EXPLORE
Jurnal Sistem Informasi dan Telematika
(Telekomunikasi, Multimedia dan Informatika)

Concept of Data Security in Digital Image Media Using Spread Spectrum Steganography and Playfair Cipher Cryptography

Natalinda Pamungkas, Bonifacius Vicky Indriyono, Ichwan Setiarso
Information Systems Study Program, Faculty of Computer Science
Dian Nuswantoro University PSDKU Kediri, Indonesia
Information Systems Study Program, Faculty of Academic Studies
University of Computer Science And Technology
Semarang, Indonesia
Visual Communication Design, Faculty of Computer Science
Dian Nuswantoro University PSDKU Kediri, Indonesia
natalinda.pamungkas@dsn.dinus.ac.id , bonifacius.vicky.indriyono@stekom.ac.id, ichwan.setiarso@dsn.dinus.ac.id

Abstract- In the world of informatics, there are many techniques that can be used to maintain the confidentiality of digital information from parties who are not responsible and have the right to access that information. One of the most common techniques today is steganography and cryptography. Steganography is a method used to secure information by hiding it in an object without having to change the shape of the object, while cryptography is a science that studies techniques for encoding original text (plaintext) by using encryption keys so that the text turns into text that is difficult to read. (ciphertext).) by users who do not have the decryption key. This research aims to build a system for securing information on digital images using spread spectrum steganography techniques and playfair cipher cryptography. From the results of research using several files including (.txt), (.docx), and (.pdf). It can be concluded that the larger the file size, the longer it takes to encrypt or decrypt the encryption or decryption process will take time. And if inserted into image media using the spreadspectrum technique, it will produce a stegano image with the RGB pixel value changing from 0 to 1 which does not affect the reproduction of the RGB color image pixels.

Keywords: Steganography, Cryptography, Spread Spectrum, Playfair Chiper.

1. Introduction

Today, the rapid development of information technology is proven to be able to provide many conveniences in completing human work. Exchanging data and information becomes easier and faster. However, on the other hand, it also has a negative impact, namely the act of stealing information by irresponsible parties. Various techniques are used to protect digital information, especially information that is kept confidential from people who are not entitled to the access rights to that information. Among them is by using steganography and cryptography techniques. According to [1], Steganography refers to concealing a secret message within a more mundane communication and removing it once the message reaches its intended recipient. Others cannot know that the message contains confidential data or encrypted data. The primary objective of steganography is to conceal the fact that covert conversations are taking place. In order to complete this process, secret information is input into the cover image in a way that does not result in major modifications [2]. Cryptography is defined as a science that is used to transmit information in a secure form and manner such that the only person who can retrieve and read this information is the intended recipient [3]. In this research, it will be explained how to secure information in the form of text data into digital image media using spread spectrum steganography techniques and playfair cipher encryption. Spread spectrum is defined as a communication method in which the information signal is spread across all available frequencies by choosing a place to insert data at a low frequency by adding pseudo-noise. In steganography, the spread sepctrum technique is suitable for embedding messages in the form of digital audio data [4]. The playfair cipher encryption technique

This work is licensed under a Creative Commons Attribution 4.0 International License

according to [5] is a form of digraphs cipher. The course of the encryption and decryption process is carried out for every two letters in pairs (bigram). This playfair cipher is in the form of a matrix with a size of 5x5 in the form of a square to accommodate 25 capital letters. All of the alphabet except J is placed in the matrix table. The letter J is considered the same as the letter I, because the letter J has the smallest frequency of occurrence. The key used is a word and there cannot be repeated letters. The key is entered into the 5×5 matrix table, the first entry is the key. Next, write the following letters in order starting from the first line.

The results of this study concluded that the process of implementing the spread spectrum algorithm was carried out with the input data being spread into a scale of four so as to produce a psoudonoise value and the digital image data as a result of the insertion did not change. This is because the insertion process is carried out at the end bit of the digital image binary value which only adds one value or subtracts one image pixel value, while the application of Playfair Cipher encryption results in concluding that the initial image before and after the information message is inserted is difficult to distinguish by naked eye so it will not be raise suspicions.

Similar research has also been carried out by previous researchers and the main difference between this research and previous research is the concept of steganography media used. If previous research did not only use image media, this research is still limited to using image media only so the results are not yet visible if applied to other media.

2. Spread Spectrum Methodology

The term "spread spectrum technique" refers to a technique in which a signal (such as an electrical, electromagnetic, or acoustic signal) that is generated with a given bandwidth is purposely spread out in the frequency domain in order to produce a signal with a broader bandwidth. Spread spectrum techniques are used in telecommunications and radio communications [6]. In general, this method is utilized for a wide range of purposes, some of which include the establishment of secure communications, an increase in resistance to natural disturbances, noise, and interference, the prevention of detection, and the facilitation of multiple access to communications.

This technique was recently developed for the adaptive spread spectrum coding method, which can simultaneously achieve robustness and reversibility of watermarking [7]. Then, according to other studies, this method was unique techniques to increase data privacy, security, and efficiency in monitoring multibiosignals in multiuser networks for electronic health care applications [8].

A. Basis Concept Spread Spectrum

The following is an explanation related to the basic concept of the spread spectrum technique according to[9-11]. Arranges information messages in the order m0, m1, m2,.....mk- of each recorded bit according to the following rules

$$\forall i \in \{0,1,\ldots,k-1\} : m_i \in \{-1,1\} \quad (1)$$

To implement direct spread spectrum technology, the following rules apply to discrete signals:

$$\Phi_i \in \Phi = \{\Phi_0, \Phi_1, \ldots, \Phi_{M-1}\},\ k \le M \quad (2)$$

The discrete signal basis B defines various spectrum reasons using the following rules:

B=TF (3)

where T is the duration of one elementary signal denoted by Φ_{ij} and F is the signal frequency band Φ_i

B. Steganography Schema Based on Spread Spectrum

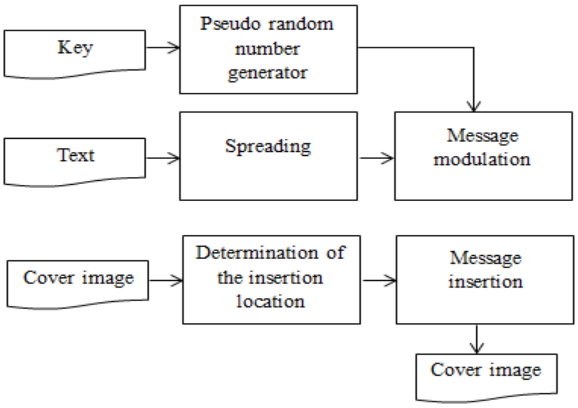


Figure 1. Schematic Of The Message Insertion Process

In the spread spectrum method, the insertion of a message or information contains a key that is used to encrypt the message. The encryption key in this study was obtained through a pseudo random number generator with the LCG (Linear Congruential Generator) algorithm. The scheme of the spread spectrum method can be seen in Figure 1.

Then after the message insertion process, followed by message extraction. The schematic of the extraction is shown in Figure 2.

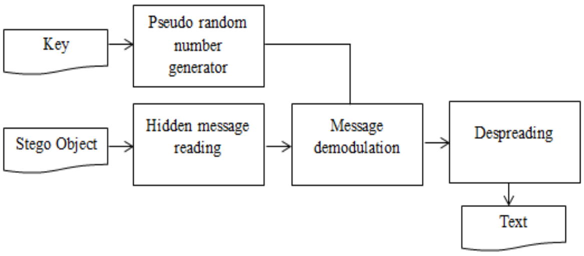


Figure 2. Message Extraction Process Schematic

This work is licensed under a Creative Commons Attribution 4.0 International License

3. Playfair Chiper Encryption Technique

The playfair cipher was initially utilized for military purposes for the first time by British forces during World War I and the Second Boer War. This algorithm for ciphering uses polyalphabetic ciphers as its foundation [12]. Because there are just 26 characters in this procedure, it is not difficult to solve as long as there is sufficient text. This method creates a table that contains plaintext that is organized according to the key value that is supplied.

Playfair Cipher is a group of substitution cipher polygram ciphers. Playfair Cipher performs a bigram substitution process (groups of two letters). This Cipher algorithm performs the process of encrypting paired letters (bigrams or digraphs) into pairs of letters as well, not like other Cipher algorithms which encrypt single letters.

The Playfair Cipher algorithm performs two stages in the cryptographic process, namely encryption and decryption. This algorithm is realized in a 5 x 5 matrix to store the key that has been set by the sender of the message [13]. To determine the key to be used in the 5 x 5 key matrix, the key only consists of capital letters A-Z by removing the letter J in the sentence [14].

The following guidelines govern the process of encryption that employs the Playfair Cipher algorithm [15]:

1. If the two letters are located in separate rows and columns, the first letter will be the one that is in line with the second letter and the column that contains the first letter. The second letter moves into the same column as the first letter and replaces the letter that was previously in line with the second letter.
2. If the positions of the two letters are in the same row but different columns, then the first letter shifts to the right to become the next letter in the same row. In reverse, the second letter takes the place of the preceding letter in the following line to the right as it moves up the alphabet.
3. If the positions of the two letters are in the same column and in a different row, then the first letter becomes the next letter in the same column (downward). And vice versa with the second letter, it becomes the next letter in a different column (towards the bottom).
4. If the position of the two letters is the same, then the letter Z can be placed between them.
5. If the number of plaintext letters is odd, then the letter Z can be added at the end of the sentence

1. Example of Encryption Process

To better understand the encryption process with Palyfair Cipher, the following example is given.

Plaintext : JAWABAN SOAL UJIAN
Keywords : TILANGAN
Key : TILANG

The steps in encrypting Plaintext include :

a. Make a key matrix, namely by inserting the key into a 5×5 matrix

$$X = \begin{bmatrix} T & I & L & A & N \\ G & B & C & D & E \\ F & H & K & M & O \\ P & Q & R & S & U \\ V & W & X & Y & Z \end{bmatrix}$$

b. On plaintext JAWABAN SOAL UJIAN there is the letter J, then the letter J is replaced with the letter I becomes IAWABAN SOAL UIIAN
c. On plaintext IAWABAN SOAL UIIAN there are two letters that are the same side by side i.e II, then insert the letter Z so that it becomes IAWABAN SOAL UIZIAN.
d. Adding the letter Z at the end of the sentence, because the number of plaintext letters is odd. IAWABAN SOAL UIZIANZ.
e. Eliminate spaces in plaintext and change the arrangement of plaintext into letter pairs. IA WA BA NS OA LU IZ IA NZ.

After changing the plaintext arrangement into letter pairs (bigrams), the next process is to encrypt it according to the Playfair Cipher encryption rules. The results obtained from this encryption process are shown in table 1.

Table 1 Result of Plaintext Encryption

Bigram	Encryption Font
IA	LN
WA	YI
BA	DI
NS	AU
OA	MN
LU	NR
IZ	NW
IA	LN
NZ	EN

From the results of the encryption process, the Ciperteks result is: YIDIAUMNNRNWLNEN

2. Example of Decryption Process

Decryption is the process of converting encrypted text (CipherText) back into original text (PlainText). According to [13], the Playfair Cipher decryption process has the following rules

a. If the two letters are found in separate rows and columns, then the first letter is the letter that should be placed in the row with the second letter and the column with the first letter. The second letter moves into the same column as the first letter and replaces the letter that was previously in line with the second letter.

This work is licensed under a Creative Commons Attribution 4.0 International License

b. If the two letters are found in the same row but in separate columns, then the first letter shifts to the position of the previous letter in the same row (moving to the left). This occurs when the two letters are located in the same row but in different columns. In the same way, the second letter transforms into the letter that came before it in the previous line, which is located further to the left.

c. If the location of the two letters is in the same column and in a different row, then the first letter becomes the previous letter in the same column (towards the top). Likewise with the second letter, it becomes the previous letter in a different column (towards the top).

To carry out the process of decrypting YIDIAUMNNRNWLNEN Ciphertext into original text (Plaintext), the following steps are required.

a. Eliminate spaces in the ciphertext and change the arrangement of the ciphertext into letter pairs. YI DI AU MN NR NW LN EN.

b. Carry out the decryption process in accordance with the rules given, so that the results of the decryption process are shown in table 2.

Table 2 Chipertext Decryption Results

Encryption Font	Bigram
LN	JA
YI	WA
DI	BA
AU	NS
MN	OA
NR	LU
NW	IZ
LN	IA
EN	NZ

From the results of the description as in table II above, it can be concluded that the message to be conveyed to the user is : JAWABAN SOAL UJIAN. Even though if you pay attention there is still the letter Z, the meaning that can be taken is JAWABAN SOAL UJIAN.

4. Result Anda Discussion

A. Spread Spectrum Calculation

The following is an overview of how to calculate the Spread Spectrum technique. For the encoding process, in this study using an image in JPEG format. Information messages contain the text FEST and use the keyword "sorry". The process that will occur is that the function in Spread Spectrum starts reading the message entered and checks the size of the information message whether it is smaller than the size of the image. To find out the size used the following calculation.

$$\text{Message Length}=((\text{message size})+28) *4*8 \tag{4}$$

Where the value 28 is the sign given to the image object that has been inserted, number 4 is the magnitude of the multiplier used to spread the bits and the value 8 is the image bit used.

After the file size has been checked, then check the image size, the steganography technique applied and the keywords used. If everything has been detected, then the insertion process is carried out. This procedure starts from reading the image, the header of the prepared image is taken then marking the part of the image to be inserted with a message. The next step before deployment is to convert text messages to binary form. The ANSI value of each character will be converted to binary based on the ASCII code table. The binary conversion results from the FEST message are shown in the following table 3.

Table 3 Text Message Convertion Results

Character	Decimal Value	Binary Value
F	70	01000110
E	69	01000101
S	83	01010011
T	84	01010100

After the binary value of the message text is known, then the next value is spread with a scalar quantity multiplied by four, so that a new segment value will be produced as shown in table 4.

Table 4 Results of Value Distribution

Char	Binary Value	Distribution of Scalar Values 4
F	01000110	000011110000000000001111 11110000
E	01000101	000011110000000000001111 00001111
S	01010011	000011110000111100000000 11111111
T	01010100	000011110000111100001111 00000000

The next process is to generate pseudonoise values based on the keyword "Mika". The steps for its generation are as follows.

a. Converts the decimal value of the keyword to a binary value. The results are shown in table 5.

This work is licensed under a Creative Commons Attribution 4.0 International License

Table 5 Key Value Convertion Results

Char	Decimal Value	Binary Value
M	109	01101101
I	105	01101001
K	107	01101011
A	97	01100001

b. Performs XOR on each key character binary value. The process is as follows:
   1. The binary value of character M is XORed with the value of key character I, resulting in the following values: 01101101 XOR 01101001 = 00000100.
   2. The resulting XOR values from characters M and I are then XORed with characters K to produce the following values: 00000100 XOR 01101011 = 01101111.
   3. The XOR value of the K character is XORed with the key character A to produce the following value: 01101111 XOR 01100001 = 00001110.
   4. Change the binary value of the final result to a decimal value so that you get a value of 7.

c. Uses the last XOR value as the initial random number generator. The method used is LCG (Linear Congruential Generator) with the following writing rules:

$X_{n+1}=(aX_n+c)\text{mod}_m$ (5)

Where Xn is the integer, a is the multiplier factor, c is a constant and m is the modulus. Determined values for generation are: a=17, c=8 and m=84. The solution is as follows :

$X_1=(17*7+8)$ mod 83 = 43

$X_2=(16*43+8)$ mod 83 = 67

$X_3=(16*2+7)$ mod 83 = 55

And so on up to Xn or as many as the number of distributions. As an example of the implementation of this LCG value with 5 times the distribution, the values are: 43, 67, 55, 19, 79 so if converted into a binary value it will produce values: 00101011 01000011 00110111 00010011 01001111.

d. Carry out the demodulation process by XORing the value of the message text data with the value of the Pseudonoise segment. Here's the process

Message Segment:
00001111000000000000111111110000
00001111000000000000111100001111
00001111000011110000000011111111
00001111000011110000111100000000

Pseudonoise Value:
00101011 01000011 00110111 00010011 01001111

Then the results of the modulation process between message segments and pseudonoise signals using the XOR function are as follows.

00100100010000011110010000011100
01000000000001110010010001001100
00111000000011100010011111110111
00100100010000011110001110011100

e. Inserts the modulation result into the image byte. As an example, ten pixels are taken from a digital image and from the modulation between the message segment and the pseudonoise signal the first thirty bits are taken.

Red =181 180 185 182 181 183 186 184 187 184
Green = 172 166 171 174 170 173 176 174 176 179
Blue = 172 169 163 169 168 171 175 173 177 174

f. The color values are then converted into binary and the results of the modulation process between the message segment and the pseudonoise signal are inserted as follows.

Table 6 Color Value Convertion Results

Red	Green	Blue
10110101	10101100	10101100
10110100	10100110	10101001
10111001	10101011	10100011
10110110	10101110	10101001
10110101	10101010	10101000
10110111	10101101	10101011
10111010	10110000	10101111
10111000	10101110	10101101
10111011	10110000	10110001
10111000	10110011	10101110

g. Demodulation binary value shrink. In this step, the results of the demodulation will be divided by 5 which will be used to shrink the demodulation results into binary samples of actual text data characters. The process of shrinking the segment is the opposite of the process of forming the scalar quantity 4, namely by removing the 3 bits of the same binary value from each binary bit, so the result is: 01000110 01000101 01010011 01010100. From these binary values will then be converted to decimal form and will produce actual text message data as shown in table 7.

Table 7 Convertion Results of Message Binary

Binary Value	Decimal Value	Char
01000110	70	F
01000101	69	E

This work is licensed under a Creative Commons Attribution 4.0 International License

Binary Value	Decimal Value	Char
01010011	83	S
01010100	84	T

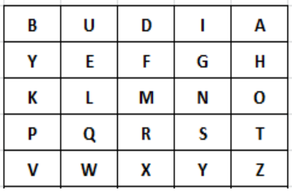
B. Text Message Encryption With Playfair Chiper

For the application of the Playfair Cipher algorithm as follows. There is a keyword: Cultivation. So from these keywords the next step is:

a. Arrange the letters of the keywords first with a note that the letters that have been mentioned are not written again so they will become : BUDIAY. If there is a letter J, replace it with the letter I.

b. Next, add the remaining letters of the alphabet that are not included in the keyword letters, namely EFGHJKLMNOPQSTVWXZ so that they become BUDIAY EFGHKLMNOPQSTVWXZ

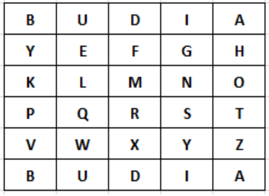
c. Arrange it into a 5x5 matrix like figure 3.



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 3. Keyword Matrix

d. Expand the password for the encryption process. The result is as shown in Figure 4 below

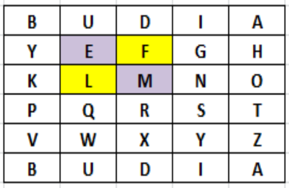


B	U	D	I	A
Y	E	F	G	H
K	L	M	N	O
P	Q	R	S	T
V	W	X	Y	Z
B	U	D	I	A

Figure 4. Keyword ExpansionMatrix

e. Perform encryption for Plainteks: MERAH PUTIH. Pair letters by removing non-letter characters so that they become: ME RA HP UT IH

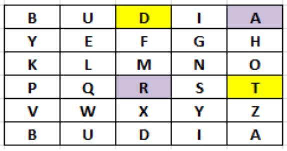
f. ME letters are encrypted to LF. The result is like figure 5



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
B	U	D	I	A

Figure 5. ME Encryption Results

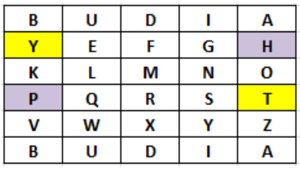
g. RA letters are encrypted to TD. The result is like figure 6.



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
B	U	D	I	A

Figure 6. RA Encryption Results

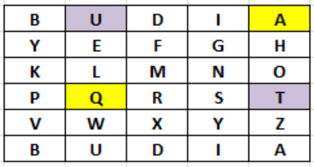
h. The letters HP are encrypted to YT. The result is like figure 7.



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
B	U	D	I	A

Figure 7. HP Encryption Results

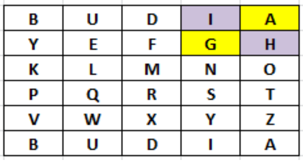
i. The letters UT are encrypted to become AQ. The result is like figure 8.



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
B	U	D	I	A

Figure 8. UT Encryption Results

j. The letters IH are encrypted to AG. The result is like 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
B	U	D	I	A

Figure 9. IH Encryption Results

From the results of the encryption that was carried out, it was obtained that Plainteks MERAH PUTIH was encrypted as: LFTDYTAQAG.

5. Conclusion

From the results of the analysis and tests carried out, it can be concluded that the spread spectrum algorithm applied. The process of implementing the spread sprectum algorithm using data distribution in scalar four can produce psoudonoise values. The digital image used has not changed significantly, this is because the insertion process is carried out at the very end of the digital image binary value which only adds one value or subtracts one image pixel value, while text data is encrypted using Palyfair Cipher making data more secure because it uses the word a lock that has many rules. The images before and after the encrypted message is inserted are very difficult to distinguish so that it will not raise suspicions for other people.

6. References

[1] G. Prabakaran, R. Bhavani and S. Sankaran, "Dual Wavelet Transform Used in Color Image Steganography Method," International Conference on Intelligent Computing Applications, pp. 193–197,ISBN. 978-1-4799-3966-4 March, 2014.

[2] A. Malik, G. Sikka, H.K. Verma, "A high capacity text steganography scheme based on LZW compression and color coding", Eng. Sci. Technol. Int. J. 20 (1) (2017) 72–79.

[3] B. Purnama and H. Rohayani, "A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext From A Message To Be Encrypted", International Conference on

This work is licensed under a Creative Commons Attribution 4.0 International License

Computer Science and Computational Intelligence (ICCSCI), pp. 195-204, 2015.

[4] M. Nutzinger, C. Fabian and M. Marschalek, “Secure Hybrid Spread Spectrum System for Steganography in Auditive Media”, Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 78-81, ISBN. 978-0-7695-4222-5, 2010.

[5] Sumarsono, M. Anshari and A. Mujahidah., “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), pp. 10-13, October 2019.

[6] A. Singh, “Performance Analysis of Spread Spectrum Techniques”, Conference on Advances in Communication and Control Systems (CAC2S), pp. 683-687, 2013.

[7] Z. Huang, B. Feng, and S. Xiang, “Robust reversible image watermarking scheme based on spread spectrum,” J. Vis. Commun. Image Represent., vol. 93, p. 103808, 2023, doi: https://doi.org/10.1016/j.jvcir.2023.103808.

[8] M. A. Murillo, et al, “Multibiosignal chaotic encryption scheme based on spread spectrum and global diffusion process for e-health,” Biomed. Signal Process. Control, vol. 78, p. 104001, 2022, doi: https://doi.org/10.1016/j.bspc.2022.104001.

[9] L. M. Marvel, C. G. Boncelet, R. Jr., and Charles T., “Methodology of Spread-Spectrum Image Steganography,” Jun. 1998.

[10] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999.

[11] F. S. Brundick and L. M. Marvel, “Implementation of Spread Spectrum Image Steganography,” Mar. 2001.

[12] M. Packirisamy, and G. Senthilkumar. "Modified version of playfair cipher using linear feedback shift register." In 2009 International Conference on Information Management and Engineering, pp. 488- 490. IEEE, 2009.

[13] R. Munir, ” Cryptography ”. Bandung: Informatics, 2008

[14] E. Nurkifli, Haodudin, ” Modification of the Playfair Algorithm and Combining with the Linear Feedback Shift Register (LFSR)”, Karawang : Singaperbangsa University Karawang, 2014.

[15] Santi, R.C.N., Implementation of the Playfair Encryption Algorithm in Text Files, Journal of Information Technology DYNAMIK, Vol. XV, No. 1, 2010

This work is licensed under a Creative Commons Attribution 4.0 International License