International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 10485-10490
© Research India Publications. http://www.ripublication.com

Steganography Methods on Text, Audio, Image and Video: A Survey

Aryfandy Febryan[1], Tito Waluyo Purboyo[2] and Randy Erfa Saputra[3]

*[1,2,3]Department of Computer Engineering, Faculty of Electrical Engineering,
Telkom University, Bandung, Indonesia.*
[2]Orcid: 0000-0001-9817-3185, [3]Orcid: 0000-0002-8537-2086

Abstract

Steganography is technique and art of hiding a secret message in carrier file so the existence of the secret messages cannot be known. During the last few decades, there have been a large number of papers that already published by all different research. If anyone knew the existence of the secret message with its carrier file then steganography is failed. This paper will be discussing the various types and techniques of steganography on text, image, audio, and video as a media.

Keywords: Steganography, Steganalysis, LSB, Spread Spectrum, DCT, DWT. Parity Coding, Phase Coding, Echo Hiding, Hash-LSB

INTRODUCTION

Words of steganography are divided into “stegos” and “grafia” which each has meant “cover” and “writing” combine the word become “covered writing” [2]. In Steganography there are two important parts, part one is the compression or embedding and part two is decompression or extracting of the data. Steganography is also an art and science of covered writing and its techniques are is use from hundreds of years.

Steganography is not a new term but has been used thousands of years ago. This is a technique for allowing two or more people to silently communicate with each other by hiding any secret message on a media cover. Files used as media can be text, audio, image or digital video formats. The secret message embedded in the media cover using the appropriate algorithm and demanding the stego file itself to be sent to the receiver [1].

There are some important things to be kept in mind before applying or performing the procedure of steganography:

a. Embedding Capacity: Data is embedding in a larger data called cover or carriers file. The carrier that used is computer files, such as image, audio, video even text files without affecting its original quality. The embedded capacity is the amount of data can be hidden or embedded on the cover and will be compared to the cover size, because if the size of data that will be inserted on the cover is greater than the cover size then steganography can’t be done [1][2].

b. Undetectability: Data should be hidden or embedded into a carrier file in such way that any secret message or information can’t be seen accidentally in the original file by anybody. If anyone detects the message in the original file then the steganography is failed [1].

c. Robustness: This is the capability of the embedding algorithm to store embedded data even after going through the process of compression and decompression a file [1].

d. Security: In most cases, security, including perceptional transparency of the hidden data is considered the most important issue of hiding data in any different formats [2]. The definition of security in steganography cases is as likely to be embedded secret messages unknown to outsider people that have no connection between sender and recipients.

e. Tamper Resistance: Resistance to intentional malfunction or sabotage of a product or system by users that have access to it. There are many reasons why tamper resistance is so important. One of the important things for steganography is how strong the carrier file that used for embedding a secret message or file will not easy to be cracked by users.1. Concealment of a secret message is done by the method of LSB (Least Significant Bit) and adaptive.

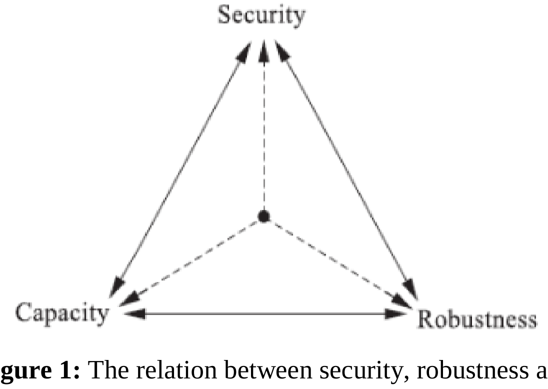

Figure 1: The relation between security, robustness and capacity [2]

In Figure 1, there is relation of security, robustness, and capacity have a contradiction that can't be independently adjusted. For example, increased capacity from data hiding will lead to decrease the robustness and security itself [2].

TYPES OF STEGANOGRAPHY METHODS

There are various types of steganography methods and techniques which used for embedded a file called as cover or carrier:

A. Text Steganography: It hides the text behind some other files, changing the format of an existing text within a file, to change the words within the text or to generate random character sequences [1][5].

Basically here we use a text file as a cover media to embed the secret information. It is more vulnerable to attack as it can be easy for an attacker to detect the pattern, text steganography its self is has this following three categories such as [1][6] :

a. Format Based Methods, in this method text data is embedded in the carrier text by changing the format of the cover text itself.

b. Linguistic Methods, in this method just doing analysis the linguistic.

c. Random and Statistical generation methods, generating its carrier text according to the statistical and embedding the information in random sequence of characters.

Text steganography is the most difficult kind of steganography because a text file lacks a large scale redundancy of information in comparison to other digital medium like image, audio and video [6]. Many languages are use to hide data like Persian, Arabic, Hindi, English etc.There is characteristic of English language such as inflexion, use of periphrases and fixed word order. Conversion means that with minimum change of the word will make the relationship of the words into a sentence may be indicated [6].

B. Image Steganography: The process of concealment of information into the carrier image in the absence of degradation in the image and make the image robust enough to not let the users who have nothing to do with this information cannot access it. The secret message is embedded into a carrier image as a noise because human eyes can not detect a difference between the original image and stego image [15][16].

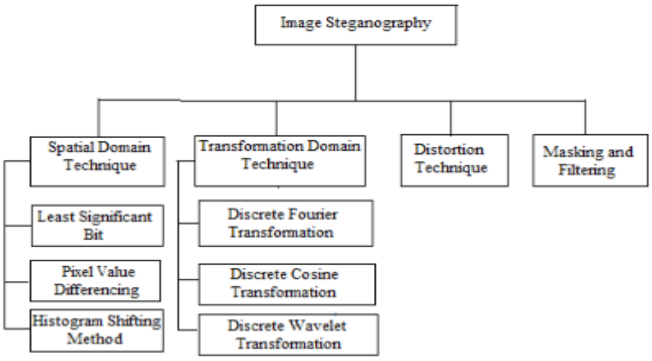
Image Steganography
Spatial Domain Technique
Transformation Domain Technique
Distortion Technique
Masking and Filtering
Least Significant Bit
Pixel Value Differencing
Histogram Shifting Method
Discrete Fourier Transformation
Discrete Cosine Transformation
Discrete Wavelet Transformation

Figure 2: Image steganography techniques [15]

In figure 2, explain about classification of image steganography such as:

a. Spatial Domain Technique, for hiding the data some bits are directly changed into the image pixel values bitwise also include, the intensity of pixels and noise manipulation. There are many ways to perform embedding file in Spatial Domain, the easiest is Least Significant Bit (LSB) [15][16].

b. Transformation Domain Technique, this technique has a threat like an image processing operations (compression, docking and enhancement) to this technique, because of that transformation domain is hides the secret message in the significant area in the carrier image.

c. In the transformation domain, the first thing to do is convert the image from spatial domain into transformation domain and then the secret message is embedded into carrier image. These techniques hide data by mathematical functions [15][16].

d. Distortion Technique, the information is embedded and store in signal distortion. This technique requires knowledge and carefulness in looking different between the original carrier image and stego image after information embeds during process of decoding [15].

e. Masking and Filtering, the image with 24bit of size or greyscale type is usually applying masking and filtering technique and using different applications to hide a message. Hiding information by marking the image, this technique is similar to paper watermark, this technique imparts information in a more significant image area than just hiding in the noise level.

C. Audio Steganography: Human Auditory System(HAS) is more sensitive than Human Visual System(HVS), that is one of the reasons that makes embedding message in audio file in any different method is more difficult than other formats [1].

These are the most common method that uses for embedding process in audio file:

a. LSB Coding

b. Parity Coding

c. Echo Data Hiding

In Audio steganography, there is some format that can use as a cover media for embedding the file such as MP3, WAV, MIDI etc.

D. Video Steganography: hiding or embedding message in the video is like an art of hiding information because the sender is not only hiding but how that message is prevented open by anyone except receiver. Hiding message in the video is part of the art of hiding information, that avert the revealing of hiding messages. Video-based steganography techniques are same like image based, its classified into spatial domain and frequency domain based methods [12][13].

Holding capacity and imperfection in video steganography are two important things that use for evaluating the performance. The results have advantage in steganography capacity when using spatial domain algorithm and directly embedding the information into the carrier image with no visual changes and good quality. Transformation domain algorithm is embedding the secret information in the transform space and the advantage of this algorithm is good stability, but with small capacity [1][13].

VARIOUS METHODS OR TECHNIQUES IN STEGANOGRAPHY

A. Text Steganography Methods

There are various techniques of text steganography :

a. Selective Hiding: It hides the characters on the first or any specific location characters of the words to combine that character and helps to extract the text. This technique requires huge amount of plain text [17].

b. HTML Web Pages: Hide the text by using the attributes in HTML, the character is then used to retrieve the original text.

c. Hiding Using Whitespaces: Smaller number of whitespaces between words can be determined that whitespace is 0, but if more numbers of whitespaces between words may determine a 1.

d. Semantic Hiding: Uses synonyms to hide the message [17].

B. Audio Steganography Methods

There are various techniques of audio steganography :

a. LSB Coding: The least significant byte of carrier file is replaced with the bytes of the secret message. Generally why the rightmost bit is chosen for the replacement, because considered as the LSB as it has the least impact on the quality of file [1].

b. Parity Coding: The parity bit of the cover file is checked for similarity, if similarity exists then no action will be done and if the dissimilarity exists then any bit LSB will be slightly changed (cover file or secret message) to make parity equal [1].

c. Echo Data Hiding: The information is inserted by adding an echo sound to the cover file. Embedding data is expressed in terms of decay rate, initial amplitude and delay [1].

a) The initial amplitude is used to determine the original data sound.

b) Decay rate is useful for determination of echo function to be made.

c) The Offset function is used to determine the distance between the original speech signals with the echo that has been made.

d. Spread Spectrum: The secret message is encoded and distributed to every available frequency spectrum. Sending a narrow band of information signal on existing broadband channels [11]. The signal spread is used to increase the level of redundancy of signal, the amount of redundancy will be determined by the value of scalar multiplier called cr. The value of the length of bits is the length of the scalar value of cr [11].

e. Direct Sequence Spread Spectrum: A signal of low bandwidth is spread over a broad frequency range. Signal will be lost and decrease from the signal strength in a noise from a carrier media [10]. To extract the embedded signal in the carrier file, the receiver side requires more knowledge of the deployment process. This knowledge can be analogous to the kind of secret key requires as input to the system. But the sender also must have the knowledge to embed the secret message into a cover media, so the secret message has characteristics such as hard to know but easy to crack it for the receiver (temper resistance) [10].

f. Phase Encoding: the block of phase spectrum as a place for embedding the message that gets from dividing the original signal of audio stream or carrier file, that is part of basic ide from phase encoding [17].

Procedure of Phase Coding is:

i. The original sound signal (C) segmented into the header of the signal. The rest is broken up into smaller segment whose have lengths equal to the size of the message that will be encoded into a cover media.

ii. Applying each of segments to create a matrix of the phase is from Discrete Fourier Transform (DFT).

iii. The formula that can calculate the value of new phase with message bit condition as follows :

$$New\ Phase = \begin{cases} Old\ Phase + \dfrac{\pi}{2}\ if\ message\ bit = 0 \\ Old\ Phase - \dfrac{\pi}{2} if\ message\ bit = 1 \end{cases}$$

Old phase is get from the original sound signal and message bit is the length of message that will encode into a cover media.

iv. Using first segment and the original phase of matrix can create a new phase of matrix.

v. Using the new phase of the matrix, the sound signals are reconstructed by applying an inverted DFT and then combine a segment of a sound in the original order.

C. Image Steganography Methods

There are various techniques of image steganography :

a. Least Significant Bit Substitution, LSB steganography of the carrier medial data is used to embed the secret message. LSB Substitution is the easiest and simple of the steganography techniques [7].

There is example for LSB, using 8-bit grayscale bitmap image each pixel is performing as a byte, the beginning of eight pixels on the original values [7]:

11100110

10101001

00100010

11011001

10101011

01001010

10010001

11010011

Insert alphabet "A" in this grayscale pixels, as we know that binary of A is 01000001. We should replace the right of the bits on these greyscale pixels to get the new values:

11100110

10101001

00100010

11011000

10101011

01001010

10010000

11010011

The human eye will not recognize if it is different between carrier image and stego image [7].

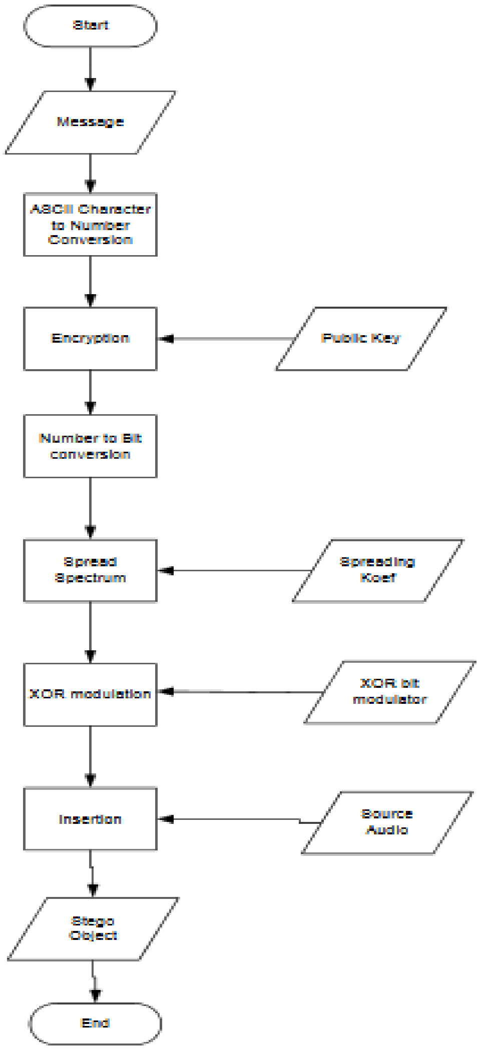

Figure 3: Steganography Process in this study [11]

There is a procedure that explain in figure 3, when doing steganography in this study, first thing you have to get your message and then convert the message into a number conversion. But don't forget to get your public key to encryption the message first before converting into a bit, After we calculate a value we will get Spreading Koef to count the spread spectrum of the message with XOR modulation after we get a file after the modulation we can insert the audio that we choose as a carrier media or sound and then we got our stego object.

b. Discrete Cosine Transform (DCT), the most popular techniques of embedding, mostly because the format of an image will be publicly available as a common type of output format from a digital camera [7].

There is an example like this, a successive 6 * 6 pixels block of the image into 36 DCT in JPG image format for color components that will be coefficients for discrete cosine transform (DCT). Coefficients of DCT is F (u, v) that will get from 6*6 block pixel are given by

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{6}\sum_{y=0}^{6} f(x,y) * \cos\frac{(2x+1)u\pi}{12}\cos\frac{(2y+1)v\pi}{12}\right]$$

Give assumption that u = horizontal spatial frequency; v= vertical spatial frequency.

$$C(x) = \begin{cases} \frac{1}{\sqrt{2}} & if\ x = 0 \\ 1 & if\ x > 0 \end{cases}$$

This C(x) will have value 1/√2 when x is 0. Otherwise C(x) will have value 1 when x is 1 [7].

c. Discrete Wavelet Transform (DWT), used to transform the image from spatial domain to its frequency domain. To get a wavelet domain or DWT from the carrier image, use a pair of a filter that called an analysis pair of filter. First, a low-pass filter is applied to each row of data to obtain a low-frequency component and then a high pass filter is applied to the data path that has the same pass component. Furthermore, the component that we got is separated and then embed into the low-pass component [7].

d. Spread Spectrum, the minimum required is needed to spread the message over a wide frequency [7].

To produce stego image in spread spectrum steganography, embed the message in noise and combine it with the cover image. The embedded image is hard-to-known with a human eye [7].

e. Hash-Least Significant Bits (Hash-LSB), determines the positions of LSB on RGB pixel and the information will be embedded into RGB pixel. The carrier image will be split or fragmented into an RGB format as well [7]. Convert the secret message into a bit; each 8 bits will be embedded in the least significant bits in RGB [7].

D. Video Steganography Methods

There are various techniques of video steganography :

a. Video Steganography by LSB substitution using different polynomial equations, Least significant bit (LSB) operates on LSB bit from media files to embed into a carrier file.

b. Video Steganography using 32 * 32 vector quantization of DCT, One method that is capable of operating 32 * 32 is the quantization of DCT vectors. The first step is that all videos are sliced differently in the number of images. After all the sliced images are passed to the 32 * 32-pixel management procedure followed by the through quantitative LSB methods [13].

The text message to be planted converts first to ASCII, encoded as a bit to make it more compatible according to the video vector. The idea is to fill the bits that used to occupy the low intensity and if there are still left pinned into the high intensity-bits. The embedding bit scheme is finally done by IDCT [13].

c. A high-capacity video steganography based on integer wavelet transform, The proposed system uses integer wavelet transforms on the cover image to obtain stego-images [13]. The proposed algorithm capacity is further enhanced by a set of confidential imagery is considered [13].

d. Video Steganography using dynamic cover generation, A new steganographic system where the cover media itself is produced by the system instead of using the existing cover and some data is the cover itself and the rest is embedded in the cover.

FUTURE WORKS

Pure steganography is a process for embed a file or information into the object with or without using private keys. This type of steganography depends on the carrier or secret information file itself, use cover or carrier file as a place to be embedding a file, personal information is transmitted and using an encryption algorithm to make it strong.

The goal of steganography is to hide messages in such a way that no one apart from intended recipient even known that a message has been sent.

The future work on this project is to improve the compression ratio of all format steganography such as text, audio, image and video in any different methods or techniques that already been reviewed in this paper review and we can combine all of techniques steganography in this paper review, to make the information is robust enough.

CONCLUSION

Steganography is a technique to embedding a secret information or message from sender to the receiver with media as it covers to embed, because of steganography it's not so easy to learn so the sender and the receiver has to understand the knowledge of technique steganography in any formats and in any conditions. Security of the information that we talk with other people is important to be protected. Because the information that we talk with other people is important and so confidential. If other people are knowing this information, so the security of this information must be gone wrong. The success of steganography is assessed on the basis of information security that no one else will know.

REFERENCES

[1] PrashantJohri, Amba Mishra, Sanjoy Das, Arun Kumar, "Survey on Steganography Methods (Text, Image, Audio, Video, Protocol and Network Steganography" 2016 International Conference on Computing for Sustainable Global Development (INDIACom).

[2] Ms. Manisha, Ms. Maneela, "A Survey on Various Methods of Audio Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.

[3] Swati Gupta, Deepti Gupta, "Text-Steganography: Review Study & Comparative Analysis", Swapti Guptaet al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol.2 (5), 2011, 2060-2062.

[4] Navneet Kaur, Sunny Behal, "Audio Steganography Techniques-A Survey", Navneet Kaur Int. Journal of Engineering Research and Applications, Vol. 4, Issue 6 (Version 5), June 2014.

[5] Neha Rani, Jyoti Chaudhary, "Text Steganography Techniques: A Review", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 7 - July 2013.

[6] Shivani Sharma, Dr. Avadesh Gupta, Munesh Chandra Trivedi, Virenda Kumar Yadav, "Analysis of Different Text Steganography Techniques: A Survey", 978-1-5090-0210-8/16 $31.00 © 2016 IEEE DOI 10.1109/CICT.2016.34.

[7] Palak R Patel, Yask Patel, "Survey on Different Methods of Image Steganography", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Issue 12, December 2014.

[8] Omkar Shetye, Chinmay Vanmali, Moses Fernandes, Prachi Patil, "Survey on Different Techniques of Images Steganography", International Journal of Computer Applications (0975 – 8887), Volume 138 – No.3, March 2016.

[9] Sumeet Gupta, Dr. Namrata Dhanda, "Audio Steganography Using Discrete Wavelet Transformation (DWT) & Discrete Cosine Transformation (DCT)", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 17, Issue 2, Ver. V (Mar – Apr. 2015), PP 32-44.

[10] Rupanshi, Preeti, Vandana, "Audio Steganography by Direct Sequence Spread Spectrum", International Journal of Computer Trends and Technology (IJCTT) – Volume 13 number 2 – Jul 2014.

[11] Priadhana Edi Kresnha, Aini Mukaromah, "A Robust Method of Encryption and Steganography Using ElGamal and Spread Spectrum Technique Based on MP3 Audio File", Proceeding Conferenced on Applied Electromagnetic Technology (AEMT), Lombok, 11 – 15 April.

[12] Souma Pal, Prof.Samir Kumar Bandyopadhyay, "Various Methods Of Video Steganography", International Journal of Information Research and Review, Vol.03, Issue, 06. Pp.2569-2573, June, 2016.

[13] K..Parvathi Divya, K. Mahesh, "Various Techniques in Video Steganography – A Review", International Journal of Computer & Organitazion Trends – Volume 5 – February 2014.

[14] Jaeyoung Kim, Hanhoon Park, Jong-Il Park, "Image Steganography Based on Blcok Matching in DWT Domain".

[15] Amritpal Singh, Satinder Jeet Singh, "An Overview of Image Steganography Techniques", International Journal of Engineering And Computer Science ISSN: 2139-7242, Volume 3, Issue 7, July 2014 Page No. 7341 – 7345.

[16] Sumeet Kaur, Savina Bansal, R. K. Bansal, "Steganography and Classification of Image Steganography Techniques", 2014 International Conference on Computing of Sustainable Global Development (INDIACom), 978-93-80544-12-0/14/$31.00, 2014 IEEE.

[17] Prof. Samir Kumar, Bandyopadhyay Barnali, Gupta Bamik, "LSB Modification and Phase Encoding Technique of Audio Steganography Revisited", International Journal of Advanced Research in Computer and Communication Engineering, Vol.1, Issue 4, June 2012.