International Journal of Computer and Communication Technology

Volume 3 | Issue 2 Article 9

April 2012

A Technique for Secure Communication Using Message Dependent Steganography

Gandharba Swain
1Department of IT, GMR Institute of Technology, Rajam, Andhra Pradesh, India,
gandharbaswain@gmail.com

Dodda Ravi Kumar
2Department of IT, GMR Institute of Technology, Rajam, Andhra Pradesh, India,
doddarabikumar@gmail.com

Anita Pradhan
3GMR Nagar, Rajam, Srikakulam District, Andhra Pradesh, India, anitapradhan@gmail.com

Saroj Kumar Lenka
4Department of Computer Engineering, MITS Deemed University, Rajasthan, India,
sarojkumarlenka@gmail.com

A Technique for Secure Communication Using Message Dependent Steganography

Gandharba Swain[1], Dodda Ravi Kumar[2], Anita Pradhan[3], Saroj Kumar Lenka[4]
[1]Department of IT, GMR Institute of Technology, Rajam, Andhra Pradesh, India.
(Research Scholar SOA University, Bhubaneswar, Orissa, India)
[2]Department of IT, GMR Institute of Technology, Rajam, Andhra Pradesh, India
[3]GMR Nagar, Rajam, Srikakulam District, Andhra Pradesh, India
[4]Department of Computer Engineering, MITS Deemed University, Rajasthan, India.

Abstract- **In this paper we present a technique for secure communication between two parties Alice and Bob. We use both cryptography and steganography. We take image as the carrier to use steganography. By using our own substitution cipher called two square reverse we encrypt the secret information. Then the cipher text of the secret information is embedded into the carrier image in LSB (least significant bit) minus one position of some selected bytes. The byte selection is done depending on the bit pattern of the secret information. Thus the embedding locations are dependent on the secret message. So the intruder will face difficulties to locate the bits. After embedding the resultant image will be sent to the receiver, the receiver will apply the reverse operation what the sender has done and get the secret information.**

Keywords: *LSB, steganography, cryptography, encryption, decryption, embedding,*

1. INTRODUCTION

Steganography is a technique of secret communication between sender and receiver. In steganography the secret information is hidden inside a carrier file such that the change in appearance of the carrier file should not be apparent to normal human eye. It is often confused with cryptography because the two are similar in the way that they both are used to protect secret information. The difference between the two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or process views the file where information is hidden, he or she will have no idea that there is hidden information, therefore the person will not attempt to decrypt the information. Where as in case of cryptography the confidential information is encrypted by a key and sent on the channel. A person or a process by seeing this can notice that something is under communication, but he cannot steal the information unless he knows the key. But in steganography the person or process who sees it will not even suspect that some secret information is on transit.

Steganography can be achieved in three ways; by using three types of carriers. Those are: Steganography in image, steganography in audio and steganography in video. There are a number of methods used to hide information inside image, audio and video files. Some of the most common methods of image steganography proposed by different researchers are discussed in the next section.

II. EXISTING APPROACHES

To a computer an image is simply a file that shows the different colors and intensities of light on different areas of an image. When hiding information inside images usually Least Significant Bit (LSB) method is used. In the LSB method the 8th bit of every byte of the carrier file is substituted by one bit of the secret information [1]. This method works fine in the image carriers because if the least significant bit is changed from 0 to 1 or vice versa, there is hardly any change in the appearance of the color of that pixel. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted. In injection method simply the secret information is injected wholly in an appropriate location of the carrier file. The main problem with this method is that it can significantly increase the size of the carrier file.

In Image encryption approach we can encrypt the image and embed the secret information in LSBs and after embedding if the entropy and correlation values of stego image and original image are the same then the process is a secure one[1,6]. Ross J. Anderson and Fabien A.P. Petitcolas argued that every steganographic approach will have its limitations; they proposed an information theoretic approach using Shannon's theory for perfect secrecy [2]. As per the labeling methods proposed by H. Motameni and his colleagues one can embed at the dark corners of an image [3]. One can also embed the secret information in frequency domain by using Discrete Wavelet Transform method [4]. In this method the embedding should be done at high frequency coefficients. As per the image in image steganography method proposed by P. Mohan Kumar and D. Roopa one can apply block matching procedure to search the highest similarity block for each block of the secret image and embed in LSBs of the cover image [5]. A very different way of steganography as proposed by Mohammed A.F. AlHusainy is by mapping the pixels of image to English letters and special characters [7]. Lisa M Marvel and Charles G Boncelet proposed to hide at the inherent noise places [8]. Ran-Zan Wang and Yeh-shun Chen also did the two way block matching for image in image steganography [9]. But this approach is suspicious to the hackers. Xinpeng Zhang and his colleagues proposed an approach called "multibit

assignment steganography for pallete images", in which each gregarious color that possesses close neighboring color in the palette is exploited to represent several secret bits [10]. In reference [11] authors have discussed a double substitution algorithm for encrypting at sender and decrypting at receiver and the embedding process was at 7^{th} and 8^{th} bit positions alternatively. In [12] an image steganography with palette based images is suggested. The method is based on a palette modification scheme, which can iteratively embed one message bit into each pixel in a palette based image. In each iteration, both the cost of removing an entry color in a palette and the benefit of generating a new one to replace it are calculated. If the maximal benefit exceeds the minimal cost, an entry color is replaced. It is found that the fundamental statistics of natural images are altered by the hidden non-natural information [13]. But if we do not touch the bytes those carry the image features and embed in the other bytes then the problem can be solved. As LSB embedding is very common, many steganalysis tools are available for it [14]. So LSB embedding is no more secure now-a-days. So new embedding techniques are to be welcomed to the steganographic world. Due to the large number of steganographic tools available over the internet, a particular threat exists when criminals use steganography to conceal their activities with in digital images in cyber space. In [15] authors suggest two steganographic schemes based on point sampled geometry. Both the schemes employ a principal component analysis to translate the points' coordinates to the new coordinate system, resulting in a blind approach. In the first approach they established a list of intervals for each axis according to the secret key and then embedded a bit into each interval by changing the points' position. In the second scheme they located a list of macro embedding primitives (MEPs), and then embedded c bits ($2 \leq c \leq 6$) at each MEP, instead of a single bit as in the first approach. In [16] a steganographic protocol based on hamming codes is proposed. Reference [17] presents two JPEG steganographic methods using quantization index modulation (QIM) in the discrete cosine transform (DCT) domain. The two methods approximately preserve the histogram of quantized DCT coefficients, aiming at secure steganography against histogram-based attacks.

Our proposed approach can be understood by referring the following sections. In section-III, the working of the Two square reverse cipher is discussed, in section-IV the embedding process, in section-V the proposed algorithm, in section-VI the experimental results and in section-VII the comparisons and in section-VIII the conclusion and future work.

III. THE TWO SQUARE REVERSE CIPHER

The Two Square Reverse cipher technique works as follows: There are two steps for encryption. In the first step we get the first step cipher by using the table-1 and table-2. In these tables we exclude the character "q". for "q" the first step of cipher is also"q". For a plain text character in table-1, the cipher text is in same row and column location of table-2.

TABLE 1: Plain Text

a	b	c	d	e
f	g	h	i	j
k	l	m	n	o
p	r	s	t	u
v	w	x	y	z

TABLE 2 : First Cipher Text

z	y	x	w	v
u	t	s	r	p
o	n	m	l	k
j	i	h	g	f
e	d	c	b	a

After getting the first step cipher we divide that into two-two characters. After that we swap the two-two characters positions and get the final cipher. For example:

Suppose the plain text is **:**

marcus was a pompian.

Then the first step cipher is:

mzixfh dzh z jkmjrzl

In the 2^{nd} step

these are reversed pair by pair including the blank spaces.

Thus the final cipher is:

zmxihfd hzz j mkrjlz

Note that while swapping a pair of characters blank spaces are also counted as a character.

At the receiver, the decryption process is just the reverse of encryption. The second step of encryption will be the first step in decryption and the first step of encryption will be the second step of decryption.

IV. THE EMBEDDING PROCESS

The cover image is divided into bytes. In each byte we do not embed; but in few selected bytes based on the bit pattern of the cipher text. In the selected bytes the 7^{th} bit position i.e LSB minus one positions are to be embedded. The 8^{th} bit means the LSB bit position. Let us understand the embedding process through this example.

Example-Assume that the data to be sent is: **11001011 01111010.** Suppose the different bytes of the image are A, B, C, D etc. The first bit 1 will be embedded in 7th bit position of A, then 1 byte (i.e B) will be left. The 2nd bit 1 will be embedded in C byte and one byte (i.e D) is left. The the third bit 0 is embedded in E and 0 byte is left. Then 4th

bit 0 is embedded in F and 0 byte left. Then 5th bit 1 is embedded in G and 1 byte (i.e F) is left and so on. That means if the present bit embedded is 1 the next byte is skipped and if the present bit embedded is 0 the next byte is not skipped.

Table-3: Selection of bytes as per the embedding process

Carrier File Byte	Operation
Byte A	Embed(1)
Byte B	skip
Byte C	Embed(1)
Byte D	skip
Byte E	Embed(0)
Byte F	Embed(0)
Byte G	Embed(1)
Byte H	skip
Byte I	Embed(0)
Byte J	Embed(1)
Byte K	skip
Byte L	Embed(1)
Byte M	skip
So on	

V. THE PROPOSED ALGORITHM

Step1 - Convert the cover image to binary
Step2 - Apply Four Square Reverse to encrypt the secret information. Now we got the cipher.
Step3 - Convert the cipher text to binary.
Step4 - Make sure that the length of cover image is sufficient enough to conceal the cipher text.
Step5 - Embed the cipher into the cover image as discussed in the embedding process.
Step6 - Now send the resultant image to receiver
Step7 - Receiver applies the reverse process what sender has done and gets the hidden information.

Now let us discuss what should be the required length of the carrier file to conceal a specific amount, say n bytes of the secret information. It is very difficult to predict the length exactly unless we know the bits of the secret information.

If all the bits of the cipher text are 0's then the n bits of cipher text need n byte length image.

If all the bits of the cipher text are 1's then the n bits of cipher text need 2n bytes of image.

In reality both the above cases will not happen. In average if we consider the 50% bits of cipher are 0's and 50% are 1's then for n cipher bits we need 1.5n byte length image.

VI. THE EXPERIMENTAL RESULTS

We had about more than hundred observations with a wide variety of images. In all the cases it works fine. Two sample observations are as given below.

Observation-1:
Figure-1 is the original image to be used as the carrier. Figure-2 the secret information to be sent. Figure-3 is the cipher text of the secret information which is to be embedded. Figure-4 is the resultant image after embedding which is transmitted and Figure-5 is the received image at the receiver and Figure-6 is the retrieved text at the receiver.

Fig. 1 The original image

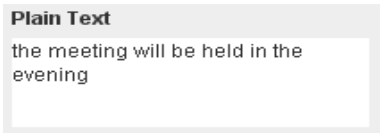

Fig.2 The secret information to be sent

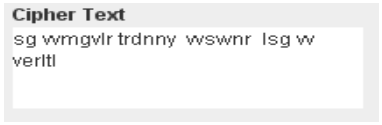

Fig. 3 The cipher text to be embedded

Fig.4 Resultant image to be transmitted (cipher texte mbedded)

Fig.5 Received image at the receiver

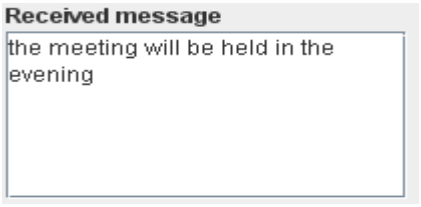

Fig.6 The retrieved text from the image at the receiver

Observation-2:

Figure-7 is the original image to be used as the carrier. Figure-8 the secret information to be sent. Figure-9 is the cipher text of the secret information to be embedded. Figure-10 is the resultant image after embedding which is transmitted and Figure-11 is the received image at the receiver and Figure-12 represents the retrieved text at the at the receiver.

Fig.7- The original image

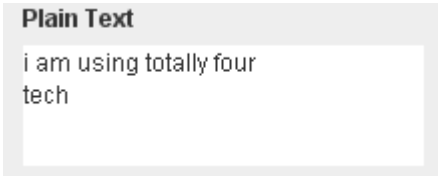

Fig.8. The secret text to be sent

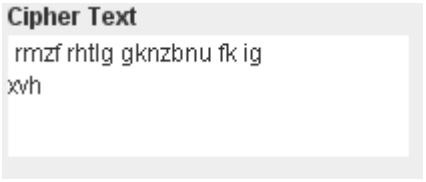

Fig.9 The Cipher text to be embedded

Fig. 10 Resultant image to be transmitted(cipher text embedded)

Fig.11 Received image at the receiver

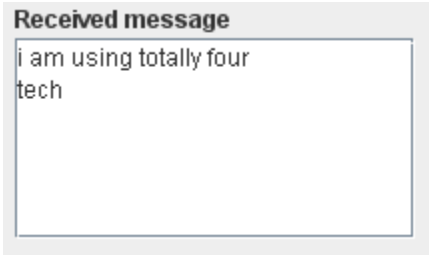

Fig.12 The retrieved text from the image at the receiver

VII. COMPARATIVE STUDY

Mostly people do steganography with LSB. In this paper we are using LSB minus one position, in some selected bytes. Here we are not embedding the secret text directly. We are embedding the cipher text. There are two levels of security in this proposed algorithm. Firstly at the cryptography level and secondly at the steganography level. As we are embedding based on the bits of the secret information; it becomes a stronger steganography. There is no chance for the intruder to identify the embedded pixels. If the intruder will try to hack by hit and trial method it is impossible for him to identify the pattern because it is dependent on the bits of the secret information.

As compared to LSB and injection methods this algorithm is much better in terms of intrusion prevention. Compared to other algorithms suggested by different experts in this field; this is a unique and stronger one. Every body is using static way of calculating the embedded byte/pixel positions; but surprisingly we are using differently.

VIII. CONCLUSION AND FUTURE WORK

We have observed through more than 100 observations by taking a wide variety of images from different sources. It works fine. It provides two levels of security. If at all the intruder suspects it is quite impossible for him to steal the data because our embedding byte positions are decided based on the bits of the cipher text. After the cipher text is embedded, the degradation in image quality is not apparent to normal human eye.

This approach can be extendable to send secret images in cover image. This approach can be extendable to audio and video carrier files.

ACKNOWLEDGMENT

I am thankful to the management of GMR Institute of Technology for their continuous support to pursue research. I thank to Dr Saroj Kumar Lenka for his timely guidance and suggestions. I thank to my co-authors Mr D. Ravi Kumar and Mrs Anita Pradhan for their support and contribution.

REFERENCES

[1] Mohammad Ali Bani Younes, Aman Jantan, "A New Steganography Approach for Image Encryption Exchange by using the LSB insertion", IJCSNS International Journal of Computer Science and Network Security, Vol 8, No 6 , pp. 247-254, June 2008.

[2] Ross J. Anderson, Fabian A.P. Petitcolas, "On The Limits of steganography", IEEE Journal of selected Areas in communication, 16(4), pp. 474-481, May 1998. Special Issue on Copyright and Privacy protection. ISSN 0733-8716.

[3] H. Motameni, M.Norouzi, M.Jahandar. and A. Hatami, "Labeling method in Steganography", Proceedings of world academy of science, engineering and technology, Volume 24, pp.349-354,October 2007, ISSN 1307-6884.

[4] Po Yuch Chen and Hung Ju Lin, "A DWT Based Approach for Image Steganography", International journal of Applied Science and Engineering, 4(3), pp. 275-290, 2006

[5] P.Mohan Kumar and D.Roopa, "An Image Steganography Framework with Improved Tamper Proofing", Asian Journal of Information Technology 6(10), pp.1023-1029, 2007. ISSN: 1682-3915

[6] Joachim J. Eggers and R.Bauml, Bernd Girod, "A Communications Approach to image steganography", proceedings of SPIE Volume 4675 Security and watermarking of Multimedia Contents IV, san Jose, Ca, pp. 1-12, Jan 2002.

[7] Mohammed A.F Al Husainy, "Image Steganography by mapping Pixels to letters", Journal of Computer science 5(1), pp. 33-38, 2009 , ISSN 1549-3636.

[8] Lisa M. Marvel, Charles G. Boncelet, "Spread Spectrum Image Steganography", IEEE Transactions on Image Processing Vol. 8, No. 8, pp.1075-1083, August 1999.

[9] Ran-Zan Wang and Yeh-Shun Chen, "High Payload ImageSteganography Using Two-Way Block Matching" , IEEE Signal Processing letters, Vol. 13, No.3, pp.161-164. March 2006.

[10] Xinpeng Zhang, Shuozhong Wang and Zhenyu Zhou, "Multibit Assignment Steganography in Palette Images", IEEE Signal Processing Transactions, Vol.15, pp. 553-556, 2008

[11] Gandharba Swain, S.K.lenka, "Steganography-Using a Double Substitution Cipher", International Journal of Wireless Communications and Networking, Volume 2, Number 1, January-June 2010. pp.35-39. ISSN: 0975-7163

[12] Mei-Yi Wu, Yu-Kun Ho, Jia-Hong Lee, "An iterative method of palette-based image steganography", pattern Recognition Letters 25 (2004), pp. 301-309.

[13] Alvaro Martin, Guillermo Sapiro and Gadiel Seroussi, "Is Steganography Natural", IEEE Transactions on Image processing, Vol. 14, No. 12, December 2005. pp.2040-2050.

[14] Sorina Dumitrescu, and Xiaolin, "A New Framework of LSB Steganalysis of Digital Media", IEEE Transactions on Signal Processing, Vol. 53, No.10, October 2005. pp.3936-3947.

[15] Chung-Ming Wang, Peng-Cheng Wang, "Steganography on point-sampled geometry", Computer & Graphics 30 (2006), pp.244-254.

[16] H. Rifa-Pous, J. Rifa, "Product Perfect Codes and Steganography", Digital Signal Processing 19 (2009), pp. 764-769.

[17] Hideki Noda, Michiharu Nimi, Eiji Kawaguchi, "High- performance JPEG steganography using Quantization index modulation in DCT domain", Pattern Recognition Letters 27 (2006) pp.455-461.

.