COMBINATION CONCEPT OF LSB AND PLAYFAIR CIPHER FOR OPTIMIZING DATA SECURITY

Moch. Sjamsul Hidajat[1], Ery Mintorini[2]

[1]Information Engineering, Faculty of Computer Science, Dian Nuswantoro University PSDKU Kediri, Indonesia
[2]Visual Communication Design, Faculty of Computer Science, Dian Nuswantoro University PSDKU Kediri, Indonesia
[1]moch.sjamsul.hidajat@dsn.dinus.ac.id, [2] ery.mintorini@dsn.dinus.ac.id

Abstract

Data security is now something that is very necessary, with the aim of ensuring that important data and information does not fall into the hands of unauthorized people. The widespread data exchange process provides opportunities for unauthorized parties to take, copy or steal the exchanged data. This is what triggers the importance of securing data when exchange occurs. In the field of computer science, there are many ways that data can be secured. These methods include the concepts of steganography and cryptography. Steganography is a way to hide data in various media, while cryptography is a way to encode data into a form that has no meaning. This research aims to design a system to secure messages in the form of text data using the Playfair cipher cryptography method and Least Significant Bit (LSB) steganography using image media and the image containing the message is not visible to the eye that the image contains a secret message.

Keywords: LSB, cryptography, playfair cipher, steganography.

1. Introduction

Data security is very important, especially in today's times where many social activities involve data exchange in almost all aspects of life. Data exchange activities provide opportunities for parties who have no interest in the data to intercept, take by force or steal information. This ultimately results in a lot of misuse of data and other losses, so that now many efforts are being made to prevent data from being leaked or falling into the hands of parties who do not have the rights to the data.

One way to overcome data security problems is to use cryptography. Cryptography is said to be an art and science that is used to protect transmitted data by converting it into a certain code (Pabokory, 2015). According to Suhardi (2016), cryptography is the science of secret writing where aspects of communication and data can be changed into certain codes so that other people cannot know the contents by applying certain algorithms. In the field of information technology, there are many techniques in cryptography, including the playfair cipher technique.

According to (Sumarsono, 2019), the playfair cipher encryption technique is a form of digraph cipher. Encryption and decryption procedures are carried out for every two letters that have a pair (bigram). The shape of this playfair cipher is a 5x5 square matrix that can accommodate 25 capital letters. For all letters except the letter J are placed in the matrix table. The letter J is considered to be similar to the letter I, because the letter J has the lowest frequency of occurrence. The key used is a word that cannot contain repeated letters. The key is entered into a 5×5 matrix table, the first entry is the key. Next, the next letters are written sequentially starting from the first line. Apart from using this cryptographic technique, so that data and information are better protected, it can be combined with techniques for hiding the message in various media. This term is widely known as steganography.

Steganography is the art of secret communication where the message created is hidden in an object that seems harmless. The existence of steganographic messages is secret. Steganography is a form of hidden communication, which literally means "closed writing." Another term for steganography is Hidden in Plain Sight, which means hidden in plain sight. (Syawal, 2016). In steganography there are several types of techniques, some of which are Least Significant Bit (LSB) and End of File (EOF). Least Significant Bit is an applied algorithm of the substitution method. Substitution is a method where normal data is replaced with secret data. This technique does not change the size of the original data much, but depends on the media file and the data to be hidden. Each message bit replaces the very last bit of the original data. The size of the number of hidden messages depends on the size of the container image, whereas The EOF method is a method that works by adding secret data or messages at the end of the file. This technique can be used to add data whose size suits your needs. A rough calculation of the size of the file into which the data has been inserted is the same as the size of the file before it was inserted, the data plus the size of the secret data that has been converted into file encoding. In this research, the LSB steganography technique was used. The Least Signification Bit (LSB) method is a fairly simple steganography method. Apart from being simple, in LSB the insertion and extraction process is also relatively fast. The LSB method inserts a message into the cover image in bits that have less meaning (Apriyani, 2016). LSB is a message hiding technique at the lowest bit location in a digital image. The secret message will be converted into binary form and hidden in a concealment medium which is usually a digital image. The results of hiding messages using the LSB method do not cause any striking changes so it does not seem suspicious.

Several previous studies that discussed the topic of applying LSB steganography and playfair cipher cryptography include: Simbolon (2016) in a research journal entitled Securing Student Grade Transcripts Using Playfair Cipher Cryptography and Steganography with the Least Significant Bit (LSB) Technique. In the journal it is explained that the playfair cipher works by encrypting pairs of letters. The application of ASCII code will also make the encryption results more difficult for unauthorized parties to understand. By implementing a combination of cryptography and steganography in securing student transcript data, it is certain that other people will not know it because it will not contain suspicion.

Then research was conducted by Sitorus (2015) in a journal entitled Steganography Technique Using the Least Significant Bit (LSB) Method. This research explains that the LSB method is a method that is simple and easy to apply to systems that require inserting data into images. By using the technique of hiding data in images, it can be a medium for securing the data that will be sent. Confidential data in the form of text can be inserted into images with a key that is created and understood by the application user.

Furthermore, Murdowo (2020) in a research journal entitled Calculation Manual Using Classic Cryptography Playfair Cipher explains that the Playfair cipher algorithm which uses long keywords in the form of a 6X6 matrix is able to produce encryption on one plaintext sentence that is long enough to become a ciphertext that is quite accurate and quite confusing for recipient of the message before the message is described.

The research journal with the title implementation of steganography LSB Method Using the PHP Program for Image Message Security written by Wiyata (2016) explains that the LSB method can hide messages that are difficult to decipher. Digital images inserted using the LSB method coupled with encryption will be increasingly difficult for unauthorized people to crack.

Laoli (2020) who wrote a research journal entitled Application of Hill Cipher and Least Significant Bit (LSB) for Securing Messages in Digital Images, explains the analysis, design and implementation of message security applications in digital images by combining the Least Significant Bit (LSB) and Hill cipher algorithm, produces the process of securing messages in digital images safely and is not known to the naked eye, because the size of the bitmap resulting from steganography does not appear to change significantly after the process of inserting binary text into the binary bitmap using the least significant bit (LSB) method.

Based on several previous studies, this research aims to design and implement a system to secure text data with a combination of LSB steganography and Playfair cipher cryptography. The results of the implementation show that message data can be encrypted well and can be returned to its original form well too. Message data inserted into the image media does not change the appearance of the image so that the presence of the message in the image media cannot be detected by the human eye.

2. Method

2.1 Research Flow

The research flow is the steps carried out by the researcher from the initial stage to the final stage of research implementation. The research stages are shown as in Figure 1.

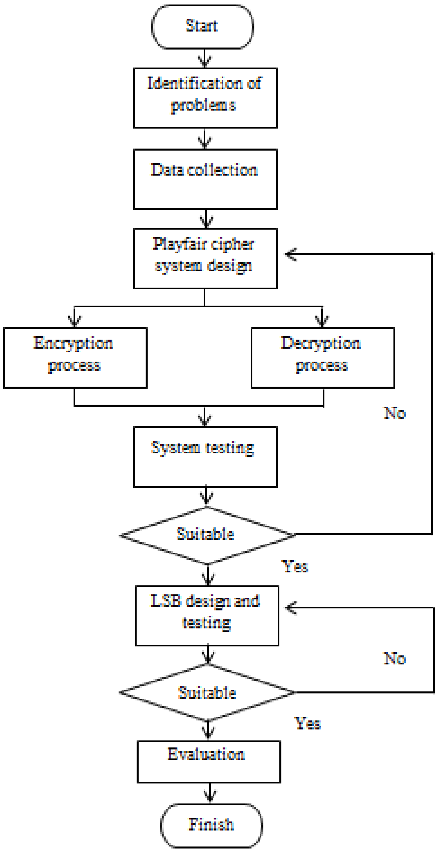


Figure 1. Research flow

2.2 Cryptography

Cryptography is divided into two syllables, namely crypto and graphia, where crypto means hiding, while graphia means writing. From the meaning of these two syllables, cryptography is said to be a science that studies mathematical techniques related to information security, such as data confidentiality, data validity, data integrity, and data authentication (Amin, 2016). According to Maulana (2012), cryptography can also be interpreted as a technique for maintaining message security. When a message is sent from one place to another, the message can be taken by someone who is not responsible so that in order to protect the message, the contents of the message can be encoded using a code that cannot be understood by other parties.

In cryptography there are several terms, including (Febriana, 2017) :

1. **Message.** Both plaintext and cipher text. Messages are information that can be read and understood. while the message that has been encoded is called ciphertext**.**
2. **Sender and Receiver.** In this data communication process there are two parties involved, namely the sender (sender) is the party who sends the message to another party, while the recipient (receiver) is the party who receives the message.
3. **Tapper.** This is a person who tries to catch the message while it is being sent.
4. **Cryptoanalysis and Cryptology.** Cryptoanalysis is the science and art of breaking ciphertext into plaintext without knowing the key used. People who can do this are known as cryptanalysts, while cryptology is the science of cryptography and cryptanalysis.
5. **Encryption and Decryption.** Encryption is the process of encoding plaintext into ciphertext, while decryption is the process of returning ciphertext to its original plaintext.
6. **Ciphers and keys.** Ciphers are rules for encrypting and decrypting, or mathematical functions used for encryption and decryption. Keys are parameters used for enciphering and decrypting transformations. The key is usually a string or series of numbers.

In general, the flow of the message encryption and decryption process is shown as in Figure 2.

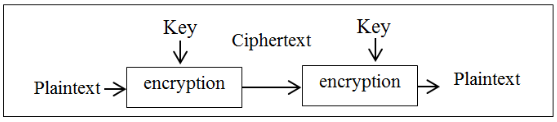


Figure 2. Flow of the encryption and decryption process

2.3 Playfair Cipher

Playfair cipher is a classic encryption method that is complicated to complete manually with the cipher table used to carry out encryption and decryption having the form of a matrix measuring (5x5) containing capital letters from A-Z with the letter J removed (Perdana, 2021). The encryption process in the playfair cipher algorithm runs every 2 letters. This is because the playfair cipher is included in the Digraph Cipher. Key letters are entered into a table measuring 5x19 and these letters cannot be entered more than once, followed by other letters that have not been entered sequentially (Sancaka, 2022).

According to Munir (2019), the Playfair cipher is included in the polygram cipher which performs bigram substitution (groups consisting of two letters). This cipher encrypts pairs of letters (bigrams or digraphs) into pairs of letters, not single letters like in other classical ciphers. Its function is to make frequency analysis very difficult because the frequency of occurrence of letters in the ciphertext becomes flat. The cryptographic key is 25 letters arranged in a 5x5 square by removing the letter J from the alphabet (in some versions, the letter Q is omitted, while in other versions the letters J and I are written in one place as I/J).

The purpose of this playfair cipher is to make frequency analysis very difficult because the frequency of appearance of characters in the encoded text becomes flat (Setyaningsih, 2015).

2.4 Steganography

Steganography is the art of hiding hidden information or messages (embedded messages) in a container (cover object) which can be in the form of text, images, audio, video and others (Yanti, 2023). According to Nugroho (2022), steganography is a technique that aims to hide secret messages or secret texts so that the information in them cannot be identified by other people (third parties) so that only the sender and recipient can know the message. Steganography is a type of hidden communication, which literally means "covered writing." The message is open, always visible, but it is not detected that there is a secret message. Another popular description for steganography is Hidden in Plain Sight, which means hidden in plain sight (Syawal, 2016).

Steganography has three main criteria, namely: 1. Imperceptibility, meaning it cannot be perceived by the five senses. 2. Fidelity, meaning that the quality of the file after being inserted is not much different from the original file and 3. Recovery, meaning that the file can be returned to its original form. (Nurmaesah, 2017).

The initial aim of this steganography technique is to secure messages in a medium, so that other people are unable to detect that the medium contains a secret message. This steganography technique is usually created and implemented via digital media.

According to Dwiyanto (2020), steganography has many methods including: Least Significant Bit (LSB), Most Significant Bit (MSB), End of File

(EOF) method, Spread Spectrum, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Bit-Plane Complexity Segmentation (BPCS). Each method has advantages and disadvantages, so no method is perfect and its use depends on needs.

2.5 Least Significant Bit (LSB)

LSB (Least Significant Bit) is one of the many stegnography methods that is considered the simplest and easiest to implement in an application. This method uses digital images as convertext. In the arrangement of bits in a byte (1 byte = 8 bits), there is the most significant bit (most significant bit or MSB) and the least significant bit (least significant bit or LSB).

The working principle of LSB is to add a data bit at the end of the bit. This method is considered safe from its output when compared to other methods (Farhani, 2022).

LSB is a popular and frequently used steganography method. In this method, the message will be inserted by replacing the smallest (last) bit of the image pixel with the message bit, because it will not have a significant influence or change on the digital image (Supardi, 2021). In simple terms, an example of the LSB method is shown in Figure 3.

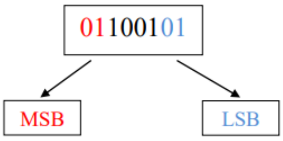


Figure 3. Example of the LSB method

From Figure 3 above, the number 0 which is at the very front is called the Most Significant Bit (MSB) so that the LSB bit in the binary is the number 1 which is located at the far right or at the very back. When the last bit of the LSB is inserted or changed to 0, this will not significantly affect the color display (the difference is not clearly visible). However, if the bits are inserted with different bits, differences will be seen in the image.

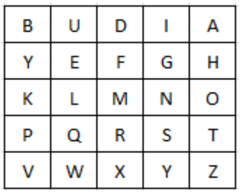
3 Results and Discussion

In this section we will explain examples of the encryption and decryption process using the Playfair Cipher algorithm. The key used is a 5*x*5 matrix containing 25 letters of the alphabet.

3.1 Playfair Cipher Encryption

An example of the keyword: **BUDIDAYA** and original text is given: **PUTIHMERAH**. From these keywords, the encryption process will be carried out in the following stages :

a. Check for the same letter on the key and if there is a letter "J", replace it with the letter "I". So, get the BUDIAY key and add the remaining letters of the alphabet that are not in the key. The results are shown as in Figure 4.

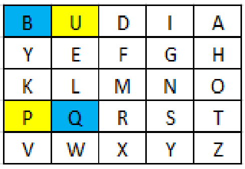


B	U	D	I	A
Y	E	F	G	H
K	L	M	N	O
P	Q	R	S	T
V	W	X	Y	Z

Figure 4. Keyword matrix

b. From the original text: PUTIHMERAH, form each into 2 letters, so that it will form: PU TI HM ER AH.

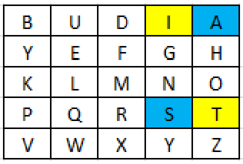
c. Encrypt the letter pair: PU. The encryption result is **QB** as shown in Figure 5.



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

Figure 5. PU encryption results

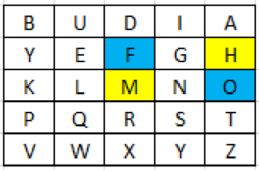
d. Encrypt the letter pair: TI. The encryption result is **SA** as shown in Figure 6.



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

Figure 6. TI encryption results

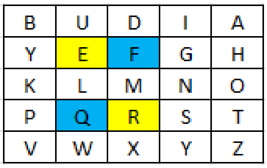
e. Encrypt the letter pair: HM. The encryption result is **FO** as shown in Figure 7.



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

Figure 7. HM encryption results

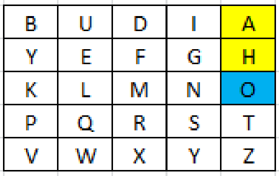
f. Encrypt the letter pair: R. The encryption result is **FQ** as shown in Figure 8.



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

Figure 8. ER encryption results

g. Encrypt the letter pair: AH. Because the AH position is in 1 column, the letter A goes down 1 down to become H and the letter H also goes down 1 down to become O so that the encryption result is **HO** as shown in Figure 9.



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

Figure 9. AH encryption results

From a series of encryption processes for pairs of letters from the original WHITERED text, the encryption result is obtained: QBSAFOFQHO.

3.2 Playfair Cipher Decryption

Basically, the decryption process is similar to the encryption process and is easier to do because decryption is the opposite of the encryption process.

The results of the encryption of the PUTIHMERAH text are known and after processing it becomes PU TI HM ER AH. The processed product is encrypted into QB SA FO FQ HO. The initial keyword used in this process is CULTURE and after processing it becomes BUDIAY. So the encryption results will be returned to the original text as follows :

Encryption text : QB SA FO FQ HO
Plain text : PU TI HM ER AH

3.3 Message Insertion Concept

In principle, to insert an encrypted text message into an image, you need to change the encrypted text into an ASCII value. Then, after obtaining the ASCII value, it is converted into binary form so that it can be inserted into the cover image.

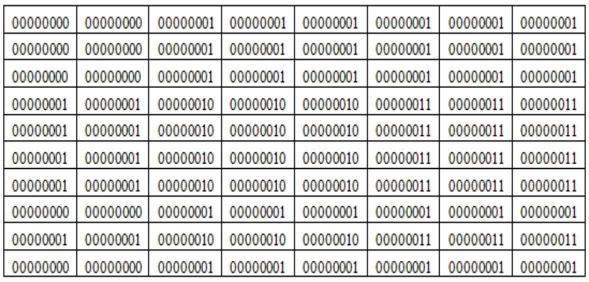
From the explanation above, the process of inserting a message into an image is as follows:

a. Enter the encryption results: QB SA FO FQ HO
b. Match the ASCII characters of each pair of encryption letters as in table 1 below.

Table 1. Character Change Table

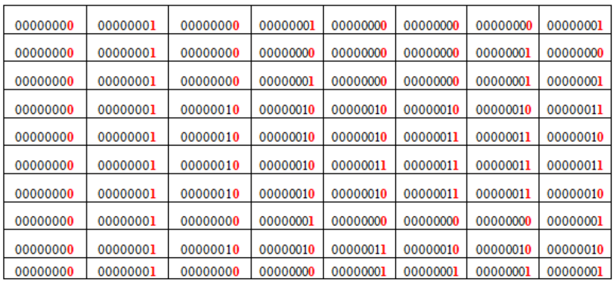
Char	ASCII	Hexadecimal	Binary
Q	81	51	01010001
B	66	42	01000010
S	83	53	01010011
A	65	41	01000001
F	70	46	01000110
O	79	4F	01001111
F	70	46	01000110
Q	81	51	01010001
H	72	48	01001000
O	79	4F	01001111

c. Prepare the image image as a holding medium and change the pixels of the image to binary value form and produce a value as in Figure 10 below.
d. Insert the binary value for each encryption character into the image binary value as shown in Figure 11 below. From the process of inserting encryption characters as shown in Figure 11, it can be seen that changes in image pixels only occur in the last bits of the stego image. With insignificant changes it will not be detected by the human eye so it will not raise suspicion. Values marked in red are examples of bit value insertion positions



00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001
00000001	00000001	00000010	00000010	00000010	00000011	00000011	00000011
00000000	00000000	00000001	00000001	00000001	00000001	00000001	00000001

Figure 10. Image binary value



00000000	00000001	00000000	00000001	00000000	00000000	00000000	00000001
00000000	00000001	00000000	00000000	00000000	00000000	00000001	00000000
00000000	00000001	00000000	00000001	00000000	00000000	00000001	00000001
00000000	00000001	00000010	00000010	00000010	00000010	00000010	00000011
00000000	00000001	00000010	00000010	00000010	00000011	00000011	00000010
00000000	00000001	00000010	00000010	00000011	00000011	00000011	00000011
00000000	00000001	00000010	00000010	00000010	00000011	00000011	00000010
00000000	00000001	00000000	00000001	00000000	00000000	00000000	00000001
00000000	00000001	00000010	00000010	00000011	00000010	00000010	00000010
00000000	00000001	00000000	00000000	00000001	00000001	00000001	00000001

Figure 11. Stego image value

e. Carry out an extraction process where the process is to change the stego image matrix values into binary form. Then taking the last bit from each pixel (the last value is red), the binary value is the binary message that has been inserted into the image.
f. Changing the binary value of the inserted message into decimal form so that the message in question can be identified. This decimal value is the ASCII form value of the message. So from table 2 it can be seen that the message inserted is QBSAFOFQHO which is called an encrypted message (ciphertext).

Table 2. Table of Changes in Binner Values

Binary	ASCII	Char	Hexadecimal
01010001	81	Q	51
01000010	66	B	42
01010011	83	S	53
01000001	65	A	41
01000110	70	F	46
01001111	79	O	4F

4 Conclusion

From the system testing carried out, it can be concluded that the combination of playfair cipher with LSB steganography is able to make messages more secure because the decryption process for encrypted messages is difficult and the media in which the message is inserted does not show any significant changes. The media used as a message container does not change the color of the image pixels so that the inserted message will not be lost or damaged. This research still uses one cryptographic algorithm concept so there is a possibility that it can be studied to dismantle it, so it is hoped that future research can use a combination of more than one cryptographic algorithm.

References:

Amin, (2016). *Implementasi Kriptografi Klasik PadaKomunikasi Berbasis Teks*, JurnalPseudocode, Volume III Nomor 2, September hal. 129-136.

Apriyani, M., & Djuwitaningrum, E. R., (2016): *Teknik Stegaografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruental Generator*, JUITA, Vol. 4 No. 2 pp. 79 – 85.

Farhani, W.S & Dwiharzandis, A, (2022), *Steganografi Metode Least Significant BIT (LSB) Pada Mpeg Spatial Audio Object Coding*, Rang Teknik Journal, Vol. 5, No. 2, pp. 364-368

Febriana, I & Aji, G, (2017), *Penerapan Teknik Kriptografi Pada Keamanan Smsandroid*, JOEICT (Jurnal of Education and Information Communication Technology), Vol. 1, No., 1, pp. 29-36.

Laoli, D, et al, (2020), *Penerapan Algoritma Hill Cipher dan Least Significant Bit (LSB) untuk Pengamanan Pesan pada Citra Digital*, Jurnal JISKa (Jurnal Informatika Sunan Kalijaga), Vol., 4, No. 3, pp. 138-148

Maulana, A., R. (2012). "*Penerapan Algoritma WAKE Pada Aplikasi Chatting & Internet Monitor Berbasis LAN*". Yogyakarta : STMIK Amikom Yogyakarta.

Munir, R. (2019). *Kriptografi*, Bandung: Informatika Bandung

Murdowo, S. (2020), *Manual Perhitungan Menggunakan Kriptografi KlasikPlayfair Chiper*," J. INFOKAM, vol. XVI, no. 19, ,doi: https://doi.org/10.53845/infokam.v16i1.217.

Nugroho,C. (2022), *Steganografi Pada Pengiriman Teks Pesan Gambar dengan Metode Least Significant Bit & Steghide*, J. Ilmu Siber, vol. 1, no. 3, hal. 44–47, 2022

Nurmaesah, N, et al.,(2017), *Aplikasi Steganografi Untuk Menyisipkan Pesan DALAM MEDIA IMAGE*, J. TAM (Technology Accept. Model., vol. 8, no. 1, pp. 13–17.

Pabokory, FN., Astuti, IF & Kridalaksana, AH .(2015): *Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard*, Jurnal Informatika Mulawarman, Vol. 10, No. 1, Februari 2015, pp. 20-31.

Perdana, G.A., et al, (2021), *Implementasi Algoritma Kriptografi Playfair Cipher untuk Mengamankan Data Aset (Studi Kasus: PT Adyawinsa Stamping Industries)*, JIP (Jurnal Informatika Polinema), Vol., 7, No. 2, pp. 109-114.

Ratnasari, A.P & Dwiyanto, F. A. (2020), *Metode Steganografi Citra Digital*, Sains, Apl. Komputasi dan Teknol. Inf., vol. 2, no. 2, hal. 52, 2020, doi: 10.30872/jsakti.v2i2.3300

Sancaka, T.M.P. & Lusiana, V, (2022), *Penerapan Metode Playfair Cipher Dalam Aplikasi Enkripsi- Dekripsi File Teks*, JURNAL ILMIAH ELEKTRONIKA DAN KOMPUTER, Vol.15, No.2, pp.260-270.

Setyaningsih E, (2015), *Kriptografi & Implementasinya Menggunakan MATLAB*, Yogyakarta: Andi Offset, 2015.

Simbolon, R.W., (2016), *Pengamanan Transkrip Nilai Mahasiswa Menggunakan Kriptografi Playfair Cipher Dan Steganografi Dengan Teknik Least Significant Bit (Lsb)*, Jurnal Teknologi Informasi dan Komunikasi, Vol. 5, No. 1, pp. 59-70.

Sitorus, M. (2015), *Teknik Steganography Dengan Metode Least Significant Bit (Lsb)*, Jurnal Ilmiah Fakultas Teknik LIMIT'S, Vol. 11, No. 2, pp. 54-59.

Suhardi, S. (2016), *Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-Or (Xor)*, Jurnal Teknovasi, Vol. 3, No. 2, pp. 23-31.

Sumarsono, et al (2019), *Expending Technique Cryptography for Plaintext Messages by Modifying Playfair Cipher Algorithm with Matrix 5 x 19*, International Conference on Electrical Engineering and Computer Science (ICECOS) 2019, pp. 10-13.

Supardi, S., Alkodri, A. A., & Isnanto, B. (2021). Teknik Steganografi Penyembunyian Pesan Text Rahasia Pada Citra Digital Dengan Metode Least Significant Bit. Jurnal Sisfotek Global, 11(1), 1–5. https://doi.org/10.38101/sisfotek.v11i1.351

Syawal, M.F. (2016), *Implementasi Teknik Steganografi Menggunakan Vigenere Cipher dan Metode LSB*, Jurnal TICOM, Vol.4 No.3 Mei 2016, pp. 91-98.

Wiyata, (2016), *Implementasi Steganografi Metode LSB Menggunakan Program PHP Untuk Keamanan Pesan Gambar*, Jurnal ICT Learning Vol.2, No.2.

Yanti, F & Budayawan, K. (2023), *Implementasi Steganografi Menggunakan Metode Least Significant Bit (Lsb) dalam Pengamanan Informasi pada Citra Digital*, Jurnal Vocational Teknik Elektronika dan Informatika, Vol. 11, No. 1 , pp. 64-70.