

PAPER • OPEN ACCESS

Application Of Hill Cipher And LSB + 1 Methods For Messaging In Messages Inpicture

To cite this article: Edy Victor Haryanto *et al* 2019 *J. Phys.: Conf. Ser.* **1361** 012009

View the [article online](#) for updates and enhancements.



IOP | ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

Application Of Hill Cipher And LSB + 1 Methods For Messaging In Messages Inpicture

Edy Victor Haryanto*, Eka Dipa Pratama Nasution, M. Barkah Akbar, Bob Subhan Riza

Universitas Pembangunan Pancabudi

Abstract. This research discusses encryption and security description of files in images with hill cipher cryptography and steganography using the lsb + 1 method, testing the results of cryptographic and stegano data security applications that are equipped with cryptography, then from the results the trial was done with the hill cipher method, by displaying data in the form of files that want to do the data security. The results of the DIPA trial with a file size of 17.2 MB after being encrypted into RNPF with a file size of 17.2 MB.

Keywords: hill cipher, lsb + 1, file, cryptography, steganography, image

1. Introduction

As time goes by, secrecy of messages for some people is very important in order to get data that is not at all other people know. Very sensitive secrecy about the illegal stealing of messages, triggering some people to convey the message's secrecy itself, in order to avoid threats from outsiders who want to forcibly take the contents of a message that some people think is very important.

Today, there are many applications about maintaining the confidentiality of the message itself. Maintaining the confidentiality of messages has been going on for a long time. People often call it steganography, which is hiding messages on the media, such as pictures. For now, steganography has been applied to the digital world such as computers. Steganography is generally use to hide information in the image, where the information in the form of text is inserted into the bits making up the image. With this method the author tries to combine the steganography method with other methods.

Cryptography itself is a science or art to maintain the security of a data. In the cryptographic world the same letter in the message has the same letter image as well. This has a high level of risk because it is easy to guess. To resolve this so the message must be encoded (encoding). The goal is to be safe from other people who want to take data contents illegally.

Hill cipher is one of the classic cryptographic methods that is often applied, hill ciphers apply simteric keys that utilize the nxn matrix as the key. The hill cipher algorithm is manipulating words that use matrix operations in the form of inverse multiplication.

Background retrieval regarding the hill cipher method and steganography itself is an application for safeguarding data that is wanted to be secured by an interested person. The hill cipher method itself is a classical cryptography or cryptography which uses the simteric key in its application, where this key is a matrix, which contains the key of the hill cipher method itself then the key that has been applied in the execution uses mod 26. This research also combines other methods namely lsb (significant bit list)



where this method implements insertion of the lowest in-bit message in a digital image, where the insertion is entered by the compiler bit of the message that you want to enter.

2. Research Methods

In carrying out research that is being carried out on the basic concepts of research from cryptographic plants, steganography, and also methods related to security. Here are some steps in conducting research.

2.1 Data Collection Method

2.1.1 Literature Study and Literature

At this stage the collection of information needed for data security systems is carried out in conducting security with the two methods. this information can be obtained from literature, books and the internet.

2.1.2 Discussion

In the form of consultation with supervisors and fellow students about problems that arise in writing.

2.2 Research Methodology

Methods used by the author is a descriptive research method which is research that provides an explanation of what is being studied so as to provide benefits from what is being studied. This research technique includes problem analysis, surveys, literature studies on the problems being studied. This research according to the author is very suitable to solve research related to the thesis. With the descriptive method, it is expected that the incoming information can be easily resolved by an efficient research.

3. Results And Discussion

3.1 The Application Of The Hill Cipher Method

Hill cipher operates using a matrix key that functions when the plaintext is executed with the nxn matrix key, which is where the hill cipher itself uses the word table which the author describes below.

The compilation of letters in the hill cipher method is as follows.

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T
20	21	22	23	24	25				
U	V	W	X	Y	Z				

Example of the calculation of encryption on a hill cipher as follows:

Determine the palaintext you want to enter. Here the author exemplifies DIPA as plaintext.

Where the numerical values of DIPA plaintext are:

$$D = 3$$

$$I = 8$$

$$P = 15$$

$$A = 0$$

And the key to the encryption matrix used is

$$\begin{bmatrix} 1 & 5 \\ 9 & 8 \end{bmatrix}$$

Enter the matrix key nx n first. And input the number from the table letters described above:

$$\begin{bmatrix} 1 & 5 \\ 9 & 8 \end{bmatrix} \begin{bmatrix} 3 \\ 8 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 * 3 + 5 * 8 \\ 9 * 3 + 8 * 8 \end{bmatrix}$$

Then it produces:

$$\begin{bmatrix} 3 + 40 \\ 27 + 64 \end{bmatrix} \Rightarrow \begin{bmatrix} 43 \\ 91 \end{bmatrix} \text{ mod } 26 \Rightarrow \begin{bmatrix} 17 \\ 13 \end{bmatrix}$$

And the result is:

$$\begin{bmatrix} 17 \\ 13 \end{bmatrix} \Rightarrow \begin{bmatrix} R \\ N \end{bmatrix}$$

and for the next addition is equal to the previous sum

$$\begin{bmatrix} 1 & 5 \\ 9 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 * 15 + 5 * 0 \\ 9 * 15 + 8 * 0 \end{bmatrix}$$

Then it produces

$$\begin{bmatrix} 15 + 0 \\ 135 + 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 15 \\ 135 \end{bmatrix} \text{ mod } 26 \Rightarrow \begin{bmatrix} 15 \\ 5 \end{bmatrix}$$

And is produced

$$\begin{bmatrix} 15 \\ 5 \end{bmatrix} \Rightarrow \begin{bmatrix} P \\ F \end{bmatrix}$$

Then the result of message encryption the hill cipher method is RNPF, where the calculation process has been explained in the previous step.

Next for the application of decryption is as follows:

Decryption itself is the opposite of encryption and the calculation is the same as counting on encryption, but what makes it different is the key of the decryption calculation is different from encryption key.

The decryption key uses:

$$\begin{bmatrix} 4 & 17 \\ 15 & 7 \end{bmatrix} \begin{bmatrix} 17 \\ 13 \end{bmatrix} \Rightarrow \begin{bmatrix} 4 * 17 + 17 * 13 \\ 15 * 17 + 7 * 13 \end{bmatrix}$$

Then it produces:

$$\begin{bmatrix} 68 + 221 \\ 255 + 91 \end{bmatrix} \Rightarrow \begin{bmatrix} 289 \\ 346 \end{bmatrix} \text{ mod } 26 \Rightarrow \begin{bmatrix} 3 \\ 8 \end{bmatrix}$$

And is produced:

$$\begin{bmatrix} 3 \\ 8 \end{bmatrix} \Rightarrow \begin{bmatrix} D \\ I \end{bmatrix}$$

And for the next addition equal to the sum previous:

$$\begin{bmatrix} 4 & 17 \\ 15 & 7 \end{bmatrix} \begin{bmatrix} 15 \\ 5 \end{bmatrix} \Rightarrow \begin{bmatrix} 4 * 15 + 17 * 5 \\ 15 * 15 + 7 * 5 \end{bmatrix}$$

And the result is:

$$\begin{bmatrix} 60+85 \\ 225+35 \end{bmatrix} \Rightarrow \begin{bmatrix} 145 \\ 260 \end{bmatrix} \pmod{26} \Rightarrow \begin{bmatrix} 15 \\ 0 \end{bmatrix}$$

And produced:

$$\begin{bmatrix} 15 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} P \\ A \end{bmatrix}$$

Then the result of decryption message on the hill cipher method back to DIPA, where the calculation process has been explained in the previous step.

3.2 Application of LSB + 1 Method

Least significant bit is one of the techniques in steganography to insert a message on each of the smallest bits in the arrangement of pixels in the image. The author develops this LSB method into LSB + 1 method where this method is almost the same as the previous method, which makes the difference is the location of the insertion message itself which is on the 7th bit or the second smallest bit.

Examples of the application of the LSB + 1 method are as follows:

Table 1. Plaintext = DIPA

NO	Character	Decimal	Binary
1	D	68	01000100
2	I	73	01001001
3	P	80	01010000
4	A	65	01000001

And the application of the LSB + 1 method uses RGB with binary value:
00100111 11101001 11001000

Table 2. The insertion of the message in RGB with the LSB + 1 method where the plaintext is DIPA:

Plaintext	Method LSB + 1	Embled insertion message
DIPA	01000001 001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0	001001 <u>0</u> 1 111010 <u>1</u> 1 110010 <u>0</u> 0 001001 <u>0</u> 1 111010 <u>0</u> 1 110010 <u>1</u> 0
D = 01000100	001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0 001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0	001001 <u>0</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0 001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0
I = 01001001	001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0 001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0	0 01001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>1</u> 0 001001 <u>0</u> 1 111010 <u>1</u> 1 110010 <u>0</u> 0
P = 01010000	001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0 001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0	001001 <u>0</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0 001001 <u>0</u> 1 111010 <u>1</u> 1 110010 <u>0</u> 0
A =	001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0 001001 <u>1</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0	001001 <u>0</u> 1 111010 <u>0</u> 1 110010 <u>0</u> 0 001001 <u>0</u> 1 111010 <u>1</u> 1 110010 <u>0</u> 0

3.3 Results Of The Research

3.3.1 Results Display

The following is a display of the results and discussion of the research on message insertion using the hill cipher method and LSB + 1. Users can be able to interpret the two methods that have been discussed.

3.3.2 Encryption and Stegno

In this display, user is asked to do encryption and stegno, for more details can be seen in Figure 1.

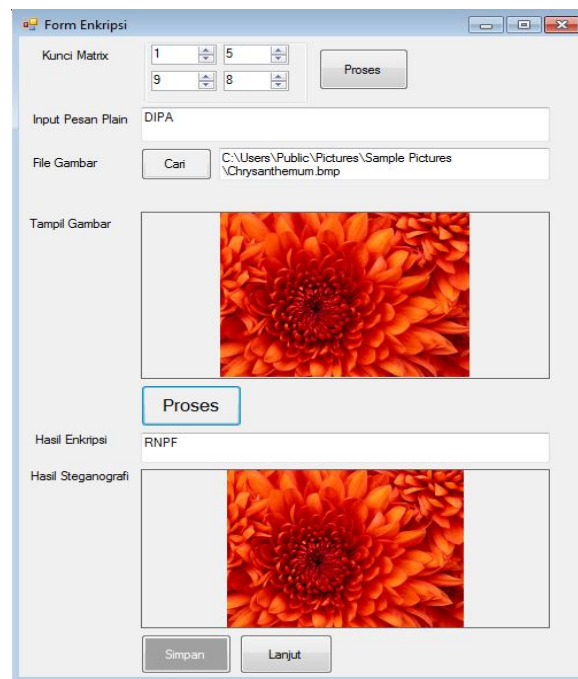


Figure 1. Encryption and Stegno Display

Display image 3 displays the components to stegno and encrypt the image and message.

3.3.3 Decryption

This display returns the data in its original form and displays hidden messages, for more details can be seen in Figure 2.

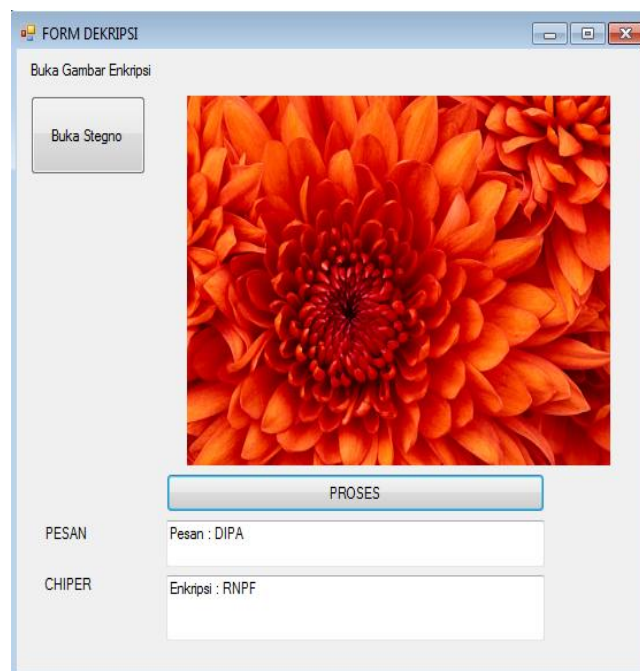


Figure2. Decryption Display

In Figure 4 displays information about data that is encrypted and text data hidden in the file.



3.4 Discussion

Results of data security system applications to provide convenience regarding security of stegano. In order for this data security system to run perfectly, there must first be a file image that you want to encrypt then run the application that the author designed.

3.4.1 Comparison of Results

Comparison of results before and after encrypted.

Table 3. Comparison of Results

No	Gambar	Ukuran Sebelum Enkripsi	Ukuran Setelah Enkripsi	Gambar Sebelum Enkripsi	Gambar Sesudah Enkripsi
1	crsanthe num.bmp	2,25 Mb	2,25 Mb		

4. Conclusions

Based on the results of the analysis carried out by the author about the message insertion security system using LSB + 1 method and hill cipher cryptography that has been built. From the overall results of the tests carried out, it can be concluded several things as follows.

1. The security system that is designed to secure confidential messages
2. The system can only execute image files with bitmap extension
3. This program is able to run confidentiality in securing messages properly
4. The system is designed to secure messages through image media

5. Suggestions

In the research conducted by the author, the method which is used very effectively in securing data that is done from the LSB + and hill cipher methods. But it does not rule out the possibility of the development of research conducted by this author to be deeper, as for the advice of the authors to develop this research to be more extensive, among others:

1. There needs to be development of this system in order to execute other files such as video, music.
2. It is hoped that further research can execute extracted files such as JPEG, PNG, GIF.
3. From the user aspect it is expected to create another form that supports the security of the text, such as the login form.

References

- [1]. AdiNugroho, 2013, *Software Engineering (software) Using UML and Java*, Publisher Andi, Yogyakarta.
- [2]. AndikSusilo, 2014, *Quick Technique Understanding Computer Security and the Internet*, Publisher: Elex Media Komputindo, Jakarta.
- [3]. Bambang P Putranto, 2013, *Protect Your Important Data with Powerful Software*, Publisher: PT Elex Media Komputindo, Jakarta.
- [4]. Hasrul, et al, 2016, *Application of Cryptographic Techniques in Databases Using One Time Pad Algorithm*, stmik-binamulia.ac.id
- [5]. InsapSantoso, 2014, *Human and Computer Interaction*, Publisher: Andi, Yogyakarta.

- [6]. Munawar, 2013, *Design-Algorithm-Security-Munawar*, [http://komputa.if.unikom.ac.id/s/data/journal/volume-01/komputa-1-1-designing algorithm ma-keamanan-munawar-2.pdf](http://komputa.if.unikom.ac.id/s/data/journal/volume-01/komputa-1-1-designing%20algorithm%20ma-keamanan-munawar-2.pdf)
- [7]. Prasetyo, Dwi, Didik, 2007, *Database Application Programming with Visual Basic .NET 2005 and MS Access*, Publisher Elex Media Komputindo, Jakarta.
- [8]. Teguh Budi Harjo, et al, 2016, *Application of Steganography Using LSB (Least Significant Bit) and Triple Dec Encryption Using C# Programming Language*, <http://journal.stmikglobal.ac.id>
- [9]. Wahana, Komputer, 2007, *The Best Encryption Tools*, Publisher Elex Media Komputindo, Jakarta.
- [10]. YudhiAndrian, 2016, *Message Size Effect Analysis on the Quality of Image Results Steganography LSBmethod*, ejournals.umn.ac.id
- [11]. Yoevestian, Whindy 2008, *Zero Knowledge*, Publisher Elex Media Komputindo, Jakarta