AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY

R.Poornima[1] and R.J.Iswarya[2]

[1] M.Tech., Department Of Advanced Computing, Sastra University,India.
[1]poorniajar@gmail.com
[2] M.Tech., Department Of Advanced Computing, Sastra University,India.
[2]iswaryajeyaraman@gmail.com

ABSTRACT

Hiding Capacity plays a vital role for efficient covert communication. This is achieved by Steganography. Steganography is the science of hiding the information into the other information so that the hidden information appears to be nothing to the human eyes. 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 gives a review of various methods such as image domain and transformation domain algorithms available for implementing Image Steganography. In this paper, a high-capacity Image Steganography schemes are discussed for different file formats. Covert communication is taking place by encrypting the password for information to be protected. The intended receiver will decrypt the information using that password.

KEYWORDS

Steganography, Encryption, Image Domain, Transform Domain.

1. INTRODUCTION

Over the last two decades, the rapid development of internet requires confidential information that needs to be protected from the unauthorized users. This is accomplished through Data hiding. It is a method of hiding secret messages into a cover medium so that an unintended observer will not be aware of the existence of the hidden messages. This is achieved by steganography. The term steganography is retrieved from the Greek words *stegos* means *cover* and *grafia* meaning *writing* defining it as *covered writing.*

The similarity between steganography and cryptography is that, both are used to conceal information. But the difference is that the steganography does not reveal any suspicious about the hidden information to the user. Therefore the attackers will not try to decrypt information. This paper reviews the various methods of steganography such as image, audio, video, text, to hide the information.

There are other two techniques that seem to be same as Steganography. They are Watermarking and Fingerprinting. Both these techniques sounds to be same and provide same end goals but both are very different in the way they working. Watermarking allows a person to provide hidden copyright notices or other verification licenses. Whereas, Fingerprinting uses each copy of the content and make it as unique to the receiver.

DOI : 10.5121/ijcses.2013.4102

Watermarking is usually a signature to identify the origin and all the copies are marked in the same way. But in Fingerprinting different unique copies are embedded for distinct copies.

Let us consider an example for a cover text:

"Day-after-tomorrow, American Henry Irish darley ignoring next group".

In this example the first letter of all the words are assembled to produce an encrypted message "Data Hiding" inside of the above sentence. Similarly encrypted message can be hidden in the cover medium by different approaches.

1.1. Embedding Process of Steganography

In this paper the main aim is to hide information in to the carrier file. The file that contains the embedded information inside of it, called as stego file. The information hiding here is text file(confidential information). Similarly we can hide different types of file formats such as video, audio, image etc.It is represented in Fig.1.

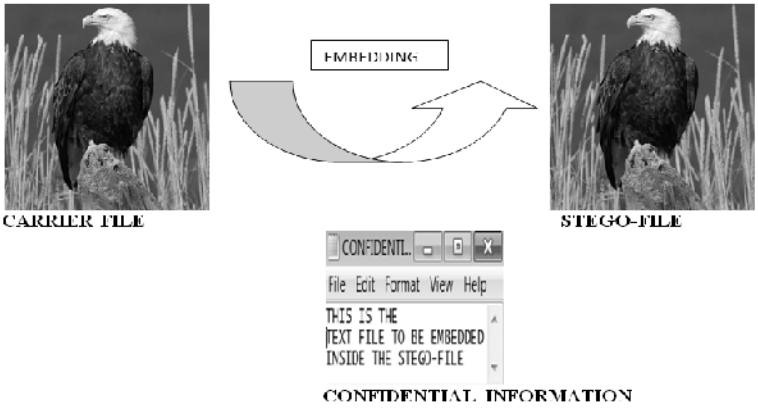

Figure 1. Embedding Process of Steganography

1.2. Era of Steganography

1. During the cold war two the Microdot technology developed by Germans which prints the clear good quality photographs shrinking to the size of a dot.

2. In Greece they select a person to send message by shaving their heads off. They write a secret message on their head and allow growing up their hair. Then the intended receiver will again shave off the hair and see the secret message.

3. During the world war two the secret message was written in invisible Ink so that the paper appears to be blank to the human eyes. The secret message is extracted back by heating the liquids such as milk, vinegar and fruit juices.

1.3. Steganography Types

There are two types of steganography they are Fragile and Robust,

1.3.1 Fragile

In Fragile steganography, if the file is modified, then the secret information is destroyed. For example the information is hidden the .bmp file format. If the file format is changed into .jpeg or some other format the hidden information is destroyed. The advantage of fragile is required to be proved when the file is modified.

1.3.2 Robust

In robust steganography the information is not easily destroyed as in fragile steganography. Robust steganography is difficult to implement than fragile [19].

2. Steganography in Image

In reference to this part of the paper. Image steganography is classified into two domains: Transform Domain (Frequency Domain technique) and Image Domain (Spatial Domain technique).Transform Domain applies image transformation and manipulation of algorithm. Image Domain applies bit insertion and noise manipulation of a covered image. Numbers of researchers have proposed various techniques for these domains intended readers may refer [14]-[18].

2.1. Data Compression

In images, there are different compression algorithm is available such as "**Lossy**" Compression is to reduce the amount of information to be transmitted. This is done by compressing the information by permanently losing some of it, particularly redundant information. JPEG (JOINT PHOTOGRAPHIC EXPERTS GROUP) is the image format that follows Lossy Compression.

On the other hand, "**Lossless**" Compression never discards any information from the target image. All the information can be restored even after the image is decompressed.GIF (GRAPHICAL INTERCHANGE FORMAT) and BMP (BIT MAP FILE) are image format that follows Lossless Compression.

Importance of Compression is that it helps us to choose the suitable technique to follow. Different stenographic algorithms are available for both types of compression which we discuss as follows.

2.2. Image Domain (Spatial Domain Technique)

2.2.1. LSB (Least Significant Bit)

LSB is common technique in encrypting and decrypting the secret information. LSB method is based on altering the redundant bits that are least important with the bits of the secret information. The aim of the LSB is to transmit the secret information to the receiver without knowing to the intruder that the message is being passed.

2.2.1.1. LSB IN BMP (BIT MAP FILE)

LSB using 24-bit BMP file format is suitable and efficient because BMP images have good quality and high resolution so that the hidden information is less prone to the human eyes. Now

800X600pixel BMP are used which can store up to 1,440,000 bits or 180,000 bytes of information [1]. BMP file format is used by Windows which is native image format in Microsoft Windows Operating System. It can supports image with 16 and 32 bit per pixel [22].

In reference to the authors Walaa Abu-Marie et al [3], the BMP file has a specific structure as follows, each bitmap file contains,

1. Bitmap header,
2. Bitmap information header,
3. Color table and
4. Array of bytes

BMP Header File

This is the file that stores common data about the BMP file and also it is at the start of the file. This file is identified by BITMAPFILEHEADER. The role of header file is to identify whether the file is the bitmap file. It contains data about,

1. Type of the bitmap file,
2. Actual Size of the bitmap file and the
3. Layout of the bitmap file.

Information Header

Information Header is defined by BITMAPINFOHEADER that says information on application based data about the image.
This structure specifies,

1. Compression type,
2. Dimension,
3. Color format.

Color Table

This color table has the definition of the colors that are used throughout the bitmap. This is identified by RGBQUAB structure. The color table should specify the colors in order that are most significant. According to the reference to the authors of E Lin, E Delp [4], LSB has the following advantages and disadvantages,

Advantages of LSB

1. Less suspicious to human eyes.
2. Simple to implement and many techniques uses this method.
3. High perceptual transparency.

Disadvantages of LSB

1. Three weakness- Robustness, Tamper and Resistance.
2. Extremely sensitive to any kind of filtering.
3. Scaling, Rotation, Cropping, adding extra noise lead to destroy the secret message.

2.3. Transform Domain (Frequency Domain)

In steganography, data is embedded in the transform domain. There are different file formats available in transform domain but JPEG file format is most popular among the others. The reason is that the size of the JPEG image is very small. Transform domain is more robust when compared to the image domain [21].

Transform Domain Techniques

Discrete Cosine Transform

The DCT technique plays a vital role in JPEG compression technique. For example, an image is split into 8X8 squares. Each square is transformed through DCT which produce 63 coefficients multi-dimensional array of outputs as shown in the figure 3. Now, the coefficient is rounded by quantized value. By using the Huffman encoding schemes the further compression can be done [13].

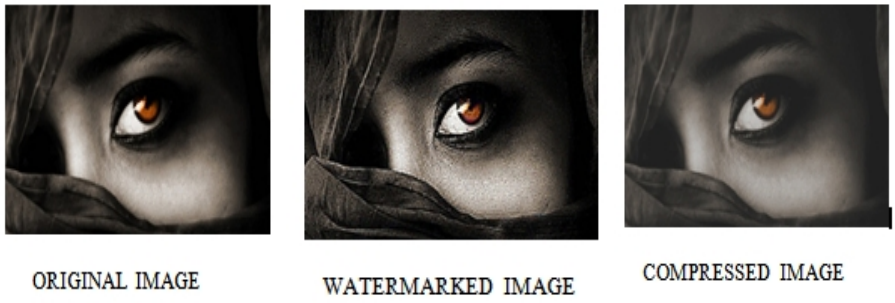

Figure 3. DISCRETE COSINE TRANSFORM

In reference to the authors, Blossom Kaur, Amandeep Kaur, Jasdeep Singh[5]:

The watermark is embed with the mid frequency band of DCT block which carrying the low frequency components. It is inserted by adjusting the DCT Coefficients of the image and using the private key.

Watermark is again extracted using the same private key without restoring the original image.

In this paper the watermarking for the digital information is used .This operates in the frequency domain and a selected set of DCT co-efficient are taken and which embeds the pseudo random sequence of real numbers without changing the original image using the statistical properties the information/message is got back.

In reference to the authors, J.K.Mandal [6]:

Transformed domain based grace scale authentication technique which is done using the Z- Transform. Each bit of the hidden image is embedded to the fourth LSB transformed Co-efficient of the source image. While embedding, the dimension of hidden image and message content are added.

In reference to the authors, Jianjua Song, Yong Zhu and Jianwei Song[7]:

This paper is based on Logistic map in DCT domain. Message encrypted using Logistics Chaotic Sequence and it is inserted in the middle frequency coefficients in DCT Domain. Extracting of the information is made without the use of original image.

3. Steganalysis

Steganalysis method is used to attack the steganographic methods by extracting, separating or detecting the embedded information. For different application different steganalysis methods are used. The different attacks are:

1. Stego only – extract only stego image
2. Known carrier – extract carrier and stego image
3. Known payload – known the protected message in the embedded file
4. Chosen stego – extract by using tool
5. Chosen payload – it is a most powerful and efficient tool among other different attacks [23][24].

3.1. Steganalysis Tools

Various tools are available for steganalysis [25].

3.1.1. Digital invisible tool kit:

It is a java based steganography tool capable of hiding information in a 24 bit color image. This tool also performs statistical analysis.

steganography analyzer signature scanning (StegAlyzerSS):

This tool efficiently scans the existence of hexadecimal byte patterns in a Stego File.

steganography analyzer artifact scanner (StegAlyzerAS):

StegAlyzerAS scans a file system as a whole or a single file system on a Stego File.for the existence of the embedded information in the Stego File.

Invisible Secret tool:

This tool is not only encrypt the message but also used for secure transformation over the internet. Using Invisible Secret tool not evens the hackers or intruders came to know the embedded information in the Stego File. In this paper Invisible Secret tool is analyzed [13]:

Step1: Select Action
Step2: Select Carrier File
Step3: Select Source File
Step4: Encryption Settings
Step5: Target File Settings
Step6: Encryption or Hiding

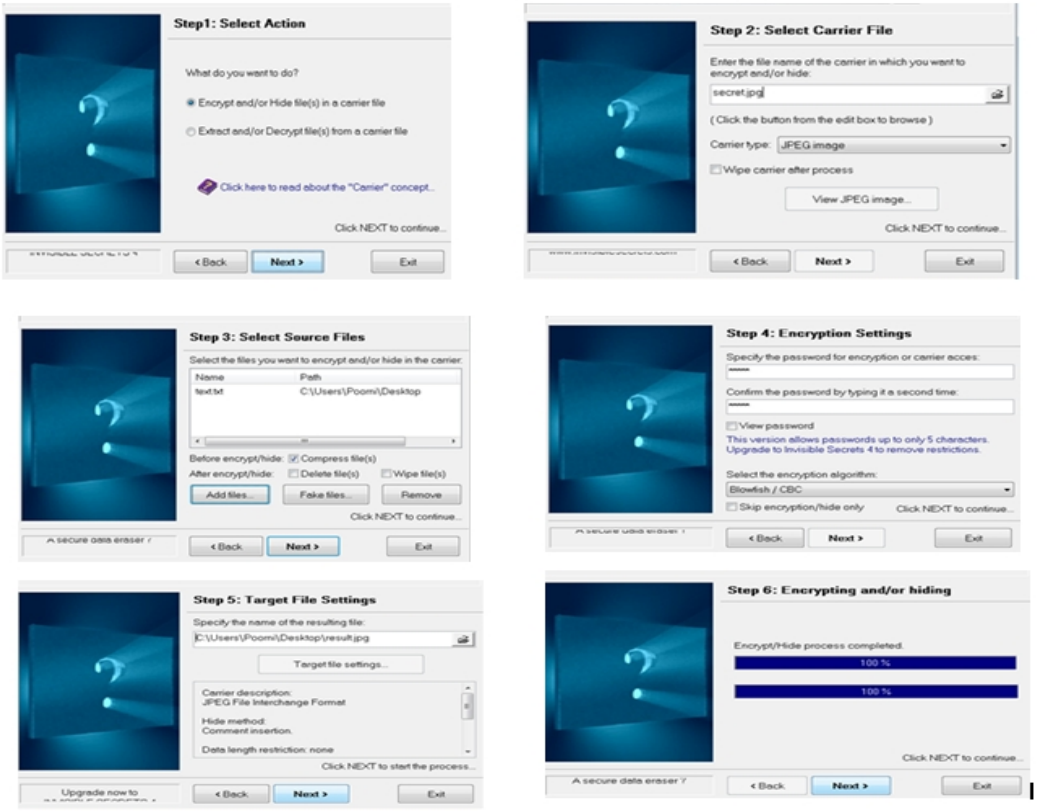

Figure.4. Screen Shots of Invisible Secret Tool

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.

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 [8].

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[9].

6.CONCLUSION

This paper provides the novel approaches for implementing Digital Image Steganography, that is to conceal secret information inside an image so that it invisible to the eyes. This paper provides efficient steganography methods, so that the person can find the variety of choosing the method to protect the information. In Image Domain, we discussed the most powerful technique called LSB to hide information particularly inside a BMP file format whereas in Transform Domain powerful DCT (Discrete Cosine Transform) was discussed. We also discussed the tool called Invisible Secret to perform Steganalysis. Finally this paper ends with Application of steganography.

REFERENCES

[1]. T. Morkel 1, J.H.P. Eloff 2, and M.S. Olivier 3, an overview of image steganography, Information and Computer Security Architecture (ICSA) Research Group.

[2]. Walaa Abu-Marie, Adnan Gutub and Hussein Abu-Mansour, Image based steganography using Truth Table Based and Determinate Array on RGB Indicator, International Journal of Signal and Image Processing (Vol.1-2010/Iss.3) Abu-Marie et al. / Image Based Steganography Using Truth Table Based and Determinate … / pp. 196-204

[3]. Abbas Cheddad, JoanCondell, KevinCurran and PaulMcKevitt, Review on Digital image steganography, http://www.ece.purdue.edu/~ace, or +1 765 494 1740.

[4]. Eugene T. Lin and Edward J. Delp, A Review of Data Hiding in Digital Images, 0165-1684/$-seefrontmatter & 2009ElsevierB.V.Allrightsreserved. doi:10.1016/j.sigpro.2009.08.010.

[5]. Blossom Kaur, Amandeep Kaur and Jasdeep Singh, Steganographic Approach For Hiding Image In DCT Domain, International Journal Of Advances In Engineering & Technology, July 2011. 72 vol. 1,issue 3,pp.72-78

[6]. J. K. Mandal , A Frequency Domain Steganography Using Z Transform (FDSZT)

[7]. Jianhua Song, Yong Zhu And Jianwei Song, Steganography: An Information Hiding Method Base On Logistic Map In DCT Domain, Advances In Information Sciences And Service Sciences(AISS) Volume4, Number2, February 2012, Doi: 10.4156/AISS.Vol4.Issue2.5

[8]. J. Flores-Escalante, J. Pérez-Díaz and R. Gómez-Cárdenas, Design and Implementation of An Electronic Identification Card, Journal Of Applied Research And Technology

[9]. Aravind K. Mikkilineni, Osman Arslan , Pei-Ju Chiang, Roy M. Kumontoy, Jan P. Allebach, George T.-C.Chiu, Edward J. Delp, Printer Forensics using SVM Techniques , This research was supported by a grant from the National Science Foundation, under Award Number 0219893

[10]. Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay And Sugata Sanyal, Steganography and Steganalysis: Different Approaches, Available from: http://arxiv.org/ftp/arxiv/papers/1111/1111.3758.pdf

[11]. Mrs. Gyankamal J. Chhajed Ms. Krupali V. Deshmukh Ms. Trupti S. Kulkarni, Review on Binary Image Steganography and Watermarking, Gyankamal J. Chhajed et al. / International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 11 November 2011 3645.

[12]. J.C. Judge, Steganography: Past, present, future. SANS Institute publication, http://www.sans.org/reading_room/whitepapers/stenganography/552.php, 2001.

[13]. Invisible Secret Tool is available from : http://www.invisiblesecrets.com/download.html

[14]. Mrs. Sivaranjani ,Ms. Semi Sara mani, 2011, Edge Adaptive Image Steganography BasedOn LSB Matching Revisited, Journal of Computer Applications (JCA) ISSN: 0974-1925, Volume IV, Issue 1.

[15]. Gyankamal J. Chhajed et al. Review on Binary Image Steganography and Watermarking International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3 No. 11 November 2011 3645.

[16]. S.K.Muttoo and Sushil Kumar, A Multilayered Secure, Robust and High Capacity Image Steganographic Algorithm, World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 6, 239-246, 2011 .

[17]. Anjali A. Sheju and Umesh L. Kulkarni . A Secure Skin Tone based Steganography Using Wavelet Transform International Journal of Computer Theory and Engineering, Vol.3, No.1, February, 2011, 1793-8201

[18]. P. Mohan Kumar and K. L. Shanmuganathan. Developing a Secure Image Steganographic System Using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate, Journal of telecommunication and information technology 2011.

[19]. Steganography And Digital Watermarking , Copyright © 2004, Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The University of Birmingham.

[20]. B. Karthikeyan et al, School of Computing, SASTRA University, LSB Replacement Stegnography in an Image using Pseudo randomized Key Generation Research Journal of Applied Sciences, Engineering and Technology 4(5): 491-494, 2012 ISSN: 2040-7467 © Maxwell Scientific Organization, 2012
Submitted: October 26, 2011 Accepted: November 25, 2011 Published: March 01, 2012

[21]. Hide and seek: an introduction to steganography published by the ieee computer society 1540-7993/03/$17.00 © 2003 ieee . ieee security & privacy.

[22]. Mamta Juneja, Parvinder Sandhu Department of Computer Science and Engineering, Rayat and Bahra Institute of Engineering and Biotechnology, Implementation of Improved Steganographic Technique for 24-bit Bitmap Images in Communication, Marsland Press Journal of American Science 2009:5(2) 36-4236.

[23]. Bin Li Junhui He Jiwu Huang, A Survey on Image Steganography and Steganalysis, Journal of Information Hiding and Multimedia Signal Processing c 2011 ISSN 2073-4212 Ubiquitous International Volume 2, Number 2, April 2011,received July 2010; revised October 2010.

[24]. Angela D. Orebaugh George Mason University, A Steganography Intrusion Detection System

[25]. Pedram Hayati1, Vidyasagar Potdar, and Elizabeth Chang, A Survey of Steganographic and Steganalytic Tools for the Digital Forensic Investigator, Institute for Advanced Studies in Basic Science of Zanjan, Iran 2 Digital Ecosystems and Business Intelligence Institute, Curtin Business School, Curtin University of Technology, Perth, Australia.

AUTHORS

R.POORNIMA[1] received the degree in information technology from M.I.E.T Engineering college in 2011. Currently, she is a M.Tech student at Sastra Uiversity. Her interests are in Steganography and RFID.

R.J.ISWARYA[2] received the degree in information technology from Sri Ramakrishna Institute Of Technology in 2011. Currently, she is a M.Tech student at Sastra Uiversity Her interests are in Steganography and data mining.