IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 8, August 2015.
www.ijiset.com
ISSN 2348 – 7968

Overview Of Image Steganography And Techniques

BOBBY.S
Computer Science ,Periyar University, St.Joseph's College of Arts and Science For Women,
Hosur Tamilnadu,India.
2

Abstract
In the recent years as security of information has become a big concern in this internet era. As involvement of delicate data via a common communication channel has become inevitable, steganography – the art and science of hiding information has enlarged much attention. We are also surrounded by a world of secret communication, Steganography derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing) .Steganography is a technology where modern data compression. There are many ways to hide information inside an image, audio/video, document etc. But Image Steganography has its own advantages and is most popular among the others. This paper is an endeavor to analyse the various techniques used in steganography and to identify areas in which this technique can be applied Image Steganography and a high capacity Image Steganography schemes are discussed for different file formats.

Keywords: Steganography, Secret Communications, Carrier-Image, , Stego-Image.

1. Introduction

The main purpose of Steganography, which means writing in **hiding'** is to hide data in a cover media so that others will not be able to notice it. The cover medium is usually chosen keeping in mind the type and the size of the secret message and many different carrier file formats can be used. In the current situation digital images are the most popular carrier/cover files that can be used to transmit secret information.

Fig 1. Data Hiding Scheme

Steganography equation is 'Stego-medium = Cover medium + Secret message + Stego key'. The embedded data is the message that one requirements to send in secretly. It is usually hidden an harmless message referred to as a cover text or cover-image or cover-audio as appropriate, producing the stego-text or other stego-object. A stego-key is used to control the hiding process so as to restrict detection and /or recovery of the embedded data to parties.

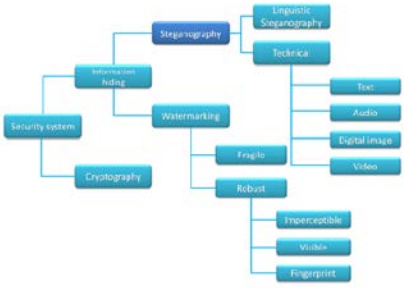

Fig .2. Steganography in security domain

A few key properties that must be considered when creating a digital data hiding system are
• **Imperceptibility:** Imperceptibility is the property in which a person should be unable to distinguish the original and the stego-image.
• **Embedding Capacity:** Refers to the amount of secret Information that can be embedded without degradation of the quality of the image.
• **Robustness:** Refers to the degree of difficulty required to destroy embedded information without destroying the cover image.

2. Overview of Steganography

To provide an overview of steganography, terms and concepts should first be explained. An overview of the different kinds of steganography is given at a later stage.

2.1 Steganography concepts

Even though steganography is an ancient subject, the modern formulation of it is often given in terms of the *prisoner's problem* proposed by Simmons , where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary internment should she suspect any covert communication. The

ISSN 2348 – 7968

warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A *passive* warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An *active* warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information..

2.2 Different kinds of steganography

Almost all digital file formats can be used for steganography, 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 and display The redundant bits of an object are those bits that can be altered without the alteration being detected easily Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.
The four main categories of file formats that can be used for steganography:

- Text
- Images
- Audio/video
- Protocol

Text: Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every n_{th} letter of every word of a text message. It is only since the beginning of the Internet and all the different digital file formats that is has decreased in importance .Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

Image: Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography.

Audio/Video: To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound .This property creates a channel in which to hide information. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images .

Protocol: The term protocol steganography 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 there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

2.3. Image steganography

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats.

2.3.1 Image definition

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image's pixels (represented as bits) where each pixel is located and its colour. These pixels are displayed horizontally row by row.T he number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel .The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel. Monochrome and greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary colour is represented by 8 bits Thus in one given pixel, there can be 256 different quantities of red, green and blue, adding up to more than 16-million combinations, resulting in more than 16-million colours Not surprisingly the larger amount of colours that can be displayed, the larger the file size.

2.3.2 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 a reasonable amount of time, techniques must be incorporated 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.

ISSN 2348 – 7968

In images there are two types of compression: lossy and lossless. Both methods save storage space, but the procedures that they implement differ. Lossy compression creates smaller files by discarding excess image data from the original image. It removes details that are too small for the human eye to differentiate ,resulting in close approximations of the original image, although not an exact duplicate. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group) .

2.3.3 Image and Transform Domain

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image. Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as “simple systems” .The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format .Steganography in the transform domain involves the manipulation of algorithms and image transforms .These methods hide messages in more significant areas of the cover image, making it more robust Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression .

2.3..3.1 Image Domain:

- Least Significant Bit.
- LSB and Palette Based Images.

LSB(Least Significant Bit):

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image .The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.

LSB and Palette Based Images:

GIF images can also be used for LSB steganography, although extra care should be taken. The problem with the palette approach used with GIF images is that should one change the least significant bit of a pixel, it can result in a completely different colour since the index to the colour palette is changed .If adjacent palette entries are similar, there might be little or no noticeable change, but should the adjacent palette entries be very dissimilar, the change would be evident. possible solution is to sort the palette so that the colour differences between consecutive colours are minimized . Another solution is to add new colours which are visually similar to the existing colours in the palette. This requires the original image to have less unique colours than the maximum number of colours (this value depends on the bit depth used) .Using this approach, one should thus carefully choose the right cover image. Unfortunately any tampering with the palette of an indexed image leaves a very clear signature, making it easier to detect.

2.3.3.2 Transform Domain

To understand the steganography algorithms 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 format is the most popular image file format on the Internet, because of the small size of the images.

- JPEG compression.
- JPEG steganography.

JPEG compression:

To compress an image into JPEG format, the RGB colour representation is first converted to a YUV representation. In this representation the Y component corresponds to the luminance (or brightness) and the U and V components stand for chrominance (or colour) .According to research the human eye is more sensitive to changes in the rightness (luminance) of a pixel than to changes in its colour .This fact is exploited by the JPEG compression by down sampling the colour data to reduce the size of the file. The colour components (U and V) are halved in horizontal and vertical directions.

JPEG steganography:

lossy compression which results in parts of the image data being altered. One of the major characteristics of steganography is the fact that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG it was feared that the hidden message would be destroyed. Even if one could somehow keep the message intact it would be difficult to embed the message without the changes being noticeable because of the harsh compression applied. However, properties of the compression algorithm have been exploited in order to develop a steganographic algorithm for JPEGs.

ISSN 2348 – 7968

3. STEGANOGRAPHY TECHNIQUES

3.1. Classification of Stenographic Categories

Steganography is classified into 3 categories,

• Pure steganography where there is no stego key. It is based on the assumption that no other party is aware of the communication.
• Secret key steganography where the stego key is exchanged prior to communication. This is most susceptible to interception.
• Public key steganography where a public key and a private key is used for secure communication.

3.2 Classification of Steganographic Methods

Steganography methods can be classified mainly into six categories, although in some cases exact classification is not possible Steganography Methods Substitution Transform domain Spread spectrum Statistical Distortion Cover generation

• Substitution methods substitute redundant parts of a cover with a secret message (spatial domain).
• Transform domain techniques embed secret information in a transform space of the signal
(frequency domain)
• Spread spectrum techniques adopt ideas from spread spectrum communication.
• Statistical methods encode information by changing several statistical properties of a
cover and use hypothesis testing in the extraction process.
• Distortion techniques store information by signal distortion and measure the deviation from the original cover in the decoding step.
• Cover generation methods encode information in the way a cover for secret communication is created.

3.3 Evaluation of different techniques

The most important requirement are:

Invisibility – The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.

Payload capacity – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore requires sufficient embedding capacity.

Robustness against statistical attacks – Statistical steg analysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a 'signature' when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.

Robustness against image manipulation – In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.
Independent of file format – With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.
Unsuspicious files – This requirement includes all characteristics of a steganographic algorithm that
may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

4. Applications of Steganography

There are various applications in steganography; it varies among the user requirements such as copyright control, covert communication, smart ID's, printers etc.

Copyright Control:

Inside an image, secret copyright information is embedded. This is achieved by Watermarking which is the complex structure. So that the intruder cannot identify the copyright information. There are various methods available to find the watermarking. It is achieved by statistical, correlation, similarity check. watermarking is used to protect the copyright information.

Covert Communication:

In general covert channel passes information by non-standard methods. Communication is obscured that is unnoticed. The aim of the covert communication is to hide the fact that the communication is being occurred. Covert communication ensures privacy. Steganography is one of the best techniques of covert communication.

ISSN 2348 – 7968

Smart Id's:

In smart ID's the information about the person is embedded into their image for confidential information. For an organization, the authentication of the resources is accessed by the people. So identifying the theft related to prevention of crimes.

Printers:

Steganography make use of some modern printers like HP printer etc. In those printers, very small yellow dots are inserted into all pages. Information is hidden inside the yellow dots like serial number, date and time stamp. Property is available in laser printer for watermarking the confidential information.

4. CONCLUSION & FUTURE WORK

In this paper different steganographic articles were studied and were categorized into different techniques. As many new Application areas are identified like internet banking, mobile communication security, cloud security etc., One can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. the insight into the steganographic principles will definitely guide us to identify new areas and to improve its applications in the already existing application areas also.

Acknowledgments

First of all, I am Happy to thank THE GOD ALMIGHTY for giving me the courage in finishing this paper. I would like to thank my family for the constant support they provided throughout my preparation. I am so grateful and appreciative of all those who have helped and supported me in this venture.

References

[1] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*,
[2] Silman, J., "Steganography and Steganalysis: An Overview", *SANS Institute*, 2001
[3] Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 18:01, 1999
[4] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*,
47:10, October 2004
[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", *IEEE Journal of selected Areas in Communications*, May 1998
[6] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", *IEEE Transactionson image processing*, *8:08*, 1999
[7] S.Shanmuga Priya, K .Mahesh and Dr. K.Kuppusamy, (2012) "Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain", International Journal of Engineering Research and Applications,, Vol2, Issue 3, pp. 2632-2637.
[8] B. Sharmila and R.Shanthakumari, (2012) "Efficient Adaptive Steganography For Colour Images Based on LSBMR Algorithm", ICTACT Journal on Image and Video Processing, Vol. 2, Issue:03, pp.387-392.
[9] Shweta Singhal, Dr.Sachin Kumar and Manish Gupta, (2011) "A New Steganography Technique Based on Amendment in Blue Factor ", International Journal of Electronics Communication and Computer Engineering, Vol.2, Issue 1, pp.52-56.
[10] Fahim Irfanet. Al. 's (2011) "An Investigation into Encrypted Message Hiding through Images Using LSB ", International Journal of EST,

Authors Biography

Bobby S was born in Chennai, Tamil Nadu (TN), India, in 1980. She received the Master of Sofware Science (M.Sc) of Software Science degree from the Periyar University, Salem, TN, India, in 2003 and Master of Philosophy (M.Phil) of Computer Science degree from the PU, in 2012. Her research interests include data mining, green computing, computer networks, steganography.