A Fingerprint Pattern Approach to Hill Cipher Implementation

Andysah Putera Utama Siahaan

Abstract— **The human fingerprint always becomes the way to verify the originality of the ownership. It can be connected to the security methods to increase the security level. Hill Cipher in one of the cryptography algorithms that can attach the digital fingerprint pattern. There are several matrix sizes to implement its process. This study focuses to a 3 x 3 matrix in the application. It provides nine integer numbers to perform the encryption which determinant has already been tested before. The concept is to link the digital fingerprint pattern to produce the automatic key generator. Not all the determinant value can get the ciphertext back to the original message. A threshold is used to adjust the determinant. It produces the different numbers when to be shifted. The correct numbers will be occupied in the matrix. When the numbers are available, the cryptography process can be performed.**

Index Terms— **Fingerprint, Hill Cipher, Cryptography, Security.**

I. INTRODUCTION

Fingerprint technique is one of the most important authentication technologies based on the pattern of ridges and valleys. Various applications are using this technology, but the security problems are still not fully solved [3]. Hill cipher uses a matrix to calulate the plaintext and produce the ciphertext. It contains nine cells. Each cell is given the integer number. These can be generated randomly. The purpose is replacing the producing technique. The digital fingerprint pattern is split into nine segments. After the image is getting thresholded, it forms a binary pattern. Each segment consists of the value of "0" and "1" where "0" represents the white color and "1" to the black or vise verse. It depends on the commitment. The total of the value becomes the number inserted to each cell in matrix. The threshold becomes the secondary key to produces the same numbers when decrypting the ciphertext.

In the digital era, the picture can be used as evidence or a key [2]. Hill Cipher can combine the static image to authenticate the user. Static, here, means the fingerprint is not captured in real time, but it has already captured as a picture. The fingerprint sample is not necessary. The image is scaled to a specific dimension. Several image processing steps are needed to process the bitmap into the binary data. This project alternatively aims to generate numbers without calculating the determinant manually.

Andysah Putera Utama Siahaan, Faculty of Computer Science Universitas Pembangunan Panca Budi Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing, 20122, Medan, Sumatera Utara, Indonesia

II. THEORIES

A. Digital Fingerprint

A pattern of the fingerprint is generated when the finger is pressed against a smooth surface. The most obvious structural characteristics of the fingerprint are ridges and valleys. They often run parallel, but they may bifurcate or terminate unexpectedly sometimes [3]. Fingerprints are the curved pattern in the skin fingertips. These streaks are not similar among human being although they are identical. So that fingerprints can be used to identify a person validity. Electronic scanners capture the fingerprints based on light reflections of the finger's ridges and valleys, ultrasonic's, or the electrical properties of the finger's ridges and valleys [4].

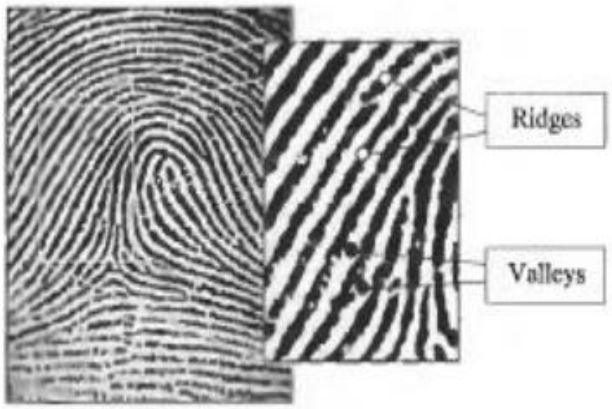

Fig. 1 Ridges and Valleys

Figure 1 show the ridges and valleys on a fingerprint. The fingerprint of every people is different. The fingerprint pattern has a different region among the model. It creates special shapes respectively. These areas may be classified into three models such as loop, delta, and whorl (Figure 2).

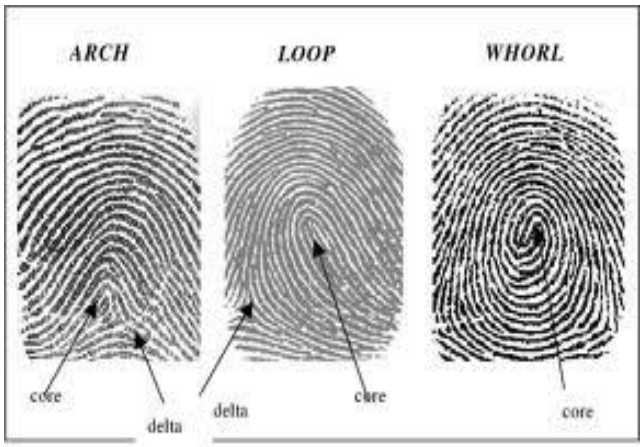

Fig. 2 Special regions and core points

B. Hill Cipher

Hill Cipher is one of the symmetric key cryptographic algorithms in data encryption [1]. To avoid the key matrix is not invertible, matrix keys are generated using a binomial coefficients newton. The encryption process and descriptions use the same key. The plaintext itself may use image, audio or text. Hill Cipher algorithm uses a matrix of m x m as a key for encryption and decryption. The basic theory of matrix used in Hill Cipher include the multiplication between the matrix and perform the inverse of the matrix. It is an application of cryptography modulo arithmetic.

Hill Cipher invented by Lester S. Hill in 1929 [5]. This cryptographic technique was created to produce the cipher text that cannot be solved by using frequency analysis techniques. It does not replace the plaintext alphabet with another for the same ciphertext. Hill Cipher is a block cipher as well. The plaintext will be divided into several blocks of a certain size. Each character in the block will affect the other characters in the encryption and decryption process. The same characters in plaintext are not mapped to the same character in the ciphertext. Hill Cipher is the classic cryptographic algorithm. It is very difficult to be solved by cryptanalyst if they have the ciphertext only. However, this technique can be solved quite easily when the cryptanalyst has the ciphertext file and a plaintext file chunks. Cryptanalysis technique is called known-plaintext attack [6].

III. Proposed Work

In this step, it figures out how the method works. The fingerprint is obtained from a scanner. The fingerprint image must be converted into a grayscale picture because it does not use a-three-layer color intensity. It must be cleaned from noise. To do this, it has to convert the grayscale into a black and white color mode. Afterward, the image is segmented into nine sections. The limit of the segment is up to the commitment. Since the fingerprint image is not square, the segmentation is not square as well. The dimension of the image is 120 x 180 pixels. The following figure is the image taken by a scanner. It is still original. The color is all mixed. There is no a threshold applied in the picture. The further process is necessary.

Fig. 3 Original fingerprint

The image needs to be converted first. After the image has been in the grayscale mode, it needs to convert it back to the black and white. In this process, there a value to limit the color intensity. It is called the threshold. After the processes are done, the segmentation is carried out. Figure 4 illustrates the segmentation after the image preprocessing. The amount of the pixel in every segment is entirely different because the shape of the finger is oval.

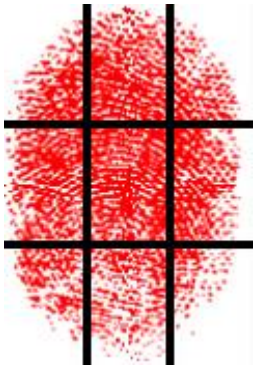

Fig. 4 Fingerprint segmentation

The fingerprint has nine segments. There are only two colors in this stage such as red and white since it limits the color intensity before.

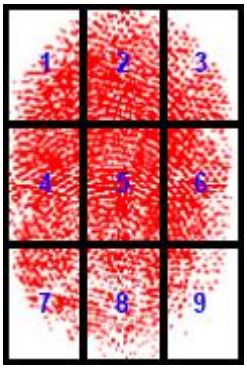

Fig. 5 Numbered fingerprint segmentation

In Figure 5, there are nine segments. For example, in segment number 1, there are many red pixels. Those indicate the value will be used in Hill Cipher. Imagine that it contains 400 dots in segment 5. This value has to face the modular expression to make the number is suitable in Hill Cipher Process. Modulo also adjusts the determinant to give the correct value. The following formula explains how it works.

$$N = TP \; Mod \; TC \qquad (1)$$

Where :

N	:	Integer Number
TP	:	Total pixel in a specific segment
TC	:	Maximum value of modular expression

The total pixel is obtained from how many red colors in the segment. The computer program calculates the red pixel one by one and store to the variable. It changes the pixels to characters. The program changes the white color to "." while the red to "X" to make them clear. The following figure shows a magnification of the fingerprint.

.....
.....
.....
.....
.....
.....
.....
.....
.....X.XX.
.....XX
.....X...
.....
.....X.....X.X
.....XX..X.XXX
.....XXX..
.....X..
.....XX.X.....
.....XX.....X
.....X.XX.....X
.....XXX.XXX
.....X.....XX.XXX
.....XXXXX.....XX....
.....XXXXXXX.X...
.....XXX.XXXX
.....X.....XXX
.....X..X..XX....X.X.....
.....X.....X....XXX
.....X..XX....X..
.....XXXXX...XX..XX..XXXXX
.....XXXX...X.XXXXXXXXXXX
.....XX...X.....XX.XXX.XXX
.....X.XX.....XXX....X
.....XXXXXXXXXX.XXXX.X
.....X.XX.XX.XX.XX.X.XXXXXXXXXXX
.....XXXXXXXXXX....XXXX.XXXXXXX
.....X.....XXXXXXXXXX..X.
.....XXXXXXXXXXX.X
.....XX..XX.XXX..XXXX.XXXXXXXX
.....X...XXXX....XX.XX..XXXXX..XXX..XX
.....XXXXX.....XXXXXXX....
.....XXXXXXXXXXXXXXXXXX
.....XXX.XXXXXXXXXXXXXX..
.....XXX..XXX.XXXXX...XXX.XXX..X
.....X.XX.XXXXX....XXXXXXXXX.XX.XX.XXX
.....XXXXXXXXX.XXX..XXXXX.XX
.....XX...X.....XXXXX.XX...XX..X.XX
.....XX.XXXXXXXX..XXX....XXXXXXX.XXX
.....XX..XXXXXXXXX.XXXXXXXXXXX.
.....X....X.X...XXXXX.X.XXXXXX..
.....XXXX.X...X..XXXXX...XXXXXXX..X
.....X.....XXXXXXXXXXX...XXXXXXX.XX
.....X.....X.XXXXXXXXXXX.X.XXXXXX
.....X..XXXXXX...XX..XXXXXXXXX...XXX
....X.....XXXXXX.XXX.XXXXXXX.XXXXXXXXX
.....XXXXXXXX.XX.X.XXXXXX.X
.....XXX.XXXXXXX..XXX.XXXXXX.XXX...X
.....XXXXXXX.XX.XX.XXXXXXXXX.XXX
.....XX...X....X.XXX.XXX.XX...XXXXXXX
.....XX.XXX.XXXXXXX..XXXXXX..X.X.XXXX

Figure 6. Extracted data from the first segment

Figure 6 illustrates the data is retrieved from the first segment. Since it is at the edge of the finger, the shape is round as well. It needs to count how many "X" in the figure. The value is inserted into the cell respectively.

IV. Evaluation

The best way to prove the method is through a test. Assume the Hill Cipher key is now empty. There are three columns and rows in every key. It has to complete the step for nine times. Table 1 below shows that the matrix model before insertion. X^{11} to X^{33} are the cells where the integer numbers are located.

TABLE I HILL CIPHER KEY

Key		
X^{11}	X^{12}	X^{13}
X^{21}	X^{22}	X^{23}
X^{31}	X^{32}	X^{33}

The experiment runs with three kinds of threshold. The first threshold is 50, the second is 125 and the last is 200. The three pictures give the different shape.

Figure 6. (a) Threshold = 50, (b) Threshold = 125, (c) Threshold = 200

The pictures in Figure 6 have the different display. The calculation of the red pixel shows the different result as well. The set of the first threshold (50) can be seen in Table 2. From the fingerprint, it produces 204, 242, 227, 166, 248, 223, 112, 220 and 84.

TABLE II KEY OF THRESHOLD 50

Key		
204	242	227
166	248	223
112	220	84

Determinant
-1103880
248

The set of the second threshold (125) is in Table 3. The fingerprint calculation produces 124, 84, 91, 214, 209, 105, 241, 29 and 39.

TABLE III KEY OF THRESHOLD 125

Key		
124	84	91
214	209	105
241	29	39

Determinant
-1961133
83

The set of the first threshold (200) generates 77, 242, 84, 163, 239, 241, 34, 235 and 220. It is in Table 4.

TABLE IV KEY OF THRESHOLD 200

Key		
77	242	84
163	239	241
34	235	220

Determinant
-4472371
205

There are three determinants. Remember, not all determinant work. Why? It is only useful if the computer generates the odd number. Those determinants show two sections. The real determinants are -1103880, -1961133 and -4472371 as showed in Tabel 2 to Table 4. The numbers have to be normalized by modulo them with the ASCII length; that is 256. The numbers will turn into the positive number. The determinant can be the odd and even number. Since it produces the even number, the value can return the plaintext. It will fail if the decryption process is done. From those tables, there are only two sets of keys can be used as the encryption keys. There are in Table 3 and Table 4. Those numbers are showing the odd number, 83 and 205. Decrypting the even number, the computer faced the forever repetition.

The research does not include the encryption and decryption process because our focus is only to generate the key using the fingerprint pattern. The readers must have been familiar with the Hill Cipher algorithm. The fingerprint image can simplify the distress of the key store. The user does not have to remember such numbers and just keep the picture and the threshold value when doing the encryption and decryption process.

V. CONCLUSION

There are many ways to construct the key in Hill Cipher. One of the techniques is using an image and threshold. The numbers are adjustable to get the correct determinant. The fingerprint has a plurality of segments. It has a pattern which consists of a collection of dark and white pixels. This situation can be utilized to produce the Hill Cipher key. The threshold can be set as desired to generate the specific numbers. Afterward, the numbers can be inserted into the Hill Cipher cells. By providing the correct threshold, the decryption process can be carried out.

REFERENCES

[1] A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," *International Journal of Science and Research,* vol. 5, no. 7, 2016.

[2] A. P. U. Siahaan, "RC4 Technique in Visual Cryptography RGB Image Encryption," *International Journal of Computer Science and Engineering,* vol. 3, no. 7, pp. 1-6, 2016.

[3] L. H. Thai dan N. N. Tam, "Fingerprint Recognition Using Standardized Fingerprint Model," *International Journal of Computer Science,* vol. 7, no. 3, pp. 11-17, 2010.

[4] S. S. Mudholkar, P. M. Shende dan M. V. Sarode, "Biometrics Authentication Technique For Intrusion Detection Systems Using Fingerprint Recognition," *International Journal of Computer Science, Engineering and Information Technology,* vol. 2, no. 1, pp. 57-65, 2012.

[5] B. Forouzan, Cryptography and Network Security, McGraw-Hill, 2006.

[6] H. Anton dan C. Rorres, Elementary Linear Algebra, 2011: John Wiley & Sons.

AUTHOR PROFILE

Andysah Putera Utama Siahaan was born in Medan, Indonesia, in 1980. He received the S.Kom. degree in computer science from Universitas Pembangunan Panca Budi, Medan, Indonesia, in 2010, and the M.Kom. in computer science as well from the University of Sumatera Utara, Medan, Indonesia, in 2012. In 2010, he joined the Department of Engineering, Universitas Pembangunan Panca Budi, as a Lecturer, and in 2012 became a junior researcher. He is applying for his Ph. D. degree in 2016. He has written in several international journal and conference. He is now active in writing papers and joining conferences.