A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm

IOP Conf. Series: Journal of Physics: Conf. Series **954** (2018) 012003 doi:10.1088/1742-6596/954/1/012003

A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm

Dicky Nofriansyah[1*], Sarjon Defit[2], Gunadi W Nurcahyo[2], G Ganefri[3], R Ridwan[3], Ansari Saleh Ahmar[4] and Robbi Rahim[5]

[1]Doctoral Student, Universitas Negeri Padang, Padang, Indonesia
[1]Department of Information System, STMIK Triguna Dharma, Medan, Indonesia
[2]Faculty of Computer Science, Universitas Negeri Padang, Padang, Indonesia
[3]Faculty of Engineering, Universitas Negeri Padang, Padang, Indonesia
[4]Department of Statistics, Universitas Negeri Makassar, Makassar, Indonesia
[5]School of Computer and Communication Engineering, Universiti Malaysia Perlis, Malaysia

*dickynofriansyah@ymail.com

Abstract. Cybercrime is one of the most serious threats. Efforts are made to reduce the number of cybercrime is to find new techniques in securing data such as Cryptography, Steganography and Watermarking combination. Cryptography and Steganography is a growing data security science. A combination of Cryptography and Steganography is one effort to improve data integrity. New techniques are used by combining several algorithms, one of which is the incorporation of hill cipher method and Morse code. Morse code is one of the communication codes used in the Scouting field. This code consists of dots and lines. This is a new modern and classic concept to maintain data integrity. The result of the combination of these three methods is expected to generate new algorithms to improve the security of the data, especially images.

1. Introduction

The rapid development of technology today makes the data storage process easier. However, many people now have doubts about the security when the computer stores the data. It can't be separated from the occurrence of various wiretapping and monitoring actions by unauthorized or irresponsible parties so that secrecy is not maintained in securing data. Many ways to secure data one of them by using Cryptography and Steganography method[1] [2] [3].

Cryptography is the science to the confidentiality of the message. While Steganography is the art of hiding messages in digital media in such a way that other people do not realize there is a message in the media. In Cryptography and Steganography then the data that is considered secret will be disguised in such a way that if the data can be obtained, then it will not be understood by unauthorized parties. One method that can be used in cryptographic techniques is Least Significant Bit (LSB) and Hill Cipher[1]. Hill Cipher is one of the key symmetric cryptography algorithms. Hill Cipher algorithm uses the m x m sized matrix as the key for encryption and decryption. While the LSB method is a simple steganography method and easy to implement [1, 2].

Morse code is a system of representation of letters, numbers, and punctuation by using code signals. Morse code was created by Samuel F.B. Morse and Alfred Vail in 1835. Morse code is also used and studied in scouting or scouting. In the scouting world, Morse code is delivered using a scout flashlight or whistle. Morse code is performed using short whistle-length whips to represent the point and blow the whistle with long duration to represent the line. In the order of bits in a byte (1 byte = 8 bits), there is the least significant bit (MSB) and least significant bit (LSB). Example byte 11010010, the bit number 1 (first, underlined) is the MSB bit, and the bit number 0 (last, highlighted) is the LSB bit. The suitable bit to replace is the LSB bit because the change only changes the byte value one or higher or one lower than the previous value

2. Methodology

Data is a record of facts. Data is a plural form of datum, derived from the Latin meaning something given. In everyday use, the data means a statement received as is.

Figure 1. Cryptography Concept

Cryptography from Greek. According to language, the term cryptographic word is divided into two, crypto and graphia. Crypto means secret and graphia means writing. According to its terminology, cryptography is the science and art of keeping messages safe when messages are sent from one place to another several mechanisms develop in modern cryptography[13][14][15] that is:

a. Hash function. The hash function is a function that mapping a message of any length to a special text called message digest with a fixed length. The hash function is used as the test value (check value) on the data integrity mechanism.
b. Encryption with a symmetric key. The encryption with the symmetric key is the encryption that the encryption key and the decryption key are equal. The key to symmetric encryption is assumed to be confidential only to those who encrypt and decrypt who knows its value.
c. Encoding with asymmetric key. Encoding with asymmetric keys or often called public key encryption is encrypted with different encryption and decryption keys. An encryption key also called a public key, is open. Meanwhile, the decryption key which is also known as the private key is closed or secret.

Steganography is a branch of science that studies about how to hide a "secret" information in other information. Steganography has a history similar to cryptography, both of which were widely used during the war era. The steganography difference with encryption lies in how the process of concealment of data and the result of the process. Encryption operates randomizing the original data to produce encrypted data that is entirely random and distinct from the original[13], whereas steganography hides data in other data to be hosted before and after the hiding process is almost the same [4].

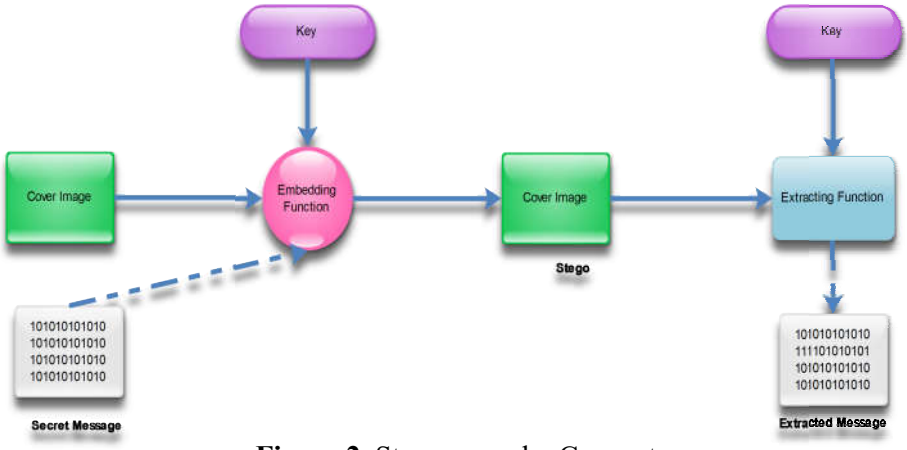

Figure 2. Steganography Concept

3. Results and Discussion

The use of cryptographic techniques with hill chipper algorithm[12], Morse code and steganography with LSB method is expected to protect and secure secret messages when the message is delivered through internet media from unauthorized parties; this is to avoid the occurrence of crimes such as taking or tapping of the secret message delivered it. This LSB method is quite vulnerable to the presence of steganography-analysis that suspects the existence of confidential information in it. If the steganography-analysis detects the presence, then the message will soon be known. Another case if the message is encrypted first using hill chipper algorithm before the insertion process. If steganography-analysis succeeds in expressing the message in the stego-image, the message is still not easily known because it is still in an encrypted state.

An improvement security by combining cryptographic techniques with hill chipper algorithms and steganography with the LSB method simultaneously will result in a better secret message security level. The secret message security process that is done is to insert the message into a container (cover) that is in the form of digital images using steganography technique, where the message before inserted already encrypted first using cryptographic techniques.

Phase 1: Hill Cipher and Converted Morse code

Before the secret message is inserted into the digital image media, the message will be encrypted using hill cipher algorithm. This encryption process requires a key that is the same length as the message text, and then the key will repeatedly be treated along the number of message text. This encryption process will produce ciphertext ready to be inserted into digital image media[5].

Following the problem limitation, the image file used is a 24-bit bitmap format. The secret message that can be accommodated in the digital image media depends on the capacities of the imagery. Example in the 24-bit digital image file measuring 400 x 267 pixels, there are 40050 pixels, each pixel (dot) in the image consists of three primary colors, namely red, green and blue (RGB), where each base color is presented with a size of 8 bits (1 byte). Total capacity of the container media is 40050 x 3 = 120150 bytes. Since each byte can insert only 1 bit of its LSB, the size of the data inserted in the image is 40050: 8 = 5006, 25 bytes (1 byte = 1 character). The size of this data should be reduced by the length of the filename because the concealment of the secret message hides not only the contents of the message but also the filename[6].

The message insertion process is done, first the message is encrypted with Hill cipher algorithm. For the use of hill chipper algorithm for this data encryption, matrix is used with order 2 * 2, with boundary value of each element between 0-255. The matrix multiplication result is then converted into Morse code in point and row model. Since Morse code recognizes the letters A to Z and 0 to 9, then the data character is additionally converted into binary data form [7] [8]. From the value, will be taken the binary value of each character that will then be inserted into the image by using the method LSB (Least Significant Bit). As an illustration, is suppose from the following matrix:

a. Element (1, 1) the binary value of 7 is 0111.
b. Element (1, 2) the binary value of 18 is 10010.
c. Element (2, 1) the binary value of 23 is 10111.
d. Element (2, 2) the binary value 11 is 1011.

The key matrix to be inserted is:
Element (1, 1) = 00000111.
Element (1, 2) = 00010010.
Element (2, 1) = 00010111.
Element (2, 2) = 00001011.
If an image has the raster data as below:

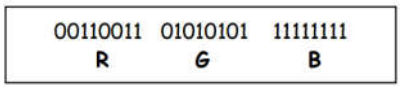

Figure 3. Examples of Raster Data

After inserted key element matrix (1, 1) by replacing 4-bit R value and value B from the right with binary value element (1,1) will become new pixel data.

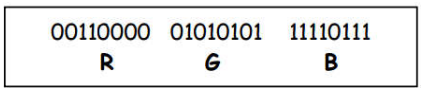

Figure 4. New Data Pixel

Phase 2: Least Significant Bit Procedure
The technique of inserting data in this image using the LSB (Least Significant Bit) method, where the data will be inserted into the lower bits (4 bits below) [3] [9] [10]. But, on the odd bits of the RGB value of a pixel (the smallest data unit that makes up the image). 2-bits into the value of R and 2 more bits into the B value, so one character will need 2-pixel containers. Suppose the steps to insert the character "I", assuming already done data randomization by Hill Cipher method and Converting to Morse Code [11] ; it will do the stages as follows:

Table I. Converting Morse code to Ascii Code

Plaintext	Morse Code	Ascii Code
A	. -	46,45
K	-.-	45,46,45
U	..-	46,46,45

After that will be converted into binary values so the resulting calculation as follows:
46 = 00101101, 45 = 00101100
45 = 00101100, 46 = 00101101, 45 = 00101100

46 = 00101101, 46 = 00101101, 45 = 00101100
Then take the value of each pixel of the image to be inserted. As in the picture below:

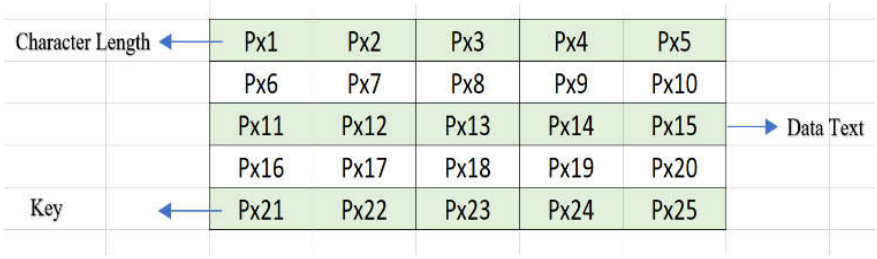

Figure 5. Illustration of a Pixel Image

From the above pixels px1 (pixel 1) - px5 (pixel 5) is used to hold the length of the character, which serves as the capture limit of data that has been inserted by other characters. Then px6 (pixel 6) - px20 (pixel 20) according to the data holding requirement is used to hold the character data, and then px21 (Pixel 21) onwards is used to store the elements of the encryption matrix. Suppose the data of each pixel is as follows:

a. Px6 -> R = 145, G = 22, B = 128
b. Px7 -> R = 150, G = 22, B = 129
c. Px8 -> R = 155, G = 21, B = 130
d. Px9 -> R = 220, G = 19, B = 131
e. Px10 -> R = 215, G = 30, B = 125
f. Px11 -> R = 214, G = 16, B = 150

Then from those values will also be converted into binary values, so the following values appear:

a. Px6 -> R = 10010001, G = 00010110, B = 10000000
b. px7 -> R = 10010110, G = 00010110, B = 10000001
c. Px8 -> R = 10011011, G = 00010101, B = 10000010
d. Px9 -> R = 11011100, G = 00010011, B = 10000011
e. px10 -> R = 11010111, G = 00011110, B = 01111101
f. px11 -> R = 11010110, G = 00010000, B = 10010110

Inserts the binary value of the character to the binary value of the above pixels.

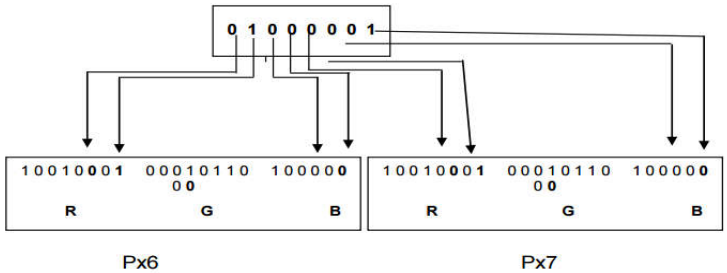

Figure 6. Illustration of a Message Insertion

In this research, at least pixel for an image is 22-pixels obtained from text data, or plain text is at least one character. In the process of the program to facilitate the calculation of each odd data, the author adds one character so that the amount of data becomes even. Data owned now into two characters where the length of the character of the data is 2. The amount of data that will be added to the duration of the binary value of 2 characters is 8 times 2 is 16. So, also added with the number of

matrices 2 x 2 is 4. The total minimum media is: Number of text data + Number of binary data + Number of matrices is 2 + 16 + 4 is 22-pixels.

4. Conclusion

From the results of design steganography security applications, then obtained a conclusion is By using the LSB and Hill Cipher method and Morse Code was able to secure data better in comparison using only 1 algorithm. Looking at the characteristics of these three methods, they can be combined into a new concept or model in securing the picture message data.

REFERENCES

[1] Z. E. Dawahdeh*, et al.*, 2017. A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher, *J. of King Saud University - Comp. Inf. Sci.*.
[2] Q. Liu*, et al.*, 2008. Image complexity and feature mining for steganalysis of least significant bit matching steganography, *Inf. Sci.,* **178**, pp. 21-36.
[3] S. Wang*, et al.*, 2015. Least significant qubit (LSQb) information hiding algorithm for quantum image, *Measurement,* 73, pp. 352-359.
[4] H. Sajedi, 2016. Steganalysis based on steganography pattern discovery, *J. of Inf. Security Appl.,* **30**, pp. 3-14, 2016.
[5] Y. Sazaki and R. S. Putra, 2016. Implementation of Affine Transform Method and Advanced Hill Cipher for securing digital images, in *2016 10th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pp. 1-5.
[6] A. A. M. Khalaf*, et al.*, 2016. A triple hill cipher algorithm proposed to increase the security of encrypted binary data and its implementation using FPGA, in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, pp. 1-1.
[7] B. Purnama and A. H. H. Rohayani, 2015. A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext From a Message to Be Encrypted, *Procedia Comp. Sci.,* **59**, pp. 195-204.
[8] D. C. Mishra*, et al.*, 2015. Security of RGB image data by affine hill cipher over SLn(qF) and Mn(qF) domains with Arnold transform, *Optik - Int. J. for Light Electron Optics,* **126**, pp. 3812-3822.
[9] Z.-H. Wang*, et al.*, 2012. Optimizing least-significant-bit substitution using cat swarm optimization strategy, *Inf. Sci.,* **192**, pp. 98-108.
[10] W.-L. Xu*, et al.*, 2016. An improved least-significant-bit substitution method using the modulo three strategy, *Displays,* **42**, pp. 36-42.
[11] C.-H. Yang, 2003. An interactive morse code emulation management system, *Comp. Math. Appl.,* **46**, pp. 479-492.
[12] A. Putera, U. Siahaan, and R. Rahim, 2016. Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm, *Int. J. Secur. Its Appl.*, **10**, 8, pp. 173–180.
[13] H. Nurdiyanto, R. Rahim, and N. Wulan, 2017. Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement, *J. Phys. Conf. Ser.*, **930**, 1, pp. 12005.
[14] R. Rahim, M. Dahria, M. Syahril, and B. Anwar, 2017. Combination of the Blowfish and Lempel-Ziv-Welch algorithms for text compression, **15**, 3, pp. 292–297.
[15] R. Rahim, 2017. Man-in-the-middle-attack prevention using interlock protocol method, *ARPN J. Eng. Appl. Sci.*, **12**, 22, pp. 6483–6487.