International Journal of Scientific Research in Science, Engineering and Technology (www.ijsrset.com)
© 2020 IJSRSET | Volume 7 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
DOI : https://doi.org/10.32628/IJSRSET20726

Review of Steganography Algorithms

Ali Mohammed Ahmed, Ibrahim Mahmood Rashid
Assistant lecturer, Collage of Agriculture, Telafer University, Nineveh, Iraq

ABSTRACT

The ability to hide plays a vital role in effective secret communication. This is achieved by hiding information (Steganography). The science of concealing information is the science of concealing information in other information so that it appears that hidden information is not something to the human eye. There are many ways to hide information within an image, audio / video, document, etc. But hiding information in pictures has its own characteristics and is the most popular among others. This paper provides a review of several methods, such as image field and conversion field algorithms available to implement image information hiding (Steganography). In this paper, high-capacity information hidings schemes are analyzed for different file formats. Secret communication is done before Password encryption to protect information. The intended recipient will decrypt the information using this password.

Keywords : Steganography, Encryption, Image Domain, Transform Domain.

I. INTRODUCTION

During the last two decades, the fast development and deployment of internet requires secret Information that needs to be protected and secured from the unauthorized users. This is achieved through Data hiding. It is a method and a way of hiding secret messages into a cover medium so that an unwanted observer will not realize of the existence of the hidden messages. This is accomplished by steganography. It is retrieved from the Greek words it's known as the term of steganography and means the cover, the *grafia* means *writing* defining it as *covered writing.*

Both steganography and cryptography are used to conceal information. The user will not reveal any suspicious about the hidden information this is the use of steganography, this distinguishes between steganography and cryptography. Therefore the attackers will not try to decrypt information. The various methods of steganography will be reviewed in this paper such as image, video, audio, text, to hide the information.

Watermarking and Fingerprinting are other two techniques that seem to be same as Steganography. Both these techniques sound to be same and provide same end goals but both have different mechanism. The technique of using each copy of the content and make it as unique to the receiver called Fingerprinting. Whereas allow a person to provide hidden copyright notices or other verification licenses called Watermarking.

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.

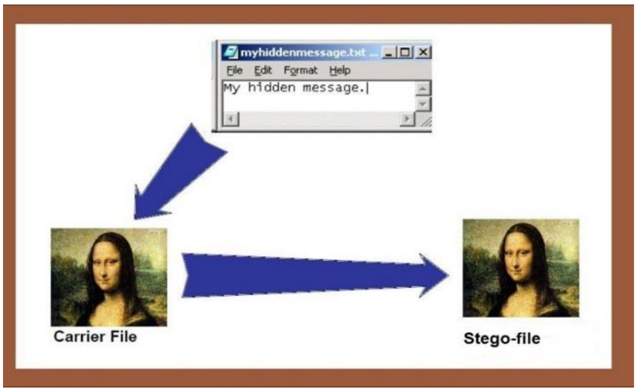
Let us assume an example for a cover text:

"Safe education creates rapid educated transmission, date after tomorrow darling".

"Secret data" This is the result of we assembled the first letter of all the words to produce an encrypted Message of the above sentence. In different approaches the cover medium can be hidden in similarly encrypted message.

1.1. Embedding Process of Steganography

In to the carrier file the information should be hidden and this is our goal in this paper.
stego file is The file that contains the embedded information inside of it . The information hiding here is text file (confidential information).for file video, audio, image etc. we can hide different types similarly. It is represented in Fig.1.



My hidden message.

Figure1. Embedding Process of Steganography

1.2. Era of Steganography

1. Germans developed the Microdot technology during the cold war two which prints the clear good quality photographs shrinking to the size of a dot.
2. To send message In Greece they select a person by shaving their heads off. They used to let their hair growing up but before that they write a secret message on their head.
3. The secret message was written in invisible Ink during the world war two so that the paper appears to be blank to the human eyes. By heating the liquids such as milk, vinegar and fruit juices the secret message is extracted back.

1.3. Steganography Types

Fragile and Robust are the types of steganography,

1.3.1 Fragile

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

1.3.2 Robust

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

1.4. ALGORITHMS USED IN STEGANOGRAPHY

Four algorithms currently are implemented, some filter the image first and some use least significant bit steganography.

1.4.1 BLINDHIDE

The simplest way to hide information in an image is blindhide. The mechanism of it is just starts at the top left corner of the image and works its way across the image (then down - in scan lines) pixel by pixel so it's blindly hides. To decode the process the least significant bits starting at the top left are read off. This is not very secure - it's really easy to read off the least significant bits. It also isn't very smart - if the message doesn't completely fill up the possible space than just the top part of the image is degraded but the bottom is left unchanged - making it easy to tell what's been changed.

Algorithm Pixel Swap

- If we randomly select 2 pixels x1 and x2 from the cover image using a pseudo–random sequence.

- If the two pixels lie within a specified distance α (α=2 or a=3 generally), they are suitable for embedding, otherwise generate another set of pixels.
- Pick up the message bit. If the message bit is zero (or one), check if x1 > x2 otherwise swap x1 and x2. Does the reverse operation for the message bit one (zero).
- For decoding, select the pixels using the same pseudo-random sequence. Check if the 2 pixels are within the pre-specified range α. If x1>x2, the message bit is zero (one) otherwise the message bit is one (zero).

Inherently without applying separate restoration process this scheme preserves the first order statistic (histogram). Any visual distortion to the image this scheme also does not add since the threshold used for swapping of pixels is kept considerably small (α <=5) which only affects the least significant bit planes of an image. To measure the distortion introduced by the embedding in the cover image, the Peak Signal to Noise Ratio (PSNR) after embedding was observed for one hundred images.

1.4.2 HIDE SEEK

To distributes the message across the image use this algorithm. After "Hide and Seek" It is named - a Windows 95 steganography tool that uses a similar technique. To generate a random seed it uses a password, then uses this seed to pick the first position to hide in. until it has finished hiding the message it continues to randomly generate positions. You have to try every combination of pixels in every order to try and "crack" the algorithm - unless you have the password so it's a little bit smarter about how it hides. It is not looking at the pixels it is hiding in - it might be more useful to figure out areas of the image where it is better to hide in so it's still not the best method.

1.4.3. FILTER FIRST

The duty of this algorithm is filtering the image using one of the inbuilt filters and then hides in the highest filter values first. To retrieve the message it doesn't require a password and It is essentially a fancier version of BlindHide. We need to be careful about filtering the picture because we are changing the pixels so we don't want to use information for filtering that might change. If we do, then it may be difficult (if not impossible) to retrieve the message again. The most significant bits will filter by this algorithm and leaves the least significant bits to be changed. Because using the filter ensures we are hiding in the parts of the image that are the least noticeable so it is less noticeable on an image.

1.4.4. BATTLE STEG

It is the best of all. This algorithm performs "Battleship Steganography". After uses the highest filter values as "ships" It first filters the image. The algorithm then randomly "shoots" at the image (like in HideSeek) and when it finds a "ship" it clusters its shots around that hit in the hope of "sinking" the "ship". Then it moves away to look for other ships. The effect this has is that the message is randomly hidden, but often hidden in the "best" parts to hide in thanks to the ships. To look for other ships it moves away so that we don't degrade an area of an image too greatly. Because you need a password to retrieve the message it is secure. It is fairly effective because it is hiding (if you set the values right) the majority of the information in the best areas.

II. METHODS AND MATERIAL

Steganography in Image

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

2.1. Data Compression

"**Lossy**" is one of different compression algorithm and it is used to reduce the amount of information to be transmitted. This is in image. 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.

Any information from the target image will never discarded by "**Lossless**" Compression, this is on the other hand. Even after the image is decompressed.GIF (GRAPHICAL INTERCHANGE FORMAT) and BMP (BIT MAP FILE) are image format that follows Lossless Compression. All the information can be restored.

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

2.2. Image Domain (Spatial Domain Technique)

2.2.1. LSB (Least Significant Bit)

In encrypting and decrypting the secret information is LSB and it is common technique. It is a method based on altering the redundant bits that are least important with the bits of the secret information. Without knowing to the intruder that the message is being passed to transmit the secret information to the receiver the aim of the LSB comes.

2.2.1.1. LSB IN BMP (BIT MAP FILE)

Because BMP images have good quality and high resolution LSB using 24-bit BMP file format is suitable and efficient 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].

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

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

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 header file has a role it is to identify whether the file is the bitmap file. It contains data about,

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

Information Header

By BITMAPINFOHEADER Information Header can be defined that says information on application based data about the image.
This structure specifies,

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

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

Disadvantages of LSB

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

2.3. Transform Domain (Frequency Domain)

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

Transform Domain Techniques

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

ORIGINAL IMAGE

WATERMARKED IMAGE

COMPRESSED IMAGE

Figure 3. DISCRETE COSINE TRANSFORM

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.

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

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

In this paper for the digital information the watermarking 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.

Transformed domain based grace scale authentication technique which is done using the Z- Transform. To the fourth LSB transformed Coefficient of the source image each bit of the hidden image is embedded. This is In reference to the authors, J.K.Mandal [6]:

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

III. RESULTS AND DISCUSSION

Steganalysis

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

1. Known payload – known the protected message in the embedded file
2. Stego only – extract only stego image
3. Chosen stego – extract by using tool
4. Known carrier – extract carrier and stego image
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:

In a 24 bit color image digital invisible tool kit is a java based steganography tool capable of hiding information. 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.

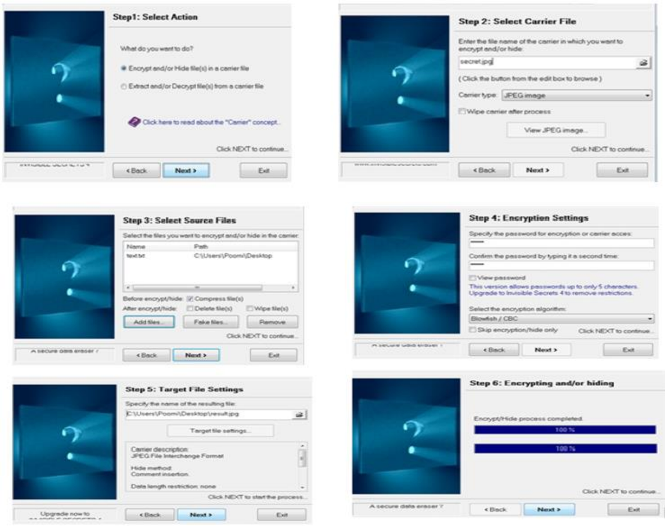
Steganography analyzer artifact scanner (StegAlyzerAS):

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.

This tool is used for secure transformation over the internet not only encrypt the message.

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



Step1: Select Action

What do you want to do?

● Encrypt and/or Hide file(s) in a carrier file

○ Extract and/or Decrypt file(s) from a carrier file

Click here to read about the "Carrier" concept...

Click NEXT to continue...

Step 2: Select Carrier File

Enter the file name of the carrier in which you want to encrypt and/or hide:

secret.jpg

(Click the button from the edit box to browse)

Carrier type: JPEG image

□ Wipe carrier after process

Click NEXT to continue...

Step 3: Select Source Files

Select the files you want to encrypt and/or hide in the carrier:

Name	Path
text.txt	C:\Users\Poomi\Desktop

Before encrypt/hide: ☑ Compress file(s)

After encrypt/hide: □ Delete file(s) □ Wipe file(s)

Click NEXT to continue...

Step 4: Encryption Settings

Specify the password for encryption or carrier acces:

Confirm the password by typing it a second time:

□ View password

This version allows passwords up to only 5 characters. Upgrade to Invisible Secrets 4 to remove restrictions.

Select the encryption algorithm:

Blowfish / CBC

□ Skip encryption/hide only

Click NEXT to continue...

Step 5: Target File Settings

Specify the name of the resulting file:

C:\Users\Poomi\Desktop\result.jpg

Carrier description:
JPEG File Interchange Format

Hide method:
Comment insertion.

Data length restriction: none

Click NEXT to start the process...

Step 6: Encrypting and/or hiding

Encrypt/Hide process completed.

100 %

100 %

Click NEXT to continue...

Figure 3. Screen Shots of Invisible Secret Tool

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:

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

Covert Communication:

The information passes In general covert channel 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. Into all pages very small yellow dots are inserted in those printers. Inside the yellow dots like serial number, date and time stamp, Information is hidden. In laser printer for watermarking the confidential information Property is available [9].

IV. CONCLUSION

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

V. 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

[14]. 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.

Cite this article as :

Ali Mohammed Ahmed, Ibrahim Mahmood Rashid, "Review of Steganography Algorithms", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 2, pp. 01-09, March-April 2020. Available at doi : https://doi.org/10.32628/IJSRSET20726
Journal URL : http://ijsrset.com/IJSRSET20726