A New Approach of Data Hiding in Images using Cryptography and Steganography

Pria Bharti
M.Tech. Scholar, CSE
OCT, Bhopal, India

Roopali Soni
Asst. Prof., CSE
OCT, Bhopal, India

ABSTRACT

Cryptography is the science of using mathematics to encrypt and decrypt data and Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. A novel scheme for the embedding data in images is CrypSteg in this method combined cryptography and Steganography process in one algorithm. First we encrypt the data and then embed with image with new Steganography algorithm. The method is very efficient especially when applied to those images whose pixels are scattered homogeneously and for small data. The given image is partitioned into four level blocks, and the data will be embedded into selected the four diagonal sub-blocks values depend upon key. This algorithm only requires fewer steps and it can embed data efficiently without discarding image. Embedding 4 bits information in a 4*4 pixel block need to change very less pixels on average. Furthermore, the quality of the produced stego-images is better than that of other methods. The quality of stego-image is greatly improved when this algorithm is used.

Keywords

Cryptography, Steganography, Security, Data, Hiding, Quality,Iimage

1. INTRODUCTION

Cryptography and Steganography are well known and broadly used techniques that use information in order to cipher or cover their existence respectively. Steganography is the art and science of communicating in an approach which hides the existence of the communication [2]. The Steganography hides the message so it cannot be seen; Cryptography jumble a message so it cannot be understood [3]. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for improved concealment and security.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message for instance, might provoke suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In fact, steganography can be useful when the use of cryptography is illegal: where cryptography and strong encryption are banned, steganography can evade such policies to pass message covertly. However, steganography and cryptography differ in the way they are judged: steganography fails when the "enemy" is able to access the content of the cipher message, while cryptography fails when the "enemy" detects that there is a secret message present in the steganographic medium.

The subject area that study techniques for decoding cipher messages and detecting hide messages are called cryptanalysis and steganalysis [4]. The previous denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of expose the covert messages. The aim of this paper is to describe a method for integrating together cryptography and steganography through some media such as image, audio, video, etc.

In this paper, we propose a new algorithm for color full image. According to the method, a given image is partitioned into 4*4 blocks, and then takes only diagonally block for data hiding based on some rules. Various data hiding techniques, for instance, LSB (Least Significant Bit) approach, have been developed in recent years, most of them are for color and gray scale images and our method is also for color images.

Although Steganography is applicable to all data objects that contain redundancy, in this article, we consider color images only (although the techniques and methods for steganography and steganalysis that we present here apply to other data formats as well). People often transmit digital pictures over email and other Internet communication, and color image is one of the most common way for sending secret messages. Moreover, steganographic systems for the color image seem more interesting because the systems operate in a transform space and are not affected by visual attacks [15].Visual attack means intruders can easily detect the message on the low bit panel of an image which generally happen color image. Steganography as a means of obscuring data indeed, along with encryption, steganography is one of the fundamental ways by which data can be kept confidential. For better security we combine steganography and cryptography together in this paper. If we transmit the secret message with the help of this approach no one can easily detect the secret message easily. Stegnography is a special case of data hiding. The main goal of stegnography is to escape detection of secret message. Steganography uses in different form generally digital form of steganography are used for communication over the internet. In this paper digital form of stegnography is used that is hiding a message inside an image.

The rest of this paper is organized as follows: A detailed review on related research is discussed in section 2. The proposed method is presented in section 3. Experimental analysis and discussion is given in section 4. Finally, conclusion will be presented in section 5.

2. RELATED RESEARCH

Earlier a problem "uneven embeddability" has been identified in [12], in which the "flippable" pixels were distributed uniformly throughout the image by a random shuffling key. They handled this problem by embedding the watermark adaptively in those embeddable blocks.

In [11], the flipping priorities are computed by partitioned an image into 3*3 sub blocks and then modifying the total number of black pixels to be either odd or even embeds data bits. The flipping priorities are determined by considering smoothness and connectivity which are related to human observation. The smoothness is measured by horizontal, vertical, diagonal and anti-diagonal transitions in a 3*3 window, and connectivity is measured by the number of the black and white clusters. Some images require a shuffling key in order to distribute the "flippable" pixels all over the image.

Choosing the randomness for the embedding locations creates poor visual effects despite the large capacity. Improvements over the visual quality is made by choosing the edge pixels in their paper that is the problem in [12]

In [12], the proposed scheme uses a secret key and a weight matrix to protect the hidden data, it also uses a weight matrix to enhance the data hiding ratio. The operator XOR is adopted so that the keys can not be compromised easily. The original image is partitioned into blocks of size m*n. In each m*n block Fi, b1, b2,…,br is the r bits of data which will be embedded into the block by the invariant I1.

I1: d=b1b2….br - SUM [(Fi q K) q W] (mod 2r)

In invariant I1, let ⊕ be the bitwise exclusive-OR, ⊗ be the pair-wise multiplication operator on two equal size integer matrices. The embedded data will be extracted by the invariant I2.

I2: b1b2….br = SUM [(Fi q K) q W] (mod 2r)

Given an m*n host image, the scheme can hide as many as log2 (mn+1) bits of data in the image. However the connectivity issue has not been taken into deliberation during the embedding process.

In [5], Pan et al. proposed a novel data hiding method by partitioning an image into blocks, where each block was repartitioned into overlapping sub-blocks. Each sub-block is connected with a level number according to its pattern, indicating power on visibility by assumed change of the central pixel in the sub-block. Data will be concealed by changing the central pixel in a sub-block.

In [6], the LSB is the most popular Steganography method. It covers the secret message in the RGB image based on it its binary coding. Figure 1 presents an example about pixel values and shows the secret message. LSB algorithm is used to hide the secret messages by using algorithm 1. LSB makes the changes in the image resolution quite clear as well as it is easy to attack [17].

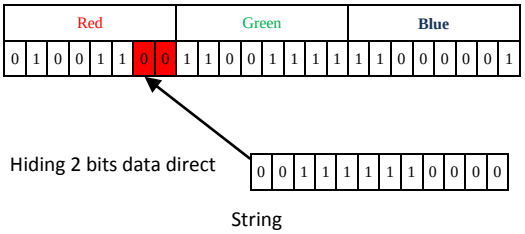

Figure 1. Least Significant Bit Hiding Technique

Algorithm (1) Least Significant Bit Hiding Algorithm.
Inputs: RGB image, secret message and the password.
Output: Stego image.

Begin
scan the image row by row and encode it in binary.
encode the secret message in binary.
check the size of the image and the size of the secret message.
start sub-iteration 1:
choose one pixel of the image randomly
divide the image into three parts (Red, Green and Blue parts)
hide two by two bits of the secret message in each part of the pixel in the two least significant bits.
set the image with the new values.
end sub-iteration 1.
set the image with the new values and save it.
End

3. THE PROPOSED METHOD

Steganography is not the same as cryptography data hiding techniques have been widely used to broadcast of hiding secret message for long time. Assuring data security is a big dispute for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide protection, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 2.In color image (e.g. scanned image) there are 3 color data values for one pixel, that is, red, green and blue. To save storage, there is 24 bit representation for each pixel. So hiding without significant distortions is very difficult for color images. As mentioned that arbitrarily flipping a pixel in a color image could be easily noticed. So only pixels on the boundary may be modified, and it also needs some constraints. Based on this criterion, in this paper propose a new method. The new method consists of two parts: embedding and extraction process. The entire process of embedding and extraction is illustrated in Fig. 2.

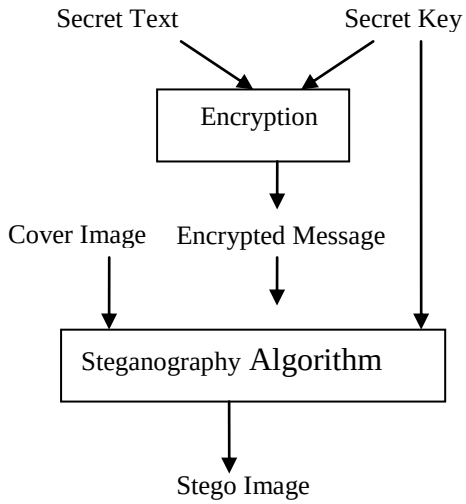

Fig.2 Block Diagram of algorithm

3.1 EMBEDDING PROCESS

The embedding process involves partitioning the original image into blocks, calculating characteristic values from the blocks and hiding data process. More details will be discussed in the following subsections.

3.1.1 ENCRYPTION (Secret Text To Encrypted Text)

Input: Secret Text and Secret Key
Output: Encrypted Text
Algorithm:

Step 1 : Concate Key 8 Times and then Choose first eight characters from KEY as (c1,c2,c3,c4, c5,c6,c7,c8)

Step 2: Convert each character (o/p of Step1) into ASCII and sum and divide from 1000 and reminder of this process is our Final Key of three digit number (N1, N2, N3)

Step 3: according to these three numbers (N1, N2, N3) we change our original message into cipher message we use shift encryption and

every 1,4,7,…. character shift by N1

every 2,5,8,…..character shift by N2

every 3,6,9,….character shift by N3 and we get cipher text

3.1.2 STEGANOGRAPHY

Suppose we have an image P which dimension is exactly divided by 4 and we partitioned image into 4*4 sized blocks. Partitioned block Fig 3(a) illustrates the partitioned block diagram for the original image P.

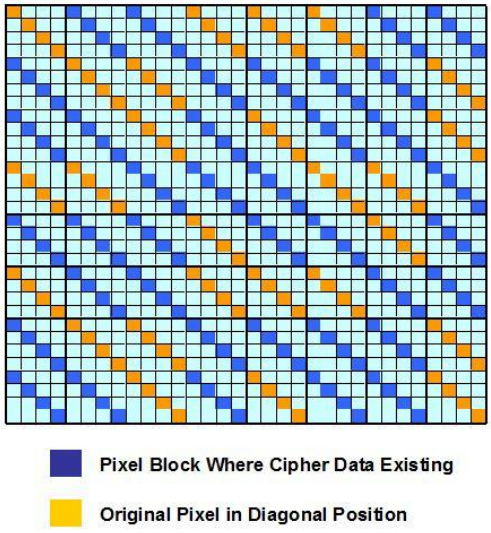

Fig 3(a) image Block format

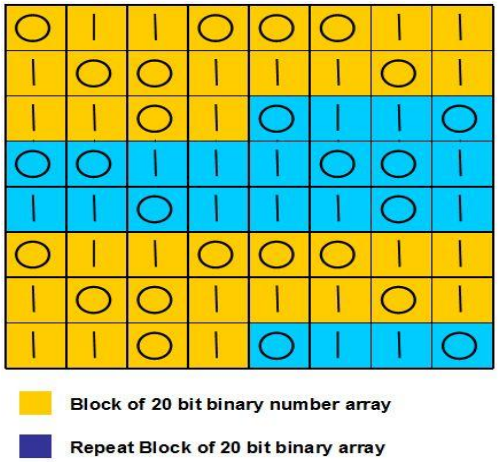

Fig 3(b) Cipher Data in Image

STEGANOGRAPHY ALGORITHM (IMAGE TO STEGO IMAGE)

Input: Secret Text, Secret Key, Image

Output: Stego Image
Algorithm:

Step 1: For Placing Data into images pixel first we will calculate DataPositionArray by concatenating of ASCII of N1, N2 and N3.

Step 2: Choose first 20 characters from DataPositionArray which is 24 characters long

Step 3: Count 1 in this 20 character long DataPositionArray
Step 4: Calculate size of Cipher Text (StrLen) in Bites Strlen=StringLength(ciphertext) * 8
Step 5: Now SizeOfImage(Length X Height) should be greater than Show The Minimum Image Size (Length X Height) as that [(CountOne/20)*(1 /4)* (Length*Height)] > StrLen Convert cipher text into array of bits and then make 4 X 4 pixel Block and choose block according to DataPositionArray
Step 6: Convert LSB Bit of block Diagonal pixel
After inserting all cipher text bit we get final image

3.2 EXTRACTION ALGORITHM

Input: Stego Image, Secret Key

Output: Plain Text
Algorithm:

Step 1: Receiving the stegoimage P.
Step 2: Convert image into 4X4 pixel Block as like of embedding algorithm.
Step 3: Choose Diagonal pixel according to datapositionarray and collect the LSB of diagonal pixel from selected block and make Cipher Text.

Step 4: This Cipher Text is input for decryption algorithm which is reverse of encryption algorithm and gets plain text.

4. EXPERIMENTAL RESULTS

The algorithm is code in Matlab and run on a Windows 7 platform. The method is applied to several color images. In our experiments, we use 32 Bytes English text document and 512X512 'lenna' image. Figure 4.1 illustrates a 512X512 original image and we can hide 256 bits in the original image which is shown in Figure 4.1 The stegoimage is shown in Figure 4.2 are embedded in it using the proposed techniques. The pixels in 'lenna' image are very approximately uniformly distributed; therefore, it is very difficult to detect the hidden data by naked eyes.

Fig 4.1 Original image

Fig 4.2 stego image

Other result comparison graphs of original and stego image histograms are

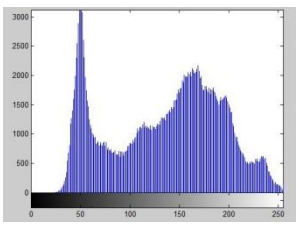

Fig 4.3(a) histogram of red colour of original image

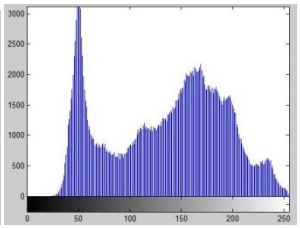

Fig 4.3(a) histogram of red colour of Stego image

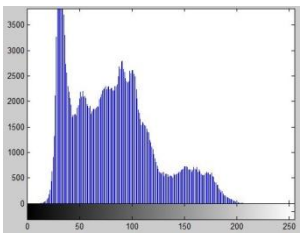

Fig 4.4(a) histogram of green colour of original image

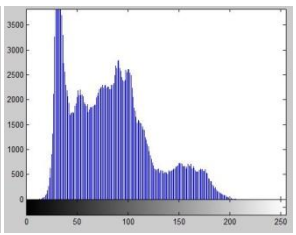

Fig 4.4(a) histogram of green colour of Stego image

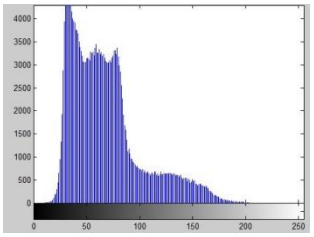

Fig 4.4(a) histogram of blue colour of original image

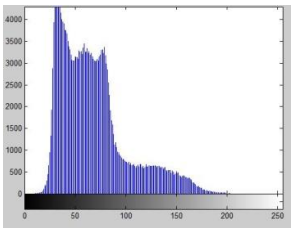

Fig 4.4(a) histogram of blue colour of Stego image

In this paper successfully applied the proposed algorithm on commonly used color images such as Lena, Baboon and Boat color test images; only one color plane is applied by the algorithm.

Table I
TEST RESULTS FOR 512X512X24 COLOR IMAGES

Comparison of LSB and Our Algorithm	Lena		Baboon	
	LSB	Our Algorithm	LSB	Our Algorithm
PSNR(dB)	36.3	41	35.1	37
Capacity (bits)	788	812	570	598
Robustness	.8	.7	1.6	1.4

Note that there is no noise in all of tests since the proposed algorithm does not use modulo-256 addition. The embedding capacity can range from 512 to 1024 bits for the purpose of authentication, and it can be adjusted by changing the block size for other applications. As shown later the PSNR is much higher than that obtained by using the method in [17]. It is noted that the data embedding capacity and the PSNR of the marked image versus the original image can be adjusted according to the password (key). Since these two performance parameters are usually conflicting each other in the sense that if the embedding capacity is improved, the PSNR will drop and vice versa, there is usually a tradeoff between the data embedding capacity and the PSNR of the marked image versus the original image for a targeted application.

5. CONCLUSION

In this paper propose a new method to embed data in color images. This method shows its larger capacity for hiding data than other methods without loss of imperceptibility. 4 bits data can be embedded in a 4*4 block and some blue part of pixels need to be changed on average. Experimental results show that the method is very efficient especially when applied to those binary images whose color pixels are distributed nearly uniformly.

6. REFERENCES

[1] Yambem Jina Chanu, Kh. Manglem Singh ,Themrichon Tuithung, " Image Steganography and Steganalysis: A Survey," International Journal of Computer Applications (0975 – 8887) Volume 52– No.2, August 2012 ,pp.1-11

[2] Bhattacharyya, S.; Khan, A.; Nandi, A.; Dasmalakar, A.; Roy, S.; Sanyal, G.; , "Pixel mapping method (PMM) based bit plane complexity segmentation (BPCS) steganography," Information and Communication Technologies (WICT), 2011 World Congress on , vol., no., pp.36-41, 11-14 Dec. 2011.

[3] Almohammad, A.; Ghinea, G.; Hierons, R.M.; , "JPEG Steganography: A Performance Evaluation of Quantization Tables," Advanced Information Networking and Applications, 2009. AINA '09. International Conference on , vol., no., pp.471-478, 26-29 May 2009.

[4] Abboud, G.; Marean, J.; Yampolskiy, R.V.; , "Steganography and Visual Cryptography in Computer Forensics," Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on , vol., no., pp.25-32, 20-20 May 2010.

[5] Li Zongqing; Zhang Hongbin; , "A New Data Hiding Method in Binary Images," Innovative Computing, Information and Control, 2006. ICICIC '06. First International Conference on , vol.3, no., pp.66-69, Aug. 30 2006-Sept. 1 2006.

[6] M. Al-Shatnawi, "A new method in image steganography with improved image quality"Appl. Math. Sci., Vol. 6, 2012, no. 77-80, 3907-3915.

[7] Neeta, D.; Snehal, K.; Jacobs, D.; , "Implementation of LSB Steganography and Its Evaluation for Various Bits," Digital Information Management, 2006 1st International Conference on , vol., no., pp.173-178, 6-6 Dec. 2006.

[8] Wai Wai Zin; Than Naing Soe; , "Implementation and analysis of three steganographic approaches," Computer Research and Development (ICCRD), 2011 3rd International Conference on , vol.2, no., pp.456-460, 11-13 March 2011.

[9] Bin Li; Yanmei Fang; Jiwu Huang; , "Steganalysis of Multiple-Base Notational System Steganography," Signal Processing Letters, IEEE , vol.15, no., pp.493-496, 2008.

[10] Yu Qiudong; Xiao-wei Liu; , "A New LSB Matching Steganographic Method Based on Steganographic Information Table," Intelligent Networks and Intelligent Systems, 2009. ICINIS '09. Second International Conference on , vol., no., pp.362-365, 1-3 Nov. 2009.

[11] Min Wu; Tang, E.; Lin, B.; , "Data hiding in digital binary image," Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on , vol.1, no., pp.393-396 vol.1, 2000.

[12] Yang, H.; Kot, A.C.; , "Pattern-Based Data Hiding for Binary Image Authentication by Connectivity-Preserving," Multimedia, IEEE Transactions on , vol.9, no.3, pp.475-486, April 2007.

[13] Hopper, N.; von Ahn, L.; Langford, J.; , "Provably Secure Steganography," Computers, IEEE Transactions on , vol.58, no.5, pp.662-676, May 2009.

[14] Ghoshal, N.; Mandal, J.K.; , "A steganographic scheme for colour image authentication (SSCIA)," Recent Trends in Information Technology (ICRTIT), 2011 International Conference on , vol., no., pp.826-831, 3-5 June 2011.

[15] Hawi, T.A.; Qutayri, M.A.; Barada, H.; , "Steganalysis attacks on stego-images using stego-signatures and statistical image properties," *TENCON 2004. 2004 IEEE Region 10 Conference* , vol.B, no., pp. 104- 107 Vol. 2, 21-24 Nov. 2004.

[16] Johnson, N.F.; Jajodia, S.; , "Steganalysis: the investigation of hidden information," *Information Technology Conference, 1998. IEEE* , vol., no., pp.113-116, 1-3 Sep 1998

[17] Khan, M.K.; Naseem, M.; Hussain, I.M.; Ajmal, A.; , "Distributed Least Significant Bit technique for data hiding in images," *Multitopic Conference (INMIC), 2011 IEEE 14th International* , vol., no., pp.149-154, 22-24 Dec. 2011

[18] C. De Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 97–105,Mar. 2003.