International Journal of Computer and Communication Technology

Volume 5 | Issue 1 Article 1

January 2014

Crypto Steganography using linear algebraic equation

Pradeep Kumar Mallick
Department of Computer Science and Engineering C. V. Raman College of Engineering, Bhubaneswar, India, pradeepmallick84@gmail.com

N.K. kamila
C.V.Raman College of Engineering and Technology, nkamila@yahoo.com

Recommended Citation
Mallick, Pradeep Kumar and kamila, N.K. (2014) "Crypto Steganography using linear algebraic equation," *International Journal of Computer and Communication Technology*: Vol. 5 : Iss. 1 , Article 1.
DOI: 10.47893/IJCCT.2014.1211
Available at: https://www.interscience.in/ijcct/vol5/iss1/1

Crypto Steganography using linear algebraic equation

Pradeep Kumar Mallick [1], Narendra Kumar Kamila[2]
Department of Computer Science and Engineering
C. V. Raman College of Engineering, Bhubaneswar, India
E-mail - pradeepmallick84@gmail.com [1], nkamila@yahoo.com[2]

Abstract
Demand of information security is increasing day by day with the exponential growth of Internet. The content of message is kept secret in cryptography, where as steganography message is embedded into the cover image. In this paper a system is developed in which cryptography and steganography are used as integrated part along with newly developed enhanced security model. In cryptography the process of encryption is carried out using symmetric block ciphers with linear algebraic equation to encrypt a message [1] and the obtained cipher text is hidden in to the cover image which makes the system highly secured. Least Significant Bit (LSB) technique is used for message hiding which replaces the least significant Bits of pixel selected to the hide the information. A large number of commercial steganographic programs use LSB as the method of choice for message hiding in 24-bit,8bit-color images, and gray scale images. It is observed from the simulation study that both methods together enhance security significantly.

Keywords: Cryptography, Steganography, LSB,

1. Introduction

Cryptography and steganography are two popular techniques for secret communication. The content of message is kept secret in cryptography, where as steganography message is embedded in to the cover image. In this paper a system is developed in which cryptography and steganography are used as integrated part along with newly developed enhanced security model. In cryptography the process of encryption is carried out using symmetric block ciphers with linear algebraic equation to encrypt a message [1] and the obtained cipher text is hidden in to the cover image which makes the system highly secured.LSB technique is used for message hiding which replaces the least significant bits of pixel selected to the hide the information.

Two other technologies closely related to steganography are watermarking and fingerprinting [20].Watermarking is a protecting technique which protects (claims) the owner's property right for digital media (i.e. images, music, video and software) by some hidden watermarks. Therefore, the goal of steganography is the secret messages while the goal of watermarking is the cover object itself.

The proposed work represents a heuristic approach to introduce the concept of Multi Layer Data Security algorithm in the field of combined Cryptography and Steganography. The algorithm, which is being proposed here, will secure the text message in multiple protection layers. Hence the concept of Cryptography and Steganography is as two Layers of Security and in between them an extra layer of security is also introduced.
The rest of the sections are organized as follows: Related works in section 2, Types of steganography and its technique in Section 3, section 4 describes PSNR, proposed problem description and algorithm is represented in section 5 and the simulation result is represented in section 6. The paper is observed by a conclusion in section 7.

2. Related works

The most of today's steganographic systems use images as cover object because people often transmit digital images over email and other communication media. Several methods exist to utilize the concept of Steganography as well as many algorithms have been proposed in this regard.

Least significant bit insertion is a common and simple approach to embed information in a cover object. For images as a covering media, the LSB of a pixel is replaced with an M's bit. If we choose a 24-bit image as cover, we can store 3 bits in each pixel by modifying the LSBs of R, G and B array. To the human eye, the resulting stego image will look identical to the cover image [2,3].

Hiding data in the features of images is also an important technique which uses the LSB

modification concept. In this method, to hide data in an image the least significant bits (LSB) of each pixel is modified sequentially in the scan lines across the image in raw image format with the binary data. The portion, where the secret message is hidden is degraded while the rest remain untouched. An attacker can easily recover the hidden message by repeating the process [3,4].

An interesting application of steganography and cryptography has been developed by Sutaone, et al. [5] where a steganography system is designed for encoding and decoding a secret file embedded into an image file using random LSB insertion method. In their method, the secret data are spreaded out among the cover image in a seemingly random manner. The key used to generate pseudorandom numbers, which will identify where, and in what order the hidden message is laid out.

The next interesting application of steganography has been developed by Miroslav Dobsicek, where the content is encrypted with one key and can be decrypted with several other keys. In this process, the relative entropy between encrypt and one specific decrypt key corresponds to the amount of information [6].

In 2007, Emam proposed an algorithmic approach to obtain data security using LSB insertion steganographic method [7]. In his approach, high security layers have been proposed to make it difficult to break through the encryption of the input data and confuse steganalysis too .

There is also a good method proposed by Sahoo at el.[8] in 2008. Their proposed method works on more than one image using the concept of file hybridization. This particular method implements the cryptographic technique to embed two information files using steganography. And due to this reason they have used a stego key for the embedding process .

The method proposed by Aziz Gutub et al. in 2007 is also a good one [9]. Their approach hides secret information bits within the letters benefiting from their inherited points. To note the specific letters holding secret bits, the scheme considers the two features, the existence of the points in the letters and the redundant Arabic extension character. They have used the pointed letters with extension to hold the secret bit ‘one’ and the un-pointed letters with extension to hold ‘zero’. This steganography technique is found attractive to other languages having similar texts to Arabic such as Persian and Urdu

Information hiding is an old but interesting technology [10]. Steganography is a branch of information hiding in which secret information is camouflaged within other information. A simple way of steganography is based on modifying the least significant bit layer of images, known as the *LSB technique*[11]. The LSB technique directly embed the secret data within the pixels of the cover image. In some cases (Fridrich et al. [12]) LSB of pixels visited in random or in certain areas of image and sometimes increment or decrement the pixel value. Habes [13] proposed a new method (4 least Significant) for hiding secret image inside carrier image. In this method each of individual pixels in an image is made up of a string of bits. He has considered the 4-least significant bit of 8-bit true color image to hold 4-bit of the secret message /image by simply overwriting the data that was already there

Unfortunately, modifying the cover image changes its properties as well as its features, so eavesdroppers can detect the distortions in the resulting stego-image’s statistical properties. In fact, the embedding of high-entropy data (often due to encryption) changes the histogram of colour frequencies in a predictable way. So, in order to obtain more security in our prescribed method, entire text information has been embedded behind the cover image by modifying the least significant bits. In true colour system, this type of modification does not affect the visual perception of human eye and thus the proposed model becomes more stringent.

3. Types of Steganography and its techniques

In general steganography can be classified into various types [7], depending upon the cover medium used. Cover medium may be text, image or audio or video file. Based on cover medium there are three types of steganography such as i) Image Steganography ii) Audio/video Steganography iii) Text Steganography

Image steganography is about exploiting the limited powers of the human visual system (HVS). Within reason, any plain text, cipher text, other mages, or anything that can be embedded in a bit stream can be hidden in an image [7]. Image steganography has come quite far in recent years with the development of fast, powerful graphical computers. Images are used for steganography in

following ways. The message in encrypted form or in the original form is embedded as the secret message to be sent into a graphic file. This results in the production of what is called a stego-image. Additional secret data may be needed in the hiding process e.g. a stegokey. The stego-image is then transmitted to the recipient. The recipient extracts the message from the carrier image. The message can only be extracted if there is a shared secret between the sender and the recipient.

Audio steganography is concerned with hiding information in a cover (host) audio signal in an imperceptible way. Hidden information from the stego, or data-embedded audio signal, is retrieved using a key similar to (or, in most cases, the same as) the one that was employed during the hiding phase. Audio and multimedia data embedding is a useful means for transmitting covert battlefield information via an innocuous cover audio signal.
Text steganography is considered to be the most difficult kind of steganography due to lack of redundancy in text as compared to image or audio but still has smaller memory occupation and simpler communication. The method that could be used for text steganography is data compression. Data compression encodes information in one representation into another representation. The new representation of data is smaller in size. One of the possible schemes to achieve data compression is Huffman coding. Huffman coding assigns smaller length code words to more frequently occurring source symbols and longer length code words to less frequently occurring source symbols.

Different steganography techniques are LSB, Masking, and Filtering and transform technique **.**In LSB least significant bit insertion is a common, simple approach to embedding information in a cover image [21]. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [22].
For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200,of which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [23]. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. The human eye cannot perceive these changes, thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [23].

A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover object, but the cover-object is degraded more, and therefore it is more detectable. Other variations on this technique include ensuring that statistical changes in the image do not occur. Some intelligent software also checks for areas that are made up of one solid color. Changes in these pixels are then avoided because slight changes would cause noticeable variations in the area.

Other techniques of steganography include spread spectrum steganography, statistical steganography, distortion, and cover generation steganography etc.

4. Peak Signal to Noise Ratio (PSNR)

The larger PSNR indicates the higher the image quality i.e. there is only little difference between the cover-image and the stego-image. On the other hand, a smaller PSNR means there is huge distortion between the cover-image and the stego image, where

the measurement of the quality between the cover image f and stego-image g of sizes $N \times N$ is defined as:

$$PSNR=10 \times \log(255^2/MSE)$$

$$\text{where } MSE = \sum_{X=0}^{N-1} \sum_{y=0}^{N-1} (f(x,y)-g(x,y))^2/N^2 \quad (1)$$

Where f(x,y) and g(x,y) means the pixel value at the position (x, y) in the cover-image and the corresponding stego-image respectively. The PSNR is expressed in dB's.

5. Proposed problem description with algorithm

In the proposed problem the plain text is encrypted by symmetric block ciphers with linear algebraic equation algorithm. Then the produced cipher text is embedded with the cover image by LSB steganography technique .The output i.e. the stego image is then transmitted to the recipient. The recipient extracts the message from the carrier image by the reverse way. The message can only be extracted if there is a shared secret between the sender and the recipient. This makes the system highly secured. The corresponding block diagram showing the proposed model is

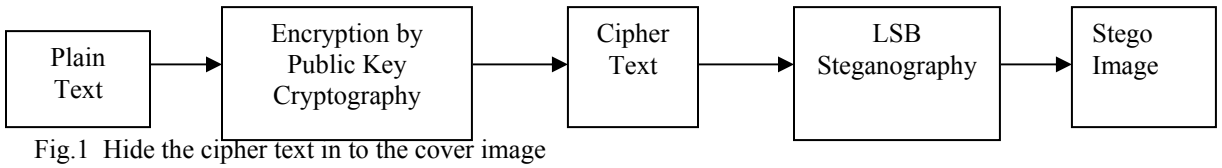

Fig.1 Hide the cipher text in to the cover image

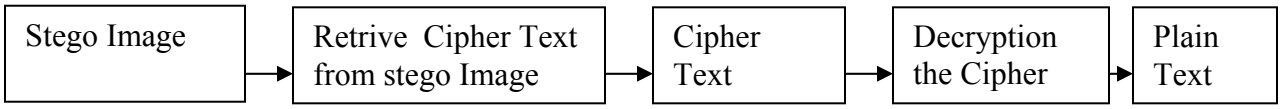

Fig.2 Extract the plain text from stego image

Algorithm

To implement lsb steganography following steps are considered.

Step 1.Read the cover image and get one array of dimension thrice.

Step 2. Each pixel of the image is represented by three values. One for R

one for G and the last one is B. Convert each value to its equivalent binary.

Step 3. Read the text which is to be kept hiding.

Step 4. Message encryption through the public key algorithm.

{

1. Take the key K_0;

2. Permute the key K_0 by using the swapping key S , Then we get K;

3. Construct the substitution table basing upon K;

4. while not end of file do

{

5. Read m characters A_i ,i=1 to m,from the input file;

6. Obtain the sequence numbers N_i , i=1 to m , corresponding to the ASCII codes of the charcters, from the Substitution Table;

// Find x_i , i=1 to n , n=2m

7. for i=1 to n do

{

$X_{2i-1} = N_i / 10$; $X_{2i} = N_i \bmod 10$;

}

// Compute S

8. S=0;

for i=1 to n do

S=S+ xi ;

//Compute C_i

9. for i=1 to n do

$C_i = S - 2X_i$;

10. for i=1 to n read K_i ;

11. for i=1 to n do

$d_i = C_i + K_i$;

12. Convert d_i into their corresponding binary form and add the parity bit;

13. Write the binary strings in the output file;

}

}

Step 5. Now get the cipher text(binary format) of each character.

Step 6. For each pixel of the input image

a. Convert the intensity value of the current pixel into

the binary form

b. Assign one bit of the text in to the last bit.

Step 7.Goto the next bit of the text

Go to the next pixel.

If no pixel is left at, exit

else

Goto step 5

Step 8.END

6. Simulation Results

In this section, some experiments are carried out to prove the efficiency of the proposed scheme. The proposed method has been simulated using the MATLAB 7 program on Windows XP platform. The proposed high secured system using cryptography is tested by taking message and hiding them in to the Lena image. The result thus obtained from the experiment is recorded and is being summarized in the following figures.

Fig. 3 Leena Original image and Stego image

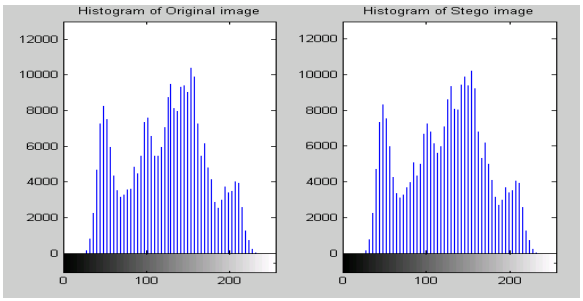

Fig.4 Histogram of Original Leena image and Stego image

Case 1 Out put

Hiding message... Please wait. Done SNR Signal to Noise Ratio 37.4684 PSNR Peak Signal to Noise Ratio 42.7777 Bit error rate 0	Hiding message... Please wait. Done SNR Signal to Noise Ratio 32.5855 PSNR Peak Signal to Noise Ratio 38.3232 Bit error rate 0

In first case 512 x 512 leena image is taken and the encrypted message is embedded with this leena image. In the second case 256 x 256 leena image is taken also the same message is embedded with this leena image.

This table exhibits the capacity, PSNR and SNR of the lenna image.

Image	Size (in Kbyte)	PSNR	SNR
Lenna	512	42.7777	37.4684
Lenna	256	38.3232	32.5855

Table 1: Capacity and PSNR of four images

Figure 3.3 depicts the original leena and stego leena image. Both images do not show any change of resolution. However figure 4 reveals histogram of both original and stego image of leena. From both histograms of figure 4 it is observed that there is no significant change of the image even though stego image is double secured. From above table and outputs it is concluded that the increase of security is directly proportional to the increase of image size. And also both PSNR and SNR value increases which signify that the system is more secured as per the theory. In other words it can be said that encryption by symmetric block cipher using linear algebraic equation with steganography enhances security of our system significantly.

7. Conclusion

In this paper we have presented a new system for the combination of cryptography and Steganography using two keys named as Cryptic-Steganography System which could be proven as a highly secured method for data communication.

Steganography, especially combined with cryptography is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality without any distortion in the image.

The main advantage of this Cryptic-Steganography System is to provide high security for key information exchanging.

Cryptic-Steganography System finds applications in medicine by doctors to combine explanatory information within x-ray images. However it can also embed corrective audio or image data in case corruption occurs due to poor connection or transmission.

References

[1] Pradeep Kumar Mallick, N.K.Kamila, S.Patnaik,B.Panda, "Computing Symmetric Block Cipher Using Linear Algebraic Equation", *International Journal of Communication Network & Security,* Page-7-11,Volume-1, Issue-1, 2011.

[2] Johnson, N. F. and Jajodia, S, "Exploring steganography: Seeing the unseen", IEEE Computer Magazine, pp.26-34, February 1998.

[3] S.K.Bandyopadhyay, Debnath Bhattacharyya, Poulumi Das, S. Mukherjee, D. Ganguly, "A Tutorial Review on Steganography", IC3 Noida, pp. 106-114, August 2008.

[4] Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS, VOL. 7, No.4, April 2007.

[5] Sutaone, M.S., Khandare, M.V, "Image based steganography using LSB insertion technique", IEEE WMMN,pp. 146-151, January 2008.

[6] M. Dobsicek, "Extended steganographic system", 8th International Student Conference on Electrical Engineering, FEE CTU 2004, Poster 04.

[7] Nameer N. EL-Emam, "Hiding a large amount of data with high security using steganography algorithm",Journal of Computer Science, Page(s): 223 – 232, April 2007.

[8] G. Sahoo, R. K. Tiwari, "Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization", IJCSNS, Vol. 8, No. 1, pp. 228-233, January 2008.

[9] Adnan Abdul-Aziz Gutub, Manal Mohammad Fattani, "A Novel Arabic Text Steganography Method Using Points and Extensions", Proceedings Of WASET, pp. 28-31, May 2007.

[10] N. F. Johnson and S. Katzenbeisser, A survey of steganographic techniques., in S. Katzenbeisser and F.Peticolas (Eds.): *Information Hiding*, pp.43-78. Artech House, Norwood, MA, 2000.

[11] Li, Zhi., Sui, Ai, Fen., and Yang, Yi, Xian. "A LSB steganography detection algorithm", *IEEE Proceedings on Personal Indoor and Mobile Radio Communications*: 2780-2783, 2003.

[12] J. Fridrich and M. Goljan, "Digital image steganography using stochastic modulation", SPIE Symposium on Electronic Imaging, San Jose, CA, 2003.

[13] Alkhrais Habes , "4 least Significant Bits Information Hiding Implementation and Analysis" , ICGST Int. Conf. on Graphics, Vision and Image Processing (GVIP-05), Cairo, Egypt, 2005.

[14] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf.

[15] DES Encryption Standard (DES), National Bureau of Standard (U.S.). *Federal Information Processing Standards Publication 46*, National Technical Information Service, Springfield, VA, 1997.

[16] Daemen,J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard", Dr. Dobb's Journal, March 2001.

[17] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communication of the ACM*: 120-126, 1978.

[18] Pfitzmann, B. "Information hiding terminology",*Proc. First Workshop of Information Hiding Proceedings*, Cambridge, U.K., Lecture Notes in Computer Science, Vol.1174: 347-350, 1996.

[19] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*, 2001

[20] Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 18:01, 1999.

[21] Moulin P and Koetter R, "Data-hiding codes", Proceedings of the IEEE, 93 (12), pp 2083-2126, 2005

[22] Krenn, R., "Steganography and Steganalysis", http://www. krenn.nl/ univ/cry/steg/article.pdf

[23] Johnson N.F. and Jajodia S, "Exploring steganography:Seeing the Unseen", IEEE Computer, 31(2), pp 26-34, 1998.

****