017.

[10] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: a survey," *IET Biometrics,* vol. 3, no. 4, pp. 219-233, Dec. 2014.

[11] R. Raghavendra and C. Busch, "Presentation attack detection algorithm for face and iris biometrics," *European Signal Processing Conference*, Lisbon, Portugal, Nov. 2014.

[12] R. Raghavendra and C. Busch, "Robust scheme for iris presentation attack detection using multiscale binarized statistical image features," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 4, pp. 703-715, Feb. 2015.

[13] R. Ng, M. Levoy, M. Bradif, G. Duval, M. Horowitz and P. Hanrahan, "Light field photography with a hand-held plenoptic camera," Tech Report CSTR 2005-02, Stanford, CA, USA, Feb. 2005.

[14] M. Levoy and P. Hanrahan, "Light field rendering," *Computer Graphics and Interactive Techniques*, New York, NJ, USA, Aug. 1996.

[15] F. Pereira and E. Silva, "Efficient plenoptic imaging representation: Why do we need it?," *IEEE International Conference on Multimedia and Expo*, Seattle, WA, USA, Jul. 2016.

[16] R. Raghavendra,, K. Raja and C. Busch, "Exploring the usefulness of light field cameras for biometrics: An empirical study on face and iris recognition," *IEEE Transactions on Infromation Forensics and Security,* vol. 11, no. 5, pp. 922-936, May 2016.

[17] R. Raghavendra, B. Yang, K. Raja and C. Busch, "A new perspective — Face recognition with light-field camera," *International Conference on Biometrics*, Madrid, Spain, Jun. 2013.

[18] A. Sepas-Moghaddam, P. Correia and F. Pereira, "Light field local binary patterns description for face recognition," *IEEE International Conference on Image Processing*, Beijing, China, Sep. 2017.

[19] A. Sepas-Moghaddam, F. Pereira and P. Correia, "Ear recognition in a light field imaging framework: A new perspective," *IET Biometrics,* in press.

[20] A. Sepas-Moghaddam, V. Chiesa, P. Correia, F. Pereira and J. Dugelay, "The IST-EURECOM light field face database," *International Workshop on Biometrics and Forensics*, Coventry, UK, Apr. 2017.

[21] R. Raghavendra, K. Raja and C. Busch, "Presentation attack detection for face recognition using light field camera," *IEEE Transactions on Image Processing,* vol. 24, no. 3, pp. 1060-1075, Mar. 2015.

[22] S. Kim, Y. Ben and S. Lee, "Face liveness detection using a light field camera," *Sensors,* vol. 14, no. 12, pp. 71-99, Nov. 2014.

[23] Z. Ji, H. Zhu and Q. Wang, "LFHOG: A discriminative descriptor for live face detection from light field image," *IEEE International Conference on Image Processing*, Phoenix, AZ, USA, Sep. 2016.

[24] A. Sepas-Moghaddam, L. Malhadas, P. Correia and F. Pereira, "Face spoofing detection using a light field imaging framework," *IET Biometrics,* vol. 7, no. 1, p. 39 – 48, Jan. 2018.

[25] A. Sepas-Moghaddam, F. Pereira and P. Correia, "Light field based face presentation attack detection: Reviewing, benchmarking and one step further," *IEEE Transactions on Information Forensics and Security,* in press.

[26] "Lytro website," Lytro Inc, [Online]. Available: https://www.lytro.com. [Accessed Jan. 2018].

[27] J. Määttä, A. Hadid and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," *International Joint Conference on Biometrics* , Washington, DC, USA, Oct. 2011.

[28] J. Maatta, A. Hadid and M. Pietikainen, "Face spoofing detection from single images using texture and local shape analysis," *IET Biometrics,* vol. 1, no. 1, pp. 3-10, Mar. 2012.

[29] A. Hadid, N. Evans, S. Marcel and J. Fierrez, "Biometrics systems under spoofing attack: An evaluation methodology and lessons learned," *IEEE Signal Processing Magazine,* vol. 32, no. 5, pp. 20-30, Sep. 2015.

[30] Z. Boulkenafet, J. Boulkenafet and A. Hadid, "Face spoofing detection using colour texture analysis," *IEEE Transactions on Information Forensics and Security,* vol. 11, no. 8, pp. 1818-1830, Aug. 2016.

[31] D. Wen, H. Han and A. Jain, "Face spoof detection with image distortion analysis," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 4, pp. 746-761, Apr. 2015.

[32] J. Yang, Z. Lei and S. Li, "Learn convolutional neural network for face anti-spoofing," arXiv preprint:1408.5601, Ithaca, NY, USA, Aug. 2014.

[33] D. Menotti, G. Chiachia and A. Pinto, "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 4, pp. 864-879, Apr. 2015.

[34] L. Li, X. Feng, Z. Boulkenafet, Z. Xia, M. Li and A. Hadid, "An original face anti-spoofing approach using partial convolutional neural network," *International Conference on Image Processing Theory Tools and Applications*, Oulu, Finland, Dec. 2016.

[35] L. Feng, L. Po and Y. Li, "Integration of image quality and motion cues for face anti-spoofing: A neural network approach," *Journal of Visual Communication and Image Representation,* vol. 38, no. 1, pp. 451-460, Jul. 2016.

[36] A. Alotaibi and A. Mahmood, "Deep face liveness detection based on nonlinear diffusion using convolution neural network," *Signal, Image and Video Processing,* vol. 11, no. 4, pp. 713-720, May 2017.

[37] "Lytro Desktop 4," Lytro, Inc., [Online]. Available: https://support.lytro.com/hc/en-us/articles/202590364-Lytro-Desktop-4-Main-Overview. [Accessed Jan. 2018].

[38] D. Dansereau, "Light Field Toolbox V. 0.4," [Online]. Available: http://www.mathworks.com/matlabcentral/fileexchange/49683-light-field-toolbox-v0-4. [Accessed Jan. 2018].

ISBN 978-90-827970-1-5 © EURASIP 2018