ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 6, June 2016

DATA HIDING TECHNIQUES BY STEGNOGRAPHY

Jyoti

M.Tech Student
School of Engineering & Sciences, B P S Mahila Vishwavidayalaya, Sonipat Haryana

----------***Abstract***----------

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. It also attempts to identify the requirements of a good steganographical go rithmand briefly reflectson which steganographic techniques are more suitable for which applications.

Index Terms: Steganography; Steganalysis; Hide & Seek; Watermarking; Compression

---

INTRODUCTION

Steganography is the art and science of invisible communication. This is a complished through hiding in formation in other information, thus hiding the existence of the communicated in formation. The word steganography is derived from the Greek words“ stegos” meaning “cover” steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography.

Different kinds of Steganography

2.1 Image definition

An image is a collection of numbers that constituted if ferent light in tensitiesin different are as of the image.This numeric representation for msagridand the individual points are referred to as pixels. These pixels are displayed horizontally row by row. The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current colors chemesis8, meaning that there are 8bits used to describe the color of each pixel.

2.2 Image compression

When working with larger images of greater bit depth, the images tend to become too large to transmit over a standard Internet connection. In order to display an image in are a son able amount of time, techniques must be in corporate to reduce the image’s file size. These techniques make use of mathematical formulas to analyse and condense image data,

resulting in smaller file sizes. This process is called compression

There are two types of compression:
lossy and lossless
Lossy compression- creates smaller files by discard in gexcess image data from the original image. It removes details that are too small for the human eye to differentiate, resulting in close approximation soft he original image, although not an exact duplicate. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group).
Lossless compression- on the other hand, never removes any information from the original image, but instead represents data in mathematical formulas. The original image's integrity is maintained and the decompressed image output is bit-by-bit identical to the original image input.

2.3 Image and Transform Domain

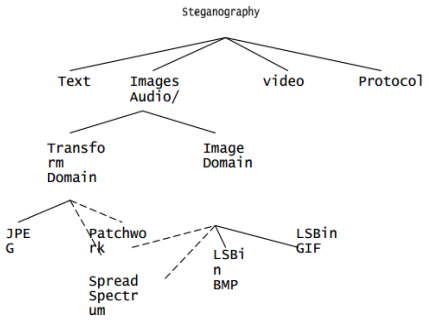


Figure 1: categories of image stegonography

3. Image Domain

• Least Significant Bit

The least significant bit (in other words, the 8 th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. For example a grid for 3pixel sofa 24-bit image can be as follows:

(0010110 00011100 1101110

(1101001 10101101 0110001

(1101001 10101101 0110001

When the number 200, which binary represent at ion is 11001000, is embed ded into the least significant bits of this part of the image, the resulting grid is as follows:

3.1 Transform Domain

The steganographyal gorithms that can be used when embedding data in the transform domain, one must first explain the type of file format connected with this domain. The JPEG file form atist he most popular image file for maton the Internet, because of the small size of the images.

3.2 Image or Transform Domain

steganographical gorithms can either becategorizedas being in the image domainor in the transform domain depending on the implementation.

• Patchwork

Patchwork is a statistical technique that uses redundant pattern encoding to embed a message in an image. The algorithm addsredundancy to the hidden information and then scatters it through out the image. A pseudorandom generator is used to select two are a sof the image (or patches), patch A and patch B

Disadvantage- A disadvantage of the patch work approach is that only one bit is embedded. One can embed more bits by first dividing the image into sub-images and applying the embedding to each of them.

Advantages-The advantage of using this technique is that the secret message is distributed over the entire image, so should one patch bedestroyed , the others mays till survive. The patch work approaches is used in dependent of the host image and prove stobequiter obustas the hidden message can survive conversionbetween lossy and losslesscompression

• Spread Spectrum

In spread spectrum techniques, hidden data is spread through out the cover-image making it hardertodetect In spread spectrum image steganographythe message is embedded in noise and then combined with the cover image to produce the stego image.

Evaluation of different techniques

• Invisibility–

The invisibility of a steganographic algorithmis the first and for emost requirement, since the strength of steganographylie sinitsability to beunnoticed by the human eye. The moment that one can see that an image has been tampered with,the algorithmis compromised

• Payloadcapacity–

Unlike water marking,which need stoembed only a small amount of copyright in formation, steganography aims at hidden communication and there fore requires sufficient embedding capacity.

• Robustness again ststatistical attacks–

Statistical steganaly is the practice f detecting hidden information through applying statistical test son image data. Many steganographical gorithms leave a‘signature’ when embedding information that can beeasily detected through statistical analysis.

• Independentoffileformat-

With many different image file for matsused on the Internet,It might seem suspicious that only one type of file form atiscontinuously communicated between woparties. Them ostpowerful steganographical gorithms thus possess the ability to embedin for mationinany type of file. This alsosolves the problem of not always being able to finda suitable image at the right moment, in the right for matto use as a cover

• Unsuspicious files–

This requirement in cludesall characteristics of a steganographical gorithm that may result in images that is not used normally and may cause suspicion. Abnormal file size,for example, is one property of an image that canresult in further investigation of the image by a warden.

Table 1: Comparison of image steganography algorithms

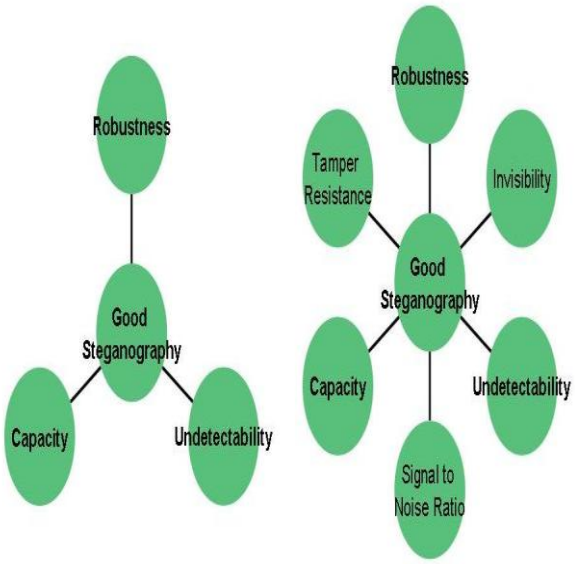
	LSB inBMP	LSB in GIF	JPEG compression	Patchwork	Spread spectrum
Invisibility	High	Medium	High	High	High
Payload capacity	High	Medium	Medium	Low	Medium
Robustnessagai nst statistical	Low	Low	Medium	High	High
Robustnessagainstimaga	Low	Low	Medium	High	Medium
Independent offile format	Low	Low	Low	High	High
Unsuspiciousfiles	Low	Low	High	High	High

USES OF STEGANOGRAPHY

1. Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.

2. It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source.

3. Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data. steganographic methods can be used to hide this.



4. E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by ausername and password, with no real method of verifying that the user is the actual card holder.

5. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them.

The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites.

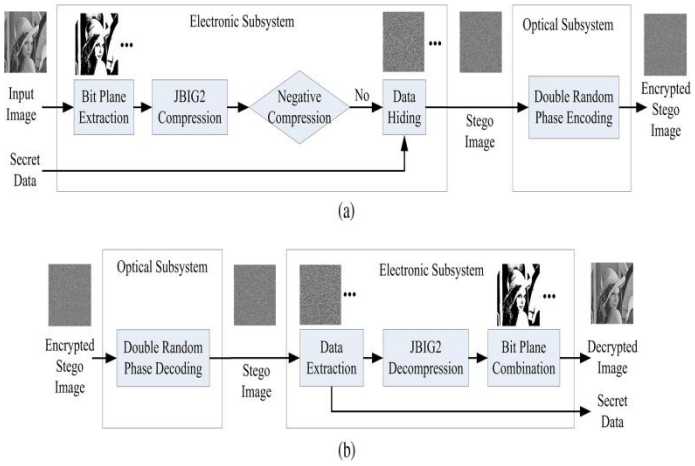


Figure:- Steganography on the Internet

STEGANOGRAPHY AND CRYPTOGRAPHY

DEFINITION & TERMINOLOGY

Cryptography defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker. Cryptosystems are computer systems used to encrypt data for secure transmission and storage.

Any attempt at cryptanalysis is defined as an attack.

Plaintext: is message or data which are in their normal, readable (not crypted) form.

Encryption: Encoding the contents of the message in such a way that hides its contents from outsiders.

Cipher text: Results from plaintext by applying the encryption key.

Decryption: The process of retrieving the plaintext back from the cipher text.

Key: Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key

Steganography: is the method of hiding secret messages in an ordinary document. Steganalysis could be simply defined as the detection of steganography by a third party.

Hash functions: generate a digest of the message. Substitution cipher involves replacing an alphabet with another character of the same alphabet set.

Mono- alphabetic system: uses a single alphabetic set for substitutions.

Poly-alphabetic system: uses multiple alphabetic sets for substitutions.

Caesar cipher: is a mono-alphabetic system in which each character is replaced by the third character in succession. Julius Caesar used this method of encryption

CONCLUSION AND FUTURE SCOPE

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. 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. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate. The possible use of steganography technique is as following:

:-Hiding data on the network in case of a breach.
:-Peer-to-peer private communications.
:-Posting secret communications on the Web to avoid transmission.
:-Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission.

REFERENCES

1. Anderson R.J. and Petitcolas F.A.P., “On the Limits of steganography,” J. Selected Areas in Comm., vol. 16, no.4, 1998, pp. 474–481.
2. Bailey, K. and Curran, K. “An evaluation of image-based steganography methods”. International Journal of Digital Evidence, Fall 2003.
3. Chapman, M. Davida G, and Rennhard M.. “A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography” found online at http://www.nicetext.com/doc/isc01.pdf
4. Dai Y., Liu G., and WangBreaking Z., “Predictive-CodingBased Steganography and Modification for Enhanced Security”, IJCSNS International Journal of Computer Science and Network Security, vol.6 no. 3b, March 2006.
5. Chin-Chen Chang , Iuan-Chang Lin, and Yaun-Hui YU, “ A new Steganographic method for color and gray scale image hiding”, Computer Vision and Image Understanding, 20 December 2006.
6. Shareza Shirali, M.H, “Anew Approach to persain/Arabic Text Stegraphy”, Computer and Information Science, 2006, ICISCOMSAR 2006, 5th IEEE/ACIS International Conference, 10- 12 July 2006 pp 310-315.