International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 3, Number 4 (2013), pp. 235-240

http://www. irphouse.com /ijict.htm

An Approach to Improve Image Steganography using Random Key Generation Method

Babita[1], Anju[2] and Ayushi[3]

[1,2]Department of Computer Science and Engineering
Hindu College of Engineering Sonepat (Affiliated to DCRUST Sonepat)
Haryana, INDIA
3Department of CSE/IT, Hindu College of Engineering Sonepat
(Affiliated to DCRUST Sonepat), Haryana, INDIA.

Abstract

The research paper is about a steganography algorithm which not only hides the message behind the image but also provides more security than others. For the purpose of security, encryption technique is used with a user-defined key. The key used in the algorithm is generated randomly that is very difficult for a hacker to know the key used for encryption. In the algorithm designed, 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 proposed 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, message file, extraction, embedding.

1. Introduction

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 main goal of steganography is to hide the message

in one to one communication. We can hide as much data as possible. 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, and 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].

1.1 Image steganography

As Duncan Sellers [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 colour 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 colour scheme is 8 that is 8-bits are utilized to represent the colour of each pixel. Both Monochrome and grey scale images usually utilize 8 bits for each pixel and such bits are capable of displaying up to 256 different colours or shades of grey. One more point to add is that almost all the colour variation for the pixels of 24-bit image are derived from three basic colour terms: red, green, and blue, and each of these colours 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 colours. 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].

1.2 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.

2. 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 include characters of length 1-16. This key will help

to provide security to the hidden message because even if third party gets 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.

2.1 Designed Embedding Algorithm

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

Output: Stego image

Begin

Step 1: 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.

Step 2: Enter the encryption key to encrypt the message file (key should have characters of length 1-16).Key is generated randomly. The random key generation method follows the steps given below-

Step 2(a): Find out the base value using the length of the key from the base value table.

Table 1: Base value table.

Length of key	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Base value	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2

Step 2(b): Calculate 'sum' as

Sum = ASCII VALUE OF 1^{ST} CHARACTER*(base value concatenate with its position) + ASCII VALUE OF 2^{ND} CHARACTER * (base value concatenate with its position) up to the last character of the key

Step 2(c): Calculate 'num' as

Num = 1^{st} character of sum * 1 + 2^{nd} character of sum * 2 +up to the last character of sum

Step 2(d): Write 'num' in 8-bit binary code.

Step 2(e): Complement the binary code of 'num'.

Step 2(f): Use this 8-bit code as key.

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).

Step 3(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.
Step 5(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

2.2 Extraction algorithm

Input: Import the image with hidden message and the same key entered by user when embedded the message

Output: RGB image file and the text message file. Extraction algorithm follows all the same steps but in reverse order.

Begin
Step1: Select the canvas image/stego image.
Step2: Enter the key which should be the same as entered at the embedding time. This will follow the same steps of key generation method in reverse order.
Step3: Header analysis (as we know the header added to the message is‘t’)
Step3 (a): if header starts with‘t’, it means that message hidden is a text file else
The message is an image with the dimensions described in the header.
Step4: We used a RGBBGRRG cycle to encode the message set. In this step we need to reverse this process using modulo arithmetic.
Step5: After finding message it will be decrypted by applying XOR operation on encoded message and key. Now we will get the original message.
Step 6: In this step message is written into a .txt file and image is saved as . jpg. End

3. Conclusion

The proposed secure steganography algorithm satisfies the entire requirements basis on security. Almost all the objectives have been met. Execution is successful by achieving the objectives using mat lab. Results areanalysed and are satisfactory according to requirements. Yes of course, it needs to be more advanced but still it is highly secure technique.

4. 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.

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).SanFrancisco: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. AvailableURL: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.,"AnIntroductiontoSteganography",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. AvailableURL: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.