Analysis of Security Level Image Steganography Using Secret Key and Gray Codes

Danny Sihombing[1], Poltak Sihombing[1] and Rahmat Widia Sembiring[1]
{dani_aseven@yahoo.com}

[1]Department of Computer Science, Universitas Sumatera Utara, Medan, Indonesia

Abstract. In Dagar et al (2013) research, message concealment into grayscale image file with Least Significant Bit (LSB) algorithm, where before it is inserted, the message is encrypted with function SN function and converted into binary value from gray code. The result of this research is that resistance to image manipulation is entered into intermediate level where the stego image of insertion result is not resistant to compression and addition of brightness. So in this study suggested to increase data security, resistance to image manipulation and efficiently hide data and time of extraction. In this research we have done Analysis of Security Level of Image Steganography Using Secret Key and Gray Codes with result obtained that on MSE parameter and image size, SNS Function Gray MLSB algorithm has image with MSE and the smallest file size compared to SN Function Gray LSB algorithm has an image with MSE and the largest file size. For process time parameters, it is concluded that each algorithm has almost the same processing time depending on the size of the image and the message to be inserted. SN Function Gray MLSB algorithm based on MSE parameter shows that, process time and image size is better than SN Function Gray LSB algorithm.

Keywords: Cryptography, Steganography, Least Significant Bit algorithm, Modified Least Significant Bit.

1. Introduction

In Dagar et al (2013) research, message concealment into grayscale image file with Least Significant Bit (LSB) algorithm, where before it is inserted, the message is encrypted with function SN function and converted into binary value from gray code. The inserted image format is the BMP format with grayscale color mode. The result of this research is resistance to image manipulation is entering into middle level, meaning stego image insertion result can not stand against compression, addition of brightness and other image processing. In this study it is suggested to add data security, resilience to image manipulation and efficient in the ability to hide data, data insertion and time of extraction.

In this research, data security will be improved on Dagar et al research by encrypting text data using Secret Key and Gray Codes algorithm and inserting ciphertext into image file (cover image) with MLSB algorithm. The insertion is performed on pixels that are randomized in RGB color

WMA-1 2018, January 20-21, Indonesia

DOI 10.4108/eai.20-9-2019.160761

mode. So if the steganalysis is about to detect the embed, then the embed can not know the location of the pixel and its contents are still in the encrypted state.

2. Sn Function And Gray Code

Gray-code or also known as reflected binary code named by Frank Gray. Gray code is a binary numbering system where two adjacent values only have exactly one digit difference. Gray-code was originally used to prevent the false output of an electromechanical signal. Today, Gray-code is used extensively to facilitate error correction in digital communications.

In the hiding data is encrypted using a symmetric key (ks) which is known to both sender and receiver. Data is encrypted using SN function which uses gray code and symmetric key. The main advantage of SN function is that it can encrypt the plain text as well as decrypt the cipher text with small changes. So in this way SN function is very easy to understand and implement (Dagar et al2013).

The SN Function cryptography algorithm is a Gray Code function algorithm in binary form that uses incrementing methods that differ from one digit to the next (Varalakshmi, R. & Uthariaraj, V. R. 2013). Gray Code is the most popular type of absolute output encoder because its use prevents certain data errors that can occur with Natural Binary during changing circumstances.

For example, in highly capacitive circuits or sluggish system responses, a natural binary state change from condition 0011 to 0100 can cause counters to look like a 0111. This kind of error is not possible with Gray Code, so the data is more reliable. With a gray code, only one bit changes from one position to another. This feature allows the system designer to check the error that if more than one bit changed, then the data can be said not true. The respresentation of decimal numbers, natural binary and Gray Code can be seen as in Table 1.

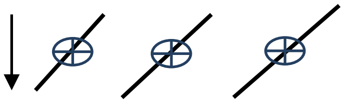
Decimal	Natural Binary	Gray Code
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111

Table 1. Decimal Representation, Natural Binary and Gray Code

Conversion from Gray Code to Binary Code

Let Gray Code be g3 g2 g1 g0. Then the respective Binary Code can be obtained as follows:

Gray code : g_3 g_2 $g_1 g_0$



Binary code : b_3 b_2 b_1 b_0

(g_3) $(b_3 \oplus g_2)$ $(b_2 \oplus g_1)$ $(b_1 \oplus) g_0$

Let Binary code be b3 b2 b1 b0. Then the respective Gray Code can be obtained is as follows

Binary code : $b_3 \oplus b_2$ b_1 b_0

Gray code : $g_3 g_2$ g_1 g_0

(b_3)(b3 ⊕b2) (b2 ⊕b1) (b1 b0⊕)

1. Modifiedleast Significant Bit (MLSB)

Modified Least Significant Bit (MLSB) or modification of the LSB algorithm is used to encode an identity into a file. MLSB uses the manipulation of several levels of insertion bits before encoding the message (Zaher, 2011).Modify messages with MLSB algorithm where message bits that should have 1 character have an 8 bit ASCII code will be modified to 5 bits. In this algorithm characters and numbers are represented in 5 bits which will then be inserted into the original file by LSB technique. The insertion is done by processes:

1. The process of altering insert data with ASCII code. For example the message "STEGO with 05 bits" which if converted to binary requires memory of 18 x 8 bits = 144 bits. In the MLSB algorithm the above message is converted to ASCII (hex) to: 53h, 54h, 45h, 47h, 4fh, 20h, 77h, 69h, 74h, 68h, 20h, 30h, 35h, 20h, 62h, 69h, 74h, 73h. Then done normalization with table Control Symbol like Table 2.

Table 2. Control Symbol

Hex Representation	Operation
1 Bh	Define Small Letter
1 Ch	Define Capital Letter
1 Dh	Define Space
1 Eh	Define Number
1 Fh	Define end of text

2. Read the insertion data (ASCII) until the space mark (20h) is 53, 54, 45, 47, 4f.
3. All values are reduced by the lowest value of 40 to 53-40 = 13, 54-40 = 14, 45-40 = 05, 47-40 = 07, 4f-40 = f.
4. The first group insertion data is 1ch, 13h, 14h, 05h, 07h, 0f where 1ch is the Control Symbol for uppercase (capital).
5. The second group insertion data is 77h, 69h, 74h, 68h reduced by the lowest value (60) to 77-60 = 17, 69-60 = 09, 74-60 = 14, 68-60 = 08.
6. The second group data is combined with the first group and assigned a Control Symbol 1dh (space) and 1bh (lowercase) to 1dh, 1bh, 17h, 09h, 14h, 08h.
7. The third group data are: 30h, 35h minus the lowest value being: 30-30 = 0, 35-30 = 05.
8. The data is combined with the previous group plus Control Symbol 1dh (space), 1eh (number) to 1dh, 1eh, 00h, 05h.
9. The data of the fourth group are: 62h, 69h, 74h, 73h reduced by the lowest value to: 62-60 = 02, 69-60 = 09, 74-60 = 14, 73-60 = 13.
10. The data is combined with the previous group plus Control Symbol 1bh (lowercase), into 1dh, 1bh, 02h, 09h, 14h, 13h and end of data (1fh).

So the message becomes:
1ch, 13h, 14h, 05h, 07h, 0hh, 1hh, 08h, 1hh, 1h, 00h, 05h, 1bh, 02h, 09h, 14h, 13h, 1fh. The above message requires 22 x 5 bits = 110 bits and converted to binary to:
11100, 10011, 10100, 00101, 00111, 01111, 11101, 11011, 10111, 01001, 10100, 01000, 11101, 11110, 00000, 00101, 11011, 00010, 01001, 10100, 10011, 11111.

2. Method Of Analysis

In this research, the analysis adds data security level to image file with cryptography technique and steganography on Dagar et al. Secured data in the form of secret text that is inserted into digital image files that are in BMP, JPG or PNG format with Modified Least Significant Bit (Modified-LSB) algorithm. Before being inserted, secret text is encrypted with SN function algorithm using Gray Code. As a comparison in this study, data security is done by SN encryption algorithm with Gray Code and insertion with Least Sifnificant Bit (LSB) algorithm. To measure the reliability of the insertion of each algorithm, measurements of size, dimensions, Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) values of the stego image were measured. And to measure the reliability of data acquisition embed, then calculate the value of Data Recovery Rate (DRR) as the value of extraction.

The Flowchart Research consists of two parts namely the flowchart insertion and extraction. Flowchart Insertion is a process flow for inserting text files into image media (cover image) to generate stego image, while flowchart Extraction is a process flow to extract insert data from stego image. Flowchart insertion can be seen as in Figure 1.

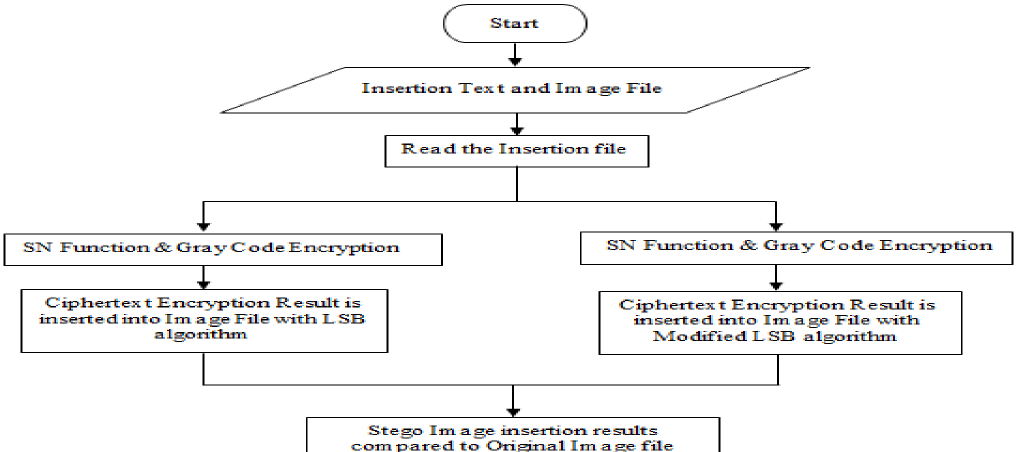

Start
Insertion Text and Image File
Read the Insertion file
SN Function & Gray Code Encryption
SN Function & Gray Code Encryption
Ciphertext Encryption Result is inserted into Image File with LSB algorithm
Ciphertext Encryption Result is inserted into Image File with Modified LSB algorithm
Stego Image insertion results compared to Original Image file

Figure 1. Flowchart Insertion

Information:
In the flowchart above there are two paths of encryption and insertion process are:

1. Encryption algorithm SN function Gray Code LSB

In this algorithm is inserted data input txt format, then do the reading file to get data and then done by encryption to insert with LSB algorithm to get ciphertext file. The ciphertext file obtained is inserted into the image file with MLSB algorithm and then calculated the value of MSE and PSNR the stego image file obtained.

2. Encryption algorithm SN function and Gray Code Modified-LSB

In this algorithm input data input inserted txt format, then do the reading file to obtain data and then done by encryption to insert with Modified-LSB algorithm to get ciphertext file. The ciphertext file obtained is inserted into the image file with the Modified-LSB algorithm and then the MSE and PSNR values of the stego image file are obtained. Flowchart Extraction of insert data from the stego image file can be seen as in Figure 2.

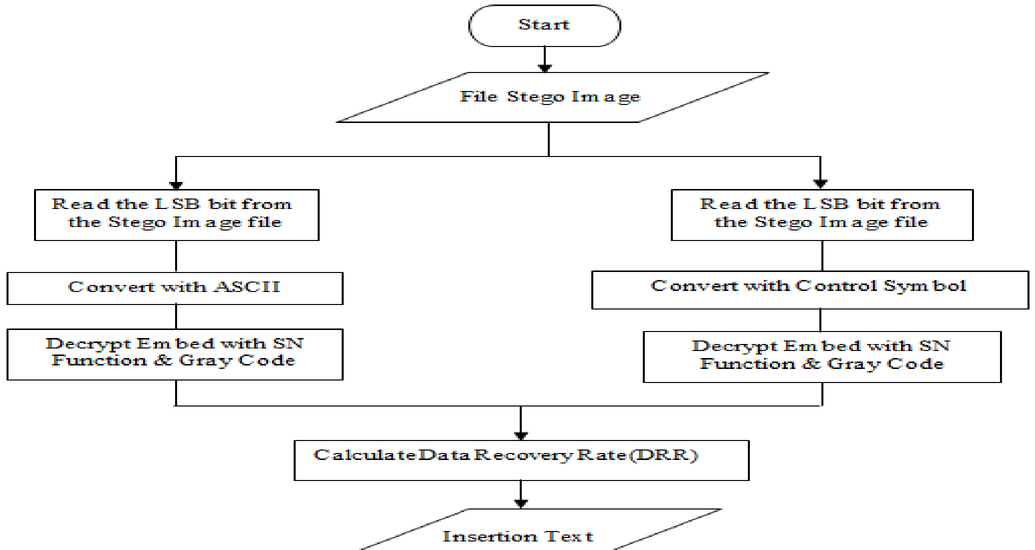

Start
File Stego Image
Read the LSB bit from the Stego Image file
Read the LSB bit from the Stego Image file
Convert with ASCII
Convert with Control Symbol
Decrypt Embed with SN Function & Gray Code
Decrypt Embed with SN Function & Gray Code
Calculate Data Recovery Rate (DRR)
Insertion Text

Figure 2. Flowchart Extraction

Information:
In the flowchart above the input stego image file that has been inserted, then read LSB bits and and converted into ASCII and Control Symbol. After conversion, the embedded decryption is done with SN Function and Modified-LSB algorithm to obtain the data of encrypted bits, then done decryption process to the insert file to get the plaintext and then calculate the value of Data Recovery Rate (DRR) as the extraction value.

3. Insertion of Sn Function and Gray Code Lgorithms

The insertion algorithm with SN Function and Gray Code is the insertion of the text of a secret message into a digital image file in BMP, JPG or PNG format with the LSB algorithm. Before being inserted, the first text message is encrypted using Gray Code and SN Function. The insertion steps with SN Function and Gray Code are as follows:

1. For example, the pixel value of the cover image is 8 x 5 pixels as shown in Table 3.

Table 3. Cover Image Matrix

50	10	60	50	58	40	44	12
10	52	40	20	34	74	30	87
12	24	45	25	60	28	20	77

10	60	40	30	54	32	24	85
12	55	22	24	33	45	37	110

2. Convert insert text into binary value, for example the text is "DANI" with binary is:

D = 01000100
A = 01000001
N = 01001110
I = 01001001

3. Formation of Ciphertext Gray Code with SN Function Encryption

Plain Text D is 01000100

Key 10011001

Encryption: (Plain Text) XNOR (Key) (same equals = 1 else 0)

```
            01000100
   XNOR   10011001
            00100010
```

Gray code for 00100010 is 00110011

Cipher text D = 00110011

So cipherteks "DANI" is 00110011 01000001 00111100 00111000. Binary messages are inserted into an Image cover file as in Table 4.

Table 4. Cover Image Matrix

50	10	60	50	58	40	44	12
10	52	40	20	34	74	30	87
12	24	45	25	60	28	20	77
10	60	40	30	54	32	24	85
12	55	22	24	33	45	37	110

4. Convert The image cover pixel value in Table 4 above is converted into binary into Table 5.

Table 5. Binary Image Cover Image Matrix

00110010	00001010	00111100	00110010	00111010	00101000	00101100	00001100
00001010	00110100	00101000	00010100	00100010	01001010	00011110	01010111
00001100	00011000	00100101	00011001	00111100	00011100	00010100	01001101
00001010	00111100	00101000	00011110	00110110	00100000	00011000	01010101
00001100	00110111	00010110	00011000	00100001	00101101	00100101	00110010

5. The insertion is done by the LSB method on each byte on the rear binary value (LSB) as in Table 6.

Table 6. Binary Image Matrix Stego Image

0011001**0**	0000101**0**	0011110**1**	0011001**1**	0011101**0**	0010100**0**	0010110**1**	0000110**0**
0000101**0**	0011010**0**	0010100**1**	0001010**0**	0010001**1**	0100101**1**	0001111**1**	0101011**1**
0000110**0**	0001100**0**	0010010**1**	0001100**1**	0011110**1**	0001110**0**	0001010**0**	0100110**0**
0000101**0**	0011110**0**	0010100**1**	0001111**1**	0011011**0**	0010000**1**	0001100**1**	0101010**1**
0000110**0**	0011011**0**	0001011**1**	0001100**1**	0010000**1**	0010110**0**	0010010**1**	0011001**1**

After insertion, the representation of the stego image pixel value becomes as in Table 7.

Table 7. Grayscale Image Stego Image Matrix

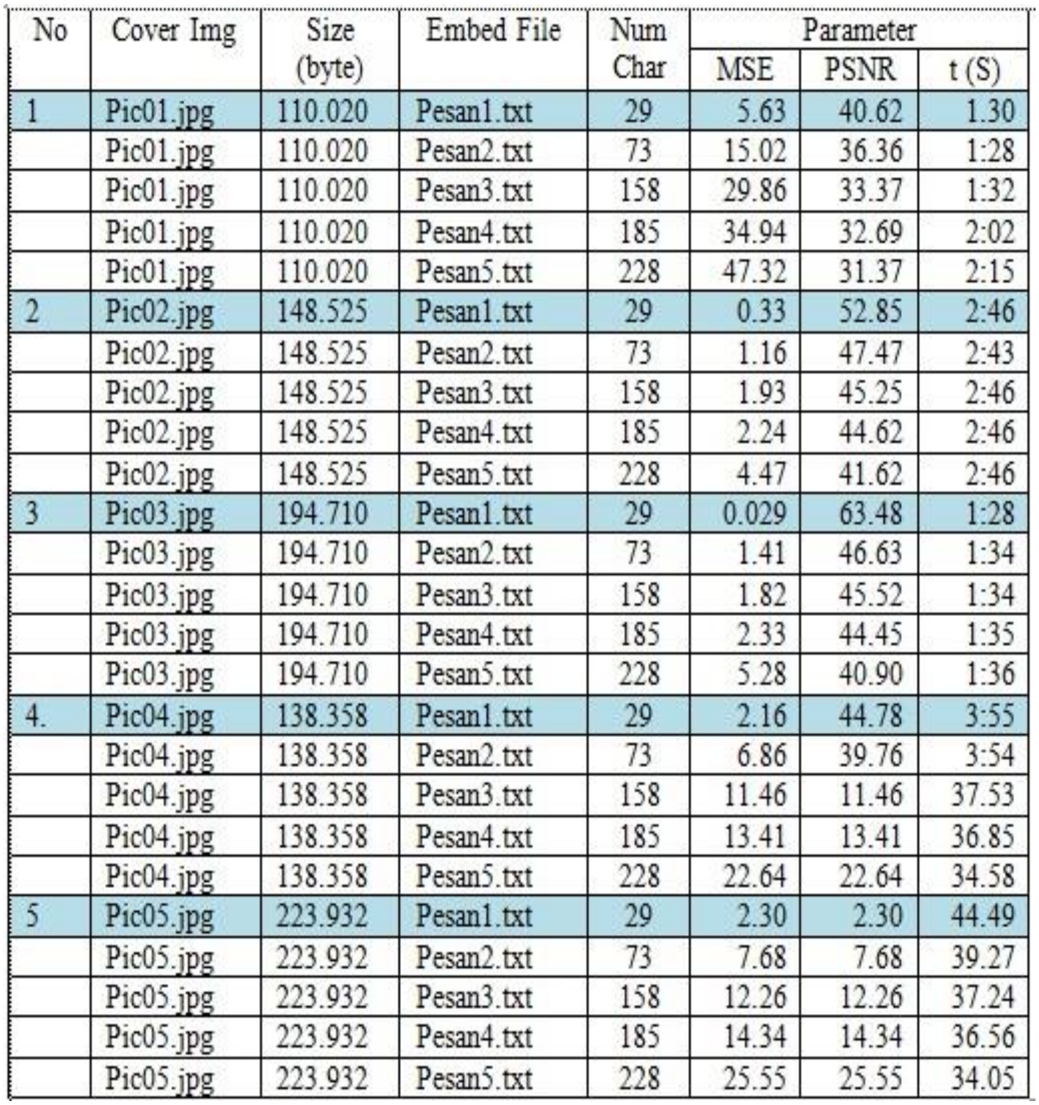
50	10	61	51	58	40	45	13
10	52	41	20	35	75	31	87
12	24	45	25	61	28	20	76
10	60	41	31	54	33	25	85
12	54	23	25	33	44	37	111

4. Findings And Discussion

The analysis by the author of the security level analysis of Image Steganography using Secret Key & Gray Codes is to increase the level of data security into image files with cryptographic and steganographic techniques as in the research of Dagar, Kumar and Bagoriya. Secured data in the form of secret text that is inserted into digital image files that are in BMP, JPG or PNG format with the Modified Least Significant Bit (MLSB) algorithm where before being inserted, secret text is encrypted with Secret Key & Gray Codes algorithm.For comparison, data is inserted into digital image files in BMP, JPG or PNG format with Least Significant Bit (LSB) algorithm and prior to being inserted, in secret text encryption with SN function using Gray Code.

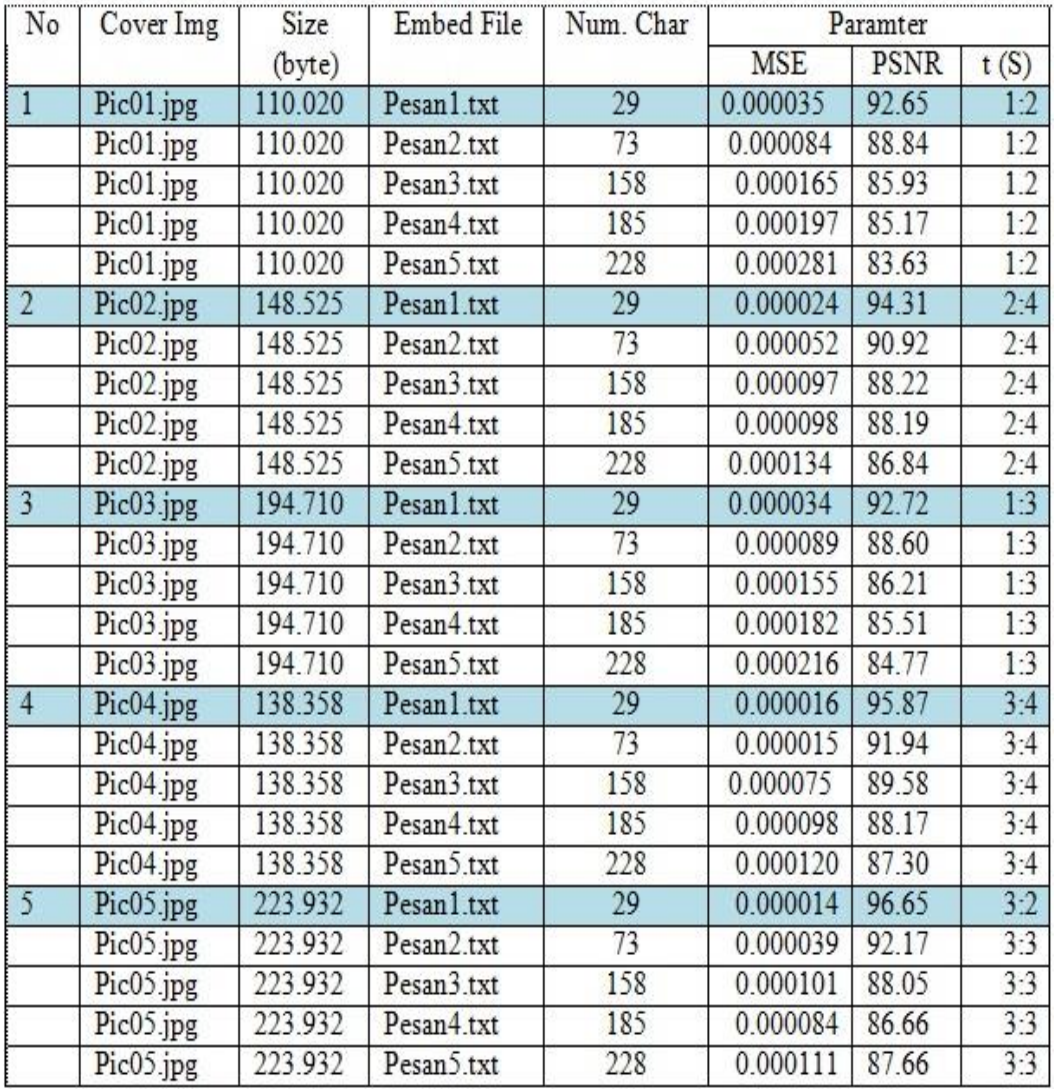
The test is performed using five different sized digital images where each image will be inserted with five different text watermarks. The parameters to be obtained are the MSE, the length of the process and the result file size. From the test results obtained as shown in Table 8. and Table 9.

Table 8. Results of Steganographic Insertion of GrayKey SN Function LSB



No	Cover Img	Size (byte)	Embed File	Num Char	Parameter		
					MSE	PSNR	t (S)
1	Pic01.jpg	110.020	Pesan1.txt	29	5.63	40.62	1.30
	Pic01.jpg	110.020	Pesan2.txt	73	15.02	36.36	1:28
	Pic01.jpg	110.020	Pesan3.txt	158	29.86	33.37	1:32
	Pic01.jpg	110.020	Pesan4.txt	185	34.94	32.69	2:02
	Pic01.jpg	110.020	Pesan5.txt	228	47.32	31.37	2:15
2	Pic02.jpg	148.525	Pesan1.txt	29	0.33	52.85	2:46
	Pic02.jpg	148.525	Pesan2.txt	73	1.16	47.47	2:43
	Pic02.jpg	148.525	Pesan3.txt	158	1.93	45.25	2:46
	Pic02.jpg	148.525	Pesan4.txt	185	2.24	44.62	2:46
	Pic02.jpg	148.525	Pesan5.txt	228	4.47	41.62	2:46
3	Pic03.jpg	194.710	Pesan1.txt	29	0.029	63.48	1:28
	Pic03.jpg	194.710	Pesan2.txt	73	1.41	46.63	1:34
	Pic03.jpg	194.710	Pesan3.txt	158	1.82	45.52	1:34
	Pic03.jpg	194.710	Pesan4.txt	185	2.33	44.45	1:35
	Pic03.jpg	194.710	Pesan5.txt	228	5.28	40.90	1:36
4.	Pic04.jpg	138.358	Pesan1.txt	29	2.16	44.78	3:55
	Pic04.jpg	138.358	Pesan2.txt	73	6.86	39.76	3:54
	Pic04.jpg	138.358	Pesan3.txt	158	11.46	11.46	37.53
	Pic04.jpg	138.358	Pesan4.txt	185	13.41	13.41	36.85
	Pic04.jpg	138.358	Pesan5.txt	228	22.64	22.64	34.58
5	Pic05.jpg	223.932	Pesan1.txt	29	2.30	2.30	44.49
	Pic05.jpg	223.932	Pesan2.txt	73	7.68	7.68	39.27
	Pic05.jpg	223.932	Pesan3.txt	158	12.26	12.26	37.24
	Pic05.jpg	223.932	Pesan4.txt	185	14.34	14.34	36.56
	Pic05.jpg	223.932	Pesan5.txt	228	25.55	25.55	34.05

Table 9. Insertion Results of GrayKey SN Function Modified-LSB Steganography



No	Cover Img	Size (byte)	Embed File	Num. Char	Paramter		
					MSE	PSNR	t (S)
1	Pic01.jpg	110.020	Pesan1.txt	29	0.000035	92.65	1:2
	Pic01.jpg	110.020	Pesan2.txt	73	0.000084	88.84	1:2
	Pic01.jpg	110.020	Pesan3.txt	158	0.000165	85.93	1.2
	Pic01.jpg	110.020	Pesan4.txt	185	0.000197	85.17	1:2
	Pic01.jpg	110.020	Pesan5.txt	228	0.000281	83.63	1:2
2	Pic02.jpg	148.525	Pesan1.txt	29	0.000024	94.31	2:4
	Pic02.jpg	148.525	Pesan2.txt	73	0.000052	90.92	2:4
	Pic02.jpg	148.525	Pesan3.txt	158	0.000097	88.22	2:4
	Pic02.jpg	148.525	Pesan4.txt	185	0.000098	88.19	2:4
	Pic02.jpg	148.525	Pesan5.txt	228	0.000134	86.84	2:4
3	Pic03.jpg	194.710	Pesan1.txt	29	0.000034	92.72	1:3
	Pic03.jpg	194.710	Pesan2.txt	73	0.000089	88.60	1:3
	Pic03.jpg	194.710	Pesan3.txt	158	0.000155	86.21	1:3
	Pic03.jpg	194.710	Pesan4.txt	185	0.000182	85.51	1:3
	Pic03.jpg	194.710	Pesan5.txt	228	0.000216	84.77	1:3
4	Pic04.jpg	138.358	Pesan1.txt	29	0.000016	95.87	3:4
	Pic04.jpg	138.358	Pesan2.txt	73	0.000015	91.94	3:4
	Pic04.jpg	138.358	Pesan3.txt	158	0.000075	89.58	3:4
	Pic04.jpg	138.358	Pesan4.txt	185	0.000098	88.17	3:4
	Pic04.jpg	138.358	Pesan5.txt	228	0.000120	87.30	3:4
5	Pic05.jpg	223.932	Pesan1.txt	29	0.000014	96.65	3:2
	Pic05.jpg	223.932	Pesan2.txt	73	0.000039	92.17	3:3
	Pic05.jpg	223.932	Pesan3.txt	158	0.000101	88.05	3:3
	Pic05.jpg	223.932	Pesan4.txt	185	0.000084	86.66	3:3
	Pic05.jpg	223.932	Pesan5.txt	228	0.000111	87.66	3:3

5. Conclusion

Based on comparison of SN Function Gray LSB and SN Function Gray MLSB algorithm on three comparison parameters: MSE image, process time and image size obtained that on MSE parameter and image size, SN Function Gray MLSB algorithm has image with MSE and the smallest file size compared to the SN Function Gray LSB algorithm that has the image with MSE and the largest file size. For process time parameters, it is concluded that each algorithm has the same processing time depends on the size of the image and the message to be inserted. SN Function Gray MLSB algorithm data show that based on MSE image parameter, process time and image size is above SN Function Gray LSB algorithm.

References

[1] Gonzalez, R.C. & Woods, R.E. 2003. *Digital Image Processing*. third edition, USA: Addison-Wesley Publishing Co, University of Tennessee.

[2] Sridevi, R. Damodaram, A. & Narasimham. 2005. *Efficient Method Of Audio Steganography by Modified LSB Algorithm And Strong Encryption Key With Enhanced Security*. Journal of Theoretical and Applied Information Technology, Vol 37, No 22. Jntuceh, Hyderabad India. Maret 2005 : 768-771.

[3] Zaher, M.A. 2011. *Modified Least Significant Bit (MLSB)*. Jurnal Computer and Information Science Vol. 4, No. 1, Januari 2011. www.ccsenet.org/cis. Diakses tanggal 15 Maret 2012 : 60-67.

[4] Dagar, S., Kumar, V. & Bagoriya Y. 2013. *Image Steganography using Secret Key & Gray Codes*. (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013.

[5] Shreya, M.S. & Khumar, S. 2013. *Separable Reversible Data Hiding In Encrypted Image Using Modified Least Significant Bit and Virtual Embedding*. *International Journal of Science and Research*. Volume 4, Issue 4, April 2015 : 3099-3106.

[6] Hammood, D.A. 2013. *Breaking A Playfair Cipher Using Memetic Algorithm*. Journal of Engineering and Development, Vol. 17, No.5, November 2013. College of Elec. & Electronic Techniques Foundation of Technical Education.

[7] Prasetiyo, B. 2013. Kombinasi Steganografi Bit Matchingdan Kriptografi DES untuk Pengamanan Data. Tesis. Universitas Diponegoro : Semarang.

[8] Sentilkumar, M. & Mathivanan, V. 2016. Analysis of Data Compression Tecniques using Huffman Coding and Arithmetic Coding. *International Journal of Advanced Research in Computer Science and Software Engineering*. Vol. 6, Issue 5, May 2016 : 930-936.

[9] Singh, S. & Siddiqui, T.J. 2012. A Security Enhanced Robust Steganography Algorithm for Data Hiding. *International Journal of Computer ScienceIssues*. Volume 9, Issue 3, No. 1, May 2012 : 131-139.

[10] Husain, M.P. & Rafat, K.F. 2016. Enhanced Audio LSB Steganography for Secure Communication. International Journal of Advanced Computer Science and Aplications,Vol. 7, No. 1 : 340-347.

[11] Kaul, N. , Bajaj, N. 2013. Audio in Image Steganography based on Wavelet Transform. International Journal of Computer Application. Vol. 79- No. 03, October 2013: 7-10.

[12] Varalakshmi, R. & Uthariaraj, V. R. 2013. *Error Correction for a Secure Multicast Group Key Management using Gray Code*. International Journal of Computer Applications (0975 – 8887) Volume 66– No.1, March 2013. Ramanujan Computing Centre, Anna University Chennai, Tamil Nadu, India.