

A New Approach for Chaotic Encrypted Data Hiding in Color Image

Ghada TH. Talee
Lecturer

Department of Computer
Science, University of Mosul,
Iraq

Melad J. Jelmeran
Lecturer

Department of Computer
Science, University of Mosul,
Iraq

Saja J. Mohammed
Lecturer

Department of Computer
Science, University of Mosul,
Iraq

ABSTRACT

Sending encrypted messages frequently will draw the attention of third parties, i.e. crackers and hackers, perhaps causing attempts and revealing the original messages. In digital world, Steganography is introduced to hide the existence of the communication by concealing encryption message inside color image. This paper proposed a steganography algorithm that hides encrypted text in color image by using chaotic hybrid approach. First, the text will be encrypted by one of substitution encrypted methods then, the result will be hidden in a color image by using the chaotic equation (which is also used to create cipher text).

Then, measurements PSNR, MSE and NC are used to calculate the effectiveness of the proposed method is described pictorially and also has been shown that a multi-level of security of data can be achieved.

General Terms

Security, Image Processing.

Keywords

Steganography, Color image, Hide data, Security, Plaintext, Chaotic, Keyword Mixed

1. INTRODUCTION

Information hiding is a general term encompassing many sub disciplines. One of the most important sub disciplines is Steganography as shown in Fig. 1. It is an ancient art of hiding information in ways a message is hidden in an innocent-looking cover media, so that will not arouse an eavesdropper's suspicion. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, Steganography focuses on keeping the existence of a message secret [1].

During the recent years, Steganography, in today's electronic era is the ability of hiding information in redundant bits of any unremovable cover media. Its objective is to keep the secret message undetectable without destroying the cover media integrity. Steganography replaces bits in image, sound and text file with secret data instead of protecting data the way cryptography does. Steganography conceals the existence of the data.

Capacity, security and robustness are the three main aspects affecting Steganography and its usefulness. Capacity refers to the amount of data bits that can be hidden in the cover medium. Security relates to the ability of an eavesdropper to point the hidden information easily. Robustness is concerned with the resistant probability of modifying or destroying the unseen data [2].

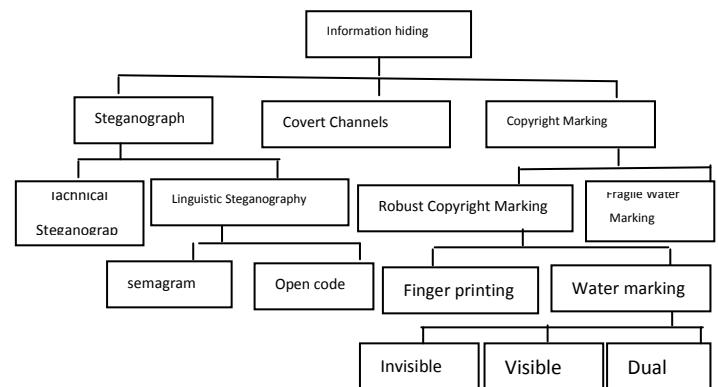


Figure1. Overview of Information Hiding Techniques

The goal of Steganography is to transmit a message through some innocuous carriers i.e. text, image, audio and video over a communication channel [3].

There are many of techniques about data hiding such as (least significant bit) LSB, planes by directly repacking the LSBs of the cover image with the message bits, (pixel-value difference) PVD, that method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block for data embedding a larger difference in original pixel values allows a greater modification, (Gray level modification) GLM. Technique which is used to map data by modifying the gray level of image pixels. GLM Steganography uses the concept of odd and even number to map data within an image [4].

In our work, a specific image based on stenographic method for color level image has proposed. Our idea is using chaotic in more than one way to make the algorithm more secure to hide data. This method is capable of extracting the secret message without changing the cover.

2. RELATED WORK

In this section, we discuss a list of work that has been done hiding information, in [5] propose an efficient steganography approach for hiding information within gray scale image then compared the new method with two-well-known method PVD and GLM. Where the goal in [6] is to propose a steganography mechanism that allows the hiding of a large quantity of data as possible in a colored image without increasing the size of the resultant image significantly. Although, in [7], they discussed a new stenographic technique based on the file hybridization, the proposed method works on more than one image. The effectiveness of the proposed method is described pictorially and also has been shown that a multi-level of security of data can be achieved. In [8] there is a proposed new

Steganography algorithm with 2 layers of security. A system named (Steganography Imaging System) SIS, has been developed by using the proposed algorithm. They tested few images with various sizes of data to be hidden, also in [9] a new image Steganography method for hiding data by using Gray level image in spatial Domain.

3. PROPOSED ALGORITHM

Our proposed algorithms encrypt secret message by using one of substitution encryption approach that is chaotic keyword mixed algorithm. A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns [10].

To hide any message by using the proposed algorithm, the hiding operation will pass the following layers:

Chaotic Layer: which produce chaotic numbers that will be used in the next two layers?

Encryption Layer: that encrypts the secret message by using the proposed chaotic key word mixed algorithm.

Hiding Layer: that uses using the results of the previous layers to hide in color image by the suggested approach.

3.1 Chaotic Keyword Mixed Encryption Algorithm

Input: secret message, chaotic number.

1. BEGIN
2. Generate 2 keys
 - a. First one is a letter; we obtain it by adding the digits of chaotic number mode result by 26.
 - b. Second one the word, we generate it by using the chaotic number. and compute the equivalent letters for all digit in it, (i.e.) if digit is 1 the letter is a, if it is 2 the letter is b and so on. Then, delete the repeated letters.
3. Pointed the position of letter in English alphabet.
4. From the previous position write the letter of keyword.
5. Complete the letters from alphabet that do not appear in word to the end of the English alphabet to create Encrypted alphabet.
6. Encrypt the secret message, by obtaining position of the letter from message in English alphabet of each and take the symmetric letter from Encrypted alphabet.
7. Repeat step (6) until end of secret message.

END

3.2 Chaotic Keyword Mixed Decryption Algorithm

Input: encrypted message, chaotic no.

1. BEGIN
2. Generate 2 keys (as above encryption algorithm).
3. Create the encrypted alphabet as encryption).

4. Decrypt the encrypted message by obtaining each letter of it encryption alphabet and taking the symmetric letter from English alphabet.
5. Repeat step (4) until end of secret message.
6. END

Output: secret message

3.3 Proposed Hiding Algorithm

Input: Original text end with (#), Cover Image

1. BEGIN
2. Apply chaotic function to generate chaotic sequence of length equal to message length*8+2.
3. Encrypt the original message by the chaotic keyword mixed encryption algorithm.
4. Convert encrypted data to Binary code.
5. Analysis cover image to its basic color level (red, green and blue).
6. Take first number of chaotic sequence to choose the image level that is used to hide data inside it (say 'L').
7. Choose the chaotic locations in L level to hide data inside them (say 'I') by using the remainder of chaotic sequence.
8. Extract the 2nd, 3rd and 4th bits of selected level (L) and location (I).
9. Convert 2nd, 3rd and 4th bits into equivalent decimal value and assign it to variable 'Num'
 - (a) If we want to insert **bit 0**, Check whether Num=0,2,4 or 6, If yes, no action, else add 1 to the selected location(I) in order to make Num is one of the values(0,2,4 or 6).
 - (b) if we want to insert bit 1, Check whether Num =1,3,5 or 7, If yes, no action, else add 1 to selected location in order to make Num is one of the values (1,3,5 or 7).
10. Repeat this step until reach end of message.
11. Send image after data hidden.
12. END

Output: Stego-image

4. RETRIEVAL ALGORITHM

Input: Stego-image

1. BEGIN
2. Apply chaotic function to generate chaotic sequence of length equal to message length*8+2.
3. Analysis Stego image to its basic color level (red, green and blue).
4. Use chaotic results to choose the image level is that used to hide data inside it (say 'L1').
5. Choose the chaotic locations in L1 level to extract hidden data (say 'I1').
6. Extract the 2nd, 3rd and 4th bits of selected level (L1) and location (I1).

Departure of two random variables from independence. This measurement calculate shown in Eq. (1) and (2):

$$MSE = \frac{1}{(N * N)^2} \sum_{I=1}^N \sum_{J=1}^N [C(IJ) - S(IJ)]^2 \quad (1)$$

$$PSNR = 10 \log_{10} 255^2 MSE \text{ db} \quad (2)$$

The Table(1) below shows the input image(cover image) , Original text and Stego- image after steganography, then compute the MSE, PSNR and NC as shown in table (2).In this method, we can hide message with length compute as follows in Eq.(3)or Eq.(4)

$$\text{Length of secret message in bits} = M*N*3 \quad (3)$$

$$\text{Length of secret message as character} = \text{length of secret message in bits}/8 \quad (4)$$

Table 1. Original Text, Cover Image and Stego_ Image





| Name | Original text | Cover image | Stego image |
|---------|---|---|---|
| Lena | Hybrid algorithm approach for hiding data using |  |  |
| Girl | Information hiding is a general term encompassing many sub disciplines. One of the most important sub disciplines is steganography |  |  |
| Natural | In this work, a specific image based stenographic method for color level image has proposed. In this method instead of embedding the secret message into cover image a mapping technique has been used to generate the Stego image. This method is capable of extracting the secret message without checking the cover image. |  |  |

Table 2, The value of MSE, PSNR and NC measurements

| Name of image | PSNR | MSE | Correlation |
|---------------|--------|---------|-------------|
| Lena | 0.0029 | 73.4400 | 1 |
| Girl | 0.0028 | 73.6474 | 1 |
| Natural | 0.0027 | 73.8405 | 1 |

5. ACKNOWLEDGMENTS

The researchers would like to thank the anonymous reviewers for their valuable suggestions.

6. CONCLUSION AND RECOMMENDATIONS

In this work, the researchers dealt with the techniques for steganography as related to color image. A new and efficient stenographic method for embedding secret message into images without producing any major changes has been proposed. This property enables the method to avoid steganalysis. This method is also capable of extracting the secret message without the cover image. Also, the researchers can hide a large number of char inside the selected cover image. Experimental results showed that the proposed method gave te best values for MSE, PSNR and CORRLATION, which means that there is no difference between the original and the Stego-images. And we consider doing the following modifications to the proposed method for the future work:

- Investigating the proposed method on video.
- Modifying the proposed approach to embed image inside another image.
- Preserve the secret message even if we do some transformations on the image like rotation, scaling compression.
- Relate the encryption process as RSA or DES with Steganography in which the researchers encrypt the message before embedding it inside the image in order to increase the security of the proposed method.
- Use the Neural Network , genetic and fuzzy logic with this method to increase the security.
- Use the chaotic function to choose the location of embedded bit.

7. REFERENCES

- [1] Banerjee, I.; Bhattacharyya, S.; and Sanyal, G. (2011). Novel Text Steganography through Special Code Generation. International Conference on Systemic, Cybernetics and Informatics, Paper Identification Number: CI-3.4, 289-303.
- [2] Alla, K.; and Prasad, S. R. (2008). A Novel Hindi Text Steganography Using Letter Diacritics and Its compound Words. International Journal of Computer Science and Network Security (IJCSNS), VOL.8 No.12, 404-409.

- [3] POR, L.Y.; and Delina, B. (2008). Information Hiding: A New Approach in Text Steganography. 7th WSEAS Int. Conf. on APPLIED COMPUTER & APPLIED COMPUTATIONAL SCIENCE (ACACOS '08), Hangzhou, China, 689-695.
- [4] Bhattacharyya, S.; and Sanyal, G. (2009). Hiding Data in Images Using PCP. International Journal of Computer and Information Engineering 3:3, 2009, 151-157. **IVSL**
- [5] Al-Taani, A.T.; and AL-Issa, A. M. (2009). A Novel Steganographic Method for Gray-Level Images. World Academy of Science, Engineering and Technology 51 2009 ,613-618.
- [6] Ibrahim, A.; Zabian, A.; Esteteya, F.N.; and Alpadawy, A. K. (2009). Algorithm for Text Hiding in Digital Image for Information Security. International Journal of Computer Science and Network Security (IJCSNS), VOL.9 No.6, 262-268.
- [7] Sahoo, G.; and Tiwari, R. K. (2008). Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization. International Journal of Computer Science and Network Security (IJCSNS), VOL.8 No.1., January, 228-233. **IVSL**
- [8] Ibrahim, R.; and Kuan, T.S. (2010). Steganography Imaging System (SIS): Hiding Secret Message inside an Image . Proceedings of the World Congress on Engineering and Computer Science Vol I , October (20-22), San Francisco, USA, 144-148.
- [9] Yadav, R.; Saini, R.; and Kamal deep. (2011).A New Image Steganography Approach for Information Security Using Gray Level Images in Spatial Domain. International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 7, 2679- 2690. **IVSL**.
- [10] Stallings, W. (2008). Cryptography and Network Security: Principle and Practice, Second Edition. Prentice Hall, 29-41.