International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 10, No.1 (Jan-2021)
http://dx.doi.org/10.12785/ijcds/100105

How to Use Bit-string Representation of the Face in a Multi-factor Authentication System

Jinho Han[1*]

[1] *Department of Liberal Studies (Computer), Korean Bible University, Seoul, Korea*

Received 5 Mar. 2020, Revised 29 May 2020, Accepted 31 Jul. 2020, Published 1 Jan. 2021

Abstract: Binary information extracted from biometrics is variable when it is generated from photographic images. If the same bit-string representation can be produced repeatedly, these bit-strings are useful for applications that require binary data (e.g., biometric cryptosystems). In this paper, multi-factor authentication using bit-string representation is proposed. For the protection of biometric information, random bits were used as the representation, and the length of the bit-string representation was decided according to the similarity level. The paper explains what "similarity enhancement" is and how to increase the similarity between images of the same person with weights added after verifying each factor in a multi-factor authentication system. Also, it discusses how to use this method in the real world and provide secret sharing using this multi-factor system. In an experiment with the Yale Face Database A and B+, it was shown that similarity enhancement could be achieved, and the same bit-string representation emerged after passing the multi-factor authentication system.

Keywords: Biometrics, Bit-String Representation, Cryptosystem, Face Recognition, Multi-Factor Authentication, Secret Sharing

INTRODUCTION

Applications using facial information are becoming increasingly important, and applications using facial recognition are being developed for personal portable devices such as mobile phones [1]. Several well-known algorithms have been used for facial recognition: principal component analysis, independent component analysis, and linear discriminant analysis [2–5]. Another recent method is three-dimensional (3-D) facial recognition [6]. Also, liveness detection schemes for facial recognition have been suggested so that fraudulent photographic images cannot be used [7].

It has been shown that fixed-length bit-strings can be used in biometric cryptosystems and that they allow fast matching due to bitwise operations. They are also useful for multi-biometric feature-level fusion [8] and biometric key generation schemes [9–10].

Fixed-length bit-string representation in biometrics was suggested for fingerprint authentication by Jin et al. [11]. They created a generic framework to extract fixed-length bit-strings from fingerprint minutiae. Also, Chen et al. [12] suggested a method to generate bits based on the likelihood ratio from fingerprint data and facial data. Vielhauer and Steinmetz [13] made bit-strings with handwriting features, and Han [14] suggested a bit-string representation of a face.

To increase security level using biometrics, two-factor authentication [15] or multi-factor authentication (MFA) has been used to verify the claimed identity of a person only after presenting two or more factors to an authentication system: the knowledge that only the user knows (e.g., password); the possession that only the user has (e.g., access card, security token); and inherence that only the user has (e.g., biometrics).

RELATED WORKS

MFA has been studied as a means of providing enhanced security in many fields, such as mobile authentication [16], IoT applications [17], and fuzzy systems for adaptive multi-factor combination authentication [18]. Ometov et al. [19] proposed secret sharing MFA based on reversed Lagrange polynomial; this is a flexible system in which the user can be authenticated even though some of the factors may be mismatched. However, these systems do not have bit-string representation.

In the present study, an MFA using bit-string representation is proposed. The contributions of this paper are as follows:

(1) An MFA system generating bit-string representation after verification of the user is proposed. For the protection of biometric

E-mail: hjinob@bible.ac.kr

information, random bits are used as the representation, and the length of the bit-string representation is decided according to the similarity level.

(2) Han's method [15] is revised to generate a bit-string more efficiently. He used a group standard face template and user's face template, but here only the user's template was used. Also, he selected 2,485 facial features and extracted 500 bits from them, but in this method, 1,300 bits were derived from 1,431 features selected as more characteristic facial features according to the experimental results. Therefore, the method became simpler but obtained more bit-strings than previously.

(3) Secret sharing MFA based on weights is proposed. In (k, N)-threshold secret sharing MFA system, 'N' is the number of all factors, and 'k' is the threshold number of verified factors that increase weights. Because the similarity level enhanced by weights decides the bit-string length, 'k' confirmed factors provide a sufficient bit-string length, which can be a secret key.

PROPOSED METHOD

In the proposed method three-factor authentication is used as an example of MFA.

3.1 Generating Bit-string Representation

To create a standard face template for one user, 54 interesting facial points were used, and Han's method was revised to increase the efficiency of generating a bit-string. Instead of comparing a group standard face template to the user's face template, as in Han's method, in this method, only the user's template is needed. All distances from point to point are estimated. The total number of distances is 1,431, using 54 points of the eyebrow, nose, eye, and mouth. Fig. 1 shows the points of a face.

Several facial images of a user are selected, and a set of 1,431 distances is made as the comparative standard features based on the images. The set is his/her "standard face template." The distance between RightEyeCenter-to-LeftEyeCenter of the facial image is transformed to 50, which is used as the conversion reference value for other distances. If the distance between the same position between a person's face and the standard face of the user is identical, it is bit '1'; otherwise, it is bit '0'. So, 1,431 bits '1' or '0' are set after the comparison. Among the 1,431 bits, the number of bits '1' is the similarity level. When two distances are compared, the error correction value is used: one through nine. In the experiment, it was shown that when the error correction value increased, the similarity increased accordingly.

Initializing random bits for a user: To protect biometric information from theft, 1,431 random bits are deployed to a user. In the MFA system, these random bits are hidden, and after the verification phase, they are opened as much as the number of verifying features. As an example, if 1,300 features of a target individual's face are verified as similar to the user's template, 1,300 bit '1s' are set during the verification phase of MFA, and the same number of random bits is opened. The opened random bits can be used for Face-ID or as a cryptographic key for the user.

Figure 1 Points of a face

3.2 Similarity Enhancement

Error correction value (ECV): 'A' is a distance of the user's face template, and 'B' is a distance of points of the facial image of a person who wants to be authorized. When the error correction value is 2, comparing 'A' to 'B' is as follows:

$$\text{If } A - 2 \leq B \leq A + 2, \text{ then } A = B.$$

In the experiment, it was found that similarity increased as ECV became greater. Table 1 shows the average number of bit '1s' (similarity %) according to ECV. When ECV is 4, the similarity between the same person's images is 74.84% and the similarity between different people's images is 38.64%. When ECV becomes 5, the similarity of the same person's images is 85.12%, which is an increase of about 10%.

"Similarity enhancement" is a method to increase ECV with a condition of the user whose identity is proven by another authentication factor, such as a password in the MFA system.

3.3 Three-factor Authentication

MFA system can be used with biometrics (e.g., face, fingerprint, voice, iris), and passwords. If this system is a three-factor authentication and the face factor is used last, the similarity for verification can be calculated as follows:

$$Sim_{Total} = Sim_{F1} + Sim_{F2} + SimEnhance_{F3} \quad (1)$$

$$SimEnhance_{F3} = Sim_{F3}(W_{F1} + W_{F2}) \quad (2)$$

Sim_{F1} is the similarity % of factor 1, Sim_{F2} is the similarity % of factor 2, and Sim_{F3} is the similarity % of

factor 3. W_{F1} is the weight of factor 1, and W_{F2} is the weight of factor 2. W_{F1} and W_{F2} are added to increase ECV. Therefore, $SimEnhance_{F3}$ is 'enhanced similarity' % of factor 3.

TABLE 1 Average number of bits that were '1' according to ECV

(ECV)	Number of bits' 1' between the same person's images (similarity %)	Number of bits' 1' between different people's images (similarity %)
1	137 (9.57)	54 (3.77)
2	514 (35.92)	224 (15.65)
3	840 (58.70)	394 (27.53)
4	1071 (74.84)	553 (38.64)
5	1218 (85.12)	680 (47.52)
6	1308 (91.40)	789 (55.14)
7	1365 (95.39)	890 (62.19)
8	1397 (97.62)	979 (68.41)
9	1413 (98.74)	1086 (75.89)

Fig. 2 shows the overall process of the proposed three-factor authentication system. In the first step, fingerprint similarity verification is undertaken. If the similarity of the first step is over the threshold, the weight of factor 1 is produced. If in the second step, the claimed person enters passwords correctly, the weight of factor 2 is also created. Finally, if the user is verified with a standard face template stored in the database, the user succeeds in passing the authentication system.

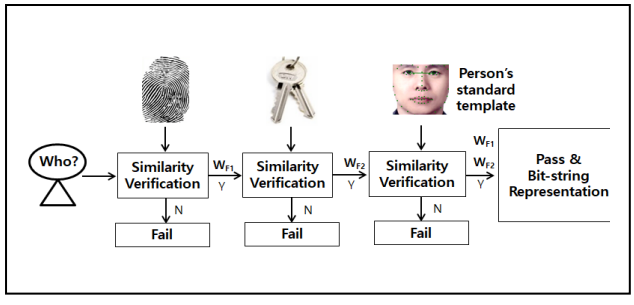

Figure 2. Three-factor authentication system

After passing the system, the user has bit-string representation, with the length decided by ECV. If the initial ECV is 4 and a user passed two factors, weight is two and the final ECV is 6: 4+2=6. Then, the user has 1,309 bits as face representation and similarity is 91.40%. See also Table 1.

(k, N)-threshold secret sharing MFA system: This system can be used as a (k, N)-threshold secret sharing system. When k is 3 and N is 5, (3, 5)-threshold means that among five factors, three factors should be used to reconstruct a secret. When one factor is verified, one weight is produced so that ECV has one increment. Two kinds of secret sharing MFA system are proposed as follows:

(1) The system is used for one user. Five factors belong to the user. The secret is decrypted with verification of any three factors, which should include the user's face recognition as the last factor.

(2) The system is used for one group. Five factors belong to five users each. In this case, five users' biometric factors should all be face recognition, or at least one user's factor is face recognition, which should be the last factor of the system.

EXPERIMENTS AND DISCUSSION

For the experiment, Neurotechnology Biometric SDK VeriLook 10.0 (www.neurotechnology.com) and Yale Face Database A and B+ (http://vision.ucsd.edu/) were used. From the face database, around 3,000 images were tested to simulate this system. Fifty-four points were selected from all the images, and 1,431 distances were measured from point-to-point. Then, 1,431 measurement values were listed for one face image. The 54 points are for eyebrows, nose, eyes, and mouth.

The standard face template was created with average distances of several images of one person. Each point-to-point distance of the claimed person's image was compared to the same point-to-point distance of the standard face template. If comparative values were identical within ECV, they were bit '1s'; otherwise, they were bit '0s'. So, each image had 1,431 bit-strings after comparison.

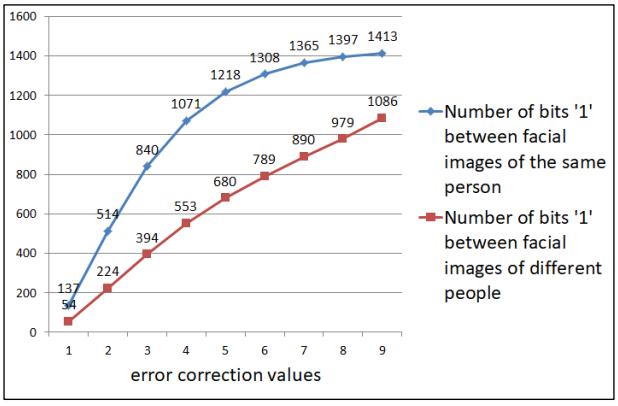

Figure 3. The average number of bits '1' according to ECV

Fig. 3 shows the average number of bits that were bit '1' according to ECV. It can be seen that there was a meaningful difference between two groups: one group comprised facial images of the same person, and the other group comprised facial images of different people.

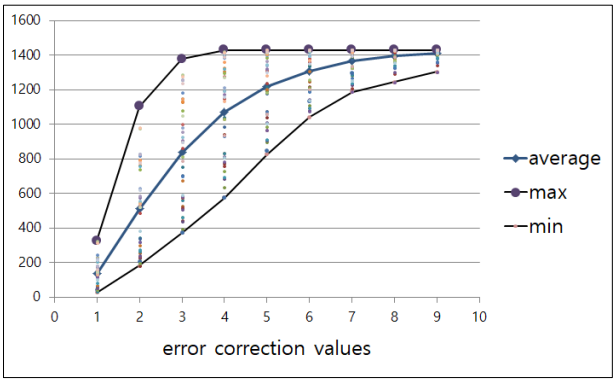

Figure 4. Distribution of the number of bits '1' between facial images of the same person

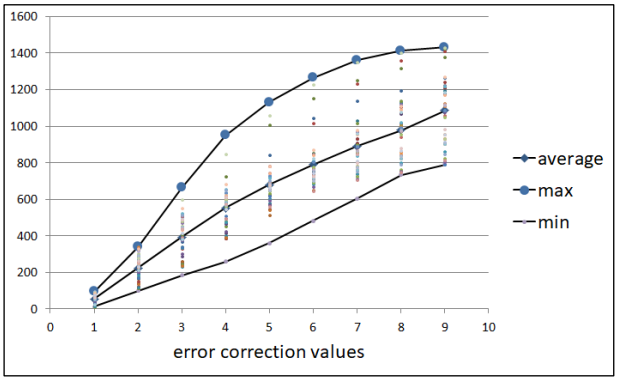

Figure 5. Distribution of the number of bits '1' between facial images of different people

For example, at ECV 4, the same person's images had 1,071 number of bit '1s', and different people's images had 553 bit '1s'. Even at ECV 7, the same group had 1,365 bit '1s', and the different group had 890 bit '1s', which was less than the same group's 1,071 bits at ECV 4. Therefore, this result showed that the proposed method distinguished a user's face from other faces, and a 1,300 bit-string Face-ID could be extracted. Also, ECV suggested the weight to be used to define the "similarity enhancement."

Fig. 4 shows the distribution of bit '1s' for facial images of the same person, according to ECV. At ECV 4, the maximum number of bit '1s' was 1,431, the minimum number of bit '1s' was 576, and the average was 1,071. Fig. 5 shows the distribution of bit '1s' for facial images of different people. In that figure, at ECV 4, the maximum number of bit '1s' was 951, the minimum number of bit '1s' was 258, and the average was 553. To determine the distribution of the two groups, standard deviations (σ) were calculated at each ECV, as shown in Table 2. The average σ was 156.07 in the group of the same person's images and 126.12 in the group of different people's images.

Figure 6. Distribution of bit-string length when $\boldsymbol{\sigma = 156}$ in the same person's images and $\boldsymbol{\sigma = 126}$ in different people's images

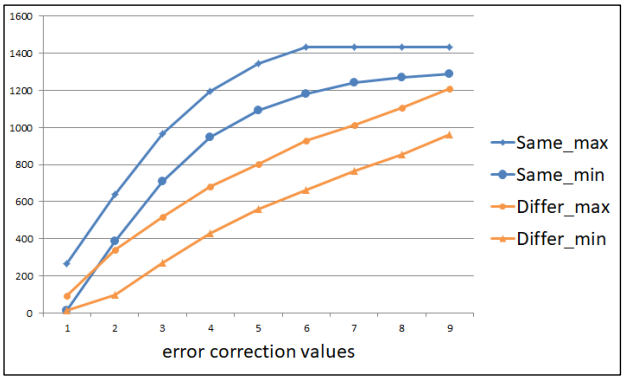

Figure 7. Distribution of bit-string length when $\boldsymbol{\sigma = 70}$ in two groups

How to use this method in the real world: Fig. 6 shows that the method has a problem because the distribution of the two groups is wide. The maximum bit-string length of the different groups is greater than the minimum bit-string length of the same group; the gray regions in the figure. To solve this problem, good quality facial images with eyes, nose, and mouth scanned more accurately should be collected. When σ of bit-string length in the two groups is less than 70, this problem is solved in the simulation. Fig. 7 shows the distribution of two groups and no overlaid gray region when σ is 70.

CONCLUSIONS

In this paper, an MFA system generating bit-string representation following the user's verification is proposed. In the experiment, 1,431 facial features were used for verification, and finally, a bit-string length of more than 1,300 emerged. Also, it was shown that this system could be used for a (k, N)-threshold secret sharing MFA system based on weights. Because the similarity level is enhanced by weights, 'k'-verified factors offer a sufficient bit-string length for the extraction of a secret key. It was explained that random bits could be used as the representation so that biometric information is protected from theft.

Because the distribution of the experimental result was wide, this MFA system should use more accurate facial images in the real world. Collecting accurate images is one of the topics of future studies for developing this MFA system.

TABLE 2. Standard deviations (σ) of bit-string length in two groups according to ECV

ECV	σ of bit-string length in the group of the same person's images	σ of bit-string length in the group of different people's images
average	156.07	126.12
1	83.02	25.21
2	259.24	72.29
3	304.43	108.74
4	266.84	123.38
5	196.34	133.41
6	129.96	147.67
7	79.89	165.22
8	51.55	174.44
9	33.35	184.69

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea (NRF) grant in 2019 (NRF-2019R1G1A1004773).

REFERENCES

[1] C. Bhagavatula, B. Ur, K. Iacovino, S.M. Kywe, L.F. Cranor, M. Savvides, Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption. In Proceedings of the Usable Security (USEC), USEC '15, 8 February 2015, San Diego, CA, USA

[2] M.Turk and A.Pentland, Eigenfaces for Recognition. Journal of Cognitive Neuroscience, 1991, Vol. 3, No. 1, pp. 71-86.

[3] M.S.Bartlett, J.R. Movellan, T.J. Sejnowski, Face Recognition by Independent Component Analysis. IEEE Trans. on Neural Networks, Vol. 13, No. 6, 2002, pp. 1450-1464.

[4] P.Belhumeur, J.Hespanha, D.Kriegman, Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. Proc. of the Fourth European Conference on Computer Vision, Vol. 1, Cambridge, UK, 1996, pp. 45-58.

[5] L.Juwei, K.N.Plataniotis, A.N.Venetsanopoulos, Face recognition using LDA-based algorithms. IEEE Transactions on Neural Networks, v.14 n.1, 2003, pp.195-200.

[6] K.W.Bowyer, K.Chang , P. Flynn, A survey of 3D and multi-modal 3D+2D face recognition. Dept. of Computer Science and Electrical Engineering Technical report, University of Notre Dame. 2004

[7] H.K.Jee, S.U. Jung, J.H. Yoo, Liveness Detection for Embedded Face Recognition System. International Journal of Biomedical Sciences, 1, No. 4, 2006, pp. 235-238.

[8] A.Gyaourova and A. Ross, Index codes for multibiometric pattern retrieval. IEEE Trans. Inf. Forensics Secur., vol. 7, no. 2, 2012, pp. 518–529.

[9] W.Sheng , S. Chen, G. Xiao, J. Mao, Y. Zheng, A biometric key generation method based on semisupervised data clustering. IEEE Trans. Syst., Man, Cybern., Syst., vol. 45, no. 9, 2015 pp. 1205–1217.

[10] E.J.C.Kelkboom et al., Binary biometrics: An analytic framework to estimate the performance curves under Gaussian assumption. IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 40, no. 3, 2010, pp. 555–571.

[11] Z.Jin, M.H.Lim, A.B. Teoh, B.M. Goi, Y.H. Tay, Generating Fixed-Length Representation From Minutiae Using Kernel Methods for Fingerprint Authentication. IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 46, Issue 10. 2016

[12] C.Chen, R.N.J.Veldhuis, T.A.M.Kevenaar, A.H.M. Akkermans, Multi-Bits Biometric String Generation based on the Likelihood Ratio. First IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007.

[13] C.Vielhauer, R. Steinmetz, Handwriting: feature correlation analysis for biometric hashes. EURASIP Journal on Applied Signal Processing, vol. 2004, no. 4, pp. 542–558, special issue on Biometric Signal Processing.

[14] J. Han, Cancellable Face Recognition System Based on Bit-string Representation. Journal of Engineering and Applied Sciences, vol.13, Issue 10 SI, 2018, pp. 8314-8316.

[15] T.Andrew, N. David, G.Alwyn, Biohashing: Two Factor Authentication Featuring Fingerprint Data And Tokenised Random Number. Pattern Recognition, Vol. 37, Issue 11, 2004, pp. 2245-2255.

[16] T.V. Goethem, W. Scheepers, D. Preuveneers, W. Joosen, Accelerometer-based device fingerprinting for multi-factor mobile authentication. In Proceedings of the International Symposium on Engineering Secure Software and Systems, London, UK, 6–8 April 2016, Springer: Berlin, Germany, 2016, pp. 106–121.

[17] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, M. Gerla, Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications. IEEE Network, vol.33, no.2, pp.82-88, 2019

[18] Z. Shao, Z. Li, P. Wu, L. Chen, X. Zhang, Multi-factor combination authentication using fuzzy graph domination model, Journal of Intelligent and Fuzzy Systems. 2019, doi: 10.3233/JIFS-181859.

[19] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, Y. Koucheryavy, Multi-Factor Authentication: A Survey. Cryptography, vol. 2, no. 1, p. 1, 2018.

Jinho Han received the B.A. degree in the Department of Forestry from Korea University and M.E. degree in the Department of Network Management at Dongguk University, Seoul, Korea, in 1990 and 2006, respectively. He received the Ph.D. degree at the Graduate School of Information Security from Korea University in 2013. He is currently an associate professor in the department of Liberal studies (computer) at Korean Bible University, Seoul, Korea. His research areas include cryptography, authentication, biometrics, and artificial intelligence.