A SECURE COMMUNICATION THROUGH STEGNOGRAPHY

B. Vivek Vardhan

B.Tech Student, Dept of CSE, CMR Technical Campus, Hyderabad, T.S. India

ABSTRACT

Many techniques are used to hide data in various formats in stegnography. The most widely used mechanism on account of its simplicity is the use of Least Significant Bit. LSB is normally used to hide data in a digital image. The other bits may be used but it is highly likely that image would be distorted. This paper discusses the art and science of stegnography in general and proposes new technique to hide data in an image using the concept of LSB.

Index Terms *– Stegnography, data hiding, digital images.*

1.INTRODUCTION AND BACKGROUND

The word Steganography literally means covered writing as derived from Greek and includes a vast array of methods of secret communications that conceal the very existence of the message. THE `PERCEPTION MANAGERS' and their `patriotic' paparazzi of the West seem to have shifted gears from singing paeans of technology to sowing suspicions about its possible misuse by the Al Queada, Taliban and their ilk! The word `Steganography' should henceforth be bandied about more for its sinister implications on the security of the civilised world. In June this year, USA Today reported that the encrypted blueprints of the next terrorist attack on the U.S. and its allies may lie hidden behind the X-rated pictures on several pornographic web sites and the posted comments on sports chat rooms.

A snake makes itself invisible in a bed of grass by natural subterfuge. For all visible signs one sees just a stretch of grass but not the snake hiding beneath. The word Steganography literally means covered writing as derived from Greek. It includes a vast array of methods of secret communications that conceal the very existence of the message. Invisible inks, microdots, character arrangement, digital signatures, covert channels and spread-spectrum communications and other artifacts of day-to-day use in communications have thus been converted into potent tools of Steganography.

As with other simple and casual things, Internet and the web have added to the might of such simple procedures. Bits and bytes have provided a powerful medium for the exchange such masqueraded messages in an unlimited and anonymous environment. Software like White Noise Storm and S- Tools can use the `least significant' bits of any digitised file to hold covert information, without changing it in any manner perceptible to the human sensory organs of sight or hearing as the case may be.

So far paranoid privacy advocates have touted Steganography, albeit openly for communication without the powers that be breathing down your shoulders.It has been quite common to hide copyright messages behind digitised files so that it may be used in civil disputes. Software professionals found another tool in Steganography apart from `Easter Eggs' to record their contributions to a software product, when they were afraid that their employers might not give them title credits.

Protection:

With Steganography `Stego Analysis' is the natural offshoot. Stego Analysis provides means to detect and destroy steganographic messages. Any image can be manipulated with the intent of destroying some hidden information whether an embedded message exists or not. However, they suggest that detection should precede destruction to target such hidden messages, which are not just innocuous copyright or ownership related info (known as `digital watermarks'). Detection may also save wasted effort Steganography and cryptography

Steganography is different from cryptography. Cryptography uses encryption to change the contents of digitised files using some known algorithm into something totally different. The same algorithm can be used to restore it to its original form. Steganography does not alter the message in any way. It simply hides it. To make detection almost impossible, encrypted messages can be hidden using Steganography.

Example: Dead drops

`Dead drop' is a Cold War-era slang connoting a place where spies left information. Cops and security experts feel that the Internet provides virtually limitless supply of `dead drops'. Officials and experts say the messages scrambled using free encryption programs set up by groups that advocate privacy on the Internet are hidden in an existing images on selected web sites. The e-mails and images can only be decrypted using a `private key' or code, selected by the recipient. Thus you very well could have a photograph and image with the time and information of an attack, say on an International airport, sitting on your computer, and you would never know it! Unlike the good old `dead drop' the Internet, is proving to be a much more secure way to conduct clandestine warfare.

2. PROPOSED SYSTEM

The system deals with security during transmission of data. Commonly used technologies are cryptography. This system deals with implementing security using steganography.In this the end user identifies an image which is going to act as the carrier of data. The data file is also selected and then to achieve greater speed of transmission the data file and image file are compressed and sent. Prior to this the data is embedded into the image and then sent.

The image if hacked or interpretted by a third party user will open up in any image previewer but not displaying the data. This protects the data from being visible and hence be secure during transmission.

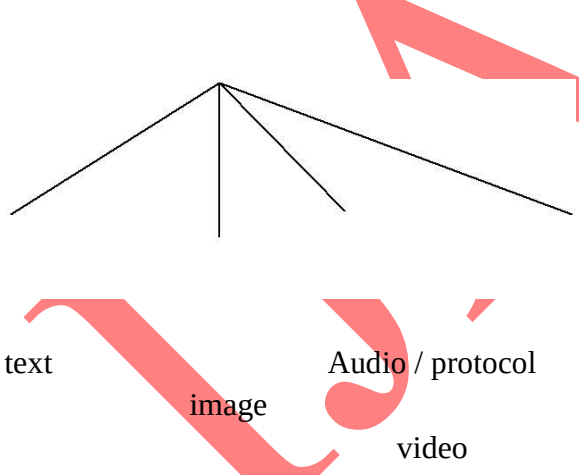
The user in the receiving end uses another piece of code to retrieve the data from the image.

3.USES OF STEGNOGRAPHY

Stegnography can send messages without anyone having knowledge of the existence of the communication. Stegnography can be a tool which makes it possible to send news and information without being censored and without the fear of messages being intercepted and traced back to you. We can use stegnography to store information on a location. Stegnography can also be used to implement water marking.

4.TYPES OF STEGNOGRAPHY

All digital file formats can be used for stegnography but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use an display. The redundant bits of an objects are those bits that can be altered without the alteration being detected easily. Image and audio files comply with these requirements.



Hiding information in text is historically the most important method of stegnography. The obvious method was to hide a secret message in every nth letter of every word of a text message. The digital images have large amount of redundant bits in the digital representation of an image, images are the most popular cover objects for stegnography. In audio files the same techniques are used as for image files. Audio files use a new technique called masking which exploits the properties of human ear to hide information unnoticeably.

Protocol stegnography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model

their exists covert channels where stegnography can be used. Eg. Header of TCP/IP packet.

One major drawback of stegnography is one can hide only little information in the media selected.

5. IMAGE CONSTRUCTION

An image is a collection of numbers that constitute different light intensities in different areas of image. This numeric representation forms a grid and the individual points are referred to as pixels. The number of bits in a color scheme called the bit depth refers to the number of bits used for each pixel. The images can be of 8 bits and 24 bits. In GIF image size of each pixel is 8 bits. In this format the colors are represented from most used to least used colors. The images with 256 colors and pixel value of 640*480 size whereas a high resolution image of 24 bits may have size larger than 2 megabits. Although larger size file facilitates larger amount of data to be hidden but transferring large size on the internet can cause suspicious as well as require more bandwidth. There are different types of image compression techniques – lossy and lossless compression techniques. JPEG is an example of lossy compression. Its advantage is that it saves more space so it looses its originality. GIF, BMP are examples of lossless compression.

Any image consists of three colors RGB. Each color of a pixel consists of a byte or 8 bits and carries certain information. As information is stored in LSB so,it doesn't affect the quality of the picture. The whole message is embedded in the image in this and results have shown hardly any degradation in the picture quality.

6. IMPLEMENTATION

The mostly 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. To hide a secret message inside a image a proper cover image is needed as this method uses bits of each pixel in the image and we should use a lossless compression format.

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 800X600 pixel image can contain a total amount of 1.440.000 bits of secret data. Eg., the following grid is 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, inserted the following grid results:

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

In this case only 3 bits needed to be changed to insert the characters successfully. On average only half of the bits in an image will need to modified to hide a secret message using the maximal cover size. The resulting changes that are made to the LSBs are too small to be recognized by the human eye, so the message is effectively hidden.

Disadvantages of using LSB alteration, are mainly in the fact that it requires a fairly large cover image to create a usable amount of hiding space. Another disadvantage occurs when compressing an image concealing a secret using lossy compression algorithm, the hidden will not survive this operation and is lost after the transformation.

7. STEGNOGRAPHYVs CRYPTOGRAPHY

Many times stegnography is related to cryptography. It may be a misleading statement with respect to a stegnography approach. Stegnography is related to cryptography by meaning that both are used for security purposes with different appraoch or implementation. Stegnography is, along with cryptography, a very ancient concept but its application varies according to emerging technologies. Both of these technologies may not be taken as rival to each other but they can play a very important role if these complement each other.

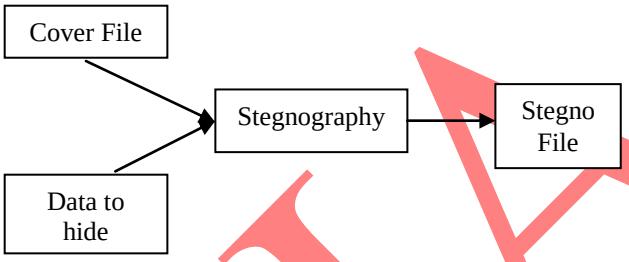


Fig 1: Process of hiding data

7. CONCLUSION

Stegnography is in the initial stage of development. In this paper we just discussed how to hide data in the image using LSB. The importance of stegnography has not been realized to that stage where it is preferred over its close rival “Encryption”. Stegnography when combined with cryptograpnhy becomes a power tool for secure transmission of data.

REFERENCES

1. Krenn, R.”Stegnography and Steg analysis”, http:\\www.krenn.nl/univ/cry/steg/article.pdf
2. Johnson, Neil F., and Sushil Jajodia, “Steg analysis of images created using current stegnographic software”, proceedings of the second information hiding workshop, April 1998.
3. Johnson, Neil F.,and Sushil Jajodia,“Exploring Stegnography: Seeing the unseen”.IEEE computer Feb’ 1998.