ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20191104190328

Original scientific paper

EVALUATING BIOMETRICS FINGERPRINT TEMPLATE PROTECTION FOR AN EMERGENCY SITUATION

Ei Ei MON, Sangsuree VASUPONGAYYA, Montri KARNJANADECHA, Touchai ANGCHUAN

Abstract: Biometric template protection approaches have been developed to secure the biometric templates against image reconstruction on the stored templates. Two cancellable fingerprint template protection approaches namely minutiae-based bit-string cancellable fingerprint template and modified minutiae-based bit-string cancellable fingerprint template, are selected to be evaluated. Both approaches include the geometric information of the fingerprint into the extracted minutiae. Six modified fingerprint data sets are derived from the original fingerprint images in FVC2002DB1_B and FVC2002DB2_B by conducting the rotation and changing the quality of original fingerprint images according to the environment conditions during an emergency situation such as wet or dry fingers and disoriented angle of fingerprint images. The experimental results show that the modified minutiae-based bit-string cancellable fingerprint template performs well on all conditions during an emergency situation by achieving the matching accuracy between 83% and 100% on FVC2002DB1_B data set and between 99% and 100% on FVC2002DB2_B data set.

Keywords: biometric-based user authentication; biometric cryptosystem; cancellable biometrics

1 INTRODUCTION

Biometric-based authentication system uses unique and measurable biological characteristics of an individual to verify a person [1]. Biometric-based authentication is more convenient than other user authentication techniques based on passwords or smartcards. Passwords can be forgotten and smartcards must be carried. Biometric-based authentication systems are used in many applications such as law enforcements, healthcare, banking, access controls and smart phones. Fingerprint is a cheap and convenient way to identify someone because fingerprint scanners are small and cheap in comparison with other biometric capturing devices [1, 2]. However, a biometric-based authentication system has a serious drawback on privacy. Under a traditional fingerprint-based authentication system, an unknown original fingerprint image can be reconstructed from a stored fingerprint template [3, 4]. Therefore, biometric template protection (BTP) methods have been used for the security of fingerprint templates. Fig. 1 shows the fingerprint-based authentication system with the template protection.

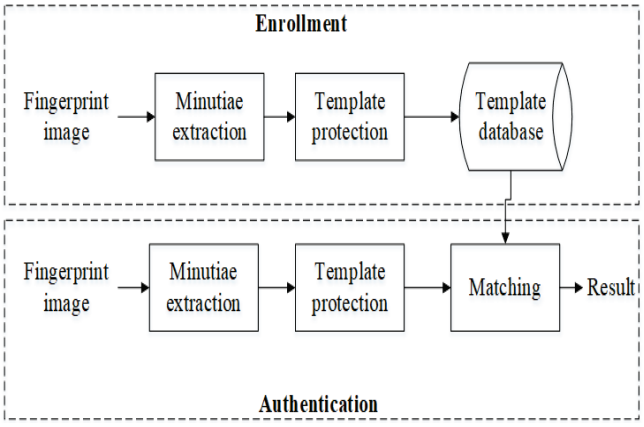


Figure 1 Fingerprint-based authentication system with a template protection

The biometric template protection schemes are commonly categorized as feature transformation (or Cancellable Biometrics (CB)) and biometric cryptosystems (BCS) as shown in Fig. 2. In this work, two CB techniques are evaluated under an emergency situation for personal health record systems. One of the challenges in fingerprint template protections is the performance degradation after performing a template protection. This issue is amplified when the user is unconscious because the quality of the fingerprint image might be affected by many environment conditions and human errors. During an emergency, the emergency service person is the main person to collect the fingerprint images from the victim. Thus, the fingerprint image quality might be affected by environment such as wet or dry fingers and the orientation of the finger during the fingerprint collection process.

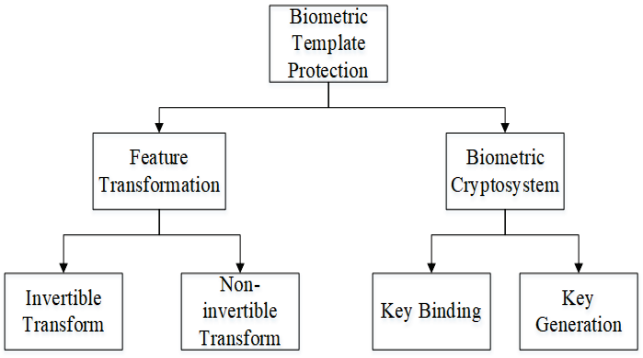


Figure 2 Biometric template protection techniques [3]

In this work, two CB techniques are evaluated with various fingerprint quality generated according to the environment conditions during an emergency situation such as wet or dry fingers and disoriented angle of fingerprint images. The result of this work will be further used for proposing an improved fingerprint feature transformation

approach for personal health record users during an emergency situation.

The remaining sections of this paper are organized as follows. Section 2 provides information on biometric template protection. The experimental settings are described in Section 3. Results and discussions are given in Section 4 while the conclusion is shown in Section 5.

2 BIOMETRIC TEMPLATE PROTECTION

The fingerprint-based authentication system consists of two main processes, including enrolment and authentication [2]. For the enrolment process, a fingerprint image is captured and features are extracted from the fingerprint image. The biometric template protection algorithm is performed on the fingerprint templates and stored in the system database as the protected templates. Depending on whether the biometric system is applied for the identification or the verification process, the authentication is performed differently. The verification system confirms the person's identity by performing a one-to-one comparison between the queried fingerprint and the stored fingerprint template. The identification system performs a one-to-many comparison by searching the entire system database.

According to the international standard ISO/IEC 24745: biometric information protection, the biometric template protection schemes must meet these properties: irreversibility, unlinkability, revocability and performance [5]. The irreversibility means the reconstruction from the protected biometric template to the original image or the biometric sample, should be difficult. The unlinkability refers to the link between the protected biometric template from one application to another application should not be possible. The revocability means that the new template can be revoked and re-issued like a password in an event of the compromising template information. The performance property means that the template protection method should not degrade the recognition performance across a number of applications.

The feature transformation consists of the distortion or the transformation of the biometric features based on the transformation function [3]. According to the characteristics of the transformation function, this category can be further divided into the invertible transform (salting) and the noninvertible transform. Salting is one of the template protections approaches. The user specific extra information is added to the original biometric features using an invertible function with a key or a password. The user needs to remember the key and presents it during the authentication. Therefore, the security of the salting is relied on the protection of the key. The template will be compromised when the key is stolen. The main advantage of the salting is the incorporation of the additional information into the biometric template in the form of keys. It makes difficult for an imposter to guess the template. The main drawback of the salting approach is that the security of this scheme relies upon the secrecy of the key. In the noninvertible transform, a one-way function is applied on the biometric features. Unlike the salting approach, the noninvertible function does not rely on the secrecy of the keys. The difficulty of reversing the transformation function is the major protection of the biometric data. The protected template can be revoked and issued a new one by changing the transformation parameter in the case of compromising.

Table 1 Existing cancellable fingerprint template generation methods

No	Reference	Template Protection Approach	Pre-processing			Feature				Matching			
			Segmentation	Enhancement	Binarization	Minutiae	Singular point	Texture	Other	Correlation	Vector	Bit-String	Other
1	[5]	CB	(P-MCC)			✓			✓				✓
2	[6]	CB	(bit-string)			✓			✓		✓		
3	[8]	CB	(MCC)			✓					✓		
4	[10]	CB	(P-MCC)			✓					✓		
5	[13]	CB				✓						✓	
6	[14]	CB				✓						✓	
7	[15]	CB	✓	✓	✓	✓	✓						✓
8	[16]	CB	✓	✓	✓	✓						✓	
9	[17]	CB	✓	✓	✓	✓							✓
10	[20]	CB		✓	✓	✓					✓		
11	[11]	CB				✓						✓	
12	[18]	CB		✓	✓			✓		✓			
13	[23]	CB		✓	✓	✓					✓		
14	[7]	CB	VeriFinger			✓					✓		
15	[12]	CB	VeriFinger			✓							✓
16	[19]	CB	VeriFinger 6.0			✓	✓						✓
17	[21]	CB	VeriFinger			✓					✓		
18	[22]	CB	VeriFinger 6.0			✓					✓		

Template protection of this work is a cancellable fingerprint template generation approach. The literature review of cancellable fingerprint template generation approaches is described in Tab. 1. Researchers used different types of fingerprint features. Some approaches extracted not only minutiae but also singular point and other features [5, 6, 15, 19]. The resulted template representation was also different. Some methods performed the correlation-based matching [18]. The protected fingerprint templates were generated as a complex vector [6-8, 10, 12, 21-23] or a binary bit-string [11, 13, 14, 16]. In the design of cancellable fingerprint templates, some researchers focused on the template generation from the minutia information [9, 13, 16, 17, 20] while some researchers spent more effort on the design of non-invertible transformations [6-8, 10-11]. The protected templates in related works were generated in a binary form because of its simplicity in the feature representation. The design of non-invertible transformation functions in the related methods used a permutation process.

3 EXPERIMENTAL SETTINGS

Two cancellable fingerprint templates (CB) namely minutiae-based bit-strings CB and modified minutiae-based bit-strings CB are evaluated in this work. Fingerprint Verification Competitions (FVC) databases were used for evaluating both CB approaches. However, the fingerprints are modified to mimic the conditions of emergency situations described previously.

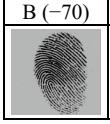
3.1 FVC Databases

The commonly used fingerprint evaluating databases are Fingerprint Verification Competitions (FVC) databases such as FVC2000, FVC2002, FVC2004 and FVC2006 [24-27]. Each FVC database is composed of four sub-databases DB1, DB2, DB3 and DB4. DB1, DB2 and DB3 were collected using optical, capacitive and thermal sensors, respectively. DB4 was created using Synthetic Fingerprint Generator (SFinGe). Each sub-database includes two subsets A and B. For three data sets (DB1, DB2 and DB3), subset A contains 100 fingers with 8 impressions (800 images) and subset B contains 10 fingers with 8 impressions (80 images). Fingers from set B have been available to allow a parameter tuning process and the benchmark is then tested by the fingers from set A. In FVC2000, the acquisition conditions were different for each database [24]. In FVC2002, the acquisition conditions were the same for each database [25]. Interleaved acquisition of different fingers causes differences in the finger placement. FVC2004 and FVC2006 databases were collected with the aim of creating a more difficult benchmark [26, 27].

3.2 Modified FVC Databases

During the emergency situation, the victim fingerprint cannot be placed in the same direction with the enrolled (registered) image. The collected fingerprint images can have variations such as wet finger, dry finger and the image acquisition style. Therefore, the input fingerprint images are modified in our work as proposed in [28] to create these three conditions. The fingerprint image brightness is changed to reduce the brightness by 70% (denoted B (-70) and to increase the brightness by 35% (denoted B (+35)). The fingerprint image is rotated clockwise by 5 degrees (denoted CW5)) and the fingerprint image is rotated clockwise by 10 degrees (denoted CW10). The fingerprint image is rotated counter clockwise by 5 degrees (denoted CCW5) and the fingerprint image is rotated counter clockwise by 10 degrees (denoted CCW10). Tab. 2 shows the samples modified fingerprint image used in this work.

Table 2 Samples of fingerprint images in modified sub-data sets

B (−70)	B (+35)	CW5	CW10	CCW5	CCW10
					

3.3 Minutiae-based Bit-strings CB

Minutiae-based bit-strings CB is proposed in [13] which the generation of the fingerprint template was performed by mapping the minutiae in the 3D array in order to remove the pre-alignment of the fingerprint requirement. The transformed fingerprint template is generated by mapping the minutiae in the 3D array and stored as bit-strings.

After scanning the finger and receiving the fingerprint image, the minutiae were extracted from the image and used as inputs in the template protection method. A 3D array which consisted of cells was created and mapped the minutiae into the cells based on the position and the orientation of the reference minutiae. One of the minutiae was chosen as the reference minutia. The position of the reference minutia was at the centre of the 3D array. 1D bit-string was generated by sequentially visiting the cells in the 3D array by setting the cells in the 3D array. If there is more than one minutia in the cell, set '1' and otherwise '0'. Random permutation was applied on the bit-string using the user specific PIN.

Matching queried template with the enrolled template is performed by computing the similarity between them. Both local similarity and global similarity are computed. Local similarity is performed by comparing the values of the bit-strings of the query template with that of the enrolled template. Practically, two 1-D bit-strings generated from the same reference minutiae are the same. However, it cannot know which 1-D bit-strings are generated from the same reference point. Therefore, each bit-string of the query template is compared with that of the enrolled template. The similarity score between the enrolled bit-strings and the query bit-strings is computed by finding the number of common one between them with a bit-wise AND operator. In global similarity, the maximum of local similarity values is compared with the (decision) threshold. If the maximum local value is greater than or equal to the threshold, this local similarity value is picked for global similarity. Otherwise the value of the global similarity is set as '0'. The final similarity value is obtained. The sum of global similarity values is divided by the number of non-zero values of the global similarity. Finally, whether to accept or reject is decided by comparing the final similarity with the (decision) threshold.

3.4 Modified Minutiae-based Bit-strings CB

The process of the modified minutiae-based bit-strings CB fingerprint template generation is shown in Fig. 3. The idea is first introduced in [16]. The main idea is to use the similar process to generate the bit-string of the minutiae except the calculation of the reference point which is influent by [29]. Under the modified minutiae-based bit-strings CB, the minutiae are firstly extracted from the input fingerprint image. The template generation is performed by measuring the average distance of all the minutiae from the reference minutia and calculating the geometric information of the minutiae. One of the minutiae is selected as the reference minutia. For each of the reference minutia, the Euclidean distance is calculated with the other minutiae. Among these distances, the distance of the farthest minutia is selected. A line segment is drawn in the direction of the orientation of the reference minutia. The length of the line is the average distance. The horizontal direction is set as the reference direction. The slope of the line and its perpendicular is calculated. The transformed fingerprint templates are generated by checking the minutiae under the line or above the line. The generated template is permuted with the user pin which is the transformation key and used as the seed value to generate the cancellable fingerprint templates. The matching

process is done exactly as same as the minutiae-based bit-strings CB method.

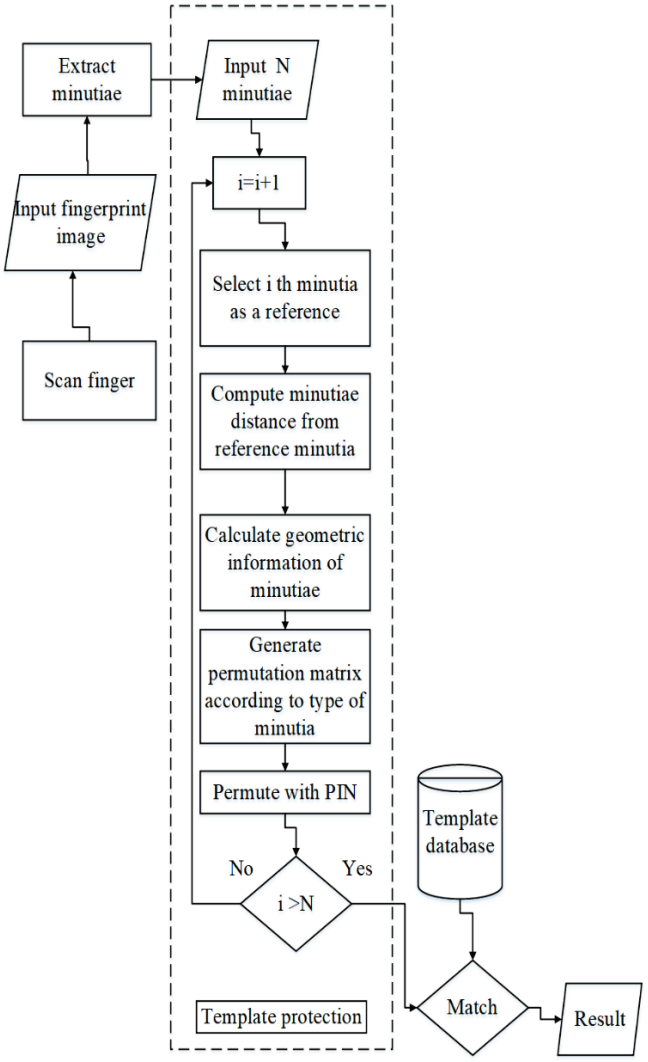


Figure 3 Modified minutiae-based bit-strings CB

3.5 Experimental Settings

The experiments are performed on Window 10, Intel (R) Core (TM) i7-8700U, 3.20 GHz processor and 8.00 GB RAM machine and implemented by using Matlab 2016a. The minutiae of every fingerprint are extracted and formatted according to the ISO standard by using the VeriFinger SDK 10.0 (trail version) of Neurotechnology [30]. The performance of the proposed method is evaluated by using the public fingerprint data set FVC2002DB1_B and FVC2002DB2_B [25] and their six modified data sets as described in the modified FVC database section. Tab. 3 shows the information of each data set used in this work.

For each fingerprint data set, three experiments are conducted. The first experiment aims to measure the accuracy of the same finger by matching the fingerprint impression and its modified images. The second experiment aims to measure the accuracy of the fingerprint impression against itself, its different fingerprint impressions and the modified image of each fingerprint impressions. Thus, there are 640 comparisons for each data set. The third experiment aims to measure the accuracy of the fingerprint impression against only its different fingerprint impressions. Thus, there are 560 comparisons for each data set.

Table 3 Information of Each Data Set

FVC2002	Sensor Type	Image Size	Resolution
DB1_B	Optical Sensor	388×374	500 dpi
DB2_B	Optical Sensor	296×560	569 dpi

4 EXPERIMENTAL RESULTS AND DISCUSSIONS

Tab. 4 presents the accuracy performance of both methods on matching the same fingerprint image with its modified fingerprint image. Minutiae-based bit-strings CB is denoted CB1 while the modified minutiae-based bit-strings CB is denoted CB2. According to the results, the modified minutiae-based bit-strings CB (CB2) performs well on the FVC2002DB2_B data set. For the FVC2002DB1_B, minutiae-based bit-strings CB (CB1) performs poorly on the rotated images of 10 degrees both clockwise and anticlockwise direction.

Table 4 Accuracy of each method when comparing the same fingerprint image with its modified images

Image	FVC2002DB1_B		FVC2002DB2_B	
	CB1	CB2	CB1	CB2
B (-70)	100%	98.75%	100%	100%
B (+35)	98.75%	98.75%	100%	100%
CW5	100%	100%	87.50%	100%
CW10	86.25%	96.25%	71.25%	100%
CCW5	93.75%	98.75%	86.25%	100%
CCW10	87.50%	96.25%	73.75%	100%

Tab. 5 presents the accuracy performance of both methods on matching the fingerprint impression against itself, its different fingerprint impressions and the modified image of each fingerprint impressions. According to the results presented in Tab. 5, the modified minutiae-based bit-strings CB (CB2) outperforms the minutiae-based bit-strings CB (CB1) in all cases for both data sets. The modified minutiae-based bit-strings CB (CB2) also provides a higher accuracy on FVC2002DB2_B than that of FVC2002DB1_B. Interesting finding is that the modified minutiae-based bit-strings CB (CB2) seems to have an issue with a fingerprint impression of a dry finger B (+35) for both data sets.

Table 5 Accuracy of each method when comparing the fingerprint image with modified images of all impressions

Image	FVC2002DB1_B		FVC2002DB2_B	
	CB1	CB2	CB1	CB2
Origin	41.41%	96.56%	35%	100%
B (−70)	38.13%	96.41%	35.94%	100%
B (+35)	37.97%	95.63%	34.69%	99.84%
CW5	41.41%	96.56%	25.63%	100%
CW10	35.16%	96.41%	22.81%	100%
CCW5	35%	96.41%	25.31%	100%
CCW10	33.44%	95.31%	22.81%	100%

Tab. 6 presents the accuracy performance of both methods on matching the fingerprint image with different impressions of the same finger and the modified different

impressions of the same finger. As expected, the modified minutiae-based bit-strings CB (CB2) outperforms the minutiae-based bit-strings CB (CB1) in all cases for both data sets. The modified minutiae-based bit-strings CB (CB2) also provides a higher accuracy on FVC2002DB2_B than that of FVC2002DB1_B.

Table 6 Accuracy of each method when comparing the same fingerprint image with different impression of the same finger and its modified images

Image	FVC2002DB1_B		FVC2002DB2_B	
	CB1	CB2	CB1	CB2
Origin	28.91%	84.06%	25.71%	100%
B (−70)	25.63%	84.06%	26.79%	100%
B (+35)	28.91%	84.06%	25.36%	99.82%
CW5	24.38%	84.06%	16.79%	100%
CW10	24.38%	83.91%	15.89%	100%
CCW5	23.28%	84.06%	16.61%	100%
CCW10	22.50%	83.28%	15.54%	100%

From all experimental results, minutiae-based bit-strings CB (CB1) performs poorly on both data sets in comparison with that of the modified minutiae-based bit-strings CB (CB2). The fingerprint template generation in CB1 was dependent not only on the size of the image but also on the number of minutiae. The minutiae information in the modified images are different from that of the original images.

The modified minutiae-based bit-strings CB (CB2) is more robust when the image quality and the rotation is changed. This causes by the information collected by the CB2 in the minutiae because CB2 collects the distance and the geometric information of the minutia. Even the direction of the minutiae is changed, the Euclidean distance between the two minutiae remains the same. Moreover, the fingerprint images in FVC2002DB2_B are high resolution images. Therefore, the modified minutiae-based bit-strings CB (CB2) obtains a better matching accuracy on FVC2002DB2_B than that of FVC2002DB1_B.

Another interesting finding is that the minutiae-based bit-strings CB (CB1) results in a better performance on the modified images when the fingerprint image brightness is decreasing (i.e., B (−70)). This event is caused by the fact that most of the non-matched images of the origin images are collected in lighted or partial images. Fig. 4 shows the sample modified images in FVC2002DB2_B.

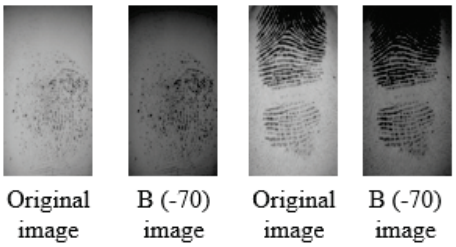


Figure 4 Sample B (−70) modified images in FVC2002DB2_B

According to the sample modified images, when the fingerprint image brightness is decreasing some minutiae points appear. Thus, more minutiae points can be extracted than that of the original images. The increasing number of minutiae points results in the increasing similarity values.

5 CONCLUSIONS

In the traditional fingerprint-based authentication system without any template protection, an unknown original fingerprint image can be reconstructed from the stored minutiae template. Obtaining minutia templates is the loss of biometrics forever. If a few templates in the database are compromised, a re-enrolment of all the users may be necessary and will cost lot of time and money. Therefore, a protected fingerprint template has been used instead.

In the real situation, the quality of the fingerprint images may not be as expected for example during an emergency situation. Different qualities of fingerprints are created according to environmental conditions during an emergency, such as wet or dry fingers and a disoriented angle of fingerprint images. These fingerprint images are used for evaluating two cancellable fingerprint template approaches. The two cancellable fingerprint template approaches have been selected because their techniques include the geometric information of the fingerprint into the minutiae. As a result, the two approaches have a high potential to be robust to the disoriented angle of the fingerprint images.

The experimental results have shown that the modified minutiae-based bit-strings CB performs well on all conditions during an emergency situation by achieving the matching accuracy between 83% and 100% on FVC2002DB1_B data set and between 99% and 100% on FVC2002DB2_B data set. The result of this work will be further used for proposing an improved fingerprint feature transformation approach for personal health record users during emergency situation as introduced in [31] under the framework proposed in [32].

Acknowledgment

This work was supported by the Higher Education Research Promotion and the Thailand's Education Hub for Southern Region of ASEAN Countries Project Office of the Higher Education Commission (Grant number THE-AC 033/2016).

Remark

The article was orally presented at the 23rd International Computer Science and Engineering Conference (ICSEC2019).

6 REFERENCES

[1] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition* (2nd ed.). Springer-Verlag. https://doi.org/10.1007/978-1-84882-254-2

[2] Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79, 80-105. https://doi.org/10.1016/j.patrec.2015.12.013

[3] Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007). Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 561-572. https://doi.org/10.1109/TPAMI.2007.1004

[4] Cao, K., & Jain, A. K. (2014). Learning fingerprint reconstruction: from minutiae to image. *IEEE Transactions on Information Forensics and Security*, 10(1), 104-117. https://doi.org/ 10.1109/TIFS.2014.2363951

[5] Jin, Z., Hwang, J. Y., Lai, Y. L., Kim, S., & Teoh, A. B. J. (2018). Ranking-based locality sensitive hashing-enabled cancelable biometrics: index-of-max hashing. *IEEE Transactions on Information Forensics and Security*, 13(2), 393-407. https://doi.org/10.1109/TIFS.2017.2753172

[6] Wang, S., Deng, G., & Hu, J. (2017). A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. *Pattern Recognition*, 61, 447-458. https://doi.org/10.1016/j.patcog.2016.08.017

[7] Wang, S., Yang, W., & J. Hu. (2017). Design of alignment-free cancelable fingerprint templates with zoned minutia pairs. *Pattern Recognition*, 66, 295-301. https://doi.org/10.1016/j. patcog.2017.01.019

[8] Ferrara, M., Maltoni, D., & Cappelli, R. (2012). Noninvertible minutia cylinder-code representation. *IEEE Transactions on Information Forensics and Security*, 7(6), 727-1737. https://doi.org/10.1109/TIFS.2012.2215326

[9] Cappelli, R., Ferrara, M., & Maltoni, D. (2010). Minutia cylinder-code: a new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(12), 2128-2141. https://doi.org/10.1109/TPAMI.2010.52

[10] Ferrara, M., Maltoni, D., & Cappelli, R. (2014). A two-factor protection scheme for MCC fingerprint templates. In *2014 International Conference of the Biometrics Special Interest Group (BIOSIG),* pp. 1-8. IEEE.

[11] Wang, S. & Hu, J. (2016). A blind system identification approach to cancelable fingerprint templates. *Pattern Recognition*, 54, 14-22. https://doi.org/10.1016/j.patcog.2016. 01.001

[12] Prasad, M. V., Anugu, J. R., & Rao, C. R. (2016). Fingerprint template protection using multiple spiral curves. In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics,* Springer, New Delhi, 593-601. https://doi.org/10.1007/978-81-322-2538-6_61

[13] Lee, C. & Kim, J. (2010). Cancelable fingerprint templates using minutiae-based bit-strings. *Journal of Network and Computer Applications, 33*(3), 236-246. https://doi.org/10.1016/ j. jnca.2009.12.011

[14] Guo, L., Mao, Y., & Guo, Y. (2016). Non-invertible fingerprint template protection with polar transformations. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 730-735, IEEE. https://doi.org/10.1109/PST.2016.7906990

[15] Das, P., Karthik, K., & Garai, B. C. (2012). A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition, 45*(9), 3373-3388. https://doi.org/ 10.1016/j.patcog.2012.02.022

[16] Kumar, N. (2012). *Cancelable fingerprint template*. Department of Mathematics, Indian Academy of Sciences.

[17] Wong, W. J., Wong, M. L. D., & Kho, Y. H. (2013). Multi-line code: A low complexity revocable fingerprint template for cancelable biometrics. *Journal of Central South University, 20*(5), 1292-1297. https://doi.org/10.1007/s11771-013-1614-8

[18] Belguechi, R., Hafiane, A., Cherrier, E., & Rosenberger, C. (2016). Comparative study on texture features for fingerprint recognition: application to the biohashing template protection scheme. *Journal of Electronic Imaging, 25*(1), 013033. https://doi.org/10.1117/1.JEI.25.1.013033

[19] Moujahdi, C., Bebis, G., Ghouzali, S., & Rziza, M. (2014). Fingerprint shell: Secure representation of fingerprint template. *Pattern Recognition Letters*, 45, 189-196. https://doi.org/10.1016/j.patrec.2014.04.001

[20] Nazmul, R., Islam, M. R., & Chowdhury, A. R. (2017). Alignment-Free Fingerprint Template Protection Technique Based on Minutiae Neighbourhood Information. In *International Conference on Applications and Techniques in Cyber Security and Intelligence*, 256-265, Edizioni della Normale, Cham. https://doi.org/10.1007/978-3-319-67071-3_32

[21] Sandhya, M. & Prasad, M. V. (2015). k-Nearest Neighborhood Structure (k-NNS) based alignment-free method for fingerprint template protection. In *2015 International Conference on Biometrics (ICB)*, 386-393, IEEE. https://doi.org/10.1109/ICB. 2015.7139100

[22] Li, G., Yang, B., Rathgeb, C., & Busch, C. (2015). Towards generating protected fingerprint templates based on bloom filters. In *3rd International workshop on biometrics and forensics (IWBF 2015),* 1-6, IEEE. https://doi.org/10.1109/IWBF.2015.7110224

[23] Kanagalakshmi, K. & Chandra, E. (2013). A Novel Technique for Cancelable and Irrevocable Biometric Template Generation for Fingerprints. *Global Journal of Computer Science and Technology,13(6)*. Retrieved from https://computerresearch. org/index.php/computer/article/view/208/208

[24] See http://bias.csr. unibo.it/fvc2000/databases.asp.

[25] See http://bias.csr. unibo.it/fvc2002/databases.asp.

[26] See http://bias.csr. unibo.it/fvc2004/databases.asp.

[27] See http://bias.csr. unibo.it/fvc2006/databases.asp.

[28] Choosang, P. (2016). Secure fingerprint identification evaluation for unconscious personal health records users: a case study in an emergency situation, *Master's thesis*, Prince of Songkla University, Thailand.

[29] Ang, R., Safavi-Naini, R., & McAven, L. (2005). Cancelable key-based fingerprint templates. In *Australasian Conference on Information Security and Privacy*, Springer, Berlin, Heidelberg, 242-252. https://doi.org/10.1007/11506157_21

[30] See http://neurotechnology.com.

[31] Choosang, P. & Vasupongayya, S. (2015). Using fingerprints to identify personal health record users in an emergency situation. In *2015 International Computer Science and Engineering Conference (ICSEC)*, 1-6, IEEE. https://doi.org/10.1109/ICSEC.2015.7401421

[32] Thummavet, P. & Vasupongayya, S. (2015). Privacy-preserving emergency access control for personal health records. *Maejo International Journal of Science and Technology, 9*(1), 108-120. Retrieved from http://www.mijst. mju.ac.th/vol9/108-120.pdf

Authors' contacts:

Ei Ei MON, M.C.Sc*
5910130005@psu.ac.th

Sangsuree VASUPONGAYYA, PhD, Assist. Prof.
vsangsur@coe.psu.ac.th

Montri KARNJANADECHA, PhD, Assoc. Prof.
montri@coe.psu.ac.th

Touchai ANGCHUAN, MSc, Assist. Prof.
touch@coe.psu.ac.th

Department of Computer Engineering,
Faculty of Engineering, Prince of Songkla University,
Hat Yai, Songkhla 90112, Thailand