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

An Overview and Survey on Image Steganography Technique

Arun Sharma
M.Tech (C.S.E.), S.A.T.I.
India

Abstract— Steganography is a one of the technique for information hiding. With the help of steganography people can communicate secretly. It involves communicating secret data in an appropriate multimedia carrier such as Text, Image, audio, and video files. The main motive of steganography is to ensure that the transmitted message is completely hidden inside the cover signal, and thereby ensuring that the message is accessible only by the intended receiver and not by any intruders or unauthorized parties. This review paper discusses state-of-the-art review and analysis of the different existing methods of steganography along with their strengths and weaknesses. This paper also provides a some common standards and guidelines drawn from the literature.

Keyword - Image steganography, payload, stego image, cover image, secret sharing.

I. INTRODUCTION

The rising possibilities of modem communications need the special means of security especially on computer networking. The network security is becoming more important as the number of data being exchanged on the Internet increases. So, the confidentiality and data integrity are required to protect data against unauthorized access and this resulted in an explosive growth of the field of information hiding. Information hiding techniques are receiving much attention today due to fear of encryption services getting illegal, and copyright owners who want to track confidential and intellectual property , copyright protection against unauthorized access and use in digital materials (music, film, book and software) through the use of digital watermarks. Advance security is not maintained by the password protection but it is gained by hiding the existence of the data which can only be done by Steganography [1].

Steganography is an art and science of hiding information in some cover media. The term originated from Greek words means "covered writing". The objective of steganography is to hide the fact of communication. In the steganography the sender embeds a secret message into digital media (e.g. im-age) where only receiver can extract this message. It simply takes one piece of information and hides it within another. This hidden information can be plain text, cipher text, or even images. It is not intended to replace cryptography but supplement it. With the help of Steganography the chance of hidden message being detected can be reduced [2].

Steganography is mainly oriented around the undetectable transmission of one form of information within another. The steganography algorithms were primarily developed for digital images and video sequence, interest and research in audio steganography started if an attacker knows the embedding method. Steganography works by replacing bits of useless or unused data in regular computer. Any steganography technique has to satisfy two basic requirements. The first requirement is perceptual transparency, i.e. cover object (object not containing any additional data) and stego object (object containing secret message) must be perceptually unclear. The second constraint is high data rate of the embedded data [3].

II. CLASSIFICATION OF STEGANOGRAPHY

Steganography techniques can be classified into 4 categories which is defined in given figure:

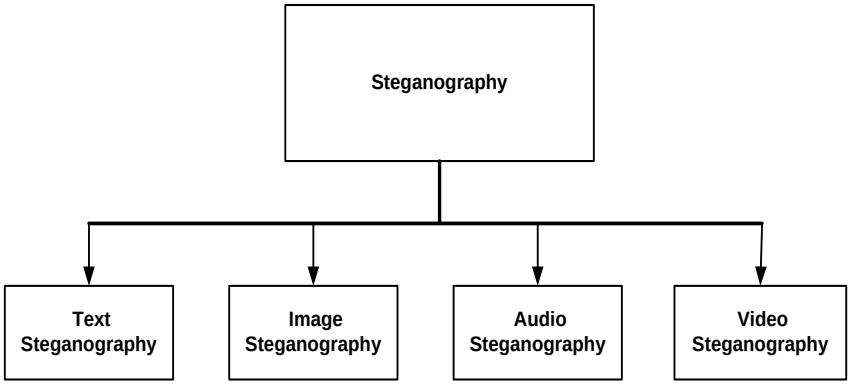

Figure 1. Classification of steganography techniques

A. Text Steganography

Text steganography simply means information is hidden inside the text files. The text steganography involves anything from changing the formatting of an existing text, to changing the word within the text, to generating random sequences or using context-free grammars to generate readable texts [4].

B. Video Steganography

Video files are generally a collection of images and sounds, therefore,most of the presented techniques on images and audio can be applied to video files too. Due to fact that video is a moving stream of images and sounds, the large amount of data that can be hidden inside the video. And because of video is continuous flow of information, any small but otherwise noticeable distortions might go by unobserved by humans. So video steganography is nothing but a combination of image and audio steganography. So, the combined evaluations i.e. the evaluations for image and audio steganography can be taken together for the evaluation of video steganography. While doing video steganography, the effect on video has to be kept in mind to achieve a secure communicating [5].

C. Image Steganography

Image steganography has been a vast area of research for many years now. It is a process that hides the secret image behind the cover image in such a way that the presence of the secret image is locked and the cover image appears to be the same [5]. In such a way, the digital information can be embedded and transferred to the destination with minimum risk of detectability. many different image file formats exist in the domain of digital images. For these different image file formats, different steganographic algorithms exist.

]D. Audio steganography

In a computer-based audio steganography system, digital sounds are used to embed secret messages and this secret message is embedded by slightly altering the binary sequence of a sound file. In existing audio steganography methods WAV, AU, or MP3 sound files are commonly used to embed secret messages. Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other digital images. a variety of methods for embedding information in digital audio have been introduced,in order to conceal secret messages successfully[5].

III. TYPES OF ATTACKS AGAINST STEGANOGRAPHY

Steganalysis is the comparison between the carrier (cover), stego-image and the hidden message. The various methods used to analyze stego-images are termed attacks and include:

a. **stego-only**, where the attacker has access only to the stego-image,
b. **known cover**, where the attacker has access only to the carrier,
c. **known message**, where the attacker has access only to the message,
d. **chosen stego**, where the attacker has access to both the stego-image and stego algorithm, and
e. **chosen message**, where the attacker generates a stego-image from a message using an algorithm, looking for signatures that will enable him to detect other stego images. Table 1 illustrates this more clearly.

Table 1: Type of attack

Attacker employs:	**When attacker has access to:**			
Attack	**Stego-Image**	**Cover**	**Message**	**Algorithm**

Amount of data that can be hidden inside the video. And because of video is continuous flow of information, any small but otherwise noticeable distortions might go by unobserved by humans. So video steganography is nothing but a combination of image and audio steganography. So, the combined evaluations i.e. the evaluations for image and audio steganography can be taken together for the evaluation of video steganography. While doing video steganography, the effect on video has to be kept in mind to achieve a secure communicating [5].

Table 1: Type of attack

Attacker employs:	**When attacker has access to:**			
Attack	**Stego-Image**	**Cover**	**Message**	**Algorithm**
Stego-only	√			
Known cover		√		
Known message			√	
Chosen stego	√			√
Chosen message			√	√

IV. ADVANTAGES AND DISADVANTAGES

It can and will be used for two purposes, good and evil. Both government and private industries need to worry about the use of Steganography inside of their respective buildings .The main advantages of Steganography are:

- It can be used for secretly transmitting message without being discovered.
- It does not allow the enemy to detect that there is secret information inside the cover file.
- It can be used by anyone using internet.
- However,Steganography has number of disadvantages.They are :
- It generally requires a lot of overhead to hide a relatively few bit of information. However, there are ways around this.
- Once a Steganography system is discovered, it is rendered useless. This problem, too, can be overcome if the hidden data depends on some sort of key for its insertion and extraction.

V. APPLICATIONS

In general, three application types for image steganography techniques [6]:

1. Secret Communication
2. Improved Communication.
3. Data Storage.

Apart from these there are many application where the image steganography is used and are listed below:

1. Steganography can be used anytime when anybody wants to hide data. It prevents unauthorized persons from becoming aware of the existence of a message.
2. In the business world it can be used to hide a secret chemical formula or plans for a new invention.
3. Steganography can be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser.
4. Terrorists can be use steganography to keep their communications secret and to coordinate attacks.
5. Steganography can be used in military for secret communication purpose.
6. Steganography can also be used to implement watermarking.

VI. IMAGE STEGANOGRAPHY MODEL

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. Steganography not only is used to prevent others from knowing the hidden information, but it also is used to prevent others from thinking that the information even exists [7].

Image steganography technique consists of Carrier file (Image), Secret message and Password. Carrier is also known as a cover-file, in which the secret information is to be embedded.Message is the data that the sender wishes to remain it confidential and wants to send inside the cover files. Message can be plain text, audio, image, or any type of file. Password is known as a stego-key, which is used to ensure that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. In general, the cover-file with the secret information is known as a stego-file.

To hide the data inside the cover image takes following two steps [7].

i. Identification of redundant bits in a cover-image. We can say that redundant bits are those bit that can be modified without corrupting the quality or destroying the integrity of the cover-image.

ii. To embed the secret information in the cover image, the redundant bits in the cover image is replaced by the bits of the secret information.

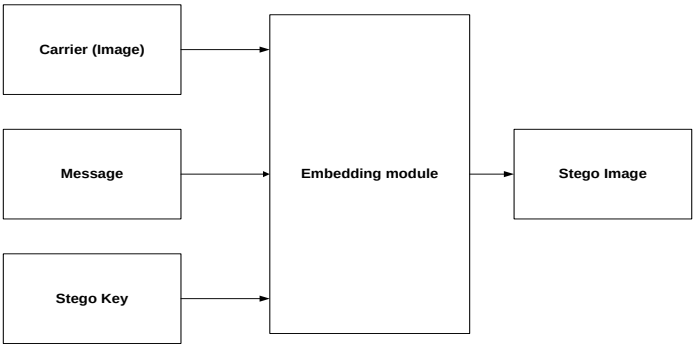

Figure 2. Basic Audio steganography model

VII. SURVEY ON IMAGE STEGANOGRAPHY

Steganography is an active field of research; many attempts are already been done. Most of them are based on LSB based lossy techniques. In this section we briefly review some of the major work in this topic of research.

In 2004 **Xinpeng Zhang et al.** [8] proposed a modified pixel value differencing steganography with larger payload and higher imperceptibility. This proposed method overcomes the disadvantage of pixel value differencing method proposed by Wu and Tasi (2003) . Pseudo-random dithering is applied to the division of ranges of the pixel-value differences which effectively handles the vulnerability of histogram analysis.

In 2007 **X. Li and Wang** [9] proposed a steganographic method which modifies the JPEG quantization table and inserts the secret bits in the middle frequency coefficients of the cover image. Secret bits are inserted into the insignificant bits of DCT coefficients. Li also proposed another method based on JPEG and Particle Swarm Optimization algorithm (PSO) techniques. With the help of PSO algorithm an optimal substitution matrix is derived for transforming a secret message. The standard JPEG quantization table is also modified to occupy more secret messages. The transformed values are hidden in the middle frequency components of the quantized DCT coefficients of the cover-image. By using JPEG entropy coding method, the JPEG stego image is generated. The proposed method achives better image quality, high payload and security.

In 2007 **Ching-Yu Yang** [10] proposed a steganography method based on the module substitutions. The secret bits to be embedded in the block are first determined by the base-value (BV) of the block in R-, G-, and B-component of a RGB trichromatic system. And then, the data bits are embedded in each component respectively by Mod u, Mod u-v, and Mod u-v-w module substitutions.

In 2008 **Hassan Mathkour et al.** [11] proposed a technique which emphasizes undetectability. It allows for the change of intensity of image planes of (24 bit) colored image to embed secret message in a specific distance between them.This technique is based on changing the distance of two random selected pixel channels in a specific range that represent hidden data.

In 2009 **Han-ling Zhang et al.** [12] presented an approach which is based on pixel value differencing. It makes use of the largest difference value between the three pixels nearer to the target pixel to calculate how many secret bits will be embedded into the pixel. Authors of this papers applied optimal pixel adjustment process (OPAP),in order to enhance the image quality of the stego-image.

In 2009 **Hassan Mathkour et al.** [13] proposed variations of LSB substitutions. In the former method key idea was to divide the image into many segments and apply a different processing on each segment. Whereas in the latter one, data is encrypted using a key and is replaced with the LSB of RGB color image. And the length of the hidden message is stored in the 1st row of stego image.

In 2011 **Subba Rao et al.** [14] presented an image steganography technique that randomizes the sequence of cipher bits. They computed the suitability measure of the various random sequences of the cipher bits against a given image and select the random sequence closest to the image. Then they generated those random sequences by the use of an L.F.S.R. Then they embed these random sequences of cipher bits in the image.

In 2011 **Velagalapalli et al.** [15] proposed a technique known as Stego JPEG to hide data in jpeg images. They perform JPEG compression on the data to be hidden. a new cryptography technique known as 'Rotatocrypt' to encrypt or decrypts data using rotations is used in this paper. A list called 'PassStore' is created from the password used. And then encryption is done by right rotating the bits as guided by the value in PassStore.

In 2012 **Anastasia Ioannidou et al.** [16] proposed an algorithm by combining a high payload embedding scheme for color images and a hybrid edge detector for secret message data embedding. Higher peak signal to noise ratio is achieved for the same number of bits per pixel of embedded image. An edge in the image is found by sobal edge detector, laplacian filters, and fuzzy edge detector. In this paper authors achieved better PSNR value but the relationship between the neighboring pixels is not considered into account for data embedding.

In 2012 **Xian-ting Zeng et al.** [17] presented a method for lossless data hiding with large payload based on histogram shifting and multi layer embedding. In this technique the original image and secret information is extracted from the stego image by using only the length of the hidden data and no other extra information is needed. In the proposed scheme 13 layer embedding could be applied and achieved greater bits per pixels compared to existing method.

In 2012 **Patel and Dave** [18] have proposed a new variant of LSB based image steganography. In this, both the parties will have to agree upon a set of carrier images and certain required parameters. Next,from the set of carrier images which requires least number of bit manipulations on LSB substitution of secret data, the sender will select an image and produce stego image. Then the receiver on receiving stego image will extract LSBs along with the help of the received parameters .Since the possibility of guessing parameters is very less,Therefore extraction without those parameters is very difficult to achieve . So in this technique both the parties agree upon a set of carrier images the visual difference between stego image and original image can be reduced.

In 2012 **Johri and Asthana** [19] proposed a steganography technique in which data is embedded using alteration component technique. In this technique, with the help of key and secret message each pixel is replaced with new values. Then for the security of stego image palette based image technique is applied by stretching process. The receiver having the same secret key applies destretching palette process on stego image using alteration component extraction process to extract the data. This technique has higher capacity and better imperceptibility.

In 2012 **Swati and Mahajan** [20] proposed a secure image steganographic model using RSA algorithm and LSB insertion. In this method, the secret data is first encrypted using recipient's RSA public key and then each bit of the encrypted message is inserted to the LSBs of image in different images so as to find the best cover image. Best cover image is the one which requires minimum number of LSB changes. The receiver on receiving the stego image will extract the message in the encrypted form and will decrypt it using private key.

VIII. CONCLUSION

This Paper briefly describes a survey on recent steganography techniques for image in spatial and transform domain. The strength of the steganographic technique depends mainly on three factors - robustness, imperceptibility level in the stego image, and embedding capacity. The steganographic system leaves unique patterns on the cover images and these

patterns feats the steganalyst. When the size of the secret message is small, the transform domain based techniques such as DCT, DWT and adaptive steganography are not less prone to steganalysis. In this technique the distortion will be also less because embedding is performed in transform domain. All the above problems must be addressed while designing a steganography technique which should be robust to attacks. We need to develop steganography techniques where we can embed data equal or more than existing techniques and without any distortion in stego image so that the security of the message can be enhanced.

REFERENCES

[1] Zaidoon Kh., AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi," Overview: Main Fundamentals for Steganography ", journal of computing, volume 2, issue 3, March 2010.

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

[3] Prof. Samir Kumar Bandyopadhyay, Tuhin Utsab Paul , Avishek Raychoudhury, " A Robust Audio Steganographic Technique based on Phase Shifting and Psycho – acoustic Persistence of Human Hearing Ability", International Journal of Computing and Corporate Research .

[4] K. Benett, "Linguistic steganography- survey, analysis and robustness concerns for hiding information in text," Purdue University, CERIAS Tech. Report 2004-13, 2004.

[5] Petitcolas, F.A.P., Anderson, R., Kuhn, M.G.,"Information Hiding - A Survey", July 1999.

[6] Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", Proceedings of the 2nd Information Hiding Workshop, April 1998.

[7] Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000.

[8] Xinpeng Zhang , Shuozhong Wang , Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security, Pattern Recognition Letters 25 (2004) 331–339 .

[9] X. Li, J. Wang, A steganographic method based upon JPEG and particle swarm optimization algorithm, Information Sciences 177 (15) (2007) 3099-3109.

[10] C. Y. Yang, "Color Image Steganography Based on Module Substitutions," in Proc. IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, vol. 2, pp. 118-121.

[11] H. Mathkour, B. Al-Sadoon, and A. Touir, "A New Image Steganography Technique," in Proc. IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008, pp. 1-4.

[12] H. Zhang, G. Geng, and C. Xiong, "Image Steganography Using Pixel-Value Differencing," IEEE Second International Symposium on Electronic Commerce and Security, 2009, pp. 109-112.

[13] H. Mathkour, G. M. R. Assassa, A. A. Muharib, and I. Kiady, "A Novel Approach for Hiding Messages in Images," in Proc. IEEE International Conference on Signal Acquisition and Processing, 2009, pp. 89-93.

[14] Y. V. Rao, S. S. Rao, and N. R. Rekha, "Secure Image Steganography Based on Randomized Sequence of Cipher Bits," in Proc. IEEE Eighth International Conference on Information Technology: New Generations, 2011, pp. 332-335.

[15] V. L. Reddy, A. Subramanyam, and P. C. Reddy, "SteganPEG Steganography+ JPEG," in Proc. IEEE International Conference on Ubiquitous Computing and Multimedia Applications, 2011, pp. 42-48.

[16] Anastasia Ioannidou , Spyros T. Halkidis , George Stephanides , A novel technique for image steganography based on a high payload method and edge detection, Expert Systems with Applications 39 (2012) 11517–11524.

[17] Xian-ting Zeng , Zhuo Li , Ling-di Ping , Reversible data hiding scheme using reference pixel and multi-layer embedding , International Journal of Electronics and Communications (AEÜ) 66 (2012) 532– 539.

[18] H. J. Patel and P. K. Dave, "Least Significant Bits Based Steganography Technique," in Proc. IJECCE 2012, vol. 3, pp. 97-103.

[19] S. Johri., "An Adaptive Steganography Technique for Gray and Colored Images," Journal of Global Research in Computer Science, vol. 3, pp. 41-45, 2012.

[20] S. Tiwari, R. P. Mahajan, and N. Shrivastava, "Steganography-an Approach for Data Hiding Based on Encryption and Lsb Insertion," IJECCE, vol. 3, pp. 76-83, 2012.

