International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

# Steganography & tools used for Steganography

**Manisha Saini, Gaurav Saini**

**Abstract**— Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography is not only valid for images but it is valid for any digital media such as images, audio files, video files, and text files etc.This paper discusses the concepts behind steganography by exploring firstly what it is and how it has been used throughout in various aspects and Basics of Modern Steganography. This is followed by technical discussions on how it works and what methods and tools are used in stegnography. The paper explores the relationship with cryptography and how the two technologies differ. Finally, the future scope & conclusion presents 'The Right Way' to use steganography as a means of concealing information and the pitfalls to be wary of by outlining key points to consider when using steganography.

**Index Terms**— cryptography, Spam Mimic, S tool

## 1. INTRODUCTION

### Steganography: What is it?

For a definition of Steganography I will quote Bryan Clair since he has defined it very elegantly:

> "Steganography is the dark cousin of cryptography, the use of codes. While cryptography provides privacy, steganography is intended to provide secrecy. Privacy is what you need when you use your credit card on the Internet -- you don't want your number revealed to the public. For this, you use cryptography, and send a coded pile of gibberish that only the web site can decipher. Though your code may be unbreakable, any hacker can look and see you've sent a message. For true secrecy, you don't want anyone to know you're sending a message at all. To achieve this secrecy, the process of steganography hides data within an image, sound file, movie, for example, so that its existence is hidden from prying eyes"

In this modern era, computers and the internet are major communication media that connect different parts of the world as one global virtual world. As a result, people can easily exchange information and distance is no longer a barrier to communication. However, the safety and security of long-distance communication remains an issue. This is particularly important in the case of confidential data. The need to solve this problem has led to the development of steganography. This term Steganography is derived from two Greek word steganos meaning "covered" and the other word graphie meaning "writing". Even according to the survey terror groups may be using the Internet to pass information using techniques including e-mail, chat rooms, bulletin boards and other web sites. There is also much speculation that these groups may be using technologies like encryption and steganography to help hid their communications Using image files to transfer information is the method that first comes to mind. Many newspapers have reported that "according to nameless 'U.S. officials and experts' and 'U.S. and foreign officials,' terrorist groups are 'hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites." This may sound difficult to do on the surface but in actuality is a simple and effective way to pass information. Another possible scenario is that public auction sites like eBay and Amazon, Jabong etc might be good places to post these files. Imagine that instead of a porno file, a person takes a picture of something they are supposedly selling, say an automobile. He then runs the picture through a stego tool and then posts it to eBay as part of an auction. Millions of people may look at that picture never knowing that it contains plans for a terrorist attack. Only the intended recipient who knows what to look for and downloads the file will receive the real message by running it back through the same stego tool. The vast size of the Internet is also a great boon for those trying to hide information.Terrorists could also have cell members working in major corporations, or at Web hosting providers, that have access to those company's web sites. It is not inconceivable that a graphic image on a company's web site could contain terrorist information totally without that company's knowledge. The possibilities are endless for hiding information within images on the Internet. Image files are not the only medium that steganography techniques could use to transfer information. Audio files like WAV,

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

MID, AU, and MP3 are also ideal carriers and are nearly as ubiquitous on the Web as are image files. There are almost as many steganography tools for audio files as there are for image files and they are just as easy to use.One major factor in steganography is that it relies on the fact that a person does not know that a picture or a sound file or a block of text actually contains hidden information. It is a much more effective means of protecting information if the attacker (unintended or unauthorised recipient of information) does not know that the material presented before them actually contains hidden information. Another benefit of the audio format of carrier files is that it can easily be hand carried to make finding its transmission even more difficult. Data could easily be hidden in MP3 files and then transferred to an MP3 player and carried by a terrorist to various locations. These MP3 devices have become so popular that if someone were stopped and such a player were found in their possession, it would raise no suspicion and would probably not be investigated further. The same holds true for WAV files. These could be burned onto a CD and a music CD would raise much less suspicion that would a CD filled with images. While using steganography may seem an ideal way for terrorists to hide information, it is far from perfect. According to many researchers the current generation of stego program doesn't really work well. Most of the programs leave some sort of fingerprint behind that allows careful observers to know that something is going on. The easiest way to determine whether a file has a stego payload is to be able to compare it to an original. This is probably much easier with audio files where there may be many copies of the same file without a payload for comparison. Image files often prove much more difficult as access to the original is often not possible and another problem with locating stego files is the size of the payload file. The smaller the payload file, the harder it is to find. For instance, a one bit, "yes" or "no" message embedded in an MP3 file would be nearly impossible to find. And another method could be Histogram analysis can be used to possibly identify a file with a hidden message. By comparing histograms, we can see this histogram has a very noticeable repetitive trend

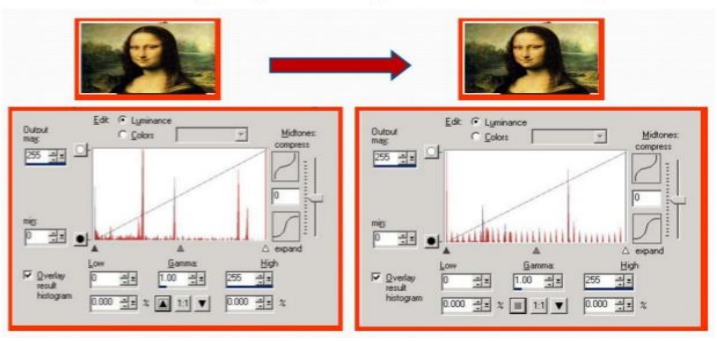


Fig1.Histogram analysis

**2. Basics of Modern Steganography**

The model for steganography is as shown in Figure 1.The cover object is a carrier or medium to embed a message. There are several suitable medium that can be used as cover-objects such as network protocols, audio, file and disk, a text file and an image file Message is the data that the sender wishes to keep confidential and will be embedded into the cover-object by using a stegosystem encoder. It can be a plain text, a ciphertext, an image, or anything that can be embedded in a bit stream such as a copyright mark or a serial number. A Stego-key is a password, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-object. The output of the stegosystem encoder is known as the stego-object. A stegosystem encoder can be represented by using the following relation

$I' = f(I, m, k)$ …… (1)

Where, I' is the stego-object

I is the cover-object

m is the message

k is the stego-key

Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message

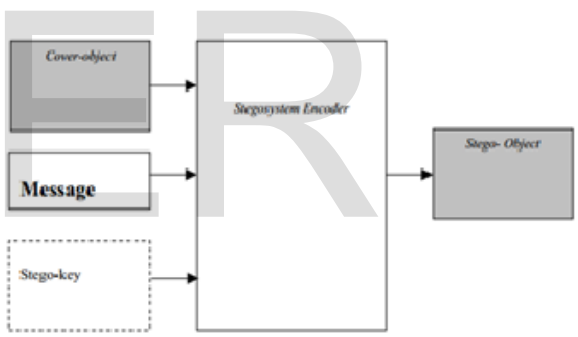



Fig2 Basic Model of steganography

**EXAMPLE**

For example, suppose there is some image given to you with some hidden message and this image is send from sender to receiver .and receiver need secrete key .the key which is only known to sender and receiver. We say there is some message hidden inside the image .if receiver give correct key then only message will appear to receiver. As shown in figure the hidden message in associated with the image is" My hidden message". It's possible that terrorist cells may use it to secretly communicate information. This is rumored to be a common technique used by Al-Qaeda. By posting the image on a website for download by another terrorist cell. Using the same Steganography program, the terrorist cell could then reveal the message with plans for a new attack. It's also a very good Anti-forensics mechanism to mitigate the effectiveness of a forensics investigation as used in Child pornography. Like this in same way we can have embed data into audio files such as songs and even possible in case of text files.

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

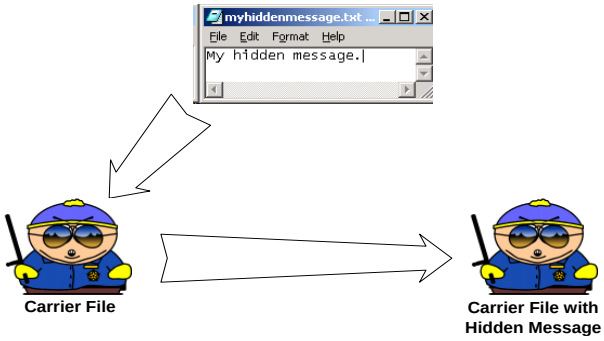



Fig3.Example of steganography

### 3. Tools used for steganoraphy

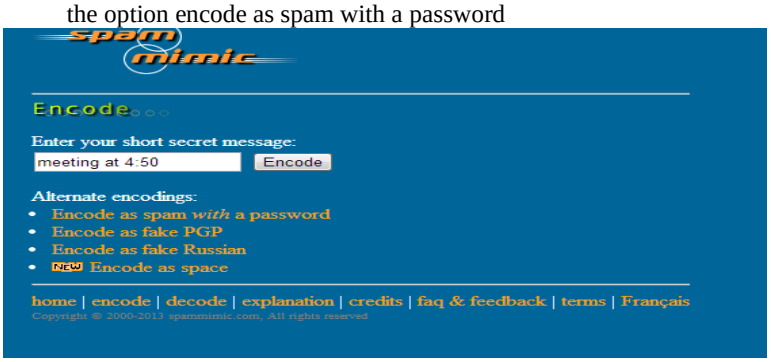
Various tools are there for Steganoraphy such as S-tool, Steganos, Steg Hide, JP hide, Hiderman etc. Some of the specific stegnography tools are used such as:-

- JSteg, JPHide and OutGuess are popular tools that hide messages in JPEG image files
- The program Mandel Steg hides information inside Mandelbrot fractal images
- general method of using images for secure communication is found in S-Tools hides information in both images and audio
- Mp3stego is a popular steganography tool using mp3 files.
- The program wbStego hides information in PDF documents
- Some tools use steganography for applications other than communication. DriveCrypt/ ScramDisk allows virtual disks to be hidden in WAV files
- StegFS is a steganographic file system for Linux. Both of these programs conceal the existence of information on a computer (ideal for hiding cryptographic keys).
- SpamMimic is a popular steganography tool that allows users to hide information inside spam messages.

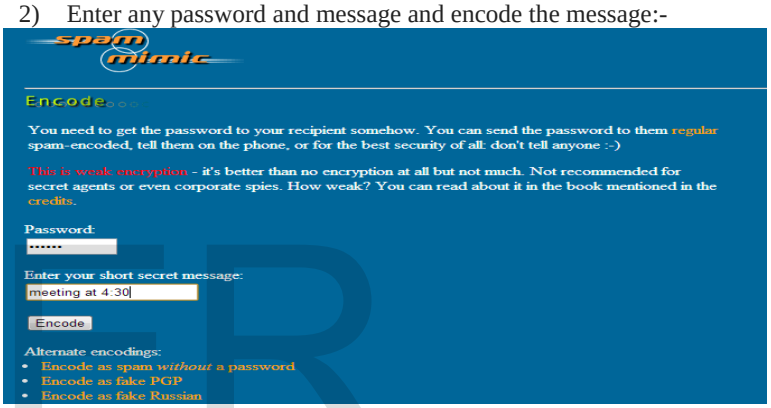
Exact working of one of the steganography tool not based on algorithm is shown here-

Spam Mimic is a web based application that will take your secret message and encode it into a spam message that looks a lot like a lot of other spam messages floating around the Internet. It also has an encryption option whereby you can supply a password and it will encrypt your secret message before encoding. I visited the website at www.spammimic.com and the following is the result:

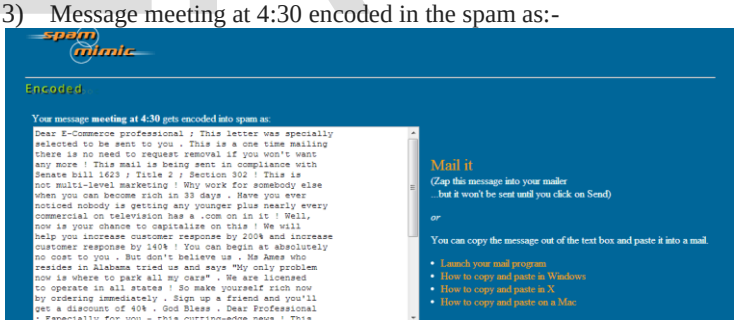
1) Enter a short message suppose meeting at 4:30 and click on the option encode as spam with a password



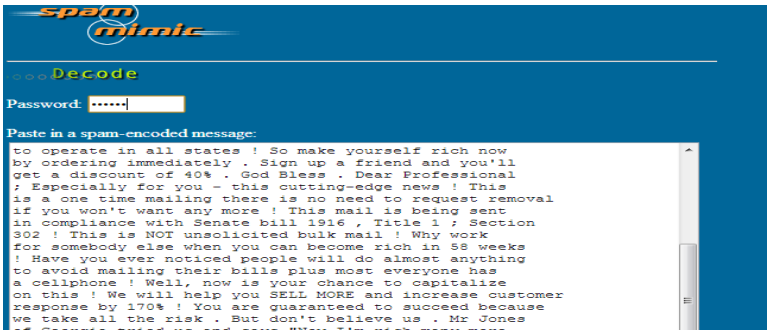

2) Enter any password and message and encode the message:-




3) Message meeting at 4:30 encoded in the spam as:-

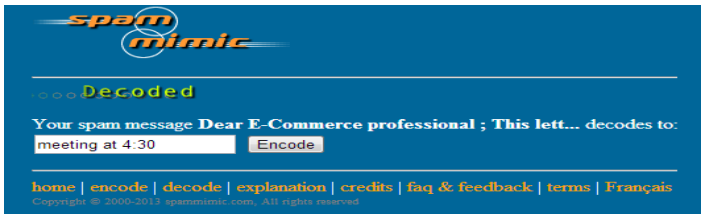



4) To decode the message enter the password and then paste the spam encoded message



International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

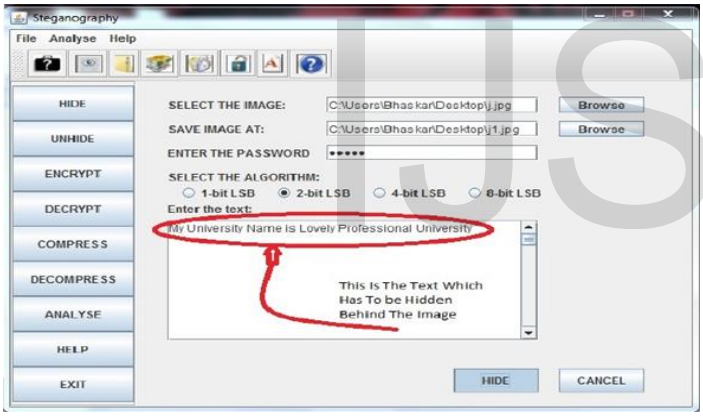
5) Message meeting at 4:30 is decoded




Spam Mimic is also one example of a Null Cipher. Null Ciphers are a way to hide a message within another message without the use of complicated algorithms.

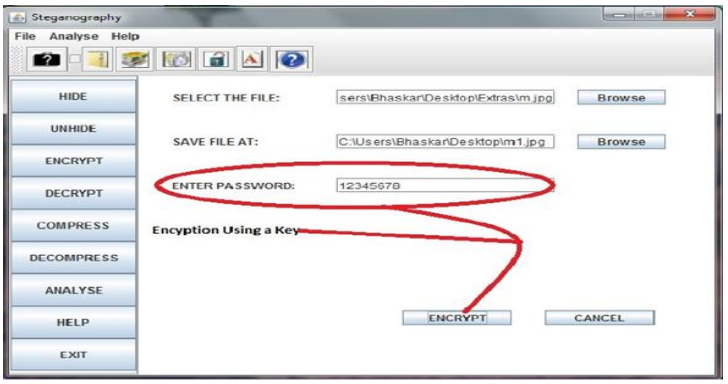
Exact working of another steganography tool based on algorithm is shown here:-

1.hidding( we will select the image from the particular location, give the path where image is stored and then enter the key or password and select the algorithm here as shown in fig we have selected 2 bit LSD then type the message you want to hide behind the image )

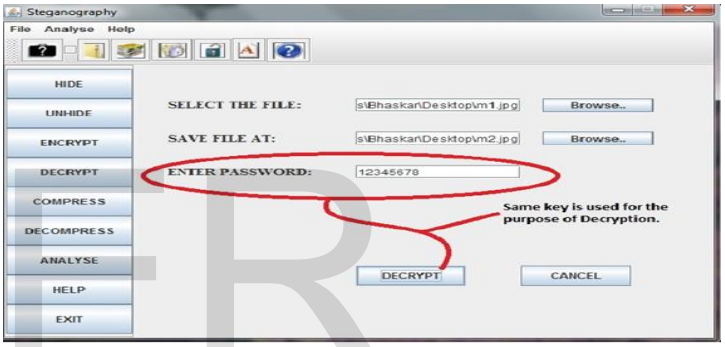



2. Hiding –message (once you have clicked the hide option then dialog box appear showing message that "congratulations your text is hidden")

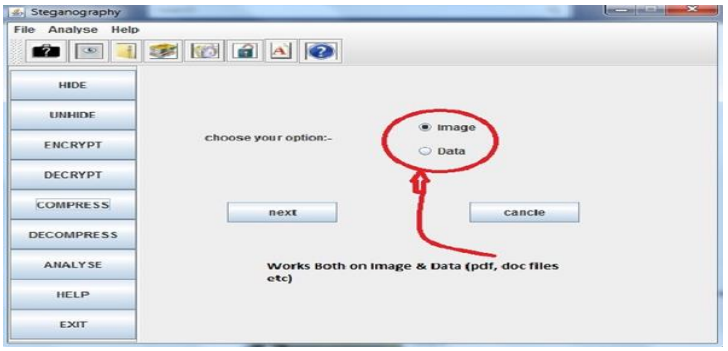

3. Encryption (sender can encrypt the text by entering the password which only the sender and receiver are aware)




4. Decryption(reciver can decrypt the text behind the message by giving the correct key or passward)




5. compress/decompress (you can get the message stored behind the image. Terrorist can use this technique to hide their planning, terrorist attack and weapon making strategy easily behind the image)




**4. Future Scope**

In the future, digital camera manufacturers could implement steganographic features as a part of camera firmware to annotate pictures with the photographer's copyright information. Camcorder manufacturers could also follow suit and implement steganography and watermarking techniques for protecting video content captured on camcorders and video cameras. Going forward, legitimate applications such as tagging of multimedia content with hidden

International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January-2014
ISSN 2229-5518

information could become an important application area for steganography**.** One of the drawbacks is during sending and receiving information can be spoofed. Another limitation could be as the confidentiality of information is maintained by the algorithm ,and if the algorithm are known then its all over .There could be another limitation as the software can be misused if it goes in wrongs hands ie.people with wrong intentions and Sometimes editing or compressing the picture do catastrophic damage to the hidden information. Sender and receiver must agree on a method in which to hide the message.

And sometimes Adding hidden data adds random noise, so it follows that a properly tuned noise detection algorithm could recognize whether or not a picture had steganographic data or not. The downside usually includes things like size and protection. You usually have to send much more padding around your secret text so that your secret text doesn't stand out. If you're only sending something simple like GPS coordinates or an email address, that's fine. But if you have a long document (e.g., a book) that you want to hide with steganography, it's pretty hard. And then there's the protection factor: typically secrets that are protected by steganography are not protected by anything else. If no one sees it, it's safe. If they see it, though, it's game over. In future stenography technique should be prepared to overcome this problem.

## 5. CONCLUSION

Steganography certainly has some beneficial advantages. It is an effective tool for protecting personal information, and organizations are spending a lot of energy and time in analyzing steganography techniques to protect their integrity. However, steganography can also be detrimental. It is hindering law enforcement authorities in gathering evidence to stop illegal activities, because these techniques of hiding information are becoming more sophisticated. Its use on the Internet is certainly promising. That is why law enforcement authorities must continually stay abreast of this technology, because there will always be some new program to hinder their efforts. This increased is evidenced in the sheer number of available tools to provide easy steganographic techniques to the end users.

## 6. REFERENCES

[1] IEEE Explore research paper -AN OVERVIEW OF IMAGE STEGANOGRAPHY - Martin S Olivier

**[2]Wikipedia** Source(s):
http://en.wikipedia.org/wiki/Steganograp…

[3] Research paper on Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned

[4] http://stega.maxant.co.uk/

[5] ) SANS Security Essentials, A Detailed look of Steganographic Techniques and their use in an Open-Systems Environment by By: Bret Dunbar

[6] http://www.slideshare.net/bhaskarnarula/steganography

[7] http://www.spammimic.com/

[8] http://www.outguess.org/