Research Paper Technology

Techniques of Steganography and Steganalysis

* Bhavsar Jaimin H ** Imran Khan

*,** Computer Science Dept, Institute of Engineering and Technology, Bhagwant University, Ajmer, India

ABSTRACT

In this paper we propose a new form of steganography, on-line hiding of information on the output screens of the instrument. This method can be used for announcing a secret message in public place Private marking system using symmetric key steganography technique and LSB technique is used here for hiding the secret information. Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. Steganographic messages are often first encrypted by some traditional means, and then a covertext is modified in some way to contain the encrypted message, resulting in stegotext. The detection of steganographically encoded packages is called steganalysis.

Keywords : Steganography, steganalysis, Cryptography, stegotext

INTRODUCTION

The word "Steganography" is of Greek origin and means "covered or hidden writing". Generally, a steganographic message will appear to be something else: a picture, an article, a shopping list, or some other message. With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important.

steganography has evolved into the practice of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. In contemporary terms, steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file (like a .wav or mp3) or even a video file. Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured.

Nowadays, using a combination of steganography and the other methods, information security has improved considerably. In addition to being used in the covert exchange of information, steganography is used in other grounds such as copyright, preventing e-document forging.

In steganography, the possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A possible formula of the process may be represented as:

cover medium + embedded message + stego key = stego-medium

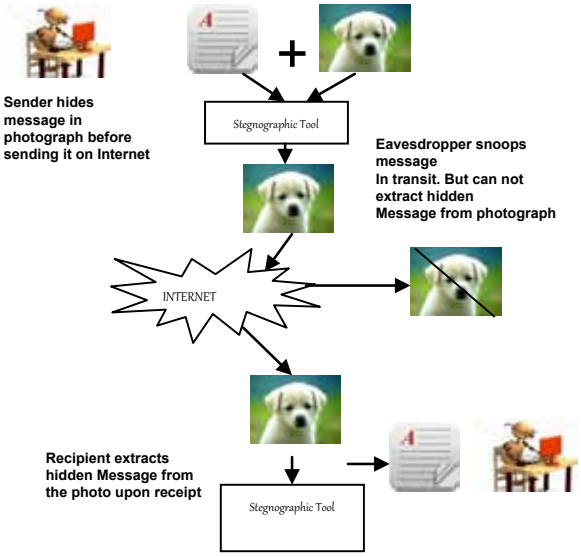

Fig 1 Steganography process

I. TYPES OF STEGANOGRAPHY

A) Robust: Robust marking aims to embed information into a file which cannot easily be destroyed
B) Fragile: This steganography involves embedding information into a file which is destroyed if the file is modified

Table1 comparison of various methods of stegnography:

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 (Least Significant Bit)	Image	It works by using the least significant bits of each pixel in one image to hide the most significant bits of another.	Simple & easiest 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 ismuch greater

II. STEGANALYSIS

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes". It is the art of discovering and rendering useless covert messages. The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information.Unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message.

Steganalysis generally starts with several suspect information streams but uncertainty whether any of these contain hidden message. The steganalyst starts by reducing the set of suspect information streams to a subset of most likely altered information streams. This is usually done with statistical analysis using advanced statistics techniques.

Steganalysis Techniques:
Hiding information within an electronic medium cause alteration of the medium properties, this can result in some form of degradation or unusual characteristics.

Unusual patterns:
Unusual patterns in a stego image are suspicious. For example, there are some disk analysis utilities that can filter hidden information in unused partitions in storage devices. Filters can also be used to identify TCP/IP packets that contain hidden or invalid information in the packet headers. TCP/IP packets used to transport information across the Internet have unused or reserved space in the packet headers.

Visual Detection:
Analyzing repetitive patterns may reveal the identification of a steganography tool or hidden information. To inspect these patterns an approach is to compare the original cover image with the stego image and note visible differences. This is called a known-carrier attack. By comparing numerous images it is possible that patterns emerge as signatures to a steganography tool. Another visual clue to the presence of hidden information is padding or cropping of an image.

Tools to Detect Steganography:
The disabling or removal of hidden information in images is dependent on the image processing techniques. For example, with LSB methods of inserting data, simply compressing the image using lossy compression is enough to disable or remove the hidden message. There are several available steganographic detection tools Such as Encase by Guidance Software Inc., I Look Investigator by Electronic Crimes Program, Washington DC, various MD5 hashing utilities, etc.

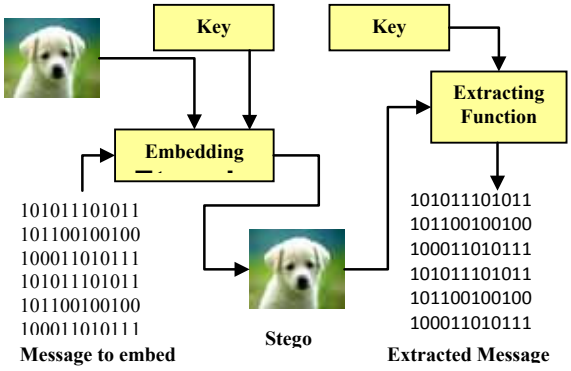

Fig 2 Tools to Detect Steganography

Comparison of Steganography and Cryptography:
Steganography and cryptography are closely related. Cryptography scrambles messages so it can't be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. With cryptography, comparison is made between portions of the plaintext and portions of the cipher text. In steganography, comparisons may be made between the cover-media, the stego-media, and possible portions of the message. The end result in cryptography is the cipher text, while the end result in steganography is the stego-media.

Combination of Steganography and Cryptography:
Those who seek the ultimate in private communication can combine encryption and steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

III. AUDIO STEGANOGRAPHY

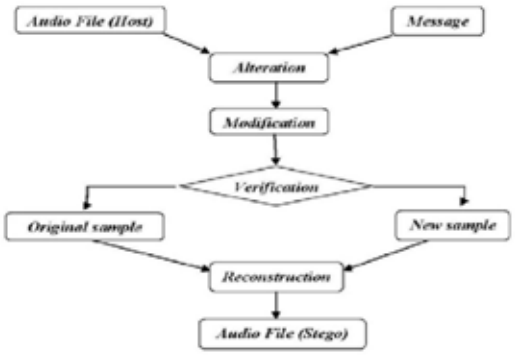

Fig 3 Audio Steganography

IV. LEAST SIGNIFICANT BIT TECHNIQUES

The most widely used technique to hide data, is the usage of the LSB. Although there are several disadvantages to this approach, the relative easiness to implement it, makes it a popular method. To hide a secret message inside a image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm.

When using a 24 bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. Thus, a 800 × 600 pixel image can contain a total amount of 1.440.000 bits (180.000 bytes) of secret data. For example, the following grid can be considered as 3 pixels of a 24 bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

V. DCT (DIRECT COSINE TRANSFORM)

Input: Message, cover image
Output: steganographic image containing message
While data left to embed do Get next DCT coefficient from cover image
If DCT not equal to 0 and DCT not equal to 1 then get next LSB from message
Replace DCT LSB with message bit
End if
Insert DCT into steganographic image
End while

VI. VIDEO STEGANOGRAPHY

The main high resolution AVI fie is nothing but a sequence of high resolution image called frames. Initially I will like to stream the video and collect all the frames in bitmap format (Fig 4). And also collect the following information:

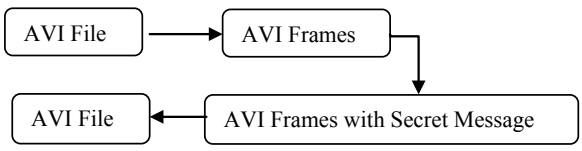

Fig 4 AVI File

VII PROPOSED WORK FOR STEGANOGRAPHY

The main goal of this method is to hide information on the output image of the instrument (such as image displayed by an electronic advertising billboard). This method can be used for announcing a secret message in a public place. In general, this method is a kind of steganography, but it is done in real time on the output of a device such as electronic billboard. Following are the steps involved in embedding the secret information within a cover media

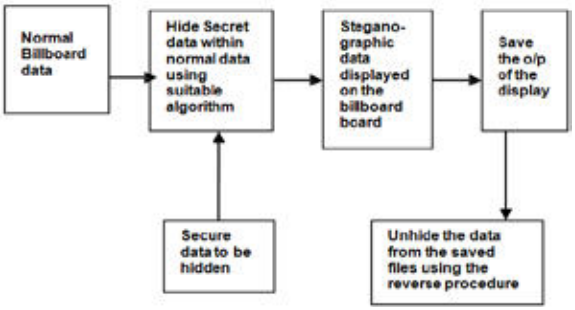

Fig 5 Block Diagram of Proposed idea

Description of the algorithm for embedding the secret message:
Algorithm for embedding the secret message is as follows:

A) Read the image from the source.
B) Divide the image into [R x C] smaller blocks .Where R & C are the first & second bytes of the key respectively [Fig 6].
C) Each smaller block is a combination of many pixels of different values.
D) The LSBs of the pixel are changed depending on the pattern bits and the secret message bits.
E) The pattern bits are considered in sequence form its MSB.
F) If the pattern bit is 0, then the first LSB of the pixel is changed [i.e. if data bit is 1 and pixel bit is 0 ,then pixel bit is changed to1 or else it is retained as it is.
G) If the pattern bit is 1, then the second LSB of the pixel is changed accordingly.
H) A single bit of the secret message is distributed throughout the block. This is done to have enough information so that correct information can be retrieved after decoding
I) similarly the other bits are inserted in the remaining blocks.
J) If the length of the secret message is large, then it can be divided and stored in two or three frames.
k) To extract the information, operations contrary to the ones carried out in embedding are performed.

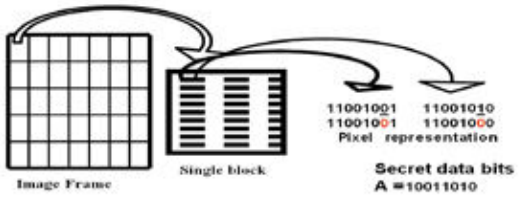

Fig 6 Bit Representation

CONCLUSION

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Digital image steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly. As with the other great innovations of the digital age: the battle between cryptographers and cryptanalysis, security experts and hackers, record companies and pirates,

steganography and Steganalysis will continually develop new techniques to counter each other. In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking.

REFERENCES

[1] Mohammad Shirali-Shahreza, "A new method for real time steganography",ICSP 2006 Proceedings of IEEE . [2]Yuk Ying Chung, fang Fei Xu, "Development of video watermarking for MPEG2 video" City university of Hong Kong ,IEEE 2006. [3] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, "Steganography and digital watermarking" School of Computer Science, The University of Birmingham. 2003. | www.cs.unibo.it/people/phdstudents/scacciag/home_files/teach/datahide.pdf [4] Martín Alvaro, Sapiro Guillermo and Seroussi Gadiel, "Is Image Steganography Natural?" IEEE Transactions On Image Processing, Vol. 14, No. 12, December, 2005 | [5] Cvejic N. and Seppänen T. "Increasing the capacity of LSB based audio steganography", Proc. 5th IEEE International Workshop on Multimedia Signal Processing, St. Thomas, VI, December 2002, pp. 336-338. | [6] Lee, Y. K. and Chen L. H. "High Capacity Image Steganographic Model". IEEE Proceedings Vision, Image and Signal Processing, pp. 288-294, 2000.