International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Issue No. 12, December 2015
www.ijates.com
ijates
ISSN 2348 - 7550

REVIEW ON STEGANOGRAPHY FOR HIDING DATA

Rohit Saluja[1], Kriti Kanwal[2], Sonal Dahiya[3]

[1,2,3]*Pursuing B.Tech in Computer Science & Engineering,*

Hindu College Of Engineering, Sonepat, (India)

ABSTRACT

Steganography is the science of hiding the fact that communication is taking place, by hiding information behind information. Many different carrier file formats can be used, but digital media are the most popular because of their usage on the Internet. For hiding secret information in digital media, there exists a large variety of steganography techniques some are more complex than others and all of them have some advantages and disadvantage. Various applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret data, while others require a larger secret data to be hidden. This paper intends to give an overview of Digital media steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which stenographic techniques are more suitable for which applications.

Keywords: Steganography; Image Processing; Data Hiding; Information; Security Cover Data

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was proposed as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the information secret. Unfortunately it is sometimes not enough to keep the contents of an information secret, it may also be necessary to keep the existence of the information secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information behind other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing".

In steganography the information is hidden exclusively in digital media. Steganography has become an interesting and challenging field of research striving to achieve greater immunity of hidden data against signal processing operations on the host cover media like image, audio, or text. A good Steganography technique should offer immunity of hidden data against loss compression, scaling, interception, modification, or removal etc. and ensure that embedded data remains inviolate and recoverable.

II. LITERATURE REVIEW

In 2010, Jing-Ming Guo, *Member, IEEE*, and Thanh-Nam Le proposed a paper on "Secret Communication Using JPEG Double Compression" which says protecting privacy for exchanging information through the media

has been a topic researched by many people. Up to now, cryptography has always had its ultimate role in protecting the secrecy between the sender and the intended receiver. However, nowadays steganography techniques are used increasingly besides cryptography to add more protective layer to the hidden data. In this paper they showed that the quality factor in a JPEG image can be an embedding space, and they discussed the ability of embedding a message to a JPEG image by managing JPEG quantization tables (QTs). In combination with some permutation algorithms, this scheme can be used as a tool for secret communication. The proposed method can achieve satisfactory decoded results with this straightforward JPEG double compression strategy.

In 2011, Wei-Jen Wang, Cheng-Ta Huang, and Shiuh-Jeng Wang proposed a paper on "Data hiding is one of the most important techniques to achieve better data and communication protection by hiding information into a media carrier. It provides a secure method to distribute data through a public and open channel. Data hiding for vector quantization (VQ)-based images focuses on the problem of embedding secret data into a cover VQ-based image to achieve secret communication and data protection. This paper provides a state-of-the-art review and comparison of the different existing data-hiding methods for VQ-based images. In this paper, we classify VQ-based data-hiding methods into four no overlapping groups according to their reversibility and output formats, introduce the details of the representative methods, summarize the features of the representative methods, and compare the performance of the representative methods using peak signal-to-noise ratio, capacity of secret data, and bit rate. This paper shows that an irreversible method is very likely a VQ-based data-hiding method that produces a stego-image as its output, and it can embed more secret data than a reversible method. Nonstandard encoding methods (e.g., joint neighboring coding) are becoming popular in reversible data hiding since they can increase the capacity for embedding the secret data.

In 2012, Fangjun Huang, *Member, IEEE*, Jiwu Huang, *Senior Member, IEEE*, and Yun-Qing Shi, *Fellow, IEEE" Suggest a* paper, which presents a new channel selection rule for joint photographic experts group (JPEG) steganography, which can be utilized to find the discrete cosine transform (DCT) coefficients that may introduce minimal detectable distortion for data hiding. Three factors are considered in our proposed channel selection rule, i.e., the perturbation error (PE), the quantization step (QS), and the magnitude of quantized DCT coefficient to be modified (MQ). Experimental results demonstrate that higher security performance can be obtained in JPEG steganography via our new channel selection rule."

III. TYPES OF STEGANOGRAPHY

Steganography works have been carried out on different transmission media like images, video, text, or audio.

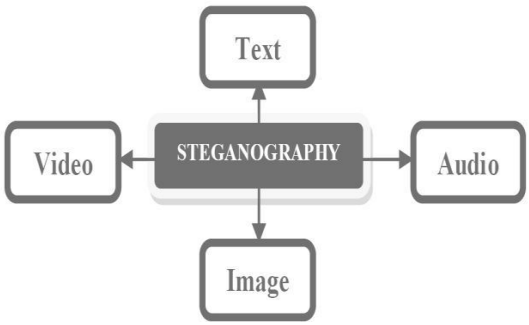

Fig.1 Types of Steganography

3.1 Image Steganography

JPEG compression is a commonly used method for reducing the size of an image, without reducing the aesthetic qualities enough to become noticeable by the naked eye. Broadly speaking, it extracts all the information from an image that the human eye is not perceptible to and would therefore not miss should it not be there.

3.2 Audio Steganography

Audio Steganography is the technology of embedding information in an audio channel. It is used for digital copyright protection. Watermarking is the technique which hides one piece of information [message] in another piece of information [carrier]. It is widely used for applications such as audio clip etc.

3.3 Video Steganography

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images & sounds. Therefore, any small out otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information.

3.4 Text Steganography

One major category, perhaps the most difficult kind of Steganography is text Steganography or linguistic Steganography because due to the lack of redundant information in a text compared to an image or audio. The text Steganography is a method of using written natural language to conceal a secret message. The advantage to prefer text Steganography over other media is its smaller memory occupation and simpler communication.

IV. ADVANTAGES

a. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

b. This method featured security, capacity, and robustness, the three needed aspects of steganography that makes it useful in hidden exchange of information through text documents and establishing secret communication.

c. Important files carrying confidential information can be in the server in and encrypted form No intruder can get any useful information from the original file during transmit.

d. With the use of Steganography Corporation government and law enforcement agencies can communicate secretly.

V. LIMITATIONS

. Huge number of data, huge file size, so someone can suspect about it.

a. If this techniques is gone in the wrong hands like hackers, terrorist, criminals then this can be very much

dangerous.

Table 1 Comparison of Secret Communication Techniques

Secret Communication Techniques	Confidentiality	Integrity	Un removability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes/No	Yes/No	Yes

Table 2 Comparison of Various Methods of Steganography

Sr. No	Steganography Techniques	Cover Media	Embedding Technique	Advantages
1.	Binary File Technique	Binary File	watermark can be embedded by making changes to the binary code that does not affect the execution of the file	Simple to implement
2.	Text Technique	Document	To embed information inside a document we can simply alter some of its characteristics.i.e. either the text formatting or characteristics of the characters	Alterations not visible to the human eye
3.	Image Hiding: 1) LSB	Image	It works by using	Simple & easiest

	(Least Significant Bit		the least significant bits of each pixel in one image to hide the most significant bits of another.	way of hiding Information.
	2) DCT (Direct Cosine Transform)		Embeds the information by altering the transformed DCT Coefficients.	Hidden data can be distributed more evenly over the whole image in such a way as to make it more robust.
	3) Wavelet Transform		This technique works by taking many wavelets to encode a whole image	Coefficients of the wavelets are altered with the noise within tolerable levels
4	Sound Technique	MP3 files	Encode data as a binary sequence which sounds like noise but which can be recognised by a receiver with the correct key	Used for watermarking by matching the narrow bandwidth of the embedded data to the large bandwidth of the medium
5.	Video Technique	Video Files	A combination of sound and image techniques can be used	The scope for adding lots of data is much greater

VI. CONCLUSION

Information hiding techniques received very much less attention from the research community and from industry than cryptography. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Here in this paper we have tried to present a new idea of Steganography by using Binary file technique, text technique, LSB, DCT, Wavelet transformation. Along with encryption of the secret Digital media this secret data has been provided with authentication security thus the secret data gets double protected and the data confidentiality increases. This property generates the stego data with minimum or zero degradation. This approach is capable of secure transfer of the message compared to earlier techniques with the addition of authenticity checking of the secret.

REFERENCES

[1]. Mohammad Shirali-Shahreza , "A new method for real time steganography", 2006

[2]. Yuk Ying Chung, fang Fei Xu, "Development of video watermarking for MPEG2 video" 2006.

[3]. Ravi Shah, Abhinav Agraval & Subramaniam Ganesham, "Frequency domain real time digital image watermarking", 2011

[4]. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, "Steganography and digital watermarking" 2011

[5]. C. Lu, J. Chen and K. Fan, "Real-time Frame-Dependent Video Watermarking in VLC Domain", 2005

[6]. H. M. Liao, and K. Fan, "Real-Time MPEG2 Video Watermarking in the VLC Domain", Proc.of 16th International Conference on Pattern Recognition, 2012

[7]. Jing-Ming Guo, Member, IEEE, and Thanh-Nam Le proposed a paper on "Secret Communication Using JPEG Double Compression", 2013