Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Review: A Steganography Approach to Protect Secret Information in Computer Network

Miss. Prajakta B. Diwan, Prof. V. B. Bhagat

Department of Computer Science and Engineering,

SGBAU University, India

Abstract—Protecting data is a demanding issue in today's era. The largest part of the data pass through the internet and it becomes complex to make data secure. There come up a need of data hiding. Steganography is distinct as the study of hidden communication. Steganography is the skill and science of hiding a top secret communication in a cover media such as image, text, signals or sound in such a manner that nobody, apart from the deliberate recipient knows the existence of the data. This paper discusses the thought behind the steganography by means of exploring initially what is the steganography and the provisions related to steganography. In this paper, we review the different security and data hiding techniques that are used to implement a steganography.

Keywords— communication, hiding, protection, security, steganography.

I. INTRODUCTION

Steganography is derived from Greek words Steganous meaning "covered" and graphy meaning "writing". So it is known as "covered writing". Steganography is a rough Greek translation of the term Steganography is secret writing technique which is used to hide the message and prevent the detection of hidden message and has been used in various forms for 2500 years. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, steganography is the expression applied to any number of processes that will hide a message within an objective where the secret message will not be visible to an viewer.

The recent approach of hiding is a Image stegnography [1] in a manner that the unnecessary community or people may not access the information. Data used to hide data in stegnography can be text or image. In modern times, image stegnography can be helpful in a number of ways such as hiding the secret data [2], data authentication, ensuring authenticated data availability for academic usage, monitoring of data piracy, labelling electronic data/contents, copyright protection, ownership identification, providing confidentiality and integrity enhancement control of electronic data piracy etc.[3]. As soon as a stenographic method is developed, it is essential to believe what the most suitable cover effort be supposed to be, as well as how the stegogramme is to get to its receiver. for instance, it is probable that an image stegogramme could be sent to a recipient via email. Otherwise it might be posted on a network medium in support of all to spot and the recipient could log onto the medium and download the image to read the message. In conditions of improvement, Steganography included two algorithms, first for embedding and second for extracting. The embedding process is concerned with hiding a secret message within a cover work, and is the most cautiously created process of the two. An immense contract of concentration is paid to make sure that the undisclosed message goes ignored if a third party were to intercept the cover Work. The extracting process is usually a much simpler process as it is simply an converse of the embedding process, where the secret message is exposed at the end.

Also there are some steganographic terms such as Cover File:It is a file in which hidden information will be stored , Stego Medium: Medium through which the information is hidden , Message: The data to be hidden or extracted , Steganalysis: Identify the existence of message.

II. RELATED WORK

Image steganography takes the advantage of limited power of human visual system (HVS). Here, unlike watermarks which embed added information in every part of an image, only the complex parts of the image holds added information. Straight message insertion will simply encode every bit of information in the image. More complex encoding can be done to embed the message only in "noisy 'areas of the image that will attract less attention [3]. The least significant bit (LSB) insertion method [4] is probably the most well known image steganography technique. The main advantage of this method is that human eye is not able to notice the change; however unfortunately, it is extremely vulnerable to attacks, such as image manipulation. The usual steganographic methods fetch few bits from the secret data to be embedded. But R. Amirtharajan [5], describes Hiding Streams of 1s and 0s method it fetches the 1s or 0s present consecutively for hiding. This is an innovative steganographic method where the data to be hidden is converted to binary. The number of 1s and 0s are counted and stored in the pixels of the cover image in this method. The number of 1s is stored in the odd columns of the pixel and the number of 0s is stored in the even columns. Jessica Fridrich and Miroslav Goljan[6],describes Digital image steganography by using stochastic modulation. Vinay Kumar*and S. K. Muttoo[7],describes the concept of finding natural relationship between a digital cover and a message which can be used

to hide the information in cover without actually replacing or distorting any useful bits of the cover. It introduces a concept called sustainable embedding of message in a cover using natural relationship and representing it using graph theoretic approach. Ankita Agrawal [8], presents a new generalized model for combining cryptographic and steganographic technique by using simplified data encryption standard(S-DES) algorithm. Samir Kumar Bandyopadhyay [9], proposed technique converts 4 bit image into 4 shaded Gray Scale image. This image will be act as reference image to hide the text. Using this grey scale reference image any text can be hidden. Graeme Bell and Yeuan-Kuen Lee [10], describes fast and accurate Detection of steganography is demonstrated experimentally here across arrange of media types and a variety of steganography approaches.

III. PROPOSED WORK

The process of hiding information inside another media is called stegnography. The media with secret information is called stego media and without hidden information is called cover media. Steganalysis is a process of extracting information from the stego media. Steganalysis is just opposite to stegnography.

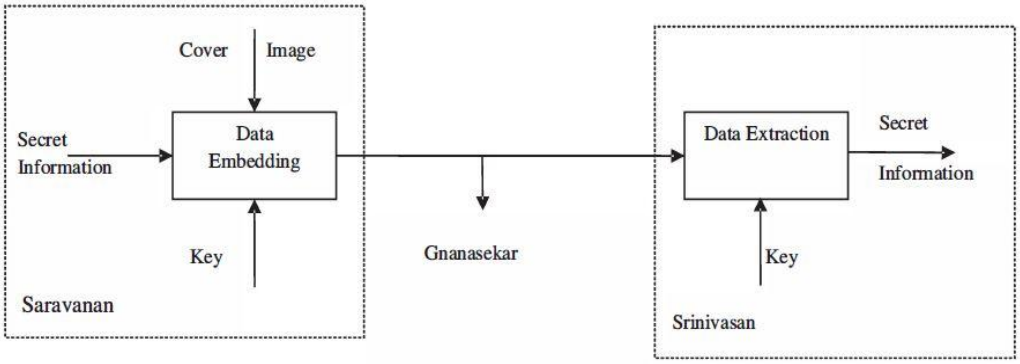

Fig.1: Block diagram of steganography process

Let as consider a situation, that a person "Saravanan" wants to send secret information to another person "Srinivasan" and the secret information is "Tomorrow Meet Me in College". This information should not be known to a person "Gnanasekar" who is an expert in hacking. In this situation Saravanan has to take a cover image of size eight times greater than secret information as shown in figure 1. He has to convert the secret information into binary form and then he has to store the secret information in the LSB of each pixel one by one. The resultant image (stego image) will be send to Srinivasan via computer network. Now the Gnanasekar will catch the packets and he can construct the image send by Saravanan to Srinivasan. Now Gnanasekar can just see the image and he might think that there is no secret in their communication. This is how one can cheat the hackers using stegnography.

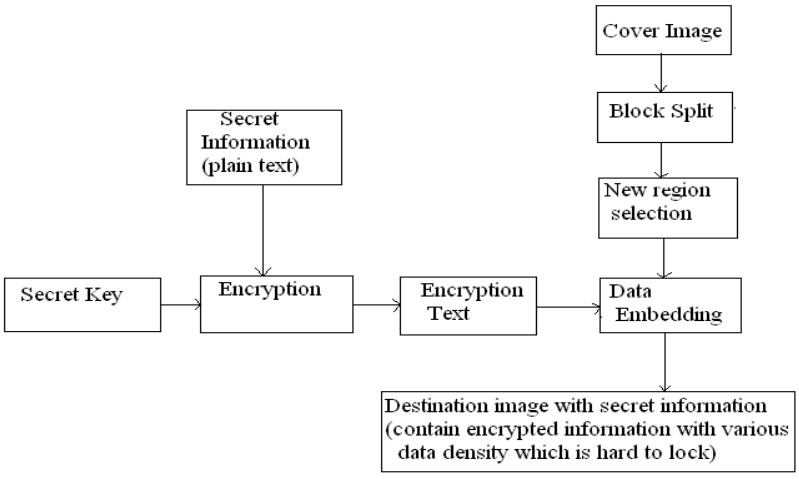

Fig. 2: Proposed method of steganography

In our proposed method, it reduces the detectable distortion in a joint photographic experts group (JPEG) file during data hiding process, by introducing new region selection rule. The new region selection rule considers three factors, i.e., the horizontal difference (HD), vertical difference (VD) and region size (RS). The JPEG image will be split into number of blocks and each pixel in it will be examined to calculate the variations. the image can be divided into number of pieces called macro blocks. Each pixel in the macro block will compare with its neighbor pixel. By doing this we can easily identify whether the macro block contain plain image or not. In plain regions, only one LSB can be altered to store the data, otherwise Detectable Distortion (DD) will increase. If the block contains high variations in the pixel values while comparing with its neighbors, then we can alter up to four or five LSBs. By doing this the originality of the image can be spoiled, but DD will not increase, since the variations in that block is high. According to the human vision system point of view, the changes in the plain region can be easily identified but not in the variation regions.

IV. CONCLUSIONS

Cryptography and steganography are two major branches of data security. In this system cryptographic and steganographic security is combined to give two tier security to secret data. In this paper we have proposed a new region selection rule for stegnography. This method makes the data embedding process to modify more LSBs of a pixel based on region type to raise the ability of the stegnography. Hence the security, capacity and DD will get improve. In future the detection algorithms can be added to increase the capacity of the stegnography process without increasing DD. Lastly we can conclude that the proposed technique is effective for secret data communication.

REFERENCES

[1] N.F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, In Proceedings of the IEEE Congress on Evolutionary Computation (CEC) 31 (2), 26–34,1998.

[2] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn, Information Hiding- A Survey, Proc of IEEE, July1999,87(7),pp.062-1078, ”

[3] C. Stanley,”Pairs of Values and the Chi-squared Attack,” Master’s thesis, Department of Mathematics, Iowa State University, 2005.

[4] M. A. F. Al-Husainy,“Message Segmentation to Enhance the Security of LSB Image Steganography”, International Journal of Advanced Computer Science and Applications, 3(3),57-62,2012.

[5] R. Amirtharajan, R. Akila, P. Deepika chowdavarapu, “A Comparative Analysis of Image Steganography”, International Journal of Computer Applications, 2(3),41-47,2010.

[6] Jessica Fridrich and Miroslav Goljan, Digital image steganography using stochastic modulation, Department of Electrical and Computer Engineering, SUNY Binghamton, Binghamton, NY 13902-6000, USA.

[7] Vinay Kumarand S. K. Muttoo, “Principle of Graph Theoretic Approach to Digital Steganography”, Proc of the 3rd National Conference, February2009,pp.26 – 27,

[8] Ankita agrawal, “Security Enhancement Scheme for Image Steganography using S-DES Technique”, International Journal of Advanced Research in Computer Science and Software Engineering, 2(4), 164-169, April 2012,.

[9] Samir Kumar Bandyopadhyay, “An Alternative Approach of Steganography using Reference Image”, International Journal of Advancements in Technology,1(1) ,June 2010,95-102.

[10] Graeme Bell and Yeuan-Kuen Lee, “A Method for Automatic Identification of Signatures of Steganography Software”, IEEE Transactions on information forensics and security, 354-358, June 2010.

