Pertanika J. Sci. & Technol. 27 (4): 1723 - 1733 (2019)

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Matching Fingerprint Images for Biometric Authentication using Convolutional Neural Networks

Abdulmawla Najih*, Syed Abdul Rahman Al-Haddad Syed Mohamed, Abdul Rahman Ramli Shaiful Jahari Hashim and Nabila Albannai

Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

ABSTRACT

The use of biometric features, to authenticate users of different applications, is growing rapidly in recent years, according to the high sensitivity of the protected information and the good security that biometric authentication provides. In this study, a method is proposed to measure the similarity between two fingerprint images, using convolutional neural networks, instead of classifying them. Thus, modifying the users that the proposed method can recognize is a matter of adding or removing model images of the users' fingerprints. The similarity between the fingerprint image and every model image was measured in order to select the user with the highest similarity to the input image as the recognized user, where that similarity measure was compared to a threshold value in order to authenticate that user. The evaluation results of the proposed method, using FVC2002_DB1 and FVC2004_DB1 showed that the proposed method had 99.97% accuracy with 0.035% False Acceptance Rate (FAR) and 0% False Rejection Rate (FRR). Hence, the proposed method has been able to maintain high accuracy while eliminating the vulnerabilities of biometric authentication systems imposed by the use of separate stages for features extraction and similarity measurement.

Keywords: Biometric authentication, convolutional neural networks, fingerprints, machine learning

ARTICLE INFO

Article history:
Received: 29 November 2018
Accepted: 25 June 2019
Published: 21 October 2019

E-mail addresses:
nabdulmawla@gmail.com (Abdulmawla Najih)
sar@upm.edu.my (Syed Abdul Rahman Al-Haddad Syed Mohamed)
arr@upm.edu.my (Abdul Rahman Ramli)
sjh@upm.edu.my (Shaiful Jahari Hashim)
rehamranemrahf2009@gmail.com (Nabila Albannai)
* Corresponding author

INTRODUCTION

The rapid growth in Information Technology (IT) has emerged the need to protect sensitive and personal data from any unauthorized access. Many techniques are proposed to protect these data, such as the secret-based method, where login credentials are required from the users to access these data.

ISSN: 0128-7680
e-ISSN: 2231-8526

However, the importance of securing these data and the sensitivity of such methods to simple attacks, such as shoulder surfing, have imposed the need for more secure techniques (Nagatomo et al., 2018; Sun et al., 2018). Thus, the use of biometric authentication systems has attracted significant attention in recent years.

Biometric authentication systems rely on collecting distinctive information from a specific part of the human body, in order to distinguish one individual from another. The recognized individual can, then, be authenticated to the system or data protected by the biometric authentication system(McAteer et al., 2019), if that individual has the required privileges. This information can be extracted from the physiological or behavioral characteristics of the individual. These characteristics are evaluated using five quality measures, which are the acceptability, accessibility, availability, robustness and distinctiveness(Najih et al., 2016). Acceptable characteristics are those that can be collected from individuals without objections from them, according to some concerns such as privacy and security. The accessibility indicates the easiness of extracting this information from the individuals. Availability measures the ratio of individuals that these characteristics can be extracted from, with respect to the population. Robustness indicates the capability of extracting the same characteristics, every time this information is extracted from the individual, while the distinctiveness measures the variation in these characteristics among different individuals (Sinha & Ajmera, 2019; Zou et al., 2018).

Fingerprints are defined as the patterns created by the ripples in the skin of the human fingers. These patterns are very distinctive, where each human has different fingerprint, and very robust, as they do not change over time or because of any external conditions, such as wounds and scratches, where the same pattern is restored. Moreover, fingerprints are highly available in most humans, and do not threaten the privacy of individuals, hence, highly acceptable. Fingerprints can also be collected using cheap sensors that scan the fingers and extract their patterns (Alotaibi & Mahhmod, 2015; Douglas et al., 2018). However, some concerns have been shown regarding using a common surface to collect the fingerprint, which can participate in germs transportation from one individual to another. Thus, some touchless sensors have been implemented to eliminate such concerns, as well as, detecting vital signs from the finger, to deny the use of fake fingerprints (Orrù et al., 2019; Wang et al., 2016). These characteristics have encouraged the use of fingerprints in biometric authentication, rather than many other features, such as the face and iris. The use of facial features has risen some privacy concerns, while collecting information from the iris requires expensive equipment (Barni et al., 2015).

Many biometric authentication systems have been proposed based on fingerprints, where the individual is recognized based on the patterns collected from the fingerprint. Most of these systems measure the similarity between the collected fingerprint and those of the individuals that have the required privileges to access the system of information protected by the biometric authentication system. Different techniques are used to measure the similarity between these fingerprints. The biometric authentication system proposed by Kumar et al., (2016) used Speeded-Up Robust Features (SURF) descriptors to measure the similarity between fingerprint images. Despite the good performance of this method, which has shown only 0.06% EER using fingerprint images selected from the FVC2002 (Maio, Maltoni, Cappelli, Wayman, & Jain, 2002) and FVC2004 (Maio et al., 2004) datasets, the use of separate features extraction and matching stages imposes vulnerabilities to the biometric authentication system. Attackers may produce false features or tamper with the descriptors generated for the features before being matched at the matching stage (Ratha et al., 2001).

According to the outstanding performance of the artificial neural networks, on both accuracy and execution time measures, these networks have been employed to accelerate the performance of fingerprint biometric authentication systems. The method proposed by Peralta et al., (2018) uses a convolutional neural network to classify the fingerprint image into one of the five classes of fingerprints, defined by Henry, (1905) and shown in Figure 1. By classifying the input fingerprint images, as well as all the images of the known individuals in the database, the comparisons conduct to recognize the individual is limited to the number of model images that belong to the same class that the input fingerprint image belongs to. The performance of the convolutional neural networks is evaluated and compared to different other classifiers, using multiple datasets. The results show that the convolutional neural networks have outperformed all other classifiers in all of the used datasets, with a maximum classification accuracy of 99.07%. Although this method does not consider matching the fingerprints, the comparison shows the superiority of convolutional neural networks in interacting with fingerprint patterns. This superiority in performance is the result of the ability of neural networks to learn intra- and inter-class variation, so that, more robust decisions can be made by these networks (Michelsanti et al., 2017).

In this paper, a novel method is proposed to measure the similarity between fingerprint images using convolutional neural networks. The proposed method extracts features directly from the pixels' information if the fingerprint image in order to measure the similarity

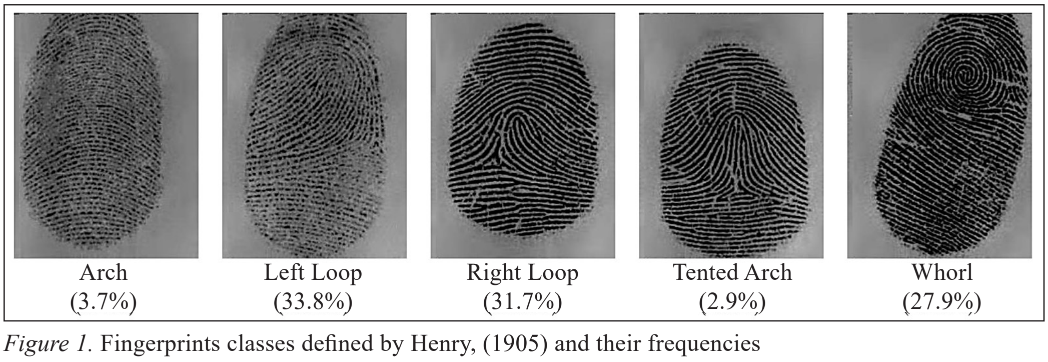

Figure 1. Fingerprints classes defined by Henry, (1905) and their frequencies

between these images. Hence, the features extraction and descriptors generation stages are fused, which eliminates the risk of manipulating these features or descriptors and produce false matches. Moreover, according to the ability of the neural networks to learn the inter- and intra-class variation, the proposed method can produce a better decision, compared to the use of computer-vision techniques like SURF. However, as the proposed method measures the similarity between fingerprint images, instead of classifying them, it is possible to use this method on any datasets without the need to retrain the neural network when the individuals in the dataset change, i.e. the number of neurons in the output layer is constant regardless of the number of individuals in the model fingerprints database.

METHOD

As the proposed method is required to process two fingerprint images and produce a single value that represents the similarity between these two fingerprint images, the input layer of the implemented neural network is required to accept a three-dimensional array while the output layer contains a single neuron. The three-dimensional input contains two fingerprint images, each represented by a two-dimensional array. The similarity measure outputted by the neuron in the output layer is limited in the interval [0,1]. Hence, the activation function used in this neuron was the sigmoid function, which produced values within the required interval, shown in Equation 1. Moreover, according to the significant improvement in the performance of neural networks when the Rectified Linear Unit (ReLU) activation function is used in the neurons of the hidden layers, this activation function is employed in the corresponding neurons(Zhang et al., 2014).

$$\sigma(x) = \frac{1}{1+e^{-x}} \qquad (1)$$

$$ReLU(x) = \begin{cases} x & x \geq 0 \\ 0 & x < 0 \end{cases} \qquad (2)$$

As shown in Figure 2, the shape of the inputs delivered to the convolutional neural network was 200×200×2, i.e., two images with 200×200 pixels each. This input layer was followed by three convolutional layers, with 32, 16 and 8 filters in each, sequentially, where each filter had a size of (10×10), (7×7) and (3×3), for these three layers. Each convolutional layer was followed by a Max-Pooling layer with the size of 2×2 to emphasize the strong features and maintain accurate positioning. The output of the last Max-Pooling layer was flattened and connected to four hidden fully-connected layers, with 512, 256, 128 and 64 neurons, each. Table 1 describes the details of each layer in the implemented neural network.

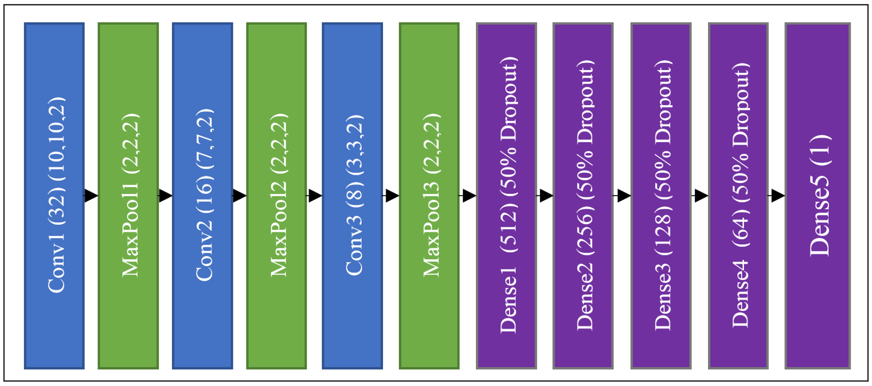

Figure 2. Topology of the convolutional neural network implemented for the proposed methoda

Table 1
Description of the layers in the implemented neural network.

Layer	Input Shape	Neurons (filters)	Activation
Input	200×200×2	-	-
Conv1	200×200×2	32 (10×10×2)	ReLU
MaxPool1	191×191×32	(2×2×2)	-
Conv2	95×95×32	16 (7×7×2)	ReLU
MaxPool2	89×89×16	(2×2×2)	-
Conv3	44×44×16	8 (3×3×2)	ReLU
MaxPool3	(42×42×8)	(2×2×2)	-
Flatten	(21×21×8)	3528	-
Dense1	3528	512	ReLU
Dense2	512	256	ReLU
Dense3	256	128	ReLU
Dense4	128	64	ReLU
Dense5	64	1	Sigmoid

According to the ability of artificial neural networks in recognizing the variation in the inter- and intra-class, the output of neural network is trained to produce the probability of the input fingerprints to be for the same individual, instead of producing an absolute similarity measure as in the use of standard computer-vision techniques, such as SURF. Hence, fingerprint images pairs that belong to the same individual were labeled with one, while pairs of fingerprint images from different individuals were labeled with zero during the training of the neural network. Labels with values of ones indicate 100% confidence that the pairs belong to the same individual, while the zeros indicate 0% confidence that the pair contains fingerprint images of the same individual. Using such approach, the convolutional neural network extracts the knowledge of how to match fingerprints, instead of classifying them, so that, the same trained model can be used with other pairs, that have never been included in the training. As the output of the network is the probability of the fingerprints to belong to the same individuals, new individuals can be recognized by the proposed method by simply including model images of their fingerprints in the pairs inputted to the neural network. Figure 3 shows samples of the inputs and outputs of the convolutional neural network, using the proposed approach.

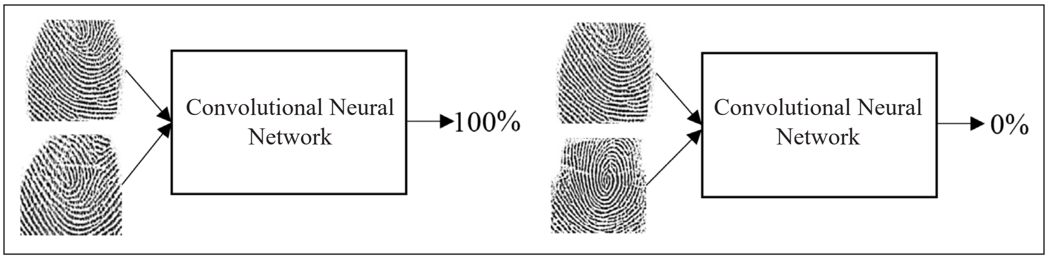

Figure 3. Similarity measurement using the proposed method. Left: fingerprint images of the same individual; Right: fingerprint images for different individuals

To train the neural network for the intended application, triplet loss was used, which was widely used to train neural network for biometric recognition and authentication applications. Per each image in the training dataset, denoted as the anchor image, two additional images were selected from that dataset. One of these images was positive, i.e. was collected from the same individual but was not the same anchor image. The other fingerprint image was the negative, which was collected from any other individual than the one that the anchor image belonged to. Hence, the number of training pars was twice the number of images in the training dataset, as per each image a positive and a negative pair were generated.

RESULTS AND DISCUSSION

In order to evaluate the performance of the proposed method, the model was implemented using Python (Sanner, 1999) programming language with a computer that ran on an Intel® Core™ i7-7700HQ CPU at 2.80GHz frequency and a 16GB of random access memory. The computer also had an Nvidia GTX1080Ti Graphical Processing Unit (GPU) with 4GB of memory, which is used to accelerate the performance of the neural network, implemented using Keras (Chollet, 2015) library, implemented on top of Google's Tensorflow (Abadi et al., 2016) machine learning library. The FVC2002_DB1 (Maio et al., 2002) and FVC2004_DB1 (Maio et al., 2004) datasets were used for the training and evaluation of the proposed method. Five individuals per each dataset, i.e. a total of 10 individuals, were excluded from the training phase and used for the evaluation.

The exclusion of 10 individuals from the training dataset, instead of excluding fingerprint images of individuals that were in the training dataset, was to illustrate the ability of the proposed method to predict the authenticity of images from individuals that were never included in the training. Each image in the training and testing dataset was paired with all the images in the same dataset, including itself. Pairs of the same individual were labeled with one, and the others were labeled with zeros. The neural network was trained for 1000 epochs, before it was evaluated using the testing dataset.

The evaluation of the proposed method was conducted using the confusion matrix shown in Table 2. The threshold value that produced Equal Error Rate was selected, i.e. the False Acceptance Rate (FAR), shown in Equation 3, and False Rejection Rate (FRR), shown in Equation 4, were equal. The value of the threshold that produced the EER was selected based on the Receiver Operating Characteristics (ROC) curve.

Table 2
Confusion matrix of the authentication system

		Predicted	
		Accept	Reject
Actual	Accept	True Acceptance (TA)	False Rejection (FR)
	Reject	False Acceptance (FA)	True Rejection (TR)

$$FAR = \frac{FA}{FA + TR} \qquad (3)$$

$$RFRR = \frac{FR}{FR + TA} \qquad (4)$$

As each individual in these datasets had 8 fingerprint images, the evaluation dataset contained 6400 pairs, 640 from the same individual and 5760 pairs from different individuals, which represented intrusion attempts. The fingerprint images were resized to 200×200 pixels to match the dimensions of the input layer of the implemented neural network and reduced the complexity of computations. Figure 4 shows the ROC curve of the proposed method for the evaluation dataset. This figure illustrates the ability of artificial

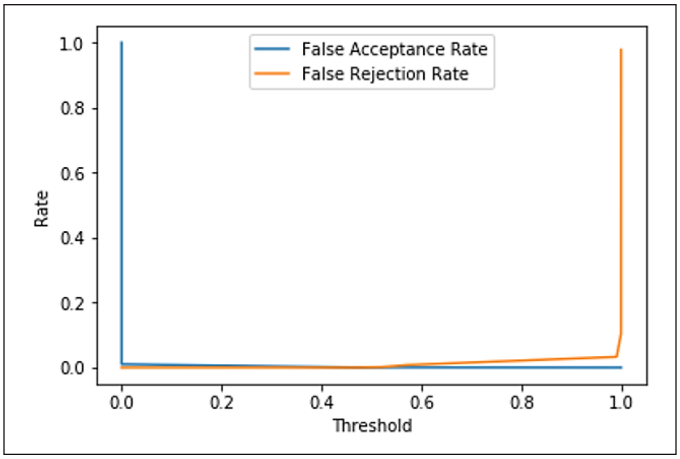

Figure 4. ROC curve of the proposed fingerprint-based authentication method

neural networks to recognize the inter- and intra-class variation, so that, extremely low values are produced per each pair of fingerprint images where each image is collected from a different user. The values produced for fingerprint image pairs collected from the same individual are extremely high, i.e. close to 100%. These values show that the output of the neural network represents the probability of the pair to be for the same individual rather than an absolute similarity measure between the images.

The threshold value that had been able to achieve EER was 0.4754, which had produced confusion matrix shown in Table 3. The accuracy of the authentication decision using the proposed method was 99.97%, with 0.035% FAR and 0% FRR. Although the FAR and FRR are not equal, these are the most similar values that the ROC curve has been able to produce, where selecting different threshold value increases the gap between the values dramatically. Hence the EER of the proposed method is calculated as the average of the FAR and FRR, which is 0.018%, similar to Kumar et al. (2016).

Table 3
Confusion matrix of the authentication decisions of the proposed method at a threshold value of 0.4754

		Predicted	
		Accept	Reject
Actual	Accept	640	0
	Reject	2	5758

Per each individual, the performance measures of the proposed method are shown in Table 4, which shows that the errors occur with a single individual in the entire testing dataset. A comparison with the method proposed by Kumar et al. (2016), which uses SURF-based matching techniques and uses the same datasets for the evaluation, shows that the

Table 4
Evaluation parameters per each individual in the testing dataset

Individual	Evaluation Parameters (%)			
	FAR	FRR	EER	Accuracy
Ind.1	0	0	0	100
Ind.2	0	0	0	100
Ind.3	0	0	0	100
Ind.4	0	0	0	100
Ind.5	0	0	0	100
Ind.6	0	0	0	100
Ind.7	0	0	0	100
Ind.8	0.35	0	0.175	99.69
Ind.9	0	0	0	100
Ind.10	0	0	0	100
Average	0.035	0	0.018	99.97

proposed method has better performance. The method proposed by Kumar et al., (2016) had 99.4% average accuracy with 0.03% average FAR and 0.05% average FRR. Moreover, as the proposed method computes the probability of input fingerprint images to be from the same individual directly from the pixels' information, the vulnerabilities, imposed by extracting features and matching them in different stages, are eliminated.

CONCLUSION

This work proposes a similarity measurement technique for fingerprint images using a convolutional neural network. The use of such approach combines the accuracy of these networks with the flexibility of matching approach, instead of the default classification approach that these networks are usually used for. The results of the performance evaluation experiments illustrate these features, where a matching accuracy of 99.97% is achieved by the neural with 0.035% FAR and 0% FRR. Moreover, the proposed method has been able to outperform the state-of-the-art technique existing in the literature while maintaining high security.

In future work, the application of the same approach is going to be evaluated on different biometric authentication systems, such as face and iris recognition. Such an application can significantly improve the performance of these authentication systems on both security and usability measures.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their constructive comments to improve the quality of this paper.

REFERENCES

Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., ... & Kudlur, M. (2016, November 2-4). Tensorflow: A system for large-scale machine learning. In *12th (USENIX) Symposium on Operating Systems Design and Implementation (OSDI' 16)* (pp. 265-283). Savannah, GA, USA.

Alotaibi, A., & Mahmmod, A. (2015, May 1). Enhancing OAuth services security by an authentication service with face recognition. In *2015 Long Island Systems, Applications and Technology* (pp. 1-6). Farmingdale, NY, USA.

Barni, M., Droandi, G., & Lazzeretti, R. (2015). Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing. *IEEE Signal Processing Magazine, 32*(5), 66-76.

Chollet, F. (2015). *Keras: Deep Learning for Humans*. GitHub repository. Retrieved November 15, 2018 from https://github.com/fchollet/keras.

Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications, 77*(13), 17333-17373.

Henry, E. R. (1905). *Classification and uses of Finger Prints*. London, England: HM Stationery Office.

Kumar, R., Chandra, P., & Hanmandlu, M. (2016). A robust fingerprint matching system using orientation features. *Journal of Information Processing Systems, 12*(1), 83-99.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002, August 11-15). FVC2002: Second fingerprint verification competition. In *Object recognition supported by user interaction for service robots* (Vol. 3, pp. 811-814). Quebec City, Quebec, Canada.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2004, July 15-17). FVC2004: Third fingerprint verification competition. In *International Conference on Biometric Authentication* (pp. 1-7). Hong Kong, China.

McAteer, I., Ibrahim, A., Zheng, G., Yang, W., & Valli, C. J. T. (2019). Integration of biometrics and steganography: A comprehensive review. *Technologies, 7*(2), 34-55.

Michelsanti, D., Guichi, Y., Ene, A. D., Stef, R., Nasrollahi, K., & Moeslund, T. B. (2017, February 27 - March 1). Fast fingerprint classification with deep neural network. In *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2017)* (pp. 202-209). Porto, Portugal.

Nagatomo, M., Kita, Y., Aburada, K., Okazaki, N., & Park, M. (2018). Implementation and user testing of personal authentication having shoulder surfing resistance with mouse operations. *IEICE Communications Express, 7*(3), 77-82.

Najih, A., Al-Haddad, S. A. R., Ramli, A. R., Hashim, S. J., & Nematollahi, M. A. (2016). An overview of multimodal biometric approaches based on digital image watermarking. *Research Journal of Applied Sciences, Engineering and Technology, 13*(6), 481-494.

Orrù, G., Casula, R., Tuveri, P., Bazzoni, C., Dessalvi, G., Micheletto, M., ... & Marcialis, G. L. (2019, In Press). LivDet in Action-Fingerprint Liveness Detection Competition 2019. *arXiv preprint arXiv:1905.00639*.

Peralta, D., Triguero, I., García, S., Saeys, Y., Benitez, J. M., & Herrera, F. (2018). On the use of convolutional neural networks for robust classification of multiple fingerprint captures. *International Journal of Intelligent Systems, 33*(1), 213-230.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal, 40*(3), 614-634.

Sanner, M. F. (1999). Python: a programming language for software integration and development. *Journal of Molecular Graphics and Modelling, 17*(1), 57-61.

Sinha, H., & Ajmera, P. K. (2019). Upgrading security and protection in ear biometrics. *IET Biometrics, 8*(4), 259-266.

Sun, H. M., Chen, S. T., Yeh, J. H., & Cheng, C. Y. (2018). A shoulder surfing resistant graphical authentication system. *IEEE Transactions on Dependable and Secure Computing, 15*(2), 180-193.

Wang, K., Jiang, J., Cao, Y., Xing, X., & Zhang, R. (2016, November 5-7). Preprocessing Algorithm Research of Touchless Fingerprint Feature Extraction and Matching. In *Chinese Conference on Pattern Recognition* (pp. 436-450). Chengdu, China.

Zhang, S., Bao, Y., Zhou, P., Jiang, H., & Dai, L. (2014, May 4-9). Improving deep neural networks for LVCSR using dropout and shrinking structure. In *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 6849-6853). Florence, Italy.

Zou, Y., Zhao, M., Zhou, Z., Lin, J., Li, M., & Wu, K. (2018). BiLock: User Authentication via Dental Occlusion Biometrics. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2*(3), 1-20.