International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 3, pp: (119-125), Month: July - September 2015, Available at: www.researchpublish.com

A Survey of Image Steganography Techniques

Sadaf A. Mulani

Electronics, Shah and Anchor Kuttchi Engineering College, Mumbai, 400088, India

Abstract: **Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message. Generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. Security of confidential information has always been a major issue from the past times to the present time. It has always been the interested topic for researchers to develop secure techniques to send data without revealing it to anyone other than the receiver. Therefore from time to time researchers have developed many techniques to fulfil secure transfer of data and steganography is one of them. 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. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.**

Keywords: **Steganography, Data hiding, Cover writing, Digital image.**

1. INTRODUCTION

With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. One of the groundsdiscussed in information security is the exchange of information through the cover media. To this end, different methods such as cryptography, steganography, coding, etc have been used. The method of steganography is among the methods that have received attention in recent years.[1] The main goal of steganography is to hide information in the other cover media so that other person will not notice the presence of the information. This is a major distinction between this method and the other methods of covert exchange of information because, for example, in cryptography, the individuals notice the information by seeing the coded information but they will not be able to comprehend the information. However, in steganography, the existence of the information in the sources will not be noticed at all. Most steganography jobs have been carried out on images, video clips, texts, music andsounds.Nowadays, using a combination of steganography and the other methods, information security has improved considerably. In addition to being used in the covert exchange of information, steganography is used in other grounds such as copyright, preventing e-document forging.

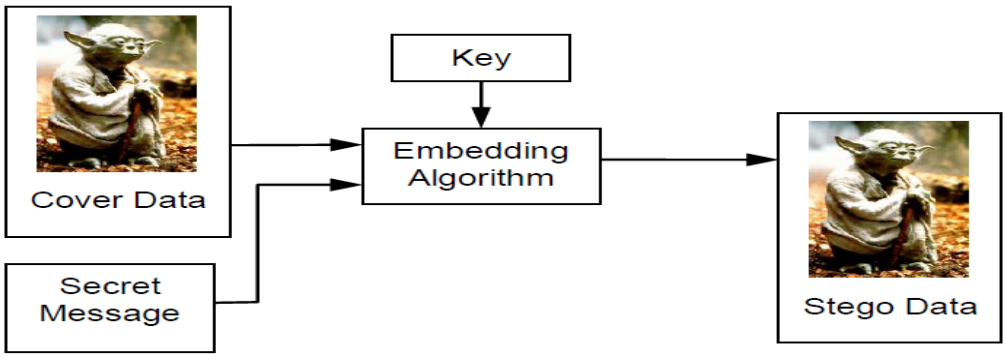

Figure 1 An overview of a generic steganographic system.

2. COMPARISON OF SECRET COMMUNICATION TECHNIQUES

The main goal of steganography is to hide information well steganographic medium of containing hidden data Simple steganography techniques have been in use for hundreds of years, but with the increasing use of files in electronic format new techniques for information hiding have become possible. Most steganography jobs have been carried out on different storage cover media like text, image, audio or video.Steganography [2] & encryption are both used to ensure data Confidentiality However the main difference between them is that with encryption anybody can see that both parties are Communicating in secret. Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. This makes steganography suitable for some tasks for which encryption aren't, such as copyright marking. Table 1 shows a comparison of different techniques for communicating in secret [4]. Encryption allows secure communication requiring a key to read the information. An attacker cannot remove the encryption but it is relatively easy to modify the file, making it unreadable for the intended.

TABLE 1
COMPARISON OF SECRET COMMUNICATION TECHNIQUES.

Secret Communication Techniques	Confidentiality	Integrity	Un removability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes/No	Yes/No	Yes

3. REQUIREMENTS OF HIDING INFORMATION DIGITALLY

There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a number of requirements so that steganography can be applied correctly.

The following is a list of main requirements that steganography techniques must satisfy:

a) The integrity of the hidden information after it has been embedded inside the stego object must be correct..

b) The stego object must remain unchanged or almost unchanged to the naked eye.

c) In watermarking, changes in the stego object must have no effect on the watermark.

d) Finally, we always assume that the attacker knows that there is hidden information inside the stego object.

4. IMAGE STEGANOGRAPHY TECHNIQUES

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [2]. 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 [20]. Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterised as "simple systems" [17]. The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format [18]. Steganography in the transform domain involves the manipulation of algorithms and image transforms [17]. These methods hide messages in more significant areas of the cover image, making it more robust [4]. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression [18].

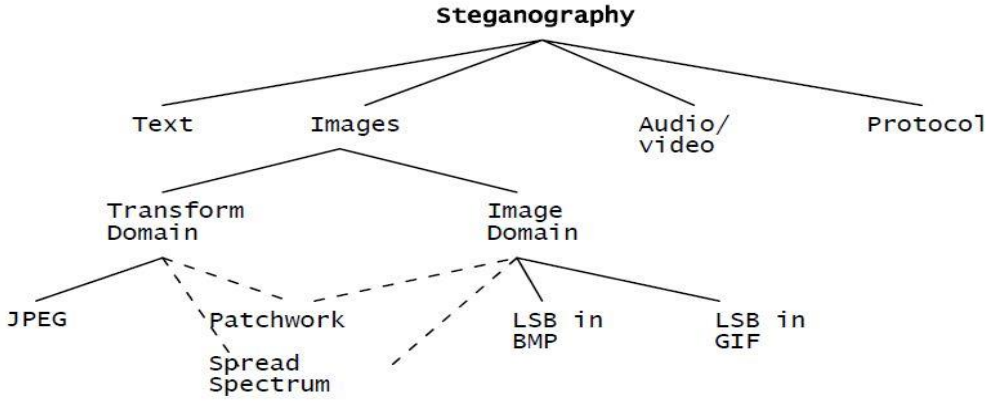

Figure 2: Categories of image steganography

4.1 Image Domain:

4.1.1 Least Significant Bit:

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image[14]. 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. When using a 24-bit image, a bit of each of the red, green and blue colourcomponents can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [19]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(10110101 01101100 10101101)
(10110110 11001101 00111110)
(10110101 01100011 10001110)

The number 150 which binary representation is 10010110 is embedded into the least significant bits of this part of the image, the resulting grid as follows:

(10110101 01101100 10101100)
(10110111 11001100 00111111)
(10110101 01100010 10001110)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [19]. Since there are 256 possible intensities of each primary colour changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [14].

4.1.2 Experimental results for LSB:

Figure 3: Experimental results for different images with different numbers of bits used

4.2 LSB and Palette Based Images:

Palette based images, for example GIF images, are another popular image file format commonly used on the Internet. By definition a GIF image cannot have a bit depth greater than 8, thus the maximum number of colours that a GIF can store is 256 [15]. GIF images are indexed images where the colours used in the image are stored in a palette, sometimes referred to as a colour lookup table [15]. Each pixel is represented as a single byte and the pixel data is an index to the colour palette [14]. The colours of the palette are typically ordered from the most used colour to the least used colours to reduce lookup time [17].

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 [17]. 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 [17]. One possible solution is to sort the palette so that the colour differences between consecutive colours are minimized [10]. 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) [1]. 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. A final solution to the problem is to use grey scale images. In an 8-bit grey scale GIF image, there are 256 different shades of grey [14]. The changes between the colours are very gradual, making it harder to detect.

5. IMAGE OR TRANSFORM DOMAIN

Some steganographic algorithms can either be categorised as being in the image domain or in the transform domain depending on the implementation.

5.1 Patchwork:

Patchwork is a statistical technique that uses redundant pattern encoding to embed a message in an image [14].The algorithm adds redundancy to the hidden information and then scatters it throughout the image [17]. A pseudorandom generator is used to select two areas of the image (or patches), patch A and patch B [22]. All the pixels in patch A is lightened while the pixels in patch B is darkened [22]. In other words the intensities of the pixels in the one patch are increased by a constant value, while the pixels of the other patch are decreased with the same constant value [6]. The contrast change in this patch subset encodes one bit and the changes are typically small and imperceptible, while not changing the average luminosity [17].

Disadvantage: of the patchwork 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 [23].

Advantage: of using this technique is that the secret message is distributed over the entire image, so should one patch be destroyed, the others may still survive [17].

This however, depends on the message size, since the message can only be repeated throughout the image if it is small enough. If the message is too big, it can only be embedded once [14].The patchwork approach is used independent of the host image and proves to be quite robust as the hidden message can survive conversion between lossy and lossless compression [23].

5.2Spread Spectrum:

In spread spectrum techniques, hidden data is spread throughout the cover-image making it harder to detect [4]. A system proposed by Marvel et al. combines spread spectrum communication, error control coding and image processing to hide information in images [6].Spread spectrum communication can be defined as the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies [6]. This can be accomplished by adjusting the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect [6]. In spread spectrum image steganography the message is embedded in noise and then combined with the cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image [6].

6. CRITICAL EVALUATION OF DIFFERENT TECHNIQUES

All the above mentioned algorithms for image steganography have different strong and weak points and it is important to ensure that one uses the most suitable algorithm for an application. All steganographic algorithms have to comply with a few basic requirements. The most important requirement is that a steganographic algorithm has to be imperceptible. These requirements are as follows:

- **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 steganalysis 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. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. 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.

The following table compares least significant bit (LSB) insertion in BMP and in GIF files, JPEG compression steganography, the patchwork approach and spread spectrum techniques as discussed in section 3, according to the above requirements:

Table 2: Comparison of image steganography algorithms

	LSB in BMP	LSB in GIF	JPEG compression	Patchwork	Spread spectrum
Invisibility	High*	Medium*	High	High	High
Payload capacity	High	Medium	Medium	Low	Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Independent of file format	Low	Low	Low	High	High
Unsuspicious files	Low	Low	High	High	High

* - Depends on cover image used

The levels at which the algorithms satisfy the requirements are defined as high, medium and low. A high level means that the algorithm completely satisfies the requirement, while a low level indicates that the algorithm has a weakness in this requirement. A medium level indicates that the requirement depends on outside influences, for example the cover image used. LSB in GIF images has the potential of hiding a large message, but only when the most suitable cover image has been chosen. The ideal, in other words a perfect; stegano graphic algorithm would have a high level in every requirement. Unfortunately in the algorithms that are evaluated here, there is not one algorithm that satisfies all of the requirements. Thus a trade-off will exist in most cases, depending on which requirements are more important for the specific application.

7. CONCLUSION

This paper gave an overview of different steganographic techniques its major types and classification of steganography which have been proposed in the literature during last few years. We have critical analyzed different proposed techniques which show that visual quality of the image is trade off in between capacity versus quality. In other words, when the number of bits of the secret data is low, the stego image quality is high and vice versa. Although only some of the main image steganographic techniques were discussed in this paper, 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. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (lsb) in both bmp and gif makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden. Thus for an agent to decide on which steganographic algorithm to use, he would have to decide on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others.

REFERENCES

[1] Moerland, T., “Steganography and Steganalysis”, Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[2] Silman, J., “Steganography and Steganalysis: An Overview”, SANS Institute, 2001

[3] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM, 47:10, October 2004

[4] Anderson, R.J. & Petitcolas, F.A.P., “On the limits of steganography”, IEEE Journal of selected Areas in Communications, May 1998

[5] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., “Spread Spectrum Steganography”, IEEE Transactions on image processing, 8:08, 1999

[6] Dunbar, B., “Steganographic techniques and their use in an Open-Systems environment”, SANS Institute, January 2002

[7] Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001

[8] Simmons, G., “The prisoners problem and the subliminal channel”, CRYPTO, 1983

[9] Chandramouli, R., Kharrazi, M. & Memon, N., “Image steganography and steganalysis: Concepts and Practice”, Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[10] Currie, D.L. & Irvine, C.E., “Surmounting the effects of lossy compression on Steganography”, 19thNational Information Systems Security Conference, 1996

[11] Handel, T. & Sandford, M., “Hiding data in the OSI network model”, Proceedings of the 1stInternational Workshop on Information Hiding, June 1996

[12] Ahsan, K. & Kundur, D., “Practical Data hiding in TCP/IP”, Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002

[13] Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998

[14] "Reference guide: Graphics Technical Options and Decisions",http://www.devx.com/projectcool/Article/19997

[15] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002

[16] Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", Proceedings of the 2nd Information Hiding Workshop, April 1998

[17] Venkatraman, S., Abraham, A. & Paprzycki, M., "Significance of Steganography on Data Security", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004

[18] Krenn, R., "Steganography and Steganalysis", http://www.krenn.nl/univ/cry/steg/article.pdf

[19] Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000

[20] Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", IEEE Security and

[21] Privacy Journal, 2003

[22] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, 1996

[23] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., "Information Hiding – A survey", Proceedings of the IEEE, 87:07, July 1999