

Application of Text Message Held in Image Using Combination of Least Significant Bit Method and One Time Pad

Eferoni Ndruru*¹, Taronisokhi Zebua²

^{1,2}STMIK BUDI DARMA; Medan, Indonesia

e-mail: *¹ronindruru@gmail.com, ²taronizeb@gmail.com

Abstrak

Stenografi dan keamanan merupakan salah satu teknik untuk mengembangkan seni dalam mengamankan data. Stenografi memiliki aspek yang paling penting adalah tingkat keamanan dalam persembunyian data, yang membuat pihak ketiga tidak dapat mendeteksi beberapa informasi yang telah diamankan. Biasanya digunakan untuk menyembunyikan informasi teks. Algoritma (LSB) adalah salah satu algoritma dasar yang diajukan oleh Arawak dan Giant pada tahun 1994 untuk menentukan kumpulan item yang sering digunakan untuk aturan asosiasi Boolean. Algoritma pastoral mencakup jenis aturan asosiasi dalam data mining. Aturan yang menyatakan asosiasi antara atribut sering disebut analisis afinitas atau analisis keranjang pasar. OTP bisa banyak digunakan dalam bisnis. Dengan pengetahuan tentang pesan teks, teknik penyembunyian akan memudahkan perusahaan mengetahui jumlah frekuensi data penjualan, sehingga memudahkan perusahaan melakukan tindakan transaksi yang sesuai. Hasil penelitian ini, sembunyikan pesan teks pada gambar (image) dengan menggunakan kombinasi metode LSB dan Otp

Kata kunci— Kriptografi, steganografi, algoritma LSB dan OTP

Abstract

Stenography and security are one of the techniques to develop art in securing data. Stenography has the most important aspect is the level of security in data hiding, which makes the third party unable to detect some information that has been secured. Usually used to hide text information. The (LSB) algorithm is one of the basic algorithms proposed by Arawak and Giant in 1994 to determine the frequent item set for Boolean association rules. A priory algorithm includes the type of association rules in data mining. The rule that states associations between attributes are often called affinity analysis or market basket analysis. OTP can be widely used in business. With the knowledge of text message, concealment techniques will make it easier for companies to know the number of frequencies of sales data, making it easier for companies to take an appropriate transaction action. The results of this study, hide the text message on the image (image) by using a combination of LSB and Otp methods.

Keywords— Cryptography, steganography, LSB and OTP algorithms

1. INTRODUCTION

With the availability of internet network, it is possible to make the process of data and information exchange. In the exchange of information, the security aspect plays an important role, especially if the information is confidential. To maintain the confidentiality of information can be used techniques steganography. Information to be sent is hidden in a digital file (text, image, audio, video). Then the digital data is sent as ordinary data, so the third party is not suspicious that in it there is confidential information. Information that is hidden in the digital data can be extracted back by the recipient of the message. The information should also be the same as the information before it is inserted in the digital data, even though the digital data has undergone manipulation processes, such as editing, cutting or compression.

Based on some previous research that I cited to support in raising the title of the cipher, about the method of LSB and OTP with the author of "Emmy Paulina be. wake up "," Entitled Analysis of Chaos Effect on Image Decryption Encryption with One Time Pad Method ", author," Jhoni Verlando Purba "entitled" Implementation of Text Message Steganography Into Sound Files (.Wav) By Byte Modification Distance On Least Significant Bit Algorithm (Lsb), Author of "Ali Mahmudi" Cryptography and Steganography Application Using Least Significant Bit (LSB) and One Time Pad (OTP) Method "Writer" Maya Sintia "security techniques for data varies on picture mri using lsb and otp method" author "Risqo Maulana "entitled" Implementation of message insertion on digital imagery using least bit bit (lsb) and one time pad encryption "and author" Arie Eko Tinikar "entitled" One Time Pad CTP Modification (OTP) Using Dynamic Padding in Data File Security " .

Steganography as an act of concealment of messages into other messages that have existed since before Christ and now along with the advancement of network technology and the development of digital technology, steganography is widely used to send messages over the Internet network without anyone else know by using digital media in the form of image files.

MethodLeast Significant Bit (LSB) is a message concealment technique by inserting messages on the lower bit or the rightmost bit of the cover work file as a medium to hide messages. In this trial used digital image media true color 24 bit with RGB color model. In digital images, there will be 3 bits that can be inserted in 1 pixel. This is because in 1 pixel the color is composed of 3 color components, namely Red, Green, and Blue which are each composed by 8 digit binary numbers from the range of values 0 to 255 in decimal or 00000000 to 11111111 in representing binary.

This research will implement One Time Pad (OTP) algorithm to encode data and information stored. Data or information stored in the application will form ciphertext so that the user gets the key to access the data or information. One Time Pad (OTP) where this algorithm uses the same unlikely in the encryption process as well as the description. This algorithm will require the sender and the receiver to agree on a certain key prior to communication between the two parties. The encryption scheme to be constructed in this research applies techniques to modern cryptography, where secrecy lies in the key of One Time Pad (OTP) keygen. Until now cryptography cannot be solved

2. METHODS

2.1 Problem Analysis

In this study, we analyzed the problems of securing text messages from third parties and for irresponsible orgs using cryptographic and steganographic techniques using a combination of LSB and OTP methods by concealing text messages on images using the LSB and OTP methods. The following is the design of the problem-solving diagram. Can be seen in the following figure1:

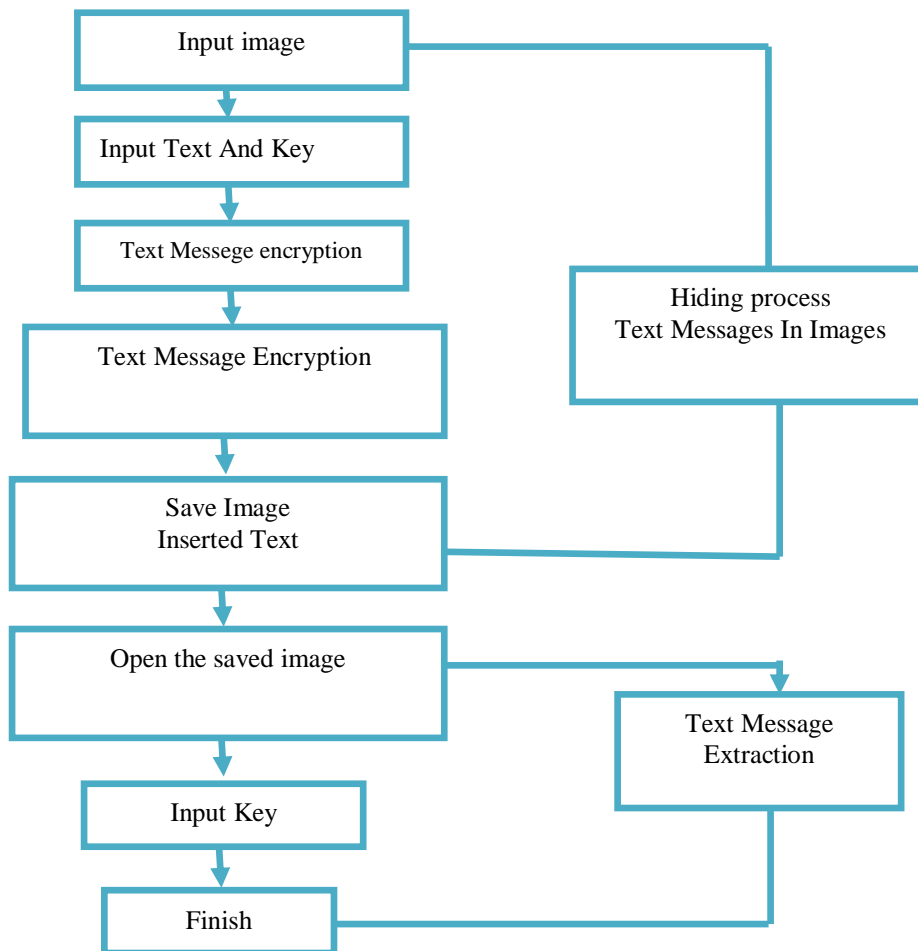


Figure 1 Message Concealment Diagram

In the first stage of the preparation of images/images that will dibleakan text messages in it, by using the technique steganogram. After that, the text that will be inserted in the image or image, first done cryptographic technique that is by inputting text message (plaintext) and then encrypted so that text message (plaintext) turn into ciphertext (scratch text) after it done decryption by returning message to the original message or original message. Here's the table 1. Here is a simple change bit values from pike (1,1) to (1.20).

Table 1 Value Conversions and Embedded

| Original Value | Original Value | Bit Original | Bit LSB | LSB value |
|----------------|----------------|--------------|----------|-----------|
| (1,1) | 193 | 11000001 | 11000000 | 192 |
| (2,1) | 198 | 11000110 | 11000111 | 199 |
| (3,1) | 195 | 11000011 | 11000010 | 194 |
| (4,1) | 195 | 11000011 | 11000010 | 194 |
| (5,1) | 200 | 11001000 | 11001001 | 201 |
| (6,1) | 201 | 11001001 | 11001000 | 200 |
| (7,1) | 199 | 11000111 | 11000111 | 199 |
| (8,1) | 202 | 11001010 | 11001010 | 202 |
| (9,1) | 197 | 11000101 | 11000100 | 196 |
| (10,1) | 198 | 11000110 | 11000111 | 199 |
| (11,1) | 196 | 11000100 | 11000100 | 196 |
| (12,1) | 192 | 11000000 | 11000001 | 193 |
| (13,1) | 192 | 11000000 | 11000000 | 192 |
| (14,1) | 193 | 11000001 | 11000000 | 192 |
| (15,1) | 190 | 10111110 | 10111111 | 191 |
| (16,1) | 186 | 10111010 | 10111010 | 186 |
| (17,1) | 198 | 11000110 | 11000110 | 198 |
| (18,1) | 184 | 10111000 | 10111001 | 185 |
| (19,1) | 182 | 10110110 | 10110110 | 182 |
| (20,1) | 179 | 10110011 | 10110011 | 179 |

2. 2.1 One-time pad formula (OTP)

$C = \text{Enc}(K, P) = P \oplus K$, dimana “ \oplus ” adalah lambang XOR.

$P = \text{Dec}(K, C) = C \oplus K = ((P \oplus K) \oplus K) = (P \oplus (K \oplus K)) = P$

Operasi XOR :

$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0 \dots\dots\dots(1)$

Least Significant Bit(LSB)

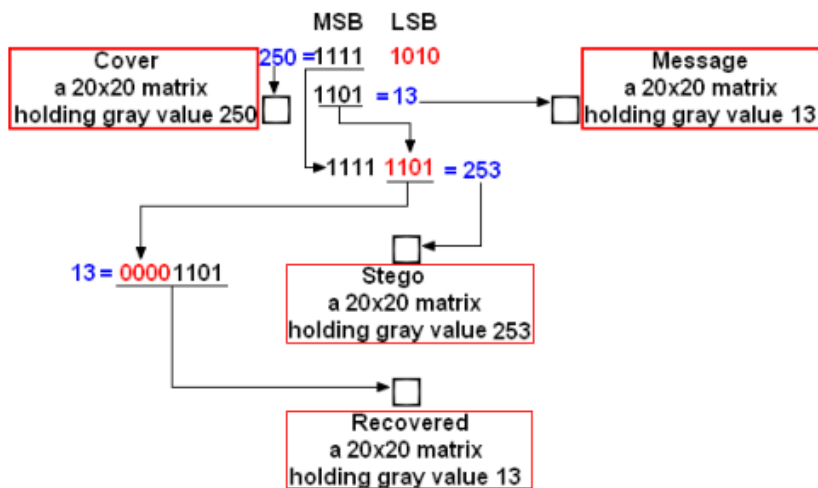


Figure 2 LSB Mechanism

2. 2.2 References Library

Steganography has two functions that hide data/information in the form of text and insert in the image, sound, and text moves. messages that will be hidden in the form of images and text. By using Steganography Techniques to gain an advantage that is in sending text

messages cannot be known by a third party that the message is in the process of delivery and make the third party did not realize it. Behind it also there is also a weakness that is to hide the message bits require a lot of space [5].

technique produces perfect security. Messages that are encrypted even though the form is random and can not be read clearly but still raises the suspicion that the random text contains an important information, it required the incorporation of cryptographic techniques [6]

There are some techniques in steganography that is Most Significant Bit (MSB) is inserting the message bit to the most meaningful bit, for example in bit 11010010 the underlined number is a meaningful bit, the bit has a large value so that the change in MSB bit value will be large provides an effect of discoloration on an invisible distinguishable image. [8] One-time pad (OTP) is one of the message encryption techniques that a pad is used only once (one time) to encrypt messages. Once the key is used when the key is destroyed so that the OTP.

The advantage of using steganography is to allow the sending of messages in secret without knowing that a message is being sent. This makes the third party unaware of the existence of the message. Steganography also has a weakness that requires a lot of space to be able to hide some message bits. However, these weaknesses can be gradually overcome along with the development of techniques in steganography. The Image File on the computer is an array of numbers representing the value of the varying intensity of light (pixels). Collection of pixels that form an image. Commonly used images are 24 bit images and 8 bit images (256 colors), can be seen in the following table :

Table 2 Table bit value

| Number of Bits | Information |
|----------------|-----------------------------|
| 1 | binary-valued image (0 - 1) |
| 8 | gray level (0 - 255) |
| 16 | high color (216) |
| 24 | 224 true color |
| 32 | true color (232) |

For example: there is a 100 pixels x 100 pixels image with 24 bits color encoding with R = 8 bits, G = 8 bits, B = 8 bits per pixel, then the color encoding will be able to represent 0 .. 16.777.215 (representing 16 million colors), and the required disk space = $100 * 100 * 3$ bytes (because RGB) = 30,000 bytes = 30 KB or $100 * 100 * 24$ bits = 240000 bits.

One time pad is a perfect secrecy password that produces a password text that has no statistical relation to the original text so statistical analysis of the original text so statistical analysis can not be performed.

Lock Passwords On One Time Pad are generated randomly and lock rows are used only once.

Encryption Process = $E () = + \text{Mod } 26$

Decryption Process = $D () = + \text{Mod } 26$

An example of a SUN word will be encrypted using a One Time Pad Password with a key using LCM (linear congruent method) where

$a = 1, = 0, C = 2$ and $M = 100$

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Least Significant Bit Method (LSB)

The LSB method is the simplest and easiest method of steganography to implement. This method uses digital images as cover text. In the order of bits in a byte (1byte = 8 bits), there are the most significant bits (MSB) and least significant bits

(LSBs). For example byte 11010010, the bit number 1 (first, underlined> is the MSB bit, and the bit number 0 (last, underlined) is the LSB bit. The suitable bit to replace is the LSB bit because the change only changes the byte value one higher or one lower than the previous value. Suppose the bytes are red, the change of one LSB bit does not change the red color significantly. The human eye can not distinguish the small change. Suppose the image/image pixel segments before adding bits are:

```
00110011 10100010 11100010 10101011 00100110 10010110 11001001
11111001 10001000 10100011
```

3. RESULTS AND DISCUSSION

Results and discussion in this research is the insertion of text messages on digital images using a combination of LSB and OTP methods. an image file in use that The type of image file type to be tested is 30 * BMP file, BMP is bitmap formed from the set of line/pixel. Picture quality depends on pixels. If the enlarged image will break. The file to be tested consists of 5 * BMP files with 512 x 512-pixel resolution, 5 files with 256 x 256 pixels and 5 files with 128 x 128 pixels resolution. All image files will be processed steganography that is using LSB method after that used OTP method for key, but before process of text insertion done, previously must have done encryption process that is randomness of message so message inserted is no longer original message but random message which no meaning to the level of security will increase more aka. The following is the index table for message encryption. For more details can be seen in the following table.

Table 3 The Karankter Index

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

Table 4 The Karankter Index

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| K | L | M | N | O | P | Q | R |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

Table 5 The Karankter Index

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| S | T | U | V | W | X | Y | Z |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

By using the formula one-time encryption pad $pi = (ci - ki) \bmod 26$ then

In this research message data consists of 25 characters ie plaintext = "Eferoni" to perform the encryption process requires key = "ndruruu $E + N (4 + 13) = 17 = R$

$$F + D (5 + 3) = 8 = I$$

$$E + R (4 + 17) = 21 = V$$

$$R + U (17 + 20) = 37 = L$$

$$O + R (14 + 17) = 31 = F$$

$$N + U (13 + 20) = 33 = H$$

$$I + U (8 + 20) = 28 = C$$

Here use the alphabet calculation process and for the program using Ascii table. So, the Chipertext is R, I, V, L, V, H, C then the ciphertext is hidden into the image by using LSB method, following insertion steps in the picture:

1. The user enters the digital image to be inserted with the message.
2. The user enters the default character of the user to be used to perform the encoding and decoding process of the character sequence.
3. The user will enter a message to be inserted in the digital image.

4. The encoding process of the messages entered by the user using the default character of the user. Namely the process of representing a message in the form of text or sequence of characters into a series of numbers.
5. Convert the result of representation of message encoding number into a binary number.
6. Arrange all messages that have been converted into binary into the one-bit package.
7. Insert each bit of the bit package that has been created in the digital image, until the last bit sequence
8. Save the new image that has been inserted with the message of each intensity.
9. Steganographic image that has been inserted message

Message Scrambling Process

Examples of secret messages: EFERONI, public key (e, N): 79, 3337

a. EFERONI plaintext conversion in ASCII encoding:

69,70,69,82,79,78,73

b. Break X into a smaller block, such as X split into five 3-digit blocks:

x1 = 656 x4 = 693x2 = 682 x5 = 787

x3 = 863

a. The plaintext blocks are encrypted as follows:

$$65679 \text{ mod } 3337 = 215 = y1$$

$$68279 \text{ mod } 3337 = 776 = y2$$

$$86379 \text{ mod } 3337 = 1743 = y3$$

$$693 \ 79 \text{ mod } 3337 = 933 = y4$$

$$78779 \text{ mod } 3337 = 1731 = y5$$

b. Thus, the resulting ciphertext is 215 776 1743 933 1731 158.

c. The secret message is then inserted into the image using the LSB method

Message Insertion

Example of conversion of pixel value:

Table 6 Image Value (RGB)


| | | | |
|---|-------------|-------------|-------------|
|  | 182,211,229 | 182,211,229 | 182,211,229 |
| | 182,211,229 | 182,212,230 | 182,211,229 |
| | 182,211,229 | 182,211,225 | 182,211,229 |

Table 7 Convert To binary

| | | |
|----------------------------|----------------------------|----------------------------|
| 10110110,11010011,11100101 | 10110110,11010011,11100101 | 10110110,11010011,11100101 |
| 10110110,11010011,11100101 | 10110111,11010100,11100110 | 10110100,11010011,11100101 |
| 10110110,11010011,11100101 | 10110110,11010011,11100001 | 10110100,11010011,11100101 |

↓ Proses penggantian bit terakhir dengan pesan

| | | |
|----------------------------|----------------------------|----------------------------|
| 10110111,11010010,11100101 | 10110110,11010011,11100101 | 10110111,11010010,11100101 |
| 10110110,11010011,11100100 | 10110111,11010100,11100111 | 10110100,11010011,11100101 |
| 10110111,11010010,11100101 | 10110110,11010010,11100000 | 10110100,11010010,11100101 |

Steganalysis refers to art and science in detecting the presence or absence of hidden messages in an object [KHA06]. Steganalysis for LSB method consists of a subjective method and statistical method [WEN00]. The subjective method involves the sense of human vision to observe the part of the suspect image, so it is also called the visual attack. One technique of visual stegan

alysis is the enhanced LSB method. This method displays the last bits of an image and relies on human vision to determine whether there is a secret message in the image. While the statistical method involves a mathematical analysis of an image to find the difference between the original image and the message the message was inserted. Although the stego-image is identical to its cover-image when captured by the sense of sight, the stego-image often shows unusual statistics that distinguish the stegoimage from its cover-image. The purpose of statistical steganalysis to show this unfamiliarity is to show a strong difference between the stegoimage and its cover-image.

The statistical methods that will be discussed are chi-square test method and RS-analysis method. The chi-square test proved to be reliable in detecting secret messages inserted sequentially. Another method is RS-analysis that proves reliable and accurate in detecting secret messages that are inserted randomly. then the following results are obtained:

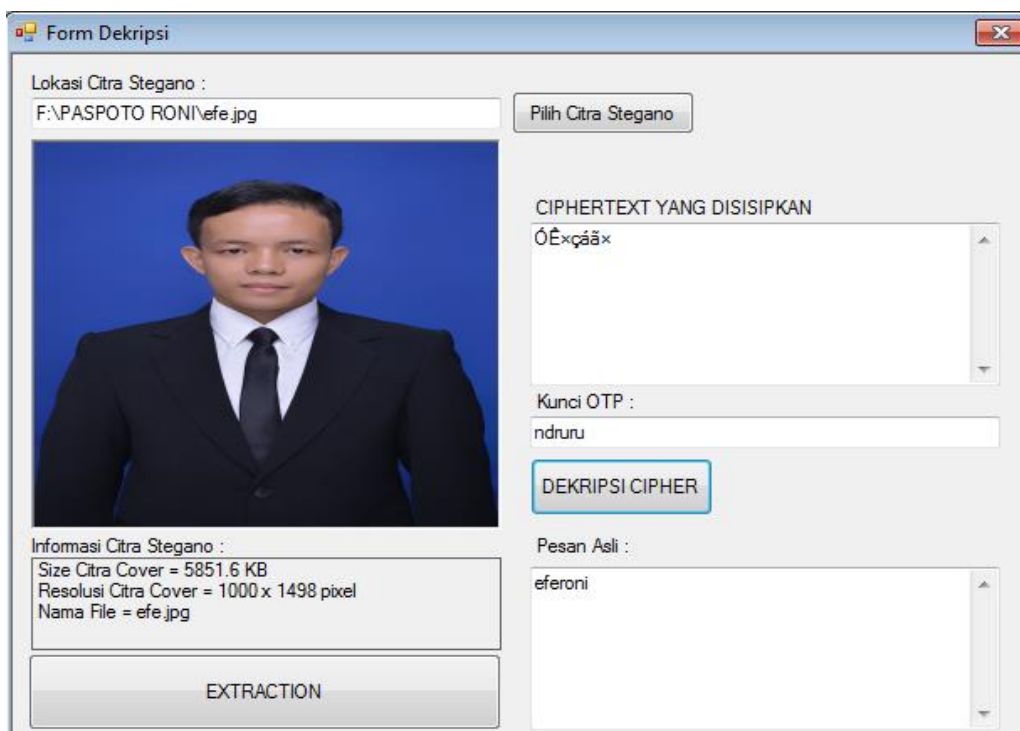




Figure 3 results from extraction

The following is the end result of the insertion process

| No | Plainteks | KEY | Chiperteks | Image Result |
|----|------------|--------|------------|--|
| 1 | EFERONI | NDRURU | “Š—§;£ž |  |
| | Chiperteks | KEY | plainteks | Image Result |
| 1 | “Š—§;£ž | NDRURU | EFERONI |  |

4. CONCLUSIONS

Based on the results of research that the authors do with the theme of steganography, by taking the title of this steganography application, is expected to be used to help internet users in exchanging messages with a better level of security.

With this steganography application can protect transactions of message delivery between two parties who exchange messages. This application can disguise the message, because the invisible message will not be seen, and seen as a regular image.

In this Internet era, the transactions are very advanced messaging, whether through electronic messaging (email), social networking (Facebook, Twitter, Google+, etc.), forums, etc. The weakness of the message transaction process in these media is the confidentiality, which when the message is sent to the destination then the message will clearly be a message, and vulnerable to attack at any time. With this steganographic application, messages are inserted into the image media, and the invisible message will not be visible, so message delivery will be safer.

REFERENCES

- [1] Dian Hafidh Zulfikar, Agus Harjoko “Perbandingan Kapasitas Pesan pada Steganografi DCT Sekuensial dan Steganografi DCT F5 dengan Penerapan Point Operation Image Enhancement” IJEIS (Indonesian J. Electron. Instrum. Syst., Vol 7, No 1, pp. 35-46, januari, 2016, [online]. Available : <https://jurnal.ugm.ac.id/ijccs/article/view/11187> [Accessed: 20-Januari-2016]
- [2] Devid Haryalesmana Wahid, Azhari SN “Peringkasan Sentimen Esktraktif di Twitter Menggunakan Hybrid TF-IDF dan Cosine Similarity” IJEIS (Indonesian J. Electron. Instrum. Syst., Vol 10, No 2, july 2016, pp.207-218 [online]. Available : <https://jurnal.ugm.ac.id/ijccs/article/view/16625>, [Accessed: 20-July-2016]
- [3] Eferoni Ndruru, Fince Tinus Waruwu, Anda Yanny “alokasi pekerja pada suatu proyek dengan metode hungarian (studi kasus: pt. ira widya utama medan)” ejurnal,

- Vol 1, No 1 ,20 Oktober 2017, Available <http://ejurnal.stmik-budidarma.ac.id/index.php/komik/article/view/500>. [Accessed: 15-Oktober-2017]
- [4] Taronisokhi Zebua, Eferoni Ndruru, "Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma Rc4", *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIK)*, Vol. 4, No. 4, Desember 2017, hlm. 275-282, [online], available: <http://jtiik.ub.ac.id/index.php/jtiik/article/view/474>, [Accessed 10-Desember-2017]
- [5] ZEBUA, T. 2015. Penerapan Metode LSB-2 untuk Menyembunyikan Ciphertext pada Citra Digital. *Pelita Inform. Budi Darma*, vol. 10, no. 3, pp. 135–140. [online] Available : <https://www.researchgate.net/publication/318420491>, [Accessed 20 januari 2017]
- [6] Mahmuddin Yunus, Agus Harjoko, "Penyembunyian Data Pada File Video Menggunakan Metode Lsb Dan Dct," *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)* Vol 8, No 1 januari 2014) [online] Available: <https://jurnal.ugm.ac.id/ijccs/article/view/3498>. [accessed 8 januari 2014]
- [7] *Dian Hafidh Zulfikar, Agus Harjoko* , "Perbandingan Kapasitas Pesan pada Steganografi DCT Sekuensial dan Steganografi DCT F5 dengan Penerapan Point Operation Image Enhancement", *IJCCS (Indonesian Journal of Computing and Cybernetics Systems/view*’, Vol 8, No 1 maret (2016) [online]: Available <https://jurnal.ugm.ac.id/ijccs/article/view/11187>, [accessed 9 maret 2016].
- [8] Manik, "Klasifikasi Belimbing Menggunakan Naïve Bayes Berdasarkan Fitur Warna RGB" (*Indonesia Journal of computing and cybernetics System*), [online] Vol 11 No. 1, 13 mei, 2017, [online], Available [:https://jurnal.ugm.ac.id/ijccs/article/view/1783](https://jurnal.ugm.ac.id/ijccs/article/view/1783), accessed [16 mei 2017]
- [9] P. Biaya, P. Barang, P. Cv, E. Nias, and S. A. Hutabarat, "Implementasi Metode Vogel ' s Approximation Method Pada," vol. 3, no. 1, pp. 12–15, 2018.
- [10] T. Zebua, R. K. Hondro, and E. Ndruru, "Message Security on Chat App based on Massey Omura Algorithm," *Int. J. Inf. Syst. Technol.*, vol. 1, no. 2, pp. 16–23, 2018.
- [11] F. T. Waruwu, E. Buulolo, E. Ndruru, K. Kunci, A. Apriori, and R. Penyakit, "KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer) IMPLEMENTASI ALGORITMA APRIORI PADA ANALISA POLA DATA PENYAKIT MANUSIA YANG DISEBABKAN OLEH ROKOK."
- [12] E. Andreas, "Aplikasi Kriptografi File DOC, DOCX, JPG dan PDF dengan Metode AES dan Kompresi Huffman," *Kriptografi AES Dengan Kompresi Huffman*, p. 8, 2014.
- [13] "Algoritma Kriptografi Aes Rijbdael," *TESLA J. Tek. Elektro UNTAR*, vol. 8, no. 2, pp. 97–101, 2006.