INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

A RESEARCH ON STEGANOGRAPHY METHODS ON TEXT, AUDIO, IMAGE AND VIDEO

[1]E. PAVAN KUMAR, [2]D. RAMMOHAN REDDY

[1]PG Scholar, Dept. of MCA, Newton's Institute of Engineering, Guntur, (A.P)

[2]Associate professor, Dept. of CSE, Newton's Institute of Engineering, Guntur, (A.P)

Abstract: Steganography is the science and art of covert communication via the use of coded information hidden inside a carrier file. several publications from several fields of study have been published during the last few decades. For steganography to be successful, it must remain hidden from prying eyes. This study will explore the different forms and methods of steganography, including its application to text, picture, audio, and video.

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

I. INTRODUCTION

Steganography literally translates to "covered writing," a combination of the Greek word's "stages" (which means "cover") and "graafian" (which means "writing") [2]. The compression or embedding of data and its subsequent extraction are the two main components of steganography. Covert writing, or steganography, is an art and science that has been practised for centuries.

The word "steganography" has really been in use for thousands of years. This is a method for clandestinely exchanging information between two or more persons via the medium of a media cover. Text, music, still picture, and digital video files may all be utilised as media.

The algorithmically-encoded hidden message on the media cover, which must be sent together with the steno file [1].

Before attempting to use or implement steganography, there are a few crucial factors to remember:

a. Embedding Capacity: Information is concealed inside a bigger file, known as a "cover" or "carriers" file. Computer files are employed as the carrier, and their quality is maintained regardless of format. When determining whether or not steganography is possible, the quantity of data that can be embedded on the cover is compared to the cover size, or "embedded

ISSN: 2057-5688

capacity." If the size of the data that will be placed on the cover is larger than the cover size, then steganography is impossible.

b. Undetectability: Information must be concealed or embedded into a carrier file such that no one may discover the hidden message or information by mistake. The steganography has failed if the hidden message can be read from the original file [1].

c. Robustness: The ability of the embedding procedure to maintain embedded data following file compression and decompression [1].

d. Security: The primary concern when concealing information in any format is security, which includes the perceived transparency of the concealed data [2]. Embedded secret messages unknown to persons who aren't involved in the exchange between the sender and receiver are a common definition of security in steganography scenarios.

When a product or system is resistant to being tampered with by those who have access to it, it is said to be tamper-resistant. The value of tamper resistance cannot be overstated. In steganography, it's crucial that the carrier file used to conceal a message or file is sufficiently robust to withstand attempts at decryption by the target audience. First, an adaptive LSB (Least Significant Bit) approach is used to obfuscate a secret message.

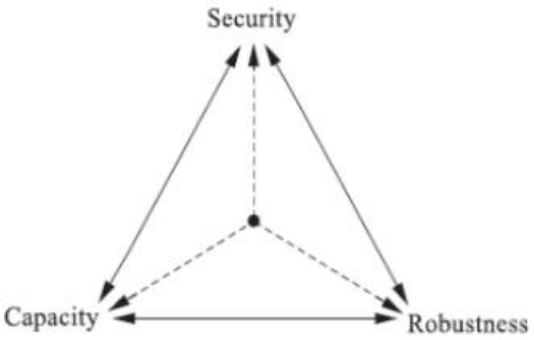

Figure 1: The relation between security, robustness and capacity [2]

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].

II. TYPES OF STEGANOGRAPHY METHODS

In steganography, a "cover" or "carrier" file is hidden using one of many ways and approaches.

A. Text steganography, in which text is hidden by rearranging its format inside a file, modifying the words within the text, or generating random character sequences, is one method. [1][5].

In this case, the secret information is hidden inside a text file. Text

ISSN: 2057-5688

steganography, which is itself divided into three types like [1][6], is more susceptible to attack since it is possible for an adversary to discern the pattern.

Textual data is inserted in the carrier text by altering the format of the cover text itself (referred to as "format-based methods").

b) language methods, which focus only on language analysis.

Its carrier text is generated statistically, and the information is embedded in a random string of letters. c. Random and Statistical Generation Methods.

Due to the lack of redundancy in a text file compared to other digital media like images, sounds, and videos, text steganography is the most challenging kind of steganography. [6]. Persian, Arabic, Hindi, English, etc. are only few of the languages used to conceal information. The English language is distinguished by its inflection, periphrases, and strict word order, among other features.

The term "conversion" refers to the process through which a sentence's word relationships may be conveyed with few alterations [6].

B. picture steganography: the practise of secreting data inside a "carrier" picture without degrading the quality of either the image or the data, and making the image secure enough that users who have no need for the hidden data are unable to access it. Since human eyes cannot tell the difference between the original picture and the steno image [15][16], the secret message is placed as noise inside a carrier image.

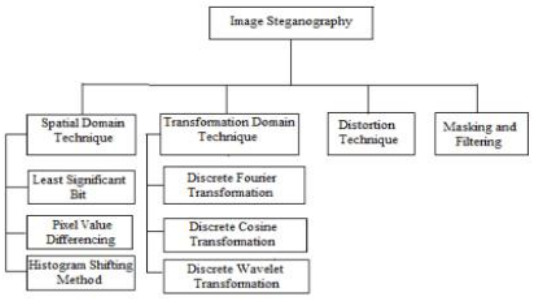

Figure 2: Image steganography techniques [15].

Figure 2: Classification of Image Steganography, including Examples

The intensity of pixels and noise modification are both part of a. Spatial Domain Technique, which is used to conceal information by directly altering specific bits into the pixel values of an image. The Least Significant Bit (LSB) is one of the simplest methods for embedding files in the spatial domain [15, 16].

b. Transformation Domain Technique, which poses risks similar to those posed by image processing procedures (compression, docking, and enhancement) due to the fact

ISSN: 2057-5688

that it conceals the secret message inside a strategically placed region of the carrier picture.

c. First, the picture is transformed from the spatial domain to the transformation domain, and then the carrier image with the hidden message is implanted into it. Using mathematical functions, these methods conceal sensitive information. [15][16].

The information is encoded and stored in the distortion of the signal, which is technique d. Decoding images using this method requires familiarity with the differences between the original carrier picture and the steno image into which the information has been embedded.

e. Masking and filtering, often used to conceal information in images of 24bit size or greyscale type using a variety of software programmes. This method, which is comparable to paper watermarks in that it conceals data by marking the picture, reveals the data in a more substantial section of the image than just in the background noise.

Embedding a message in an audio recording using any technique other than steganography is challenging because the human auditory system (HAS) is more sensitive than the human visual system (HVS). [1]

III. METHODS OR TECHNIQUES IN STEGANOGRAPHY

A. Techniques for Steganography in Text

Different forms of text steganography include:

It conceals the characters at the beginning or end of words to make it easier to combine those characters and extract the content. a. Selective Hiding. This method needs a substantial quantity of simple text.

Web pages written in HTML may have content hidden using the language's attributes; the character can then be used to reveal the hidden material.

b. Concealment through Blank Spaces: When there are fewer white spaces between words, we know that each one is a 0, but when there are more, we can get a 1.

c. Semantic Hiding, also known as "message hiding through the use of synonyms"

Steganographic Techniques for Sound B. Multiple audio steganographic methods exist, including:

a. The secret message bytes are substituted for the carrier file's least significant bytes (LSB) using LSB encoding. Because it has the least effect on file quality, the

ISSN: 2057-5688

rightmost bit is usually the one to be swapped out [1].

b. Parity Coding: If the cover file's parity bit is the same as the secret message's parity bit, no action is taken; otherwise, any bit LSB is modified (cover file or secret message) significantly to make parity equal [1].

The data is hidden by inserting an echo sound into the cover file, which is known as c. Echo Data Hiding. Embedding information is often represented as a function of delay, amplitude, and decay rate [1].

The original data sound is identified by the beginning amplitude.

b) The echo function may be determined with the help of the decay rate, and c) the Offset function can be used to calculate the gap between the source and reflected voice signals.

Spread Spectrum (d) encrypts a message and broadcasts it across a wide range of frequencies. Using pre-existing broad-band channels to transmit a narrow-band information signal. Signal redundancy is improved by the use of signal spread; the degree of improvement is set by the value of a scalar multiplier termed cr. The scalar value of cry corresponds to the number of bits in a value.

e. In a Linear Fashion Spread spectrum refers to the practise of dispersing a signal with limited bandwidth over a wide frequency spectrum. There will be signal attenuation and weakening due to noise in the carrier medium. The receiver side needs further information about the deployment procedure in order to recover the hidden signal from the carrier file. You may think of this information as a secret key that the system needs to function. The secret message is hard to know but simple to crack for the recipient (temper resistance), but the sender must also know how to embed it into a cover material [10].

The fundamental idea behind phase encoding involves using a chunk of the phase spectrum as a location to hide a message derived by decomposing the original signal of an audio stream or carrier file.

Phase Coding Methodology Consists Of:

The original audio stream, broken down into its component parts (C). The remaining information is divided into sub-sections whose lengths are proportional to the total size of the message to be encoded into the cover medium.

The DFT matrix representing the phase may be constructed by applying the transform to each of the segments.

ISSN: 2057-5688

In order to determine the value of the new phase under the given message bit conditions, the following formula must be used:

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

Old phase is got 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 steno image [7].

ISSN: 2057-5688

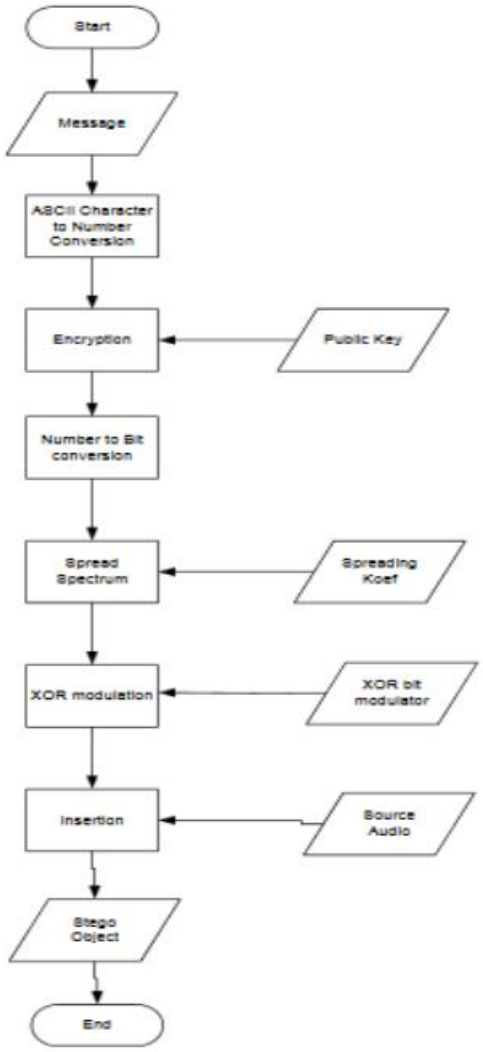

Figure 3: Steganography Process in this study [11]

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 Kouf 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 steno object.

IV. CONCLUSION

Because steganography is not simple to learn, both the sender and the recipient must be well-versed in the technique in order to successfully use it, regardless of the medium or environment in which the information is being transmitted. The confidentiality of our conversations with others is crucial. Considering the gravity and sensitivity of the matters discussed in our conversations with others. The information's security has obviously been compromised if others have access to it. Steganography is successful if the information it conceals can't be accessed by anybody else.

REFERENCES

[1] Prashant Johri, 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).

ISSN: 2057-5688

[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] Prasadu Peddi (2021), "Deeper Image Segmentation using Lloyd's Algorithm", ZKGINTERNATIONAL, vol 5, issue 2, pp: 1-7.

ISSN: 2057-5688

[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] Naga Lakshmi Somu, Prasadu Peddi (2021), An Analysis Of Edge-Cloud Computing Networks For Computation Offloading, Webology (ISSN: 1735-188X), Volume 18, Number 6, pp 7983-7994.

[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] Prasadu Peddi (2023), Using a Wide Range of Residuals Densely, a Deep Learning Approach to the Detection of Abnormal Driving Behaviour in Videos, ADVANCED INFORMATION TECHNOLOGY JOURNAL, ISSN 1879-8136, volume XV, issue II, pp 11-18.