A MINI PROJECT REPORT

On

Selenography

Submitted for partial fulfillment of award of

BACHELOR OF TECHNOLOGY
Degree
In
Computer Science & Engineering

By

Nishant kumar vidhuri ***1902250100094***

Under the Guidance of
Paramjeet Kaur
Assistant Professor Department of CSE

DR. A. P. J ABDUL KALAM TECHNICAL UNIVERSITY,
UTTAR PRADESH, LUCKNOW

CERTIFICATE

Certified this students has carried out the Project work presented in this project entitled "COLLEGE REVIEW WEBSITE" for the award of Bachelor of Technology from Dr. A.P.J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow under my supervision. The Project embodies result of original work and studies carried out by Student themselves and the contents of the Project do not form the basis for the award of any other degree to the candidate or to anybody else.

(Paramjeet Kaur)
Assistant Professor
Department of CSE

Date:

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the Report of the Project undertaken during B.Tech Second Year. First and foremost We wish to thank our Guide ***Prof. (Name of Guide) Department of Computer Science and Engineering , AIMT*** *for his kind blessings to us . She allowed us the freedom to explore, while at the same time provided us with invaluable sight without which this Project would not have been possible.*

We also do not like to miss the opportunity to acknowledge the contribution of all faculty members of the Department for their kind assistance and cooperation during the development of our project.

Nishant kumar vidhuri

1902250100094

ABSTRACT

"The Right to privacy…is the most comprehensive of rights and the right most valued by civilized man".

- Justice Louis Brandies, US Supreme Court, 1928.

Steganography (a rough Greek translation of the term Steganography is secret writing) has been used in various forms for 2500 years. Steganography is the art and science of ***hiding information*** *by embedding messages within other, seemingly harmless messages. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer. This paper will explore steganography from its earliest instances through potential future application.*

This paper introduces steganography by explaining what it is, providing a brief history with illustrations of some methods for implementing steganography. Though the forms are many, the focus of the software evaluation in this paper is on the use of images in steganography. We have even discussed various secret communication methods used, its comparison with Cryptography and Digital Watermarking. Finally, future projections on this perfect file encryption technique are made, along with few explanations using our own software and programs.

KEYWORDS*: Cryptography, Watermark, Steganalysis, JPEG, BMP, Encryption, Covert channels, Decryption, Least Significant Bit.*

INTRODUCTION

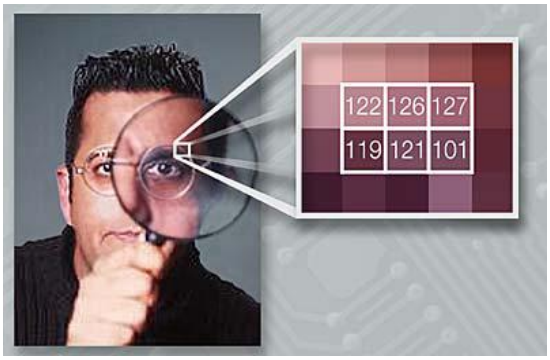
Johannes Trithemius (1462-1516) was a German Abbot. His writing, "Steganographia: hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa" is ostensibly a work describing methods to communicate with spirits. A rough translation of the Latin title is: "Steganography: the art through which writing is hidden requiring recovery by the minds of men." Although people have hidden secrets in plain sight—now called steganography—throughout the ages, the recent growth in computational power and technology has propelled it to the forefront of today's security techniques.

***What is Steganography*:** Steganography literally means covered writing or hidden writing i.e., writing that is known to casual observer, is derived from Greek words 'steganos' meaning covered or secret and 'graphy' meaning writing or drawing. This technique includes all methods of secure and secret communication that conceal the existence of secret message. From the time of Herodotus in Greece till today, Steganography has been used in various places. Today the field attains new dimensions with the advent of digital computer.

When a message is encrypted, it has no meaning, and it's easy to understand that it contains sensitive information, a ***secret*** – and someone might try to break it. Steganography solves this problem by hiding the sensitive information in a harmless file called **carrier** file**.** Steganographic software enables information to be hidden in graphics, sound files. By this technique data can be hidden inside the normal picture without changing its appearance or size. The hidden messages need not be encrypted and it can be in plain everyday English. Recent advances in computing and recent interest in privacy has led to the development of steagnography.

SECRET COMUNICATION METHODS

The secret communications methods are invisible dots, microdots, character arrangement (other than cryptographic methods of permutation and substitution), digital signatures, covert channels and spread-spectrum signals.



Allows the secure transfer of passwords between two computers using an encrypted internet line.

An Application Locker to password protects any application installed on your computer.

Features five innocent carriers for hiding: JPEG, PNG, BMP, HTML and WAV.

It's also notoriously known that there are different ways of hiding writing between the lines of an ordinary letter. The text or picture that you drew would only appear if you colored over the written area with a special marker. In this case a chemical reaction would take place once the two substances touched thus revealing the hidden message.

The common form of invisible writing is through the use of invisible inks whose sources are milk, vinegar, fruit juices and urine. These darken when heated and they are easy to decode. With improvements in technology, many sophisticated inks were developed which react with various chemicals. Some messages had to be 'developed' much as photographs are developed with a number of chemicals in processing labs.

The Germans developed microdot technology during World War II which was referred to as 'the enemy's masterpiece of espionage'. Microdots are photographs, the size of a printed period having the clarity of standard-sized type-written pages. In the USSR all international mailings were screened in attempt to detect any hostile activities.

IMPLEMENTATION OF STEGANOGRAPHY

There are ways to hide information in an image, audio and even text files. Moreover, if that message is in addition encoded then it has one more supplemental level of protection. Computer steganography is based on two principles. The first one is that the files that contain digitized images or sound can be altered to a certain extend without loosing their functionality unlike other types of data that have to be exact in order to function properly, an example of that would be a computer program.

If one step is missed or overlooked you cannot continue the process. The other principle deals with the human inability to distinguish negligible changes in image color or sound quality, which is especially easy to make use of in objects that contain redundant information, be it 16-bit sound, 8-bit or even better 24-bit image. This just meaning that it is very hard to distinguish minor changes in images with the human eye. Speaking of images, changing the value of the least significant bit of the pixel color

Won't result in any perceivable change of that color. One of the best and most widely spread steganographic products for Windows95/98/NT is S-Tools.

Background, Evaluation method and Software evaluation which include S-Tools and Hide and Seek v4.1 are the software packages which were reviewed with respect to Steganographic manipulation of images. A very useful feature is the status line that displays the largest message size that can be stored in the carrier

file. All the softwares uses the LSB method to both images and audio files. Steganography allows you to hide information in five innocent looking files types: JPEG, PNG, BMP, HTML and WAV.

Null ciphers (unencrypted messages) were also used. The real message is "camouflaged" in an innocent sounding message. Due to the "sound" of many open coded messages, the suspect communications were detected by mail filters. However "innocent" messages were allowed to flow through. An example of a message containing such a null cipher is German Spy in World War II:

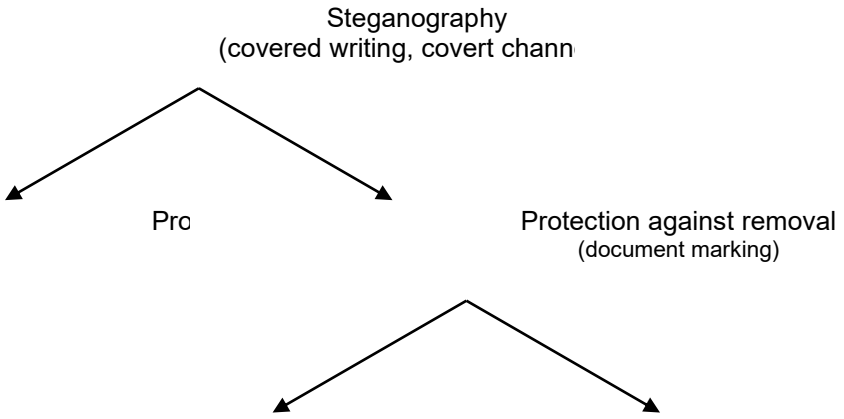
"Apparently *n**e**utral's p**r**otest i**s** t**h**oroughly d**i**scounted*
*And i**g**nored. I**s**man h**a**rd h**i**t. B**l**ockade i**s**sue a**f**fects*
*Pretext f**o**r e**m**bargo o**n** b**y** p**r**oducts, e**j**ecting s**u**ets a**n**d*
*Vegetable o**i**ls.*"

Taking the second letter in each word the following message emerges:

Pershing sails from NY June 1.

TYPES OF STEGANOGRAPHY

Steganography can be split into two types, these are Fragile and Robust. The following section describes the definition of these two different types of steganography.

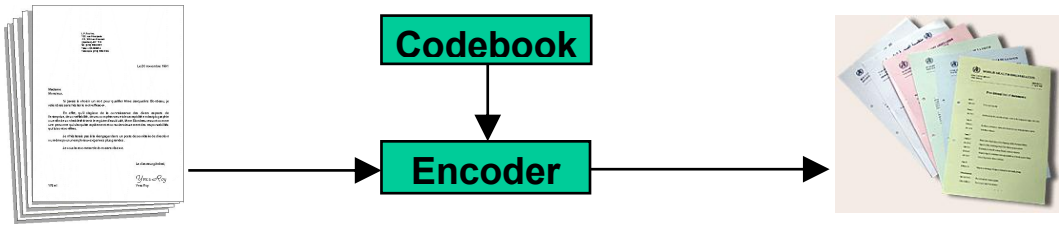


- *Fragile* – Fragile steganography involves embedding information into a file which is destroyed if the file is modified. This method is unsuitable for recording the copyright holder of the file since it can be so easily removed, but is useful in situations where it is important to prove that the file has not been tampered with, such as using a file as evidence in a court of law, since any tampering would have removed the watermark. Fragile steganography techniques tend to be easier to implement than robust methods.
- *Robust* – Robust marking aims to embed information into a file which cannot easily be destroyed. Although no mark is truly indestructible, a system can be considered robust if the amount of changes

required to remove the mark would render the file useless. There are two main types of robust marking: Fingerprinting and Water marking.

Text Techniques

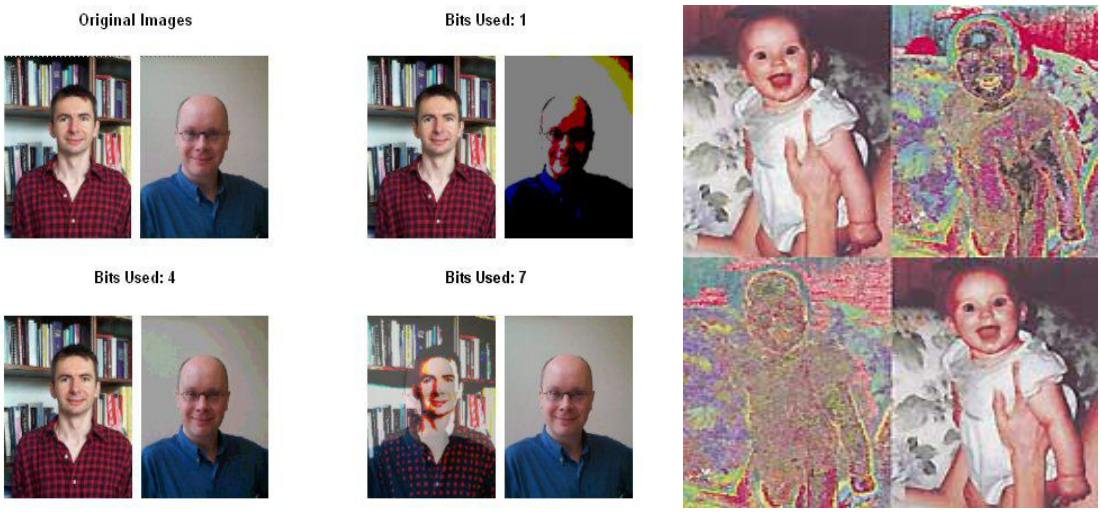
Hiding information is to conceal it in what seems to be inconspicuous text. It is more difficult when it comes to electronic versions of text. Copies are identical and it is impossible to tell if it is an original or a copied version. To embed information inside a document we can simply alter some of its characteristics. These can be either the text formatting or characteristics of the characters. The key to this problem is that we alter the document in a way that it is simply not visible to the human eye yet it is possible to decode it by computer. Figure shows the general principle in embedding hidden information inside a document.



Again, there is an encoder and to decode it, there will be a decoder. The codebook is a set of rules that tells the encoder which parts of the document it needs to change. It is also worth pointing out that the marked documents can be either identical or different. By different, we mean that the same watermark is marked on the document but different characteristics of each of the documents are changed.

Image Techniques

- *LSB – Least Significant Bit Hiding (Image Hiding)* –This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another.



(i) First load up both the host image and the image you need to hide.

(ii) Next chose the number of bits you wish to hide the secret image in. The more bits used in the host image, the more it deteriorates. Increasing the number of bits used though obviously has a beneficial reaction on the secret image increasing its clarity.

(iii) Now you have to create a new image by combining the pixels from both images. If you decide for example, to use 4 bits to hide the secret image, there will be four bits left

for the host image.

Host Pixel: 10110001

Secret Pixel: 00111111

New Image Pixel: **10110011**

(iv) To get the original image back you just need to know how many bits were used to store the secret image. You then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change - the bits extracted now become the most significant bits.

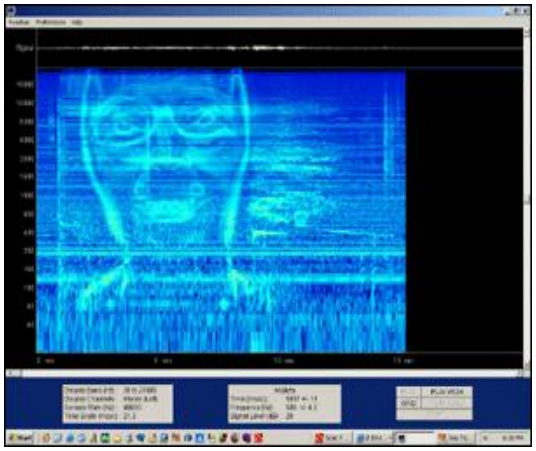
Host Pixel: 10110011

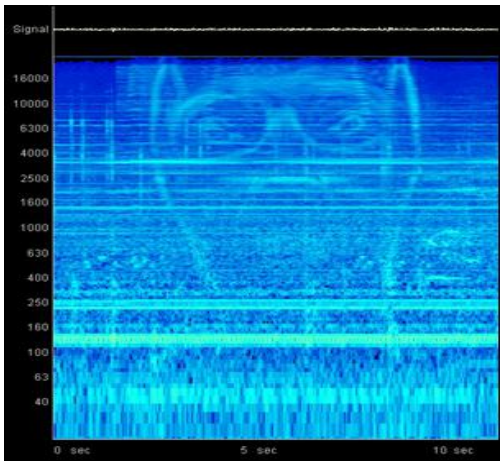
Bits used: 4

New Image: **00110000**

Audio Techniques

- *Spread Spectrum* — spread spectrum systems encode data as a binary sequence which sounds like noise but which can be recognised by a receiver with the correct key.
- *MIDI* — MIDI files are good places to hide information due to the revival this format has had with the surge of mobile phones, which play MIDI ring tones.
- *MP3* — The MP3 format is probably the most widespread compression format currently used for music files. Due to this, it also happens to be very good for hiding information in. The more inconspicuous the format, the more easily the hidden data may be overlooked.





- *Video* — For video, a combination of sound and image techniques can be used. This is due to the fact that video generally has separate inner files for the video (consisting of many images) and the sound. So techniques can be applied in both areas to hide data. Due to the size of video files, the scope for adding lots of data is much greater and therefore the chances of hidden data being detected is quite low.

Limitations

There are limitations on the use of steganography due to the size of the medium being used to hide the data. In order for steganography to be useful the message should be hidden without any major changes to the object it is being embedded in. This leaves limited room to embed a message without noticeably changing the original object. This is most obvious in compressed files where many of the obvious candidates for embedding data are lost. Detecting hidden data remains an active area of research. How do you protect against malicious Steganography?

Unfortunately, all of the methods mentioned above can also be used to hide illicit, unauthorized or unwanted activity. What can be done to prevent or detect issues with steganography? Other uses for steganography range from the trivial to the abhorrent, including Criminal communications, Fraud, Hacking, Electronic payments, Gambling, pornography, Harassment, Intellectual property offenses ,Viruses, Pedophilia.

Advantages

Attempting to detect the use of steganography is called **Steganalysis** (the task of detecting and possibly disabling steganographic information) and can be either passive, where the presence of the hidden data is detected, or active, where an attempt is made to retrieve the hidden data it is not infallible. But it considerably **increases the work of any experienced code-breaker**, who must identify first the right carrier, extract the sensitive data from it, and only after that (if he gets this far) – the hard work of breaking the code. Today, less painful but more cryptic methods could be used to hide information in publicly

available web site images. The image is visibly indiscernible even to a trained eye. The only hope is to enlist science to see past the pixels, but is this possible?

Hides your sensitive data into innocent files, so nobody can find them.

STEGANOGRAPHY vs CRYPTOGRAPHY

Cryptography

(i) Message is not hidden.

(ii) Enemy can intercept the message.

(iii) Enemy can decrypt the message.

Steganography

(i) Message is hidden.

(ii) Enemy must discover the medium.

File encryption is based on encryption algorithms - a process capable of translating data into a secret code. In Cryptography, encrypted message is sent. If it is intercepted, the interceptor knows that the text is an encrypted message. In Steganography, the fact that the message is being sent is unknown. So, the interceptor may not know the object contains a message. Steganography is not intended to replace Cryptography but supplement it, Cryptography + Steganography = Secured Steganography.

STEGANOGRAPHY vs DIGITAL WATERMARK

Digital watermark

Digital watermarks are employed in an attempt to provide proof of ownership and identify illicit copying and distribution of multimedia information. The role of digital watermarking as a means of aiding in copyright and ownership issues. Alternatives to digital watermarking techniques are explored as countermeasures to distortion attacks against carrier. Despite, Steganography may have nothing to do with the cover which is the object of communication.

CONCLUSION

Steganography is a dynamic tool with a long history and the capability to adapt to new levels of technology. It has its own place in computer data security. By the amount of free and commercial tools available today, one can deduce that the use of steganography is growing. Steganography is just another tool for someone to use to hide data, and I believe it will be used more often in the future, whether for

covert communication or personal data concealment. Security professionals will surely need to be aware of its existence as its use becomes more prevalent. Hiding a message with steganography methods reduces the chance of a message being detected. In and of itself, steganography is not a good solution to secrecy, but neither is simple substitution and short block permutation for encryption. But if these methods are combined, you have much stronger encryption routines. Like any tool, steganography is neither inherently good nor evil, it is the manner in which it is used which will determine whether it is a
benefit or a detriment to our society.

REFERENCES

http://www.jjtc.com

http://www.stegoarchive.com

http://www.forensics.nl/steganography