A Similar Fingerprint Information Detection Algorithm for the Security Enhancement of Biometric Access Authentication Systems in Nuclear Power Plants

Young-Hyun Baek [a*], Sun-Dong Kim [a], Seok-Yun Kim [a], Jun-Myung Lee [a]
[a] *Unioncommunity Co.Ltd, R&D Center*
[*] *Corresponding author: neural76@unioncomm.co.kr*

1. Introduction

The access authentication system is evolving from a physical card method to a biometrics method based on physical characteristics. Types of biometric technology applied to access control systems include fingerprint recognition, face recognition, iris recognition, and vein recognition. This method has the advantage of high security in terms of the convenience of not having to carry a separate physical access tool and the use of unique characteristics of the human body [1–3].

However, illegal acts, including theft of social security numbers or illegal use of access cards when registering biometrics for access, have occurred. For example, in 2019, a security incident occurred in Shin-Gori Units 1 and 2 operated by Korea Hydro & Nuclear Power (KHNP), a national security facility, in which the biometric fingerprints of others were stolen from the resident partner's pass for retirees.

The proposed algorithm can prevent theft of resident registration numbers and the illegal use of access cards by unauthorized persons in the biometric information registration process required for access authentication to security facilities. As a result, a stronger security-access authentication system can be built. The proposed similar-fingerprint-information detection algorithm normalizes the image center coordinates of the registered user fingerprint information and the fingerprint information to be newly registered and then verifies the feature point direction and location information generated through the extraction step. The algorithm calculates the number of similar feature points through 1:1 matching between the acquired feature-point information assigns a score according to the similarity of the fingerprint information.

As a result of the simulation, the proposed algorithm determines the similarity of newly registered fingerprints to previously registered fingerprints and inputs information on the former.

2. Proposed Algorithm

2.1 Characteristic Elements of Biometric Fingerprint

The characteristic elements of a biometric fingerprint are a central point, end point, bifurcation point, and delta, as shown in Fig.1, where the black line is defined as a ridge, and the white area is defined as a valley, representing a valley-like space between the ridges. A fingerprint image is acquired through the process shown in Fig.2 using a dedicated input sensor, and a template is created through an extraction process from the acquired image.

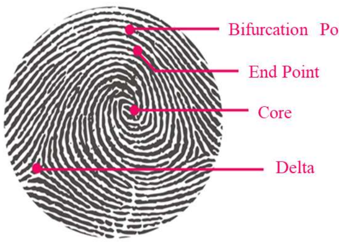


Fig.1. Characteristic elements of a biometric fingerprint.

The step of saving the created template is defined as user registration, and the step of matching the registered template with the new input template is called the user authentication step [1–3].

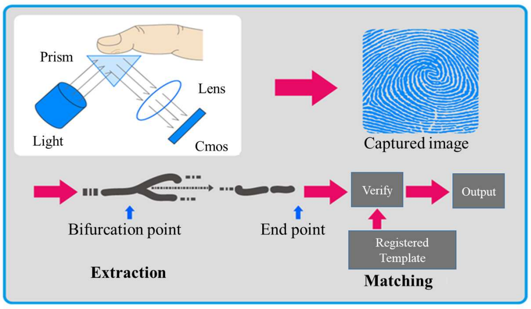


Fig.2. Fingerprint image is acquired process.

2.2 Biometric Access Authentication System

The biometric access authentication system combines the convenience and security of access management using efficient management support to identify the status of visitors based on biometric information (fingerprint, face, iris, and vein) and remote control in case of emergency.

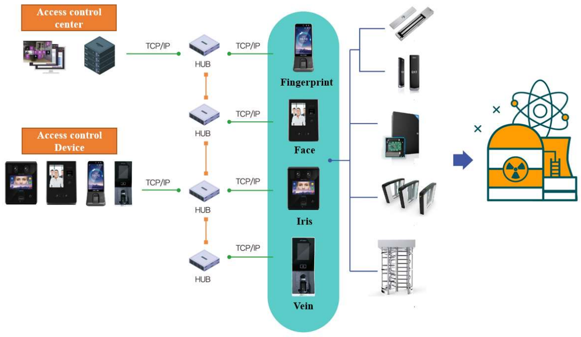


Fig.3. Biometric access authentication process structure diagram in Nuclear Power Plants.

The system composition consists of a communication environment, access control, and card reader, as shown in Fig.3.

2.3 Proposed Fingerprint Similar Information Detection Algorithm

In this study, fingerprint feature points are utilized, and information between stored feature points and newly input feature points is used [5]. The proposed algorithm performs a preprocessing step to compare registered fingerprint information, extracts the number of similar feature points, and compares similarity scores using the number of extracted feature points.

The algorithm is configured to determine whether fingerprints are similar through the final calculated similarity score. In the algorithm-processing step, as shown in Fig.4, the process of normalizing the center coordinates of feature points, calculating the direction of feature points, and verifying the direction of feature points is completed, followed by saving. After storing the feature points, the registered feature points and number of input feature points are extracted, respectively, and the final number of similar feature points is obtained through 1:1 matching.

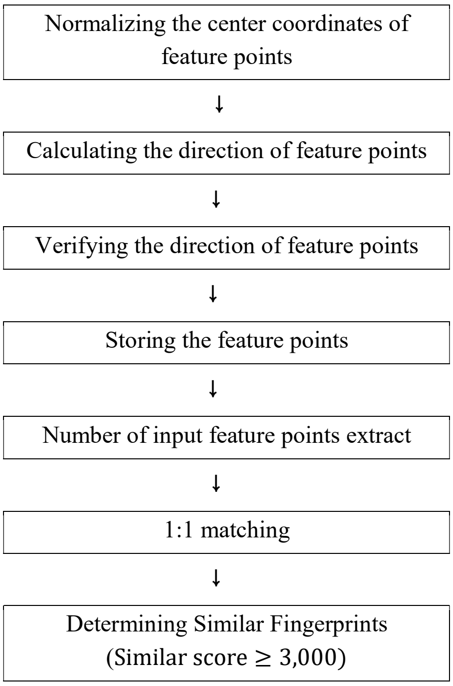

Normalizing the center coordinates of feature points
Calculating the direction of feature points
Verifying the direction of feature points
Storing the feature points
Number of input feature points extract
1:1 matching
Determining Similar Fingerprints
(Similar score ≥ 3,000)

Fig.4. Proposed algorithm processing step.

In order to check the similarity with the registered biometric information, the coordinate system is moved from the left end to the center of the image before saving the feature point, and the coordinates of all feature points according to the moved coordinate system are changed, as shown in Fig.5.

The direction of the feature point is created using the feature-point-direction search algorithm and the array according to the direction, processing the feature point differently depending on whether it is a branch point or end point, and selecting the processed feature point through the feature point direction and verification step.

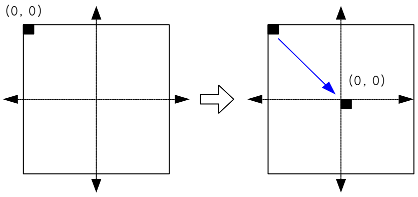


Fig.5. Coordinate normalization for similarity comparison.

In the screening method, if the direction of a feature point is significantly different from the direction of the block to which it belongs, it is removed, and the feature point already registered is compared with the distance to exclude those that are close to it from registration.

The structure is shown in Table I, and the array size is defined as up to 200. The order of saving is designed to be stored sequentially from the top left of the image to the bottom right.

Table I: Problem Description

Structure	Data Type	Value Stored
x	Int	x-coordinate of feature point
y	Int	y-coordinate of feature point
o	Byte	Direction of feature points
w	Byte	Bifurcation = 0, End = 1

Through these steps, the characteristics of the registered biometric information and the input biometric information are matched. The similarity score conversion method using the number of matched feature points is shown in Equation (1).

$$\text{score} = \frac{k}{(n+m)/2} \tag{1}$$

In Equation (1), m and n denote the number of feature points in the pre-registered fingerprint information (T) and newly input fingerprint information (I), respectively. The average number of feature points at T and I is $\frac{(m+n)}{2}$, which is calculated by normalizing the number of matching feature points (expressed as k). For similar-fingerprint detection, a pair of three elements is expressed as p for a feature point and is defined as $p = \{x, y, \theta\}$, where x, y is a feature-point location coordinate and θ is a feature-point angle.

$$\begin{gathered} T = \{p_1, p_2, \cdots, p_m\},\ p_i = \{x_i, y_i, \theta_i\}, i = 1 \cdots m \\ I = \{p^1, p^2, \cdots, p^n\},\ p^j = \{x_j, y_j, \theta_j\}, j = 1 \cdots n \end{gathered} \tag{2}$$

The feature point p^j in I of Equation (2) and the feature point p_i in T have a spatial distance smaller than the given tolerance r_0 in the same space. When the direction difference between the two feature points is smaller than the angular tolerance of θ_0, it is judged to be matching and designated as a similar fingerprint.

3. Simulation

To evaluate the performance of the proposed similar-fingerprint-information detection algorithm, images were obtained twice for the same fingerprint and twice for different fingerprints. The resolution and size of the acquired bitmap image are 500 dpi and 260 × 330 pixels, respectively. Fig.6(a) shows an image obtained by acquiring a fingerprint from the same finger, and Fig.6(b) displays an image obtained by acquiring a fingerprint from another finger.

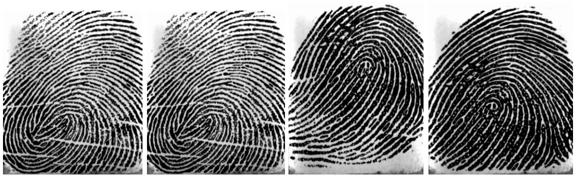
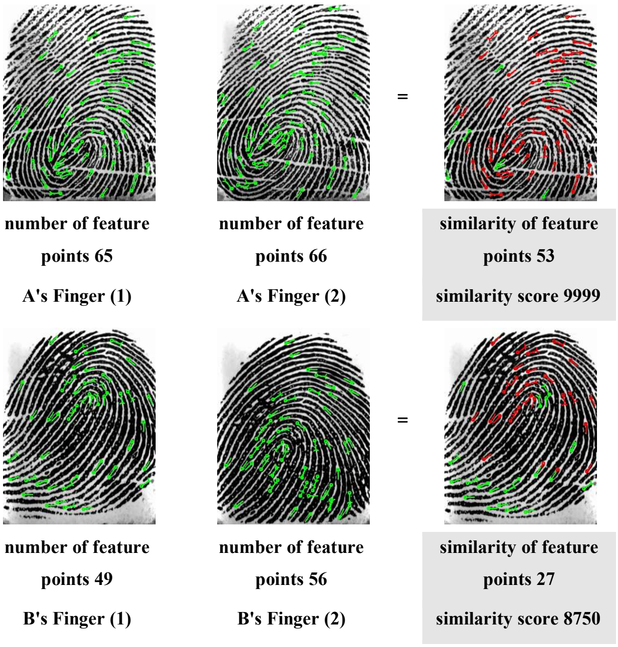

(a) Experimenter A's Finger (b) Experimenter B's Finger

Fig.6. Similar fingerprints image for experimentation

In Fig.7, each feature point extracted from the acquired fingerprint image is displayed in green, and the resulting image after applying the proposed similar-fingerprint-information detection system is shown in red. Furthermore, the number of feature points and similarity score were calculated to determine whether the fingerprints were similar.


=
=
number of feature points 65
A's Finger (1)
number of feature points 66
A's Finger (2)
similarity of feature points 53
similarity score 9999
number of feature points 49
B's Finger (1)
number of feature points 56
B's Finger (2)
similarity of feature points 27
similarity score 8750

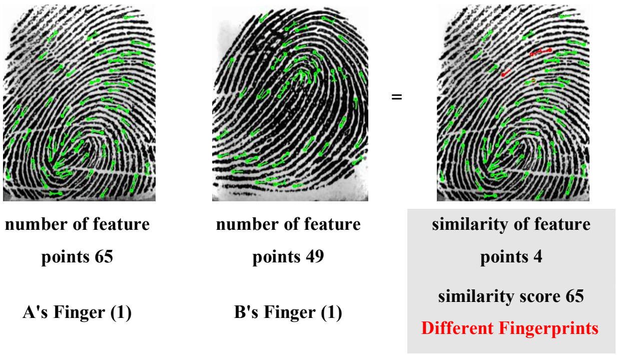

=
number of feature points 65
A's Finger (1)
number of feature points 49
B's Finger (1)
similarity of feature points 4
similarity score 65
Different Fingerprints

Fig.7. Similar fingerprint detection result image.

4. Conclusion

The algorithm proposed in this paper for enhancing the security of biometric access authentication systems used in nuclear power plants analyzes the fingerprint information of registered users and that of new registrants and determines their similarity. Using the proposed method, it is possible to effectively identify an abnormal visitor who has stolen another person's resident registration number or is illegally using an existing access card. As a result of the simulation, if the experimenter's fingerprint information is input, the proposed detection algorithm is processed after the step of extracting the number of similar feature points. By scoring the processed results, the similarity of the fingerprint information was accurately determined.

In the future, this algorithm for fingerprint recognition biometric access authentication can be applied more broadly as a security technology for nuclear facilities other than nuclear power plants.

Acknowledgments

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KoFONS) using the financial resource granted by the Nuclear Safety and Security Commission(NSSC) of the Republic of Korea. (No. 2101067)

REFERENCES

[1] Hyungy Lee, Yongki Kim "Biometric (Biometric Recognition) Techno-logy Trend Using Physical Characteristics", COMPA, 2021.
[2] Dohun Kim, "Recent Biometric Industry Trends and Implications", Issue Analysis Vol.188, https://now.k2base.re.kr, 2021.
[3] Young-Hyun Baek, "Security Enhancement of Biometric Fingerprints Using Human Heart rate Dependent Signal Wavelength Analysis," IEEK. 57, No. 6, pp.78-83, June 2020.
[4] Atomic Energy Newspaper, "Preferably national security facility "KHNP nuclear power plant hole drilled". https://www.knpnews.com, 2020.
[5] S.M Jung, "Preprocessing Algorithm for Enhancement of Fingerprint Identification," IEEK, Vol.44, No.3, pp.61-69, May 2007.No. 6, 78-83, June 2020.