IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

A Review on Major Image and Video Steganography Techniques

Athira R Warier[1] and Remya R[2]
Student, Department of Computer Science, Santhigiri College of Computer Sciences, Thodupuzha[1]
Assistant Professor, Department of Computer Science, Santhigiri College of Computer Sciences, Thodupuzha[2]

Abstract: *With the growing expansion of the intensive sharing of multimedia content and secret communications, data concealing techniques have become increasingly crucial. Steganography is a mechanism for sharing data covertly and securely. It is the science of embedding hidden information into cover media by altering the cover image in a way that is difficult to detect by human eyes. Audio, video and image files can all benefit from steganography techniques. Video steganography is the process of hiding secret information in a video file. Video Steganography is concealing a secret message, which might be a secret text message or an image within a bigger one, in such a way that an unwelcome person cannot determine the presence of the concealed message just by looking at it. There are several Steganography strategies for hiding hidden information in videos, which are further detailed in this paper, along with some of the research efforts done in some disciplines under video steganography by some authors.This article discusses the advancements in the subject of image and video steganography, as well as a comparison of its many applications and methodologies. It is critical to secure digital information while communicating over the internet in today's digitally-driven society. One of the techniques utilised for this is steganography. The importance of steganography and the numerous types of steganography are discussed in this study. It also clarified the vocabulary for the general model of digital steganography. The traditional steganography approach of most minor significant bit substitution is explored. Furthermore, in terms of several performance metrics, a comparison is made between the conventional technique and other techniques for covering media quality and imperceptibility. The size of the hidden message that can be embedded in the image is estimated.*

Keywords: MajorTechniquesinImageSteganography,MajorTechniquesinVideoSteganography, Image Steganography,VideoSteganography, etc.

I. INTRODUCTION

Steganography is a phrase that has been used for thousands of years. This is a method of letting two or more people communicate silently with each other by concealing any hidden message on a media cover. Text, music, image, and digital video files are all acceptable as media. The secret message is encoded in the media cover using the appropriate technique and requires the receiver to send the stego file itself. There are several different sorts of steganography methods and procedures that are used to embed a file known as a cover or carrier. Image steganography is the process of hiding information in a carrier image without causing it to degrade and making the image resilient enough to prevent users who have no business with the information from accessing it.The secret message is encoded as noise in a carrier image since human eyes cannot discern the difference between the original and the stego image.

Video Steganography is the art of hiding or embedding a message in a video. The sender is not only hiding but also how that message is protected from being opened by anybody but the receiver. The art of hiding information, which avoids the disclosure of hidden communications, includes hiding messages in videos.

Video-based steganography techniques are categorised into spatial domain and frequency domain-based methods, just like image-based steganography techniques [2][5]. In video steganography, holding capacity and imperfection are two significant factors to consider when assessing performance.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

II. LITERATUREREVIEW

Chan and Cheng (2003) [1] suggested a simple LSB Substitution approach for hiding data in photos. The paper uses the optimal pixel adjustment process (OPAP) to improve the stego image quality achieved using the simple LSB replacement approach. OPAP is used to check for embedding errors between the original image and the stego image. This method is used on greyscale photographs, in which the secret data bits are embedded using 2-4 bits of the original cover image pixels. The image quality is calculated using the PSNR of the image.

LSB Steganography Detection Algorithm Gradient Energy-Flipping Rate detection was proposed by Zlii, Yang, and Xian (2003) [2]. (CEFR). The secret message embedded in the target image is discovered and the length of the embedded message is determined using LSB Steganography in colour and greyscale images based on the fluctuation of the gradient energy. This approach concludesRandom insertion LSB for image Steganography has been proposed by Sutaone and Khandare (2004) [3]. With the external secrete key, this approach converts the message to ASCII binary and spreads it out in the carrier picture in an apparently random manner. Steganography and cryptography are both provided by this technology.

Ru, Zhang, and Huang (2005) [4] proposed the Steghidesteganographic programme for identifying hidden information in WAV files. In this research, a linear predictor was used to extract significant statistical features from the amplitude of wavelet sub band coefficients, and support vector machines were utilised to detect the presence of hidden messages. Wavelet decomposition was utilised to examine multi-resolution data. A linear predictor was employed to capture the subtle changes in relation between neighbouring samples that embedding causes.

III. ANALYSIS

A. ImageSteganography

The process of concealing information in a carrier image without causing image deterioration and making the image resilient enough that users who have no connection to the information cannot access it. Because human eyes cannot distinguish between the original image and the stego image, the secret message is encoded as noise in a carrier image.

There are several types of image steganography techniques:

LeastSignificantBitSubstitution: The hidden message is embedded via LSB steganography of carrier medial data. The simplest steganography technique is LSB Substitution [5]. There is an example for LSB, where each pixel in an 8-bit grayscale bitmap image is treated as a byte, with the first eight pixels on the original values [5]:

11100110
10101001
00100010
11011001
10101011
01001010
10010001
11010011

In this grayscale pixel, type the letter "A," because A's binary code is 01000001. To achieve the new values, we need to replace the right bits on these grayscale pixels:

11100110
10101001
00100010
11011000
10101011
01001010
10010000
11010011

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

The human eye is incapable of distinguishing between carrier and stego images [5].

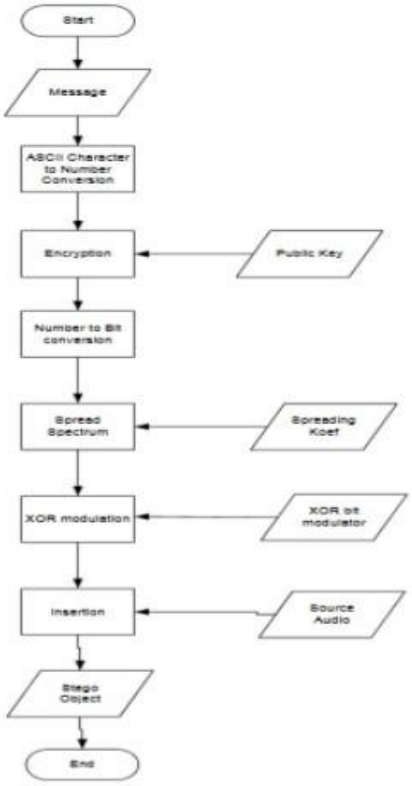

Figure. 1: Steganography Processinthis Study

When practising steganography in this study, you must first obtain your message and then convert it to a number conversion, as shown in figure 3. But don't forget to collect your public key to encrypt the message before converting it to a bit. After we calculate a value, we'll use Spreading Koef to count the message's spread spectrum using XOR modulation. Once we have a file, we can input the audio we want to use as a carrier media or sound, and we'll have our stego object.

Discrete Cosine Transform (DCT), the most popular embedding approach, owing to the fact that the image format will be publicly available as a typical type of digital camera output format [5].

Thereisanexamplelikethis,a successive 6 * 6 pixels image block into 36 DCT in JPG image format for color components that will be discrete cosine transform coefficients (DCT). The DCT coefficients F (u, v) that will be obtained from a 6*6 block pixel are provided 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.

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

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

ThisC(x)willhavevalue1/√2whenxis0.Otherwise,C(x)willhavevalue1whenxis1 [5].The image is transformed from the spatial domain to the frequency domain using the Discrete Wavelet Transform (DWT). Use a pair of filters termed an analysis pair of filters to get a wavelet domain or DWT from the carrier image. After applying a low-pass filter to each row of data to produce a low-frequency component, a high-pass filter with the same pass component is applied to the data route. Furthermore, the obtained component is isolated and subsequently incorporated into the low-pass component. [5]

The minimum required to spread the message over a wide frequency is spread spectrum [5]. In spread spectrum steganography, embed the message in noise and mix it with the cover image to create a stego image. The attached image is difficult to recognize with the naked eye [5].

The least significant bits (LSB) placements on RGB pixels are determined using Hash-LSB, and the information is incorporated in the RGB pixel. In addition, the carrier picture will be broken or fragmented into RGB format [5].Convert the secret message to a bit; in RGB [5], each 8 bit is encoded in the least significant bits.

B. Video Steganography

Hiding or embedding a message in a video is similar to the art of concealing information in that the sender is not only concealing but also preventing the message from being read by anybody other than the intended recipient. The art of hiding information, which avoids the disclosure of hidden communications, includes hiding messages in videos. Video-based steganography techniques are categorised into spatial domain and frequency domain-based methods, similar to image-based steganography techniques [6][7].

In video steganography, holding capacity and imperfection are two significant factors to consider when assessing performance. When applying the spatial domain approach and immediately embedding the information into the carrier image with no visual alterations and good quality, the results have an advantage in steganography capacity. The secret information is embedded in the transform space using the transformation domain algorithm, which has the advantage of being stable but limited in capacity [1][7].

There are several types of videosteganography techniques:

Least significant bit (LSB) operates on LSB bit from media files to embed into a carrier file using different polynomial equations for video steganography.

Video steganography based on DCT vector quantization (32 * 32). The quantization of DCT vectors is one approach that can operate at 32 * 32. The first step is to slice each video into a variable number of pictures. After that, the sliced images are sent to a 32 × 32-pixel management operation, which is followed by quantitative LSB approaches [7]. The planted text message is converted to ASCII and then encoded as a bit to make it more compatible with the video vector. The goal is to fill the low-intensity bits that are still pinned into the high-intensity bits. IDCT [7] fully completes the embedding bit scheme.

An integer wavelet transform-based high-capacity video steganography is used to create stegoimages; the proposed approach applies integer wavelet transforms to the cover image [7]. A set of confidential imagery is used to improve the suggested algorithm's capacity [7].Video Steganography using dynamic cover generation,a new steganographic system in which the system creates the cover media rather than using an existing one, and some data is embedded in the cover while the rest is hidden.

IV. CONCLUSION

Steganography is a technique for embedding a secret message or information from the sender to the receiver with media as it covers to embed. Because steganography is not easy to learn, the sender and receiver must comprehend the knowledge of steganography technique in all formats and situations. It is critical to protect the information we share with others. Because the information we share with others is both valuable and private. If other people get access to this information, something has gone wrong with its security. Steganography's success is measured by the information security that no one else has access to.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 3, June 2022
Impact Factor: 6.252

ACKNOWLEDGMENT

We have taken efforts in this paper. However, it would not have been possible without the kind support and help of many individuals. I would like to extend my sincere thanks to all of them. I am highly indebted to RemyaDepu for their guidance and constant supervision as well as for providing necessary information regarding the paper & also for their support in completing the seminar. I would like to express my gratitude towards my parents & friends for their kind cooperation and encouragement which help me in completion of this paper.

REFERENCES

[1] PrashantJohri,AmbaMishra,SanjoyDas,ArunKumar,"Survey on Steganography Methods (Text, Image, Audio, Video,ProtocolandNetworkSteganography"2016InternationalConference 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, Volume4, Issue5, May2014.

[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, 20602062.

[4] Navneet Kaur,Sunny Behal,"Audio Steganography Techniques-A Survey", Navneet Kaur Int. Journal of EngineeringResearchandApplications,Vol.4,Issue6(Version5),June2014.

[5] Yang C. H, Weng C. Y, Wang S. J and Sun H. M (2008), "Adaptive data hiding in edge areas ofimages with spatial LSB domain systems," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 488–497.

[6] Bhaumik A. K, Choi M, Robles R. J and Balitanas M. O (2009), "Data Hiding in Video",International Journal of Database Theory and Application Vol. 2, No. 2, pp.9-16.

[7] Kiah E,Zaidan B. B and Zaidan A. A (2009), "High-rate video streaming steganography",International Conference on Information Management and Engineering, pp.550-554.

BIOGRAPHY

Athira R Warier is studying Master of Computer Applications in Santhigiri College of Computer Sciences, Vazhithala, Idukki, Kerala. She has completed her Bachelor of Computer Applications from Mahatma Gandhi University, Kerala.

RemyaDipu received the MCA professional degree. She is working as an assistant professor in Santhigiri College of Computer Sciences, Vazhithala.