J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

심층 학습 기반의 수기 일회성 암호 인증 시스템☆

Handwritten One-time Password Authentication System Based On Deep Learning

리 준[1] 이 혜 영[1] 이 영 준[1] 윤 수 지[1] 배 병 일[1] 최 호 진[1*]
Zhun Li HyeYoung Lee Youngjun Lee Sooji Yoon Byeongil Bae Ho-Jin Choi

요 약

심층 학습 및 온라인 생체 인식 기반 인증의 급속한 개발에 영감을 받아, 본 논문에서는 심층 학습을 기반으로 필체 인식 및 작성자 검증을 수행하는 수기 일회성 암호 인증 시스템을 제안한다. 본 논문에서는 수기로 작성된 숫자를 인식할 수 있는 합성곱 신경망과, 입력된 필체와 실제 사용자의 필체 사이 유사성을 계산할 수 있는 Siamese 신경망을 설계한다. 본 논문에서는 작성자 검증을 위한 NIST Speical Database 19 제 2판의 첫 번째 응용 사례를 제시한다. 본 논문이 제안하는 시스템은 네 장의 입력 이미지를 기반으로 한 숫자 인식 작업에서 98.58%, 작성자 검증 작업에서 93%의 정확도를 달성했다. 본 논문의 저자들은 제안한 필체 기반 생체 인식 기술이 FIDO 프레임워크 기반의 다양한 온라인 인증 서비스에 활용될 수 있을 것이라 예상한다.

☞ 주제어 : 심층 학습, 수기 인식, 작성자 검증, 인증 시스템, 일회성 암호, FIDO

ABSTRACT

Inspired by the rapid development of deep learning and online biometrics-based authentication, we propose a handwritten one-time password authentication system which employs deep learning-based handwriting recognition and writer verification techniques. We design a convolutional neural network to recognize handwritten digits and a Siamese network to compute the similarity between the input handwriting and the genuine user's handwriting. We propose the first application of the second edition of NIST Special Database 19 for a writer verification task. Our system achieves 98.58% accuracy in the handwriting recognition task, and about 93% accuracy in the writer verification task based on four input images. We believe the proposed handwriting-based biometric technique has potential for use in a variety of online authentication services under the FIDO framework.

☞ keyword : Deep Learning, Handwriting Recognition, Writer Verification, Authentication System, One-time Password, FIDO

1. Introduction

For decades, the main user identification method has been based on the ID-Password (ID-PWD) authentication scheme. Although the ID-PWD scheme is convenient to implement and deploy, it is subject to several risks including forgotten passwords and hacking [1], [2]. For example, anyone who knows the password can easily pass authentication by inputting the password. Biometric techniques have been developed to reduce reliance on passwords, and most mobile devices in use today have adopted biometric authentication. Since biometric identifiers are unique to individuals [3], they can verify the user's identity more reliably than the ID-PWD authentication.

Biometric authentication [4] refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. Physical biometrics are based on physiological characteristics inherent to the user, whereas behavioral biometrics are related to non-physiological characteristics which a user is able to repeat in a unique manner. For example, face, fingerprint, palmprint, and iris are representative physical biometrics, while voice, handwriting, gait, and keystroke are classified as behavioral biometrics. In general, behavioral biometrics are changeable, while physical biometrics cannot be changed. Therefore, it is more challenging to build strong authentication methods

1 School of Computing, KAIST, Daejeon, 34141, Korea
* Corresponding author (hojinc@kaist.ac.kr)
[Received 29 October 2018, Reviewed 1 November 2018, Accepted 4 December 2018]
☆ This work was funded by the Korea Meteorological Administration Research and Development Program under Grant KMI(2017-00410).

based on behavioral biometrics. Fast IDentity Online (FIDO), the world's largest ecosystem for interoperable standards-based authentication, has made biometrics much easier to use by standardizing a variety of authentication methods. It has enabled enterprises and service providers to deploy strong authentication solutions that rely on one or more of the physical biometric characteristics mentioned above. However, few solutions are currently based on behavioral biometrics.

With the rapid development of deep learning techniques, an increasing amount of research has been addressing challenges in biometric authentication using deep learning. Many advancements have been reported in the literature, not only in the physical biometrics domain [5]-[8], but also in the behavioral biometrics domain [9]-[13]. For a more comprehensive survey of the literature, see [14]. Signature is one of the most widely used behavioral biometrics, and various approaches have been proposed for signature-based individual authentication. As a signature usually contains the same content each time it is written, and is written with legal intention, it is often and easily forged. In comparison to signatures, handwriting in general is produced with a natural writing attitude and may contain various characters. Mocking the overall writing style and habits of a person is much more difficult than forging a signature. Therefore, our research problem investigates how a user could be authenticated by recognition of the content and writing style of a given handwritten image.

This problem can be divided into two important tasks: handwriting recognition and writer recognition. Handwriting recognition [15] is the ability of a computer to receive and classify handwritten input from sources such as paper documents, photographs, touchscreens, and other devices. The state of the art of handwriting recognition has been significantly advanced by the emergence of deep learning [16]. Writer recognition is the process of finding (writer identification) or verifying (writer verification) the author of a specific document by comparing the writing to documents in a database of known writers. The goal of writer identification is to match the handwriting specimens to those of the writers, while the goal of writer verification is to verify whether a given document is written by a certain individual. In this work, we concentrate on the issue of offline text-dependent, writer-independent writer verification. Off-line means that the input data are static images of handwritten documents which do not contain any sequential information such as writing speed, pressure, etc. Text-dependent assumes that the reference and the query contain the same text content. Writer-independent means the verification model still works well for new writers without retraining.

In this paper, we propose a handwritten one-time password (OTP) authentication system using deep learning-based handwriting recognition and writer verification techniques. We design a deep convolutional neural network (CNN) model to recognize handwritten digits, and design a Siamese network model [17] to compute the similarity between input and user handwriting. Our proposed system first classifies the given handwritten digit. Then, the system decides whether to accept the writer as a registered user by assessing the similarity between the input handwriting and the user's handwriting. To obtain sufficient data for training, we propose the first known application of the second edition of NIST Special Database 19 (SD19) in a writer verification task.

As an illustration of our proposed approach, we implement a demo of the enhanced OTP authentication system. In the demo, users first register their handwriting in the system. The users' handwriting is saved in a database to be used as the genuine handwriting during authentication. Figure 1 shows an illustrative case of the enhanced OTP authentication system. The user intends to login to a website. After they enter the user ID and password correctly, they must then pass the enhanced OTP authentication. The client in the mobile phone opens an OTP authentication interface and collects the handwritten digits from the users. The authentication system recognizes the digits of the OTP and assesses the similarity between the input handwriting and the registered users' handwriting stored in the database. If the user is a registered user, he/she will pass the authentication. However, attackers who attempt to login to the website with stolen ID, password, and mobile phone will not pass the writer verification step even if they write the correct OTP.

As shown in the demo (Figure 1), the handwritten OTP authentication system differs from a general OTP authentication system in two important ways. First, it utilizes handwritten input instead of keyboard input. Second, it

contains a writer verification mechanism based on a general OTP authentication system. To pass the enhanced authentication, the OTP entered should be not only correct but also written by a registered user. Therefore, the security of the system is enhanced. We believe the proposed method has potential for use in a variety of online authentication services under the FIDO framework.

(Figure 1) Illustrative use of the enhanced OTP authentication system

The rest of the paper is organized as follows. Related work is discussed in Section 2, and Section 3 introduces the detailed implementation methods for the enhanced OTP authentication system. Experimental results are presented in Section 4 and discussed in Section 5, before conclusions are made in Section 6.

2. Related Work

In this section, we present a survey of the literature on handwriting recognition, writer verification, and handwriting-based biometric authentication. We only focus on off-line mode for all of these topics, and mainly consider deep learning-based approaches.

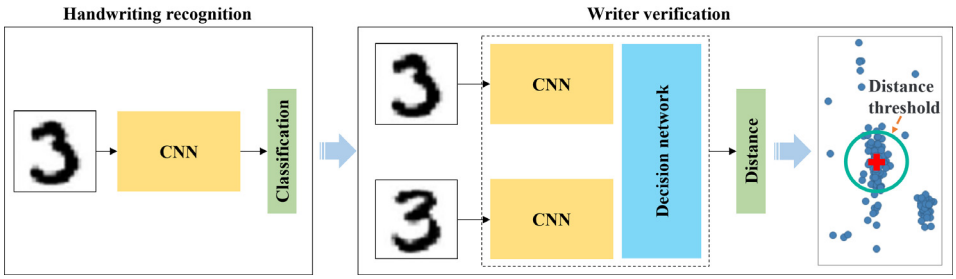
2.1 Handwriting Recognition

Handwriting recognition is one of the critical issues in machine learning. Various promising techniques addressing this problem have been proposed [15], [18], [19]. Among these techniques, deep learning has greatly advanced the capabilities of handwriting recognition. Both CNN [16], [20]-[24] and recurrent neural networks (RNN) [25], [26] have been widely used for off-line handwritten character, digit, and text recognition tasks. To the best of our knowledge, CNN [23] achieves the highest performance in handwritten digit recognition tasks, while RNN [26] achieves the best performance in handwritten text recognition tasks. As our system requires the recognition of handwritten digits, we exploit the CNN model to handle the handwriting recognition task.

2.2 Writer Verification

Extensive literature exists in the field of writer recognition; see [27]-[30] for a survey of the progress in writer identification and verification. As mentioned before, writer identification and writer verification are two different sub-tasks of writer recognition. One difference between these two tasks is that whereas a writer identification system provides classification results for unknown writers, a writer verification system must reject all unknown writers. Some studies have proposed writer verification systems in combination with writer identification tasks [31]-[35], while other research has focused on writer verification tasks directly [36]-[38]. All of the aforementioned writer verification systems are constructed upon handcrafted features, and some of these features (e.g., estimation of the pressure when writing) can only be used in the case of handwriting on paper. Compared to these other approaches, our proposed system can learn features automatically and perform verification efficiently in an end-to-end manner. Moreover, apart from [37], [38], most previous studies have used large handwriting samples for verification. In our approach, we first train a character-level verifier, and then combine multiple characters for the final verification.

Kutzner et al. [39] proposed user verification on the basis of “handwritten password,” which is a handwritten character password sequence on a touch-screen device. However, the resultant system is more similar to a signature-based method because each writer has a unique password. In addition, they classified handcrafted features with Bayes-Nets, KStar, and K-Nearest Neighbor classifiers in a writer identification way.



(Figure 2) Deep learning model for the enhanced OTP authentication system

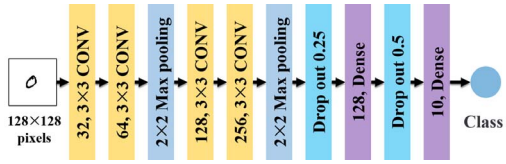
2.3 Biometric Authentication Using Handwriting

To the best of our knowledge, previous studies on handwriting-based biometric authentication have been conducted only in relation to signature verification. See [40] for a survey of off-line signature verification. Various deep learning approaches have been proposed for offline signature verification. Some studies [11], [41]-[43] used CNN in a two-stage manner. First, they trained the CNN to learn writer-independent feature representations. Subsequently, they used these CNN features to train a writer-dependent classifier (e.g., Support Vector Machine) to distinguish between genuine and forged signatures. Our approach differs from these methods in that it is writer-independent. Other studies [44]-[46] utilized deep metric learning to learn a writer-independent distance metric which can reflect similarities and dissimilarities between genuine and forged signatures. The core ideas of these studies are similar to those of ours. Especially, Dey at al. [46] also utilized a convolutional Siamese network to model a signature verification task. However, our approach differs from these studies in two important ways. First, we use handwriting as the input and aim to learn the real writing style and habits of a person. Second, we propose a character-level verifier, which has broader applicability than the signature-based verifier.

3. Method

The enhanced OTP authentication system consists of two modules. One is for handwriting recognition, and the other is for writer verification. We trained a deep CNN model to recognize handwritten digits, and trained a Siamese network model to compute the similarity between input handwriting and user handwriting. After training the two models, we connected them together to implement the core functions of the system. As shown in Figure 2, given one handwritten digit input, our system first classifies the image using the CNN model. Then, the system compares it with the user handwriting of the same class in the database. If the distance between the input handwriting and the user handwriting is below the preset threshold, the system accepts the writer as a registered user.

3.1 Handwriting Recognition

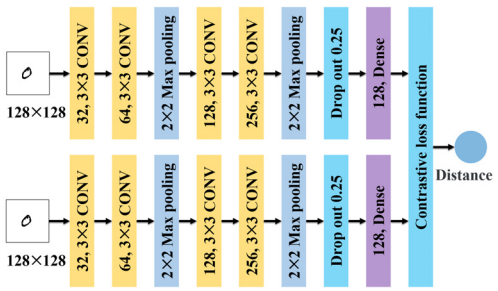


(Figure 3) CNN model for handwriting recognition

As shown in Figure 3, our proposed CNN model is composed of four convolutional layers and two full connected layers. We conducted 2×2 max pooling after every second convolutional layer and drop out before each full connected layer. We used a categorical cross entropy loss function and Adadelta optimizer. In addition, we trained the model with data augmentation. Specifically, we randomly modified the data according to specified shear range, horizontal flip, rotation range, width shift range, and height shift range. In this work, we applied early-stopping to avoid the problem of over-fitting.

3.2 Writer Verification

Siamese networks are a class of neural network architectures that contain twin sub-networks. As shown in Figure 4, our proposed Siamese network model is comprised of two CNN sub-networks which have the same configuration and share weights. Each CNN model has the same architecture as the CNN model of the previous section, except for in the last full connected layer. The CNN models extract features from the input handwriting and the user handwriting. The Siamese model then computes the distance between the two features and outputs the distance. Note that the entire model is trained without data augmentation.



(Figure 4) Siamese model for writer verification

In the Siamese network, the loss function is the key structure that models the similarity metric. One of the most frequently used loss functions in Siamese networks is the contrastive loss function, which was proposed by Hadsell et al. [47]. This loss function can effectively deal with the relationship between the paired data of the twin networks. The detailed function is as follows:

$$L(W,Y,X_1,X_2) = YD^{2}{}_{W} + (1-Y)[\max(0,m-D_W)]^2 \quad (1)$$

where W is the parameter, (Y,X_1,X_2) is the labeled sample pair, D_W is the Euclidean distance of the sample pair, and $m > 0$ is a margin. As shown in equation (1), the contrastive loss function is composed of two parts: the sum square distance of similar pairs and the sum square distance of dissimilar pairs. Minimizing L with respect to W would result in low values of D_W (close to 0) for similar pairs and high values of D_W (close to m) for dissimilar pairs. In this work, we refer to similar pairs as positive pairs and dissimilar pairs as negative pairs. Positive pairs are labeled with 1, and negative pairs are labeled with 0.

4. Experiments

4.1 Data Set

Since the main application of our authentication system involves writing the OTP on the screen of a mobile phone with a finger or capacitive stylus, the ideal training data for our model would be handwritten digits collected from mobile phones. To the best of our knowledge, there is no such data set readily available. Therefore, we proposed training the models with the SD19* data set, which contains NIST's entire corpus of training materials for handprinted document and character recognition. SD19 contains 810 000 128×128-pixel PNG images of digits and alphabetic characters collected from 3600 writers. We used digit images from 3500 writers in our experiment. As handwriting on a mobile phone screen is somewhat different from handwriting on paper, in future research we may consider fine-tuning the models with a small quantity of user-inputted handwriting images.

4.2 Data Partitioning and Preparation

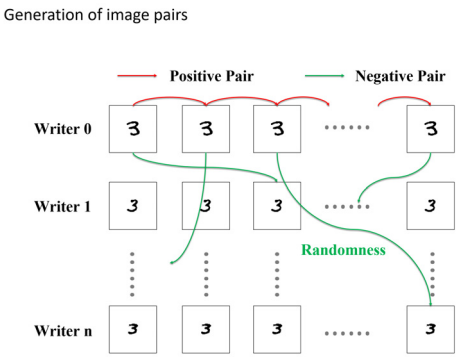
For the CNN model used for handwriting recognition, the size of the training set was 344 307, and the size of the test set was 57 557. For the Siamese network model used for writer verification, pairwise images needed to be generated from the original data set. With 400 000 digital images from 3500 writers, approximately $C^{2}{}_{400000} \approx 80$ billion pairs could be generated. However, this number of pairs would be too large for the system to handle. Thus, the size of the data set was reduced by dividing the data set into small groups and only using part of the total number of pairs. Specifically, the original data set was divided into 7 groups by writer, where each group contained images from 500 writers. Each group was then divided into training, validation, and test sets. The details of data allocation for each group are shown in Table 1. As a second method for reducing the size of the data set,

* https://www.nist.gov/srd/nist-special-database-19

only a small subset of all possible pairs was used. As shown in Figure 5, for each digit class (0 to 9), two adjacent images from the same writer composed a positive pair, and each image combined with a random image from another random writer composed a negative pair. A total of (402 953-(3500×3))×2 = 784 906 pairs were generated, with an equal amount of positive and negative pairs.

(Table 1) Data allocation by group

Data	Writer Index	Number of Writers
Test	1 to 320	320
Validation	321 to 400	80
Training	401 to 500	100
Total	1 to 500	500



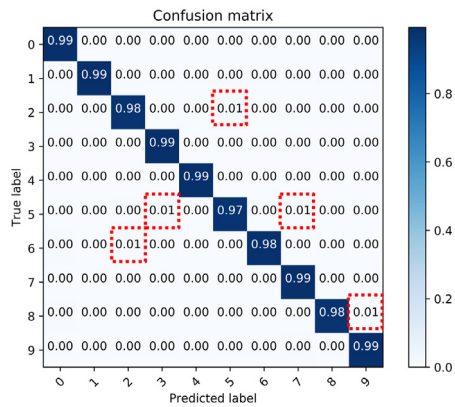
(Figure 5) Generation of image pairs

4.3 Result of Handwriting Recognition Model

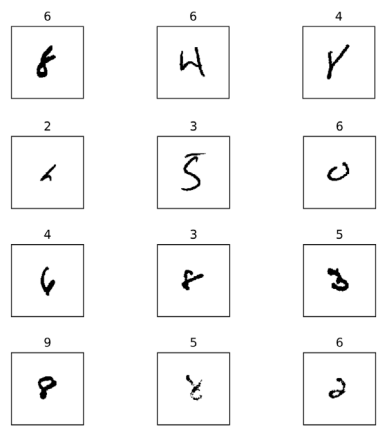
There are several tunable parameters that affect the performance of the CNN model, such as filter size and the number of feature maps in the CNN architecture. We adjusted these parameters to achieve a high performance with a relatively simple architecture. After training the CNN model for handwriting recognition with a total of 344 307 training data points, we achieved 98.58% accuracy on the test set. We also explored a pre-trained model, Inception V3, which only achieved an accuracy of 95.5%.

To the best of our knowledge, SD19 has rarely been used in academic research, so it is difficult to directly compare our results with those of others. As an alternative, we considered handwriting recognition studies based on the MNIST data set. MNIST is a small subset of SD19 and consists of 70 000 down-sampled 28×28-pixel images. The state-of-the-art classification accuracy using the MNIST data set is more than 99.7%. Our classification accuracy obtained using the SD19 data set is comparable to this value.

Furthermore, we analyzed the causes of classification errors. From the confusion matrix shown in Figure 6, it can be observed that classification errors occur when classifying similar characters, such as 2 and 5, 5 and 3, or 8 and 9. In addition, we inspected some samples which were classified incorrectly. As shown in Figure 7, some handwritten digit images are ambiguous and indistinguishable even by the human eye.



(Figure 6) Confusion matrix



(Figure 7) Error Samples. The number above each box is the number identified by the system

4.4 Result of Writer Verification Model

We explored the final CNN model architecture described in the previous section to build the Siamese network. The distance threshold was set to 0.5; a discussion regarding how to select a proper threshold follows later. With about 630 000 training data points and 150 000 test data points, our Siamese network achieved an average accuracy of 81.89% on a test set of 7 groups.

(Table 2) Model performance for different writer groups

	Group 1 (Census employees)	Group 2 (High school students)
Test set size	19 156 pairs	21 738 pairs
Elapsed Time	35 s	40 s
Test accuracy	82.13%	77.39%
FRR on test set	16.15%	15.14%
FAR on test set	19.59%	30.09%

Furthermore, we compared the experimental results of the test sets of group 1 and 2 to reveal the factors affecting the test accuracy. From Table 2, it is seen that our writer verification model performed differently for different writer groups. Accuracy for the test set of group 1 was 82.13%, for the test set of group 2 it was only 77.39%. By decomposing the error rate into false rejection rate (FRR) and false acceptance rate (FAR), we found that the FRR of group 1 (16.15%) was very similar to the FRR of group 2 (15.14%). However, the FAR of group 1 (19.59%) was much lower than the FAR of group 2 (30.09%). The higher FAR for group 2 indicates that the negative pairs in group 2 were more difficult to distinguish than those of group 1. One important difference is that the writers comprising group 1 are Census employees, while the writers in group 2 are high school students. Students in the same class could presumably write digits in a similar way, as they could be affected by the same teacher. This analysis implies that the performance of our model depends on the specific user. In the following analysis, we suppose the users come from group 1.

5. Discussion

5.1 Verification with Multiple Input Images

Thus far, we were able to verify the user with approximately 82% accuracy based on only one input image. However, this is not sufficient for a high-performance authentication system. One simple way to improve the accuracy of the system is to require verification of multiple input images. We herein assume that the authentication is successful only when all n input digit images pass verification. We also assume that all of the n digits are different from each other. Then, the relationship between the false positive rate (FPR) for n digits and the FPR for one digit can be deduced, as shown in equation (2). A similar relationship exists between the true positive rate (TPR) for n digits and the TPR for one digit:

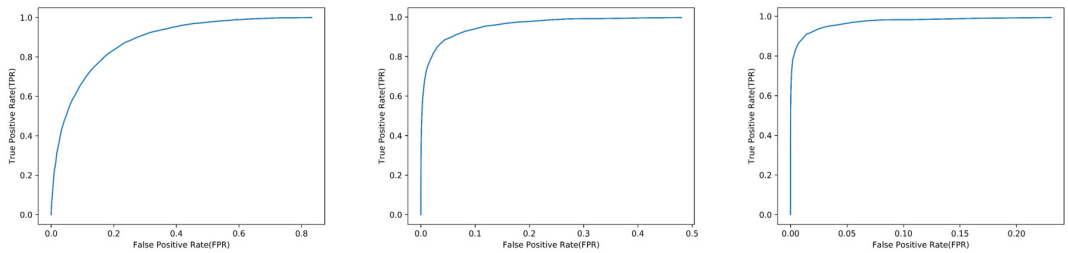
$$FPR_n = FPR_1^n$$
$$TPR_n = TPR_1^n \quad (2)$$

where FPR_n is the FPR for n digits, FPR_1 is the FPR for one digit, TPR_n is the TPR for n digits, and TPR_1 is the TPR for one digit. Additional relationships are $FAR = FPR$ and $FRR = 1 - TPR$.

As shown in Figure 8, the verification performance continually improved as more input images were added. However, in consideration of the user experience, it is best to avoid forcing the users to input too many digits. To choose an appropriate n, we explored the equal error rate (EER). From Table 3, it can be observed that the EER decreased significantly when four input images were used instead of only one image. Upon adding four more images (a total of 8), the EER only decreased by approximately 2% more. Therefore, $n = 4$ was adopted as the optimal number of input digits in our system.

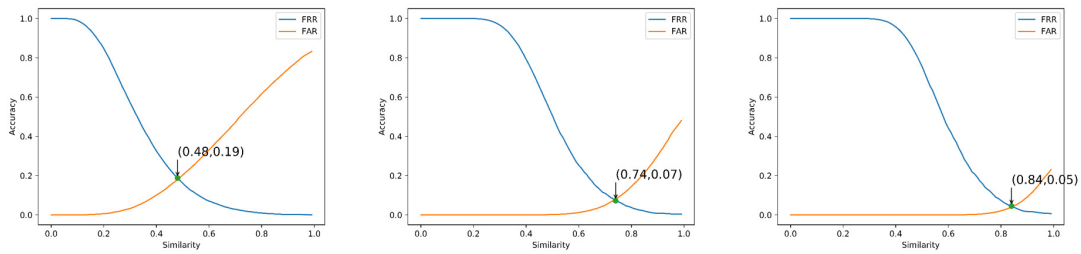
(Table 3) Equal error rate (EER) for different numbers of input digits

Number of digits	EER
1	19%
4	7%
6	6%
8	5%



(a) n = 1 (b) n = 4 (c) n = 8

(Figure 8) Comparison of ROC curves when using multiple input images



(a) n = 1 (b) n = 4 (c) n = 8

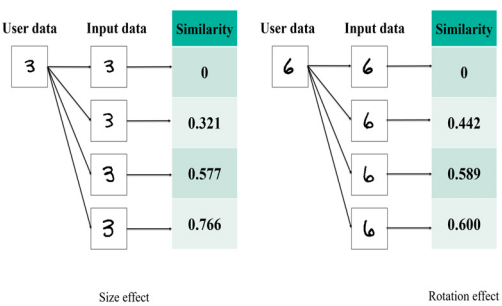
(Figure 9) Comparison of EER curves when using multiple input images

5.2 Determination of Distance Threshold

In this section, we discuss how to select a proper distance threshold to balance the FAR and FRR. As shown in Figure 9, the intersection of the FAR and FRR curves corresponds to the EER and the corresponding distance threshold. As more input images were employed, the EER decreased and the distance threshold increased. With $n = 4$, the EER was about 7% and the distance threshold was 0.74. We were able to verify the user with approximately 93% accuracy using four input images.

5.3 How to Fake the User's Handwriting

Several experiments were conducted to reveal some factors that affect our verification model. These factors would be the key points for someone wishing to fake the user's handwriting, and thus they are also the key points governing the security for users. As shown in Figure 10, the first factor identified was the size of the handwritten digits. When a larger digit was written, the distance between the input image and the genuine user handwriting became larger. The second factor was the angle of handwriting. As an input digit was rotated to more extreme angles, the distance also became larger. In addition, it was found that the position of the digit within the input box was also a factor affecting the verification model. Therefore, to fake the user's handwriting, the hacker would need to reproduce not only the same handwritten character but also the size, angle, and position of the digit. In other words, our system explored various aspects of writing style to improve user security.



(Figure 10) Some factors affecting the verification model

6. Conclusion

In this report, we proposed a handwritten OTP authentication system using deep learning-based handwriting recognition and writer verification techniques. Our proposed system is able to recognize the handwritten OTP input and verify a registered user based on his/her writing style. We implemented a demo of the enhanced OTP authentication system based on the SD19 data set. To the best of our knowledge, this is the first application of the SD19 data set in a writer verification task. Our system achieves 98.58% accuracy in the handwriting recognition task and about 93% accuracy in the writer verification task based on four handwritten digits. We believe that the proposed handwriting-based biometric technique has great potential for use in a variety of online authentication services under the FIDO framework.

Although the accuracy of the proposed system is still not on par with that of existing authentication systems based on fingerprint or face recognition techniques, its performance can be improved by requiring verification of more complex text or by combining it with other behavioral biometrics such as behavioral patterns. In the future, we plan to adopt emerging deep learning architectures for the handwriting recognition and writer verification tasks. Another worthwhile pursuit will be the extension of our system to the verification of both digits and letters.

References

[1] B. Ives, K. R. Walsh, and H. Schneider, “The domino effect of password reuse,” Communications of the ACM, vol. 47, no. 4, pp. 75 – 78, 2004. http://dx.doi.org/10.1145/975817.975820

[2] S. Chakrabarti and M. Singhal, “Password-based authentication: Preventing dictionary attacks,” Computer, vol. 40, no. 6, pp. 68 – 74, 2007. http://dx.doi.org/10.1109/MC.2007.216

[3] V. Matyas and Z. Riha, “Toward reliable user authentication through biometrics,” IEEE Security & Privacy, vol. 99, no. 3, pp. 45 – 49, 2003. http://dx.doi.org/10.1109/MSECP.2003.1203221

[4] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4 – 20, 2004. http://dx.doi.org/10.1109/TCSVT.2003.818349

[5] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “Deepface: Closing the gap to human-level performance in face verification,” in IEEE Conference on Computer Vision and Pattern Recognition, pp. 1701 – 1708, 2014. http://dx.doi.org/10.1109/CVPR.2014.220

[6] R. Wang, C. Han, and T. Guo, “A novel fingerprint classification method based on deep learning,” in 23rd International Conference on Pattern Recognition, pp. 931 – 936, 2016. https://doi.org/10.1109/ICPR.2016.7899755

[7] S. Minaee and Y. Wang, “Palmprint recognition using deep scattering convolutional network,” arXiv preprint arXiv:1603.09027, 2016. https://doi.org/10.1109/ISCAS.2017.8050421

[8] A. Gangwar and A. Joshi, “Deepirisnet: Deep iris representation with applications in iris recognition and cross-sensor iris recognition,” in IEEE International Conference on Image Processing, pp. 2301 – 2305, 2016. http://dx.doi.org/10.1109/ICIP.2016.7532769

[9] Y. Lei, N. Scheffer, L. Ferrer, and M. McLaren, “A novel scheme for speaker recognition using a phonetically-aware deep neural network,” in IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1695 – 1699, 2014. http://dx.doi.org/10.1109/ICASSP.2014.6853887

[10] M. Fayyaz, M. H. Saffar, M. Sabokrou, M. Hoseini, and M. Fathy, “Online signature verification based on feature representation,” in IEEE International Symposium on Artificial Intelligence and Signal Processing, pp. 211 – 216, 2015. http://dx.doi.org/10.1109/AISP.2015.7123528

[11] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Learning features for offline handwritten signature verification using deep convolutional neural networks,” Pattern Recognition, vol. 70, pp. 163 – 176, 2017.

http://dx.doi.org/10.1016/j.patcog.2017.05.012

[12] M. Alotaibi and A. Mahmood, “Improved gait recognition based on specialized deep convolutional neural network,” Computer Vision and Image Understanding, vol. 164, pp. 103 – 110, 2017. http://dx.doi.org/10.1016/j.cviu.2017.10.004

[13] L. Sun, Y. Wang, B. Cao, S. Y. Philip, W. Srisa-An, and A. D. Leow, “Sequential keystroke behavioral biometrics for mobile user identification via multi-view deep learning,” in Joint European Conference on Machine Learning and Knowledge Discovery in Databases, pp. 228 – 240, 2017. http://dx.doi.org/10.1007/978-3-319-71273-4_19

[14] K. Sundararajan and D. L. Woodard, “Deep learning for biometrics: A survey,” ACM Computing Surveys, vol. 51, issue 3, no. 65, 2018. http://dx.doi.org/10.1145/3190618

[15] R. Plamondon and S. N. Srihari, “Online and off-line handwriting recognition: a comprehensive survey,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 1, pp. 63 – 84, 2000. http://dx.doi.org/10.1109/34.824821

[16] D. Ciregan, U. Meier, and J. Schmidhuber, “Multi-column deep neural networks for image classification,” in IEEE Conference on Computer Vision and Pattern Recognition, pp. 3642 – 3649, 2012. https://doi.org/10.1109/CVPR.2012.6248110

[17] J. Bromley, I. Guyon, Y. LeCun, E. Säckinger, and R. Shah, “Signature verification using a ″siamese″ time delay neural network,” in Advances in Neural Information Processing Systems, pp. 737 – 744, 1993. http://dx.doi.org/10.1142/9789812797926_0003

[18] M. Patel and S. P. Thakkar, “Handwritten character recognition in English: A survey,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, no. 2, pp. 345 – 350, 2015. http://dx.doi.org/10.17148/IJARCCE.2015.4278

[19] A. Priya, S. Mishra, S. Raj, S. Mandal, and S. Datta, “Online and offline character recognition: A survey,” in International Conference on Communication and Signal Processing, pp. 0967 – 0970, 2016. http://dx.doi.org/10.1109/ICCSP.2016.7754291

[20] D. Bouchain, “Character recognition using convolutional neural networks,” Institute for Neural Information Processing, vol. 2007, 2006. http://www.academia.edu/download/35095159/Bouchain.pdf

[21] T. Wang, D. J. Wu, A. Coates, and A. Y. Ng, “End-to-end text recognition with convolutional neural networks,” in 21st International Conference on Pattern Recognition, pp. 3304 – 3308, 2012. https://ieeexplore.ieee.org/document/6460871

[22] A. Yuan, G. Bai, L. Jiao, and Y. Liu, “Offline handwritten English character recognition based on convolutional neural network,” in 10th IAPR International Workshop on Document Analysis Systems, pp. 125 – 129, 2012. https://doi.org/10.1109/DAS.2012.61

[23] L. Wan, M. Zeiler, S. Zhang, Y. Le Cun, and R. Fergus, “Regularization of neural networks using dropconnect,” in International Conference on Machine Learning, pp. 1058 – 1066, 2013. http://proceedings.mlr.press/v28/wan13.html

[24] D. S. Maitra, U. Bhattacharya, and S. K. Parui, “CNN based common approach to handwritten character recognition of multiple scripts,” in 13th International Conference on Document Analysis and Recognition, pp. 1021 – 1025, 2015. http://dx.doi.org/10.1109/ICDAR.2015.7333916

[25] A. Graves and J. Schmidhuber, “Offline handwriting recognition with multidimensional recurrent neural networks,” in Advances in Neural Information Processing Systems, pp. 545 – 552, 2009. http://dx.doi.org/10.1007/978-1-4471-4072-6_12

[26] J. Puigcerver, “Are multidimensional recurrent layers really necessary for handwritten text recognition?” in 14th IAPR International Conference on Document Analysis and Recognition, pp. 67 – 72, 2017. http://dx.doi.org/10.1109/ICDAR.2017.20

[27] L. Schomaker, “Advances in writer identification and verification,” in 9th International Conference on Document Analysis and Recognition, vol. 2, pp. 1268 – 1273, 2007. http://dx.doi.org/10.1109/ICDAR.2007.4377119

[28] C. Halder, S. M. Obaidullah, and K. Roy, “Offline writer identification and verification－a state-of-the-art,” in Information Systems Design and Intelligent Applications, pp. 153 – 163, 2016.
http://dx.doi.org/10.1007/978-81-322-2757-1_17

[29] Y.-J. Xiong, Y. Lu, and P. S. Wang, “Off-line text-independent writer recognition: A survey,” International Journal of Pattern Recognition and Artificial Intelligence, vol. 31, no. 05, p. 1756008, 2017.
http://dx.doi.org/10.1142/S0218001417560080

[30] C. Adak, B. B. Chaudhuri, and M. Blumenstein, “Writer identification and verification from intra-variable individual handwriting,” arXiv preprint arXiv:1708.03361, 2017.
https://arxiv.org/abs/1708.03361

[31] M. Bulacu and L. Schomaker, “Combining multiple features for text-independent writer identification and verification,” in 10th International Workshop on Frontiers in Handwriting Recognition, 2006.
https://hal.inria.fr/inria-00104189/document

[32] M. Bulacu and L. Schomaker, “Text-independent writer identification and verification using textural and allographic features,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 701 – 717, 2007.
http://dx.doi.org/10.1109/TPAMI.2007.1009

[33] D. Bertolini, L. S. Oliveira, E. Justino, and R. Sabourin, “Texture-based descriptors for writer identification and verification,” Expert Systems with Applications, vol. 40, no. 6, pp. 2069 – 2080, 2013.
http://dx.doi.org/10.1016/j.eswa.2012.10.016

[34] V. Christlein, D. Bernecker, F. Honig, and E. Angelopoulou, “Writer identification and verification using gmm supervectors,” in IEEE Winter Conference on Applications of Computer Vision, pp. 998 – 1005, 2014.
http://dx.doi.org/10.1109/WACV.2014.6835995

[35] M. N. Abdi and M. Khemakhem, “A model-based approach to offline text-independent arabic writer identification and verification,” Pattern Recognition, vol. 48, no. 5, pp. 1890 – 1903, 2015.
http://dx.doi.org/10.1016/j.patcog.2014.10.027

[36] M. Okawa and K. Yoshida, “Text and user generic model for writer verification using combined pen pressure information from ink intensity and indented writing on paper,” IEEE Transactions on Human-Machine Systems, vol. 45, no. 3, pp. 339 – 349, 2015.
http://dx.doi.org/10.1109/THMS.2014.2380828

[37] A. Bensefia and T. Paquet, “Writer verification based on a single handwriting word samples,” EURASIP Journal on Image and Video Processing, vol. 2016, no. 1, p. 34, 2016.
http://dx.doi.org/10.1186/s13640-016-0139-0

[38] V. Aubin, M. Mora, and M. Santos-Peñas, “Off-line writer verification based on simple graphemes,” Pattern Recognition, vol. 79, pp. 414 – 426, 2018.
http://dx.doi.org/10.1016/j.patcog.2018.02.024

[39] T. Kutzner, F. Ye, I. Bönninger, C. Travieso, M. K. Dutta, and A. Singh, “User verification using safe handwritten passwords on smartphones,” in 8th International Conference on Contemporary Computing, pp. 48 – 53, 2015.
http://dx.doi.org/10.1109/IC3.2015.7346651

[40] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Offline handwritten signature verification－literature review,” in 7th International Conference on Image Processing Theory, Tools and Applications, pp. 1 – 8, 2017.
https://doi.org/10.1109/IPTA.2017.8310112

[41] B. Ribeiro, I. Gonçalves, S. Santos, and A. Kovacec, “Deep learning networks for off-line handwritten signature recognition,” in Iberoamerican Congress on Pattern Recognition, pp. 523 – 532, 2011.
http://dx.doi.org/10.1007/978-3-642-25085-9_62

[42] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Writer-independent feature learning for offline signature verification using deep convolutional neural networks,” in International Joint Conference on Neural Networks, pp. 2576 – 2583, 2016.
http://dx.doi.org/10.1109/IJCNN.2016.7727521

[43] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, “Analyzing features learned for offline signature verification using deep cnns,” in 23rd International Conference on Pattern Recognition, pp. 2989 – 2994,

2016.
http://dx.doi.org/10.1109/ICPR.2016.7900092

[44] A. Soleimani, B. N. Araabi, and K. Fouladi, “Deep multitask metric learning for offline signature verification,” Pattern Recognition Letters, vol. 80, pp. 84 – 90, 2016.
http://dx.doi.org/10.1016/j.patrec.2016.05.023

[45] H. Rantzsch, H. Yang, and C. Meinel, “Signature embedding: Writer independent offline signature verification with deep metric learning,” in International Symposium on Visual Computing, pp. 616 – 625, 2016.
http://dx.doi.org/10.1007/978-3-319-50832-0_60

[46] S. Dey, A. Dutta, J. I. Toledo, S. K. Ghosh, J. Lladós, and U. Pal, “Signet: Convolutional siamese network for writer independent offline signature verification,” arXiv preprint arXiv:1707.02131, 2017.
https://arxiv.org/abs/1707.02131

[47] R. Hadsell, S. Chopra, and Y. LeCun, “Dimensionality reduction by learning an invariant mapping,” in IEEE Computer Society Conference on Computer Vision and Pattern Recognition, vol. 2, pp. 1735 – 1742, 2006.
http://dx.doi.org/10.1109/CVPR.2006.100

◐ 저 자 소 개 ◑

리 준(Zhun Li)
2006년 북경대학교 수학과(이학사)
2008년 인민대학교 통계학과(경제학석사)
2017년~현재 KAIST 전산학부 (이학석사)
관심분야 : 심층 학습, 데이터 마이닝
E-mail : lizhun@kaist.ac.kr

이 혜 영(HyeYoung Lee)
2003년 충남대학교 정보통신컴퓨터공학부 정보통신공학(공학사)
2017년~현재 KAIST 전산학부 (이학석사)
관심분야 : 컴퓨터 비전
E-mail : gracever@kaist.ac.kr

이 영 준(Youngjun Lee)
2017년 성균관대학교 소프트웨어공학과 (공학사)
2017년~현재 KAIST 전산학부 (이학석사)
관심분야 : 자연어 처리
E-mail : yj2961@kaist.ac.kr

윤 수 지(Sooji Yoon)
2017년 전남대학교 컴퓨터정보통신공학과 (공학사)
2017년~현재 KAIST 전산학부 (이학석사)
관심분야 : 자연어 처리
E-mail : sooji@kaist.ac.kr

배 병 일(Byeongil Bae)
2017년 부산대학교 정보컴퓨터공학과(공학사)
2017년~현재 KAIST 전산학부 (이학석사)
관심분야 : 소프트웨어 공학, 기계 학습
E-mail : bae.b.i@kaist.ac.kr

최 호 진(Ho-Jin Choi)
1982년 BS in Computer Engineering from Seoul National University, Korea
1985년 MSc in Computing Software and Systems Design from Newcastle University, UK
1995년 PhD in Artificial Intelligence from Imperial College London, UK
2009년~현재 KAIST 전산학부 교수
관심분야 : 인공 지능, 자연어 처리, Biomedical informatics
E-mail : hojinc@kaist.ac.kr