A Tutorial Review on Steganography

Samir K Bandyopadhyay, Debnath Bhattacharyya[1], Debashis Ganguly[1], Swarnendu Mukherjee[1] and Poulami Das[1]

University of Calcutta, Senate House, 87 /1 College Street, Kolkata – 700073
[1]Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, Kolkata – 700107
E-mail : skb1@vsnl.com ; DebashisGanguly@gmail.com ; dippoulami@yahoo.com

ABSTRACT

The growth of high speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. Ironically, the cause for the development is also of the apprehension - use of digital formatted data. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. But this type advancement in the field of data communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the sender to the receiver. So, Information Security is becoming an inseparable part of Data Communication. In order to address this Information Security, Steganography plays an important role. Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. This paper is a tutorial review of the steganography techniques appeared in the literature.

1. INTRODUCTION

The desire to send a message as safely and as securely as possible has been the point of discussion since time immemorial. Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing [1]. The purpose of steganography is covert communication to hide a message from a third party.

Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information [34]. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them.

Generally, in steganography, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message (known as cover text in usual terms) is sent through the network to the recipient, where the actual message is separated from it.

In this paper, we have tried to present a detail survey on Steganography and we hope that this work will definitely provide a concrete overview on the past, present and future aspects in this field.

2. OVERVIEW

Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing). The origin of steganography is biological and physiological. The term "steganography" came into use in 1500's after the appearance of Trithemius' book on the subject "Steganographia". A short overview in this field can be divided into three parts and they are Past, Present and Future [2].

2.1 Past

The word "Steganography" technically means "covered or hidden writing". Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists [4, 16].

Cryptography became very common place in the middle ages. Secret writing was employed by the Catholic Church in its various struggles down the ages and by the major governments of the time. Steganography was normally used in conjunction with cryptography to further hide secret information [4, 5].

2.2 Present

The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication [3]. In modern approach, depending on the nature of cover object, steganography can be divided into five types:

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

So, in the modern age so many steganographic techniques have been designed which works with the above concerned objects. More often in today's security advancement, we sometimes come across certain cases in which a combination of Cryptography and Steganography are used to achieve data privacy over secrecy. Various software tools are also available in this regard [35].

2.3 Future

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography this problem is often taken as Steganalysis [18]. Steganalysis is a process in which a steganalyzer cracks the cover object to get the hidden data. So, whatever be the technique will be developed in future, degree of security related with that has to be kept in mind. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem.

3. DETAILS AND TECHNIQUES

Information can be hidden inside a multimedia object using many suitable techniques. As a cover object, we can select image, audio or video file. Depending on the type of the cover object, definite and appropriate technique is followed in order to obtain security. In this section, we will discuss different techniques or methods which are often used in image, audio and video steganography.

3.1 Text Steganography

Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, you will see that it is possible and not very difficult. Hiding

information in plain text can be done in many different ways [4].

Many techniques involve the modification of the layout of a text, rules like using every n-th character or the altering of the amount of white space after lines or between words [24]. The last technique was successfully used in practice and even after a text has been printed and copied on paper for ten times, the secret message could still be retrieved. Another possible way of storing a secret inside a text is using a publicly available cover source, a book or a newspaper, and using a code which consists for example of a combination of a page number, a line number and a character number. This way, no information stored inside the cover source will lead to the hidden message. Discovering it relies solely on gaining knowledge of the secret key.

3.2 Image Steganography

To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in "noisy" areas that draw less attention—those areas where there is a great deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include

- Least significant bit insertion
- Masking and filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Algorithms and transformations

Each of these techniques can be applied, with varying degrees of success.

3.2.1 Least significant bit insertion

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works good for image, audio and video steganography. To the human eye, the resulting image will look identical to the cover object [1, 16].

For example, if we consider image steganography then the letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may be

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

The binary value for A is 10000001. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

The underlined bits are the only three actually changed in the 8 bytes used. On average, LSB requires that only half the bits in an image be changed. You can hide data in the least and second least significant bits and still the human eye would not be able to discern it. The resultant image for the above data insertion and the original cover image are given below.

Fig. 1: The cover image

Fig. 2: The stego-image (after A is inserted)

3.2.2 Masking and filtering

Masking and filtering techniques are mostly used on 24 bit and grey scale images. They hide info in a way

similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking images entails changing the luminance of the masked area. The smaller the luminance change, the less of a chance that it can be detected. Observe that the luminance in Figure 2 is at 15% in the mask region if it was decreased then it would be nearly invisible [1, 4, 5].

Masking is more robust than LSB insertion with respect to compression, cropping, and some image processing. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. This makes it more suitable than LSB with, for instance, lossy JPEG images.

Fig. 3: Masking

3.2.3 Redundant Pattern Encoding

Patchwork and other similar tools do redundant pattern encoding, which is a sort of spread spectrum technique. It works by scattering the message throughout the picture. This makes the image more resistant to cropping and rotation. Smaller secret images work better to increase the redundancy embedded in the cover image, and thus make it easier to recover if the stego-image is manipulated [1, 4].

3.2.4 Encrypt and Scatter

The Encrypt and Scatter technique tries to emulate white noise. It is mostly used in image steganography. White Noise Storm is one such program that employs spread spectrum and frequency hopping. It does this by scattering the message throughout an image on eight channels within a random number that is generated by the previous window size and data channel. The channels then swap rotate, and interlace amongst each other. Each channel represents one bit and as a result there are many unaffected bits in each channel. This technique is a lot harder to extract a message out of than an LSB scheme because to decode you must first detect that a hidden image exists and extract the bit pattern from the file. While that is true for any stego-image you will also need the algorithm and stego key to decode the bit pattern, both of which are not required to recover a message from LSB. Some people prefer this method due to the considerable amount of extra effort that someone without the algorithm and stego-key would have to go through to extract the message. Even though White Noise Storm provides extra security against message extraction it is just as susceptible as straight LSB to image degradation due to image processing [1, 5].

3.2.5 Algorithms and transformations

LSB modification technique for images does hold good if any kind of compression is done on the resultant stego-image e.g. JPEG, GIF etc [20].

JPEG images use the discrete cosine transform to achieve compression. DCT is a lossy compression transform because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depend on the method used to calculate DCT [6, 7, 8].

3.3 Audio Steganography

In a computer-based audio steganography system, secret messages are embedded in digital sound. The secret message is embedded by slightly altering the binary sequence of a sound file. Existing audio steganography software can embed messages in WAV, AU, and even MP3 sound files [22].

Embedding secret messages in digital sound is usually a more difficult process than embedding messages in other media, such as digital images. In order to conceal secret messages successfully, a variety of methods for embedding information in digital audio have been introduced. These methods range from rather simple algorithms that insert information in the

form of signal noise to more powerful methods that exploit sophisticated signal processing techniques to hide information. The list of methods that are commonly used for audio steganography are listed and discussed below.

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

3.3.1 LSB coding

Using the least-significant bit is possible, as modifications will usually not create audible changes to the sounds. Another method involves taking advantage of human limitations. It is possible to encode messages using frequencies that are inaudible to the human ear. Using any frequencies above 20.000 Hz, messages can be hidden inside sound files and will not be detected by human checks [14].

Fig. 3: The signal level comparisons between a WAV carrier file before (above) and after (below) the LSB coding is done

3.3.2 Parity coding

Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion.

3.3.3 Phase coding

Phase coding addresses the disadvantages of the noise-inducing methods of audio steganography. Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is. Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-perceived noise ratio.

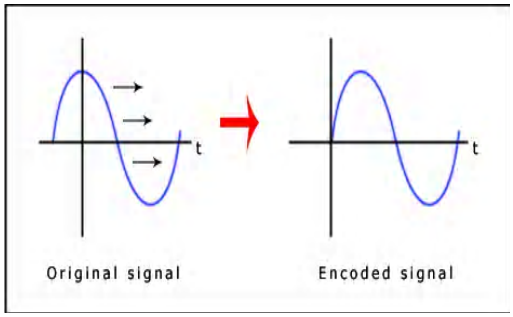

Fig. 4: The signals before and after Phase coding procedure

3.3.4 Spread spectrum

In the context of audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is analogous to a system using an implementation of the LSB coding

that randomly spreads the message bits over the entire sound file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for transmission [21].

3.3.5 Echo hiding

In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods. If only one echo was produced from the original signal, only one bit of information could be encoded. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.

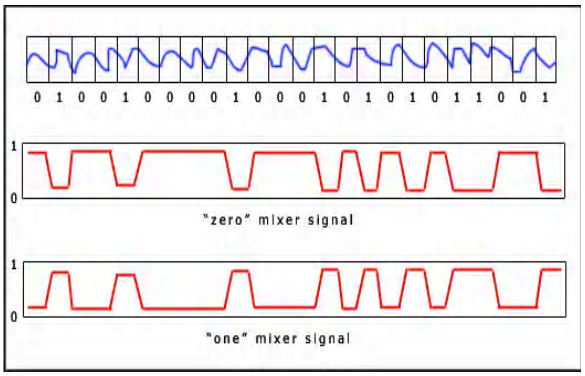

Fig. 5: An example of echo hiding

Also, a message can be encoded using musical tones with a substitution scheme. For example, a Fis-tone will represent a 0 and a C tone represents a 1. A normal musical piece can now be composed around the secret message or an existing piece can be selected together with an encoding scheme that will represent a message [4, 5].

3.4 Video Steganography

Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too [23]. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds. Therefore, any small but otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information [4, 14].

3.5 Protocol Steganography

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission [24]. In the layers of the OSI network model there exist covert channels where steganography can be used [25]. 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. A paper by Ahsan and Kundur provides more information on this [24].

4. APPLICATION

Steganography can be used anytime you want to hide data. There are many reasons to hide data but they all boil down to the desire to prevent unauthorized persons from becoming aware of the existence of a message. In the business world steganography can be used to hide a secret chemical formula or plans for a new invention. Steganography can also be used for corporate espionage by sending out trade secrets without anyone at the company being any the wiser. Steganography can also be used in the non-commercial sector to hide information that someone wants to keep private. Spies have used it since the time of the Greeks to pass messages undetected. Terrorists can also use steganography to keep their communications secret and to coordinate attacks. It is exactly this potential that we will investigate in the next section.

Because you can hide information without the cover source changing, 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. The main difference is on intent, while the

purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, steganographic methods can be used to hide this [4, 17].

5. DETECTION

As more and more techniques of hiding information are developed and improved, the methods of detecting the use of steganography also advance. Most steganographic techniques involve changing properties of the cover source and there are several ways of detecting these changes. We will now discuss the detection procedures separately depending on the type of the cover media [18].

5.1 Detection technique for Text steganography

While information can be hidden inside texts in such a way that the presence of the message can only be detected with knowledge of the secret key, for example when using the earlier mentioned method using a publicly available book and a combination of character positions to hide the message, most of the techniques involve alterations to the cover source. These modifications can be detected by looking for patterns in texts or disturbing thereof, odd use of language and unusual amounts of white space [4].

5.2 Detection technique for Image steganography

Even though stego-images can rarely be spotted by the naked eye, they usually leave behind some type of fingerprint or statistical hint that they have been modified. It is those discrepancies which an analysis tool may be able to detect. Since some techniques and their effects are commonly known, a statistical analysis of an image can be performed to check for a hidden message(s) in it [5, 15].

A widely used technique for image scanning involves statistical analysis. Most steganographic algorithms that work on images, assume that the least-significant bit is more or less random. This is however, an incorrect assumption. While the LSB might not seem to be of much importance, applying a filter which only shows the least significant bits, will still produce a recognizable image [18, 19]. Since this is the case, it can be concluded that the LSB are not random at all, but actually contain information about the whole image. When inserting a hidden message into an image, this property changes. Especially with encrypted data, which has very high entropy, the LSB of the cover image will no longer contain information about the original, but because of the modifications they will now be more or less random [9, 16, 30].

With a statistical analysis on the LSB, the difference between random values and real image values can easily be detected. Using this technique, it is also possible to detect messages hidden inside JPEG files with the DCT method, since this also involves LSB modifications, even though these take place in the frequency domain [10, 28, 30].

5.3 Detection technique for Audio and Video steganography

The statistical analysis method can be used against audio files too, since the LSB modification technique can be used on sounds too. Except for this, there are several other things that can be detected. High, inaudible frequencies can be scanned for information and odd distortions or patterns in the sounds might point out the existence of a secret message. Also, differences in pitch echo or background noise may raise suspicion. Like implementing steganography using video files as cover sources, the methods of detecting hidden information are also a combination of techniques used for images and audio files. However, a different steganographic technique can be used that is especially effective when used in video films [11, 15, 29]. The usage of special code signs or gestures is very difficult to detect with a computer system. This method was used in the Vietnam War so prisoners of war could communicate messages secretly through the video films the enemy soldiers made to send to the home-front [4, 12].

6. EVALUATION

In this section, we will try to evaluate different steganographic techniques that we have discussed

already depending on certain criteria. When we follow any kind of approach to obtain data security, we always keep focusing on the degree of security that we are getting by that. For steganography also we use the same concept. So, before we follow a certain technique, we have to evaluate that to match our desired goal. The evolutions are described below.

6.1 For Text steganography

The first-letter algorithm used in general is not very secure, as knowledge of the system that is used, automatically gives you the secret. This is a disadvantage that many techniques of hiding secrets inside plain text have in common.

6.2 For Image steganography

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. The authors propose a set of criteria to further define the imperceptibility of an algorithm. 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 [32].

Payload capacity – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography in other hand requires sufficient embedding capacity [33].

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 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 [1, 26].

The ideal, in other words a perfect steganographic 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 [26, 27].

6.3 For Audio steganography

We believe that the flexibility of audio steganography is what makes it so potentially powerful. The five methods discussed provide users with a large amount of choice and makes the technology more accessible to everyone. A party that wishes to communicate can rank the importance of factors such as data transmission rate, bandwidth, robustness, and noise audibility and then select the method that best fits their specifications. For example, two individuals who just want to send the occasional secret message back and forth might use the LSB coding method that is easily implemented. On the other hand, a large corporation wishing to protect its intellectual property from "digital pirates" may consider a more sophisticated method such as phase coding, SS, or echo hiding.

6.4 For Video steganography

As we have discussed earlier that a video file is a combination of both image an audio. So, video steganography is nothing but a combination of image and audio steganography [31]. So, the combined evaluations i.e., the evaluations for image and audio steganography can be taken together for the evaluation of video steganography. While doing video steganography, the effect on video has to be kept in mind to achieve a secure communicating media.

4. DISCUSSION

Steganography is used to have a level of privacy while doing data communication with others. We have already discussed several methods related with that. But only the concealment of data may not give the best result always. So, some extra level of security along with the privacy has to be incorporated. Steganography, especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The methods used in the science of steganography have advanced a lot over the past centuries, especially with the rise of the computer era. Although the techniques are still not used very often, the possibilities are endless. Again the concept of Dual Steganography i.e., first application of steganography in between the embedding object and the cover object and then again apply the same method with the help of other object, can be developed to obtain a new definition of security. Concept of object self encryption technique before the application of steganography to hide that inside a cover can also be developed to achieve a level of security.

5. CONCLUSION

Many different techniques exist and continue to be developed, while the ways of detecting hidden messages also advance quickly. Since detection can never give a guarantee of finding all hidden information, it can be used together with methods of defeating steganography, to minimize the chances of hidden communication taking place. Even then, perfect steganography, where the secret key will merely point out parts of a cover source which form the message, will pass undetected, because the cover source contains no information about the secret message at all.

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. Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down.

Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate. More restrictions on the use of privacy-protecting technologies are not very unlikely, especially in this period of time with great anxiety of terrorist and other attacks.

REFERENCES

1. Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2):26–34.
2. Saraju P. Mohant. Digital Watermarking: A Tutorial Review
3. Niels Provos, Peter Honeyman, Hide and Seek: Introduction to Steganography (2003).
4. Robert Krenn. Steganography and steganalysis
5. Francesco Queirolo. Steganography in Images
6. Westfeld, A. (2001). F5-a steganographic algorithm: High capacity despite better steganalysis. In Proc. 4th Int'l Workshop Information Hiding, pages 289–302.
7. W. Brown and B.J. Shepherd, Graphics File Formats: Reference and Guide, Manning Publications, Greenwich, Conn, 1995.
8. E. Koch, J. Rindfrey, and J. Zhao, "Copyright Protection for Multimedia Data," Proc. Int'l Conf. Digital Media and Electronic Publishing, Leeds, UK 1994.
9. R. Chandramouli, Nassir Menon. Analysis of LSB based Image Steganographic techniques
10. Moerland, T., Steganography and Steganalysis
11. R. Chandramouli. A Mathematical approach to Steganalysis
12. F.A.P.Petitcolas, et al.,"Information Hiding - A Survey", Proceedings of the IEEE, Vol.87, No.7, July 1999, pp.1062-1078.
13. B.Pfitzmann, "Information Hiding Terminology", Proc. of First Int. Workshop on Information Hiding, Cambridge, UK, May30-June1, 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.347-350.
14. David Kahn, "The History of Steganography", Proc. of First Int. Workshop on Information Hiding, Cambridge,UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson (Ed.), pp.1-7.
15. Gary C. Kessler. An Overview of Steganography for the Computer Forensics Examiner
16. Alain C. Brainos II. A Study Of Steganography And The Art Of Hiding Information
17. Ingemar J. Cox, Ton Kalker, Georg Pakura and Mathias Scheel. Information Transmission and Steganography
18. Debashis Ganguly. Swarnendu Mukherjee, Mohit Mundhra (2006). Digital Watermarking: A New Approach. In Proc. 41st Annual conference, CSI'06, paper no. : 11.
19. Eugene T. Lin, Edward J. Delp. A Review of Data Hiding in Digital Images
20. Kathryn Hempstalk. Hiding Behind Corners: Using Edges in Images for Better Steganography
21. Bogdan J. Falkowski. Lossless binary image compression using logic functions and spectra
22. Katzenbeisser, Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking.
23. Brian Jacokes, Yuliya Kodysh, Andrew Lisy. Audio Steganography
24. Udit Budhiaa, Deepa Kundura. Digital video steganalysis exploiting collusion sensitivity
25. Handel, T. & Sandford, M., "Hiding data in the OSI network model", Proceedings of the 1st International Workshop on Information Hiding, June 1996
26. Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002
27. T. Morkel , J.H.P. Eloff , M.S. Olivier., An Overview of Image Steganography
28. Mehdi Kharrazi Husrev, T. Sencar, Nasir Memon., Performance study of common image steganography and steganalysis techniques, SPIE Proceedings Vol. 5681.
29. Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, 1996
30. Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., "Information Hiding – A survey", Proceedings of the IEEE, 87:07, July 1999
31. Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", Proceedings of the 2nd Information Hiding Workshop, April 1998
32. Zenon Hrytskiv, Sviatoslav Voloshynovskiy, Yuriy Rytsav., Cryptography and Steganography of Video information in modern communication, Electronics and Energetics, Vol 11, No. 1, 115-225
33. Dean Lewandowski, Mike Palmisano., Steganography
34. R. Chandramouli and N.D. Memon., Steganography Capacity: A Steganalysis Perspective
35. Luis von Ahn, Nicholas J. Hopper., Public-Key Steganography