THE APPLICATION OF CONVOLUTIONAL NEURAL NETWORKS FOR FINGERPRINT RECOGNITION: A COMPARATIVE ANALYSIS

Srđan Barzut[1]*,
Milan Milosavljević[2]

[1]Academy of Applied Technical Studies Belgrade, Belgrade, Serbia

[2]Singidunum University, Belgrade, Serbia

Abstract:

The use of convolutional neural networks (CNNs) in the domain of biometric identification is examined in this paper. On a well-known fingerprint evaluation dataset, the three most widely used networks AlexNet, GoogLeNet, and ResNet were tested in the positive identification scenario. In order to improve interclass discrimination and coherence of input data, image enhancement and region of interest segmentation were used to remove inconsistent regions that are typically present on the image peripheral, generating spurious features that negatively affect the neural network learning rate. The fingerprint database prepared in this technique represents the input data of the identification system entirely based on the capabilities of the CNN, allowing direct comparison of networks performances and selection for further implementation. As a result, trained CNNs can be used as a feature extraction module in biometric cryptosystems or robust authentication systems. However, testing results reveal that the proposed technique outperforms many biometric authentication systems, with 97% accuracy rate.

Keywords:

Biometry, Fingerprint Recognition, Convolutional Neural Networks.

INTRODUCTION

The increasing usage of neural networks for the classification and recognition of objects in images has been influenced by breakthroughs in the development of machine learning in recent years. Convolutional neural networks (CNNs) are a promising field of artificial intelligence development, mainly in the function of categorization of input data, with its output being the determination of a preset class of input data. They were named after convolution, an image processing operator that is commonly used to detect object edges and sharpen or blur images. They are categorized as deep neural networks due to their architecture, and they represent the evolution of artificial neural networks known as Multi-Layer Perceptron (MLP). The neural network consists of layers with learning weighted neurons. Each neuron gets input data multiplied by its weights and uses activation functions to apply nonlinearity.

Correspondence:

Srđan Barzut

e-mail:

sbarzut@tehnikum.edu.rs

DOI: 10.15308/Sinteza-2022-224-229

Because fingerprint texture is commonly employed in traditional biometric systems for fingerprint categorization, the usage of CNNs has arisen as a novel way that can help improve the process. However, the texture of fingerprints carries enough distinctive information that when decomposed, the essential differentiation for use in authentication can be attained.

2. RELATED WORK

The preliminary findings of using CNNs to compare or extract biometric features show promise. Transfer learning on two convolutional networks, VGG-F and VGG-S achieved 94.4% and 95.05% fingerprint classification accuracy, respectively, to the applied neural network in [1]. With the development of a novel FCTP-Net neural network architecture in [2], fingerprint classification into six classes achieved the accuracy of 94.87%. Using the National Institute of Standards and Technology (NIST) database and classification into four classes, the accuracy of 92.90% was reached. The architecture of a light convolutional network is presented in [3], which uses segregated ROIs containing singular points for classification. Image normalization and enhancement algorithms are used to fingerprint input images, and findings suggest that utilizing fewer neurons while increasing noise resistance can reach 93% accuracy. Res-FingerNet, a deep neural network for fingerprint categorization, was proposed by the authors in [4]. They used the central loss in the network training phase to minimize intraclass variation and raise interclass fingerprint variance, making the learnt features more discriminant, therefore, enhancing classification accuracy by roughly 1.5%. The performance of the approach was evaluated on the NIST-DB4 data set, achieving the classification accuracy of 97.9%. In [5], a comparison was made between the three most common neural networks for fingerprint type classification in systems with four, five, and eight classes on two fingerprint databases. For the NIST fingerprint database, the average accuracy of 95.55%, 92.51%, and 94.88% was achieved using AlexNet, GoogleNet, and ResNet neural networks, respectively, while evaluation on the Hong Kong Polytechnic University (PolyU) fingerprint database resulted in more than 99% precession for all three networks.

The presence of sufficient discriminant information in fingerprint texture for use in biometric identification systems was first verified in [6]. Machine learning and deep neural networks have advanced to the point where it is now interesting to explore if these techniques have improved enough to extract biometric features and therefore replace the appropriate extraction modules in existing biometric cryptosystems. In [7], a biometric verification system based on two CNN modules was presented, which parallelly extracts features from two fingerprints that are compared. The AlexNet neural network [8] was chosen to extract features, and the concatenation of the extracted features forms the input of the last layer, which calculates the score of their matching. This approach does not use pre-processing and image enhancement, yet the entire system relies on the capabilities of CNN. The EER of the reported results is 17.5%. In the field of CNN applications for minutiae extraction, [9] presents the concept of minutiae extraction by categorizing each pixel of an image into one of 36 classes corresponding to minutiae and one class that does not represent a minutia, while preserving data on point location and orientation. In [10] the module for extracting biometric features from the texture of fingerprints was developed by applying transfer learning to the Alexnet neural network, which completely replaced the traditional module based on Gabor filters. The output layer of the neural network is modified to generate fixed length array, which is then converted into binary domains using quantization techniques, enabling the use of Heming's metrics comparison techniques or the formation of a biometric cryptosystem based on a fuzzy commitment scheme with key lengths of 133 and 199 bits and EERs of 1.13% and 1.23%, respectively.

3. COMPARISON OF CONVOLUTIONAL NEURAL NETWORKS

In order to build a CNN and optimize its performance, the neural network must go through a lengthy training process on a significant set of data, which is time-consuming and has a high computational cost. Instead, we can apply transfer learning to networks that have already been created and trained on data sets with thousands of images and hundreds of classification categories. By customizing existing layers and retraining with a much smaller training set, we can set the network for new classification tasks. The main properties of the three CNNs that were experimentally tested and evaluated in this article are summarized in Table 1.

CNN	Input image size	Total number of layers	Year
AlexNet	227 x 227 x 3	25	2012
GoogLeNet	224 x 224 x 3	144	2014
ResNet	224 x 224 x 3	50 / 101 / 152	2015

Table 1 - Properties of the evaluated CNN

CNNs require as many samples as possible in a training set. In case of fingerprints, this cannot be achieved, but it is necessary to enroll one identity with only a few sample images. This negatively affects the accuracy of the neural network and is a challenge for CNN's application in biometrics. By generating multiple instances of one input image, by rotating it in the range of ± 24 ° with a step of 6 °, we achieve a larger training set [10]. This improves the system's accuracy while also making it less sensitive to minor fingerprint rotations during sampling. With fingerprint rotations prepared in this approach, we gain 45 images for each class, which we use to retrain the CNN.

In any traditional biometric system, it is necessary to enhance the input data. In the case of fingerprints, image enhancement is necessary to eliminate background noise that occurs during acquisition and to reduce intensity variability as a result of differences in surface pressure on sensor during sampling. The reference point plays a key role in the segmentation of the region of interest and its precise determination greatly affects the accuracy of the system. The central point of the core print, i.e., the pixel in which one papillary line forms the maximum concavity compared to the others, was chosen as the reference point. The region of interest is selected in accordance with the input parameters of the applied neural network. For the AlexNet neural network, the size of the input image is 227 x 227 px, while GoogleNet and ResNet require a size of 224 x 224 px. The image is cropped to the desired dimensions, with the reference point in the ROI's center. In this approach, the region of the fingerprint that has been proven to have the required discrimination and coherence is retrieved from the image, and inconsistencies in the image that could negatively affect the neural network's learning are discarded.

The original AlexNet neural network [8] has five convolutional layers and three fully connected layers. This network comprises 650 thousand neurons and 60 million parameters. The last fully connected layer is adapted to generate 1024 features that can be used to form a biometric template, i.e., a digital representation of the input fingerprint image. An additional fully connected layer was added to classify 100 fingerprints based on the number of different identities found in the fingerprint databases used. The results presented in the paper were achieved by training the network with an initial learning rate of 0.001 in a series of 96. Figure 1 shows the network performance after the training process in 400 epochs.

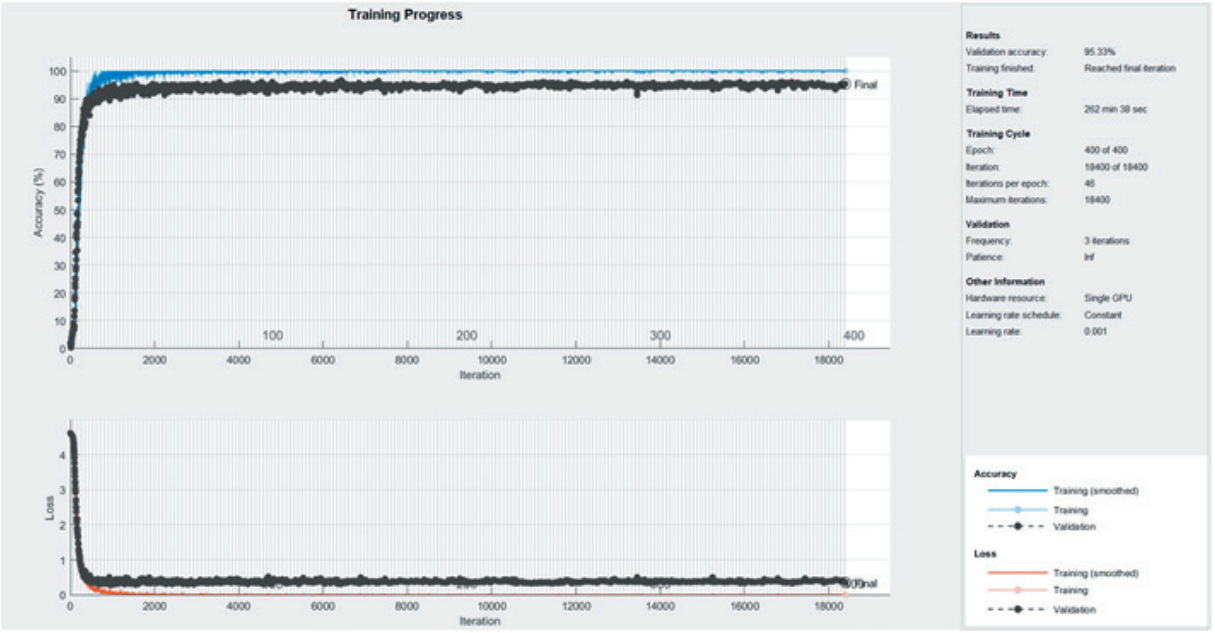

Figure 1 - AlexNet training performance.

GoogLeNet [11] is a convolutional neural network that was constructed in 2014. It has 144 layers, with 22 layers holding function parameters and five layers for compression. GoogLeNet is based on small convolutions, which minimize the number of parameters significantly. This network has only seven million parameters compared to the AlexNet network, which has 60 million. This was accomplished by employing the concept of combining multidimensional convolutions into a single layer. The benefit of applying different dimensions of convolutional filters in parallel is that the global (5x5) and local (3x3) properties may now be distinguished independently. The last fully connected layer is modified to extract 1024 features, and another fully connected layer is added to represent the output for 100 classes, just as it was done in AlexNet. The transfer learning is conducted with an initial learning rate of 0.001 in a series of 48. Figure 2 shows the achieved network performance after the training process in 100 epochs.

ResNet (Residual Network) [12] was developed into three different models, each with a different number of layers. In this research, an experimental version with 101 layers and approximately 43 million parameters was used. In terms of compression, its architecture differs significantly from AlexNet and GoogLeNet networks. The invention of this network was followed by a study into why, rather than improving, the performance of the neural network is degraded when the number of layers is increased. ResNet's fundamental aim was to create a "identity shortcut link" that bypasses one or more layers. The authors proposed the introduction of blocks to overcome this problem, in which the middle layers of each block learn the function of the residual relative to the block's input, as opposed to the traditional network, in which each layer is expected to learn only new and different feature maps. The middle layers can gradually reduce their weights to zero, resulting in a block residual that reflects the function of identity. The classification layer was modified to work with 100 classes based on the specified fingerprint test database, and the last fully connected layer was adjusted to extract 1024 features when customizing this network. The results provided in the research were obtained by training the network in a series of 10 with an initial learning rate of 0.001. Figure 3 depicts the network performance achieved after 15 epochs of training.

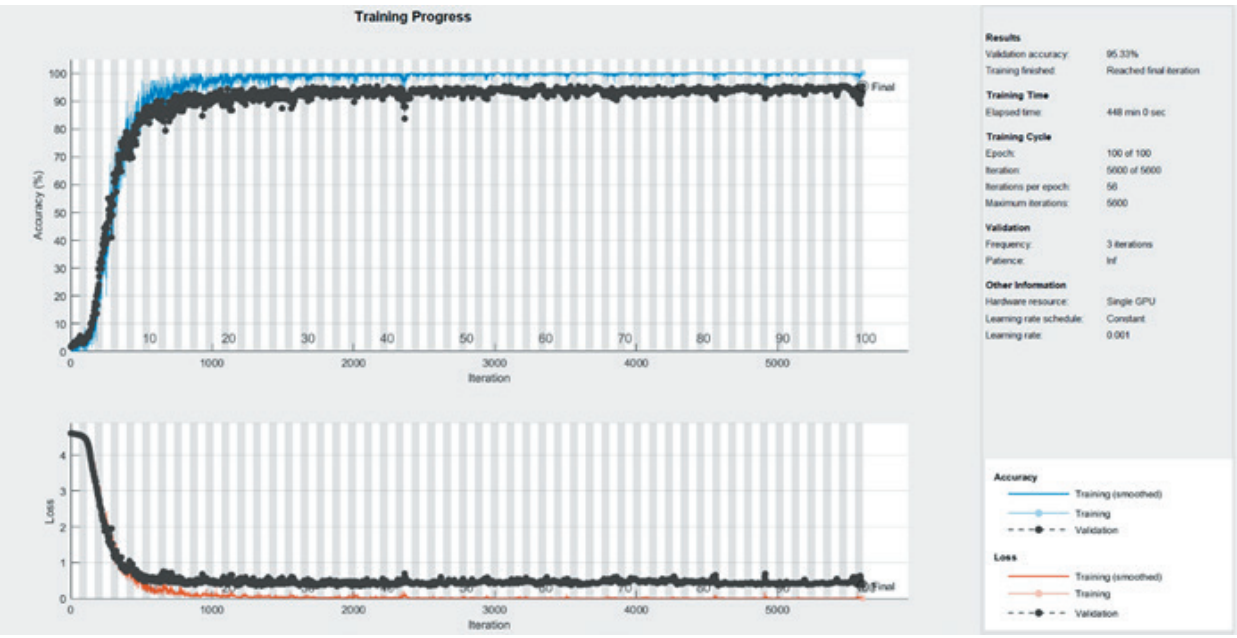

Figure 2 - GoogLeNet training performance.

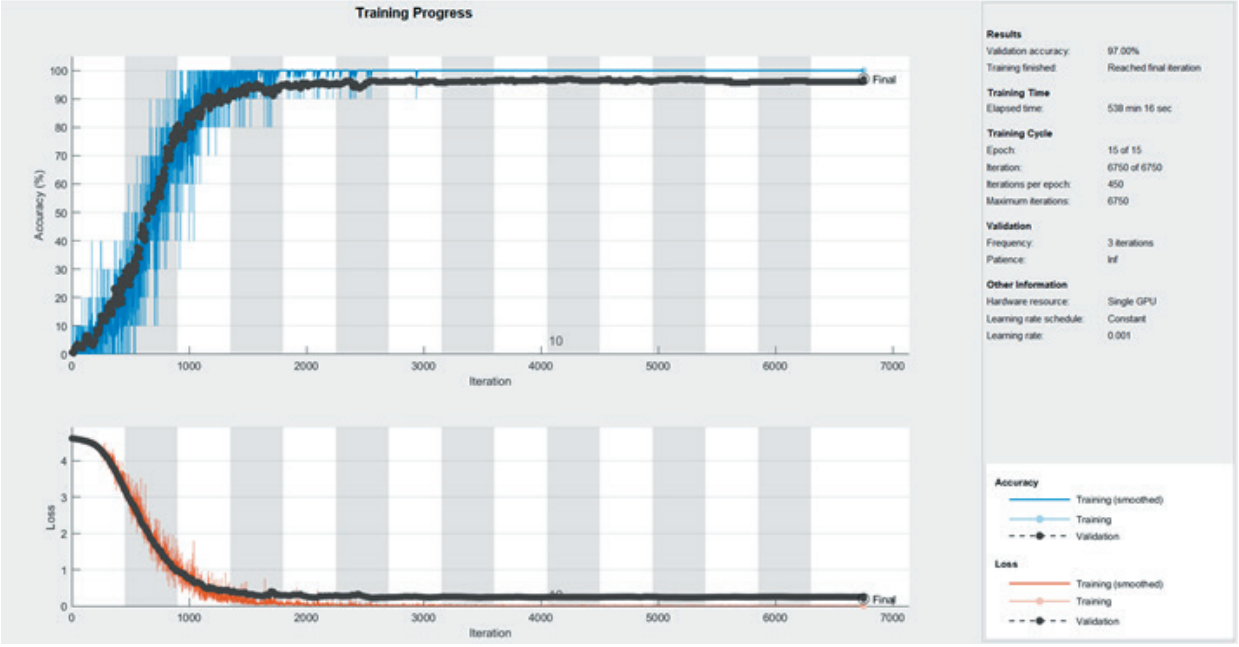

Figure 3 - ResNet training performance.

4. EXPERIMENTAL RESULTS

For effective comparison with other concepts, Fingerprint Vendor Competition database DB2 (FVC2000 DB2) [13] was used for experimental testing of the proposed fingerprint identification system. The database consists of 800 fingerprints collected by a capacitive sensor, and each identity is represented by eight fingerprints. The dimensions of the images are 256 x 364 px in resolution of 500 dpi.

Each class's first five fingerprints were used for network training and identity registration, while the last three were used for system accuracy verification. The experiment was run on a laptop with an Intel i7-8750H processor, 16GB of RAM, and an Nvidia GeForce GTX1050 graphics card, using Matlab 2018a. To examine the accuracy of CNNs, we used the same learning set and a variety of epoch lengths to train all three networks. Table 2 compares the accuracy gained, the amount of time spent on network training, and the number of epochs used.

CNN	Verification accuracy [%]	Training time [min]	Number of epochs
AlexNet	93.67	33	50
AlexNet	94.33	142	200
AlexNet	95.33	263	400
GoogLeNet	94.00	149	40
GoogLeNet	94.67	179	60
GoogLeNet	95.33	448	100
ResNet	96.33	225	6
ResNet	96.67	375	10
ResNet	97.00	538	15

Table 2 - Comparative overview of CNNs performances

5. CONCLUSION

Biometrics has long been used in criminology for positive and negative identification, and it has become increasingly prevalent in the commercial sector for access control, time and attendance, authentication on mobile devices, ATMs, mobile banking, etc. As a result of the foregoing, biometric authentication technique research and development are extremely important. The use of CNNs in biometric identification is analyzed in this research. The experimental results of the three most frequent CNNs in the positive identification scenario support the proposed system's perspective and the application of CNNs in biometric-based authentication systems and cryptosystems. All three networks achieved a high level of accuracy. In terms of accuracy, the ResNet neural network achieved the best verification result of 97%, while the AlexNet neural network reached 100% training accuracy in just 33 minutes, resulting in 93.67% verification accuracy. The comparative analysis and experimental findings reported here are expected to serve as a springboard for further research, improvements to existing solutions, and inspiration for future breakthroughs.

6. REFERENCES

[1] D. Michelsanti, A. D. Ene, Y. Guichi, R. Stef, K. Nasrollahi and T. B. Moeslund, "Fast Fingerprint Classification with Deep Neural Networks," in *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*, 2017.

[2] F. Wu, J. Zhu and X. Guo, "Fingerprint pattern identification and classification approach based on convolutional neural networks," *Neural Computing and Applications*, vol. 32, no. 10, p. 5725–5734, 2020.

[3] W. Jian, Y. Zhou and H. Liu, "Lightweight Convolutional Neural Network Based on Singularity ROI for Fingerprint Classification," *IEEE Access*, vol. 8, p. 54554–54563, 2020.

[4] S. Ge, C. Bai, Y. Liu, Y. Liu and T. Zhao, "Deep and discriminative feature learning for fingerprint classification," in *3rd IEEE International Conference on Computer and Communications (ICCC)*, 2017.

[5] C. Militello, L. Rundo, S. Vitabile and V. Conti, "Fingerprint Classification Based on Deep Learning Approaches: Experimental Findings and Comparisons," *Symmetry*, vol. 13, p. 750, 2021.

[6] A. K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, p. 846–859, 2000.

[7] B. Bakhshi and H. Veisi, "End to End Fingerprint Verification Based on Convolutional Neural Network," in *27th Iranian Conference on Electrical Engineering (ICEE)*, 2019.

[8] A. Krizhevsky, I. Sutskever and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Communications of the ACM*, vol. 60, no. 6, p. 84–90, 2017.

[9] V. H. Nguyen, J. Liu, T. H. B. Nguyen and H. Kim, "Universal fingerprint minutiae extractor using convolutional neural networks," *IET Biometrics*, vol. 9, no. 2, p. 47–57, 2019.

[10] S. Barzut, M. Milosavljević, S. Adamović, M. Saračević, N. Maček and M. Gnjatović, "A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks," *Mathematics*, vol. 9, no. 7, p. 730, 2021.

[11] C. Szegedy, Wei Liu, Yangqing Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke and A. Rabinovich, "Going deeper with convolutions," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015.

[12] K. He, X. Zhang, S. Ren and J. Sun, "Deep Residual Learning for Image Recognition," in *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016.

[13] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of fingerprint recognition, 2nd ed., London: Springer, 2009.