STEGANOGRAPHY TECHNIQUE FOR HIDING DATA IN AN IMAGE

[1]Dr.K. Prasanthi Jasmine, [2]B. Bharath Kumar Reddy, [3]G. Suresh Babu,[4]J. Praveen Kumar
[1]Professor, [2]Student,[3]Student,[4]Student
[1]Electronics and Communication Department,
[1]Andhra Loyola Institute of Engineering & Technology, Vijayawada, India.

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 proposed efficient Steganography techniques that are used for hiding secret messages i.e. LSB Steganography using the last two significant bits. Symmetric and asymmetric** key has **been used to secure the data from the unauthorized persons.**

Index Terms - Steganography, Steganalysis, Cryptography, Data hiding

1. Introduction

With rapid developments in the technology of telecommunication especially the internet and mobile networks have the domain of information transmission, which in turn present new challenges for protecting the information from unauthorized access and use, the data integrity and confidentially are required. Data security over the networks is an important challenge for researchers and computer engineers for decades. Satellite communication has been used for transfer of images and data to far end places. In order to prevent the unauthorized to access the data we have to encrypt the data that is being send through the network. 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 and encryption techniques are found to be the main mechanisms in data security. However, the use of formal mechanisms for hiding the data has come into process recently.

The formal mechanism of data encryption uses the ciphertext that is been used for the transmission to the required person and this text is been embedded and a security key is been used for the data encryption. To receive the original message which has been sent by the sender, receiver has to use the key that is been used at the sender. Any misleanous person who tries to break the key gets a garbage code for his key. 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 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. By this the unauthorized person who tries and didn't get the code may have the chance of destroying the ciphertext and another disadvantage is that the data is not been hidden. By this if the unauthorized person sits for more time he can retrieve the data that has been encrypted. For this reason, research on data hiding has been increasing recently.

A solution to this problem is data hiding. Data hiding techniques could play a major role to embed important data into multimedia files such as images, video's or sounds. Because digital images are insensitive to human visual system. Therefore, images could be good cover carriers. Data hiding has two major applications watermarking and steganography. Steganographic techniques are used to store watermarks in data. Steganography is an ancient art of hiding messages for making the messages not detectable to malicious users. Steganography is the science of invisible communication. Information is transmitted by hiding it in innocuous cover objects to maintain security and confidentiality. In image steganography the cover object is the image and information are embedded in to images which may be color, greyscale binary. A stego image is obtained from the cover image by accommodating the secret message into a digital image using some embedding algorithm that slightly modifies the cover image. In this case, no substitution or permutation was used. The hidden message is plain, but unsuspected by the reader.

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. 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. We 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.

In this paper, we proposed a technique i.e. substitution based on Steganography techniques using last two significant bits. However, LSB based techniques are well-known techniques whereas the Steganography using last pixels of the image is the novel technique, which is proposed in this paper. 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 technique. 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 substation matrices. The texts, which are used as the hidden texts are evenly distributed among all the pixels of the last significant bits. 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 in each pixel in the given image, therefore the first operation used rightmost two bits for LSB substitution. In this 8bit greyscale and 24-bit color images are used. In 8-bit grayscale image, rightmost two bits are used in each pixel. 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 greyscale 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 image of size $P_{I_{gray}}$ X $Q_{I_{gray}}$ Pixels.it can be represented by

$$I_{gray} = \{ X_{ij}\ 10 \le i \ge P_{I_{gray}}, 0 \le j \le Q_{I_{gray}}, X_{ij} \epsilon \{0,1..255\} \} \quad (1)$$

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

$$I_{color-red} = \{ X_{ij}^{red}\ 10 \le i \ge P_{I_{color-red}}, 0 \le j \le Q_{I_{color-red}}, \quad X_{ij}^{red} \epsilon \{0,1..255\} \}$$

$$I_{color-green} = \{ X_{ij}^{green}\ 10 \le i \ge P_{I_{color-green}}, 0 \le j \le Q_{I_{color-green}}, X_{ij}^{green} \epsilon \{0,1..255\} \} \quad (2)$$

$$I_{color-blue} = \{ X_{ij}^{blue}\ 10 \le i \ge P_{I_{color-blue}}, 0 \le j \le Q_{I_{color-blue}}, X_{ij}^{blue} \epsilon \{0,1..255\} \}$$

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

$$M = \{ M_i \; I \; 0 \le i \le n \ldots, M_i \in \{0, 1\} \} \quad (3)$$

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

$$M' = \{ M'_i \; I \; 0 \le i \le n' \;,\; M'_i \in \{0, 1, .. 2^{k-1}\} \} \;; \quad (4)$$

Where $n' = P_{\frac{i}{grey}} \; X \; Q_{\frac{I}{grey}}$ and $n' = P_{\frac{I}{grey}} \; X Q_{\frac{I}{grey}}$ .Now a mapping is defined between the secret M' = $\{M_i\}$ and the embedded message M' = $\{M_i\}$.

Further this can be described by the following mathematical formulation.

$$M'_i = \sum_{j=0}^{k-1} M_i \, X \, k + j \, X \, 2^{k-1-j} \quad (5)$$

At this stage, all the pixels are chosen from the cover image where the rightmost one bit and rightmost two bit 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 is storing the K-bit message to form the stego-pixel as follows.

$$X'_i = X_i \bmod 2^k + M'_i \quad (6)$$

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 M'_i. Mathematically it can be represented by

$$X'_i = X_i - X_i mod \; 2^k + M'_i \quad (7)$$

In Equations (6) and (7), X_I and X'_I 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

$$M'_i = X'_i \; mod \; 2^k \quad (8)$$

3 LSB Substitution Based on 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 which at the strongest. The purpose of steganography implementation chooses rightmost LSBs (K=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 greyscale 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.
- 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 nth column or diagonal elements of each dimension of an image is used. The secret message has 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 nth 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 nth 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

3.3 Block diagram of encryption

In the encryption phase we will embedded the data that is to be sent for the receiver. In order to do this, we are considering the cover image and the message that is to be sent. Here we are using the LSB algorithm for encrypting the message into the cover image. The encrypted image is called the stego-image where data is present. The stego-image is same as that of the cover image.

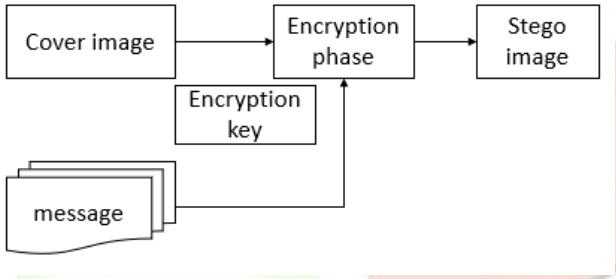

Fig. 1. Block Diagram of Encryption

3.4 Steganalysis

Steganalysis 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 2, 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 the original image is obtained.

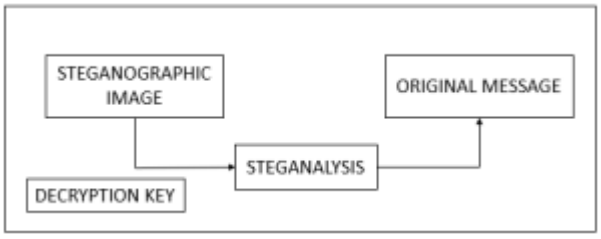

Fig. 2. Block Diagram of Steganalysis

3.5 Security using private key

To increase the security of the message hidden inside the Stego-image we are adding a private key. The key cannot be known to anyone except the sender. If the receiver needs to access the message he must get the code from the sender only. If not, the message cannot be retrieved.

4.Results and Discussions

The Steganographic method 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. The proposed two LSB substitution based steganographic techniques have been tested with grayscale and color images. In this section, results of proposed methods are shown. Figure 3 and Figure 4 show the results obtained by applying the proposed method. In Figure 3, original grayscale image is taken for steganography application and a resultant image stego-image is obtained.). In Figure 4, 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 original matrix which is generated from the original image is shown in left and the stego-image 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 last two significant bits.

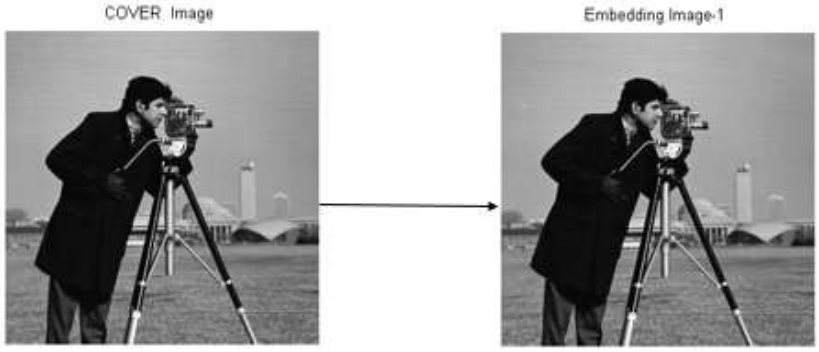

Fig 3: Original (Left) and Stego (right) images of grey are shown

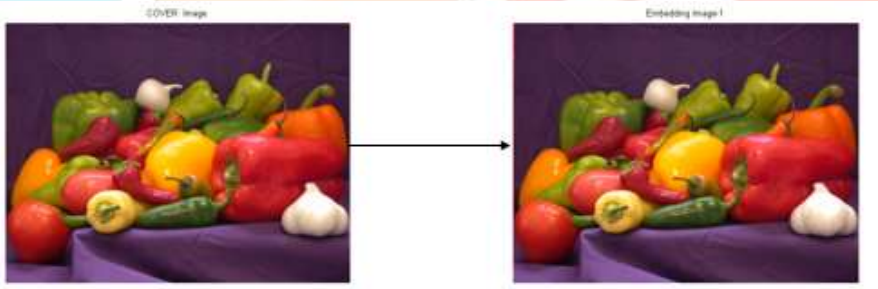

Fig 4. Original (Left) and Stego (right) images of color are shown

5.Conclusion

This paper proposes an efficient technique 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. This method is one of the best methods used for hiding data in an image. The proposed method shows remarkable performance in terms of accuracy and less distortions of extracted secret message from stego-image while these steganography technique is used. It also provides high security at the data retrieval. It is very fast and takes less time for retrieving the encrypted data.

References: -

1. A. Menezes, P. Oorschot, S. Vanstone, and A. J. Menezes, “Handbook of Applied Cryptography”, CRC Press, Boca Raton, FL, 1997.
2. S. Katzenbeisser S. and F. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House Press, 2000.
3. N. Provos N. and P. Honeyman, “Hide and seek: An introduction to steganography”, IEEE Security and Privacy, vol. 1, no.3, pp. 32-44, 200

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. M. Li, W. Cai, and Z. Tan, ‘‘A region-based multi-sensor image fusion scheme using pulse-coupled neural network,’’ Pattern Recognit. Lett., vol. 27, no. 16, pp. 1948–1956, 2006.
8. G. Bhatnagar, Q. M. J. Wu, and Z. Liu, ‘‘Directive contrast based multimodal medical image fusion in NSCT domain,’’ IEEE Trans. Multimedia, vol. 15, no. 5, pp. 1014–1024, Aug. 2013.
9. Accessed on Jan. 1, 2017. [Online]. Available: https://en.wikipedia.org/ wiki/Deep learning.
10. G. Swain and S. K. Lenka, “Steganography using one sided” CSI Transactions on ICT, vol. 1, no. 2, pp. 127–133, 2013.