JOIV : Int. J. Inform. Visualization, 6(1) - March 2022 103-108

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Design on Novel Door Lock Using Minimizing Physical Exposure and Fingerprint Recognition Technology

Seungdo Jeong [a,*]

[a] *Department of Smart Information and Telecommunication Engineering, Sangmyung University, Cheonan, Chungnam, Republic of Korea*
Corresponding author: [*]sdjeong@smu.ac.kr

***Abstract*— Digital door locks are widely used in general homes such as houses and apartments and in spaces where external intrusion must be prevented based on high security and convenience. Recently, smart door locks with additional technologies such as fingerprint recognition and Bluetooth communication have also been developed, and the door lock market is on the rise. Digital door locks are more convenient to use than the existing key-type door locks. However, there are often cases of exploiting security vulnerabilities such as exploiting and invading the user's trace remaining on the door lock. This paper proposes a door lock with a structure that can complement the shape of the current door lock exposed to the outside and minimize the user's fingerprint trace. In addition, a method of reinforcing security is applied using fingerprint recognition through image processing and a random pattern number arrangement. An experiment was conducted to confirm whether the door lock of this type was usable, and the recognition of partially damaged fingerprints was also confirmed. It was shown that the door lock structure proposed in this paper could maximize security by combining fingerprint recognition technology and random pattern numbering while minimizing external exposure.**

***Keywords*— Door lock; fingerprints recognition; random number placement; image processing; convolutional neural network.**

Manuscript received 25 Oct. 2021; revised 5 Nov. 2021; accepted 11 Dec. 2021. Date of publication 31 Mar. 2022.

I. Introduction

Compared to the existing mechanical auxiliary key that uses a key, the digital door lock has high security and has the advantage that it can be used conveniently without carrying the key. Because of these advantages, it is popularly applied to not only industrial door locks but also home door locks, and the door lock market is also showing an upward trend. In particular, Korea is actively exporting overseas and achieved 6th in market share in the US door lock market as of 2019 and 3rd in market share in Thailand and Japan as of 2018 [1]–[3].

By the popularization of digital door locks, convenience has been increased so that an individual can open the door without having a key, but there have been cases in which this advantage is exploited for criminal purposes [4]. In July 2019, a hidden camera that looks the same as a fire alarm was installed to obtain the door lock password of the apartment resident. Afterward, he took advantage of the absence of residents to steal valuables and run away [5]. In January 2019, in Cheongju, Korea, it was revealed that theft was carried out by combining passwords by analyzing fingerprint traces on the door lock number plate installed on the house's front door that was the target of the crime [6].

As can be seen from these examples, digital door locks are more secure than mechanical auxiliary keys, but there is a vulnerability that residential intrusion is possible if only passwords are identified, even if they are not actual residents. For this reason, in order to strengthen the security of the door lock, various door locks such as door locks use short-range wireless communication such as NFC [7], [8] and Bluetooth [9], fingerprint recognition [10, 11], face recognition [12], [13], and voice recognition [14] door locks have been developed and studied [15].

In order to strengthen the security of digital door locks that input passwords, research on biometric door locks using biometric information have been actively conducted. In the case of fingerprint recognition door locks, a door lock that uses the existing pattern of entering password and fingerprint recognition together [11] and a door lock that can open the door immediately through the fingerprint recognition sensor installed on the handle without a password have been developed. However, there is a possibility that this door locks also acquire fingerprints through the oil remaining in the process to open the door.

Door locks using face recognition instead of fingerprint have also been developed [12], [13]. This is convenient

because the door is opened after acquiring a face image through a camera and comparing it with a registered user. However, in the case of a simple 2D image, there may be cases where it is not possible to distinguish a face in a photo, such as an image of an actual face taken by a camera for face recognition and a printed image. To prevent this, research to improve the reliability of facial recognition using a depth camera has also been conducted, but there is a disadvantage that using a depth camera increases the cost and puts a burden on the user [13].

With the recent development of 5G and Internet of Things (IoT) technologies, the smart home market is gradually growing [16], [17]. A smart door lock that can open a door through a mobile phone application that uses short-range wireless communication such as NFC and Bluetooth is also being developed and studied [7]–[15]. Smart door locks have great advantages, such as remotely controlling the door lock through a popular smartphone or checking the door lock status in real-time. However, there is a paradox that it is possible to break in by unlocking the door with only one Smartphone that can open the door. Recently, cyber security issues for these IoT products have emerged, and research to find various threats has been actively conducted [4], [18]–[20]. In order to solve the security vulnerability of such a door lock, fingerprints acquired based on image processing, and door locks using random patterns are presented. It measures the misrecognition rate using open datasets and conducts experiments on actual availability.

II. Materials and Method

Generally used digital door locks are exposed to the outside and may cause a physical impact. To compensate for this problem, a door lock structure that can be buried in a door or wall is proposed, and a password display having a random pattern and a door lock that sets fingerprints used for each number input differently are proposed.

A. Proposed Door Lock Design

1) Structure of door lock: The structure of the door lock proposed in this paper is shown in Fig. 1.

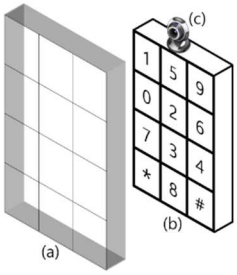

Fig. 1 Example of the door lock structure (a) Tempered glass (b) Display for numeric display (c) Webcam

- (a) is for users to enter the door lock password, and transparent tempered glass, acrylic, etc. are used to reduce external impact and minimize external exposure by allowing additional burying in doors and walls. This reduces the possibility of password-stealing through the aforementioned hidden camera. In addition, it is expected that it will be possible to reduce traces of fingerprints by coating using special materials [21, 22].
- (b) is a display that displays screens to confirm the location of passwords when entering password, increasing security by continuously arranging them to have irregular patterns every time user enters password. (c) is a camera that can observe the location of the number entered by the user and whether the correct fingerprint is used.

2) Process of entering the password: The door lock proposed in this paper has no limit on the number of digits of the password, and it is assumed that there are ten registered fingerprints. When the password is 1234, the fingerprints used in each of the 1, 2, 3, and 4 are different, and all four digits of the password must be entered to ensure that all passwords match and whether or not the door is opened or closed will be decided later. Figure 2 shows the password verification process proposed in this paper. Although the proposed method uses fingerprint recognition technology, there is no need to determine whether or not the fingerprints match if the password does not match. Therefore, it is first checked whether the registered passwords match the numeric keypad provided in a random pattern [23]. If the passwords match, the next check would see if the fingerprints registered in each password match. At this time, if even one fingerprint registered for each number does not match, the door lock cannot be unlocked. For convenience, users can register all numbers using only one of the ten registered fingerprints. In this way, it is possible to increase the number of items that can combine a number and a fingerprint simultaneously, thereby improving security. In addition, when applied as a method using only one fingerprint, convenience similar to the existing fingerprint recognition method may be provided.

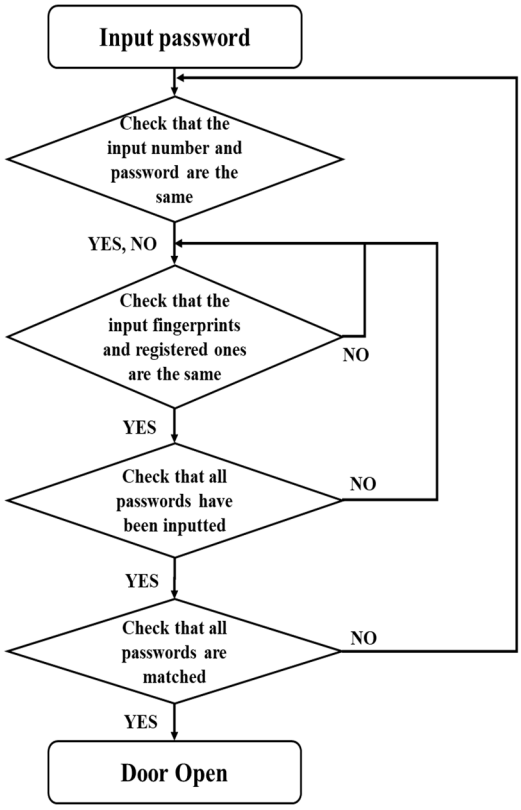

Fig. 2 The flow chart about the password input process

3) Fingerprint recognition: The fingerprint consists of ridges and valleys. The ridge is the convex part where the pores protrude, and the valley is the relatively concave part between the ridge and the ridge. Each fingerprint can be distinguished through the different shapes and features of the ridges and valleys.

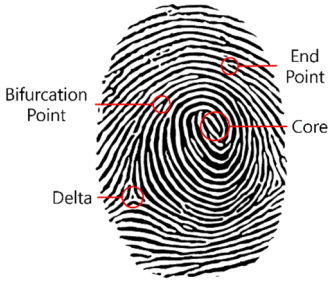

Fig. 3 Features of fingerprint

As shown in Fig. 3, the fingerprint is largely composed of a bifurcation point, endpoint, core, and delta. To facilitate the extraction of these features, methods such as smoothing and binarization are used. After extracting the features, they are compared to confirm the fingerprint matching result [24, 25, 26]. However, in the case of the door lock proposed in this paper, there is a possibility that the features of the fingerprint may be crushed in the process of inputting a number by pressing a finger on a top plate such as transparent glass. To this end, a feature model having a structure of a convolutional neural network (CNN) is used to extract features to determine whether fingerprints match [27, 28].

B. Data and Feature Extraction Model

Even if a door lock is used in one household, several people use it. In this paper, the Sokoto Coventry Fingerprint Dataset (SOCOFing) [29] is used to learn the crushed fingerprints of a large number of people.

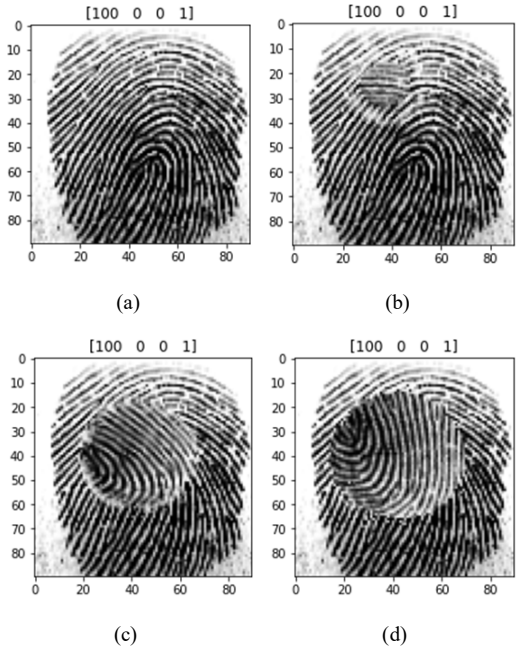

Fig. 4 Examples of the dataset used

(a) Original image (b) Easy level of the altered image (c) Medium level of the altered image (d) Hard level of altered image

1) Data: The SOCOFing dataset provides four types of 55,273 fingerprint images. There are 10 original fingerprint images per person, as shown in Fig. 4(a), and 600 fingerprints are included. In addition, fingerprint images that progressively progressed image conversion, such as optimization, central rotation, and z-cut, as shown in (b), (c), and (d) of Figure 4, are also included [30].

TABLE I
INDEX OF FINGERPRINT IMAGES

Id	Gender	Hand	Finger
1~600	0: male 1: female	0: left 1: right	0: little 1: ring 2: middle 3: index 4: thumb

Also, as shown in Table 1, an index is provided for each image and represents Id, Gender, Hand, and Finger, respectively. As shown in the table, a total of 10 fingerprints are included for each person. This paper proposes a method to register and use different fingerprints according to the password of the door lock. Therefore, it can be said that this fingerprint dataset is suitable for application to the proposed method.

2) Feature extraction model: To open the door lock by fingerprint recognition, it is necessary to compare the fingerprint registered by the user with the fingerprint of the person entering the password on the door lock. For this, open-source is used [31].

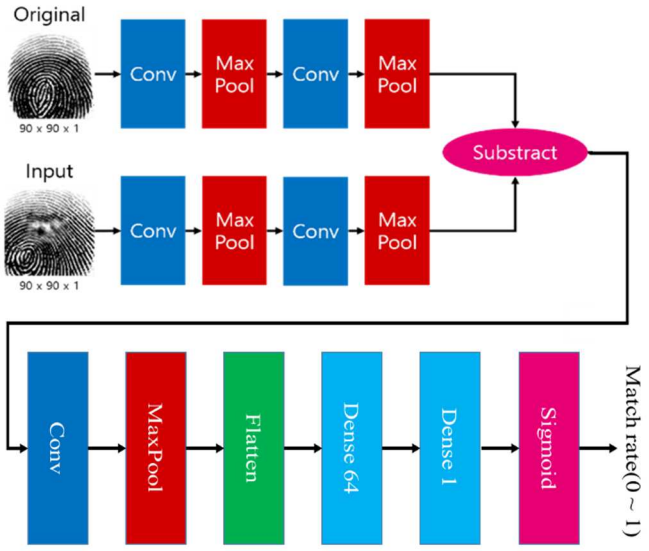

Fig. 5 The architecture of the feature model

The architecture of the model for fingerprint feature extraction and comparison is shown in Fig. 5. The fingerprint image used is a 90 x 90 x 1 image, the original image is the fingerprint registered by the door lock user and stored in the database, and the input image is the fingerprint of the person who enters the password to open the door lock. The feature is extracted and subtracted through two convolutions and MaxPooling. Finally, the concordance rate of the two fingerprints is calculated through the sigmoid function.

III. Results and Discussion

In the proposed door lock, the determination of whether the password matches or not is the same algorithm applied to most door locks, so no individual verification is required. However, in the case of fingerprint recognition, transparent glass is also blocked in the input part to minimize external exposure. Therefore, there is a very high possibility that the resolution may deteriorate even in acquiring a fingerprint image, or distortion may occur in the input process. In other words, the most important part of the verification of the proposed door lock is the accuracy of fingerprint recognition.

Assuming that the door lock presented in this paper is actually used, there is a possibility that the finger is not input in the face but in a rotated form when inputting the password. The SOCOFing data set used for the experiment does not include an image with rotation applied to the entire fingerprint. There is a problem in that it cannot respond to the input type in the environment to which it is actually applied. Therefore, in this paper, rotation of the entire fingerprint can be made in the train and test process so that it can be applied to real cases. In addition, various forms respond to image distortion and perform data augmentation through image processing such as blur, scaling, and translation to supplement learning data.

In the experiment, 100 different fingerprints were used as the test dataset, and the concordance rate was calculated by comparing the original fingerprint image of each fingerprint 1000 times. Thereafter, results with a concordance rate of 80% or less are judged as misrecognition.

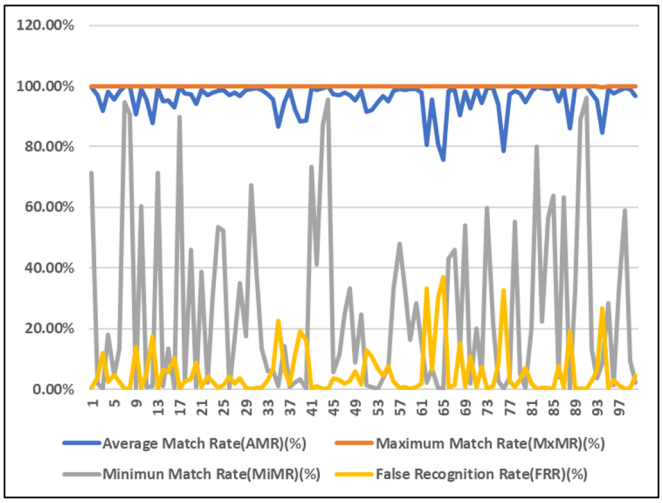

Fig. 6 Experimental results for match rates and false recognition rate

In Fig. 6, the horizontal axis is the index of the test image used in the experiment, and the vertical axis is the ratio (%). Here, the Maximum Match Rate (MxMR) means the value when the highest match rate is obtained among 1000 trials and shows 100% in almost all test images. Minimum Match Rate (MiMR) means the value of the lowest match rate among 1000 trials in the same way. Average Match Rate (AMR) means the average of each match rate over 1000 trials. Finally, False Recognition Rate (FRR) shows the rate of failure to recognize the same fingerprint as the matching rate is less than the threshold value among 1000 attempts. A case where the average was less than 80% was taken as the threshold for misrecognition, and as shown in the figure, most of the test cases showed a concordance rate of 80% or more, indicating that there was no misrecognition. For example, looking at the test result of fingerprint 10, in the order of MxMR, MiMR, AMR, and FRR, they are 100%, 60.51%, 99.03%, and 0.5%, respectively. Interpreting these results, the highest matching rate among 1000 matching tests for fingerprint 10 was 100% and the minimum matching rate was 60.51%. AMR 99.03% means the average matching rate for 1000 times. And the false recognition rate of 0.5% means that only 5 times out of 1000 tests, the matching rate was less than 80%.

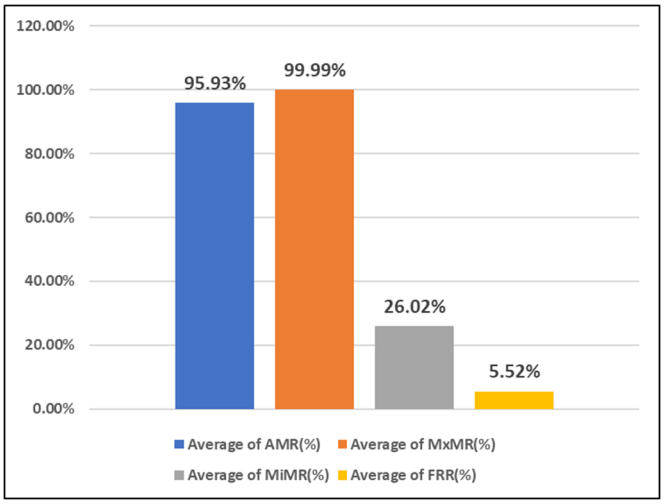

Fig. 7 Average for match rates and false recognition rate

Figure 6 shows the evaluation results for each test case. In order to understand the overall performance, the average of 100 test data for each item was obtained and presented in Fig. 7. The average AMR will be the most important indicator when applied to actual door locks. As shown in the figure, the average AMR is 95.93%, which shows high performance and is evaluated at a level that can be practically applied. The average FRR was 5.52%, which does not seem to be a big problem for door locks used in normal cases. For reference, the average of MxRR and average of MiRR showed results of 99.99% and 26.02%, respectively. The average of MiRR can be interpreted as reaching a level where, on average, 25% of the fingerprints are the same, even in the case of severe damage.

In the next experiment, the difference in recognition rate according to the threshold of false recognition was compared. In the previous experiment, a case where the matching rate was less than 80% in the recognition experiment for the test data was defined as false recognition. However, to strengthen security, it is necessary to raise the threshold of false recognition. Therefore, in this experiment, a case where the matching rate was less than 90% was defined as false recognition, and the resulting false recognition rate was compared. The comparison results are presented in Fig. 8. As shown in the figure, when the matching rate threshold was set to 80%, the false recognition rate was 5.52%. This means that the matching rate did not exceed 80%, with less than about 6% of the total number of trials. If the matching rate threshold is raised to 90%, the false recognition rate will naturally increase, and as shown in the figure, it was confirmed that the actual experiment increased to 9.16%. The matching rate of 90% is a very high reference value in practical application.

When inputting a fingerprint, it is very difficult to record a 90% concordance rate even if there is distortion in the image acquired from the camera, the difference in input angle, rotation of the image, or damage to some fingerprints. Nevertheless, it can be confirmed that the false recognition rate in the proposed method is less than 10%, even based on the 90% matching rate. This is the result of clarifying that the numerical value is sufficiently applicable to practical applications.

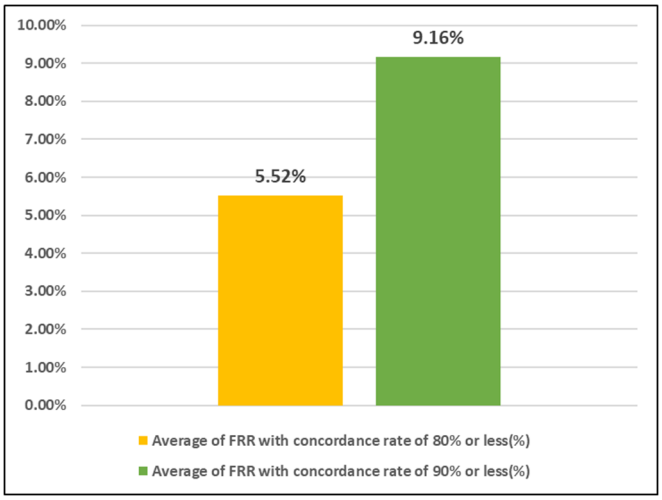

Fig. 8 The result of the false recognition rate according to criteria change

Next, the state of the actual image of the input with a high false recognition rate was examined. Figure 9 is a photograph of the real image showing the lowest matching rate among the three fingerprint images with the highest false recognition rate. The left is the input for recognition, and the right is the original registered image. As shown in the figure, the concordance rates were 13.38%, 4.83%, and 0.31% in the order of (a), (b), and (c). From the results, in (a) case, the rotation has almost no difference from the original image, but the central part of the fingerprint is partially damaged. As a result, it can be seen that the concordance rate is about 13%. In the case of (b), a lot of rotation was made compared to the original image. The degree of damage to the fingerprint in the center was similar to (a), but the coincidence rate was lowered to around 4% due to the degree of rotational difference. Lastly, in the case of (c), it seems that the degree of damage to the central part is the highest among the three. Moreover, the degree of rotation is also more different than the case of (b). This resulted in almost inconsistent results.

As shown in the results of Fig. 9, since the recognition of the input fingerprint uses the CNN network structure to extract and match features, it can be confirmed that the features are extracted without much effect on the damage of the fingerprint itself, matching rate is high. However, when an input is made to the actual door lock, the possibility that the user's input intentionally presses the number with the fingerprint damaged is low. It can be seen that the difference in the input angle at the moment of selecting a number has a greater effect on the matching rate than the damage of the fingerprint itself. The SOCOFing dataset used for training the CNN network does not include rotation data in this paper. To overcome the issue, the rotation data of the fingerprint image was intentionally augmented in training and included in the test data. However, it was difficult to include enough data, and it can be seen that the corresponding learning was not performed properly.

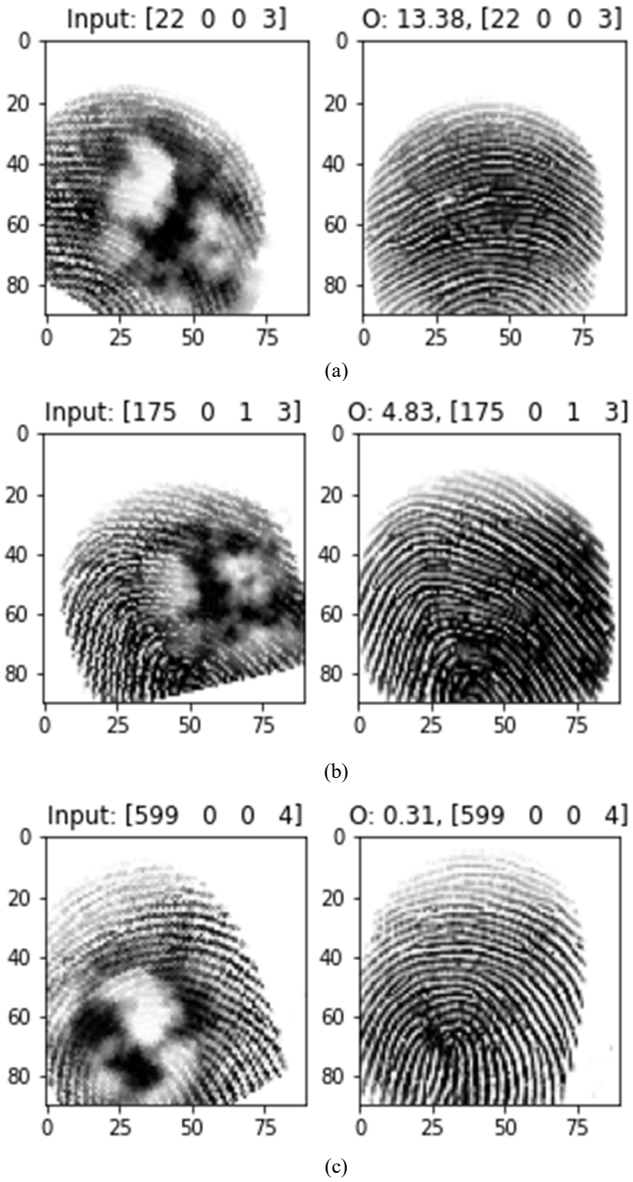

Fig. 9 Part of fingerprint image with high false recognition rate. (a) Image with lowest matching rate among the group with a 37.1% false recognition rate (b) Image with lowest matching rate among the group with a 33.4% false recognition rate (c) Image with lowest matching rate among the group with a 32.8% false recognition rate

IV. Conclusion

Digital door locks have great advantages in high security and portability compared to mechanical door locks that use existing keys and have become the most used device in businesses as well as homes. In addition, with the development of IT technology, products with higher security and convenience, such as fingerprint recognition and facial recognition, are increasing, and the market is also showing growth. Nevertheless, there are a number of cases where the password is used for criminal purposes in various malicious ways. This is because the existing door locks were exposed to the outside, and there were disadvantages of leaving traces of using the door lock. This paper proposes a novel door lock

structure that can recognize fingerprints through image processing to compensate for these shortcomings. In addition, for higher security, a number arrangement with a random pattern and a method using multiple fingerprints were also applied.

In addition, to check whether this door lock is usable, an experiment comparing 100 fingerprints each 1000 times was conducted, and the average coincidence rate was 95.93% and the false recognition rate was 5.52%. Through this, it showed the possibility that the door lock proposed in this paper could be used in practice. It is expected that this door lock can be used in the future if a more detailed door lock structural design and sufficient dataset are used.

REFERENCES

[1] S. H. Lim, “The market trend of door lock in US,” Kotra, Accessed on August 14, 2020. [Online]. Available: https://news.kotra.or.kr/user/globalAllBbs/kotranews/album/781/globalBbsDataAllView.do?dataIdx=183960&column=&search=&searchAreaCd=&searchNationCd=&searchTradeCd=&searchStartDate=&searchEndDate=&searchCategoryIdxs=&searchIndustryCateIdx=&searchItemName=&searchItemCode=&page=1&row=10

[2] M. S. Kim, “The market trend of digital door lock in Thailand,” Kotra, c2020. Accessed on June 11, 2020. [Online]. Available: https://news.kotra.or.kr/user/globalAllBbs/kotranews/album/781/globalBbsDataAllView.do?dataIdx=182562&column=&search=&searchAreaCd=&searchNationCd=&searchTradeCd=&searchStartDate=&searchEndDate=&searchCategoryIdxs=&searchIndustryCateIdx=&searchItemName=&searchItemCode=&page=1&row=10

[3] J. S. Seok, “Smartphone becomes the key! The popularity of smart door lock in Japan,” Kotra, 2019. Accessed on August 1, 2019. [Online]. Available: https://news.kotra.or.kr/user/globalAllBbs/kotranews/album/781/globalBbsDataAllView.do?dataIdx=176490&column=&search=&searchAreaCd=&searchNationCd=&searchTradeCd=&searchStartDate=&searchEndDate=&searchCategoryIdxs=&searchIndustryCateIdx=&searchItemName=&searchItemCode=&page=2&row=10

[4] M. Pavelić, Z. Lončarić, M. Vuković and M. Kušek, "Internet of Things Cyber Security: Smart Door Lock System," International Conference on Smart Systems and Technologies (SST), 2018, pp. 227-232, doi: 10.1109/SST.2018.8564647.

[5] Y. J. Bae, “Thief stealing money by finding a password with a 'fire detector hidden camera'”, CHANNEL A, Accessed on July 17, 2019. [Online]. Available: http://www.ichannela.com/news/main/news_detailPage.do?publishId=000000157205

[6] C. H. Jeon, A man in his 30s who invade an empty house eight times after seeing the fingerprints on the door lock was arrested., Yonhap News Agency, viewed at January 21, 2019. [Online]. Available: https://www.yna.co.kr/view/AKR20190121099600064

[7] R. L. Jorda et al., "Comparative Evaluation of NFC Tags for the NFC-Controlled Door Lock with Automated Circuit Breaker," IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM), 2018, pp. 1-6, doi: 10.1109/HNICEM.2018.8666375.

[8] V. J. Govindraj, P. V. Yashwanth, S. V. Bhat and T. K. Ramesh, "Smart Door Using Biometric NFC Band and OTP Based Methods," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-4, doi: 10.1109/INCET49848.2020.9153970.

[9] M. S. Hadis, E. Palantei, A. A. Ilham and A. Hendra, "Design of smart lock system for doors with special features using bluetooth technology," International Conference on Information and Communications Technology (ICOIACT), 2018, pp. 396-400, doi: 10.1109/ICOIACT.2018.8350767.

[10] Paul, Piash, et al. "Smart Door Lock Using Fingerprint Sensor." BRAC University, pp. 1-13, 2019.

[11] J. Baidya, T. Saha, R. Moyashir and R. Palit, "Design and implementation of a fingerprint based lock system for shared access," IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), 2017, pp. 1-6, doi: 10.1109/CCWC.2017.7868448.

[12] M. Waseem, S. A. Khowaja, R. K. Ayyasamy and F. Bashir, "Face Recognition for Smart Door Lock System using Hierarchical Network," International Conference on Computational Intelligence (ICCI), 2020, pp. 51-56, doi: 10.1109/ICCI51257.2020.9247836.

[13] Zhu, Zhiguo, and Yao Cheng. "Application of attitude tracking algorithm for face recognition based on OpenCV in the intelligent door lock." Computer Communications, vol. 154, pp. 390-397, 2020.

[14] Aiswarya, I. P. "Real Time Smart Door Lock System Using Image Detection and Voice Recognition," International Research Journal of Modernization in Engineering Technology and Science, vol.2, pp. 393-407, 2020.

[15] Patil, Karthik A., et al. "Smart door locking system using IoT." International Research Journal on EngTechnol (IRJET), pp. 3090-3094, 2020.

[16] Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev. "A review of Internet of Things for smart home: Challenges and solutions." Journal of cleaner production, vol.140, pp. 1454-1464, 2017.

[17] Sovacool, Benjamin K., and Dylan D. Furszyfer Del Rio. "Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies." Renewable and sustainable energy reviews, vol.120, 2020.

[18] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." Computer networks, vol.148, 2019, pp. 283-294.

[19] Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future generation computer systems, vol.82, pp. 395-411, 2018.

[20] Amanullah, Mohamed Ahzam, et al. "Deep learning and big data technologies for IoT security." Computer Communications, vol.151, pp. 495-517, 2020.

[21] Belhadjamor, M., et al. "Anti-fingerprint properties of engineering surfaces: a review." Surface Engineering, vol.34, no.2, pp. 85-120, 2018.

[22] Forchelet, Sandra, and Andy Bécue. "Impact of anti-fingerprint coatings on the detection of fingermarks." Journal of Forensic Identification, vol.68, no.3, pp. 348-368, 2018.

[23] Schulz, Marc-André, et al. "A cognitive fingerprint in human random number generation." Scientific reports, vol.11, no.1, pp. 1-7, 2021.

[24] Alsmirat, Mohammad A., et al. "Impact of digital fingerprint image quality on the fingerprint recognition accuracy." Multimedia Tools and Applications, vol.78, no.3, pp. 3649-3688, 2019.

[25] Hindi, Amjad, Majed Omar Dwairi, and Ziad Alqadi. "Analysis of procedures used to build an optimal fingerprint recognition system." International Journal of Computer Science and Mobile Computing, vol.9, no.2, pp.21-37, 2020.

[26] Liu, Feng, et al. "Robust and high-security fingerprint recognition system using optical coherence tomography." Neurocomputing, vol.402, pp. 14-28, 2020.

[27] Minaee, Shervin, Elham Azimi, and Amirali Abdolrashidi. "Fingernet: Pushing the limits of fingerprint recognition using convolutional neural network." arXiv preprint arXiv:1907.12956, 2019.

[28] Tereikovskyi, I. A., et al. "The procedure for the determination of structural parameters of a convolutional neural network to fingerprint recognition." Journal of Theoretical and Applied Information Technology, vol.97, no.8, pp. 2381-2392, 2019.

[29] I. S. Yahaya, R.-G. Ariel, P. Vasile, J. Anne, Sokoto Coventry Fingerprint Dataset, TarXiv preprint arXiv:1807.10609, July. 2018.

[30] Papi, S., Ferrara, M., Maltoni, D., & Anthonioz, A, On the generation of synthetic fingerprint alterations, 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), IEEE, pp.1-6, September 2016.

[31] kairess, https://github.com/kairess/fingerprint_recognition