MATEC Web of Conferences **197**, 03011 (2018) https://doi.org/10.1051/matecconf/201819703011
AASEC 2018

Enhanced pixel value differencing with cryptography algorithm

Robbi Rahim[1*], *Nuning* Kurniasih[2], *Frisma* Handayanna[3], *Linda* Sari Dewi[3], *Erene Gernaria* Sihombing[3], *Ester* Arisawati[3], *R* Rinawati[3], *Agus Perdana* Windarto[4], *Erlin Windia* Ambarsari[5], *S* Sriadhi[6], and *Indah* Sulistiyowati[7]

[1]Universiti Malaysia Perlis, School of Computer and Communication Engineering, Perlis, Malaysia
[2]Universitas Padjadjaran, Faculty of Communication Science, Library and Information Science Program, Bandung, Indonesia
[3]STMIK Nusa Mandiri, Jakarta, Department of Information System, Indonesia
[4]STIKOM Tunas Bangsa, Department of Informatics, PematangSiantar, Indonesia
[5]Universitas indraprasta PGRI, Department of Informatics, Jakarta, Indonesia
[6]Universitas Negeri Medan, Department of Education Information Technology and Computers, Medan, Indonesia
[7]Universitas Muhammadiyah Sidoarjo, Department of Electrical Engineering, Sidoarjo, Indonesia

Abstract. The combination of Steganography and cryptography algorithms can improve the security of data you want to keep secret. Pixel Value Differencing (PVD) algorithm combined with Word Auto Key Encryption (WAKE) algorithm and Modular Multiplication Block Cipher algorithm can produce good ciphertext and inserted on image media by using PVD algorithm that convert each ciphertext into pixel.

1 Introduction

Today's communication and information technology is growing rapidly and almost all communications are connected with internet technology. For example the development of Internet network that allows anyone to exchange data or information through the internet network. Communication becomes very important and there are times when communication is confidential and do not want to know the other party [1–3].

Steganography and cryptography [4–8] is an existing technique to accommodate the security of communication made by users, steganography is a technique used to hide information on the media. The most important aspect of steganography is the security level of information concealment, which refers to how much the inability of third parties to detect the existence of hidden information [9–11]. Cryptography has a different way of working, especially in terms of data security, cryptography change the data you want to secure in a form that is difficult to understand by others but this raises suspicion for others [12,13].

Pixel Value Differencing [6,14,15] is a steganography algorithm that can be used to hide messages into image pixels by converting messages into RGB hexadecimal shapes and replacing pixel values in images with hexadecimal RGB message values [14], the pixel value differencing method is quite good compared to other steganography algorithms [15] but to increase the security of hidden messages is combined with Word Auto Key Encryption (WAKE) [16] cryptographic algorithms and Modular Multiplication Block Cipher (MMB) [13,17].

The combination of WAKE and MMB algorithm in encryption process on steganography Pixel Value Differencing will be increase security of message and it is not easy to be known by irresponsible party.

2 Methodology

2.1 Pixel Value Differencing

Pixel Value Differencing Scheme using a pixel value between two blocked pixel and determine how many secret bits to be embedded [6]. Pixel Value differencing was using Wu and Tsai scheme for wide range and large capacity. The insertion process in this method perform by comparing the two neighboring pixels Pi and Pi + 1 using equation.

$$d= |P_i - P_{i+1} \quad (1)$$

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]}[6]. The scheme determines the range of values to be between 2 pixels, then the value of the range is calculated by the equation [14,15].

$$t = | \mathrm{Log}_2 \, w_i| \quad (2)$$

Wi: The smallest value of the scheme Wu and Tsai. Furthermore, the difference value is calculated a new value for insertion into the image using equation

*Corresponding author: usurobbi85@zoho.com

$$d'_i = l_i + b \tag{3}$$

di: The smallest value of the scheme wu and tsai. To insert a message there are several rules that must be met

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

$$m = | d'_i - d_i| \tag{4}$$

All processes are performed continuously until all message bits inserted into the image.

2.2 Word Auto Key Encryption

WAKE stands for Word Auto Key Encryption, this method was invented by David Wheeler in 1993. The WAKE method uses a 128 bit key and a 256 x 32 bit table. In the algorithm, this method uses XOR, AND, OR and Shift Right operations [16,18]. The main process of WAKE consists of:

1) The process of forming table S-Box (Substitution Box).
2) The process of forming the key.
3) Encryption and decryption process.

The core of the WAKE method lies in the process of forming the S-Box table and the key building process. The S-Box table of the WAKE method is flexible and varies for each round.

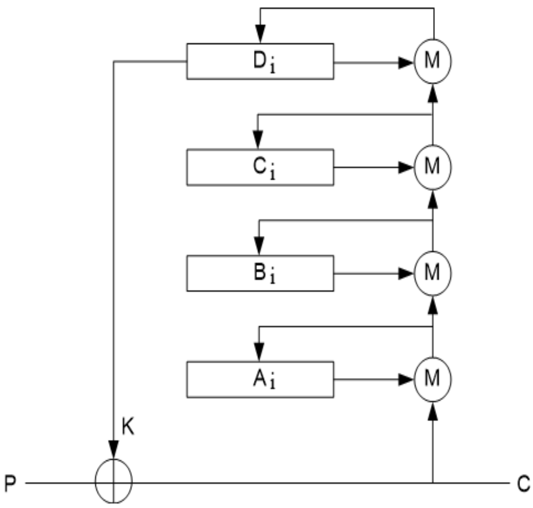

Fig. 1. Key Generation Diagram.

P = Plaintext
K = Key
C = Ciphertext
M = Function M
I = Starting from 0 to n
Ai = The first part of the key fragment
Bi = The second part of the key fraction
Ci = The third part of the key fraction
Di = Fourth part of key fraction

The core of the WAKE method does not lie in the encryption and decryption process, since the encryption and decryption process are just XOR operations of the plaintext and keys to generate ciphertext or XOR ciphertext operations and keys to produce plaintext.

$P = C \oplus K$
$C = P \oplus K$

2.3 Modular Multiplication Block Cipher

The weakness of IDEA method using 64 bit plaintext and multiplication of modulo 216 + 1 is solved by the presence of MMB algorithm (Modular Multiplication Block cipher). MMB algorithm uses 64 bit plaintext (4 pieces 16 bit subblock text) [13]. The cryptography MMB algorithm uses 128-bit plaintext and iterative algorithms such as XOR as well as parallel applications of four reversible non-linear substitutions. This substitution is determined by a multiplication operation modulo 2^{32} - 1 with a constant factor, which has a higher securities rate. A non-linear function, f, is applied six times along with the XOR function.

The process of encryption and decryption MMB method can be seen in the following diagram:

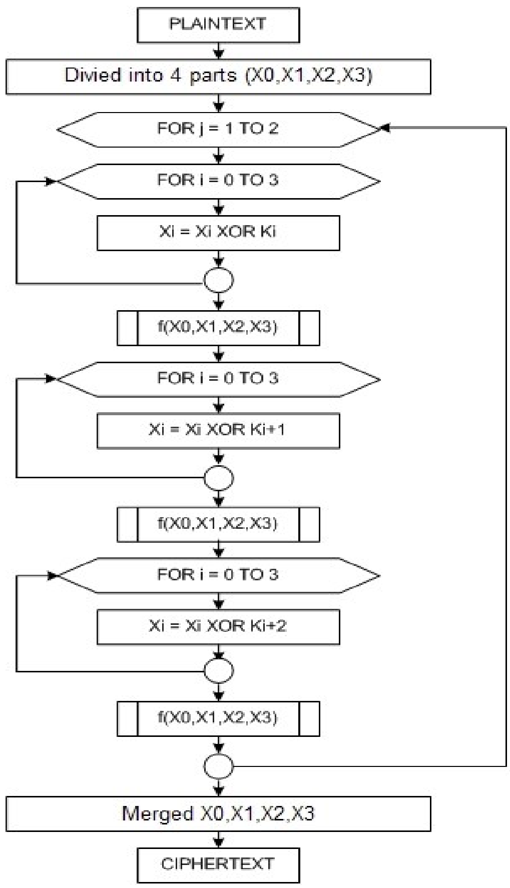

Fig. 2. Encryption MMB Diagram.

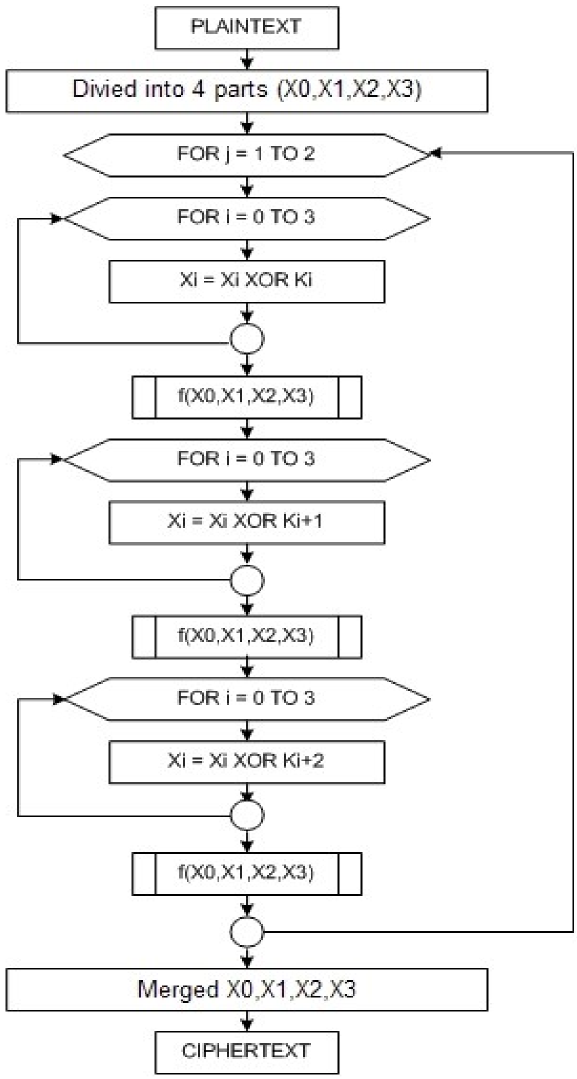

Fig. 3. Decryption MMB Diagram.

3 Results and Discussion

The first experiment is determine the message and key that will be used for the encryption process using the WAKE algorithm.

Plaintext = Modular
Key = researchpapersme
Round key = 1

First step is generate key from key and round, the process are below:

Key 'researchpapersme' change into hex form = 72657365617263687061706572736D65

Split key for 4 part and put in A(0), B(0), C(0) dan D(0).
A(0) = 72657365
B(0) = 61726368
C(0) = 70617065
D(0) = 72736D65

FungsiM(A[0],D[0]) = FungsiM(72657365,72736D65) = (72657365 + 72736D65)>>8 XOR T[(72657365 + 72736D65) AND 255(10)] = E4D8E0CA>>8 XOR T[202] = 00E4D8E0 XOR AD9D8A61 = AD795281
A[1] = AD795281

Key= D[1] = 019790B7

After the key is formed next is to perform the encryption process with WAKE algorithm with the process as follows:

Plain Text : 'Modular'
ASCII 'M' = 4D
ASCII 'o' = 6F
ASCII 'd' = 64
ASCII 'u' = 75
ASCII 'l' = 6C
ASCII 'a' = 61
ASCII 'r' = 72
Plain Text = 4D6F64756C6172

Key = 019790B7

Cipher Text = Plain Text XOR Key
4D XOR 01 = 4C = 'L'
6F XOR 97 = F8 = 'ø'
64 XOR 90 = F4 = 'ô'
75 XOR B7 = C2 = 'Â'
6C XOR 01 = 6D = 'm'
61 XOR 97 = F6 = 'ö'
72 XOR 90 = E2 = 'â'

Ciphertext = LøôÂmöâ

After the ciphertext results WAKE algorithm process then re-encrypted with MMB algorithm using different keys, the use of different keys for each algorithm adds security from ciphertext and complicate cryptanalyst.

Plaintext= LøôÂmöâ
Key=DRAGONBALL SUPER

Change key into binary and split into 4 (four) parts :
K(0) = 01000100010100100100000101000111
K(1) = 01001111010011100100001001000001
K(2) = 01001100010011000010000001010011
K(3) = 01010101010100000100010101010010

Based on the process of encrypting the MMB algorithm according to figure 2 obtained ciphertext as follows:

Result in binary=
1001100101100000011111001110101010111110000100
1100001000111110101010110011111000001101000110
100100100000101111000100100100110000011

Ciphertext = ™`yÕ|&õYðhÒBñ$Ã

Next is determine the media that will be used to insert a message, for example as below:

→

50	**167**	89
80	20	17
25	30	90

Fig. 4. Image with Pixel Value.

The pixel values above assumption are only given to testing steganography with Pixel Value Differencing Algorithm after the pixel values obtained subsequent process can continue by inserting a message with the following steps:

a. Messages to hidden is Ã = 11000011
b. 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 50 and 167.
c.

Table. 1. Pixel value.

50	**167**	89
80	20	17
25	30	90

d. Calculate the value of the second pixel value differencing
e. Finding the location continues the range of score difference value on *wu* and *tsai* scheme
f. Count how many bits of messages that can be inserted into both pixels
g. Changing the value of bits as *t* into a decimal value.
h. Inserting a message by changing the value of the pixel compared with the new pixel value accordance with existing rules
i. Save the new pixel value so as to be like in the figure 5 below:

→

50	**167**	189
80	220	117
125	130	90

Fig. 5. Image with Pixel Value after Insert Message.

Message extraction process can be perform in the same way as the embedded process and using *Wu* and *Tsai* scheme, and then use MMB and WAKE algorithm for decryption process by using key for each algorithm too.

4 Conclusion

WAKE and MMB algorithm on the process of inserting messages in the image with Pixel Value Differencing algorithm can provide a better level of security because the message will be encrypted before it is inserted, and for cryptanalyst takes a very long time to decrypt the ciphertext.

References

1. M. Attaran and I. VanLaar, "Privacy and security on the Internet: how to secure your personal information and company data," Inf. Manag. Comput. Secur., vol. **7**, no. 5, pp. 241–247, (1999)
2. S. Hawkins, D. C. Yen, and D. C. Chou, "Awareness and challenges of Internet security," Inf. Manag. Comput. Secur., vol. **8**, no. 3, pp. 131–143, (2000)
3. R. Rahim, D. Hartama, H. Nurdiyanto, A. S. Ahmar, D. Abdullah, and D. Napitupulu, "Keylogger Application to Monitoring Users Activity with Exact String Matching Algorithm," J. Phys. Conf. Ser., vol. **954**, no. 1, p. 12008, (2018)
4. R. Rahim, I. Zulkarnain, and H. Jaya, "Double hashing technique in closed hashing search process," IOP Conf. Ser. Mater. Sci. Eng., vol. **237**, no. 1, p. 12027, Sep. (2017)
5. H. Nurdiyanto, R. Rahim, and N. Wulan, "Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement," J. Phys. Conf. Ser., vol. **930**, no. 1, p. 12005, Dec. (2017)
6. H. Nurdiyanto and R. Rahim, "Enhanced pixel value differencing steganography with government standard algorithm," *in 2017 3rd International Conference on Science in Information Technology (ICSITech),* pp. 366–371. (2017)
7. A. Putera, U. Siahaan, and R. Rahim, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," Int. J. Secur. Its Appl., vol. **10**, no. 8, pp. 173–180, Aug. (2016)
8. R. Rahim et al., "Combination Base64 Algorithm and EOF Technique for Steganography," J. Phys. Conf. Ser., vol. **1007**, no. 1, p. 12003, Apr. (2018)
9. P. M. Vidhya and V. Paul, "A method for text steganography using malayalam text," in Procedia Computer Science, vol. **46**, pp. 524–531. (2015)
10. E. Kartikadarma, T. Listyorini, and R. Rahim, "An Android mobile RC4 simulation for education," World Trans. Eng. Technol. Educ., vol. **16**, no. 1, pp. 75–79, (2018)
11. R. Rahim et al., "Searching Process with Raita Algorithm and its Application," J. Phys. Conf. Ser., vol. **1007**, no. 1, p. 12004, Apr. (2018)
12. H. Li and P. Liu, "An Identification System Combined with Fingerprint and Cryptography," *in First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06),* pp. 105–108. (2006)
13. R. Rahim and A. Ikhwan, "Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher," Int. J. Sci. Res. Sci. Technol., vol. **2**, no. 6, pp. 71–78, (2016)
14. W. Luo, F. Huang, and J. Huang, "A more secure steganography based on adaptive pixel-value differencing scheme," Multimed. Tools Appl., vol. **52**, no. 2–3, pp. 407–430, (2011)
15. H. Zhang, Q. Guan, and X. Zhao, "Steganography based on adaptive pixel-value differencing scheme revisited," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial

Intelligence and Lecture Notes in Bioinformatics), vol. **8389** LNCS, pp. 32–47. (2014)
16. L. Legito and R. Rahim, "SMS Encryption Using Word Auto Key Encryption," Int. J. Recent Trends Eng. Res., vol. **3**, no. 1, pp. 251–256, (2017)
17. R. Rahim and A. Ikhwan, "Study of Three Pass Protocol on Data Security," Int. J. Sci. Res., vol. **5**, no. 11, pp. 102–104, Nov. (2016)
18. H. Gultom, "Penyandian Email Menggunakan Algoritma Kriptografi WAKE(Word Auto Key Encryption)," Pelita Inform. Budi Darma, vol. **4**, no. 1, pp. 107–111, (2013)