High Complexity with Steganography in LSB and MSB

Salam R. Mahdi , Yahia Najar, Mahmood Shaar
Department of Computer Engineering Electronic College
University of Aleppo. Syria

ABSTRACT: *Steganography is a modern, yet ancient, method of secret storage and access of communication, in contrast to cryptography, where the "enemy" is permitted to detect, intercept and modify messages without being able to violate certain security premises protected by the cryptosystem. Steganography is an art and a science. in our previous research, we showed that we had been able to hid information in every bit of every byte in the cover without condition or restriction, and by extracting the complete hidden message with high complexity proportionate to the length of the cover and the number of position in the color values, and hiding the number of positions in the color values, and hiding the number of the sites in the color values. Our new research shows that the information hidden in the eighth position is not in a position with higher security than the first position because the Steganography I the first or eighth bit (as one it) of the cover has the same values of complexity. Our research also makes clear the integrity of the cover when hidden in Least Significant Bit (LSB) and Most Significant Bit (MSB).*

Keywords: Steganography, Least Significant Bit, Most Significant Bit (MSB). Cryptosystem

Received: 19 February 2012, Revised 314 March 2012, Accepted 7 April 2012

1. Introduction

Information hiding represents a class of processes used to embed data into various forms of media such as image, audio, video, and text or any unused area in the storage media. The embedded data should be invisible and inaudible to a human observer. This means that the information is hidden in such manner that it cannot be detected by human senses or deliberately damaged. Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks. Steganography System consists mostly of two systems are the watermark system and Steganography System [1, 2].

2. Steganography Definitions

Steganography is the art and science of hiding the fact that communication is happening. While classical steganographic depend on keeping the encoding system secret , modern steganography is detectable only if secret information's known ,e.g. a secret key. Steganography is a two-part word of Greek origin. "*Stegano*", or "*covered*" and "*graphy*" or "*writing*", it does not convey the transformation of information, but rather its hidden aspect. The first steganographic technique was developed in ancient Greece around 440 B.C [2].

3. Embedding Data

Embedding Data is a form of Steganography hiding of data into digital media for the purpose of identification, annotation, and copyright. Embedding Data represents a class of processes used to hidden data, such as copyright information, into various of media such as image, audio, video (sequence of images), or text with minimum amount of perceivable degradation to the "*host* " signal, i.e. the embedded data should be invisible and inaudible to a human observer. These processing need two files, the first file is the cover file cover, and the second file for secret message [3,4].

4. Steganography and Cryptography

Steganography encompasses techniques of transmitting secret data through innocuous such that its presence cannot be detected. Steganography can be viewed as akin to cryptography. Both have been used throughout recorded history as means to add elements of secrecy to communication. More comparison notes are shown in table (1.1) [1,3,4].

Encryption	Steganography
Cryptography is the science/art of transform	Steganography is science/ art of hiding
The data visible Using the key to encrypt the data	The data visible Using the key for hidden position
Any person has the ability of detecting and modifying the encryption messages	The hidden message is imperceptible to anyone, but the cover is perceptible
The secret messages have size in encryption files	The hide messages do not have size in cover files
The secret messages is broken when the attacker can read the secret message (decrypt the ciphered message)	Breaking a steganography system has two stages: The attacker can detect the embedded message. The attacker is able to read embedded message
The goal of secure cryptographic system is to prevent an interceptor from gaining any information about the plaintext from the intercepted Ciphertext	The goal of secure steganographic system is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data

Table 1. Comparision Between Steganography and Cryptograpgy

5. Least Significant Bit Insertion (LSB)

LSB is the most common way to hide data in the image or in any other medium. And to maintain the image data carrier of the secret message. Through this method we change (flip) the first bit to hide the message. When we want to hide one (1) within the first bit we check the value of one, the contents in first bit of cover bytes if it is the same leave it as is, if zero (0), flipped to 1. This is the biggest error is 1. If the value of the byte in cover for example 56 (00111000) after hiding data within first bit in the left of cover byte, the value has changed (to 57 = 00111001) or stays same the 56 independent of last the bit of cover byte and the value of secret message then the secret message is hidden with 1 maximum error, or 0 not error. In same way we can hide in first and second of LSB with maximum error are 2 [3].

6. Shifting of the Frame

The frame is the images displayed per second in the video, whenever it was more than a video as soon as the truth. The frame or image can make it as a form of a matrix composed of rows and columns, the elements of the matrix are called pixels. To shifting the values of this matrix by adding limit value as we need the value of error (if need the error 1 added 2 or need error 2 added 4 to shift all values). New values of matrix can be found by following the equation: {(VF + C * N) mod 256 = new value}, C is shifting value, if the value of C = 4, the error is 2, and if c=2, then error is 1, which is the least error possible. N: Represents the number or sequence of shifting where number of shifting can be found by 256/C. VF: the color value (the values of pixels in the frame), in table (2) shows examples about shifting operation.

3	255	36	45
56	124	47	243
13	74	112	250
22	200	254	88

(a) Before Shift

7	3	40	45 + 4 = 49
60	127	51	247
17	78	116	254
26	204	2	92

(b) After First Shift c = 4

255	251	32	41
52	120	43	239
9	70	108	246
18	196	250	84

(c) After 63 Shift c = 4

3	255	36	45
56	124	47	243
13	74	112	250
22	200	254	88

(d) After 64 Shift c = 4

Table 2. Explains the Shifting Operation in the Frame

Note, The frame after the 64 shift (see tables d and a) same the frame before any shift, that mean the frame return to the original case (values) [1,4].

7. Mean Square Error (MSE)

MSE computes the signal difference between the distorted image and the original, computing by the following formula:

$$MSE = \frac{1}{W \times H} \sum_{x=0}^{W-1} \sum_{y=0}^{H-1} (I_{xy} - \tilde{I}_{xy})^2$$

Where W, H is the Width and Height of the image; I_{xy}, $\tilde{I}_{xy}$ represents the pixel with row number x and column number y in the original image and the distorted image respectively [2].

8. Peak Signal to Noise Ratio (PSNR)

PSNR is another difference distortion metrics that is adopted to obtain the visual quality of the preprocessed image or the stego-image, computing by the following formula [2]:

$$PSNR = 10 \times \log_{10} \frac{W \times H \times 255^2}{\sum_{x=0}^{W-1} \sum_{y=0}^{H-1} (I_{xy} - \tilde{I}_{xy})^2}$$

9. New Steganography with Most Significant Bits

A byte consists of eight bits in binary numbering (binary) which correspond to the values 0 to 255 in decimal numbering

(00000000 to 11111111), for each bit (0 or 1) has impact in the value of the byte (increase or decrease) commensurate with the bits site of a byte. For example when change first bit in the byte (color value in pixel) increase, or decrease 1 of the byte value (in decimal numbering), and if change the site number 6^{th} (bit number 6) the byte value change 32, and position 8^{th} increase 128 or decrease 128, so the greatest change in 8^{th} site (position). Therefore we cannot insert any information in MSB. In our research we were able to develop a new method, which was published in Aleppo university magazine in 2010 and we were able to solve this problem and managed to hide in all bits of byte with the highest error amount of 1 or 2 according to what we want to be the value of the error. The possibility of steganography in all bytes of the cover, without exception, are managed at the expense of the complexity of this steganography, when the up the sequence of bits in the byte.

9.1 Steganography processing in Most Significant Bits

I will explain the processing of steganography in MSB through simple change in the value of the byte values in some serial color values of the cover. The steganography operation will focus on neighboring color values (serial) which includes the secret letter in the desired site to hide its data.

9.2 Steganography in the Eighth Position of the Byte

To hide the Message 01 in the eighth position of the byte from the cover, if the bytes cover is 10000000 =128 and 01111111=127, these values after the steganography become 00000000=0 and 11111111 =255. The value of the error, 128 very large and loses the characteristics of the frame. To get rid of this problem, when the steganography is 128=10000000, to hide 0 in 8^{th} position (site), we are looking for the nearest neighbor of 128, and search for which value has 0 in position 8th with maximum 0 or 1 error (or any error we needed). Then the value is 01111111=127; thus we hid the letter 0 in value 128 and changed the value 128 to 127 with error of 1 (now the 0 is hidden in 8th site of byte in the cover 10000000=128 with 1 error). In the same way, we hide the remain of the secret letter in the cover values of cover by shifting the color values a number of offsets by 2 each time and looking for the values 127 and 128, which can hide confidential secret infirmities with error of the amount is 1. To shift 125 by 2 it equals 127. Table 3 shows the steganography mechanism in position number 8th of the byte, in the same steps that we had previously.

Value of the byte	Position Bit	Secret Bit	
		0	1
127	8^{th}	No change	128 = 1000 0000
127	8^{th}	127 = (0111 1111)	No change

Table 3. Explain the process of steganography in 8^{th} position

Value of the byte	Position Bit	Secret Bit	
		0	1
63	7^{th}	No change	64 = 0100 0000
64	7^{th}	63 = 0011 1111	No change
127	7^{th}	128 = (1000 0000)	No change
127	7^{th}	No change	127 = 0111 1111
191	7^{th}	No change	192 = 1100 0000
192	7^{th}	191 = 1011 1111	No change

Table 4. Explain the process of steganography in 7^{th} position

9.3 Steganography in the Seventh Position of the Byte

The steganography in the seventh bit (site) would be according to Table (4) and same steps that we had in the steganography in the eighth site, but with more color value.

Table (4) shows the color values and how they steganography. This is the zero shifting and shifting the frame C=2 look table (4), and the frame to hide the new secret message, and continue until shifting the number 31 then and stop. This will the message in the same byte of cover, but still some bytes in the frame do not have a hidden message like 0, 193-255, so it will continue to shift and hide only in 63 and 64, with shifting numbers from 32 to 63, and continue shifting form 64 to 127 without hiding. See in shifting number 128 the frame, return to the original case with maximum error of 1 in same of byte value to the frame (image or cover).

Following is some shifting of operation:

(255 + 2 * 32) Mod 256 = 63

(0 + 2 * 32) Mod 256 = 64

(194 + 2 * 63) Mod 256 =(194 + 126) Mod 256 = 320 Mod 256 = 64.

(193 + 2 * 63)Mod 256 = 63.

(63 + 2 * 65) Mod 256 = (63 + 130) Mod 256 = 193

(193 + 2 * (63 + 65)) Mod 256 = (193 + 2 * 128) Mod 256 =193

See 193 before shifting and 63 shifting and

after 65 + 63=128 return to 193 (original case)

(193 + 2 * (63 + 65)) Mod 256 = (193 + 2 *128) Mod 256 =195

Range	Position Bit	Secret Bit	
		0	1
30-31	6th	No change	32 = 0010 0000
32-33	6th	31 = 0001 1111	No change
62-63	6th	64 = 0100 0000	No change
64-65	6th	No change	63 = 0011 1111
94-95	6th	No change	96 = 0110 0000
96-97	6th	95 = 0101 1111	No change
126-127	6th	128 = 1000 0000	No change
128-129	6th	No change	127 = 0111 1111
158-159	6th	No change	160 = 1010 0000
160-161	6th	159 = 1001 1111	No change
190-191	6th	192 = 1100 0000	No change
192-193	6th	No change	191 = 1011 1111
222-223	6th	No change	224 = 1110 0000
224-225	6th	223 = 1101 1111	No change

Table 5. Explain the process of steganography in 6th position

9.4 Steganography in the Sixth Position of the Byte

Table (5) represents the steganography mechanism in position number 6 of the byte in the cover, and greatest errors is 2 with a

shifting value of 4. We used the same processing and same steps in 7^{th} and 8^{th} position.

10. Extracting the Hidden Message

For extracting the message hidden by searching for the values match with values in the tables such as Table 3.4 and 5 and by the key (the key used by sender and receiver) can know in which bit of the byte from the color the secret message is. For example, Table 3 tells the secret data in bits position sixth in the bytes of cover, so easy to take it (represents a bit-message hidden), and make shift to all value of the frame of the matrix of picture by the value of C that is defined for looking of new value has secret message, and continue.

11. Results Notes

From the testing results of the hiding techniques (shown in tables 6 and 7), one can notice the following:

11.1 Steganography Results

The test results of the steganography in MSB given in table 6 and 7 show that all new steganography methods and the value of complexity have better quality than LSB methods. And the test results of Variable MSB methods given in table 6 show the high quality of the cover, where this method has better security and quality compared with all other methods. This means we have got to good results and we were able to find a solution to the big problem in steganography, can't steganography in MSB, just in LSB, but in our last research, we were able to hide in all bits of bytes in each pixel which represents the value of color, and we were able to hide in all bytes and pixels of the cover file without exceptions (it was just on the bytes that appear in the table).

However, the new steganography (in MSB) has better security, and has very good quality (PSNR), and no change between the caver before and after embedded data (MSE).

Video Samples	Secret Message Size/Byte	No. of Needed Frames	MSE		PSNR	
			All	Avg.	All	Avg.
P1	41400	1	1.25	1.25	48.1	48.1
P2	83000	2	2.60	1.25	96.1	48.2
P3	125000	3	4.0	1.20	142.1	48.5
P4	166660	4	5.1	1.19	189.8	48.3
P5	208000	5	6.2	1.19	241.2	48.6

Table 6. The results of the Variable MSB techniques of text steganography

The small problem with new steganography are summarized by processor speed and the processing time is bigger than LSB, because match the color value with table value, and hide in the values of the framework corresponding to the values of the tables and then clear out the values of the frame and shift the table value look for other values match the values of the tables to hide other secret messages until hide all messages with each byte we need it in cover, so this needs more time, space in RAM, and processing speed than in the LSB which is made by direct change or not change (flip) the first or second bits of bytes in each pixel. But everyone knows that the computer is faster day by day.

11.2 Complexity in Steganography

Table (7) shows the amount of complexity when hiding in one or two bits,.., until eight bits.

Table (7) shows the amount of complexity at steganography in one bit or two until eight bits, as shown in the table when steganography in one bit for example in the first bit of the byte from cover, the value of the complex is very small or not complex, the reason when used one bit that the enemy knows exactly that the secret message hidden in the first bit without other bit as in LSB and they can know and get the secret messages from the first bit. However, if there are more than one site (position) to

hide the message, the attacker or enemy cannot detect the secret message as hide in one bit, the complexity to access and reveal the message will increase the likelihood of error with greater the number of position, steganography in two positions better than one and three positions (bits) of byte better than tow or one bits, final, highest security and complexity when hidden 8 bits distributed in pixels from cover. Table (7) shows that the value of complexity are 4 When hide a message in two bits (positions) of the cover, this is difficult for the enemy to detect the message because he does not know where it is, is it in the first or the second or the first bit and the second, or in the second and first, this shows the size complexity with the increase with great number of bits of steganography, if hide in all bites (8 position) in bytes of the cover the attacker or enemy try 256 times to fond the secret message, If the cover has 100 bytes, the attacker try $100 * 265$ times detect to detect the message. If the length of the cover N bytes, the complexity is equal to the value of $256 * N$ (256 multiplied by N). It is known that the steganography was limited in the first, second and some other sites of bytes and under certain conditions narrowing of the area and increase the extracting problems and can reduce the complexity of steganography.

In this research, the developing of a new method of steganography, where we were able to hide information in every bit of the bytes in the cover without condition or restriction, and retrieve the complete hidden message with high complexity proportion to the length of the cover and number of positions in the color values.

Our new research shows the information hidden in the eighth position are not higher security than the first position, no!! Because the steganography in the first or the eighth bit (as one bit) of the cover has same value of the complexity. Also the steganography in the eighth and the seventh is the same as the complexity of steganography in the first and second or first and fourth (value of complexity = 4), so the complexly is increased when the increase the number of position (sites) is used in the cover steganography. But the most important site with steganography!! It is the impact position (site) to decide on the safety of cover. Sometimes the enemy knows the secret message in the eighth or the seventh bit but could not read it, because encrypted. The enemy breaks these positions and, thus destroys the cover because these bits are more important and more influential than the first or second position.

Bit position	The complexity of steganography with each position	The complexity in the cover has 100 bytes	The complexity in the cover has 100 bytes
1	0	0	0
2	$2^2 = 4$	4*100 = 400	4N
3	$2^3 = 8$	8*100 = 800	8N
4	$2^4 = 16$	16*100 =1600	16N
5	$2^5 = 32$	32*100 = 3200	32N
6	$2^6 = 64$	64*100 = 6400	64N
7	$2^7 = 128$	128*100 = 12800	128N
8	$2^8 = 256$	256*100 = 25600	256N

Table 7. The complex with steganography in LST until MSB

References

[1] Aleksandar, K. (2009). Cryptanalysis of Symmetric Key Primitives. *Concordia University*, Montreal, Canada.

[2] Yang M,Trifas M, Francia III, G., Chin, L. (2009). Cryptographic and Steganographic Approaches to Ensure Multimedia Information Security and Privacy. *Jacksonville University*, USA.

[3] Stefan, K., Fabien, A., Petit Colas, P. (2005). Information Hiding Techniques for Steganography and Digital Watermarking. Artech house press.

[4] Yahia Najar, Mahmood Shaar, Salam Mahdi. (2011). New Steganography in all Bits from the Bytes in the Cover, Dept. of Computer Engineering, Electronic College, University of Aleppo, SYRIA.