ISSN: 2348 9510

International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

A comprehensive study of steganography: A method of hiding information in other information

Vaidehi Verma[a] , Sudhadevi Kore[b]

(a) Mtech ScholaR,Department of computer science,SD Bansal college of technology,INDORE.

(b) Mtech scholar,school of future studies and planning,DAVV,INDORE

Abstract

Steganography is a art of communicating by hiding a type of information in other information.In the present era, the more attention is given to the art of displaying and sending hidden information because of security purpose.Therefore, different methods have been proposed so far for hiding information in different cover media. In this review paper, we are highlights the various study and research done before.Steganography's primary goal is to hide data within some other data such that the hidden data cannot be detected even if it is being sought.A lot of researchers has done tremendous work in this art but there is lack of a single means to concrete all the information in single study.This paper aims to fulfill that dearth.

Introduction

The word steganography when decomposed gives two greek words namely "STEGANOS" meaning "Covered" and "GRAPHIE means "Writing"[1]. The definition obtained from the literatures is very much matching the line-"steganography is the art and science of communicating in such a way that the presence of a message cannot be detected" which is very first given by Cachin[2].In other words it is an art of writing hidden messages in such a way that no one apart from the intended recipient even knows that a message has been sent.Simple steganographic techniques have been in use for hundreds of

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible.security has become one of the most significant problems for distributing new information technology. It is necessary to protect this information while communicated over insecure channels. Thus, a need exists for developing technology that will help protect the integrity of digital content and secure the intellectual property rights of owners. Steganography are mainly of two types namely FRAGILE and ROBUST steganography[11].The former involves embedding information into a file which is destroyed if the file is modified while later aims to embed information into a file which cannot easily be destroyed.

Cryptography and Steganography are the two major techniques for secret communication. The contents of secret message are scrambled in cryptography, where as in steganography the secret message is embedded into the cover medium. In this proposed system we developed high security model by combining cryptographic and Steganographic security. In cryptography we are using advanced encryption standard (AES) algorithm to encrypt secret message and then pixel value differencing (PVD) with K-bit least-significant-bit (LSB) substitution is used to hide encrypted message into true color RGB image.The extractor should have secret key to extract the data.

The secret key designed in such a manner that it can't be find out by an unusual user[5].
A better difference between both the phenomenon is given by Jonathan et. Al.[3].According t them 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 is not, such as copyright marking. Adding encrypted copyright information to a file could be easy to remove but embedding it within the contents of the file itself can prevent it being easily identified and removed.

Popa[4] has given the difference in tabular form which is given below:

	Confidentiality	Integrity	Unremovability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes / No	Yes / No	Yes

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

In Digital signatures,integrity is maintained because it allows the authorship to be asserted with the fact that if changes made in the signature during sending or displaying,the signature becomes invalid.However in Encryption,an attacker can not remove the it but he can easily modify it which makes it unreadable.
Steganography resolve all this problems,because it provides a means of secret method os sending the file which cannot be altered or removed.The embedded file will be confidential unless a way to detect it is find out.
The figure given below shows the different elements of the steganography:

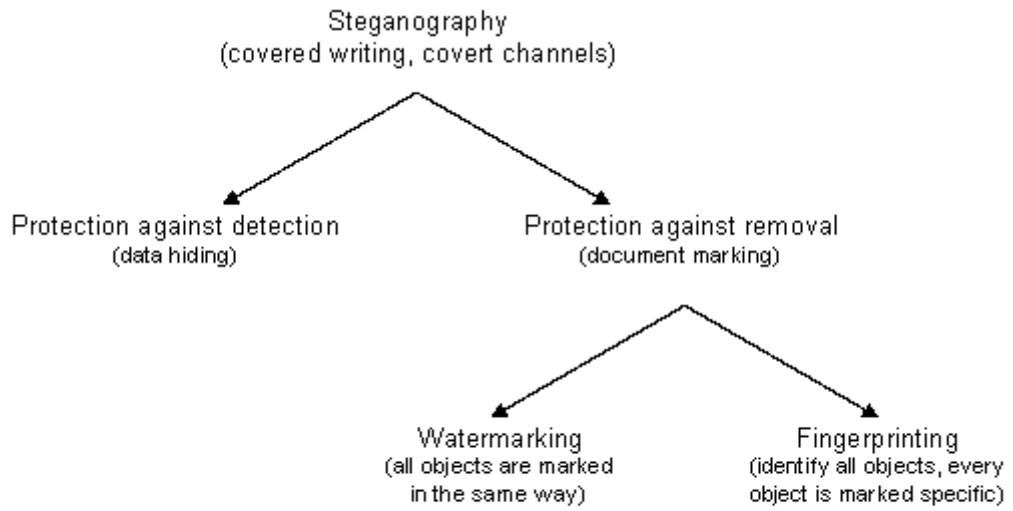

Fig. 1[4] Different elements of steganography.

Techniques Of Steganography

On a broader sense,the word steganography is divided into three major techniques.They are:
1)Injection: Injection is quite a simple method which simply involves directly injecting the secret information into the carrier file.

2)Substitution: Replacement of the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

3)Generation: The generation technique, unlike injection and substitution, requires only a covert file, as it is used to create the overt file.

A steganography must have the integrity of the hidden information after it has been embedded inside the stego object must be correct.Moreover,it also ensure that the stego object must be remain unaltered when see by the naked eye.The techniques are implemented with a assumption that the attackers knows that there is a hidden information inside the stego object.

Files having high degree of redundancy has more suitable for steganography.Redundancy can be defined as the bit so fan 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 with out the alteration being detected easily [6,7].Text steganography Using digital files is not used very often since text files have a very small amount of redundant data[7].

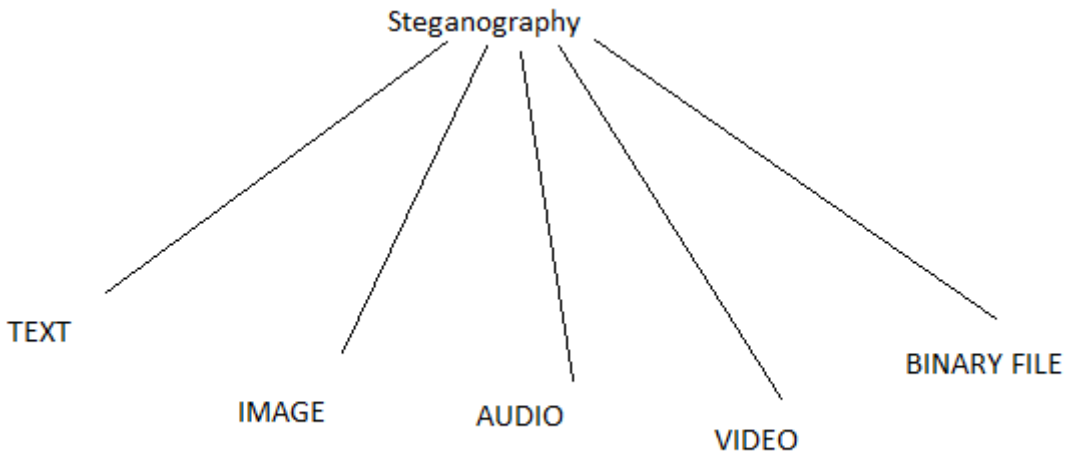

Fig.2[8] Different types of steganography techniques.

Text Steganography

This type of steganography can be achieved by changing the text formatting and/or by altering the particular characteristics of various textual elements[9]. The main motto in the design of coding methods is to develop changes that are de-codable,even in the presence of noise,yet largely indiscernible to the reader.The file formats describing the document

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

content and page layout Uses PostScript2, TeX, @off, etc. Standard languages.

Line shift coding,feature coding and word shift coding are three main techniques used in text steganography.Chapman[10] describe on more technique as text steganography in which he proposed to use written natural languages to conceal a secret message.

In Line shift coding,one can alter the existing document by vertically shifting the locations of the text lines to encode the documents while opposite to this in word shifting coding,one has to change the document by horizontally shifting the locations of words within text lines to encode the documents uniquely.In feature coding method,depending upon the codeword,the features of the image is altered.Before doing the alterations,the image is examined for chosen that features.This method is used to format file as well as to a bitmap image of a document.The main advantage of the text steganography is that the alterations are not visible to the human eye.

Image Steganography

Images are the most popular cover objects used for steganography.An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups.The various steps involved in this type of steganography is given in figure 3.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

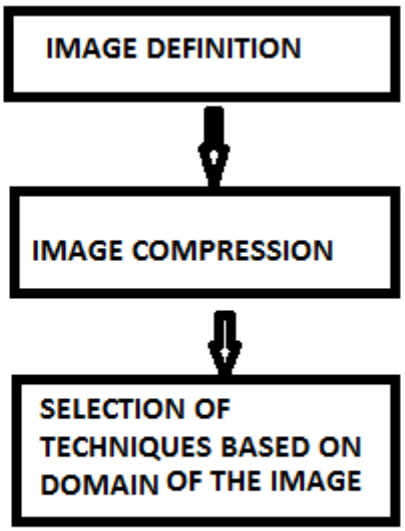

Fig.3 Steps Involved In the Implementation of Image Steganography.

Image definition is the process in which a computer identify the image in a numeric representation.The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel[7].There are 8 bits used to describe the color of each pixel.Monochrome and gray scale images used 8 bits for each pixel but digital color images stored in 24 bit file.All color variations for the pixel of a 24 bit image are derived from three basic color namely red,green and blue.The larger amount of colors that can be displayed,the larger the file size.Image compression is defined as the techniques which make use of mathematical formulas to analyse and condense image data and reduce its file sizes.This is an important step before applying steganography methods since larger images of greater bit depth tends to become too large to transmit over a standard internet connection and displaying such image consume more time as compared to compressed image.As surveyed from from past work on compression,there are mainly two types of compressions[12]:

a) **Lossy compression**: In this type of compression,very small details which are not differentiate for human eye are remove and thus discard excess image data to create a smaller file.JPEG format of image makes use of this type of compression.

b) **Loseless compression**: This type of compression uses mathematical formulas to

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

represent the data rather than the removing any data from the image.GIF uses this type of compression.The original image's integrity is maintained and the decompressed image output is bit-by-bit identical to the original image input[12,7].

Both type of compression has its own limitations and advantages.Dunbar [13] elaborate in his paper that Lossy compression results in smaller file sizes but the possibility of losing embedded message due to removing to excess image data during compression.Unlike,Lossless compression keeps the original digital image without the chance of lost, but is does not compress the image to such a small file size. Depending upon the method of compression used different steganography techniques are used.

A classification tree of the image steganography is shown below:

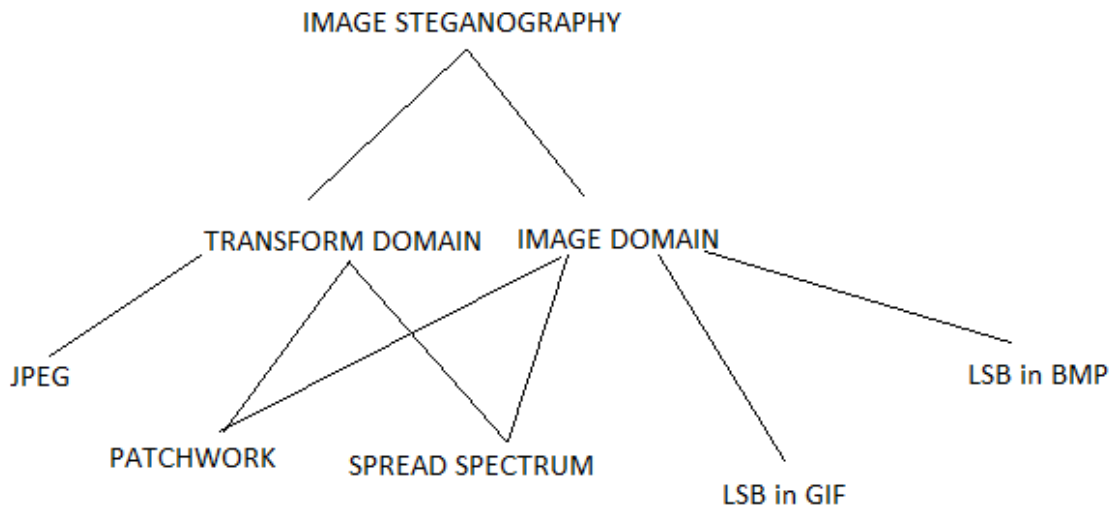

Fig.4 [14] Classification of Image Steganography.

Image domain 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. Lossless compression is most suitable for the image domain techniques.Steganography in the transform domain involves

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

the manipulation of algorithms and image transforms.

In image domain under the LSB(Least significant Bit) method,least significant bits of each pixel in one image to hide the most significant bits of another.It is the easiest and simplest method way of hiding information.LSB method can be implemented in both GIF as well as BMP formats.In LSB,the first step is to load the host image which is to be hide.The next step is to decide the number of bits to hide the secret image in.Increasing the number of bits increases the clarity of the secret image.By combining both the image create a new one which will be used to transmits the message.Now for a receiver to get the original image,he has to just know the number the bits which were used to store the secret message.The method works remarkably good when both the host and secret images are given equal priority,however,when one of the image has given more room than one has to compromised with the quality[3].

There is another method of hiding data is Direct Cosine Transformation(DCT).It embeds the information by altering the transformed DCT coefficients.The main advantage of this method is that the Hidden data can be distributed more evenly over the whole image in such a way as to make it more robust[11].The DCT algorithm is one of the main components of the JPEG compression technique [15].Chao et al.[16] and Gailly et al.[17] in their papers separately depicted the methods of DCT.

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

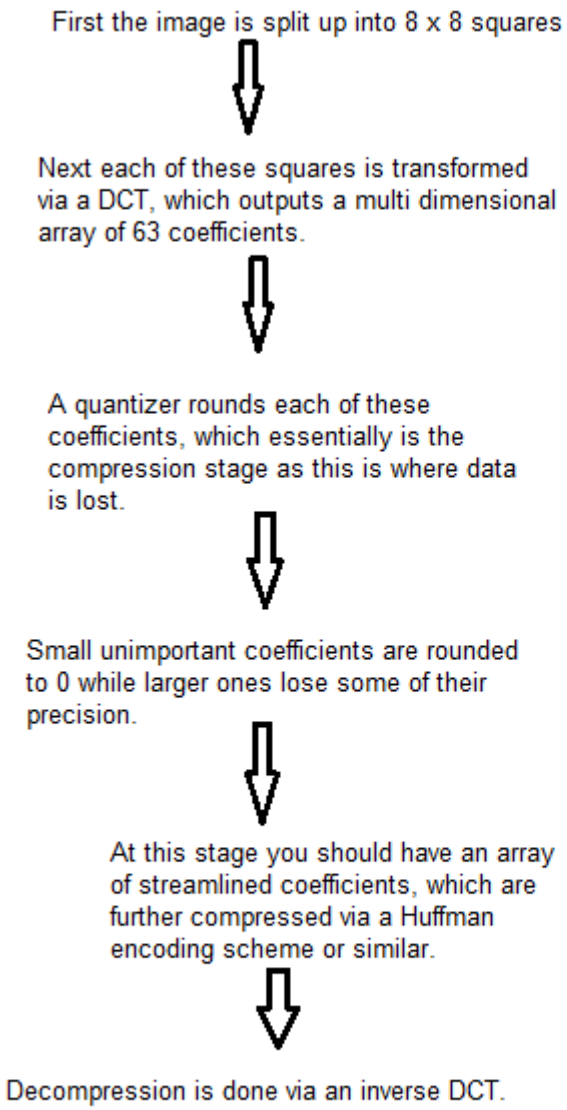

Fig.5 [16][17] Step by step procedure for DCT transformation technique.

Another method of hiding data in image steganography is wavelet transformation.DCT method can not give satisfactory result at higher compression levels.Wavelet transformation overcome this limitations to a great extent.This techniques enjoys the

ISSN: 2348 9510
International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

advantage that the coefficients of the wavelets are changed with the noise within tolerable limits and thereby increase the robustness of the hidden information,which is very essential in areas like watermarking[18].In this techniques many wavelets are taken to encode a single image which allows the image to be compressed more at high frequency.The low frequency areas can then be compressed which is acceptable as they are most viable for compression[19].

Sound or audio steganography is used for MP3 files.In this,the encode data as a binary sequence which sounds like noise but which can be recognised by a receiver with the correct key.Used for watermarking by matching the Narrow bandwidth of the embedded data to the large bandwidth of the medium.There are very few working examples of hiding information in MP3 files but one freely available program is MP3Stego [20].In that technique, the data to be hidden is stored as the MP3 file is created, that is during the compression stage [21].

As the sound file is being compressed during the Layer 3 encoding process, data is selectively lost depending on the bit rate the user has specified. The hidden data is encoded in the parity bit of this information. As MP3 files are split up into a number of frames [22] each with their own parity bit, a reasonable amount of information can be stored. To retrieve the data one need to do is uncompress the MP3 file and read the parity bits as this process is done. This is an effective technique which leaves little trace of any distortions in the music file.

Other techniques like video steganography in which A combination of sound and image techniques can be used .The scope for adding lots of data is much greater.While in binary file techniques,binary files are used to hide the data.In this technique,watermark can be embedded by making changes to the binary code that does not affect the execution of the file Simple to implement.Various good work available which helps to understand this techniques also.

Conclusion

Steganography is a broad area of research.In present and future,many researchers choose their area of research as steganography due to hike in demands of techniques of hiding

ISSN: 2348 9510

International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

data.This paper acts as a beginner guide to all such researchers.This paper clearly depicts a outer zest of all the techniques of steganography.However,this study depends on the past study of research work done on steganography and so depending upon the limitations of literature study,one can find more detailed information on a particular technique as compared to the information available in this paper.

References

[1] Moerland T.,"Steganography and Stegan alysis",Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.

[2] C. Cachin, "An Information-Theoretic Model for Steganography", *Proceedings of 2nd Workshop on Information Hiding*, MIT Laboratory for Computer Science, May 1998.

[3] Jonathan Cummins, Patrick Diskin, Samuel Lau & Robert Parlett,"steganography-the art of hiding data " http://www.gnu.org/copyleft/fdl.html.

[4] R. Popa, *An Analysis of Steganographic Techniques*, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering,http://ad.informatik.uni-freiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf, 1998.

[5] Rakhi, Suresh Gawande,"A REVIEW ON STEGANOGRAPHY METHODS " International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering ,Vol. 2, Issue 10, October 2013.

[6] Anderson,R.J.&Petitcolas,F.A.P.,"On the limits of steganography",IEEE Journal of Communications, May1998.

[7] Maninder Singh Rana, Bhupender Singh Sangwan, Jitendra Singh Jangir, " Art of Hiding: An Introduction to Steganography",International Journal Of Engineering And Computer Science ,Volume1 Issue 1 Oct 2012 Page No. 11-22.

[8]B.Rajkumar,S.S.Aravinth,M.Kavipriya,M.Ramkumar,.M.MohanaPriya,M.Kalaivani," Data Hiding Images Using Spread Spectrum in Cloud Computing",International Journal

ISSN: 2348 9510

International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

of Scientific & Engineering Research, Volume 4, Issue 8, August-2013 396 ISSN 2229-5518.

[9] Masoud Nosrati ,Ronak Karimi ,Mehdi Hariri,"An introduction to steganography methods",*World Applied Programming, Vol (1), No (3), August 2011. 191-195.*

[10] M.Chapman, G. Davida, and M. Rennhard, "A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography",Proceedings of the Information Security Conference, October 2001, pp. 156-165.

[11] Shashikala Channalli,Ajay Jadhav,"Steganography:An art of hiding Data",International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.

[12]Moerland,T.,"Steganography and Steganalysis",*Leiden Institute of Advanced Computing Science*, www.liacs.nl/home/ tmoerl/privtech.pdf .

[13] Dunbar B., "Steganographic techniques and their use in an Open-Systems environment", *SANS Institute*, January2002.

[14] Silman J., "Steganography and Steg analysis: An Over view ",*SANS Institute*, 2001.

[15] L. Leurs, *JPEG Compression*, http://www.prepressure.com/techno/compression jpeg.htm, 2001.

[16] A. K. Chao and C. Chao, *Robust Digital Watermarking & Data Hiding*, Image Systems Engineering Program, Stanford University, http://ise.stanford.edu/class/ee368a_proj00/project7/index.html, May 2000

[17] J. Gailly, *comp.compression Frequently Asked Questions (part 2/3)*, Internet FAQ Archives, http://www.faqs.org/faqs/compression-faq/part2/, September 1999.

[18] National Academy of Sciences, *How do Wavelets work?*, National Academy of Sciences, http://www.beyonddiscovery.org/content/view.page.asp?I=1956, 2003

ISSN: 2348 9510

International Journal Of Core Engineering & Management (IJCEM)
Volume 1, Issue 5, August 2014

[19] C. Shoemaker, *Hidden Bits: A Survey of Techniques for Digital Watermarking*, http://www.vu.union.edu/~shoemakc/watermarking/watermarking.html# watermark-object, Virtual Union, 2002

[20] F. A. P. Petitcolas, *mp3stego*, http://www.petitcolas.net/fabien/steganography/mp3stego/, September 2003

[21] Fraunhofer-Gesellschaft, *Audio & Multimedia MPEG Audio Layer-3*, Fraunhofer-Gesellschaft, http://www.iis.fraunhofer.de/amm/techinf/layer3/index.html.

[22] S. Hacker, *MP3: The Definitive Guide*, chapt. 2 - How MP3 Works: Inside the Codec, http://www.oreilly.com/catalog/mp3/chapter/ch02.html, O"Reilly, March 2000.