LSB based Digital Image Steganography System

Rawan Mualla M. AlKhuwaytiri
Taibah University

Salah Eldin Z. Olaymi
Taibah University

ABSTRACT

Steganography can be defined as inserting information, such as a text file or a picture file into different types of files such as a picture file, audio file, or a video file.Digital picture steganography is a branch of computer science that is interested in inserting textual/pictorial confidential messages into digital pictures. The purpose of digital picture steganography is securing private and sensitive textual/pictorial information by inserting it into a shield digital picture. Nowadays, digital picture steganography has become an important topic since there is a need for securing digital information.In this paper, a digital picture steganography system is proposed. The proposed system is implemented as a desktop application. The system consists of two parts: confidential picture hiding and confidential picture extraction. To hide a confidential picture into a shield picture, both pictures are shuffled using Arnold Transform. Then, the confidential picture is encrypted and embedded into the shield picture using LSB technique. After that, the stego picture is de-shuffled using Arnold Inverse Transform. To take out a confidential picture from a stego picture, a stego picture is shuffled using Arnold Transform. Then the confidential picture is taken out from the LBS of stego picture. After that, the confidential picture is decrypted and de-shuffled using Arnold Inverse Transform. To evaluate the performance of the system, it was experimented in different gray scale images and PSNR and MSE were calculated and compared.

Keywords

Digital Picture, Steganography, Cryptography, Information Security.

1. INTRODUCTION

Steganography comes from a Greek term meaning confidential writing. The term "steganos" represents "covered" and "graphical" means writing. Steganography is hiding the confidential data, such as text or a digital picture, into another media file, such as a digital picture, an audio file, or a video recording, in such a way that only the receiver knows the existence of the confidential data.There are several real-life applications of steganography such as protection from data modifications, confidential communications, copyright protection, and confidential storage of data [1].

In this paper, a system for encrypting and hiding data in digital pictures is suggested. The suggested system is implemented as a desktop application using MATLAB software. The input of the system is cover picture and confidential pictures. The cover picture is used to hide the confidential picture. The proposed system consists of four phases. In the first phase, the cover picture as well as the confidential picture are divided into blocks. In the second phase, the cover picture and the confidential picture are shuffled. In the third phase, the confidential picture is encrypted using XOR encryption algorithm with random generated key. In the fourth phase, the encrypted confidential picture is embedded into the cover picture using Least Significant Bit (LSB) algorithm. The output of the system is a stego picture which is the cover picture with the embedded confidential picture.

The remainder of this paper is structured as follows. Section 2 presents different types of steganography and reviews some research articles for each type. Section 3 introduces the proposed system. The experiments are discussed in Section 4. Results are presented in Section 5. Conclusions and future work are given in Section 6.

2. LITERATURE REVIEW

There are three main techniques for hiding information in digital media: text hiding, picture/video hiding, and audio hiding.

2.1 Text Steganography

Text steganography is shown in Figure 1 where the input to the system is a shield text and a confidential message. Then, the system hides the message into the shield text and produces a stego text. The stego text is then stored in the computer hard drive or transmitted over a network such as the Internet. The last step is taking out the confidential message from the stego text by the receiver using a recovery algorithm.

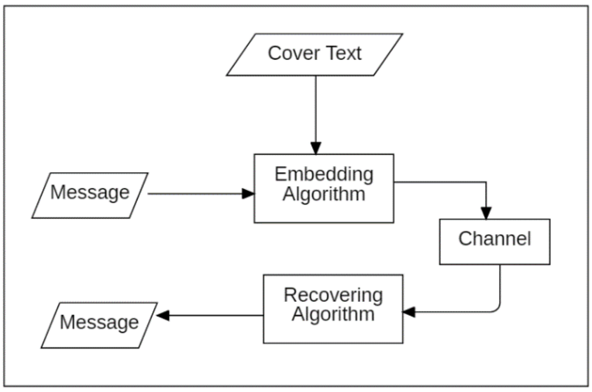

Figure 1. Text Steganography

L.Y. Por et al. [2], proposed a steganography system for hiding data into textual files. The proposed system is based on using spaces between paragraphs and between words in text file to hide confidential data. This method is advantageous because there are more whitespaces in the text than the presence of the term. It offers more room for data hiding. This technique dynamically generates the shield text based on the size of the confidential message.

M. Garg et al. [3], have suggested an HTML-document based text steganography method. The proposed system used HTML documents as a cover medium. According to the suggested method, the confidential data is inserted in HTML tags and their properties.

2.2 Picture/Video Steganography

In this technique, data is inserted into digital pictures/videos using different algorithms. Digital pictures and video files have great amount of insignificant information, which may be exploited to insert large amounts of data. There are two major types of this techniques. Hiding information in the spatial domain such as Least Significant Bit (LSB) and frequency domain method such as Discrete Cosine Transform (DCT)-based technique.

S. Laskar et al. [4], developed a technique for hiding information in digital pictures. The developed technique inserts the confidential data in the Least Significant Bit (LSB) of the shield picture. To make the technique more secure, the developed technique uses transposition cipher to encrypt the confidential data before inserting it into the shield picture.

P. Bhautmage et al [5], proposed a system for hiding information in digital videos. The confidential message is first ciphered using XOR operation with a random generated key. Then, the digital video is divided into frames. After that, the cipher confidential message is inserted into the video frames using LBS technique.

2.3 Audio Steganography

In this technique, data is embedded into digital audio file using different algorithms. Like digital pictures and video files, audio files have redundant contents which could be used to hide information.

K. Saroha et al. [6], proposed a steganography system for hiding digital pictures into digital audio files. The proposed system is based on using least significant bit algorithm for hiding a digital picture into an audio file. Three LSBs of the sound recording are used to insert the digital picture content.

3. PROPOSED SYSTEM

The system consists of two parts: Confidential Picture Insertion, and Confidential Picture Extraction.

3.1 Picture Insertion

Confidential Picture Insertion (CPI) part consists of four main steps which are shown in Figure. 2.

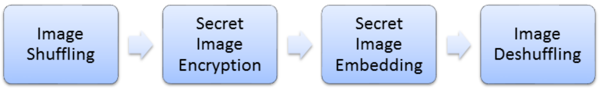

Figure 2. Picture Insertion

The input to this part is a shield picture and a confidential picture. The result from this part is a stego picture, which is the shield picture with the confidential picture inserted in it.

3.1.1 Picture Shuffling

In this step, both cover picture as well as embedded picture are shuffled using Arnold Chaotic Maps (ACM) algorithm. The cover picture as well as confidential picture to be embedded are both split into square areas of length 8 X 8 pixels. Then the pixel positions of the picture blocks are changed using Arnold Transform given by Equation (1) [7]. The purpose of this step is to improve the reliability of the algorithm by making extracting the embedded confidential picture difficult.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & m \\ n & nm-1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod(M) \qquad (1)$$

Where N is the size of the block, m variable and n variable are controlling variables, mod (A, N) is the remainder of dividing A by N, and (X, Y) are the coordinates of a pixel in the horizontal axis and vertical axis respectively.

3.1.2 Confidential Picture Encryption

In this step, the embedded picture is converted into binary and encrypted with a random generated key using XOR operation. The purpose of this step is to make the hiding algorithm stronger even if the hidden picture is extracted, it is difficult to decrypt it since the encryption key is unknown. Encryption using XOR has several advantages including it is fast, easy to implement, and difficult to break [8].

3.1.3 Confidential Picture Embedding

In this step, the encrypted confidential picture is inserted into the shield picture using Least Significant Bit (LSB) technique, where the LSB (lowest bit) of pixels of the shield picture are replaced by bits of the confidential picture [9].

3.1.4 Picture De-shuffling

In this step, positions of pixels of cover picture are changed with their original values using Inverse Arnold Transform given by Equation (2).

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} mn-1 & -m \\ -n & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod(M) \qquad (2)$$

Where N is the length of the picture, m variable and n variable are controlling variables, mod (A, N) is the remainder of dividing A by N.

3.2 Confidential Picture Extraction

Confidential Picture Extraction (CPE) part consists of four main modules which are shown in Figure 3.The input to this part is a stego picture and a key. The output from this part is the original confidential picture extracted from the stego picture.The steps of this part are the same steps of the confidential picture hiding part, but in reverse order.

The steps of this part are described as follows:

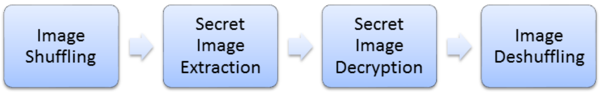

Figure 3 Confidential Picture Extraction

3.2.1 Picture Shuffling

In this step, the stego picture is split square areas of size 8 X 8. Then the pixels' positions are modified using Arnold Transform given by Equation (1)

3.2.2 Confidential Picture Extraction

In this step, the hidden confidential picture is taken out from LSBs (lowest bits) of the stego picture.

3.2.3 Confidential Picture Decryption

In this step, the extracted confidential picture is decrypted with the key provided by the user using XOR binary operation.

3.2.4 Picture De-shuffling

In this step, the extracted decrypted picture is de-shuffled using the Inverse Arnold Transform given in Equation (2).

4. EXPERIMENTS

Two experiments were conducted to test the performance of the system. In the first experiment, the sample image shown in Figure 4 was used as a cover image and the sample image shown in Figure 5 was used as a secret image.

Figure 4 Cover Image 1

Figure 5 Secret Image 1

In the second experiment, the sample image shown in Figure 6 was used as a cover image and the sample image shown in Figure 7 was used as a secret image.

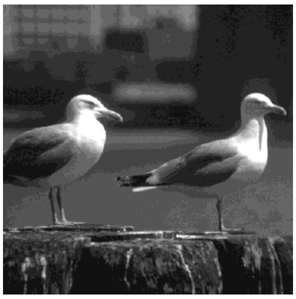

Figure 6 Cover image 2

Figure 7 Secret image 2

Both experiments were repeated four times; each time with different size of the secret image. The size of the cover images is 512 X 512. The sizes of secret images are 64 X 64, 128 X 128, 256 X 256, 384 X 384, and 512 X 512.

To evaluate the performance of the system. two evaluation metrics were used which are: Peak Signal to Noise Ratio(PSNR) and Mean Squared Error (MSE).Original cover images and stego images were compared in terms of PSNR and MSE values.TheMSE and PSNR can be calculated from Equations 3 and 4 respectively.

$$MSE = \frac{1}{MN}\sum_{1=0}^{M-1}\sum_{j=0}^{N-1}(C(i,j) - S(i,j))^2 \text{(3)}$$

$$PSNR = 10\, log_{10}(\frac{MN}{MSE}) \text{(4)}$$

Where C is the cover image, S is the stego image, M and N are the width and height of the cover image respectively.

5. RESULTS

The PSNR and MSE values for different cover images and different sizes of secret images are listed in Tables 1 and 2 and shown in Figures 8 and 9.

Experimental results show that the values of PSNR and MSE vary according to the size of the secret image. The PSNR decreases when the size of the secret images increases while the MSE increase when the size of the secret image increases.

Table 1 PSNR

Image Size	**64**	**128**	**256**	**384**	**512**
Experiment 1	55.2	49.9	43.8	40.2	37.8
Experiment 2	55.3	49.8	43.5	40	37.5

Table 2 MSE

Image Size	**64**	**128**	**256**	**384**	**512**
Experiment 1	0.78	2.6	10.8	24.6	43.2
Experiment 2	0.7	2.7	11.6	26.1	46.6

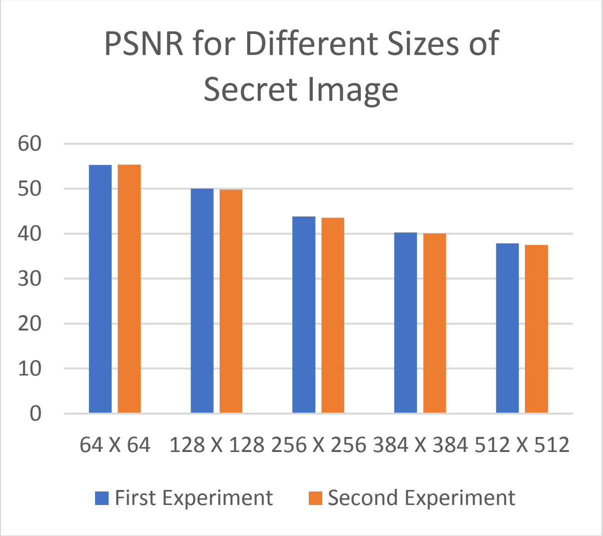

Figure 8 PSNR for different sizes of secret image

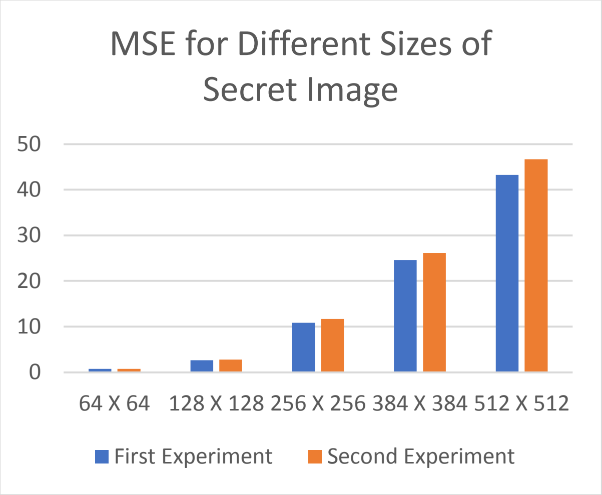

Figure 9 MSE for different sizes of secret image

6. CONCLUSIONS

In this paper, a system for hiding digital pictures into other digital pictures is presented. The presented system is grounded on using LSB steganography information hiding method. Additionally, the confidential picture is shuffled using ACM algorithm and then encrypted using XOR operation. The system was experimented on different standard gray scale images and the performance of the system was evaluated in terms of PSNR and MSE. The proposed system performed well and obtained the minimum MSE for secret images of small size. In the future work, the system will be improved to obtain high PSNR and low MSE values through embedding the confidential picture into audio and video files.

7. REFERENCES

[1] D. Artz, “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing, pp. 75-80, May-Jun 2001.

[2] L. Y. Por and B. Delina, “Information hiding: A new approach in text steganography”, 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science (Acacos'08), Hangzhou, China, April 6-8, 2008.

[3] M. Garg, “A novel text steganography technique based on html documents”, Int. Journal of Advanced Science and Tech., Vol. 35, October 2011.

[4] S. A. Laskar and K. Hemachandran, “High capacity data hiding using LSB steganography and encryption”, Int. Journal of Database Management Systems (Ijdms) Vol.4, No.6, December 2012.

[5] P. Bhautmage, A. Jeyakumar and A. Dahatonde, “Advanced video steganography algorithm”, Int. journal of engineering research and applications (IJERA) ISSN: 2248-9622, Vol. 3, Issue 1, January -February 2013, pp.1641-1644.

[6] K. Saroha and P. K. Singh, “Variant of LSB steganography for hiding pictures in audio”, Int. Journal of Computer Applications (0975 – 8887), Vol. 11, No.6, December 2010.

[7] Zhengchao Ni, Xuejing Kang, and Lei Wang,” A Novel Picture Encryption Algorithm Based on Bit-level Improved Arnold Transform and Hyper Chaotic Map”, IEEE International Conference on Signal and Picture Processing, 2016.

[8] S. A. Thileeban, "Encryption of pictures using XOR Cipher," 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai, 2016, pp. 1-3, doi: 10.1109/ICCIC.2016.7919607.

[9] Fauzi Adi Rafrastara, RakaPrahasiwi, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, and Christy Atika Sari, “Picture Steganography using Inverted LSB based on 2nd, 3rd and 4th LSB pattern”, International Conference on Information and Communications Technology, 2019.