International Journal of Research In Science & Engineering
Volume: 2 Issue: 6

e-ISSN: 2394-8299
p-ISSN: 2394-8280

COMBINATION OF PIXEL VALUE DIFFERENCING ALGORITHM WITH CAESAR ALGORITHM FOR STEGANOGRAPHY

Dicky Nofriansyah[1], Robbi Rahim[*2]

[1]*Lecturer, Departement of Computer System, STMIK Triguna Dharma, JL.Pintu Air I 73F, Medan, Indonesia, dickynofriansyah@gmail.com*
[2]*Lecturer, Departement of Computer Engineering, Medan Institute of Technology, Jalan Gedung Arca No.52, Medan, Indonesia, usurobbi85@zoho.com*

ABSTRACT

Steganography is a method that can be used to secure information. Steganography is hiding information or messages into other media such as digital images, text, voice or video so as not to arouse suspicion of others. Steganography methods that are widely used today still have shortcomings regarding quality, capacity, and robustness. Therefore, it needs steganography methods other better, and to add to the information security, steganography can combine with cryptography. Steganography method used is the method of pixel value differencing (PVD). This approach can insert a message more to the pixels you pick a high contrast value. To increase the security level of information to be embedded into the image, use cryptography such as Caesar cipher algorithm. Caesar cipher is an algorithm that used as a standard encryption by using an alphabet. Research conducted that combine cryptography steganography in digital imagery. Then testing the steganography methods used to determine the capacity of the image, the performance of the method pixel value differencing (PVD), the resulting image quality, and resistance to manipulation of image and Steganalysis.

Keyword: Cryptography, Steganography, Pixel Value Differencing, Caesar Cipher, Security, Hidden Text

1. INTRODUCTION

Confidentiality and security of information in the era of globalization are increasingly becoming a vital need in various aspects of life [1] [2] [3]. A piece of information will have rated higher if it concerns aspects of business decisions, security, or the interests of the public and private [1]. There are various methods used to protect data such as providing passwords, but this approach can be cracked by pirates because the user can make the possibilities of words used as passwords by the parties locked. Another way is to ciphertext [4] [5], in this way the data that will store will encrypt in advance, but this can attract suspicion by parties who are not responsible, so the user will attempt to break the ciphertext so that data can hijacke [1] [4]. Therefore, we need a way of being able to make the unsuspecting pirates and users do not immediately know that no data are stored, and that's the Steganography work.

Steganography is a method that can be used to secure information [6] [7]. Steganography is different from the cryptography or other information security method; this method is to hide information or messages into other media such as digital images, text, voice or video so as not to arouse suspicion of others [6]. Steganography requires two properties, namely information and media container [6]. Media container used to hide information that is digital imagery [7]. Insertion of information on digital media image carried on bits of pixels contained in the picture. The use of the digital image as a media container has the advantage because the human visual perception has limitations of the color so that with the limitations of the human being is difficult to distinguish the original digital image with the digital image which has inserted a secret message [8].

Pixel Value Differencing method is one method that can use in the manufacture of steganography [9] [10] [11]. This method offers a storage capacity larger messages, with better image quality compared to other methods [9]. To increase the security level of information to be inserted into the picture, steganography can be combined with encryption, so that the embedded information will not be easily read by people who are not responsible. One encryption algorithm that can used is the Caesar Cipher. Caesar cipher method comes from Julius Caesar, a Roman emperor, and he uses the substitution cipher to send a message to the commander of the war [12]. Caesar Cipher knew by several names such as Shift Cipher, Caesar's code or Caesar Cipher shift [12] [13].

2. THEORIES

Cryptography is the science of the encryption technique where data is encrypted using an encryption key to be something that 's hard to read by someone who does not have the decryption key [2]. Decryption using the decryption key to

e-ISSN: 2394-8299
p-ISSN: 2394-8280

get back the original data. The encryption process is done using an algorithm with few parameters such as the random number and the key [1] [2].

In classical cryptography, encryption technique used is a symmetric encryption where the decryption key together with the encryption key [4]. For public key cryptography, asymmetric encryption techniques required which the decryption key is not the same as the encryption key [1] [2]. Encryption, decryption and key generation for asymmetric encryption techniques require more computing intensive than symmetric encryption [2] because asymmetric encryption uses numbers are vast. However, although the asymmetric encryption longer in the process of computing than symmetric encryption, public key cryptography is very useful for the major management and digital signature [2].

2.1 Caesar Cipher

Substitution encryption technique that was first known and simplest discovered by Julius Caesar [14]. The method used in the Caesar cipher is by exchanging each letter of the plaintext with another letter to the interval three letters of plaintext letter [14]. As an example can be seen below:

Table 1. Caesar Cipher

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

To encrypt a message, only look for each letter to be encoded alphabet usual, and write the corresponding letter in the alphabet password. To break the password using the opposite way. Examples of encoding a message is as follows:
plaintext: Universitas Prima Indonesia
ciphertext: xqlyhuvlwdv Sulpd Lqgrqhvld
The process of encryption (encryption) can be mathematically using a modulo operation by converting letters into numbers, A = 1, B = 2, ..., Z = 26. The formula is as follows:

$$C = E(P) = (P + K) \bmod (26)$$

While in the process of decoding (decryption), the result of decryption is:

$$P = D(C) = (C-K) \bmod (26)$$

Each of the same letters is replaced by the same letter throughout the message, so the cipher is classed to monoalphabetic substitution, as opposed to substitution polyalphabetic. To encrypt a message, only look for each letter to be encoded, and write the corresponding letter in the password. To break the password using the opposite way. Examples of encoding a message are as follows.
Ordinary alphabet: 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
Alphabet Password: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Original text: MAKAN NASI GORENG
Text Password: PDNDQ QDVL JRUHQJ
For ASCII characters from letters A to Z, as follows:

Table 2. ASCII Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

2.2 Pixel Value Differencing

Pixel Value Differencing Scheme using a pixel value of the difference between two consecutive blocked to determine how many secret bits to be embedded [9] [10] [11]. There are two types of quantization tables range in the method of Wu and Tasi it [9]. The first step selecting a wide range [8, 8, 16, 32, 64, 128] to provide a large capacity [9]. The second is based on selecting a wide range [2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64, 64] [9], to provide high imperceptibility. Most of the research related to focus on increasing the capacity using the LSB and the adjustment process so that their approaches are conformable with the LSB approach. There are very few studies that focus on the design of the table range. Also, intuitive to design using the width of the power of two. This work table design new quantization scale based on the number of perfect squares to decide payload with the value of the difference between pixels in a row [11]. This research provides a new angle that if we choose the right width for each range and using the proposed method, we can obtain better picture number and a higher capacity. Also, we offer a theoretical analysis to demonstrate our method is well defined. The results also show that the proposed scheme has some images are better and higher capacity.

The insertion process in this method done by comparing the two neighboring pixels Pi and Pi + 1 using equation.

e-ISSN: 2394-8299
p-ISSN: 2394-8280

$$d= |P_i – P_{i+1}$$

The results of the comparison are used to determine how many bits can insert into the two pixels are compared. This method uses a scheme of Wu and Tsai to ascertain the range of the previous pixel comparison. Wu and Tsai scheme used is R = {[0.7], [8.15], [16.31], [32.63], [64.127], [128.255]} [9].

This scheme is used to determine where the differences are in the range of two pixels that, if it had known where equation could ascertain the location of his range, then the number of message bits inserted.

$$t = | Log_2 w_i|$$

wi: The smallest value of the scheme Wu and Tsai, lies the difference in the comparison of two-pixel range. Insertion of messages can be done by taking as many t bits of the message to be inserted. Furthermore, the difference value is calculated a new value for insertion into the image using equation [9].

$$d'_i = l_i + b$$

di: The smallest value of the scheme wu and tsai, lies the difference in the comparison of two pixel range [9]. To insert a message there are several rules that must be met, namely:

a. If Pi≥Pi + 1 and d i> in, then (Pi + | m / 2 |, Pi + 1 | m / 2 |)
b. If Pi <Pi + 1 and d i> in, then (Criminal | m / 2 |, Pi + 1 + | m / 2 |)
c. If Pi≥Pi + 1 and d'i≤di, then (Criminal | m / 2 |, Pi + 1 + | m / 2 |)
d. If Pi <Pi + 1 and d'i≤di, then (Pi + | m / 2 |, Pi + 1 | m / 2 |)

Where *m* obtained from the difference d'i within using the equation

$$m = | d'_i - d_i|$$

Such processes are performed continuously until all message bits inserted into the image. The process of extracting the message from the steganography images using this method begins by calculating the difference value (in) between two neighboring pixels. Value difference value is used to determine the value of continuous ranges (R), which is defined using Wu scheme and Tsai [9] [11].

3. RESULT AND DISCUSSION

Caesar algorithm is an algorithm type monoalphabetic swapping letters of a sentence into another letter, in this research Caesar cipher algorithm used to secure the message before insert to image, the following were the message "UNIVERSITAS PRIMA INDONESIA" with the number of shifts by five characters

Plaintext = UNIVERSITAS PRIMA INDONESIA
Key = 5

The first step that must make is to make a substitution table, as shown below

Table 3. Shift Caesar Cipher

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	26
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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

From the above table perform the encryption process by applying the Caesar cipher algorithm, the following are the results of the process:

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (20+6) Mod 26
= (26) Mod 26
=26
=Y

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (13+6) Mod 26
= (19) Mod 26
=19
=R

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (8+6) Mod 26
= (14) Mod 26

e-ISSN: 2394-8299
p-ISSN: 2394-8280

=14
=M

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (21+6) Mod 26
= (27) Mod 26
=27
=Z

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (4+6) Mod 26
= (10) Mod 26
=10
=I

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (17+6) Mod 26
= (23) Mod 26
=23
=V

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (18+6) Mod 26
= (24) Mod 26
=24
=W

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (8+6) Mod 26
= (14) Mod 26
=14
=M

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (19+6) Mod 26
= (25) Mod 26
=25
=X

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (0+6) Mod 26
= (6) Mod 26
=6
=E

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (18+6) Mod 26
= (24) Mod 26
=24
=W

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (15+6) Mod 26
= (21) Mod 26
=21
=T

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (17+6) Mod 26
= (23) Mod 26
=23
=V

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (8+6) Mod 26
= (14) Mod 26
=14
=M

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (12+6) Mod 26
= (18) Mod 26
=18
=Q

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (0+6) Mod 26
= (6) Mod 26
=6
=E

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (8+6) Mod 26
= (14) Mod 26
=14
=M

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (13+6) Mod 26
= (19) Mod 26
=19
=R

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (3+6) Mod 26
= (9) Mod 26
=9
=H

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (14+6) Mod 26
= (20) Mod 26
=20
=S

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26

e-ISSN: 2394-8299
p-ISSN: 2394-8280

= (13+6) Mod 26
= (19) Mod 26
=19
=R

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (4+6) Mod 26
= (10) Mod 26
=10
=I

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (18+6) Mod 26
= (24) Mod 26
=24
=W

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (8+6) Mod 26
= (14) Mod 26
=14
=M

Ci = E(P) = (P + K) Mod 26
= (P+6) Mod 26
= (0+6) Mod 26
= (6) Mod 26
=6
=E

From the results of the above process is the result of encryption of the message "UNIVERSITY PRIMA INDONESIA" with the message "YRMZIVWMXEW TVMQE MRHSRIWME." The ciphertext results will be inserted into an image file by using the pixel value differencing algorithm; The first step is to change it into a binary message as below

YRMZIVWMXEW TVMQE MRHSRIWME = 01011001 01010010 01001101 01011010 01001001 01010110 01010111 01001101 01011000 01000101 01010111 00100000 01010100 01010110 01001101 01010001 01000101 00100000 01001101 01010010 01001000 01010011 01010010 01001001 01010111 01001101 01000101

The next stage is to take the value of the pixel of an image, an image with the name assumed tower.bmp, here is the pixel value of the image to be inserted message, the pixel value obtained by using Matlab software

65 122 170
109 203 204
156 209 222

Fig 1. RGB Value From Image

After receiving the pixel values of the image, the next step is inserting a message; the following are the steps

a. Take a neighboring pixel of the image is pixel (0,0) and pixel (0.1), the pixel value is made to do the insertion, the following is a table of neighboring pixel values are 65 and 122

Table 4. Neighboring Pixel Values

65	122	170
109	203	204
156	209	222

b. Calculate the value of the second pixel value differencing the use of = | 65-122 |, thus obtained d = 67
c. Finding the location continues the range of score difference value on wu scheme and tsai R = {[0.7], [8.15], [16.31], [32.63], [64.127], [128.255]} , The layout continues range obtained from d = 67 ie [64, 127] where ik = 64, and uk = 127.
d. Count how many bits of messages that can be inserted into both pixels than that t = log 2 (127-64) thus obtained = 5, then grab bits of the message as much as t is 01010.
e. Change the value of bits as t into a decimal value, of which 01 010 after being converted to decimal is 10 or b = 10, then calculate the new value differencing d '= 42 + 10 to get the value of d' = 52
f. Insertion by changing the value of the pixel compared with the new pixel value by the rules - the rules that exist, where m = 15 obtained from = | 67-52 |. The rules are met and that '<d and 'i <P'i + 1 then Pi = 65 + | 10/2 | and Pi + 1 = 122 - | 10/2 |
g. Save the new pixel value is i = 70 and i + 1 = 117 into the image. This stage carried out until all messages inserted, the following result

e-ISSN: 2394-8299
p-ISSN: 2394-8280

70 117 170

109 203 204

156 209 222

Fig 2. New Pixel Value

Values above picture are the result of applying the method of differencing pixel value. After the insertion process or commonly referred to decoding the message, the next message or the reading process commonly referred to as decoding messages. The initial stage of the process of extracting the message that is taking the pixel values of the image that has been inserted message.

The next stage is the process of extraction method differencing pixel value with the stages are as follows:

a. Take a neighboring pixel of the image. Examples of the neighboring pixel is a pixel (0,0) to pixel (0,1) as shown above. The value of the neighboring pixel is taken to do the insertion. If Pi and Pi + 1 is a neighboring pixel, then = 70 and + 1 = 117.
b. Calculate the value of the second-pixel value differencing the equation = | 70-117 |, thus obtained = 47.
c. Finding the location continues the range of score difference value on wu scheme and tsai R = {[0.7], [8.15], [16.31], [32.63], [64.127], [128.255]}, The layout continues range obtained from = 47 ie [32, 63] where = 32, and = 63.
d. Count how many bits of information has been inserted into the second pixel. Many bits are calculated using the equation is = 2 (63-32) thus obtained = 5, or there is a 4-bit message is posted on the second pixel
e. Change the decimal value in the form of message bits as t, and then we got the message bits b = 01010.
f. The next process is repeated until all the pixels in the know.

4. CONCLUSION

The combination of algorithms Pixel Value Differencing and Caesar Cipher can be analyzed properly, the message is stored in the image according to the process that has been done does not have a lot of changes, which means conceptually that if analyzed using special software will not be known for a message or not, then with Caesar cipher algorithm implementation inserted messages will advance at random so that if done cryptanalysis process will produce a ciphertext.

REFERENCES

[1] R. Rahim and A. Ikhwan, "Study of Three-Pass Protocol on Data Security," *International Journal of Science and Research (IJSR)*, vol. 5, no. 11, pp. 102-104, 2016.

[2] R. Rahim and A. Ikhwan, "Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher," *International Journal of Scientific Research in Science and Technology (IJSRST)*, vol. 2, no. 6, pp. 71-78, 2016.

[3] E. Hariyanto and R. Rahim, "Arnold's Cat Map Algorithm in Digital Image Encryption," *International Journal of Science and Research (IJSR)*, vol. 5, no. 10, pp. 1363-265, 2016.

[4] B. Oktaviana and A. P. U. Siahaan, "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography," *IOSR Journal of Computer Engineering (IOSR*, vol. 18, no. 4, pp. 26-29, 2016.

[5] H.-t. Cui, "Research on the Model of Big Data Serve Security in Cloud Environment," in *First IEEE International Conference on Computer Communication and the Interne*, 2016.

[6] K. Kumar, S. Pabboju and N. M. S. Desai, "ADVANCE TEXT STEGANOGRAPHY ALGORITHMS: AN OVERVIEW," *International Journal of Research and Applications*, vol. 1, no. 1, pp. 31-35, 2014.

[7] R. Ibrahim and T. S. Kuan, "Steganography Algorithm to Hide Secret Message inside an Image," *Computer Technology and Application*, pp. 102-108, 2011.

[8] O. M. Al-Shatanawi and N. N. El. Emam, "A New Steganography Algorithm Based on MLSB Method With Random Pixels Selection," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 7, no. 2, pp. 37-53, 2015.

[9] J. K. Mandal and D. Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain," *International Journal of Information Sciences and Techniques*, vol. 2, no. 4, pp. 83-93, 2012.

[10] J. Salunkhe and S. Sirsikar, "Pixel Value Differencing a Steganographic method: A Survey," in *International Conference on Recent Trends in Engineering & Technology*, India, 2013.

[11] H.-W. Tseng and H.-S. Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," *Journal of Applied Mathematics*, p. 8, 2013.

[12] B. Mohammed, "Automatic Key Generation of Caesar Cipher," *International Journal of Engineering Trends and*

e-ISSN: 2394-8299
p-ISSN: 2394-8280

Technology, vol. 6, no. 6, pp. 337-339, 2013.

[13] P. Patni, "A Poly-alphabetic Approach to Caesar Cipher Algorithm," *International Journal of Computer Science and Information Technologies*, vol. 4, no. 6, pp. 954-959, 2013.

[14] B. Purnama and H. Rohayani.AH, "A New Modified Caesar Cipher Cryptography Method With Legible Ciphertext From A Message To Be Encrypted," in *International Conference on Computer Science and Computational Intelligence*, 2015.