Secure Image Steganography Algorithm using RGB Image Format and Encryption Technique

Babita
Dept. of computer science and engg.
Hindu college of engineering Sonepat,
Haryana, India
Chhikara8190@gmail.com

Mrs. Ayushi
Assistant Professor (Dept. of computer science and engg.)
Hindu college of engineering Sonepat,
Haryana, India
ayushibmiet@gmail.com

Abstract— The aim of this research is to design a steganography algorithm which not only hide the message behind the image but also provide more security than others. For the purpose of security, encryption technique is used with a user-defined key. In the algorithm designed by author a message is hide into an image in the form of an image that is using image generation method message is converted into the image of predefined format and then by using designed algorithm that image will hide into the cover image. RGB image format is used to improve the quality of the stego image. At last that RGB image will saved as BMP image file so that no lossy compression can occur and the original message do not destroy and can be extract as it is.

Keywords-Steganography, Image, Security, message file, extraction, embedding

I. INTRODUCTION

In the modern era security plays an important role in each and every field. Steganography techniques are one of the solutions to get secure. Steganography, literally means, "Covered writing" which is derived from the Greek language. Steganography is defined by Markus Kahn [5] as follows, "Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present". Hiding message may be text or secret message into another media file such as audio, video, image.

The main terminology used in the Steganography systems are-

- the cover message,
- secret message,
- secret key,
- Embedding algorithm [4].

The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. The secret message is the information which is needed to be hidden in the suitable media. The secret key is usually used to embed the message depending on the hiding algorithm. The embedding algorithm is the way or the idea that usually used to embed the secret information into the cover message [6] [2]. This study include image inside the other image so first of all need to know about an image [1].

II. TYPES OF STEGANOGRAPHY

A. Fragile

Fragile steganography involves embedding information into a file which is destroyed if the file is modified. This method is unsuitable for recording the copyright holder of the file since it can be so easily removed, but is useful in situations where it is important to prove that the file has not been tampered with such as using a file as evidence in a court of law, since any tampering would have removed the watermark. Fragile steganography techniques tend to be easier to implement than robust methods.

B. Robust

Robust marking aims to embed information into a file which cannot easily be destroyed. Although no mark is indestructible, a system can be considered robust if the amount of changes required to remove the mark would render the file useless. Therefore the mark should be hidden in a part of the file where its removal would be easily perceived.

C. Key Features

- The main goal of steganography is to hide the message in one to one communication.
- WE can hide as much data as possible.
- Ease of detection level should be difficult.
- Extraction of message should be similar with the original message.

D. Applicaions

Different areas where steganography is used-

- Media database systems
- Cover communication by executives
- Drug dealers
- Terrorists
- Access control system for digital content distribution
- Protection of data altering
- Confidential communication and secret data storing

III. IMAGE STEGANOGRAPHY

A. Image Files

As Duncan Sellars [7] explains "To a computer, an image is an array of numbers that represent light intensities at various points, or pixels and These pixels make up the images raster data."Pixels are displayed horizontally row by row. In a color scheme, the number of bits is known as the bit depth and this basically refers to the number of bits assigned to each pixel [1]. Moreover the smallest bit depth in the color scheme is 8 that is 8-bits are utilized to represent the color of each pixel. Both Monochrome and gray scale images usually utilize 8 bits for each pixel and such bits are capable of displaying up to 256 different colors or shades of gray. One more point to add is that almost all the color variation for the pixels of 24-bit image are derived from three basic color terms: red, green, and blue, and each of these colors is represented by 8-bits [3].Thus, in any given pixel, the number of different shades of red, green, and blue can reach 256 that adding up to more than 16 million combinations that finally result in more than 16 million colors. The most prominent image formats, exclusively on the internet are the GIF, JPEG, and to lesser degree PNG format. The important issue to touch here is that most of the steganography techniques attempt to exploit the structure of these formats. However some literary contribution use the bitmap format (BMP) simply because of its simple and uncomplicated data structure [8] [9].

B. RGB Image Files

The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 11111111 and 11111111) for white pixels. The RGB image is the most suitable because it contains a lot of information that help in hiding the secret information with a bit change in the image resolution which does not affect the image quality and make the message more secure. In this research paper the RGB images are used as a carrier message to hide the secret message by using new proposed method.

IV. PROPOSED ALGORITHM

The proposed algorithm includes four parts in it:-

1. User-defined key – This includes the key entered by user to encrypt the message. The key should be an integer between 0-255. This key will help to provide security to the hidden message because even if third party will get the stego image he/she cannot extract the message without exact key.
2. Encryption - In this part of algorithm the message is encrypted using key by applying the method of encryption that is XOR the message binary values with the key and gets the cipher message.
3. Embedding –Using embedding algorithm given below, the message is embedding into an image of RGB format.
4. Extraction –The message can be extracted if the exact key is known.

Embedding algorithm

Input: RGB image file, a secret text message, and a key.

Output: Stego image

Begin

Step1: Select the "canvas image" in which the message will hide into the 255*255 matrix and the message file (should include characters only) to hide.

Step2: Enter the encryption key to encrypt the message file between 0-255.

Step3: Now convert the message into their ASCII integer values

Step3 (a): Apply header to the beginning of the message (so that at the extraction time it will easy to find from where our message is starting).

Step3 (b): XOR the binary format of message with the key entered by user.

Step4: convert the message into the image file of the same dimensions.

Step5: Hide the data points using the RGBBGRRG order.

Step5 (a): Hide the data along the columns moving from left to right through the target image.

Step6: Determine whether or not we have reached the end of the image. Then need to move to the next column and reset our pattern to the top row.

Step7: step6 will follow until the complete message is hidden into the image.

Step8: Convert the RGB stego file into the bitmap file format.

End

Extraction algorithm

Input: Import the image with hidden message and the same key will be entered by user when embed the message

Output: RGB image file and the text message file.

Extraction algorithm follows all the same steps but in reverse order and in the last step the message file and the image file will save separately.

V. PROGRAMMING ENVIRONMENT

The MATLAB is high-performance language for technical computing integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. It allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar non-interactive language such as C or Fortran.

The image processing tool is used to implement the algorithm.

VI. IMPLEMENTATION RESULTS

This algorithm is implemented using MATLAB 7.6.0 and gives satisfactory results. Figures are shown below to show the execution results. The message hidden in the image is "hello how are you "

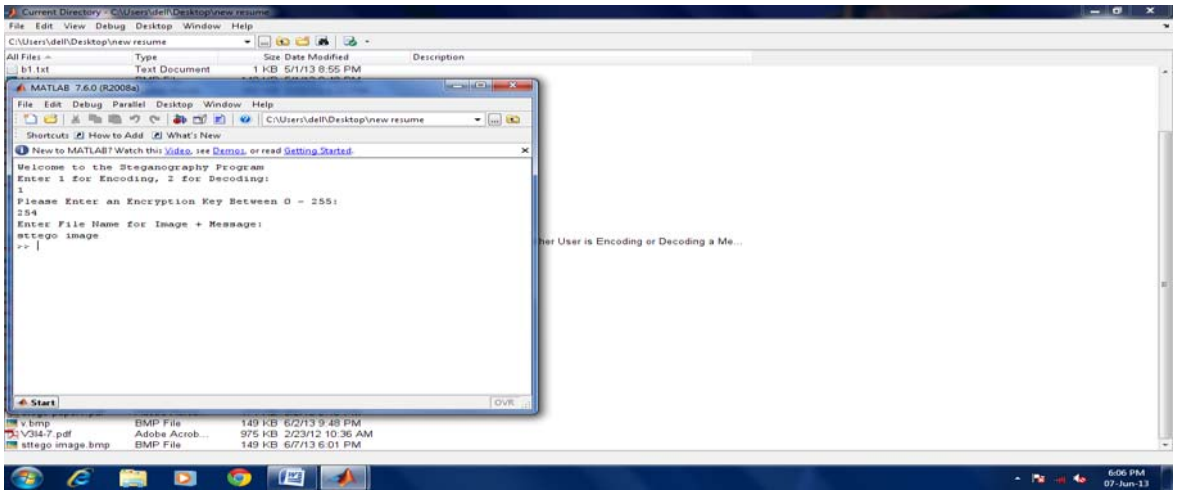

Figure1. Window showing execution of algorithm

Figure2. Cover image to hide the message.

Figure3. Stego image with hidden message.

Result for the extraction algorithm:-

As for extraction, image file with hidden message is input and we get two files as output one is text message file and other is cover image file. Both are shown below:-

Figure4. Stego image with hidden message

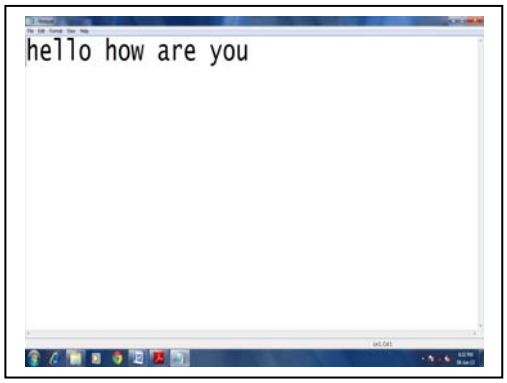

Figure5. Text file extracted from stego image.

VII. CONCLUSION

In this paper the steganography algorithm is presented and implementation results on MATLAB 7.6.0 are shown. The secure steganography algorithm has been developed to satisfy all proposed requirements. Almost all the objectives have been met. Execution is successful by achieving the objectives. Results are analyzed and are satisfactory according to requirements. Yes, of course, it needs to be more advanced but still it is highly secure technique.

VIII. FUTURE SCOPE

There is a wide scope for future development of the software. The world of computer field is not static it is always subject to change. For example, in this proposed algorithm the method used to hide the message inside the image may improve by using some more advanced features. Improvement is the important part of life in every field.

ACKNOWLEDGMENT

I express my gratitude to all my friends and faculty members of the Computer Science Department of Hindu College of engg.Sonepat, Haryana, India, for their support and enthusiasm. I am very grateful to Mrs. Ayushi (Assistant professor in computer science department) Hindu college of engg. Sonepat,for her guidance in my work. Last but not least I am very thankful to our HOD Mr. Neeraj Gupta for giving opportunity to work in the field of data hiding and retrieval.

REFERENCES

[1] T.Morkel, J.H.P Eloff, and M.S Oliver, “An overview of image steganography” in proc.ISSA, 2005, pp. 1-11.
[2] W, peter. Disappearing Cryptography: Information Hiding: Steganography & Watermarkking(second edition).San Francisco: Morgan Kaufmann. 3(1992).
[3] N.F. Johnson and S. Jajodia (1998, feb). “Exploring steganography: seeing the unseen”IEEE Computer Journal,[online]. 31(2), pp. 26-34. Available URL:http://www.jjtc.com/pub/r2026.pdf [jun, 2011].
[4] M.D. Swanson, B.Zhu and A.H. Tewfik, Robust data hiding for images,IEEE Digital Signal Processing Workshop, University of Minnesota,September 1996 (37-40).
[5] Johnson, Neil F., “Steganography”,2000, URL:http://www.jjtc.com/stegdoc/index2.html.

[6] N.Johnson, Survey of Steganography Software, Technical Report, January 2002.
[7] Sellars, D., "An Introduction to Steganography",URL: http://www.cs.ucat.ac.za/courses/CS40W/NIS/papers99/dsellars/stego.html.
[8] A.Cheddad, J.Condell, K.Curran and P.M Kevitt (2010). "Digital image steganography:survey and analysis of current methods" Signal Processing Journal.[online].90(3).pp.727-752.Available URL: http://www.abbascheddad.net/survey.pdf [aug. 2011].
[9] M.Fortrini, "Steganography and digital watermarking: a global view" University of california, Davis. Available URL:http://lia.deis.unibo.it/courses/retidicalcolatori/progetti00/fortini/project.pdf. [june 2011].
[10] Mehdi kharrazi, H.T. sencar, and N. Memon, Image steganography concepts and practices, lecture notes series, institute for mathematical sciences, National University of Singapore, Singapore 2004.
[11] Mehdi kharrazi, H.T. sencar, and N. Memon, "Performance study of common image steganography and steganalysis techniques"Journal of Electronic imaging 15(4),041104 (oct-dec 2006)
[12] AndrewS.Tanenbaum, Computer Networks forth edition, 2004.
[13] Cryptography and Network Security- By William Stallings, Fifth Edition
[14] Introduction to Cryptography- by Asel Ozgur.