Çukurova Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 35(4), ss. 1103-1110, Aralık 2020
Çukurova University Journal of the Faculty of Engineering and Architecture, 35(4), pp. 1103-1110, December 2020

Face Anti-Spoofing Scheme Using Handcraft Based and Deep Learning Methods

Omid SHARIFI[*1]

[1]*Toros University, Engineering Faculty, Software Engineering Department, Mersin*

Geliş tarihi: 23.11.2020 *Kabul tarihi: 30.12.2020*

Abstract

Malicious parties which impersonate systems by fake identities affect recognition performance of biometric systems. This study focuses on a strength anti-spoofing scheme based on decision level fusion to monitor individuals in term of real and fake. The proposed fake detection scheme involves consideration of both handcrafted and deep learned techniques on face images to differentiate real and fake individuals. In this context, convolutional neural network (CNN) and Log-Gabor filter methods are used to learn deep representations and extract facial features of images respectively. In order to improve the robustness of proposed anti-spoofing framework, fusion of Log-Gabor and CNN methods is considered by applying decision-level-fusion technique. Finally, the performance of proposed anti-spoofing scheme is examined on public spoof databases such as Print-Attack and Replay-Attack face databases to detect fake facial images.

Keywords: Spoof attacks, Handcrafted texture extraction, Convolutional neural network, Decision level fusion

El Yapımı Tabanlı ve Derin Öğrenme Yöntemlerini Kullanan Yüz Yanıltma Önleme Şeması

Özet

Sahte kimliklerle sistemleri taklit eden kötü niyetli kişiler, biyometrik sistemlerin tanınma performansını etkilemektedir. Bu çalışma, bireyleri gerçek ve sahte terimlerle izlemek için karar düzeyinde füzyona dayalı güçlü bir sahtekarlık önleme şemasına odaklanmaktadır. Önerilen sahte tespit şeması, gerçek ve sahte bireyleri ayırt etmek için yüz görüntülerinde hem el yapımı hem de derin öğrenme tekniklerinin dikkate alınmasını içerir. Bu bağlamda, evrişimsel sinir ağı (CNN) ve Log-Gabor filtre yöntemleri sırasıyla görüntülerin derin temsillerini öğrenmek ve görüntülerin yüz özelliklerini çıkarmak için kullanılmaktadır. Önerilen sahteciliği önleme çerçevesinin sağlamlığını geliştirmek için, Log-Gabor ve CNN yöntemlerinin füzyonu, karar seviyesinde füzyon tekniği uygulanarak değerlendirilmiştir. Son olarak, önerilen sahteciliği önleme planının performansı, sahte yüz görüntülerini tespit etmek için Print-Attack ve Replay-Attack gibi halka açık veri tabanlarında incelenmiştir.

Anahtar Kelimeler: Sahte saldırılar, El yapımı doku çıkarma, Evrişimsel sinir ağı, Karar düzeyinde füzyon

[*]Sorumlu (Corresponding author) yazar: Omid SHARIFI, *omid.sharifi@toros.edu.tr*

1. INTRODUCTION

In biometric recognition systems a spoofing attack is done by a person or agent to gain an illegitimate access to identify as another by falsifying data. In this area, some important types of attacks can be considered as replay video attack, digital photo attack, printed photo attack, and mask attack [1]. Typically, direct and indirect attacks are investigated on biometric systems [2]. The goal of direct attacks is to consider biometric sensors for impersonating a fake template as a genuine. In fact, the attackers to apply the direct attack don't require any knowledge about details of biometric system such as feature extractors and matching techniques. In order to counter direct attacks, the primary techniques such as liveness, texture and motion detection methods are generally applied. On the other hand, the concentration of indirect attacks is based on awareness of certain information about the system such as template format and communication protocol by attackers. Additionally, the attackers require to access internal parts of the system physically or logically and therefore countermeasures for indirect attacks involve physical or logical security aspects. The concentration of this study is on direct or spoofing attacks specially print and video attack in the area of face biometric. The main goal of print attack is to spoof biometric systems by printing modality images of subjects, whereas video attack focuses on spoofing using video sequences of live subjects on a screen to biometric systems in term of fixed or hand-held to prevent liveness detection. In general, spoof detection is quite challenging in the biometric area and accordingly the investigation of its effect on different modalities such as face, iris, fingerprint, multimodal biometric systems, etc. is encouraged [2-13]. Typically, texture, motion and liveness analyses are common techniques in biometric systems to counter spoofing attacks [2,14-16]. Texture analysis technique concentrates on texture patterns such as print failures and overall image blur to detect the attacks. While motion detection emphasizes on motion features of patterns such as optical flow to alleviate the problem of certain texture patterns dependency. On the other hand, liveness detecting techniques overcome the problem of spoofing by consideration of vitality signs of biometric characteristics and analyzing spontaneous movements such as eye blinking and lip movements. Therefore, consideration of a global approach for all types of attacks is not possible due to the nature of attacks, biometric traits and spoof detection techniques.

In this paper, the aim is to propose a novel solution based on decision level fusion against video and print attacks. The facial images are used to learn deep representation and extract texture information of individuals using convolutional neural network (CNN) [17,18] and Log-Gabor filter [19] methods respectively. The strength of handcrafted and deep learnt features is then combined through decision level fusion (DLF) with OR rule. As a strong and popular handcrafted method Log-Gabor feature extracts the phase information of face to encode the unique pattern of facial images into bit-wise biometric template. In addition, considering deep learning method as a powerful anti-spoofing technique improves the detection rate. The contribution of the proposed scheme can be considered as: proposing a robust face spoof detection scheme concentrating on print and video attacks. The use of both handcrafted and deep learnt decisions enhances detection performance of the anti-spoofing framework with consideration of both methods advantages. The experiments are performed on two publicly available face spoofing databases namely Idiap Print-Attack [20] and Replay- Attack [21] to represent the robustness of proposed anti- spoofing method in term of detection performance, computational complexity and reduction in detection alteration.

The rest of paper is organized 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.

2. RELATED WORKS

The anti-spoofing methods for face biometric has been studied recently using different handcrafted and deep learnt techniques [4,7,14-16,22-29]. In [27] multi-level local binary (MLBP) and CNN schemes has been proposed to obtain hybrid features from two different exploited feature vectors. To classify face images as real or fake support vector machine (SVM) has been utilized on the hybrid features. The authors of [7] a double anti-spoofing pipeline method employed to select optimized textures of face image and image quality assessment techniques for print and video attacks. Finally, the paper applied different texture and image quality algorithms to compare the ability of their proposed framework. Effectiveness of employing multiple methods with the aim of print attack detection for face biometric has been studied in [14]. They compared different techniques based on motion analysis, texture analysis and liveness detection to detect 2D facial print-based spoof attacks.

Furthermore, a CNN based face spoofing detection method has been proposed in [30] where local binary patterns (LBP) has been integrated to extract deep texture features. NUAA spoofing database has been used to evaluate performance of their proposed method that is called LBPnet and n-LBPnet. In [31] a nonlinear diffusion-based method has been employed on an additive operator splitting scheme to detect face images edges. Additionally, specialized CNN has been used to extract discriminative and high-level features of the input diffused image to differentiate between a fake face and a real face. In [32] a new hybrid scheme has been presented to control the authenticity of the users in order to login a system. The scheme uses handcrafted and CNN methods to verify real or spoof entities. First, the scheme uses the hash of a fingerprint to compare with the fingerprint database. After a successful match of the fingerprint, it is tested on a CNN-based model. The proposed method first matches entities with the corresponding databases by integrating fingerprint, palm vein print and face recognition, then the scheme uses anti-spoofing CNN based models to detect spoofing using fingerprint, palm vein print and face. Also, the similar processes are done for the palm and face respectively to collect efficient and robust evidence. On the other hand, face anti-spoofing based on CNN architecture has been presented in [33] by putting a long short-term memory (LSTM) layer over the fully connected layers for feature extraction. The architecture employs LSTM along with extracting local and dense features through convolution operations. On the other hand, two different deep learning methods for attack detection in several biometric recognition systems such as iris, face, and fingerprint has been introduced in [4]. The authors reported high detection performance of deep learning technique in their work, however the method was not able to improve always the detection rate specifically for face biometric. The concentration of [27] is on a new method based on feature level fusion strategy to fuse handcrafted and deep learnt facial features spoof detection improvement. In order to differentiate real and fake identities, the authors applied SVM classifier.

In [34], score-level-based face anti-spoofing method is proposed using CNN and overlapped histograms of local binary patterns (OVLBP) 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.

3. HANDCRAFTED FACIAL TEXTURE EXTRACTION USING LOG-GABOR FILTER

This step aims to extract handcrafted facial features to be used in classification processes using 1D Log-Gabor filter [35]. In general, 1D Log-Gabor filter provides helpful frequency information. By using Log-Gabor filter natural images are better fit compared with Gabor and other wavelet filters. Log-Gabor function has the frequency response as (1).

$$G(f)=\exp\left(\frac{-(\log(f/f_0))^2}{2(\log(\sigma/f_0))^2}\right) \quad (1)$$

Where f_0 and σ represent parameters of the filter. In fact, f_0 presents the center frequency and σ affects the bandwidth of filter. Generally, it is better to consider the same shape while the frequency parameter is varied. Therefore, the ratio σ/f_0 should be considered constant.

Log-Gabor filter method is exploited in some works to extract features. In [36] multi-resolution 2D Log-Gabor filter has been used to extract features along with spectral regression kernel discriminant analysis (SRKDA) in order to reduce features dimensionality. In [37, 38] also 2D Log-Gabor filter has been used in different scales and orientations. A new score-level and feature-level fusion scheme has been proposed in [19]. They employed One-dimensional Log-Gabor to extract facial and iris features. In this study, in the handcrafted facial texture extraction part 1D Log-Gabor filter has been employed to extract optimal and meaningful features.

4. DEEP LEARNING EXTRACTION USING CNN

In this study in order to improve the detection rate of print and video attacks the proposed scheme employs CNN learning-based approach to extract more representative feature set of information. The most significant layer of CNN structure is convolutional layers and fully connected layers. In the convolutional layers, convolution operations are used to extract and manipulate image features.

A training process is needed based on the characteristics of images to achieve filter coefficients. To imagine general structure of CNN consideration of a cross-channel normalization layer, a rectified linear unit (ReLU) and a pooling layer is needed for each convolutional layer. ReLU, tanh and sigmoid are activation functions which mostly used in the CNN in order to detect non-linear features. Additionally, mostly used max and average pooling operations are employed to reduce feature maps dimension. At the end, for further classification the constructed feature map is sent to fully-connected layers.

The structure of proposed CNN anti-spoofing framework to learn facial features in this study is based on VGG-16 architecture that was presented by the Oxford Visual Geometry Groups' model in ImageNet Large-Scale Visual Recognition Challenge (ILSVRC) [39].

Generally, VGG-16 is more extensive and richer with compare to other earlier versions of CNN structure, it includes five batches of convolution operations. The architecture of VGG-16 is illustrated in Figure 1. Generally, each batch includes 2–3 adjacent convolution layers connected via max-pooling layers. The 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 is used for all convolutional layers in this model.

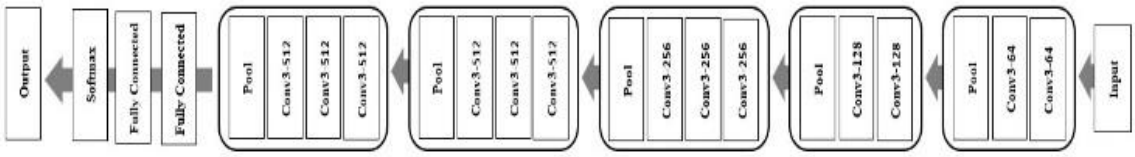

Figure 1. The structure of VGG-16

The proposed anti-spoofing method contains only two type of classes for detection as real and fake, therefore the total number of output neurons is considered as two in the last layer. In order to alleviate the effect of overfitting for training step of CNN, the proposed method applies several learning rate policies in different layers. Additionally, training part of the study includes data augmentation technique by cropping different regions of input and their fillips.

5. PROPOSED ANTI-SPOOFING SCHEME

The study proposed a robust anti-spoofing scheme to detect print and video attacks in face databases by exerting texture-based 1D Log-Gabor filter and CNN-based deep learning methods. Figure 2 depicts the general structure of the proposed method.

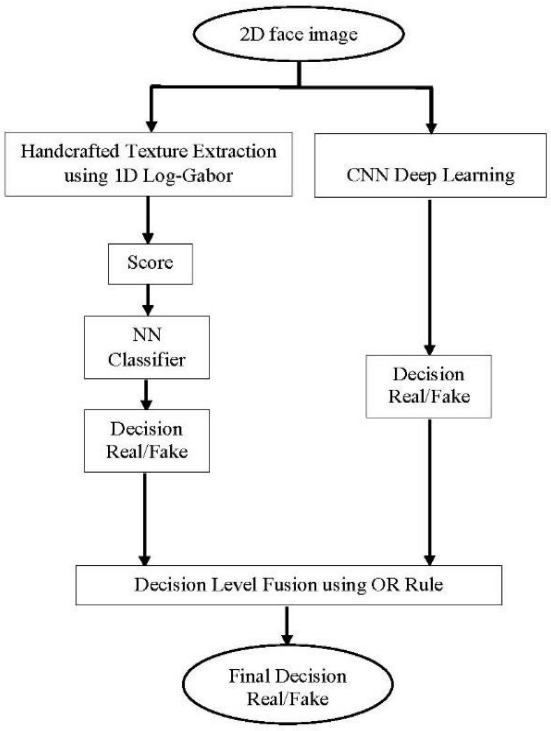

Figure 2. The proposed anti-spoofing diagram

In order to improve the ability of the proposed method for detecting print and video attacks the facial features are extracted using Log-Gabor filter and CNN methods separately. In the handcrafting part of the method nearest neighbor classifier (NNC) is used on set of calculated scores to provide classification and decision. Finally, decision-level fusion (DLF) with OR rule is used to provide final common decision based on two separate obtained decisions (handcrafted and CNN). Generally, OR rule logic represents genuine if the result of one decision be genuine, otherwise it is fake.

6. EXPERIMENTAL RESULTS AND DATABASES

The experimental result part of this study aims to evaluate the performance of proposed anti-spoofing scheme based on Repla-Attack and Idiap Print-Attack databases. Under different lighting conditions, Repla-Attack databases includes 1300 video clips of photograph and video attack access of 50 individuals where Print-Attack database contains 200 short videos of printed photograph and real-access of 50 individuals.

Prior to performing the experiments, the proposed scheme attempts to extract the face images from video sequences and subsequently detected face images aligned according to center position of left and right irises. In order to perform the experiments, randomly 30 individuals for training and 20 individuals for testing is selected for accessing real and attack images. The total number of 750 real access images, 750 print attack images and 1000 video attack images extracted from videos is used in this work to perform the experiments. Training dataset includes 450 real, 450 print attack and 600 video attack images and test dataset contains 300 real images, 300 print attack images and 400 video attack images. The images are divided into train and test datasets three times and the averaged result of these three sets is considered to report the final performance.

The preprocessing step of proposed method contains image resizing of size 256 ×256. This work considers ten different cropped size of 227×227 and their flip for data augmentation. Therefore, the total number of train augmented database contains 9000 real, 9000 print attack and 12000 video attack images. Regularization, momentum parameters and learning rate for this study are considered as 0.1, 0.9 and 0.001 with batch size of 32 respectively to avoid overfitting in this work. The evaluation protocol of proposed method considers Half Total Error Rate (HTER)

that is half of sum of False Genuine Rate (FGR) and False Fake Rate (FFR) of spoof detection errors.

The concentration of experiments for this study is on handcrafted texture extraction method, CNN learnt based extraction method and also fusion of them against print and video attacks. The classification part of handcrafted extraction method contains nearest-neighbor classifier (NN). Generally, NN is considered as a method of data classification to approximate how likely a data point is to be a member of one group. Table 1 shows the experimental results performed using Log-Gabor filter handcrafted extraction method and CNN learnt based extraction method separately for print and video attacks.

Table 1. Experimental results related to Log-Gabor and CNN extractors for print and video attacks in HTER (%)

Method	**Print-Attack HTER (%)**	**Video-Attack HTER (%)**
Log-Gabor	37.45	37.30
CNN	18.26	22.18

Investigation of results demonstrates the superiority of CNN method over Log-Gabor handcrafted extractor against both print and video attacks. In fact, handcrafted feature extractor has obtained similar performance for both kinds of attacks while applying CNN learnt based extractor performed better for print attack. Analyzing the results demonstrates 19.19% and 15.12% improvement on accuracy for CNN method against print and video attacks compared to Log-Gabor technique. On the other hand, in order to improve the detection performance of anti-spoofing scheme Table 2 attempts to apply the effect of different fusion techniques on datasets.

As depicted in Table 2, fusion of handcrafted and learnt based methods for feature, score and decision levels outperforms detection rate of spoofing for print and video attacks. The review of results shows higher detection rate for print attacks in all fusion steps compared to video attacks. The best accuracy is obtained using proposed method to fuse the decision of CNN along with Log-Gabor method using OR rule.

Indeed, the proposed method achieved 27.85% and 26.30% improvement over applying only Log-Gabor filter technique on face spoofing for print and video attacks respectively.

Table 2. Experimental results related to handcrafted and learnt based fusion for print and video attacks in HTER (%)

Method	**Print-Attack HTER (%)**	**Video-Attack HTER (%)**
CNN+Log-Gabor using Feature Level Fusion	15.00	15.25
CNN+Log-Gabor using Score Level Fusion	10.14	11.00
CNN+Log-Gabor using Decision Level Fusion (Proposed Method)	9.60	11.00

7. CONCLUSION

This study involves consideration of an effective anti-spoofing framework based on log-Gabor and CNN feature extractors. The proposed pipeline implemented both handcrafted and learn based techniques on face images and then in order to recognize real and attack attempts the fusion strategy has been applied. In fact, decision level fusion combines the decisions of both methods using OR rule to improve the detection rate of face spoofing. The focus of this study for introducing the anti-spoofing framework is on print and video attacks. The performance of proposed anti-spoofing pipeline has been investigated on two public spoof databases namely Print-Attack and Replay-Attack The comparison of proposed method with other fusion techniques demonstrated the effectiveness of decision level fusion for face anti-spoofing.

8. REFERENCES

1. Galbally, J., Marcel, S., Fierrez, J., 2014. Biometric Antispoofing Methods: A Survey in Face Recognition. IEEE Access, 2, 1530-1552.

2. Martinez-Diaz, M., Fierrez, J., Galbally, J., Ortega-Garcia, J., 2011. An Evaluation of Indirect Attacks and Countermeasures in Fingerprint Verification Systems. Pattern Recognition Letters, 32(12), 1643-1651.

3. Nguyen, D.T., Yoon, H.S., Pham, T.D., Park, K.R., 2017. Spoof Detection for Finger-vein Recognition System Using NIR Camera. Sensors, 17(10), 2261.

4. Menotti, D., Chiachia, G., Pinto, A., Schwartz, W.R., Pedrini, H., Falcao, A.X., Rocha, A., 2015. Deep Representations for Iris, Face, and Fingerprint Spoofing Detection. IEEE Transactions on Information Forensics and Security, 10(4), 864-879.

5. Ratha, N.K., Connell, J.H., Bolle, R.M., 2001. An Analysis of Minutiae Matching Strength. In International Conference on Audio-and Video-Based Biometric Person Authentication, Springer, Berlin, Heidelberg, 223-228.

6. Tirunagari, S., Poh, N., Windridge, D., Iorliam, A., Suki, N., Ho, A.T., 2015. Detection of Face Spoofing Using Visual Dynamics. IEEE Transactions on Information Forensics and Security, 10(4), 762-777.

7. Eskandari, M., Sharifi, O., 2018. Designing Efficient Spoof Detection Scheme for Face Biometric. In International Conference on Image and Signal Processing, Springer, Cham, 427-434.

8. Anjos, A., Marcel, S., 2011, October. Counter-measures to Photo Attacks in Face Recognition: a Public Database and a Baseline. In 2011 International Joint Conference on Biometrics (IJCB) IEEE. 1-7.

9. Gupta, P., Behera, S., Vatsa, M., Singh, R., 2014. On Iris Spoofing Using Print Attack. In 2014 22nd International Conference on Pattern Recognition, IEEE, 1681-1686.

10. Hadid, A., Ghahramani, M., Kellokumpu, V., Pietikäinen, M., Bustard, J., Nixon, M., 2012. Can Gait Biometrics be Spoofed?. In Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012), IEEE, 3280-3283.

11. Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G.L., Roli, F., 2012. Security Evaluation of Biometric Authentication Systems Under Real Spoofing Attacks. IET biometrics, 1(1), 11-24.

12. Gomez-Barrero, M., Galbally, J., Fierrez, J., 2014. Efficient Software Attack to Multimodal Biometric Systems and its Application to Face and Iris Fusion. Pattern Recognition Letters, 36, 243-253.

13. Akhtar, Z., Kale, S., Alfarid, N., 2011. Spoof Attacks on Multimodal Biometric Systems. In International Conference on Information and Network Technology, 4, 46-51.

14. Chakka, M.M., Anjos, A., Marcel, S., Tronci, R., Muntoni, D., Fadda, G., Pili, M., Sirena, N., Murgia, G., Ristori, M., Roli, F., 2011. Competition on Counter Measures to 2-d Facial Spoofing Attacks. In 2011 International Joint Conference on Biometrics (IJCB), IEEE, 1-6.

15. Kollreider, K., Fronthaler, H., Bigun, J., 2005. Evaluating Liveness by Face Images and the Structure Tensor. In Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05), IEEE, 75-80.

16. Kollreider, K., Fronthaler, H., Bigun, J., 2008. Verifying Liveness by Multiple Experts in Face Biometrics. In 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, IEEE, 1-6.

17. Krizhevsky, A., Sutskever, I., Hinton, G.E., 2012. Imagenet Classification with Deep Convolutional Neural Networks. In Advances in Neural Information Processing Systems, 1097-1105.

18. Druzhkov, P.N., Kustikova, V.D., 2016. A Survey of Deep Learning Methods and Software Tools for Image Classification and Object Detection. Pattern Recognition and Image Analysis, 26(1), 9-15.

19. Eskandari, M., Toygar, Ö., 2015. Selection of Optimized Features and Weights on Face-iris Fusion Using Distance Images. Computer Vision and Image Understanding, 137, 63-75.

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

21. Replay Attack face database, 2014, https://www.idiap.ch/dataset/replayattack, Accessed October 2014.
22. Galbally, J., Marcel, S., Fierrez, J., 2013. Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. IEEE Transactions on Image Processing, 23(2), 710-724.
23. Bharadwaj, S., Dhamecha, T.I., Vatsa, M., Singh, R., 2013. Computationally Efficient Face Spoofing Detection with Motion Magnification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 105-110.
24. Määttä, J., Hadid, A., Pietikäinen, M., 2011. Face Spoofing Detection from Single Images Using Micro-texture Analysis. In 2011 International Joint Conference on Biometrics (IJCB), IEEE, 1-7.
25. de Freitas Pereira, T., Komulainen, J., Anjos, A., De Martino, J.M., Hadid, A., Pietikäinen, M., Marcel, S., 2014. Face Liveness Detection Using Dynamic Texture. EURASIP Journal on Image and Video Processing, 2014(1), 2.
26. Wen, D., Han, H., Jain, A.K., 2015. Face Spoof Detection with Image Distortion Analysis. IEEE Transactions on Information Forensics and Security, 10(4), 746-761.
27. Nguyen, D.T., Pham, T.D., Baek, N.R., Park, K.R., 2018. Combining Deep and Handcrafted Image Features for Presentation Attack Detection in Face Recognition Systems Using Visible-light Camera Sensors. Sensors, 18(3), 699.
28. Ojala, T., Pietikäinen, M., Harwood, D., 1996. A Comparative Study of Texture Measures with Classification Based on Featured Distributions. Pattern Recognition, 29(1), 51-59.
29. Benlamoudi, A., Samai, D., Ouafi, A., Bekhouche, S.E., Taleb-Ahmed, A., Hadid, A., 2015, May. Face Spoofing Detection Using Local Binary Patterns and Fisher Score. In 2015 3rd International Conference on Control, Engineering & Information Technology (CEIT), IEEE, 1-5.
30. De Souza, G.B., da Silva Santos, D.F., Pires, R.G., Marana, A.N., Papa, J.P., 2017. Deep Texture Features for Robust Face Spoofing Detection. IEEE Transactions on Circuits and Systems II: Express Briefs, 64(12), 1397-1401.
31. Alotaibi, A., Mahmood, A., 2017. Deep Face Liveness Detection Based on Nonlinear Diffusion Using Convolution Neural Network. Signal, Image and Video Processing, 11(4), 713-720.
32. Sajjad, M., Khan, S., Hussain, T., Muhammad, K., Sangaiah, A.K., Castiglione, A., Esposito, C., Baik, S.W., 2019. CNN-based Anti-spoofing Two-tier Multi-factor Authentication System. Pattern Recognition Letters, 126, 123-131.
33. Xu, Z., Li, S., Deng, W., 2015. November. Learning Temporal Features Using LSTM-CNN Architecture for Face Anti-spoofing. In 2015 3rd IAPR Asian Conference on Pattern Recognition (ACPR), IEEE, 141-145.
34. Sharifi, O., 2019. Score-level-based Face Anti-Spoofing System Using Handcrafted and Deep Learned Characteristics. International Journal of Image, Graphics and Signal Processing, 11(2), 15.
35. Field, D.J., 1987. Relations Between the Statistics of Natural Images and the Response Properties of Cortical Cells. Josa a, 4(12), 2379-2394.
36. Ammour, B., Bouden, T., Boubchir, L., 2018. Face–iris Multi-modal Biometric System Using Multi-resolution Log-gabor Filter with Spectral Regression Kernel Discriminant Analysis. IET Biometrics, 7(5), 482-489.
37. Du, Y., 2006. Using 2D log-Gabor Spatial Filters for Iris Recognition. In Biometric Technology for Human Identification III,. International Society for Optics and Photonics, 6202, 62020F
38. Bounneche, M.D., Boubchir, L., Bouridane, A., Nekhoul, B., Ali-Chérif, A., 2016. Multi-spectral Palmprint Recognition Based on Oriented Multiscale log-Gabor Filters. Neurocomputing, 205, 274-286.
39. Simonyan, K., Zisserman, A., 2014. Very Deep Convolutional Networks for Large-scale Image Recognition. arXiv Preprint arXiv:1409.1556.