Journal of Computing and Applied Informatics (JoCAI) Vol. 03, No. 2, 2019 | 86 – 94

DATA SCIENCE
Journal of Computing and Applied Informatics

Data Security Using Multi-bit LSB and Modified Vernam Cipher

G T Simbolon[1], Opim Salim Sitompul[2], E B Nababan[3]

[1] *Graduate School of Computer Science*
[2,3] *Department of Information Technology, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Medan, Indonesia*

Abstract. LSB is a steganographic algorithm that is often used to store data in the last bit. Vernam is one of the most popular methods used to encrypt messages easily and quickly. But some possibilities can make LSB and Vernam less safe to use in the long run. Modification of Vernam are made to the bits of each character, the rotation by a certain amount can randomi ze the plaintext content before Vernam encryption is performed. While modifications to the LSB can be performed on some multi-bit models. Bit on LSB can be inserted data as much as 1, 2, 3 or 4-bit information. Based on PSNR and MSE values achieved, 1-bit LSB is superior compare to 2, 3 or 4-bit information.

Keyword: Cryptography, LSB, Steganographic, Vernam Encryption

Abstrak. LSB adalah algoritma steganografi yang sering digunakan untuk menyimpan data pada bit terakhir. Vernam adalah salah satu metode yang sangat populer digunakan untuk mengenkripsi pesan dengan mudah dan cepat. Tetapi beberapa kemungkinan dapat menjadikan LSB dan Vernam tidak begitu aman digunakan dalam waktu jangka panjang.. Modifikasi Vernam dilakukan pada susunan bit tiap karakter, rotasi dengan jumlah terentu dapat mengacak isi plaintext sebelum dilakukan enkripsi Vernam. Sementara itu modifikasi pada LSB dapat dilakukan pada beberapa model multi-bit. Bit pada LSB dapat disisip data sebanyak 1, 2, 3 atau 4-bit informasi. Berdasarkan nilai PSNR dan MSE yang didapat, 1-bit LSB lebih baik dibandingkan dengan informasi 2, 3 dan 4 bit.

Kata Kunci: *Cryptography, LSB, Steganographic, Vernam Encryption*

Received date month year. | Revised date month year | Accepted date month year

1. Introduction

According to the Cisco Visual Networking Index (VNI), the total IP traffic that occurred in 2016 is expected to reach 91.3 exabytes per month. With the amount of traffic this big, the security of data becomes very important. Especially for sensitive data such as enterprise data and information relating to the security of the State [1]. Digital information will be transmitted over the data network indirectly through a small electrical current used as a link to analog signals [2]. Data is very important information that must be secured properly in order to avoid data theft by certain

*Corresponding author at: Department of Information Technology, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Medan, Indonesia

E-mail address: ernabrn@usu.ac.id

ISSN: 2580-6769 | e-ISSN: 2580-829X | DOI: 10.32734/jocai.v3.i2-1048
Journal Homepage: https://jocai.usu.ac.id

parties. Steganography and cryptography are two ways that can be used to secure data and have each way. Steganography performs data hiding, while cryptography performs data security by encrypting plaintext. The crime is growing so that both ways often conceded. Various acts of data theft are done to solve the ciphertext that has been well encrypted. This results in steganographic and cryptographic forces to be enhanced in various ways.

The weakness of this LSB technique is the storage of plaintext bits in a row helps intruders to extract bits of confidential information easily. In this we will improve data security by combining steganography and cryptographic techniques. Vernam algorithm encrypts data by performing XOR operations on each plaintext character by rotating bits. Then the ciphertext will be hidden by the LSB steganography technique on 24-bit imagery by comparing several storage bit models. LSB will hide each bit of information into RGB color elements by creating variations of the LSB technique [2] - [5]. Multi-bits can be determined based on the ability of the image to store the ciphertext into the image. We then calculate MSE (Mean Squared Error) and PSNR (Peak Signal to Noise Ratio) which method obtain the least error rate [6], [7] . The method with least MSE value will improve data security.

2. Methodology

2.1 Modification of Vernam Chiper

In this section we will explain how the Vernam algorithm is modified using bit rotation. During the encryption process the character bit rotation will be left to the left and the key bit rotation to the right. Bit rotation will be done before the XOR operation is performed. When plaintext and the key is given, it will then rotate the position of the 1st to the 8th bit. During the decryption process, the first thing to do is XOR operation between the ciphertext and the key (which has been done right bit rotation), the XOR results are then rotated to the right so that the message returns to its original position (plaintext). Process of modifying Vernam's encryption algorithm is as follow:

Plaintext:

P0	P1	P2	P3	P4

Bit Plaintext:

B07	B06	B05	B04	B03	B02	B01	B00	→	P0
B17	B16	B15	B14	B13	B12	B11	B10	→	P1
B27	B26	B25	B24	B23	B22	B21	B20	→	P2
B37	B36	B35	B34	B33	B32	B31	B30	→	P3
B47	B46	B45	B44	B43	B42	B41	B40	→	P4

1-bit Rotation to Left:

B06	B05	B04	B03	B02	B01	B00	B07	→ P0
B16	B15	B14	B13	B12	B11	B10	B17	→ P1
B26	B25	B24	B23	B22	B21	B20	B27	→ P2
B36	B35	B34	B33	B32	B31	B30	B37	→ P3
B46	B45	B44	B43	B42	B41	B40	B47	→ P4

Key:

K0	K1	K2	K3	K4

Bit Key:

K07	K06	K05	K04	K03	K02	K01	K00	→ K0
K17	K16	K15	K14	K13	K12	K11	K10	→ K1
K27	K26	K25	K24	K23	K22	K21	K20	→ K2
K37	K36	K35	K34	K33	K32	K31	K30	→ K3
K47	K46	K45	K44	K43	K42	K41	K40	→ K4

1-bit rotation to Right:

K00	K07	K06	K05	K04	K03	K02	K01	→ K0
K10	K17	K16	K15	K14	K13	K12	K11	→ K1
K20	K27	K26	K25	K24	K23	K22	K21	→ K2
K30	K37	K36	K35	K34	K33	K32	K31	→ K3
K40	K47	K46	K45	K44	K43	K42	K41	→ K4

Ciphertext / XOR Operation:

B06⊕K00	B05⊕K07	B04⊕K06	B03⊕K05	B02⊕K04	B01⊕K03	B00⊕K02	B07⊕K01	→ C0
B16⊕K10	B15⊕K17	B14⊕K16	B13⊕K15	B12⊕K14	B11⊕K13	B10⊕K12	B17⊕K11	→ C1
B26⊕K20	B25⊕K27	B24⊕K26	B23⊕K25	B22⊕K24	B22⊕K23	B20⊕K22	B27⊕K21	→ C2
B36⊕K30	B35⊕K37	B34⊕K36	B33⊕K35	B32⊕K34	B31⊕K33	B30⊕K32	B37⊕K31	→ C3
B46⊕K40	B45⊕K47	B44⊕K46	B43⊕K45	B42⊕K44	B41⊕K43	B40⊕K42	B47⊕K41	→ C4

Therfore the process of modifying Vernam's decryption algorithm:

Ciphertext:

C0	C1	C2	C3	C4

2.2 Multi-bit LSB

Multi-bit LSB is done with several bit insertion models. Following are the steps carried out in the multi-bit LSB process, by inserting messages in specified bits on three elements of color (Red, Green and Blue) in each pixel.

Character storage on 1-bit LSB:

R	7	6	5	4	3	2	1	0
G	7	6	5	4	3	2	1	0
B	7	6	5	4	3	2	1	0
R	7	6	5	4	3	2	1	0
G	7	6	5	4	3	2	1	0
B	7	6	5	4	3	2	1	0
R	7	6	5	4	3	2	1	0
G	7	6	5	4	3	2	1	0

Character storage on 2-bits LSB:

R	7	6	5	4	3	2	1	0
G	7	6	5	4	3	2	1	0
B	7	6	5	4	3	2	1	0
R	7	6	5	4	3	2	1	0

Character storage on 3-bits LSB:

R	7	6	5	4	3	2	1	0
G	7	6	5	4	3	2	1	0
B	7	6	5	4	3	2	1	0

Character storage on 4-bits LSB:

R	7	6	5	4	3	2	1	0
G	7	6	5	4	4	2	1	0

The four patterns above save as much as 1 character (8 bits). The more bits used, the less number of pixels used as information storage. 1-bit storage uses less than 3 pixels, on 2-bit storage using less than 2 pixels, 3-bit storage uses exactly 1 pixel and 4-bit storage also uses 1 pixel. In empty

color elements can be stored for the next character or can be skipped and restarted on the next color pixel element, which is Red.

2.3 Calculation of MSE and PSNR

The image used is 24-bit color image. The calculation of MSE and PSNR aims to determine how much the image changes after message insertion. There is 1-bit storage up to 4-bit LSB to be performed, each stego-image will be calculated MSE and PSNR values to determine which image is better or how many better bits to store information or messages. The following is the formula used to calculate MSE and PSNR.

$$MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} (f(i,j) - g(i,j))^2 / M * N \quad (1)$$

Information:

MSE = The MSE value of image

M = Image of length

N = Image of width

f (i,j) = The pixel coordinate value of the image before the message is inserted

g (i,j) = The pixel coordinate value of the image after the message is inserted

Example:

Table 3.1 RGB Pixel

Red			Green			Blue		
R1	...	Rn	G1	...	Gn	B1	...	Bn

$$\text{MSE} = \frac{1}{M*N}$$
$$\left(\frac{(R_1' - R_1)^2 + \cdots + (R_n' - R_n)^2 + (G_1' - G_1)^2 + \cdots + (G_n' - G_n)^2 + (B_1' - B_1)^2 + \cdots + (B_n' - B_n)^2}{3}\right)$$

$$PSNR = 10 \log_{10}\left(\frac{C^2_{max}}{MSE}\right) \quad (2)$$

Information:

PSNR = The PSNR value of image

C^2_{max} = The highest pixels of the RGB image

3. Result and Discussion

This section will test the success of combining steganography and cryptography with modifications made. This test with 1-bit rotation and determines the MSE and PNSR values of each stego-image. Examples of images used are 4 x 4 pixels. This image can accommodate as many as 48-bits. If converted to characters, it can accommodate as many as 6 characters for the use of 1 bit. The following tests are carried out on this method.

Plaintext : Secret

83	101	99	114	101	116
01010011	01100101	01100011	01110010	01100101	01110100

Rotation : 1-bit to the left

10100110	11001010	11000110	11100100	11001010	11101000
166	202	198	228	202	232

Key : World

87	111	114	108	100
01010111	01101111	01110010	01101100	01100100

Rotation : 1-bit to the right

10101011	10110111	00111001	00110110	00110010
171	183	57	54	50

Ciphertext : -}ÿÊ°C

13	125	255	210	248	67

The results of the ciphertext will be stored in an image with several bit storage models, such as the following illustration. In this test, an image piece of 4 x 4 pixels will be taken as a cover image. The capacity that can be accommodated by this image is 4 x 4 x 3 bits = 48 bits (6 characters) on the use of 1 bit.

RGB bit for the 4 x 4 pixel cover image:

Red			
65	58	187	190
222	171	203	63

Green			
87	176	149	241
223	74	221	68

Blue			
116	249	167	229
150	134	191	182

246	101	32	89
192	151	36	11

205	204	143	53
125	130	167	60

128	84	243	163
226	101	153	23

:

The ciphertext bit that will be inserted: -}ÿÊ°C

00001101	01111101	11111111	11010010	11111000	01000011

Stego-image results on 1-bit LSB:

Red			
64	58	**186**	**191**
223	171	203	63
247	101	**33**	89
193	**150**	36	**10**

Green			
86	**177**	149	241
223	**75**	221	**69**
205	204	**142**	53
124	130	**166**	**61**

Blue			
116	249	**166**	229
150	**135**	191	**183**
128	84	243	163
226	101	**152**	23

MSE = $\frac{1}{16}(7)$

= 0,4375

PSNR = $10 * Log10\left(\frac{249^2}{0,4375}\right)$

= 51,5142

Stego-image results on 2-bit LSB:

Red			
64	**57**	187	**191**
223	**170**	**202**	**60**
246	101	32	89
192	151	36	11

Green			
84	**177**	149	**243**
221	**75**	**220**	68
205	204	143	53
125	130	167	60

Blue			
119	**251**	167	**231**
148	**135**	**189**	**183**
128	84	243	163
226	101	153	23

MSE = $\frac{1}{16}(10,67)$

= 0,6667

PSNR = $10 * Log10\left(\frac{249^2}{0,6667}\right)$

= 49,6846

Stego-image results on 3-bit LSB:

Red			
64	**63**	**191**	**188**
220	171	203	63
246	101	32	89
192	151	36	11

Green			
83	**182**	**151**	**246**
218	74	221	68
205	204	143	53
125	130	167	60

Blue			
113	**255**	**166**	**231**
144	134	191	182
128	84	243	163
226	101	153	23

MSE = $\frac{1}{16}$ (18)

= 1,125

PSNR = $10 * Log10\left(\frac{249^2}{1,125}\right)$

= 47,4142

Stego-image results on 4-bit LSB:

Red			
64	**61**	**189**	**184**
222	171	203	63
246	101	32	89
192	151	36	11

Green			
93	**191**	**146**	**244**
223	74	221	68
205	204	143	53
125	130	167	60

Blue			
119	**255**	**175**	**227**
150	134	191	182
128	84	243	163
226	101	153	23

MSE = $\frac{1}{16}$ (19,333)

= 1,2083

PSNR = $10 * Log10\left(\frac{249^2}{1,2083}\right)$

= 47,1022

Information:

Bold and underlined pixel bits are pixel bits that have been inserted into the message. In 1-bit LSB storage more image pixels are used because each RGB color element can only store 1-bit. For storing 4-bit LSB fewer pixels are used because each RGB color element can store 4-bit ciphertext.

4. Conclusion

The level of data security is increased by combining steganographic techniques with cryptographic algorithms. Image resolution for the cover image and character length of the message, greatly affect the value of the MSE and PSNR parameters. Seeing the results of the calculation of MSE and PSNR, the use of 1-bit LSB is much better than 2, 3 or 4-bit. This happens because the MSE value in 1-bit is much smaller and also the PSNR value is above 40 db. The use of 2-bit can still be considered to obtain good results because the value of MSE is still small and the PSNR still remains above the stipulated value. The implementation of the multi-bit LSB method in steganography activities provides advantages where each pixel can hold more message bits than the usual LSB method.

REFERENCES

[1] Cisco Visual Networking Index. 2017. Forecast and Methodology. *cisco.com*, http://www.cisco.com/c/en/us/solutions/collateral/ service-provider/ip-ngn-ip-next-generation-network/white_ paper_c11-481360.html. [Accessed: 30-Mar-2018]

[2] B. Datta, P. K. Pal, and S. K. Bandyopadhyay, "Multi-bit Data Hiding in Randomly Chosen LSB Layers of an Audio," in *2016 International Conference on Information Technology (ICIT)*, 2016, pp. 283–287.

[3] M. Kaur and M. Juneja, "A new LSB embedding for 24-bit pixel using multi-layered bitwise XOR," in *2016 International Conference on Inventive Computation Technologies (ICICT)*, 2016, pp. 1–5.

[4] R.-J. Chen, Y.-C. Chen, Jui-Linlai, and S.-J. Horng, "Data Hiding Using Flexible Multi-bit MER," in *2013 International Symposium on Biometrics and Security Technologies*, 2013, pp. 24–31.

[5] S. Goel, S. Gupta, and N. Kaushik, "Image Steganography – Least Significant Bit with Multiple Progressions," 2015, pp. 105–112.

[6] "The Vernam Cipher," *Crypto Museum*. [Online]. Available: http://www.cryptomuseum.com/crypto/vernam.htm.

[7] C. . B. S., P. K., and R. D. K., "Least Significant Bit Algorithm for Image Steganography," *Int. J. Adv. Comput. Technol.*, vol. 3, no. 4, pp. 34–38, 2014.