Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review -Steganography

Shilpa Thakar
Student
Department of Electronics & Comm. Engg.
BGIET,Sangrur(Pb)-India

Monika Aggarwal
Associatet Professor
Department of Electronics & Comm. Engg.
BGIET,Sangrur(Pb)-India

***Abstract*— This Paper gives a review on the steganograpy,Image Steganography and methods used for Image Steganography . Steganography is a powerful security tool with which we can hide a secret message inside an object. The object can be text,image,audio or video. Security ,Integrity and Capacity of hidden information is the main concept in this. Image Steganography is the most widely used of all methods in the digital world of today .**

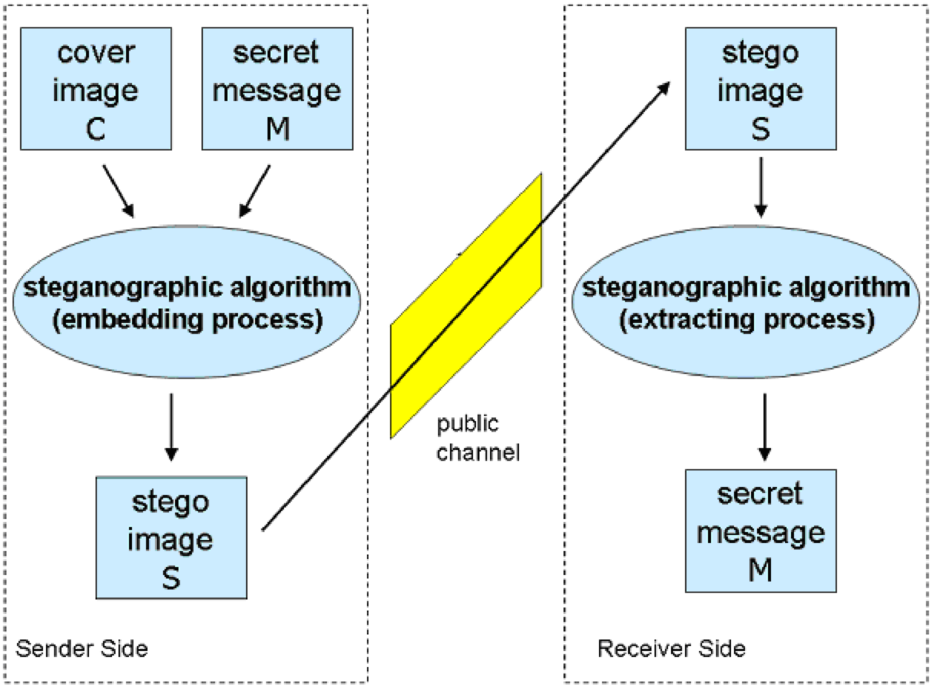
***Keywords*— Steganography,Image Steganography,Stego Image,Cover Image,Steganalysis,Cryptography, Hiding Capacity, Perceptual Transparency,Robustness,Tamper Resistance,LSB(Least Significant Bit)**

I. INTRODUCTION

Since the rise of the internet, the most important factor of information technology and communication has been the security of information. Since the ancient times data has been hidden in some ways or other and with the advancement Steganography has come into place. Steganography plays an important role in information security. It deals with embedding information in a given media without making any visible changes to it. In simple words it is a technology that hides a message within an object. In other words Steganography is the process of hiding a secret message within a larger one in such a way that someone can not know the presence or contents of the hidden message. Steganography techniques, on the other hand, tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where the message is. The purpose of Steganography is to maintain secret communication between two parties.

II. IMAGE STEGANOGRAPHY

Image Steganography is encoding secret messages in Images. Secret message can be any plain text, cipher text, image and any other media. An image consists of pixels. Pixel is the representation of light intensities at various points. Figure shows the Steganographic Model. Secret message M is hidden inside the cover image C by steganographic algorithm (embedding process) which gives a stego image S. This Stego image is transmitted over the channel and received at the receiver end. Again by using the steganographic algorithm (extracting process) secret message M is extracted.



Steganographic Model

III. STEGANOGRAPHY HISTORY

The word Steganography comes from the Greek origin that means “concealed (covered) writing”. The word “steganos” means “covered or protected” and “graphie” means “writing” [20]. Steganography thus not only emphasizes on the art of hiding information but also the art and science of hiding the communication that takes place [18]. First applications of Steganography were documented by Herodotus, a Greek historian. Steganography can be traced back to ancient Greek centuries when the message is tattooed on the messengers shaved heads. The hair then grows to hide the message. Their head will be shaved when they reach the recipient of the message [14,12,11].Another steganography method that was used during those days is tablet wax. In order to hide the message, the tablet was erased by wax and text was etched on and then again covered it by wax and appeared blank upon inspections [12,13]. During the century, the methods of using invisible inks were extremely popular [12]. During the World War II where people used ink for writing hidden messages, this was true [14]. The mixture will turn darker and the written message becomes visible upon heating. After some time, the Germans introduced the microdot technique where microdots are considered as photographs as small as a printed period, but with a clear format of a typewritten page [14, 17]. They were included in a letter or an envelope, and because of their tiny sizes, they could be indiscernible. Microdots were also hidden in body parts including nostrils, ears, or under fingernails [12].The military and several governmental agencies are looking into steganography for their own secret transmissions of information. They are also desirous of discerning secret information communicated by criminals, terrorists, and other aggressive forces. Following investigations into the Al-Qaeda attack, steganography was suspected to be made use of in their attack of the World Trade Centre [3].

IV. APPLICATIONS OF STEGANOGRAPHY

Steganography is used in a lot of useful applications:

- Smart identity cards where the details of individuals are embedded in their photographs.
- Video-audio synchronization
- TV broadcasting
- TCP/IP packets where a unique ID is embedded in an image to analyse the network traffic of particular users [13].
- Medical Imaging Systems is one of the modern applications that use Steganography where a separation is recommended between patients‟ image data or DNA sequences and their captions for security or confidentiality reasons. Thus, embedding the patient’s information in the image could be a security measure to help solving security issues [19].
- Digital technologies have swept the confidence in the integrity of visual imagery [10]; a matter that motivated researchers to conduct research on digital document forensics. In 2009, Cheddad and his colleagues proposed a steganographic scheme which protects scanned documents from forgery using self-embedding techniques. It also allows legal or forensics experts to access the original document though it is manipulated [4].

V. DIFFERENCE BETWEEN CRYPTOGRAPHY AND STEGANOGRAPHY

With the increasing number of users and the number of unauthorized access has also increased. Hence, Information security plays an important role. Keeping this concept in mind cryptography and steganography both are used. Therefore, the main issue now is to mitigate and to lessen the impact of the chances of the information being detected during transmission. Cryptography deals message encryption but the communication is visible but on the other hand, steganography deals with secret message hiding but the communication is invisible. This is the major difference between cryptography and steganography. Although by encrypting the traffic, the communications will be secured but people become aware of the existence of information by observing coded information, although they are unable to comprehend the information. Steganography hides the existence of the message so that intruders can’t detect the communication and thus provides a higher level of security than cryptography. Both steganographic and cryptographic systems provide secret communications but different in terms of system breaking. Steganography system is more fragile than cryptography systems in terms of system failure.

VI. RELATED WORK

Information hiding has been used since long time. In ancient times head of the person was shaved to hide information and he was sent with the hidden message when his hair grew back. In Modern times Steganography is being used for hiding the data. Research in hiding data inside image using steganography technique have been done by many researchers. In the field of steganography a method to hide data in binary images, including scanned text, figures, signatures was proposed by Min Wu and Bede Liu[15] in 2004. The manipulation of “flippable” pixels was done in order to embed a significant amount of data . To equalize the uneven embedding capacity from region to region shuffling before embedding was done. The hidden data can then be extracted without using the original image and can also be accurately extracted. Miroslav Dobsicek[7] in the field of image security, has developed an application of steganography in 2004 where the content is encrypted with one key and can be decrypted with several other keys. An approach to hide data inside the audiovisual files was introduced by Warkentin et al.[23] in 2008 . In their steganography algorithm cover image was used to hide the secret content . The majority of today’s steganographic systems use images as cover media because people often transmit digital pictures over email and other Internet communication. The rapid development of data transfer through internet made it easier to send the data accurate and faster but the most important factors of information technology and communication has been the security of the information. In 2007 El-Emam[8] proposed a steganography algorithm to hide a large amount of data with high security. His steganography algorithm is based on

hiding a large amount of data (image, audio, text) file inside a colour bitmap (bmp) image. Several methods exist to employ the concept of Steganography as well as plenty algorithms have been proposed in this regard. proposed an algorithmic approach to obtain data security using LSB insertion steganographic method. This is the simplest and the most common steganographic technique. It provides to embed the data into the least significant bit.
By using the LSB we can store 3 bits of data in each pixel for 24-bit images and 1 bit in each pixel for 8-bit images. So more information can be stored in a 24-bit image file. It is possible to take 2LSB's from one byte without the human visual system (HVS) being able to tell the difference. The only problem with this technique is that it is very vulnerable to attacks such as image changes and formatting (i.e., changing from .GIF to .JPEG). The most common and popular method of modern day steganography is to make use of the LSB of a picture's pixel information. This technique works best when the image file is larger than the message file and if the image is gray scale.

E.g. A sample raster data for 4 pixels (12 bytes) may be:

11100111 11101011 11001010
00100111 11001100 11101011
11001100 00110111 11101011
00111010 10101011 10001010

Hiding the secret message (100110000110) inside the above data changes 6 bits

11100111 1110101**0** 11001010
00100111 1100110**1** 1110101**0**
11001100 0011011**0** 1110101**0**
0011101**1** 10101011 10001010

With this method secret message is embedded without any remarkable changes in the cover image data. This is a common and simple approach to embed information in a cover file. It overwrites the LSB of a pixel with a message bit. If we choose a 24-bit image as cover, we can store 3 bits in each pixel. To the human eye, the resulting stego image will look identical to the cover image.

In 2008, Mohammad Tanvir Parvez and Adnan Abdul-Aziz Gutub[16] presented a new algorithm for RGB image based steganography. Their algorithm introduces the concept of storing variable number of bits in each channel (R, G or B) of pixel based on the actual color values of that pixel: lower color component stores higher number of bits. This algorithm offers very high capacity for cover media compared to other existing algorithms.S. K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulami Das [5] in 2008 has proposed an approach to hide huge amount of data using LSB steganography technique. In their method, they have first encoded the data and afterwards the encoded data is hidden behind a cover image by modifying the least significant bits of each pixel of the cover image. The resultant image was distortion less. Also, they have given much emphasis on space complexity of the data hiding technique.In 2010, Samir Kumar Bandyopadhyay & Sarthak Parui [6] proposed a public key method of Steganography is proposed under standard cryptographic assumptions. The byte location in LSB of which the secret bit is to be embedded is found out by public key of the receiver and receiver apply private key of itself to reconstruct the secret message.
In 2012, Vikas Tyagi[22] , discussed a technique used on the LSB (least significant bit) and a new encryption algorithm. By matching data to an image, there is less chance of an attacker being able to use steganalysis .
Different methods were adopted for steganography.Various features characterize the strengths and weaknesses of the methods.

Hiding Capacity: Hiding capacity is the size of information that can be hidden relative to the size of the cover. A larger hiding capacity allows the use of a smaller cover for a message of fixed size resulting in decrease of the bandwidth required to transmit the stego-image.

Perceptual Transparency: Hiding the message in the cover results some changes in the cover image e.g. Noise modulation or distortion. It is important that the embedding occurs without significant degradation or loss of perceptual quality of the cover. If there is some distortion in the image attacker notices it and the steganographic encoding fails even if the attacker is unable to extract the message. Preserving perceptual transparency is required for the integrity.

Robustness: Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes any transformations.

Tamper Resistance: Tamper-resistance refers to the difficulty for an attacker to alter an message once it has been embedded in a stego-image. More difficulty for an attacker means less alteration in stego image results in integrity of image.

VII. DISCUSSION AND RESEARCH SCOPE

After reviewing the various papers in area of steganography it is found that a lot of work has been done in the field of Steganography as well as in Image Steganography. It is observed that most of the Steganography techniques are suitable to hide data either text or binary message. Image steganography is most popularly used technique in comparison with video and audio steganography.Image steganography techniques used for gray scale images are best suitable as secret message embedded in gray scale images is very harder to detect. With the most commonly used LSB Insertion method only one bit is embedded in a byte. Future scope requires increasing the hidden capacity without any remarkable change in the cover image data and maintaining the integrity of the stego image so that there should not be any distortion. data Although implementations have been done in this field .It is possible to take 2 LSB's from one byte without the human visual system (HVS) being able to tell the difference. The problem with this technique is that it is very vulnerable to attacks such as image changes and formatting (i.e., changing from .GIF to .JPEG).

VIII. CONLUSION

The Paper gives the review of Steganography, Image Steganography alongwith the LSB insertion method used in Image Steganography. The paper suggested a few for future research like integrity and data capacity of cover image. Some steganographic methods need to improve security by using cryptography against attacks.

REFERENCES

[1] Adel Almohammad "*Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility*" A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing, Brunel University, August,2010.

[2] Arvind Kumar and Km. Pooja "*Steganography- A Data Hiding Technique*", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[3] M. Bachrach, and F.Y. Shih, "*Image steganography and steganalysis*,"Wiley Interdisciplinary Reviews: Computational Statistics, Vol. 3, pp. 251-9, 2011.

[4] Cheddad, A., J. Condell, K. Curran, & P. Mc Kevitt. "*A skin tone detection algorithm for an adaptive approach to steganography*". Signal Processing, 89(12): 2465-2478. doi: 10.1016/j.sigpro.2009.04.022, 2009.

[5] S.K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulumi Das, "*A Secure Scheme for Image Transformation*", August 2008, IEEE SNPD Page(s) 490-493

[6] Samir Kumar Bandyopadhyay & Sarthak Parui proposed "*A Method for Public Key Method of Steganography*" International Journal of computer Applications(0975-8887) Volume 6-No.3,September,2010

[7] Dobsicek, M., "*Extended steganographic system*", In: 8th Intl. Student Conf. On Electrical Engineering, FEE CTU 2004, Poster 04.

[8] El-Emam N.N. (2007)." *Hiding a Large Amount of Data with High Security using Steganography Algorithm*", Journal of Computer Science 3 (4), pp 223-232.

[9] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn "*Information Hiding A Survey*"Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.

[10] Farid,H."*Image forgery detection*". Signal Processing Magazine, IEEE, 26(2): 16-25. doi: 10.1109/msp.2008.931079, 2009.

[11] J. Fridrich, "Steganography in Digital Media: Principles",Algorithms, and Applications, Cambridge, England: Cambridge University Press; 2009.

[12] J.C. Ingemar, M.L. Miller, J.A. Bloom, J. Fridrich, and T. Kalker, "*Digital watermarking and steganography*", Burlington: Morgan Kaufmann; 2008.

[13] N.F. Johnson, and S. Jajodia, "*Exploring steganography: Seeing the unseen*," Computer, IEEE, Vol. 31, pp. 26-34, 1998.

[14] R. Krenn, "*Steganography and steganalysis*," An Article, Santa Barbara, California, January 2004, available from: http://www.krenn.nl/univ/cry/steg/article.pdf [Last accessed on 1 November 2013]

[15] Min Wu,Member,IEEE and Bede Liu,Fellow,IEEE, "*Data Hiding in Binary Image for Authentication and Annotation*", IEEE Trans. Image Processing, volume 6,Issue 4, Aug. 2004 Page(s): 528-538

[16] Mohammad Tanvir Parvej and Adnan Abdul-Aziz Gutub "*RGB Intensity based Variable –Bits Image Steganography*", IEEE Asia-Pacific Services Computing Conference.2008

[17] 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 (ISSA2005), Sandton, South Africa, pp. 1-12, 29 Jun.-1 Jul. 2005.

[18] Angela D. Orebaugh " *Steganalysis: A Steganography Intrusion Detection System*" , George Mason University

[19] Petitcolas, F.A.P." *Introduction to information hiding*". In S. Katzenbeisser & F. A. P. Petitcolas (Eds.), Information hiding techniques for steganography and digital watermarking (pp. 1-12). Boston, London: Artech House,2000.

[20] Rajkumar Yadav "*Study of Information Hiding Techniques and their Counterattacks: A Review Article*" , International Journal of Computer Science & Communication Networks, Vol 1(2), 142-164, Oct-Nov 2011.

[21] BANASTHALI VIDYAPITH, RJASTHAN "*IMAGE STEGANOGRAPHY TECHNIQUES: A REVIEW ARTICLE*", BULLETIN OF ENGINEERING, FACULTY OF ENGINEERING, HUNEDOARA, ROMANIA, JULY-SEPTEMBER,2013.

[22] Vikas Tyagi," *Data Hiding in Image using least significant bit with cryptography*" International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 4,April 2012

[23] Warkentin M., Schmidt M.B. and Bekkering E. (2008). "*Steganography and Steganalysis*" Premier reference Source – Intellectual Property Protection for Multimedia Information technology, Chapter XIX, pp 374-380.