I.J. Image, Graphics and Signal Processing, **2019, 2, 15-20**
Published Online February 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2019.02.02

Score-Level-based Face Anti-Spoofing System Using Handcrafted and Deep Learned Characteristics

Omid. Sharifi
Department of Computer and Software Engineering, Toros University, Mersin, Turkey
Email: omid.sharifi@toros.edu.tr

Received: 04 January 2019; Accepted: 20 January 2019; Published: 08 February 2019

***Abstract*—**Recognition performance of biometric systems is affected through spoofing attacks made by fake identities. The focus of this paper is on presenting a new scheme based on score level and decision level fusion to monitor individuals in term of real and fake. The proposed fake detection scheme involve consideration of both handcrafted and deep learned techniques on face images to differentiate real and fake individuals. In this approach, convolutional neural network (CNN) and overlapped histograms of local binary patterns (OVLBP) methods is used to extract facial features of images. The produced matching scores provided by CNN and OVLBP then combined to form a fused score vector. Finally, the last decision on real and attack images is done by combining decisions of hybrid scheme using majority vote of CNN, OVLBP and their fused vector. Experimental results on public spoof databases such as Print-Attack and Replay-Attack face databases demonstrate the strength of the proposed anti-spoofing method for fake detection.

***Index Terms*—**Spoof detection, handcrafted texture extraction, convolutional neural network, decision level fusion, score level fusion.

I. INTRODUCTION

Currently, the use of biometric recognition systems in term of identification and/or verification of individuals according to their physical or behavioral characteristics is extensively studied in situations with high security demands [1-10]. In fact, the ability of biometrics to improve recognition performance and security of applications considered as increasing interest of researchers compared to conventional techniques such as token-based and knowledge-based methods. On the other hand, technology development causes vulnerability of biometric systems to fake samples specially through image acquisition step [1,11-13]. Previously, the aim of biometric systems was only to recognize the individuals without considering the spoof attacks. In general, the attacks on biometric systems are categorized into direct and indirect attacks [14]. The concentration of direct attacks is on biometric sensors in order to submit a fake template with the aim of impersonating a real user. Generally, to apply direct attacks, attackers don’t need to have any knowledge about different parts of biometric system such as feature extractors and matching techniques. Liveness, texture and motion detection techniques are considered as primary methods to counter this kind of attack. On the other hand, to present indirect attacks, attacker needs to be aware of specific information about the system such as template format and communication protocol. Furthermore, access to internal parts of the system physically or logically is needed for attackers. Countermeasures in this kind of attack include physical or logical security aspects.

The main interest of this study is on direct or spoofing attacks specifically print and video attack for face biometric. Print attack aims to spoof biometric systems by printing modality images of individuals, while video attack concentrates on spoofing by submitting video sequences of live individuals on a screen to biometric systems in term of fixed or hand-held to avoid liveness detection. Spoof detection in biometrics is quite challenging and therefore has encouraged the biometric society to investigate the effect of this kind of counterfeit events on different modalities such as face, iris, fingerprint, multimodal biometric systems, etc. [11-22]. As abovementioned, texture, motion and liveness analyses can be considered in biometric systems to counter spoofing attacks [14, 23-25]. In general, the focus of texture analysis is on detecting texture patterns such as print failures and overall image blur to detect attacks. On the other hand, motion detection concentrates on motion features of patterns such as optical flow to overcome the problem of certain texture patterns dependency. Spoof detection using liveness analysis attempts to solve the problem by focusing on vitality signs of biometric characteristics and analyzing spontaneous movements such as eye blinking and lip movements in 2D recognition systems. However, taking into account a global solution to all kinds of attacks is not possible because of nature of attacks, biometric characteristics and spoof detection approaches.

This paper proposes a novel solution based on score level and decision level fusion against print and video attacks. The facial features are extracted using convolutional neural network (CNN) [26, 27] and overlapped histograms of local binary patterns (OVLBP) [28] methods. The strength of handcrafted and deep learnt features is then combined through score level fusion. Weighted sum rule (WS) fusion strategy is used in this paper to fuse the scores. Finally, the last decision is made by combining the decisions of each classifier (OVLBP, CNN and score level fusion). Majority voting is employed in this study to fuse the results of classifiers by outputting the label with majority of the votes. Therefore, the contribution of the proposed scheme can be reviewed as: proposing a robust face anti-spoofing method with print and video attacks, the use of score and subsequently decision level fusion strategies improves detection performance of proposed methods with consideration of lower computational burden compared to schemes involving feature level fusion. The experiments performed on publicly available Idiap Print-Attack [29] and Replay- Attack [30] face spoofing databases demonstrate the superiority of proposed anti-spoofing method in term of detection performance, computational complexity and reduction in detection alteration.

On the other hand, the key issue and core technologies of this study can be summarized as: applying OVLBP feature extractor as an strong and popular handcrafted method, and therefore considering more local primitive textures for better video and print spoofing attack detection, considering deep learning feature extraction method as a powerful anti-spoofing extractor, combining the methods using two level of fusions in order to improve the detection rate, and then comparing the proposed method with state-of-the-art handcrafted and deep-learnt methods in field of print and video attacks.

The rest of paper is ordered as follows. Section 2 involves previous studies of spoofing attacks and protection techniques in field of biometrics. The concentration of sections 3 and 4 is on handcrafted and deep learnt techniques applied in this study for spoof detection. In section 5, the overall architecture of proposed scheme is described. The demonstration of experimental results and databases is presented in section 6. Finally, Section 7 provides conclusion of this study.

II. Related Works

The problem of spoof attack detection for face biometric has been studied recently using different handcrafted and deep learnt techniques [12, 16, 23-25,31-38]. In [16], a novel double anti-spoofing pipeline has been proposed for face biometrics based on selection of optimized textures and image quality assessment techniques for print and video attacks. The paper applied different texture and image quality algorithms to compare the ability of their proposed framework. Effectiveness of applying multiple techniques to detect print attack for face biometric has been studied in [23]. The authors of this study compared several methods based on motion analysis, texture analysis and liveness detection for detection of 2D facial print-based spoof attacks. The use of liveness detection for evaluation of trajectory of different parts of face has been presented in [24] using the optical flow of lines successfully. In fact, they used a model-based local Gabor decomposition and Support Vector Machine (SVM) experts to detect different parts of face in their liveness proposed detection method. In [25], a holistic liveness detection paradigm has been proposed for face biometric to detect spoof attacks. The authors suggested fusion of anti-spoofing methods in interactive situations for obtaining reliable liveness detection strategy. In [31], image quality assessment strategy is used to propose a novel software-based spoof detection framework. The authors of this study employed 25 different image quality features to distinguish fake samples. A face anti-spoofing framework for video attack has been proposed in [32] using motion magnification. The proposed method developed performance of LBP feature extractor to detect attacks. The authors of this study used a motion estimated based method using Histogram of Oriented Optical Flow (HOOF) descriptor for Print-Attack and Replay-Attack databases effectively. The researchers of [33] employed multi-scale LBP method to transform the micro-textures into an improved feature histogram for face fake detection. The classification of fake and real samples has been done in their study using SVM. In [34], the structures and dynamics of facial micro-textures have been applied to propose an anti-spoofing technique on Replay-Attack and CASIA Face Anti-Spoofing databases. The concentration of authors of [35] for spoof detection is on image distortion analysis (IDA) method to exploit specular reflection, blurriness, chromic moment, and color diversity feature of 2D face images. On the other hand, the authors of [12] applied two different deep learning methods to detect attacks in several biometric recognition systems such as iris, face, and fingerprint. Although, their experimental results demonstrated the high detection performance of deep learning technique, but it was not able to improve always the detection rate specifically for face biometric. In [36], a new method based on feature level fusion strategy is used to combine handcrafted and deep learnt facial features in order to improve the spoof detection. They applied SVM classifier to differentiate real and fake identities.

The concentration of current study therefore is to combine both handcrafted and deep learnt methods with proposing a novel scheme. The proposed scheme considers a robust face anti-spoofing method for both print and video attacks. Employing combination strategy using score and decision level fusion leads to detection performance improvement.

III. Handcrafted Facial Texture Extraction Using Ovlbp

The feature extraction step of this study considers an extension of LBP texture extractor called OVLBP in order to describe the local spatial structure of face images. In general, LBP introduced by Ojala et al. as a gray-scale and powerful subpattern-based texture operator for analyzing face biometric [37]. By using LBP texture extractor images are divided into several blocks and subsequently local textures of blocks are extracted. In fact, histogram extraction of features associated to the patterns on a set of pixels in each block is performed and then concatenating the local extracted features is done to present a single global feature vector. Therefore, binary patterns are calculated by comparing its value with those of its neighbor according to a central pixel in an image. The concentration of first version of LBP for feature extraction is done on a 3 × 3 window size which leads to preventing large scale structures capturing. However, Uniform Local Binary Pattern (ULBP) [28] as extension of original version focuses on implementation of the operator to circular neighborhoods with a different radius size to solve the problem of basic LBP. The main goal of uniform LBP is to provide an independent output label for each uniform pattern of mapping while for non-uniform patterns a single output label is considered.

In general, the use of histogram-based methods for face spoof scenarios to detect attacks specifically print and video attacks has been considered as sufficient factor in several studies [16, 18, 32-34]. This study applies idea of overlapped LBP histograms to obtain more significant histograms as handcrafted facial texture extractor for print and video attacks. In OVLBP method [28], images are divided into overlapped blocks with the aim of achieving more sub-windows over the image. Therefore, the extracted sub-windows contain micro-textons of more local primitive textures related to spots, flat areas, edges, edge ends and curves [28]. The extracted textures from small windows usually include more specific and precise texture information because of involving more informative histograms of overlapped regions and consequently capable to better managing of print and video attacks in face spoofed framework. All the face images are divided into 36 sub-regions of 10 × 10 window size without and with 50% overlapping of sub-regions in this study.

IV. Deep Learning Extraction Using CNN

In order to include more representative feature set of information in the proposed method, the paper attempts to apply CNN learning-based strategy to improve the detection rate of print and video attacks. In general, any CNN structure contains two significant layers called convolutional layers and fully connected layers. The convolutional layer aims to extract image features and manipulate them using the convolution operation. A training process is needed based on the characteristics of images to achieve filter coefficients. In order to make the final CNN structure, consideration of a cross-channel normalization layer, a rectified linear unit (ReLU) and a pooling layer is needed for each convolutional layer. Finally, the constructed feature map is sent to fully-connected layers for further classification.

The construction of CNN method for the anti-spoofing proposed framework to extract the deep facial features is based on VGG-16 architecture introduced by the Oxford Visual Geometry Groups' model in ImageNet Large-Scale Visual Recognition Challenge (ILSVRC) [39]. Compared to earlier version of CNN structure VGG-16 is more extensive and richer with including five batches of convolution operations. Fig.1 illustrates the architecture of VGG-16. In general, each batch includes 2–3 adjacent convolution layers connected via max-pooling layers. All convolution layers consist of kernel sizes of 3 ×3 with same number of kernels inside each batch starting 64 in the first group to 512 in the last one.

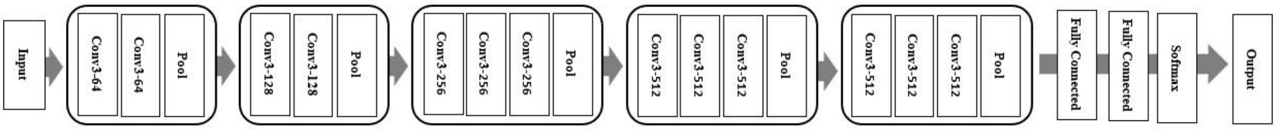

Fig.1. The architecture of VGG-16.

Since in spoof detection method only two type of classes as real and fake is used, the number of output neurons in the last layer of model is changed to two. On the other hand, in order to reduce the overfitting affection of training step of CNN, this study employs different learning rate policy for different layers. Furthermore, data augmentation technique by cropping different regions of input and their fillips is used in training part of this work.

V. Proposed Anti-Spoofing Scheme

The proposed anti-spoofing framework detects print and video attacks in face databases based on score level and decision level fusion strategies as depicted in Fig.2. The facial features are extracted using CNN and OVLBP methods in order to improve the ability of the proposed method for detecting print and video attacks. This study considers score level fusion due to ease in accessing, simplicity, low computational complexity and usually similar and/or equivalent performance compared to feature level fusion. Therefore, the proposed method first produces the scores of handcrafted and deep learnt facial extractors using Manhattan Distance technique and then the produced scores are combined using weighted sum rule (WS) strategy.

In general, weighted sum rule technique combines the matching scores of individual matchers. In this study, computation of weights is performed according to quality of individual classifiers in term of performance improvement. Weighted sum rule of different matching scores is shown as equation 1.

$$ws = w_1 \times s_1 + w_2 \times s_2 + \cdots + w_n \times s_n \qquad (1)$$

Where $w_1, w_2, \dots, w_n$ are the computed weights for different classification methods and $s_1, s_2, \dots, s_n$ are the set of matching scores.

Nearest neighbor classifier (NNC) is then applied on set of calculated scores to provide singular classification of each set of score. Finally, the last decision as real or attack is made by combining the decisions of each classifier (OVLBP, CNN and score level fusion) using majority votes of the three classifiers in this study. Majority voting combines the results of classifiers by outputting the label with majority of the votes.

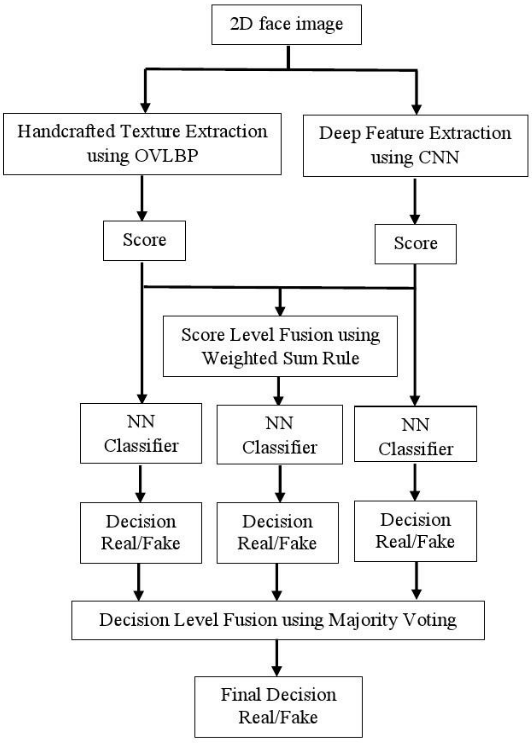
2D face image
Handcrafted Texture Extraction using OVLBP
Deep Feature Extraction using CNN
Score
Score
Score Level Fusion using Weighted Sum Rule
NN Classifier
NN Classifier
NN Classifier
Decision Real/Fake
Decision Real/Fake
Decision Real/Fake
Decision Level Fusion using Majority Voting
Final Decision Real/Fake

Fig.2. The proposed anti-spoofing framework.

VI. Experimental Results and Databases

In order to evaluate the performance of the anti-spoofing method, Idiap Print-Attack and Repla-Attack databases are employed in this study. Print-Attack database consists of 200 short videos of printed photograph and real-access of 50 individuals while Repla-Attack databases contains 1300 video clips of photograph and video attack access of 50 individuals under different lighting conditions. In order to perform the experiments, this study first detected the face images from video sequences and then the detected face images were aligned according to center position of left and right irises. This study randomly, assigned 30 subjects for training and 20 persons for testing to extract the real and attack images from videos. In total, in order to perform the experiments, 750 real access images, 750 print attack images and 1000 video attack images were extracted from the videos in this work. Therefore, training dataset contains 450 real, 450 print attack and 600 video attack images while the number of images for real, print attack and video attack in test dataset is 300, 300 and 400 respectively. The division of datasets into train and test is done three times and the averaged result of these three sets is reported in this study.

In order to perform the experiments in CNN part of the proposed method, the images are resized to 256 ×256 size. The data augmentation part of training contains ten different cropped size of 227 ×227 and their flip. Therefore, train augmented database takes into consideration of 9000 real, 9000 print attack and 12000 video attack images. In order to avoid overfitting of training data this study also considered the regularization as 0.1, momentum parameters as 0.9 and learning rate as 0.001 with batch size of 32. The process of training is done for 50 epochs. Half Total Error Rate (HTER) that is half of sum of False Genuine Rate (FGR) and False Fake Rate (FFR) of spoof detection errors is considered as evaluation protocol of proposed anti-spoofing method in this study.

The first set experiments done in this study concentrates on applying handcrafted texture extraction method for print and video attacks and comparison with some other handcrafted methods in field of fake detection. In order to classify the images nearest-neighbor classifier (NN) is applied for all the implemented methods. In general, NN is a method of data classification to approximate how likely a data point is to be a member of one group. In fact, the algorithm classifies a sample according to the category of its nearest neighbor.

Table 1. Results of applying handcrafted texture extraction methods for print and video attacks in HTER (%)

Method	Print-Attack HTER (%)	Video-Attack HTER (%)
Gabor [33]	37.45	37.30
LBP [38]	18.26	22.18
HOG [40]	25.40	27.47
IQA [31]	34.72	33.35
OVLBP	**14.35**	**15.75**

Analyzing the results of Table 1 shows the superiority of OVLBP for both print and video attacks as 14.35% and 15.75%. As shown in the table, all LBP based methods outperform other implemented handcrafted methods for video and print attacks. It should be stated that, in order to apply image quality assessment method, mean-squared error (MSE) measurement is used in this study. On the other hand, in order to investigate the effect of CNN on print and video attacks another set of experiment was performed in Table 2, using only CNN and CNN + OVLBP with Score Level Fusion. Selection of OVLBP here is due to providing better detection performance in term of HTER for spoofing in this study.

As depicted in Table 2, employing CNN in both scenarios with and without the handcrafted feature extractor leads to detection improvement for both print and video attacks. However, in case of applying only CNN (without OVLBP combination) video attack achieved better detection in term of HTER in this study.

Generally, combining CNN and OVLBP using score level fusion achieved 4.05% and 3.20% spoof detection rate enhancement over applying only CNN against print and video attacks respectively in this work. Moreover, in order to examine the effect of proposed scheme against video and print attack the paper compare the result of applying only handcrafted, CNN and CNN + OVLBP + Score Level Fusion with the proposed scheme as the last set of experiment in Table 3.

Table 2. Results of applying CNN and combination of CNN and handcrafted texture extraction methods using score level fusion for print and video attacks in HTER (%)

Method	Print-Attack HTER (%)	Video-Attack HTER (%)
CNN	14.45	14.20
CNN + OVLBP using Score Level Fusion	**10.40**	**11.00**

Table 3. Results of applying proposed method for print and video attacks in HTER (%)

Method	Print-Attack HTER (%)	Video-Attack HTER (%)
OVLBP	14.35	15.75
CNN	14.45	14.20
CNN + OVLBP + Score Level Fusion	10.40	11.00
Proposed Method	8.50	8.65

The experiments performed in Table 3 demonstrate the effectiveness of proposed anti spoofing method based on score and decision level fusion strategy for both print and video attacks. The general analysis of table however shows detection of print attack is more successful using combination of CNN and handcrafted methods with score level fusion and decision level fusion according to the experiments done in this study. The proposed scheme obtained 5.85% and 7.10% improvement over using only OVLBP for print and video attacks. In addition, improvement of 5.95% and 5.55% detection rate in term of print and video attack detection over employing just CNN extractor.

VII. Conclusion

This paper presented a new anti-spoofing method based on combination of CNN and handcrafted techniques in two level of fusion against print and video attacks. The proposed method first applied handcrafted and CNN methods to extract the facial features and then the computed scores of each method along with combination of them using weighted sum rule strategy are sent to a decision level fusion for further spoof detection. The paper improved the detection rate of attack by combining the decisions obtained from CNN, OVLBP and fused scores of these two methods. Performing different set of experiments in this study showed the effectiveness of print attack over video attacks detection through proposed scheme. The concentration of this paper for experiments was on Idiap Print-Attack and Repla-Attack face spoofing databases with 50 individuals. The proposed method has 5.85% improvement over only using handcrafted texture analysis for print attack while video attack over handcrafted technique obtained 7.1% improvement in this study.

References

[1] A.K Jain,.; A.Ross,; Prabhakar, S. An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. 2004, 14, 4–20.

[2] A. K., Jain, S. Z Li,. Handbook of face recognition. New York: springer, 2011.

[3] M. Ç. Yildiz, O.Sharifi, and M. Eskandari, Log-Gabor Transforms and Score Fusion to Overcome Variations in Appearance for Face Recognition, International Conference on Computer Vision and Graphics, – Proceedings of International Conference on Computer Vision and Graphics, ICCVG 2016, Warsaw, Poland, September 19-21, 2016. Springer 2016 Lecture Notes in Computer Science.

[4] H. S. Bhatt., S. Bharadwaj, R. Singh,& M, Vatsa. Recognizing surgically altered face images using multiobjective evolutionary algorithm. IEEE Transactions on Information Forensics and Security, 2013, 8(1), 89-100.

[5] O. Sharifi, M. Eskandari, and M. Ç Yildiz., Scheming an Efficient Facial Recognition System using Global and Random Local Feature Extraction Methods, 2nd International Conference on Computer Science and Engineering UBMK'17, October 5-8, 2017, Antalya, Turkey, DOI: 10.1109/UBMK.2017.8093508.

[6] D. Zhang, Z. Guo, G. Lu,.; L. Zhang,; Y. Liu,; W. Zuo, Online joint palmprint and palmvein verification. Expert Syst. Appl. 2011, 38, 2621–2631.

[7] M. Eskandari, O. Sharifi. Optimum scheme selection for face–iris biometric. IET Biometrics, 2016, 6(5), 334-341.

[8] K. Nguyen, C. Fookes,; R. Jillela,; S. Sridharan,; A. Ross,. Long range iris recognition: A survey. Pattern Recognit. 2017, 72, 123–143.

[9] O. Sharifi, M. Eskandari, Optimal Face-Iris Multimodal Fusion Scheme. Symmetry, 2016, 8(6), 48.

[10] D.T Pham, Y.H. Park, D.T Nguyen, S.Y. Kwon,; K.R Park,. Nonintrusive finger-vein recognition system using NIR image sensor and accuracy analyses according to various factors. Sensors 2015, 15, 16866–16894.

[11] D.T. Nguyen, H.S. Yoon, D.T. Pham,; K.R Park,. Spoof detection for finger-vein recognition system using NIR camera. Sensors 2017, 17, 2261.

[12] D. Menotti, G. Chiachia,; A. Pinto, W.R Schwartz, H. Pedrini,; A.X. Falcao,; A. Rocha, Deep representation for iris, face and fingerprint spoofing detection. IEEE Trans. Inf. Forensic Secur. 2015, 10, 864–879.

[13] K.R. Nalini, H.C. Jonathan, M.B. Ruud,: An analysis of minutiae matching strength. In: Audio- and Video-Based Biometric Person Authentication, Proceedings of 3rd AVBPA ed.,2001, vol. 2091, pp. 223–228.

[14] M. JMarcos, F. Julian, , et al.: An evaluation of indirect attacks and countermeasures in fingerprint verification systems. Pattern Recognit. Lett. 2011, 32(12), 1643–1651.

[15] T. Santosh, P. Norman, et al.: Detection of face spoofing using visual dynamics. IEEE Trans. Inf. Forensics Secur. 2015, 10(4), 762–777.

[16] M., Eskandari, & O.Sharifi, Designing Efficient Spoof Detection Scheme for Face Biometric. In International Conference on Image and Signal Processing, 2018, July; pp. 427-434. Springer, Cham.

[17] A. Anjos, M.M. Chakka, S. Marcel,: Countermeasures to photo attacks in face recognition. Biom. IET, 2014, 3(3), 147–158.

[18] P. Gupta, et al. "On iris spoofing using print attack." Pattern Recognition (ICPR), 2014 22nd International Conference on. IEEE, 2014.

[19] H. Abdenour, G. Mohammad, et al.: Can gait biometrics be spoofed. In: 2012 21st International Conference on Pattern Recognition.

[20] B. Biggio, Z. Akhtar, G. Fumera, , G. L Marcialis., & F. Roli,. Security evaluation of biometric authentication systems under real spoofing attacks. IET biometrics, 2012, 1(1), 11-24.

[21] M. Gomez-Barrero, G. Javier, and F. Julian. "Efficient software attack to multimodal biometric systems and its application to face and iris fusion." Pattern Recognition Letters 36, 2014: 243-253.

[22] A., Zahid, S. Kale, and N. Alfarid. "Spoof attacks on multimodal biometric systems." Proc. International Conference on Information and Network Technology (IPCSIT). Vol. 4. 2011.

[23] M.M. Chakka, A. Anjos, et al.: Competition on counter measures to 2D facial spoofing attacks. In: 2011 International Joint Conference on Biometrics.

[24] K. Kollreider, H. Fronthaler, J. Bigun, Evaluating liveness by face images and the structure tensor. In: Automatic Identification Advanced Technologies, 2005.

[25] K. Kollreider, H. Fronthaler, J. Bigun, Verifying Liveness By Multiple Experts In Face Biometrics. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 2008.

[26] A. Krizhevsky, I. Sutskever, G.E Hinton, ImageNet classification with deep convolutional neural networks. In Proceedings of the Advances in Neural Information Processing Systems, Lake Tahoe, NV, USA, 3–8 December 2012.

[27] P.N. Druzhkov , V.D. Kustikova , A survey of deep learning methods and soft-ware tools for image classification and object detection, Pattern Recognit. Image Anal. 26 (1) (2016) 9–15.

[28] Z. Guo, D. Zhang, D. Zhang, A completed modeling of local binary pattern operator for texture classification. IEEE Transactions on Image Processing, 19(6) (June 2010) 1657-1663.

[29] Print Attack face database, https://www.idiap.ch/dataset/printattack, Accessed October 2014.

[30] Replay Attack face database, https://www.idiap.ch/dataset/replayattack, Accessed October 2014.

[31] J. Galbally, M. Sébastien and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition." IEEE transactions on image processing 23.2 (2014): 710-724.

[32] Samarth, et al. "Computationally efficient face spoofing detection with motion magnification." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2013.

[33] J. Määttä, H. Abdenour, and P. Matti. "Face spoofing detection from single images using micro-texture analysis." Biometrics (IJCB), 2011 international joint conference on. IEEE, 2011.

[34] P. de Freitas, Tiago, et al. "Face liveness detection using dynamic texture." EURASIP Journal on Image and Video Processing 2014.1 (2014): 1-15.

[35] D. Wen, H. Hu, and A. K. Jain. "Face spoof detection with image distortion analysis." IEEE Transactions on Information Forensics and Security 10.4 (2015): 746-761.

[36] D. Nguyen, Tien, et al. "Combining Deep and Handcrafted Image Features for Presentation Attack Detection in Face Recognition Systems Using Visible-Light Camera Sensors." Sensors 18.3 (2018): 699.

[37] T. Ojala, M. Pietikäinen, D. Harwood: A comparative study of texture measure with classification based on feature distributions. Pattern Recognit. 29, 51–59.

[38] A. Benlamoudi; D. Samai.; A. Ouafi.; S.E Bekhouche, A. Taleb-Ahmed, Hadid, Face spoofing detection using local binary patterns and Fisher score. In Proceedings of the 3rd International Conference on Control

[39] K. Simonyan; A. Zisserman, Very deep convolutional neural networks for large-scale image recognition. In Proceedings of the International Conference on Learning Representations, Kunming, China, 25–27 September 2013.

[40] A. Pinto, et al. "Using visual rhythms for detecting video-based facial spoof attacks." IEEE Transactions on Information Forensics and Security 10.5 (2015): 1025-1038G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529–551, April 1955.

Author’s Profile

Omid. Sharifi received his Ph.D. degree from the Department of Computer Engineering, Eastern Mediterranean University, North Cyprus in 2014. Currently, he is an Assistant professor in the Department of Computer and Software Engineering, Toros University, Turkey. His current research interests include biometrics, face recognition, iris recognition and multimodal fusion.

How to cite this paper: Omid. Sharifi, "Score-Level-based Face Anti-Spoofing System Using Handcrafted and Deep Learned Characteristics", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.11, No.2, pp. 15-20, 2019.DOI: 10.5815/ijigsp.2019.02.02