Combination Playfair Cipher Algorithm and LSB Steganography for Data Text Protection

by Apri Siswanto

Submission date: 09-Aug-2019 11:02PM (UTC+0800)
Submission ID: 1158899282
File name: TURNTINOKE.docx (514.4K)
Word count: 1936
Character count: 10161

Combination Playfair Cipher Algorithm and LSB Steganography for Data Text Protection

Apri Siswanto[1], Sri Wahyuni[2]
[1 2]*Department of Informatic, Faculty of Engineering, Universitas Islam Riau, 28284, Perhentian Marpoyan, Pekanbaru, aprisiswanto@eng.uir.ac.id, yuniayu@student.uir.ac.id*

Keywords: Cryptography, Steganography, Playfair Cipher, Grayscale, Least Significant Bit (LSB).

Abstract: Encryption and steganography are needed to ensure the integrity and confidentiality of data in the process of sending data on the internet. In this paper, there are two stages to securing the message. The first step is to randomize messages to be sent with Polygram cipher substitution. The second step is to avoid messages from third party suspicions that can be done with the steganography process. The message used in this study is text. In the cryptographic process, the message in the form of text will be encrypted with the Playfair Cipher method, and then the encrypted message will be carried out in the LSB steganography process on a gray scale 8-bit digital image on a scale of 0-255. This study shows that by using Playfair Cipher and cryptographic Steganography in insertion, encrypted messages will be difficult to return to original messages by unauthorized parties. The result of this application is that you can insert hidden messages in text form into PNG format digital image files and can extract hidden messages from the image (stego-image).

1 INTRODUCTION

Encryption is one way to secure data, namely by encoding the original message (plaintext) into a secret message (ciphertext). This security process involves algorithms and keys. The encryption key can easily restore the plaintext from the ciphertext. Therefore, we need a strong encryption algorithm. With the development of encoding, people can easily obtain encryption keys in various ways (Schneier, 1996).

Therefore the development of cryptographic methods needs to be extended to use which is not only limited to encoding in the form of text but also in the type of images, audio and video (Soplanit & Bandaria, 2007). There are two techniques used for encoding data/images i.e., classical cryptography and modern cryptography. Encryption using classical cryptography is a method for converting original data (plain text) to a secret message (ciphertext) using the same key. While modern cryptography used two keys, one key called a public key that can be published, while another key called the private key must be kept secret (Stinson, 2005).

Playfair Cipher is one of the methods classified in classic cryptography. The encryption process used processing in the form of very large blocks. Playfair treats diagrams in the plaintext as single units and translates these units into ciphertext diagrams. The Playfair algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword. The rules for filling in this 5x5 matrix are: L to R, top to bottom, first with keyword after duplicate letters have been removed, and then with the remain letters, with I/J used as a single letter (Desai & Rathod).

This method is one way to overcome the weaknesses of other classic cryptographic methods that are easily guessed because there is a one-on-one correspondence between plaintext and ciphertext. Like text messages in maintaining confidentiality, text messages also require encryption techniques that are as simple as possible but difficult to solve. The process of securing messages can be done by encrypting messages into images with certain algorithms. This is possible considering a message can be represented in a matrix containing integers (Rahim & Ikhwan, 2016).

Furthermore, steganography is the science and art of hiding secret messages in a way so that no one suspects the existence of the message. The aim is how to hide the message so that the presence not detected by third parties to avoid conspicuous suspicions

(Munir, 2016). The development of computer capabilities, the internet is accompanied by the development of digital signal processing, information theory, cryptography and steganography has transformed digital media (Siswanto, Syukur, & Husna, 2018). In this realm digital steganography has created an atmosphere where companies develop attractive applications, so the evolution of this field is guaranteed. One of the early methods of discussing digital steganography was put forward Kurak and McHugh (1992). They proposed a method which breaks down and adds information at least significant bits (LSB). They study images at the lower level and insert new information now known as image-based steganography.

LSB is a technique commonly used in encryption and decryption of confidential information. LSB works by changing the redundant bits of the cover image that have no significant effect on the bits of the secret message (Pelosi et al., 2018). Figure 1 below shows the mechanism of the LSB method in 8-bit images by utilizing 4 bits LSB.

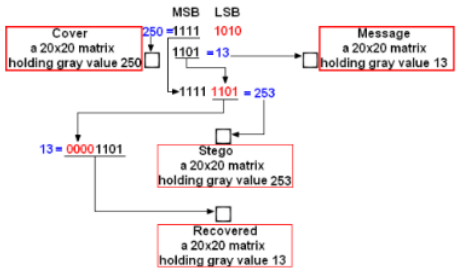

Figure 1: LSB Mechanism

In this paper, the Playfair Cipher method implemented to encode a text message into a form of an image to maintain secrecy with the increasingly broad composition of cybercrime. Then the ciphertext will be processed with LSB Steganography.

2 RELATED RESEARCH

Hatta, Ardi, and Maharani (2017) researched how to maintain message security when sent via an SMS (Short Message Service) network. The problem in this study is that someone who carries a message to the other person wants it can be read-only by the legal person. Encryption is needed to solve this problem to maintain message confidentiality. The researcher proposed an SMS cryptographic application on an Android-based Smart Phone using the Playfair cipher method. It can be sent cipher SMS messages and receive encrypted text messages then also can be decrypted in the receiver side. This application performs cryptography in the form of text letters. The key used is in the way of letters. The results of this study is an Android-based application that can send encrypted SMS messages using the Playfair cipher method so that the confidentiality of the message can be protected.

Then MU'MI (2017) proposed a cryptographic application to counteract the dangers of theft and message manipulation. The method used is hybrid Playfair cipher and caesar cipher method and steganography on message insertion. The Playfair cipher method is used in the encryption process, followed by the Caesar cipher method. The results of encryption from a combination of the two ways are inserted into the image (embedding process). Insertion Simulation The encrypted message is simulated with MATLAB as a computing aid. The simulated image is saved in the bitmap (.bmp) format. The results of this study indicate that by using a combination of Playfair cipher and Caesar cipher in encryption, encrypted messages are increasingly difficult to return to original messages by unauthorized parties. Inserting it into the image makes the observer not aware of the information embedded in the image that acts as a message.

Furthermore, Simbolon (2016) discussed how to keep the secret of the student academic transcript. The problem in this study is that someone who sends a message wants the message to be secure and reaches the right person. To solve this problem, an encryption system is needed that can maintain the confidentiality of the message by using Playfair cipher cryptography and LSB steganography technique. A combination of cryptography and steganography can enhance the message security. In this study, Playfair ciphers are included in the Polygram Cipher. This algorithm encrypts the alphabet pair (bigram) in the plaintext. In their research, they proposed the Playfair matrix table used is a 6x6 matrix. Steganography used is a spatial domain method with the Least Significant Bit (LSB) technique which consists of 2 parts, namely LSB Embedding Process and LSB Extracting Process. This research used a quantitative research method. The results obtained from this study are in the form of 8-bit grayscale bitmap image files per pixel with a scale of 0 to 255, or with the binary format. The successful secret message is fully returned to the original message with the decryption process.

3 RESEARCH METHOD

Playfair Cipher, and LSB Steganography algorithms are implemented using the PHP programming language. The encryption process is done step by step for each message that will be embedded in various media. The first step is the text message will be encrypted with the Playfair Cipher method, and then the text cipher will be steganography on 8-bit grayscale digital images on a scale of 0-255, with the Least Significant Bit (LSB) method. The encryption process is as shown Figure 2.

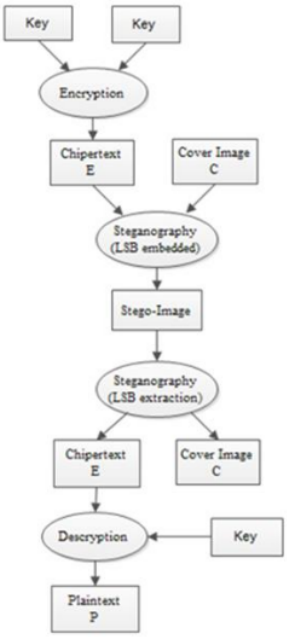

Figure 2: encryption and decryption process

The Playfair cipher pseudo-code algorithm is as follows :

STEPS :
1. A plaintext message is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter
2. The rules of encryption are
3. If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom)
4. If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)
5. If neither of the preceding two rules is true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle

4 RESULT AND DISCUSSION

The results obtained after the coding implementation with php like Figure 3. The first process that is done is the message input, key and original image.

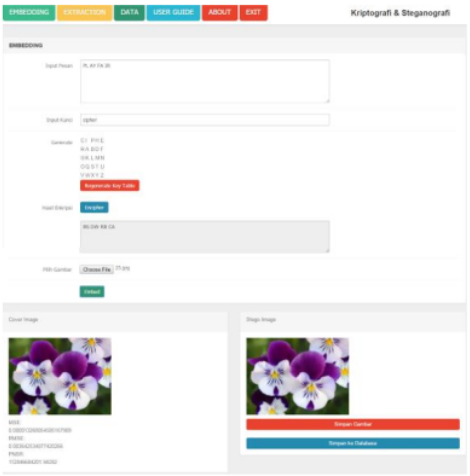

Figure 3: Embedding Process

After inputting the message and key, the system will proceed with the encryption process. Ciphertext encryption results later Inserted in the image. The last step is saving the stego image in the database. The system showed the MSE (Mean Square Error) and PNSR (Peak Signal to Noise Ratio) normal results. MSE valued between the original image and the manipulated image. In the case of steganography; MSE is the mean square error value between the original image (plain image) with the cipher image. PSNR is usually measured in decibels (dB) (Mohsin et al., 2018). PSNR is used to find out the comparison of the quality of the plain image and cipher image (Challita & Farhat, 2011). PSNR is defined as:

$$PSNR = 10log_{10}\left(\frac{C^2 max}{MSE}\right)$$

To determine the PSNR, the MSE (Mean Square Error) value must first be determined. MSE is defined as:

$$MSE = \frac{1}{MN}\sum_{X=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2$$

Extraction Menu System Testing
The first step is to select the image that was processed previously. Then input the same key during the encryption process. Can be seen in Figure 4.

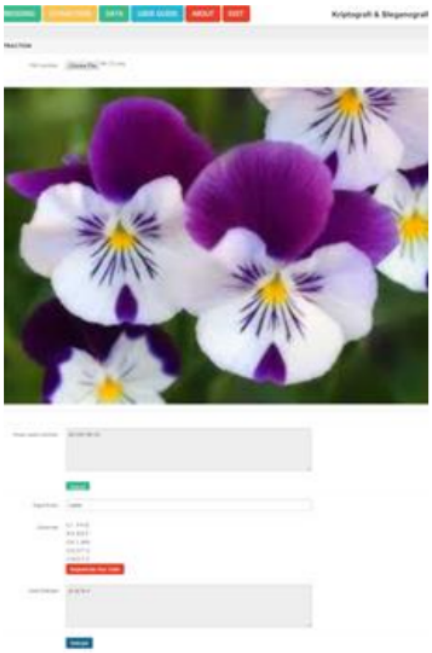

Figure 4: Extraction Process

After embedding and extraction the next step is the result of the embedding and extraction process contained in the data menu can be seen in table 1.

Table 1: MSE and PSNR result

Message	Plain Image	Cipher Image	MSE	PSNR
IA LA NU TA MA	flower1.jpg	flwcipher1.jpg	1.02881e-005	1.4533e+011
SE MO GA BE RH AS IL	Flower2.jpg	Flwcipher2.jpg	1.7683e-005	8.46721e+010
PL AY FA IR	Flower3.jpg	Flwcipher3.jpg	1.32681e-005	1.12847e+011

Based on the results from table 1, it shows that there is no significant change in the stego image from plain image that has been inserted a secret message.

5 CONCLUSIONS

Based on the results of analysis and testing, a combination of Playfair Cipher Cryptography and Steganography with LSB for Text Data Security, several conclusions can be drawn, i.e.:

1. Combination system Cryptography and Steganography can help users maintain the confidentiality of a message so that it reaches the rightful person.
2. Can block attacks carried out by cryptanalysts by using Cryptography and Steganography.
3. The results of the program simulation, namely the initial image before the message is inserted and after the message is inserted in plain view is difficult to distinguish.

For future research is expected to develop this system for mobile devices. Review further about the combination of cryptographic algorithms with methods and data other than text, such as images, videos or audio.

REFERENCES

Combination Playfair Cipher Algorithm and LSB Steganography for Data Text Protection

ORIGINALITY REPORT

12%	10%	3%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.cmscbe.com Internet Source	4%
2	www.slideshare.net Internet Source	4%
3	www.tutorialspoint.com Internet Source	1%
4	Lecture Notes of the Institute for Computer Sciences Social Informatics and Telecommunications Engineering, 2013. Publication	1%
5	Submitted to University of Mauritius Student Paper	1%
6	ejournal.stiki-indonesia.ac.id Internet Source	1%
7	www.utc.edu Internet Source	<1%
8	Muhtadin, Kiki Fatimah, Yoyon K. Suprapto. "Brittle Ancient Document Using Adaptive	<1%

Local Thresholding", 2018 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM), 2018

Publication

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		