Hand-Based Biometric System Using Convolutional Neural Networks

Katerina Prihodova [1] 🆔, Miloslav Hub [1] 🆔

Abstract

Today, data security is an increasingly hot topic, and thus also the security and reliability of end-user identity verification, i.e. authentication. In recent years, banks began to substitute password authentication by more secure ways of authentication because passwords were not considered to be secure enough. Current legislation even forces banks to implement multi-factor authentication of their clients. Banks, therefore, consider using biometric authentication as one of the possible ways. To verify a user's identity, biometric authentication uses unique biometric characteristics of the user. Examples of such methods are facial recognition, iris scanning, fingerprints, and so on. This paper deals with another biometric feature that could be used for authentication in mobile banking applications; as almost all mobile phones have an integrated camera, hand authentication can make a banking information system more secure and its user interface more convenient. Although the idea of hand biometric authentication is not entirely new and there exist many ways of implementing it, our approach based on using convolutional neural networks is not only innovative, but its results are promising as well. This paper presents a modern approach to identifying users by convolutional neural networks when this type of neural network is used both for hand features extraction and bank user identity validation.

Keywords: Data Security, Authentication, Biometric Authentication, Convolutional Neural Networks, Hand-base Biometric System.

1 Introduction

In general, security is a topical issue both for the public and the private sectors (Fuka, Baťa & Lešáková, 2017). By a directive of the European Banking Authority (EBA) on payment services in the internal market (PSD2), banks are forced to implement a double authentication method for payment transaction verification. In the past, it was enough for a bank to authenticate its electronic banking client only in one way (often by a static password or by a one-time password sent by SMS). Nowadays, however, at least two independent authentication methods must be used. It means that authentication must be implemented by combining two of the three authentication options: knowledge-based (what you know), token-based (what you have), and biometrics (what you possess) (Joshi, 2012).

Higher e-banking security requirements, which are simultaneously enforced by corresponding legislation, force banks to look for new ways of verifying their clients' identities. Therefore, banks often consider implementing biometric systems in their banking information systems,

[1] Institute of System Engineering and Informatics, Faculty of Economics and Administration, University of Pardubice, Studentská 84, Pardubice 2, Czech Republic

✉ katerina.prihodova@student.upce.cz

whose part is a mobile application through which the bank's clients control their bank accounts. By definition, biometric systems use unique biometric characteristics to determine a person's identity (Clodfelter, 2010). Generally, these biometric characteristics can be split into two categories based on their nature: physiological (e.g. fingerprint, iris, face, hand) and behavioral characteristics (e.g. signature, gait, gesture) (Faundez-Zanuy, 2006). In practice, biometric systems can work in two modes – verification mode or identification mode. The goal of verification mode is to determine whether the authenticated user has provided a true identity, based on a comparison with the user's record in the database. In identification mode, a user does not claim his or her identity; instead, their identity is automatically determined based on a comparison with the records of all users in the database (Jain et al., 2000). Biometric systems are considered to be highly secure and practical compared to other methods (Prabhakar, 2003; Unar, 2014).

Of course, banks' concern is not only increasing the security of their information systems (double authentication) but also the convenience of the user interface of the applications through which their clients control their bank accounts. At present, banks often allow their clients to sign in the mobile banking application by a fingerprint. Fingerprint readers are quite often integrated into present-day mobile devices but are still not standard equipment for cheaper mobile devices. Also, with this method of verification, certain groups of users, especially the elderly, have problems. Unlike the fingerprint reader, an integrated camera is quite common in today's mobile devices.

The integrated camera on mobile devices can be used to recognize a person by face or hand. Face recognition encounters security issues; for example, there are cases when an impostor signed in by using a freely available photograph of the victim's face. Moreover, using a face as a biometric feature requires a front camera called a selfie camera. If we want to maximize the number of users for whom biometric authentication will be accessible on a mobile device, it is preferable to choose the hand as a biometric characteristic. We believe that the use of these integrated cameras represents a considerable potential for hand-based biometric systems, and we focus on increasing the reliability of this way of verifying end-user identity.

2 Current hand-based biometric systems

In the relevant current literature on hand-based biometric systems, we encounter the traditional model of a biometric system, where images of the hand are obtained by using a camera or by a scanner in the first step. Characteristic features are then extracted for subsequent comparison with the saved templates.

The biometric sample is most often obtained by a CCD camera (Sanchez-Reillo et al., 2000, Duta, 2009) or by a scanner (Gonzalez et al., 2003, Ferrer et al., 2007). Most hand-based biometric systems work with 2D hand images (Xu, 2013). However, there are also hand-based biometric systems emerging that work with 3D models which can be obtained by using two cameras, mirrors (Sanchez-Reillo 2000), or by using a commercially available 3D digitizer (Ilua et al., 2014).

When the hand image is obtained, the image is pre-processed, and the features are extracted – thus creating a feature set. A requirement for these features is that they have the lowest internal variability and the highest external variability. It means that they are as stable as possible for a given user and that they differ as much as possible between different users. Feature sets are obtained mainly by traditional methods when geometric measurements are used: the width and length of the fingers, finger area, the radii of circles on the fingers and palm. The number of measurements can vary, commonly from 13 to 50 measurements is used (Morales et al., 2008,

Adán et al., 2008). The following traditional method extracts the shape of the hand by the boundary-selection algorithm for silhouette extraction (Fouquier et al., 2008).

Feature extraction is followed by classification in which statistical methods based on different distances can be use as classifiers, e.g. Euclidean (Charfi, 2015), Hamming (Sanchez-Reillo, 2000), or Gaussian mixture model (Sanchez-Reillo, & Gonzalez-Marcos, 2000), or alternatively the Active Appearance Model (Gross et al., 2007). Moreover, it is possible to use Machine Learning algorithms using the method of k-nearest neighbor (Osslan et al., 2011), Support Vector Machines (Marcos 2005, Shanmukhappa & Sanjeevakumar 2016), or use neural networks, e.g., BPNN (Firas et al., 2014). The latest methods used to extract biometric features include the use of Siamese convolutional neural networks. These networks have a symmetrical structure and share the values of some parameters. (Ungureanu et al., 2020)

3   Research objective and methodology

So far, deep learning neural networks have been used for feature extraction in biometric systems (Qin, & Yacoubi, 2017, Baldominos et al., 2018), and convolutional neural networks can be included among them.

The objective of this paper is to increase the security of information systems by proposing, validating, and evaluating a modern approach to hand-based biometric systems based on convolutional neural networks. This type of neural network is used not only for feature extraction but both for hand feature extraction and user identity validation. The primary basic concept (Prihodova, 2019) will be extended to further types of convolutional neural networks, and their parameters will be optimized in accordance with user validation accuracy.

Generally, convolutional neural networks can be used for features extraction to images classification. The problem of identification can be understood as a type of classification problem. The typical architecture of the convolutional neural network is shown in Figure 1.
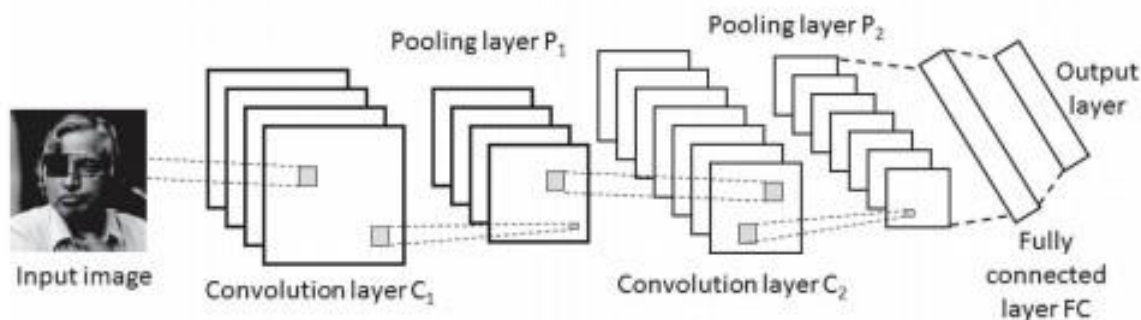

Fig. 1: Typical Convolutional Neural Network architecture. Source: (Sundararajan & Woodard, 2018).

The architecture of a convolutional neural network comprises the input layer and the hidden layers with a different function.

The first hidden layer is a convolutional layer with activation function, for example Relu. This convolutional layer extracts functions and serves for color and edge detection. Deeper convolution layers detect more complex tasks. The second hidden layer is the pooling layer. The tie layer reduces the image and is followed by other convolution layers with an activation function followed by a pooling layer. At the end of the convolutional neural network are fully connected layers with activation function Softmax, used for classification.

For our convolutional neural network learning and testing, the acquired data (hand images) will be split to training and testing data by using the hold-out method, where the data will be divided at a rate of 80% training data and 20% test data. Images of users' hands will be resampled using the nearest neighbor interpolation method to the required size, which is to be the input for individual convolutional neural networks.

Convolutional neural networks will then be used for the identification of particular persons. Firstly, the convolutional neural networks will be taught on training data by optimizing the Learning Rate and Momentum parameters and the backpropagation method. Then, the proposed model will be validated by using the training data, and their accuracy will be determined, compared with each other, and compared with existing approaches.

4   Model creation and validation

The hand-based biometric system model based on a convolutional neural network was created and validated in MATLAB, and experiments were conducted on Intel Core i5 at 1,3GHz. Three pre-taught convolutional neural networks were gradually used in the models – the most commonly used convolutional neural networks AlexNet, GoogLeNet, and ResNet (Karpathy, 2017). The reason why AlexNet was chosen is its testing, which in 2012 was more popularized by CNN in the field of computer vision, compared to newer networks. One of the more modern networks is GoogLeNet; the authors of this network have dramatically reduced the number of parameters (to 4 million, compared to 60 million from AlexNet). The case study will test whether the enormous reduction in the number of parameters affects the recognition of hand images. The last tested network is ResNet, which, as one of the few convolutional neural networks, does not have a fully interconnected output layer. Alex consists of 8 layers, GoogLeNet consists of 22 layers, and ResNet consists of 18 layers.

For the proposed model learning and validation, the 'The Hong Kong Polytechnic University Contact-free 3D/2D Hand Images Database version 1.0' (HKPU, 2019) was used. It is a commonly used reference database and therefore it can be compared with the results of previous research. This database consists of 570 hand images. There were right-hand images from 114 persons in the database, each person having provided five hand images. The participants were mainly students and employees of Hong Kong Polytechnic University, aged 18 to 50, from multiple ethnic groups. The database was created within four months. All hand images were taken indoors. During the measurement, it was necessary to hold the hand at a distance of 0.7 m from the scanner, empirically chosen to maximize the relative size of the hand in the acquired image frame. Participants were asked to keep their hands parallel to the digitizer, palm facing the camera. Each time a scan was taken, the participant changed the position of the hand slightly in order to simplify the hand segmentation task, the background behind the user's hand was ensured to be of black color. The obtained images were numbered for each user by an identification number. The resolution of these images is 640 x 480 pixels (Kanhangad et al., 2011). A sample of the right-hand pictures from the database is shown in Figure 2.

***Fig. 2**. Right hand images from the database. Source: (Kanhangad et al., 2011).*

These datasets of 570 hand images were split into training data (456 images) and test data (114 images) by using the hold-on method with the rate 80:20.

After that, these images were converted to the required size of 227x227x3 for AlexNet and 224x224x3 for both GoogLeNet and ResNet model by using the nearest neighbor interpolation method. In the pre-processing phase, adjusting the size of the input is a single point.

After that, the Mini-batch training method, which is one of a variety of back-propagation algorithms, was used for the training of individual variants of convolutional neural networks. Mini-batch training methods were chosen because the frequency of model update is higher than the batch gradient descent, which allows more robust convergence and avoids local minima. Another advantage is that Mini-batch is computationally more efficient than stochastic gradient descent. However, its disadvantage is that Error information must be accumulated across mini-batches of training examples as batch gradient descent. Next, the size of the batch had to be determined. Given the computing technology on which the implementation was performed, and the size of the dataset, the batch size was determined to be 128.

The training of neural networks was performed experimentally. Finding the network parameters that ensured the value of the learning error kept below the desired limit is the result of many different test scenarios. The properties of neural networks during the optimization phase are, for example, Learning Rate and Momentum. Parameters were optimized for Learning Rate 0.001 and Momentum 0.9. The contribution of the previous step was set quite high. The learning rate was set very low, since learning takes longer, but when the learning rate decreased, the classification results deteriorated significantly.

A large amount of input data is needed to retrain a convolutional neural network that will provide satisfactory results. Our used dataset is relatively small. In order not to over-train the network, premature termination of learning was used at the moment when the test error started to grow again. All experiments were performed for max 30 epochs with 45 iterations; at these values, there was no over-training of the network. The learning of individual networks lasted from 30 minutes to 5 hours.

All 114 hand images were used to test the models. As a result, the person's identity was determined by using our convolutional neural networks. The success rate of the biometric system is expressed by the ratio of correctly classified persons to the total number of classified persons.

The proposed models of hand-based biometric systems based on the convolutional neural network had an accuracy of 98% to 100 % during the training phase. After the training, the trained models were tested against testing data, and the accuracy ranged from 94.74% to 100.00%. In the testing, the user identification accuracy reached 100% in the model with ResNet. The results of training and testing accuracy of all convolutional neural networks are shown in Tab. 1, and Tab. 2 shows the comparison of our results with related works. Table 3 compares our approach with other biometric characteristics.

Tab. 1. Accuracy of CNNs. Source: Authors.

CNN	Training Accuracy	Test Accuracy	FRR
AlexNet	98.00%	94.74%	5.20%
GoogLeNet	99.80%	99.90%	0.10%
ResNet	100.00%	100.00%	0%

Tab. 2. Comparison with related works. Source: Authors.

Sources	Techniques Applied for Recognition	Size of the Database	Accuracy
Osslan et al. (2011)	Nearest Neighbour	120	70.20%
Firas et al. (2014)	BPNN with MSE value	100	93.00%
Gross et al. (2007)	AAMs	54	90.70%
Marcos (2005)	SVM (Radial basic function)	220	90.00%
Shanmukhappa & Sanjeevakumar (2016)	SVM	570 (same database)	93.23%
Own research	CNN AlexNet	570	94.74%
Own research	CNN GoogLeNet	570	99.90%
Own research	CNN ResNet	570	100.00%

Tab. 3. Comparison with other biometric characteristics. Source: Authors.

Sources	Biometric Characteristic for Recognition	Size of the Database	Accuracy
Liu et al. (2005)	Iris	4 249	97.80%
Monro et al. (2007)	Iris	5 111	100.00%
Cho et al. (2014)	Face	16 128	97.30%
Sharif (2013)	Face	400	99.50%
Mngenge (2015)	Fingerprint	3 904	89.60%
Jain & Feng (2011)	Fingerprint	29 257	74,00%
Own research	CNN AlexNet	570	94.74%
Own research	CNN GoogLeNet	570	99.90%
Own research	CNN ResNet	570	100.00%

5 Discussion

As pointed out, hand-based biometric systems have a vast potential in mobile electronic banking applications that are subject to increased security requirements because almost all current mobile devices are equipped with a rear integrated camera through which biometric features can be obtained.

In this paper, the hand-based biometric system based on convolutional neural networks used both for handheld feature extraction and user identity validation was proposed, modeled,

optimized, verified, and evaluated on actual data. Overall, three types of neural networks (AlexNet, GoogLeNet, and ResNet) were tested, and the results were compared with each other and also with the existing methods.

The results of this comparison support our proposed hand-based biometric authentication model. All three variants (AlexNet, GoogLeNet, and ResNet) achieve more accurate results than previous work; ResNet was able to identify users with 100% reliability on our data. This paper is a case study aiming to demonstrate whether it is at all possible to use such a system. The results of the system are partly influenced by the relatively small number of persons. A small dataset often causes network overtraining. To partially solve the problem of network overtraining which the properties of manual images can bring, the data used was obtained in a partially limited system (hand was always at the same distance from the sensor, fingers always slightly outstretched, even black background).

Another security threat are attacks on the biometric system. The biometric system can be attacked in all its phases, the most common attacks being the forgeries of biometric patterns. Since the proposed method does not have liveness detection, it is possible to bypass it by photographing a hand, which can be done, for example, when a person is sleeping. However, achieving it is more complicated than obtaining a fingerprint, of which we leave a large number. One way of preventing these types of attacks is to use thermal images of the hand, which could detect liveliness.

Further research can be directed to a combination of two-hand and face characteristics that could give much better results. With the ever-improving parameters of cameras in mobile devices, it is also possible to focus on research in which a better camera would be used.

Acknowledgements

ORCID

Katerina Prihodova https://orcid.org/0000-0002-2983-4194

Miloslav Hub https://orcid.org/0000-0002-3167-0918

References

Adán, A., Adán, M., Vázquez, A. S., & Torres, R. (2008). Biometric verification/identification based on hands natural layout. *Image and Vision Computing*, 26(4), 451–465. https://doi.org/10.1016/j.imavis.2007.08.010

Baldominos, A., Saez, Y., & Isasi, P. (2018). Evolutionary convolutional neural networks: An application to handwriting recognition. *Neurocomputing*, 283, 38–52. https://doi.org/10.1016/j.neucom.2017.12.049

Charfi, N., Trichili, H., Alimi, A. M., & Solaiman, B. (2015). Personal recognition system using hand modality based on local features. In *Proceedings of the 11th International Conference on Information Assurance and Security* (pp. 13–18). IEEE. https://doi.org/10.1109/ISIAS.2015.7492764

Cho, H., Roberts, R., Jung, B., Choi, O., & Moon, S. (2014). An efficient hybrid face recognition algorithm using PCA and GABOR wavelets. *International Journal of Advanced Robotic Systems*, 11(4), 59. https://doi.org/10.5772/58473

Clodfelter, R. (2010). Biometric technology in retailing: Will consumers accept fingerprint authentication? *Journal of Retailing and Consumer Services*, 17(3), 181–188. https://doi.org/10.1016/j.jretconser.2010.03.007

Directive. (2015). *Directive EU 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366

Duta, N. (2009). A survey of biometric technology based on hand shape. *Pattern Recognition*, 42(11), 2797–2806. https://doi.org/10.1016/j.patcog.2009.02.007

Faundez-Zanuy, M. (2006). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine*, 21(6), 15–26. https://doi.org/10.1109/MAES.2006.1662038

Faundez-Zanuy, M., & Mérida, G. M. N. (2005). Biometric identification by means of hand geometry and a neural net classifier. In Cabestany J., Prieto A., Sandoval F. (Eds.) *Computational Intelligence and Bioinspired Systems, IWANN 2005*, (pp. 1172–1179). Springer. https://doi.org/10.1007/11494669_144

Ferrer, M. A., Morales, A., Travieso, C. M., & Alonso, J. B. (2007). Low cost multimodal biometric identification system based on hand geometry, palm and fingerprint texture. In *Proceedings of the 41st Annual IEEE International Carnahan Conference on Security Technology* (pp. 52–58). IEEE. https://doi.org/10.1109/CCST.2007.4373467

Firas M., & Zainab S. (2014). A New Features Extracted for Recognition a Hand Geometry using BPNN. *International Journal of Scientific & Engineering Research*, 5(9), 232–237.

Fouquier, G., Likforman, L., Darbon, J., & Sankur, B. (2007). The biosecure geometry-based system for hand modality. In *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP* (pp. I-801-I-804). IEEE. https://doi.org/10.1109/ICASSP.2007.366029

Fuka, J., Baťa, R., & Lešáková, P. (2017). The Phenomenon of Terrorism as a Challenge for the Czech Republic. In *Proceedings of 29th International Business Information Management Association Conference* (pp. 1483–1493). International Business Information Management Association.

Gonzalez, S., Travieso, C. M., Alonso, J. B., & Ferrer, M. A. (2003). Automatic biometric identification system by hand geometry. In *Proceedings of the IEEE 37th Annual 2003 International Carnahan Conference on Security Technology* (pp. 281–284). IEEE. https://doi.org/10.1109/CCST.2003.1297573

Gross, R., Li, Y., Sweeney, L., Jiang, X., Xu, W., & Yurovsky, D. (2007). Robust Hand geometry Measurement of Personal Identification using Active Appearance Models. In *Proceedings of the First IEEE International Conference on Biometric: Theory, Applications and systems* (pp. 1–6). IEEE. https://doi.org/10.1109/BTAS.2007.4401936

Iula, A., Hine, G., Ramalli, A., & Guidi, F. (2014). An improved ultrasound system for biometric recognition based on hand geometry and palmprint. *Procedia Engineering*, 87, 1338–1341. https://doi.org/10.1016/j.proeng.2014.11.709

Jain, A. K., & Feng, J. (2011). Latent fingerprint matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 33(1), 88–100. https://doi.org/10.1109/TPAMI.2010.59

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM*, 43(2), 90–98. https://doi.org/10.1145/328236.328110

Joshi, A., Kumar, S., & Goudar, R. H. (2012). A more multifactor secure authentication scheme based on graphical authentication. In *Proceedings of the 2012 International Conference on Advances in Computing and Communications* (pp. 186–189). IEEE. https://doi.org/10.1109/ICACC.2012.43

Kanhangad, V., Kumar, A., & Zhang, D. (2011). A unified framework for contactless hand verification. *IEEE Transactions on Information Forensics and Security*, 6(3), 1014–1027. https://doi.org/10.1109/TIFS.2011.2121062

Karpathy, A., Johnson J., & Fei-Fei L. (2017). *CS231n: Convolutional Neural Networks for Visual Recognition*. http://cs231n.github.io/convolutional-networks/

Liu, X., Bowyer, K. W., & Flynn, P. J. (2005). Experiments with an improved iris segmentation algorithm. In *Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies* (pp. 118–123). https://doi.org/10.1109/AUTOID.2005.21

Mngenge, N. A., Mthembu, L., Nelwamondo, F. V., & Ngejane, C. H. (2015). A fingerprint indexing approach using multiple similarity measures and spectral clustering. In *Proceedings of the* 12th Conference on Computer and Robot Vision (pp. 208–213). IEEE. https://doi.org/10.1109/CRV.2015.34

Monro, D. M., Rakshit, S., & Zhang, D. (2007). DCT-based iris recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 586–595. https://doi.org/10.1109/TPAMI.2007.1002

Morales, A., Ferrer, M., Díaz, F., Alonso, J., Travieso, C. (2008). Contact-free hand biometric system for real environments. In *Proceedings of the 16th European Signal Processing Conference*. IEEE.

Osslan, O., Humberto, D., Vianey, G., Leticia, O., & Hiram, M. (2011). Biometric Human Identification of Hand Geometry Features using Descrete Wavelet Transform. In H. Olkkonen (Ed.) *Discrete Wavelat Transform – Biomedical Applications* (pp.251–266). InTech. https://doi.org/10.5772/19508

Patel, S., & Pingel, J. (2019). *Introduction to Deep Learning: What Are Convolutional Neural Networks*. MatlabWorks. https://uk.mathworks.com/videos/introduction-to-deep-learning-what-are-convolutional-neural-networks--1489512765771.html

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, 1(2), 33–42. https://doi.org/10.1109/MSECP.2003.1193209

Příhodová, K. (2019). Convolutional neural networks in hand-based recognition system. In *Proceedings of the 34th International Bussiness Information Management Association Conference*. International Business Information Management Association.

Qin, H., & El-Yacoubi, M. A. (2017). Deep representation-based feature extraction and recovering for finger-vein verification. *IEEE Transactions on Information Forensics and Security*, 12(8), 1816–1829. https://doi.org/10.1109/TIFS.2017.2689724

Ross, A., & Jain, A. (2003). Information fusion in biometrics. *Pattern Recognition Letters*, 24(13), 2115–2125. https://doi.org/10.1016/S0167-8655(03)00079-5

Sharif, M., Shah, J., Mohsin, S., & Raza, M. (2013). Sub-Holistic Hidden Markov Model for Face Recognition. *Research Journal of Recent Sciences*, 2, 10–14.

Sanchez-Reillo, R. (2000). Hand geometry pattern recognition through gaussian mixture modelling. In *Proceedings 15th International Conference on Pattern Recognition* (pp. 937–940). https://doi.org/10.1109/ICPR.2000.906228

Sanchez-Reillo, R., & Gonzalez-Marcos, A. (2000). Access control system with hand geometry verification and smart cards. *IEEE Aerospace and Electronic Systems Magazine*, 15(2), 45–48. https://doi.org/10.1109/62.825671

Sanchez-Reillo, R., Sanchez-Avila, C., & Gonzalez-Marcos, A. (2000). Biometric identification through hand geometry measurements. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22(10), 1168–1171. https://doi.org/10.1109/34.879796

Shanmukhappa, A., & Sanjeevakumar, M. (2016). Biometric Personal Identification System: A Multimodal Approach Employing Spectral Graph Charakteristics of Hand Geometry and Palmprint. *International Journal of Intelligent Systems and Applications*, 8(3), 48–58. https://doi.org/10.5815/ijisa.2016.03.06

Sundararajan, K., & Woodard, D. (2018). Deep learning for biometrics: A survey. *ACM Computing Surveys*, 51(3), 1–34. https://doi.org/10.1145/3190618

HKPU. (2019). The Hong Kong Polytechnic University Bezkontaktní 3D / 2D ruční Images Database verze 1.0. http://www.comp.polyu.edu.hk/~csajaykr/myhome/database_request/3dhand/Hand3D.htm

Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition*, 47(8), 2673–2688. https://doi.org/10.1016/j.patcog.2014.01.016

Ungureanu, A. S., Salahuddin, S., & Corcoran, P. (2020). Towards unconstrained palmprint recognition on consumer devices: A literature review. *IEEE Access*, 8, 86130–86148. https://doi.org/10.1109/ACCESS.2020.2992219

Xu, S., Li, M., Ding, J. F., & Cui, Y. Q. (2013). Personal identification by fusing hand shape geometry and palmprint features. *Applied Mechanics and Materials*, 278–280, 1228–1231. https://doi.org/10.4028/www.scientific.net/AMM.278-280.1228