THE COMBINATION OF THE CANCELABLE BIOMETRIC KEY AND THE CRYPTOGRAPHIC KEY FOR SECURING THE TEXT FILE

Fritz Gamaliel

Sekolah Tinggi Elektro dan Informatika, Institut Teknologi Bandung
Jl. Ganesha No.10, Jawa Barat 40132, Indonesia

fritzgamaliel@gmail.com

***Abstract* – Cryptography needs a key. Key which generated from the biometric template more represent the individuality but it endures irrevocability. The cancelable transformation makes the biometric template become revocable. In here, one of the cancelable transformation method is applied to one of the biometric-based key generation method. An issue which arising from that application is answered by combining a short key which generated from the transformed template with a key generated from the system to obtain the length which required by the used cryptographic algorithm. That proposal is implemented into Matlab 7.11.0 and PHP 5.4.7. The implementation result is tested using fingerprint samples which taken from The Third International Fingerprint Verification Competition (FVC2004). The testing result show that same person generate different key, different person generate same key, and the cancelable transformation can be executed repeatably. It concluded that combining the short key which generated from a transformed template with a cryptographic key can be used to obtain the length which required by the used cryptographic algorithm.**

***Keywords* - Biometric, Cancelable, Fingerprint, Cryptography, Key Generation**

I. INTRODUCTION

The communication between the sender and receiver can be either verbal or non-verbal. It needs to more pay attention on the security aspect of that data communication. Cryptography, a method for ensuring the security aspect, needs a key. The conventional key is not represent the individuality but the key which generated from the biometric template is represent the individuality. Biometric is irrevocable but the biometric cancelable transformation result is revocable.

Bais et all. (2012) key generation method had reduced the complexity of the biometric-based key generation algorithm. Solanki (2013) method provided the better solution if there exist the biometric compromised event by combining the key which generated from the biometric template with the cryptographic key. The experimental result which written on both paper show that Solanki (2013) and Bais et all. (2012) used the same method (pre-processing, minutiae extraction, and the key generation). Ang et al. (2005) method applied the key concept on the cancelable transformation method so that more than one cancelable template can be generated from one original template (more secure).

The need of many-to-one aspect must be fulfilled by the cancelable transformation method for ensuring the non-invertibility of the transformed template. On the other hand, it resulting in decreasing the number of features that can be extracted from the transformed template. This resulting in shortening the key which can be generated from the transformed template.

In here, the raising issue is answered by combining the short key which generated from the transformed template with the cryptographic key to obtain the length which required by the used cryptographic algorithm. In here, the key combination result is used by the blowfish algorithm for securing a text file.

II. BASIC THEORY

II.1 CRYPTOGRAPHY

It needs to build the security system of the private data for the unauthorized person can’t know it or change it. Cryptography is a method for securing the data. The development in cryptography is followed by the development in its compromising effort. In principle, cryptography has four major components as show in Figure I. First, the plaintext (message that can be read). Second, the cipher-text (message that can not be read). Third, key (key to encrypt and decrypt). Fourth, the algorithm (a method for encrypting and decrypting).

According to Mandal (2012), blowfish has the advantage in encrypting and decrypting the text file. Blowfish has two parts: key expansion and encryption / decryption. Key expansion is executed prior to encryption / decryption.

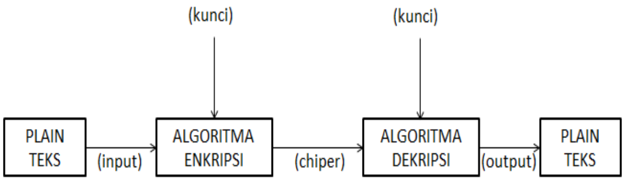


Figure I. Cryptographic system model

II.2 FINGERPRINT

A fingerprint pattern is consist of the ridge and the valley. At the global level, the pattern is categorized into types: loop, arch, and whorl as shown in Figure II. At the local level, the pattern is categorized into types: ridge ending and ridge bifurcation as shown in Figure III. Loop is the fingerprint pattern that recurve back on themselves to form a loop shape. Arch is the fingerprint pattern in which the line coming from the one side of the painting and flows into the other side of the painting with a wave up in the middle of the painting. Whorl is the fingerprint pattern which has two deltas and at least one circular line. Ridge ending is the point where the ridge ends, while ridge bifurcation is the point where the ridge branched.

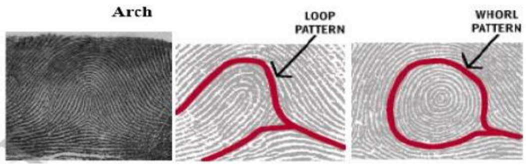


Figure II. Fingerprint global feature

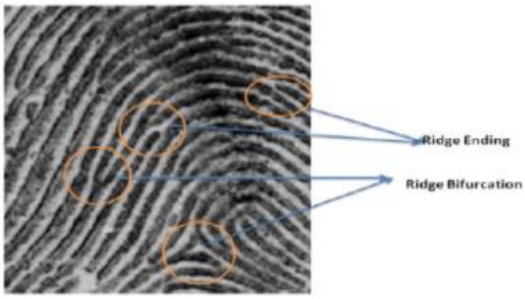


Figure III. Fingerprint local feature

General stages of the fingerprint image processing are: acquisition, preprocessing, minutiae extraction, and matching. Acquisition is the fingerprint image capturing stage. Preprocessing is the ridge and the valley clarification stage. Preprocessing stages consist of: segmentation, normalization, filter, binerization, and thinning. Segmentation separates foreground and background. Normalization makes the image has the desired mean and variance. Filter cleans up the image from the noise. Binerization converts the gray image into the binary image. Thinning reduces the width of the ridge for the ridge has one pixel width. Minutiae extraction extracts the ridge ending and the ridge bifurcation. Matching matchs the minutiae template and the minutiae query.

II.3 CANCELABLE TRANSFORMATION

Cancelable transformation (the transformation that can be canceled) concept was first proposed by Ratha et all. (2001). This idea arose because there exist two shortcomings in the previous biometric template security method. First, the hash system can't accommodate the subject interactive variation to the acquisition device. Second, the cryptographic system itself can't accommodate attacks on its decryption point. The cancelable transformation concept using a model as shown in Figure IV. Enrollment is used to store the individual data as the transformed template. Identification is used to compare the input data with all of the stored transformed template data until a match is found. Verification is used to determine whether the input data match to exactly one of the stored transformed template data. Either at the enrollment or at the identification and verification, the transformation function unit is used to convert the input data based on a rule. The matching unit compares the input data with the template data and determines whether they match based on a threshold.

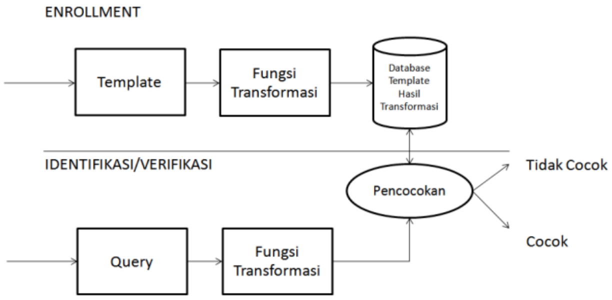


Figure IV. Cancelable system model

III. PROPOSED METHOD

In here, the cancelable transformation method is applied to the irrevocable fingerprint key generation method. More specifically, Ang et all. (2005) method is applied to the irrevocable fingerprint key generation method proposed by Bais et all. (2012) and Solanki (2013). An issue which arising from that application is the lower the number of features that can be extracted from the transformed template. This resulting in shortening the key that can be generated from the transformed template. That issue is answered by combining the key which generated from the transformed template with the key from the cryptographic system to obtain the length which required by the used cryptographic algorithm. The result can be described as shown in Figure V. In this figure, it appears that a fingerprint should be through the stages (pre-processing, minutiae extraction, cancelable transformation, and key combination) before it can be used at the key expansion stage and at the encryption-decryption stage in the blowfish algorithm.

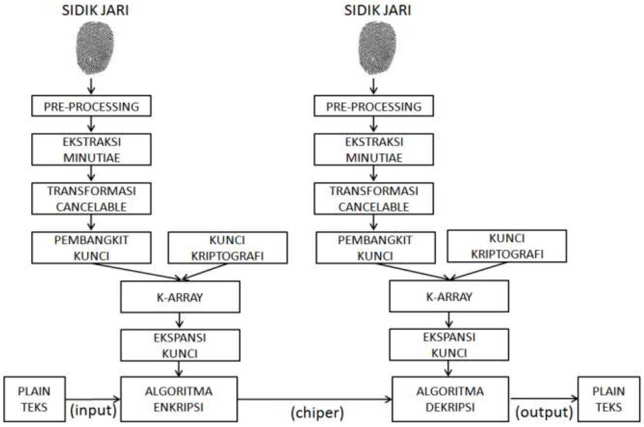
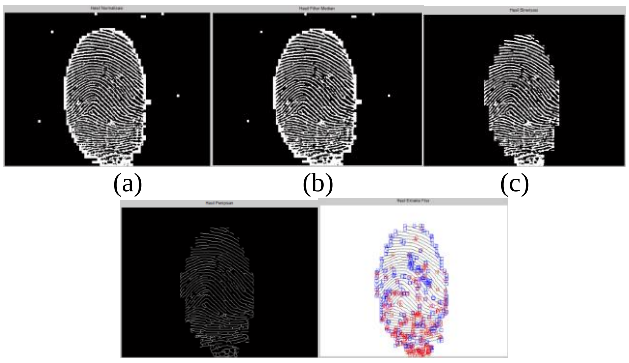


Figure V. Proposed method

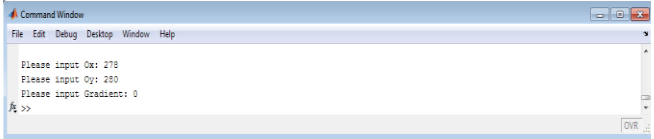
IV. IMPLEMENTATION

The proposed method has been implemented into Matlab 7.11.0 and PHP 5.4.7. The final results as shown in Figure VI.



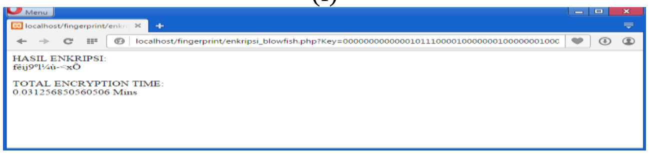
(a) (b) (c)

(d) (e)



```
Please input Ox: 278
Please input Oy: 280
Please input Gradient: 0
>>
```

(f)

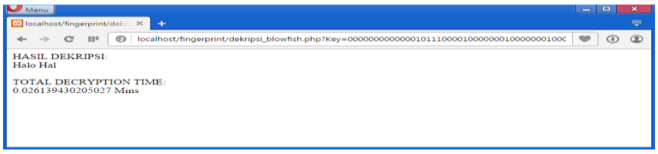


localhost/fingerprint/enkripsi_blowfish.php?Key=00000000000001011100001000000010000000100C

HASIL ENKRIPSI:
fëij9º1¼ù-<xÕ

TOTAL ENCRYPTION TIME:
0.031256850560506 Mins

(g)



localhost/fingerprint/dekripsi_blowfish.php?Key=00000000000001011100001000000010000000100C

HASIL DEKRIPSI:
Halo Hal

TOTAL DECRYPTION TIME:
0.026139430205027 Mins

(h)

Figure VI. a) The image after normalization b) The image after median filter c) The image after binerization d) The thinned image e) Minutiae extraction f) Transformation parameter g) Encryption result h) Decryption result

V. EXPERIMENT AND EXPLANATION

The implementation result were tested using fingerprint samples which taken from The Third International Fingerprint Verification Competition (FVC2004). The following table is one of the obtained experimental result.

Table I: Experimental Result

Fingerprint Image	Transformation Parameter	Key From Transformed Template
	O_x:300 O_y:300 Φ: 0	011110
	O_x:300 O_y:300 Φ: 0	1
	O_x:300 O_y:300 Φ: 0	0111
	O_x:300 O_y:300 Φ: 0	1
	O_x:300 O_y:300 Φ: 0	0

The experimental result shows that there exist the possibility where same person have different key, different person have same key, and cancelable transformation can be executed repeatably. More spesifically, there exist same key which generated from the same transformation parameter applied to different individual template. That thing leads to the security aspect (confidentiality and integrity) can't be fulfilled. Additionally, the cancelable transformation result can be generated repeatably so that the key from the transformed template can be generated repeatably too. It should be noted that the key combination result may not be generated repeatably because the key which generated from the transformed template must be combined first with the key generated from the random function to obtain the length which required by the used cryptographic algorithm.

VI. CONCLUSION AND FUTURE WORK

Required steps to generate the cryptographic key from the cancelable transformation template result are: First, minutiae extraction. Second, the extracted minutiae is transformed by using the cancelable transformation function. Third, the transformed minutiae is used to generate the key. Finally, the key which generated from the transformed minutiae is combined with the cryptographic key. It concluded that those steps can be used to obtain the length which required by the used cryptographic algorithm. Because fingerprint is not universal, multimodal biometric will be used at the next work.

REFERENCES

Christina and Irudayaraj, J. (2014) :Optimized Blowfish Encryption Technique, *International Journal of Innovative Research in Computer and Communication Engineering*, **2,**5009-5015.

Solanki, K. (2013) : A New Approach To Symmetric Key Generation Using Combination Of Biometric Key And Cryptographic Key To Enhance Security Of Data, *International Journal of Engineering Research & Technology*, **2,**1-7.

Bais, R. and Mehta, K. (2012) :Biometric Parameter Based Cryptographic Key Generation, *International Journal of Engineering and Advanced Technology*, **1,**157-160.

Ang, R., Naini, R., and McAven, L. (2005) :Cancelable Key-Based Fingerprint Template, *Australasian Conference on Information Security and Privacy*, 242-252.

Patel, V., Ratha, N., and Chellappa, R. (2015) :Cancelable Biometric: A Review, *IEEE SIGNAL PROCESSING MAGAZINE*, 54-65.

Mastali, N. (2013) :*Synergizing Fingerprint Biometrics And Cryptography for Improved Authentication*, Tesis Program Magister, University of Technology Sydney

Thai, R. (2003) :*Fingerprint Image Enhancement and Minutiae Extraction*, Tesis Program Magister, The University of Western Australia

Jovanovic, N., Kruegel, C., and Krida, E. (2006) : Pixy : A Static Analysis Tool for Detecting Web Application Vulnerabilities, *Proceeding of the 2006 IEEE Symposium on Security and Privacy.*