Data Hiding in Images Using Some Efficient Steganography Techniques

Chandreyee Maiti[*], Debanjana Baksi, Ipsita Zamider, Pinky Gorai,
and Dakshina Ranjan Kisku

Department of Computer Science and Information Technology,
Asansol Engineering College, Kanyapur,
Asansol – 713305, India
{chandreyee.jannat,debbie_2k6,er.pink07_it}@yahoo.co.in,
ipsita.zamider@rediffmail.com,
drkisku@ieee.org

Abstract. Steganography is the art of hiding data in a seemingly innocuous cover medium. For example – any sensitive data can be hidden inside a digital image. Steganography provides better security than cryptography because cryptography hides the contents of the message but not the existence of the message. So no one apart from the authorized sender and receiver will be aware of the existence of the secret data. Steganographic messages are often first encrypted by some traditional means and then a cover image is modified in some way to contain the encrypted message. The detection of steganographically encoded packages is called steganalysis. In this paper, we propose three efficient Steganography techniques that are used for hiding secret messages. They are LSB based Steganography, Steganography using the last two significant bits and Steganography using diagonal pixels of the image. Symmetric and asymmetric key cryptography has been used to encrypt the message.

Keywords: Steganography, Steganalysis, Cryptography, Data Hiding.

1 Introduction

Data security [1]–[3] over the networks is an important challenge for researchers and computer engineers for decades. Internet is a great convenience which offers secure data communication of important messages, secret information, variety of images and documents. In order to prevent the unauthorized access of important messages and images from malicious fraudsters, one need to make it more secure by sending the encrypted messages over the networks. To accomplish and build such secure systems, many data hiding and encryption techniques have been proposed in the last few decades. Both the data hiding [3] and encryption techniques [3] are found to be the main mechanisms in data security. However, use of former mechanism has been increasing recently due to some demerits have been found in the later mechanism.

[*] Corresponding author.

T.-h. Kim et al. (Eds.): SIP 2011, CCIS 260, pp. 195–203, 2011.

The formal mechanism of data encryption [3], [5] uses the method to convert a message into a ciphertext message by using some encryption algorithm and the ciphertext message is then sent to the recipient who has the authorization to receive and get the original message. To receive the original message which has been sent by the sender, recipient uses a key to obtain the decrypted message. Any malicious user who does not have the key cannot break the security of ciphertext which looks like some meaningless code. Though data encryption is proved to be a secure method to hide data, it has some weaknesses. For example, sometimes appearance of ciphertexts could give a clear impulse to an unauthorized user and this might lead to unauthorized access to the original content by breaking it. As a result the original receiver would not be able to receive the cipher texts sent by the sender. Often unauthorized users may take advantage by destroying the cipher text when it cannot be recovered. Another major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually decrypt the data. For this reason research on data hiding has been increasing recently.

A solution to this problem is data hiding. Data hiding techniques [3]-[4] could play a major role to embed important data into multimedia files such as images, videos or sounds. Because digital images are insensitive to human visual system, therefore images could be good cover carriers. Data hiding has two major applications [5] – watermarking and steganography. Watermarking merely extends the cover source with extra information. Steganographic techniques are used to store watermarks in data.

Steganography [4]-[5] is an ancient art of hiding messages for making the messages not detectable to malicious users. In this case, no substitution or permutation was used. The hidden message is plain, but unsuspected by the reader. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood. Steganography has been widely used, including in recent historical times and the present day. Possible permutations are endless and known examples include: (i) hidden messages within wax tablets, (ii) hidden messages on messenger's body, (iii) hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages, and (iv) agents used photographically produced microdots to send information back and forth.

Steganography includes the concealment of information within computer files. In digital Steganography, electronic communications may include Steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for Steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it. Digital Steganography has three basic components. (a) Obtain the data to be hidden, i.e., secret message, (b) embed the secret message into the cover medium, i.e., images, sounds or videos, etc., and (c) lastly, obtain the stego-carrier to be sent.

In the last decades, many Steganography based data hiding techniques have been proposed in [4]-[6]. There exist plenty of Steganography based data hiding techniques which use LSB based algorithms for hiding the secret messages by embedding it into cover media like images. In [7], authors proposed a data hiding technique which is based on simple LSB substitution method by selecting optimal numbers of *k* LSB substitution method to solve the problem while *k* is found to be large. Another work proposed in [8] uses dynamic programming approach to find optimal LSB which later embedded into image. The proposed method reduces the computation time while it is compared the work discussed in [7] uses approximate optimal LSB. Sometimes LSB based substitution method is not sufficient to generate for embedding the secret message into an image. Therefore, the authors in [9] uses genetic algorithm to find an optimal substitution matrix for embedding of the secret message into the mages. Authors also use local pixel adjustment process (LPAP) to improve the quality of the stego-image as carrier.

In this paper, substitution based three different Steganography techniques have been presented and they are LSB based Steganography with the least significant bit, Steganography using last two significant bits and LSB based Steganography using diagonal pixels of the image. However, LSB based techniques are well-known techniques whereas the Steganography using diagonal pixels of the image is the novel technique, which is proposed in this paper along with the well-known techniques.

The rest of the paper is organized as follows. Section 2 has introduced the basic paradigm of LSB based data hiding operation. The next section presents the proposed Steganographic techniques. Results obtained from the proposed techniques are discussed in Section 4 and conclusion is made in the last section.

2 Preliminaries

To perform the experiment, gray scale and color images are taken and then Steganography techniques are applied by generating the LSB based substitution matrices. The texts, which are used as the hidden texts are evenly distributed among all the pixels of the MxN image matrix. Finally, the resultant stego image is generated.

2.1 Basic Paradigm of LSB Based Data Hiding Operation

Since the rightmost bits are used for LSB substitution [6]-[9] in each pixel in the given image, therefore the first operation used rightmost bit and the second operation used rightmost two bits for LSB substitution. The last operation uses diagonal pixels of an image and the rightmost one bit of those diagonal pixels is used for substitution. In these operations, 8-bit grayscale and 24-bit color images are used. In 8-bit grayscale image, rightmost two bits are used in each pixel and rightmost bit is used for diagonal pixels also. The color image uses three color components – red, green and blue which constitute each pixel. The identical phenomenon is used in color image as that of grayscale image. However, for the color image three different matrices are generated and therefore, LSB substitution is used separately for these three matrices.

Let, $I_{Grayscale}$ be the 8-bit grayscale cover image of size $P_{I_{gray}} \times Q_{I_{gray}}$ pixels. It can be represented by

$$I_{gray} = \left\{ x_{ij} \mid 0 \le i \le P_{I_{gray}},\ \ 0 \le j \le Q_{I_{gray}},\ \ x_{ij} \in \{0,1,2,...,255\} \right\} \quad (1)$$

Also let, I_{color} be the 24-bit color cover image of size $P_{I_{color}} \times Q_{I_{color}} \times 3$ pixels. Therefore, it can be represented for three color components red, green and blue by

$$\begin{aligned} I_{color-red} &= \left\{ x_{ij}^{red} \mid 0 \le i \le P_{I_{color-red}},\ 0 \le j \le Q_{I_{color-red}},\ x_{ij}^{red} \in \{0,1,2,...,255\} \right\} \\ I_{color-green} &= \left\{ x_{ij}^{green} \mid 0 \le i \le P_{I_{color-green}},\ 0 \le j \le Q_{I_{color-green}},\ x_{ij}^{green} \in \{0,1,2,...,255\} \right\} \quad (2) \\ I_{color-blue} &= \left\{ x_{ij}^{blue} \mid 0 \le i \le P_{I_{color-blue}},\ 0 \le j \le Q_{I_{color-blue}},\ x_{ij}^{blue} \in \{0,1,2,...,255\} \right\} \end{aligned}$$

Suppose S is the n – bit secret message and it can be defined by

$$S = \left\{ s_i \mid 0 \le i \le n,\ \ s_i \in \{0,1\} \right\} \tag{3}$$

The secret message S of n – bits is to be embedded into the 8-bit grayscale as well as 24-bit color image with three color components. The secret message S is rearranged to form a k – bit virtual image S' which can be described as

$$S' = \left\{ s_i^{'} \mid 0 \le i \le n',\ \ s_i^{'} \in \{0,1,....,2^{k-1}\} \right\}; \tag{4}$$

where $n' = P_{I_{gray}} \times Q_{I_{gray}}$ and $n' = P_{I_{color}} \times Q_{I_{color}}$. Now a mapping is defined between the secret messages $S = \{s_i\}$ and the embedded message $S' = \{s_i^{'}\}$. Further this can be described by the following mathematical formulation

$$s_i^{'} = \sum_{j=0}^{k-1} s_i \times k + j \times 2^{k-1-j} \tag{5}$$

At this stage, all the pixels are chosen from the cover image where the rightmost one bit and rightmost two bits are chosen for the proposed first and second methods and rightmost one bit is selected for the third method in which a subset of pixels are selected containing diagonal pixels only of the image matrix. Hence, the embedding process is completed by replacing the k *(k=1,2)* LSBs of each pixel by $s_i^{'}$. Mathematically, each pixel is storing the k – bit message to form the stego-pixel as follows.

$$x_i^{'} = x_i \bmod\ 2^k + s_i^{'} \tag{6}$$

Embedding process for a subset of pixels which contain diagonal pixels only is completed by replacing the k LSBs of each pixel in the subset by $s_i^{'}$. Mathematically, it can be represented by

$$x_i^{'} = x_i - x_i \bmod\ 2^k + s_i^{'} \tag{7}$$

In Equations (6) and (7), x_i and $x_i^{'}$ be the original pixel in cover image and stego-pixel in stego-image respectively.

The embedded message extraction process is accomplished from stego-image by without referring to original cover image. Therefore, *k* LSBs of all pixels and subset of pixels are extracted and reconstruct the secret message bits. The embedded message can be extracted from stego-image by the following mathematical formulation

$$s_i^{'} = x_i^{'} \bmod\ 2^k \tag{8}$$

3 LSB Substitution Based Steganographic Techniques

3.1 LSB Substitution in Grayscale Image

A grey scale digital image is an image in which the value of each pixel carries only intensity information. They are also known as black and white images and are composed of shades of grey varying from black at the weakest intensity to white at the strongest. The proposed Steganographic implementation chooses rightmost LSBs (*k = 1, 2*) of each pixel to replace with the secret message bits. The secret message is evenly distributed among all the pixels of the image matrix for the first and second method. However, for the last method a subset of diagonal pixels of the image matrix are used and the secret message is evenly distributed among the diagonal pixels only. The message is encoded in the least significant bit of each pixel in the cover image. This produces no visible change in the original image. The process of LSB substitution in grayscale image is given below.

- An image is read. In case of a gray scale image, a 2-dimensional matrix of unsigned integers with values between 0 and 255 is obtained.
- The pixels are extracted accordingly and converted to binary.
- The secret message can be encrypted using symmetric key or RSA cryptographic techniques.
- The text is encoded in the least significant bits of the pixels. The pixel values of the matrix are changed with a value of (+1) or (-1).
- The pixels are re-inserted into the image.
- Save the image using any lossless compression technique.

3.2 LSB Substitution in Color Image

Each pixel in RGB image is specified by three values, one each for red, blue and green color components. The RGB image is represented by row×column×3 array of class uint8/uint16 or double. In this section, LSB substitution based Steganography is presented where RGB color image is used. The secret message or plaintext is evenly distributed among the three color components red, green and blue. A subset of pixels of the n^{th} column or diagonal elements of each dimension of an image is used. The secret message has been encoded in the least significant bits of these pixels. The process of LSB substitution in color image is given below.

- A RGB image of 3-D matrix is read and the pixel corresponding to the n^{th} column and diagonal elements of each dimension is extracted and converted into binary. The last significant bits are extracted from binary matrix.
- A secret message entered and which is encrypted using symmetric key or RSA cryptography techniques. The encrypted message is then converted to binary sequence.
- The message has been encoded in the bits of the n^{th} column or diagonal pixels and the secret message is evenly distributed among the three color components - red, green and blue.
- The extracted bits are changed according to the text bits and inserted into the binary matrix. Thus each bit is changed with a value of 1.

3.3 Steganalysis

Steganalysis [10] is the process of decoding the secret message from the stego-image. The appropriate pixels of the image, in which the text is stored, are extracted. The pixels are then converted into binary form. Eight bits are extracted at a time and converted into a string. The extracted string can be decrypted using the decryption key. The original message is obtained after string manipulation. In Figure 1, the block diagram of Steganalysis is illustrated. After obtaining the Steganographic or stego-image Steganalysis approach is applied while decryption key is available and finally original message is obtained.

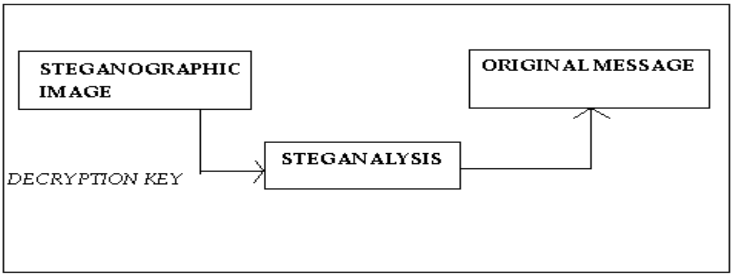

Fig. 1. Block Diagram of Steganalysis

3.4 Message Encryption Using RSA Algorithm

To increase the security of the message hidden inside the Stego-image, the message can be encrypted using RSA [11]. The encrypted message can then be hidden using any of Steganographic techniques. Firstly, plaintext message is converted into cipher text using encryption key determined from initial constraints and this cipher text is then embedded into an image using the proposed Steganographic techniques. Finally, recipient uses the decryption key or private key to decrypt the cipher text message and this decryption key is determined from the preliminary considerations of prime numbers and its associated operations. The RSA algorithm is described below.

Step 1: Choose two large prime numbers p and q.

Step 2: Calculate $n = p \times q$.

Step 3: Calculate $\phi = (p-1) \times (q-1)$.

Step 4: Choose the public key (encryption key) e such that it is not a factor of ϕ and also calculate private key (decryption key) d so that $d \times e = 1 \ mod \ \phi$.

Step 5: Make e and n public and keep ϕ and d secret.

Step 6: Calculate cipher text ct, such that $ct = pt^e \ mod \ (n)$, where pt is the plain text.

Step 7: The message is decrypted using the formula $pt = ct^d \ mod \ (n)$.

4 Results and Discussions

None of the Steganographic methods used in this work produce any visible change in the color or appearance of the image. The size of the image does not change. The proposed work provides two levels of security. It hides the existence of secret message from malicious users. Since the message is further encrypted using RSA encryption algorithm, an intruder will be unable to decipher the image. The proposed three LSB substitution based steganographic techniques have been tested with grayscale and color images. In this section, results of first two methods are not shown. Since these two techniques are found to be simple when compared with the third method in which LSB substitution is made with the diagonal pixels. Figure 2 and Figure 3 show the results obtained by applying the third method which uses n^{th} column of diagonal pixels for LSB substitution. In Figure 2, original grayscale image is taken for steganography application and a resultant image stego-image is obtained. In Experiment with grayscale image, only one matrix is generated and considered for LSB substitution. In contrast, RGB image contains three color components – red, green and blue and due to that 3D matrix is generated. These three matrices are treated separately for LSB substitution for each color component. In Figure 3, left RGB image shows cover image whereas the right image depicts stego-image in which the secret message is hidden. In this experiment, 24-bit true color image is used. In Figure 4, original matrix which is generated from the original image is shown in left and the stego matrix which is generated from stego-image is shown in right. In this stego matrix the secret message is hidden and evenly distributed among all diagonal pixels.

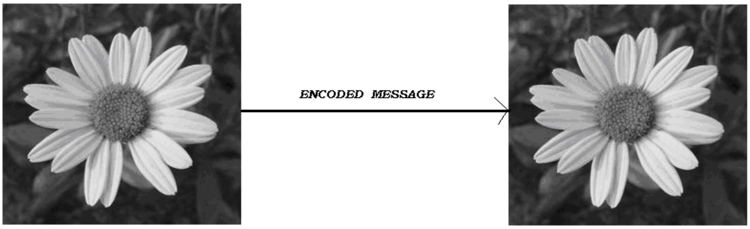

Fig. 2. Original Image (left) and Stego-Image (left) are shown

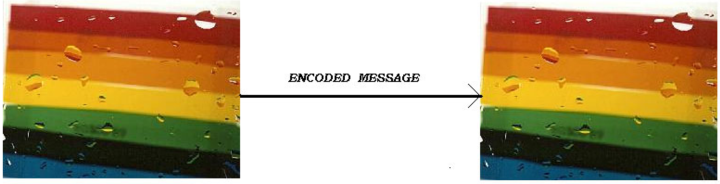

Fig. 3. Original (left) and Stego (right) Images are shown

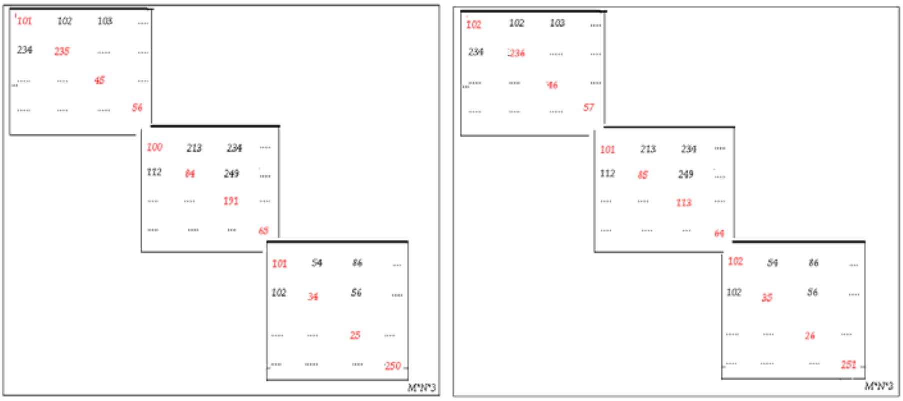

Fig. 4. Original Matrix (left) and Matrix with Encoded Texts (right) are shown

4.1 Limitations of the Proposed Techniques

A few demerits have been determined from the proposed methods. Since, the amount of data hidden inside an image depends upon its size. Therefore, a fairly large cover image has to be selected. Secondly, a lossy compression technique cannot be used in compressing an image concealing a secret message. The hidden message will not survive this operation and lost after the transformation. Lastly, any distortion in the image during transmission may lead to loss of the secret message.

5 Conclusion

This paper proposes three simple and efficient steganographic techniques which can be used to allow the users to securely transmit a confidential message through images without any detection by an intruder or malicious users. The methods presented do not produce any visible change in the cover image. Among these three methods the last steganographic method can hide maximum information by selecting the diagonal pixels only from the image matrix for LSB substitution. The proposed methods show remarkable performance in terms of accuracy and less distortions of extracted secret message from stego-image while these Steganographic techniques are used.

References

1. Johnson, N.F., Jajodia, S.: Exploring Steganography: Seeing the Unseen. Computer 31(2), 26–34 (1998)
2. Artz, D.: Digital Steganography: Hiding Data within Data. In: IEEE Internet Computing, pp. 75–80 (2001)
3. Li, X., Wang, J.: A Steganographic Method based Upon JPEG and Particle Swarm Optimization Algorithm. Information Sciences 177(15), 3099–3109 (2007)
4. Chandramouli, R., Memon, N.D.: Analysis of LSB based image steganography techniques. In: IEEE International Conference on Image Processing, vol. 3, pp. 1019–1022 (2001)
5. Kutter, M., Hartung, F.: Introduction to Watermarking Techniques in Information Techniques for Steganography and Digital Watermarking. In: Katzenbeisser, S.C. (ed.), pp. 97–119. Artec House (1999)
6. Mohamed, M., Al-Afari, F., Bamatraf, M.: Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation. International Arab Journal of e-Technology 2(1), 11–17 (2011)
7. Wang, R.Z., Lin, C.F., Lin, J.C.: Image Hiding by Optimal LSB Substitution and Genetic Algorithm. Pattern Recognition 34(3), 671–683 (2001)
8. Chang, C.C., Hsiaob, J.Y., Chan, C.S.: Finding Optimal Least-Significant-bit Substitution in Image Hiding by Dynamic Programming Strategy. Pattern Recognition 36, 1583–1595 (2003)
9. Chan, C.K., Cheng, L.M.: Hiding Data in Images by Simple LSB Substitution. Pattern Recognition 37(3), 469–474 (2004)
10. Krenn, J.R.: Steganography and Steganalysis. XIDC.NL (2004)
11. Rivest, R., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21(2), 120–126 (1978)