The Act of Steganography from Ancient Era to Digital Age

N.D. Jambhekar
Department of Computer Science
S.S.S.K.R. Innani Mahavidyalaya
Karanja (Lad), Dist. Washim (M.S.), India

C.A. Dhawale
MCA Department
P.R. Pote College of Engineering & Management
Amravati (M.S.), India

ABSTRACT

Digital data in the form of text, images, audio and video are transmitted over the internet by means of communication links. The confidentiality of secret data should preserve from intruders. Steganography has a group of methods with which different algorithms are used to embed the secret data under the cover medium such as image, without any detectable indications on the cover image. This paper focuses on some image steganographic methods used from many years, the methods used currently and the capabilities of steganography in future.

Keywords

Steganography, attacks, steganalysis.

1. INTRODUCTION

Effective and efficient steganographic algorithms are those who hide the sensitive data under the cover medium such as image, without leaving any detectable clue to the intruders. The strength of the steganographic algorithms is to keep the confidential information under an image such a way that, no any steganalysis method, or tool extracts the original secret message from the cover image without finding right stegokey. Stegokey is used to merge the secret data under the cover image. The stegokey is unique and used for encryption and same for decryption. This stegokey must be preserved by both sender and receiver. Recently, many researchers have worked on steganography and written the benefits of the different steganographic algorithms. In this paper, we are analyzing some digital image steganographic algorithms used in past years, currently practiced methods and giving focus on the capabilities of steganography in the future.

Steganography is a group of methods used for securing the secret information under the cover medium such as an image using some translation rules. Here the translation rules merge the selected text into the image, that makes the simple text secure and no one can easily plunder the secret information.

Because of steganography two communication sides transfer the confidential data secretly where attacker unknown the secret message covered in other medium such as cover images [19]. Steganography is the technique in which the original message which is being transmitted over the unsecured communication channel will be masked into the cover medium such as image, audio or video such that any human being, the device or the specialized software cannot predict the original hidden data. In steganography, the secret message transmission is possible using two entities such as the original message to be transmitted and the message carrier used to cover the transmitting message. Using the image steganographic method, the secret message is covered by an image in such way that the original message cannot predict by the intruders. The variations are done slightly that do not reflect the visual changes on the cover image.

2. STEGANOGRAPHY IN THE EARLY AGE

The Steganography suggest itself as a Greek word made from steganos - covered or secret and graphy - writing or drawing. The first steganographic technique was coming in the history of ancient Greece around 440 B.C. The Greek swayer Histaeus use the steganography in a new way to hide secret messages by shaving messenger's head, waiting to grow hair again, then again shaving the head and waiting to grow hair, so that the it will hide the secret message under long hair. On the other side, recipient finding the secret message by trimming hairs of messenger. The recipient was also using the same method to reply.

During 480 B.C. the next steganographic technique was evolved. Demerstus use the technique of writing the secret message to the Spartans that warns high intrusions by Xerxes. The secret message was put on the surface of wooden wax tablet and again covered with fresh wax. This tablet was delivered to the destination place with its hidden secret message [15, 16].

Johannes Trithemius (1 February 1462 – 13 December 1516) is a first person who was the German Renaissance humanist, advisor to Emperors in Germany, the founder of scientific bibliography and one of the founders of modern cryptography also wrote the "Steganographia". He is a first author of the first printed work on cryptography, the Polygraphia [1].

With the publication of Auguste Kerchoffs', cryptography militaire, although this work was mostly about cryptography, but describes the principal that was helpful in designing the new steganographic system, known as Kerchoff's principal regarding the steganography [3]. During both world wars, steganography helped to hide the confidential message using invisible ink which would gleam by keeping on the flame [15].

3. DIGITAL STEGANOGRAPHY TODAY

Thereafter the ancient steganographic techniques, many researchers discovered the steganographic algorithms that provide the high security features to secure the digital document. Intruders also develop methods that evacuate the safe message known as the steganalysis. Moreover, the ultimate use of the internet for the communication of the digital document was coming into existence in the recent days. Due to intensive use of internet- an unsecured communication channel, the sensitive data is not safe today.

The mathematical techniques that available in the cryptography have some limitations and can prone to crack mathematically by anyone with little efforts. The image steganography is more secure, but the processing and extraction of the secret message from the cover image required some processing time. But in the present digital era, by using the advanced computer systems with massive processing speed, this task is under control. Today the secret sharing over the internet is possible by applying the steganography, by carrying the following process effectively.

- Confidential data to be transmitted firmly.
- Cover image selection to hold secret message.
- Selection and implementation of the method that merge the secret message in the cover medium.
- The key that is used for the conversion method and also to uncover the secret message.

To secure the text using the steganographic techniques, the original text message is scrambled, shuffled or mixed with other text data with the help of mathematical function. Only the legal receiver can reverse this process to extract the message. The image steganographic technique hides the secret information under the cover image. In audio steganography, the multimedia such as text, image or sound can be put in the other cover audio signals that do not give the impression of this mixing. This is similar for the video steganography, where two videos intermix with each other, or any carrier date like text, image or audio signals are merged with the covert video.

The algorithms used today to secure the digital document, commonly follows the steganographic rules as the one shown in the following figures.

The following figure shows the steganographic system.

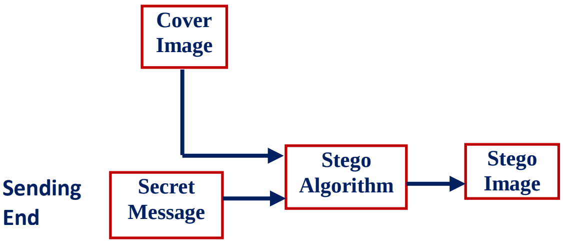

Fig 1: Sender side Steganographic system

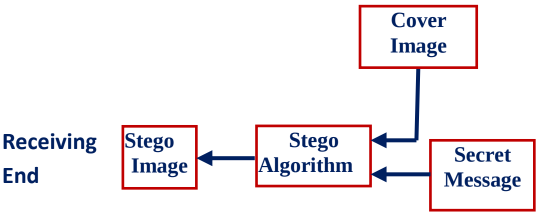

Fig 2: Receiver side Steganographic system

Before moving to the steganographic techniques, lets first understand about the digital image formats. Today for the steganography, the BMP- Bitmap, GIF- Graphics Interchange Format, JPEG- Joint Photographic Experts Group image formats are widely used.

BMP-Bitmap

Most operating systems support bitmap images with 1, 4, 8, 16, 24 and 32 bits per pixel. Here, the concentration is largely on the monochrome i.e. grayscale images and 24 bit color images because of the requirement of processing power, storage and transmission capacity of the network.

GIF-Graphic Interchange Format

GIF is CompuServe's standard that defines the generalized color raster images. This Graphics Interchange Format permits high-quality, high-resolution graphics compatible for a variety of graphics hardware and is proposed as an exchange and display mechanism. It uses up to 256 colors from the 24-bit RGB color space, and stores both the palette and the pixel matrix.

JPEG-Joint Photographic Experts Group

It is the most commonly used standard for lossy and lossless compression till today. It is very efficient photographic image technique and can make an excellent quality image even if it is a lossy compression technique. Because of the lossy compressed nature, some visual quality is lost in the compression process. With the lossless compression, the quality is great. The images used for the steganography are the 8 bit grayscale images as well as color images.

The steganographic methods used today are categories into image domain, transform domain, spread spectrum domain and statistical technique.

3.1 Image or Spatial Domain

Implant secret information in a cover image by changing the intensity of Least Significant Bits.

3.1.1 Least Significant Bit

Image's every Least Significant Bits are somewhat randomly noisy and when replaced or modified, do not affect the visual quality of the image. Using the LSB substitution technique, the secret message in binary format is first permuted and then substituted in the image in place of every bytes least significant bit place, bit by bit fashion [8]. The bit insertion depends on the bits available in the secret message. If the message is bigger, then the cover image should be enough bigger to hide it [20]. The LSB substitution is suitable for BMP images where they are lossless.

LSB Substitution Algorithm

Step 1: Scan the secret message (text or image) along with the cover image

Step 2: Convert secret message to binary data.

Step 3: Permute the binary bits of secret message

Step 4: Calculate LSB position of every byte of the cover image.

Step 5: Substitute every bit of cover image to the LSB of the cover image bit by bit.

Step 6: Save the image after LSB substitution and is the Stego image.

LSB Algorithm to read the secret message from Stego image

Step 1: Scan the Stego image

Step 2: Estimate LSB position of each byte of Stego image.

Step 3: Extract each LSB bit and convert each 8 bits into a character.

3.1.2 Spread Spectrum

In spread spectrum techniques, data hidden inside the cover image is spread completely making undetectable [10]. Using this technique, the message is planted in noise and then mixed with the cover image producing the stego image. The cover image has powerful signals than the embedded signals. Therefore, it is difficult to notice by the human eye or even by the computer system [11].

The Spread spectrum technique is statistically robust where the information is spread completely in the cover image. Here the secret data are dispersed throughout the cover image, without modifying the statistical parameters of the cover image. Most steganographic applications now use the spread spectrum techniques because of its extreme mathematical and complex approach.

3.2 Transform Domain Techniques

Transform domain provides the robust watermarking feature because of its data embedding technique and greater capacity. Transforms domain techniques include the discrete cosine transform (DCT), discrete Fourier transform (DFT) and discrete wavelet transform (DWT). When data inserted or embed using the transform techniques, the secret data can stay in the robust zones, scattered across the cover image and provides safety against any signal processing attack.

3.3 Statistical Method

Encrypt valuable information by applying specific statistical functions on a cover image and performing the variable possible test to extract the hidden information.

3.3.1 Patchwork

This uses statistical method to create a redundant pattern of secret data scattered over the cover image [6, 7]. In this, two different sections of cover image selected, where the secret message will completed embedded on two different patches. The implementation is redundant because, if any patch get destroyed, then the secret message can be easily available from other patch. But if the message is bigger, then only the single patch is possible depending on the size of the cover image. All this procedure is done on the grayscale image, because of the time, speed and space complexity of the algorithms and processors. This patch work is done by increasing the pixel intensity of one patch and decreasing the pixel intensity of another patch [9], also known as masking approach. Here the change is not noticeable and do not affect the quality of the cover image.

Because of its robustness, it is advantageous over the malicious manipulation of images. Because of the secret data distributed over various parts of the cover image and if the data is lost due to cropping of modification in the image, then it can be accessed through other part because of the multiple copies embedded as patches. Patchwork is beneficial to transfer highly sensitive small amount data.

The steganographic system is efficient enough to secure the hidden messages, but many researchers are working on the Steganalysis that accept the challenge to break the security to extract the secrets.

4. STEGANALYSIS

Steganalysis is the technique with which, anyone can extract the secret message from the cover image. But the requirement is only the right algorithms or method to unhide the information from the cover image. Many researchers work on the steganalysis to break the hidden system of steganography and extract the secret message [5]. The attacks on the steganography in the form of steganalysis are discussed below.

4.1.1 Stego-only Attack

Only the Stego image is analyzed and feasible methods are applied to discover the secret signals.

4.1.2 Known Cover Attack

Both cover and stego object is compared and pattern differences are detected suck as the secret image and the image with the hidden information are selected for comparison.

4.1.3 Known Message Attack

The sample stego image with known secret hidden message is analyzed. The similar technique will be applied to extract the hidden message from other stego images.

4.1.4 Chosen Stego Attack

The hidden information is known with respect to the stego object and the steganographic method (tools) to extract it.

4.1.5 Chosen Message Attack

The stego object is generated from the chosen message using the steganographic tools. This type of attack checks the matching patterns of the newly generated stego object and can determine the particular steganographic algorithm or tools used.

4.1.6 Known Stego Attack

The verification of actual and stego object is done using known steganography algorithms or tool [21].

5. FUTURE OF STEGANOGRAPHY

Early days, the war has been come into exists by actually demolishing the countries physically by harming the living creature using mechanical, chemical weapons. Today is the digital era. The future war will not happen on any physical surface. It was already started digitally. The destruction of sensitive data is done everywhere. The future of steganography is moreover needed to be powerful. It makes powerful by applying the hybrid methods from the existing methods. This integrated use of steganographic methods can reduce the harm from the digital war. The future needs the powerful communication medium like 3G-3rd generation and 4G-4th generation spectrum of mobile telecommunications technology. This requirement is essential because the future steganographic algorithms might need more processing capabilities and space and keys might be longer to transmit the communication channels. Depending on the efficiency of the steganographic algorithms [13], the integrated or hybrid techniques are beneficial for the future applications.

In spite of the different attacks on steganographic system, following are some factors need to be rigorously carried out such as

5.1.1 Steganographic Security Enhancement

The strength of the steganographic algorithm must be improved to increase the security of the information transmitted over the mobile communication channel. Some factors affected the security mechanism should be improved.

5.1.2 Efficient Embedding

The embedding efficiency will be increased that causes the larger secrets to be efficiently embedded in the cover image without any noticeable effect on the image.

5.1.3 Reducing Distortion

An optical phenomenon, resulting from the failure or noticeable production of a stego image, due to the bad embedding process from the steganographic method. Choosing the efficient embedding method makes the lossless, distortion free stego image, makes the stego and the cover image perceptually and statistically closer together. The calibration method as proposed by Jessica Fridrich [22] for JPEG images, the calibration is carried out by restoring the stego image to uncompressed original form, clipping in all sides slightly by a few pixels and recompressing with the help of a similar quantization table.

5.1.4 Suitable cover Selection

The proper selection of cover image makes the unnoticeable detection of the secret information. Kharrazi et al. [23] gives the result indicates that the minimization of the number of changes made to the cover image serves as a reliable measure

6. DISCUSSION & FUTURE SCOPE

The steganography itself is a secret for many hundred years. The appearance and use it in secret writing or hiding is different. The secrets are something that baffles understanding and cannot be explained is in existence because of the steganography. In the current era, efficient algorithms are designed that helps to keep the intruders away from the secret information hidden in the cover image. Many steganalysis methods are developed to extract the hidden information. The effectiveness of the steganographic algorithms will be increased by Security Enhancement discuss in this paper such as efficient embedding, reducing distortion, suitable cover selection. Therefore, no any type of steganographic attack breaks the security mechanism implemented by the advanced steganograhic algorithm.

7. REFERENCES

[1] Reeds, J. 1998. Solved: The Ciphers in Book III of Trithemius's Steganographia. AT&T Labs Research. Florham Park. New Jersey 07932.

[2] Morkel, T., Eloff, J.H.P. and Olivier M.S. 2005. An Overview of Image Steganography. Proceedings of ISSA 2005. New knowledge Today Conference. Sandton South Africa.

[3] Rabah, K. 2004. Steganography- The Art of Hiding Data. Information Technology Journal. 3(3), pp. 245-269. ISSN 1682-6027.

[4] Ker. A. 2005. Improved Detection of LSB Steganography in Grayscale Images. Lecture Notes in Computer Science. vol. 3200, pp. 97-115.

[5] Staff, CACM. 2014. Know your Steganographic Enemy. Communications of the ACM, Vol. 57 No. 5, Page 8.

[6] Kaur, S., Bansal, S., Bansal, R.K. 2014. Steganography and classification of image steganography techniques. International Conference on Computing for Sustainable Global Development (INDIACom). pp.870-875.

[7] Johnson, N. F. and Jajodia, S. 1998. Steganalysis of Images Created Using Current Steganography Software. Information Hiding. Springer. Lecture Notes in Computer Science. Volume 1525, pp. 273-289.

[8] Thangadurai, K., Sudha Devi, G. 2014. An analysis of LSB based image steganography techniques. International Conference on Computer Communication and Informatics (ICCCI). pp.1-4.

[9] Bender, W., Gruhl, D., Morimoto, N. and Lu, A. 1996. Techniques for data hiding. IBM Systems Journal. vol.35, no. 3.4, pp. 313-336.

[10] Wang, H. and Wang, S. 2004. Cyber warfare: Steganography vs. Steganalysis. Communications of the ACM. 47:10.

[11] Marvel, L. M., Boncelet Jr., C. G. and Retter, C. 1999. Spread Spectrum Steganography. IEEE Transactions on image processing. 8:08.

[12] Ge Huayong, Huang Mingsheng, Wang Qian 2011. Steganography and steganalysis based on digital image. 4th International Congress on Image and Signal Processing (CISP). vol.1, pp. 252-255.

[13] Jambhekar, N.D., Dhawale, C.A. and Hegadi, R. 2014. Performance Analysis of Digital Image Steganographic Algorithm. ICTCS '14 Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies. Udaipur, Rajasthan, India, Article No. 82. ACM.

[14] Johnson, N. and Katzenbeisser, S. 2000. A Survey of steganographic techniques. Information Hiding. Artech House, pp. 43-78.

[15] Siper, A., Farley, R. and Lombardo, C. 2005. The Rise of Steganography. Proceedings of Student/Faculty Research Day. CSIS. Pace University.

[16] Judge, J. C. 2001. Steganography: Past, Present, Future. SANS Institute.

[17] Bilal, I., Roj, M.S., Kumar, R. and Mishra, P.K. 2014. Recent advancement in audio steganography. International Conference on Parallel, Distributed and Grid Computing (PDGC). pp.402-405.

[18] Zielińska, E., Mazurczyk, W. and Szczypiorski, K. 2014. Trends in Steganography. Communications of the ACM, Vol. 57 No. 3, Pages 86-95.

[19] Petitcolas, A. P., Fabien, R. J., Anderson, M. G., Kuhn 1999. Information hiding-a survey. Proceedings of the IEEE. vol.87, no.7, pp.1062, 1078.

[20] Kessler, G.C. 2004. An Overview of Steganography for the Computer Forensics Examiner. FBI Forensic Science Communications. 6(3).

[21] Richer, P. 2003. Steganalysis: Detecting hidden information with computer forensic analysis. SANS Institute InfoSec Reading Room.

[22] Fridrich, J. 2004. Feature-based steganalysis for jpeg images and its implications for future design of steganographic schemes. Proc. of the 6th Information Hiding Workshop. Springer, vol. 3200, pp. 67-81.

[23] Kharrazi, M., Sencar, H. T. and Memon, N. 2006. Cover selection for steganographic embedding. In proceedings of IEEE International Conference on Image Processing. pp. 117-120.

[24] Amin, M.M., Salleh, M., Ibrahim, S., Katmin, M.R. and Shamsuddin, M.Z.I. 2003. 4th National Conference on Information hiding using steganography Telecommunication Technology NCTT Proceedings IEEE. pp. 21-25.