Nadia Mohammed, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.2, February- 2016, pg. 34-38

Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 2, February 2016, pg.34 – 38

INCREASING SECURITY in STEGANOGRAPHY by COMBINING LSB and PRGN

Nadia Mohammed

Computer Science Department, College of Education for Pure Science / Ibn-Alhaitham, Baghdad University, Iraq

Email: omrahuma@yahoo.com

Abstract---- With the increasing rate of unauthorized access and attacks, security of confidential data is of utmost importance. While Cryptography only encrypts the data, but as the communication takes place in presence of third parties, so the encrypted text can be decrypted and can easily be destroyed. Steganography, on the other hand, hides the confidential data in some cover source such that the existence of the data is also hidden which do not arouse suspicion regarding the communication taking place between two parties. This paper presents to provide the transfer of secret data embedded into master file (cover-image) to obtain new image (stego-image), which is practically indistinguishable from the original image, so that other than the indeed user, cannot detect the presence of the secrete data sent. Least Significant Bit (LSB) and Pseudo Random Number Generator (PRGN) are used to hide the secrete data. The Proposed approach is better in PSNR value and Capacity as shown experimentally than existing techniques.

Keywords---- Steganography, Cryptography, Pseudo random number generator

I. Introduction

With the rapid development of the internet technologies, digital media needs to be transmitted conveniently over the network [1]. While encryption masks the meaning of a communication, instances exist where we would prefer that the entire communication process not be evident to any observer that is, even the fact that communication is taking place is a secret.

Steganography is an art and science of hiding information in some cover media. The word Steganography comes from the Greek origin, means “concealed (covered) writing”. The word ‘steganos’ means “covered or protected” and ‘graphie’ means “writing” [2]. Steganography is thus, not only the art of information hiding, but also the art and science of hiding the fact that communication is even taking place [3],[4]. By embedding one piece of data inside of another, the two become a single entity, thus eliminating the need to preserve a link between the two different pieces of data, or risk the chance of their separation. One application than exhibits the advantage of this facet of steganography is the embedding of patient information within the medical imagery. By doing so a permanent association between these two information objects is created [5]-[7].

The concept of "What You See Is What You Get" which we encounter sometimes does not always hold true. Images can be more than what we see with our Human Visual System (HVS); hence they can convey more than merely 1000 words. Figure1 shows how a Steganographic system works [8],[9].

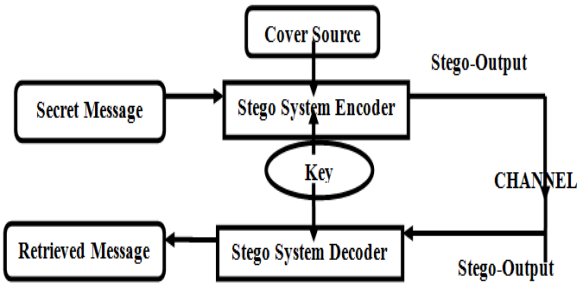

Figure 1: An Overview of Steganographic System

Steganography is not a new science. It dates back to 1499, and it has long history [10]. According to Greek historian Herodotus, the famous Greek tyrant Histiaeus, while in prison, used unusual method to send message to his son-in-law. He shaved the head of a slave to tattoo a message on his scalp. Histiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-in-law. Herodotus provides the first records of steganography in Greece. To communicate Greeks would etch the message they wished to send into the wax coating of a wooden tablet. The tablet would then be transported to the recipient who would read the message, then re-melt the wax to etch their reply [4],[6].

Messages were written on envelopes in the area covered by postage stamps. Messages were hidden using secret inks. Later, chemical effected sympathetic inks were developed. These were chemicals that could be treated with other chemicals causing reactions that would make the result visible. Messages were also hidden in living creatures, for example, by feeding a letter in meat to a dog and then killing him to retrieve it [6], [10], [11].

II. Using PRNG:

The pixels for message embedding are chosen randomly using a pseudo-random number generator seeded with a secret key. The pixel's components (red, green and blue) for message embedding are also chosen randomly using PRNG. The 3 LSBs of the pixel's components for message embedding are also chosen randomly using PRNG. Save all previous results in index table to use it in embedding and extracting process. Pseudo-random number generator is an algorithm that generates a sequence of numbers, the elements of which are approximately independent of each other. To use a PRNG, it first requires a seed. Seeding is the technical term for giving it an initial value, from which it can shoot out a sequence.

III. Proposed Approach

Apply Encryption on input text using RSA algorithm, this will increase the security level to the proposed approach, then select a cover-image to hide the secret message, if the cover-image is suitable for embedding process and sufficient to contain the whole secret message, then use PRGN to generate the index table which determine where to hide the secret message as we mentioned above in Section 2. This will increase the complexity level to the proposed approach. We will get the stego-image as a result for the proposed approach and send it to the recipient.

IV. Algorithms of the Proposed Approach

A. Embedding Algorithm

In this approach, to generate the index table, random key is used and then hides the secrete bit of the message into the cover-image using least significant bit method. Stego-key and random-key is shared by transmitting and receiving ends. The random-key is usually used to seed a pseudorandom number generator to select pixel locations in an image for embedding the secret message.

Input: Cover-Image, Secrete message and stego-key

Output: Stego-image

1) Read character from text file that is to be hidden and convert the ASCII value of the character into equivalent binary value into an 8 bit integer array and encrypt it with RSA algorithm.
2) Read the RGB color image (cover-image) into which the message is to be embedded.
3) If the cover-image is suitable for embedding process and sufficient to contain the whole secret message then initialize the stego and random key and generate the index table else goto step 2.
4) Insert the bits of the secret message to the LSB of the pixels according to the index table.
5) Write the above pixel to Stego-Image File.
6) Send the Stego-Image to the recipient.

B. Extracting Algorithm

Here we reverse the embedding algorithm to extract the secret message.

Input: Stego-Image, random-key and stego-key

Output: secret message

1) Open the Stego-image file in read mode and from the Image file, read the RGB color of each pixel.
2) Initialize the stego and random key that gives the position of the message bits in the pixels that are embedded randomly.
3) Extract the data from the LSB of the pixels according to the index table.
4) Read content of the array, converts into decimal value that is actually ASCII value of hidden character.
7) ASCII values got from above is converted to the characters which gives the encrypted message file, which we hide inside the cover-image and decrypting it.
8) Write the secret message.

V. Comparison Based on PSNR

MSE (Mean Square Error) is the average squared difference between a reference image and a distorted image. It is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count [12]. It defines the differences between the Cover Image and Stego-Image. Lower the MSE, better the quality of Stego-Image.

PSNR (Peak Signal to Noise Ratio) is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [13], [14]. This ratio is often used as a quality measurement between the original (cover) image and a stego-image as it defines the similarities between cover image and stego image. Higher the PSNR, better the quality of the stego-image.

The PSNR and MSE results for some standard images of different sizes with variable length of message are shown in Table (1).

VI. Results and Discussions

Figure (2) presents the results of applying the proposed approach to standard image Lena.

Figure (2): a) lena cover-image b) lena stego-image

Experimental results proved that the proposed approach provides higher values of PSNR and lower values of MSE for different test images under consideration. The PSNR and MSE results for some standard images of different sizes with variable length of message are shown in Table (I) below:

Table I: PSNR (in dB) and MSE of the Proposed approach

Cover Image	Message Length (in Bytes)	PSNR	MSE
Lena(204X 204)	1000	41.5688	0.1321
Baboon(225 X225)	4017	56.4062	0.1081
Peppers(512 X 384)	16550	62.6658	0.0113

VII. Conclusion

The paper proposed a new technique for information security. It presents an improved steganography method for embedding secret message bit in least significant byte of nonadjacent and random pixel locations of images. No original cover image is required for the extraction of the secret message. The research was aimed towards the evaluation and development of a new and enhanced data hiding technique based on LSB and PRNG. The primary objective of this paper is to propose a solution that is robust, effective and to make it very hard for human eye to predict and detect the existence of any secret data inside the host image. This has been achieved by using those bits for data storage of color image to which human eye is least perceptive. Experimental Results shows that the proposed approach provides higher PSNR and lower MSE values and thus the proposed approach is proved to be robust.

References

[1] A. Kumar and K. Pooja, "*Steganography- A Data Hiding Technique*", International Journal of ComputerApplications, vol. 9, no. 7 , (2010).

[2] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "*Information Hiding: A Survey*". In Proceedings of the IEEE, Special issue on protection of multimedia content, (1999).

[3] J. Kaur and S. Kumar, "*Study and Analysis of Various Image Steganography Techniques*", International Journal of Computer Science and Technology, vol. 2, no. 3, (2011).

[4] R. Yadav, "*Study of Information Hiding Techniques and their Counterattacks: A Review Article*", International Journal of Computer Science & Communication Networks, vol. 1, (2011), pp. 142-164.

[5] L. M. Marvel, "*Image Steganography for Hidden Communication*". University of Delaware , Electrical Engineering, PhD Thesis, Springer, (1999).

[6] M. Kharrazi, H. T. Sencar and N. Memon, "*Image Steganography: Concepts and Practices*", Polytechnic University, Brooklyn, USA, (2004).

[7] A. Almohammad, "*Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility*", Department of Information Systems and Computing, Brunel University, PhD Thesis, (2010).

[8] T. Morkel, J.H.P. Eloff and M.S.Olivier, "*An Overview of Image Steganography*", in Proceedings of the Fifth Annual Information Security South Africa Conference Sandton, South Africa, (2005).

[9] A. Cheddad, J. Condell, K. Curran and P. McKevitt, "*Digital image steganography: Survey and analysis of current methods*", Signal Processing, vol. 90, (2010), pp. 727—752.

[10] J. Ashok, Y. Raju, S. Munishankaraiah and K. Srinivas, "*Steganography: An Overview*", International Journal of Engineering Science and Technology, vol. 2, no. 10, (2010).

[11] R. Yadav, "*Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters*" International Journal of Computer Technology and Applications, vol. 2, no. 6, (2011), pp 1867-1870.

[12] C.-K. Chan and L. M. Cheng, "*Hiding data in images by simple LSB substitution*" The Journal of Pattern Recognition Society, (2004), pp 469—474.

[13] N. F. Johnson and S. Jajodia, "*Exploring Stenography: Seeing the Unseen*" IEEE Computer, (1998), pp 26-34.

[14] C.-M. Wang, N.-I Wu, C.-S. Tsai and M.-S. Hwang, "*A high quality steganographic method with pixel- value differencing and modulus function*", J. Syst. Software, (2007).

