Enhancing Ensemble Learning Using CNN for Spoof Fingerprints

Subjects: Computer Science, Artificial Intelligence

Contributor: Naim Reza , Ho Yub Jung

Convolutional Neural Networks (CNNs) have demonstrated remarkable success with great accuracy in classification problems. Using an ensemble of neural networks offers a simple yet effective measure to improve performance and robustness beyond that of a single network.

ensemble learning convolutional neural network class activation map fingerprint

1. Introduction

Ensembling of neural networks to enhance their accuracy and robustness has been a well-established concept since 1990 when it was first introduced by [1]. Subsequently, numerous ensemble techniques have been developed, such as the cross-validation ensemble [2], model averaging ensemble, weighted average ensemble, horizontal and vertical ensemble [3], which are notable among others. While these methods have achieved significant success at enhancing the accuracy of a model's predictions, they are also associated with a large training cost. To address this issue, the authors of [4] proposed a method that uses a cyclic cosine annealing learning rate, as proposed by [5], to guide a neural network towards different local minima and to save the weights of the network at the end of each cycle. This approach produces diverse ensemble members under a single training session. Furthermore, in [6], the authors introduced Stochastic Weight Averaging, a method that forms an ensemble in the weight space by implementing a moving average of the weights of the models, as opposed to averaging the outputs of the models. These ensemble learning methods provide a convenient approach to enhance a network's performance and robustness.

In security applications such as detecting spoof biometrics, maintaining the robustness of the network is crucial. While the ensemble method offers potential to enhance network robustness, it often involves various trade-offs. As depicted in **Figure 1**, implementing the snapshot ensemble method [4] in conjunction with the cyclic cosine annealing learning rate [5] for all four sets of sensor data present in the LivDet [7] dataset leads to the degradation of accuracy in a network that had already been producing state-of-the-art results. This observation suggests that in cases for which the training dataset is small and homogeneous in nature, the number of available local minima is very limited, and it is challenging to ensure diversity among the ensemble members. The availability of biometric datasets, such as a fingerprint dataset for training a spoof detection network, is limited due to the sensitive nature of the data. The small size of the dataset can introduce significant biases during training, which may cause a reduction in ensemble accuracy.

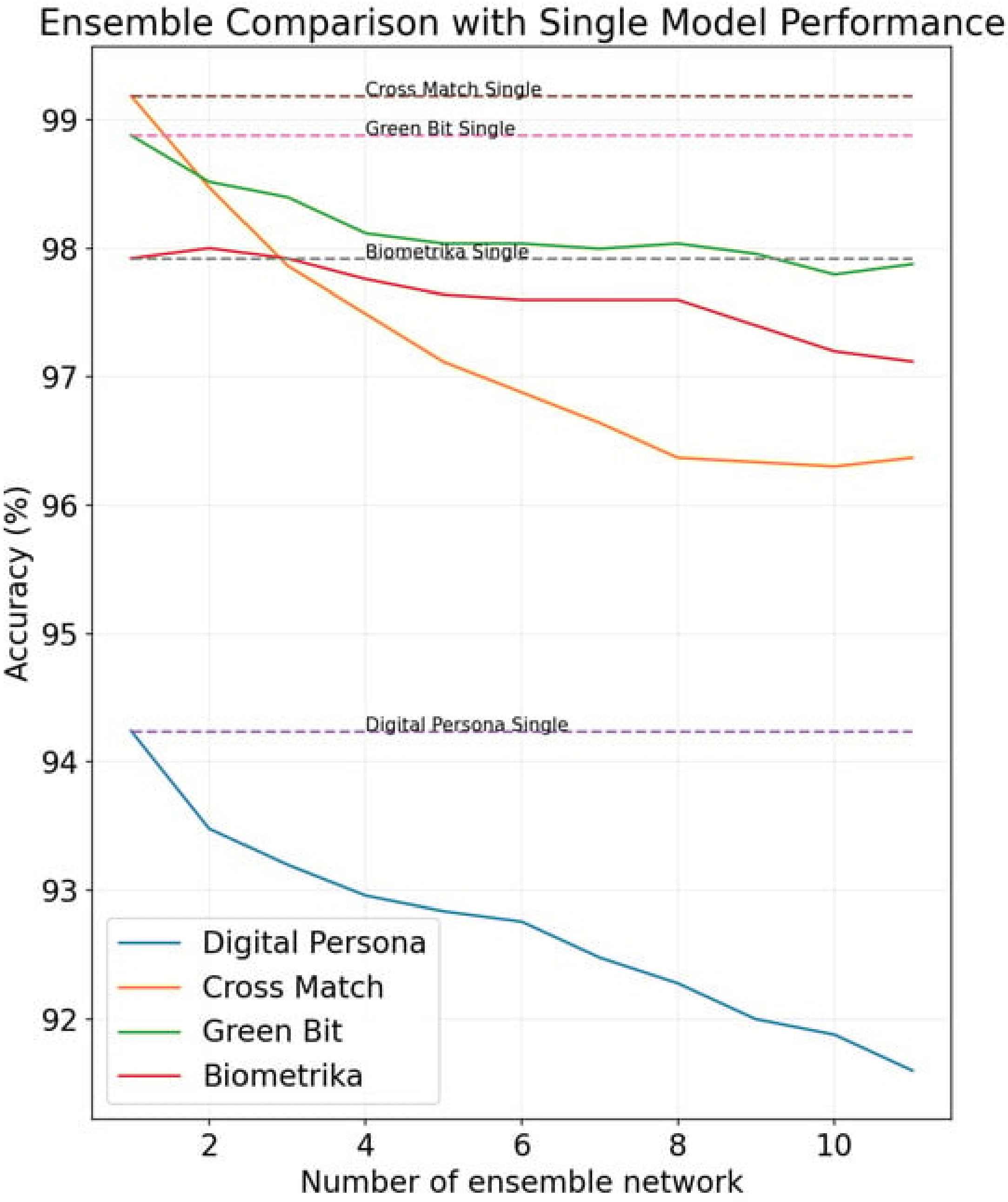

Figure 1. Performance variation of a CNN-based spoof detection network when subjected to an ensemble setting.

Explanation of the learned features of a network is instrumental to investigate potential failure modes resulting from biases in the dataset. Additionally, the ability to explain the functioning of a spoof detection network is imperative to enhance the system’s reliability. Recognizing the complexity associated with interpreting CNNs, various methodologies have been proposed, such as the Class Activation Map (CAM) [8] and the Gradient-weighted Class Activation Map (Grad-CAM) [9], to identify and visualize the specific image regions that the network utilizes for prediction. Thus, the explanations are mainly limited to the production of a saliency map, and the internal representation of the CNN is still mostly unexplainable. Furthermore, the produced saliency maps are specific for each sample, and the global interpretation of the network or the dataset is not easily found.

Nevertheless, sample-wise saliency maps can be effective information for training new networks that can use different regions for classification.

After analyzing the class activation map of a previously trained model, certain areas of the input image are entirely disregarded by the network for classification, despite containing critical features, as demonstrated in **Figure 2**. Additionally, strong activation regions are relatively small, which indicates that the network may ignore important parts of the input image, which could include essential information such as textures or patterns. This observation also suggests that activation perturbation of a network can be utilized to generate diverse models that can serve as ensemble members to enhance the network's robustness and accuracy.

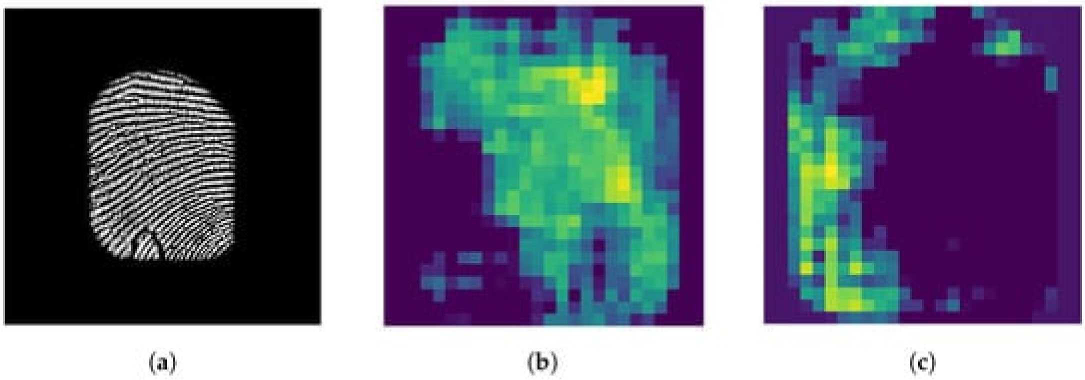

Figure 2. Impact of the proposed training method on the activation patterns of a CNN: (**a**) input fingerprint, (**b**) activation of the base network, and (**c**) activation of one of the ensemble members after being trained with the proposed method.

Though spoof fingerprints can be easily created using low-cost and readily available materials such as wood glue, Play-Doh, gelatin, and latex-like substances [7][10] to deceive a biometric authentication system, fabricating such spoof fingerprint can be time consuming. As a result, the datasets available for training a spoof detection network are comparatively very small in size.

2. Enhancing Ensemble Learning Using Explainable CNN for Spoof Fingerprints

Using an ensemble of neural networks offers a simple yet effective measure to improve performance and robustness beyond that of a single network [11][12][13]. Notably, in high-profile competitions such as ImageNet [14] and Kaggle (www.kaggle.com, accessed on 26 November 2023), ensembles of deep learning architectures have consistently outperformed individual models. Prior studies have demonstrated that ensembling can enhance both accuracy and robustness by exploiting network diversity [15][16][17][18][19][20][21]. Despite these benefits, the use of ensembling for neural networks remains limited due to high training costs. In light of this problem, Snapshot Ensemble [4], Fast Geometric Ensemble [22], and Stochastic Weight Averaging ensemble [6] have been proposed, wherein the authors exploit model diversity and geometric properties of the loss surface to achieve the benefits of ensembling. However, these techniques have mainly been evaluated on relatively large datasets, wherein at least

50,000 images are available in the training set, and there has been limited exploration of their effectiveness on smaller datasets such as LivDet 2015 [7].

Grad-CAM has been successfully applied to explain classifiers in image classification, image segmentation [23], and visual question answering (VQA) [24]. Its success has led to the development of Grad-CAM++ [25], which further enhances the explanation capabilities of Grad-CAM and has been used for object detection and localization [26][27][28]. The authors in [29] employed Grad-CAM as a visualization tool to identify and highlight noise across various channels of a network when processing a fingerprint image. The use of CAM is also presented in the study by [30], where it was used for patch extraction during the inference stage.

The detection of spoof fingerprints remains a prominent research topic, and CNNs have proven to be a successful approach [31]. To stimulate further research efforts in this field, several spoof detection competitions (LivDet 2009–2021) have been organized [7][10][32][33]. Notably, in the LivDet 2015 competition, the authors of [34] employed a transfer learning approach using deep CNNs, specifically AlexNet [35] and VGGNet [36], which were pre-trained on the ImageNet [14] dataset, and fine-tuned some of the layers for spoof detection of fingerprints. Meanwhile, [37] proposed a CNN architecture with similar performance but reduced test time. Improving the robustness of CNN-based spoof detection systems has been explored by [38], who adopted a hybrid approach that combines hyper-parameter tuning of a CNN and Support Vector Machines (SVMs). Siamese network architecture has been employed by the authors of [39] to improve the robustness of a fingerprint spoof detection system. The authors of [40] have proposed an altered ResNet architecture to achieve smaller parameter size and computational efficiency for a practical spoof detection application. Additionally, [41] have improved the accuracy and robustness of their system using the MobileNet-V1 [42] architecture in conjunction with the fusion of minutiae-based center-aligned local patches. However, their approach involves several complex algorithms, such as minutiae detection, local patch extraction, and patch alignment, in the training and testing procedures. Several techniques [43][44][45][46] have been proposed to generate synthetic fingerprints by leveraging style-transfer techniques. The primary objective of these approaches is to increase the number of data samples in order to address challenges associated with limited dataset sizes. A brief summary of the relevant studies is presented in **Table 1**.

Table 1. Summary of studies focused on fingerprint spoof detection using CNNs.

Method	Approach	Database	Performance
Emanuela et al. [39]	Employment of Siamese network	LivDet 2013	Avg. Accuracy = 93.1%93.1%
Menotti et al. [38]	Combination of hyper-parameter tuning of a CNN and use of SVM for prediction	LivDet 2015	Avg. Accuracy = 93.745%93.745%
Nogueira et al. [34]	Transfer learning using VGG network	LivDet 2015	Avg.Accuracy = 95.5%95.5%
Jung et al. [37]	Liveness detection of probe fingerprint using template fingerprint through two sequential	LivDet 2015	Avg. Accuracy = 96.99%96.99%

Method	Approach	Database	Performance
	custom CNNs		
Chugh et al. [41]	Minutiae-centered local patch extraction and detection through MobileNet	LivDet 2011-2015	ACE = 1.48%1.48% (LivDet 2015)
Zhang et al. [40]	Slim-ResCNN and patch extraction via center of gravity	LivDet 2017	Avg. Accuracy = 95.25%95.25%
Chugh et al. [43]	Style transfer between known spoof materials to generate synthetic data for network training	LivDet 2017	Avg. Accuracy = 95.88%95.88%
Liu et al. [30]	Fusion of global and local spoofness score and patch extraction using Grad-CAM during inference	LivDet 2017	TDR = 91.19%91.19% @FDR = 1%1%
Proposed Approach	Ensemble of CAM-guided models generated from a pre-trained CNN	LivDet 2015	Avg. Accuracy = 97.94%

References

1. Hansen, L.; Salamon, P. Neural network ensembles. IEEE Trans. Pattern Anal. Mach. Intell. 1990, 12, 993–1001.
2. Krogh, A.; Vedelsby, J. Neural Network Ensembles, Cross Validation and Active Learning. In Proceedings of the 7th International Conference on Neural Information Processing Systems (NIPS'94), Cambridge, MA, USA, 1 January 1994; pp. 231–238.
3. Xie, J.; Xu, B.; Zhang, C. Horizontal and Vertical Ensemble with Deep Representation for Classification. arXiv 2013, arXiv:1306.2759.
4. Huang, G.; Li, Y.; Pleiss, G.; Liu, Z.; Hopcroft, J.E.; Weinberger, K.Q. Snapshot Ensembles: Train 1, get M for free. arXiv 2017, arXiv:1704.00109.
5. Loshchilov, I.; Hutter, F. SGDR: Stochastic Gradient Descent with Restarts. arXiv 2016, arXiv:1608.03983.
6. Izmailov, P.; Podoprikhin, D.; Garipov, T.; Vetrov, D.P.; Wilson, A.G. Averaging Weights Leads to Wider Optima and Better Generalization. arXiv 2018, arXiv:1803.05407.
7. Ghiani, L.; Yambay, D.A.; Mura, V.; Marcialis, G.L.; Roli, F.; Schuckers, S.A.C. Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015. arXiv 2016, arXiv:1609.01648.
8. Zhou, B.; Khosla, A.; Lapedriza, À.; Oliva, A.; Torralba, A. Learning Deep Features for Discriminative Localization. arXiv 2015, arXiv:1512.04150.
9. Selvaraju, R.R.; Das, A.; Vedantam, R.; Cogswell, M.; Parikh, D.; Batra, D. Grad-CAM: Why did you say that? Visual Explanations from Deep Networks via Gradient-based Localization. arXiv

2016, arXiv:1610.02391.

10. Mura, V.; Orrù, G.; Casula, R.; Sibiriu, A.; Loi, G.; Tuveri, P.; Ghiani, L.; Marcialis, G.L. LivDet 2017 Fingerprint Liveness Detection Competition 2017. arXiv 2018, arXiv:1803.05210.
11. Zheng, H.; Gu, Y. EnCNN-UPMWS: Waste Classification by a CNN Ensemble Using the UPM Weighting Strategy. Electronics 2021, 10, 427.
12. Jamali, A.; Mahdianpari, M.; Brisco, B.; Granger, J.; Mohammadimanesh, F.; Salehi, B. Comparing Solo Versus Ensemble Convolutional Neural Networks for Wetland Classification Using Multi-Spectral Satellite Imagery. Remote Sens. 2021, 13, 2046.
13. Zahoor, M.M.; Qureshi, S.A.; Bibi, S.; Khan, S.H.; Khan, A.; Ghafoor, U.; Bhutta, M.R. A New Deep Hybrid Boosted and Ensemble Learning-Based Brain Tumor Analysis Using MRI. Sensors 2022, 22, 2726.
14. Deng, J.; Dong, W.; Socher, R.; Li, L.J.; Li, K.; Fei-Fei, L. ImageNet: A large-scale hierarchical image database. In Proceedings of the 2009 IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA, 20–25 June 2009; pp. 248–255.
15. Liu, X.; Cheng, M.; Zhang, H.; Hsieh, C.J. Towards Robust Neural Networks via Random Self-ensemble. In Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, 8–14 September 2018.
16. Pang, T.; Xu, K.; Du, C.; Chen, N.; Zhu, J. Improving Adversarial Robustness via Promoting Ensemble Diversity. In Proceedings of the 36th International Conference on Machine Learning; Chaudhuri, K., Salakhutdinov, R., Eds.; PMLR: London, UK, 2019; Volume 97, pp. 4970–4979.
17. Liu, L.; Wei, W.; Chow, K.H.; Loper, M.; Gursoy, E.; Truex, S.; Wu, Y. Deep Neural Network Ensembles Against Deception: Ensemble Diversity, Accuracy and Robustness. In Proceedings of the 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Monterey, CA, USA, 4–7 November 2019; pp. 274–282.
18. Wu, B.; Wang, S.; Yuan, X.; Wang, C.; Rudolph, C.; Yang, X. Defeating Misclassification Attacks Against Transfer Learning. IEEE Trans. Dependable Secur. Comput. 2023, 20, 886–901.
19. Wu, Y.; Liu, L. Boosting Deep Ensemble Performance with Hierarchical Pruning. In Proceedings of the 2021 IEEE International Conference on Data Mining (ICDM), Virtual, 7–10 December 2021; pp. 1433–1438.
20. Wu, Y.; Liu, L.; Xie, Z.; Chow, K.H.; Wei, W. Boosting Ensemble Accuracy by Revisiting Ensemble Diversity Metrics. In Proceedings of the 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA, 20–25 June 2021; pp. 16464–16472.
21. Wu, Y.; Liu, L.; Xie, Z.; Bae, J.; Chow, K.H.; Wei, W. Promoting High Diversity Ensemble Learning with EnsembleBench. In Proceedings of the 2020 IEEE Second International Conference on

Cognitive Machine Intelligence (CogMI), Atlanta, GA, USA, 28–31 October 2020; pp. 208–217.

22. Garipov, T.; Izmailov, P.; Podoprikhin, D.; Vetrov, D.; Wilson, A.G. Loss Surfaces, Mode Connectivity, and Fast Ensembling of DNNs. arXiv 2018.
23. Xiao, M.; Zhang, L.; Shi, W.; Liu, J.; He, W.; Jiang, Z. A visualization method based on the Grad-CAM for medical image segmentation model. In Proceedings of the 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS), Changchun, China, 23–26 September 2021; pp. 242–247.
24. Panesar, A.; Doğan, F.I.; Leite, I. Improving Visual Question Answering by Leveraging Depth and Adapting Explainability. In Proceedings of the 2022 31st IEEE International Conference on Robot and Human Interactive Communication (RO-MAN), Napoli, Italy, 29 August–2 September 2022; pp. 252–259.
25. Chattopadhyay, A.; Sarkar, A.; Howlader, P.; Balasubramanian, V.N. Grad-CAM++: Generalized Gradient-based Visual Explanations for Deep Convolutional Networks. arXiv 2017, arXiv:1710.11063.
26. Yamauchi, T.; Ishikawa, M. Spatial Sensitive GRAD-CAM: Visual Explanations for Object Detection by Incorporating Spatial Sensitivity. In Proceedings of the 2022 IEEE International Conference on Image Processing (ICIP), Bordeaux, France, 16–19 October 2022; pp. 256–260.
27. Dreyer, M.; Achtibat, R.; Wiegand, T.; Samek, W.; Lapuschkin, S. Revealing Hidden Context Bias in Segmentation and Object Detection through Concept-specific Explanations. In Proceedings of the 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Vancouver, BC, Canada, 17–23 June 2023; pp. 3829–3839.
28. Gwon, C.; Howell, S.C. ODSmoothGrad: Generating Saliency Maps for Object Detectors. In Proceedings of the 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Vancouver, BC, Canada, 18–19 June 2023; pp. 3686–3690.
29. Liu, F.; Kong, Z.; Liu, H.; Zhang, W.; Shen, L. Fingerprint Presentation Attack Detection by Channel-Wise Feature Denoising. IEEE Trans. Inf. Forensics Secur. 2022, 17, 2963–2976.
30. Liu, H.; Zhang, W.; Liu, F.; Wu, H.; Shen, L. Fingerprint Presentation Attack Detector Using Global-Local Model. IEEE Trans. Cybern. 2022, 52, 12315–12328.
31. Militello, C.; Rundo, L.; Vitabile, S.; Conti, V. Fingerprint Classification Based on Deep Learning Approaches: Experimental Findings and Comparisons. Symmetry 2021, 13, 750.
32. Orrù, G.; Casula, R.; Tuveri, P.; Bazzoni, C.; Dessalvi, G.; Micheletto, M.; Ghiani, L.; Marcialis, G.L. LivDet in Action—Fingerprint Liveness Detection Competition 2019. In Proceedings of the 2019 International Conference on Biometrics (ICB), Crete, Greece, 4–7 June 2019; pp. 1–6.

33. Casula, R.; Micheletto, M.; Orrú, G.; Delussu, R.; Concas, S.; Panzino, A.; Marcialis, G.L. LivDet 2021 Fingerprint Liveness Detection Competition - Into the unknown. In Proceedings of the 2021 IEEE International Joint Conference on Biometrics (IJCB), Shenzhen, China, 4–7 August 2021; pp. 1–6.

34. Nogueira, R.F.; de Alencar Lotufo, R.; Campos Machado, R. Fingerprint Liveness Detection Using Convolutional Neural Networks. IEEE Trans. Inf. Forensics Secur. 2016, 11, 1206–1213.

35. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. ImageNet Classification with Deep Convolutional Neural Networks. In Proceedings of the Advances in Neural Information Processing Systems, Lake Tahoe, NV, USA, 3–6 December 2012; Pereira, F., Burges, C., Bottou, L., Weinberger, K., Eds.; Curran Associates, Inc.: New York, NY, USA, 2012; Volume 25.

36. Simonyan, K.; Zisserman, A. Very Deep Convolutional Networks for Large-Scale Image Recognition. arXiv 2015, arXiv:1409.1556.

37. Jung, H.Y.; Heo, Y.S.; Lee, S. Fingerprint Liveness Detection by a Template-Probe Convolutional Neural Network. IEEE Access 2019, 7, 118986–118993.

38. Menotti, D.; Chiachia, G.; Pinto, A.; Schwartz, W.R.; Pedrini, H.; Falcão, A.X.; Rocha, A. Deep Representations for Iris, Face, and Fingerprint Spoofing Detection. IEEE Trans. Inf. Forensics Secur. 2015, 10, 864–879.

39. Marasco, E.; Wild, P.; Cukic, B. Robust and interoperable fingerprint spoof detection via convolutional neural networks. In Proceedings of the 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 10–12 May 2016; pp. 1–6.

40. Zhang, Y.; Shi, D.; Zhan, X.; Cao, D.; Zhu, K.; Li, Z. Slim-ResCNN: A Deep Residual Convolutional Neural Network for Fingerprint Liveness Detection. IEEE Access 2019, 7, 91476–91487.

41. Chugh, T.; Cao, K.; Jain, A.K. Fingerprint Spoof Buster: Use of Minutiae-Centered Patches. IEEE Trans. Inf. Forensics Secur. 2018, 13, 2190–2202.

42. Howard, A.G.; Zhu, M.; Chen, B.; Kalenichenko, D.; Wang, W.; Weyand, T.; Andreetto, M.; Adam, H. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. arXiv 2017, arXiv:1704.04861.

43. Chugh, T.; Jain, A.K. Fingerprint Spoof Detector Generalization. IEEE Trans. Inf. Forensics Secur. 2021, 16, 42–55.

44. Lekshmy, G.; Namboodiri, A. One-Shot Sensor and Material Translator: A Bilinear Decomposer for Fingerprint Presentation Attack Generalization. In Proceedings of the 2022 IEEE International Joint Conference on Biometrics (IJCB), Abu Dhabi, United Arab Emirates, 10–13 October 2022; pp. 1–10.

45. Grosz, S.A.; Jain, A.K. SpoofGAN: Synthetic Fingerprint Spoof Images. IEEE Trans. Inf. Forensics Secur. 2023, 18, 730–743.
46. Zhang, K.; Huang, S.; Liu, E.; Zhao, H. LFLDNet: Lightweight Fingerprint Liveness Detection Based on ResNet and Transformer. Sensors 2023, 23, 6854.

Retrieved from https://encyclopedia.pub/entry/history/show/121885