IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305378 |

Video Steganogrphy by Image Processing

Prof. Vishwas C N B. E M. Tech, Prof. Vishwas C N B. E M. Tech, Akhila B, Priyanka M, Divyabharathi J P S, Manu V

Department of Computer Science, SJM Institute of Technology Chitradurga, Karnataka, India

ABSTRACT: It is an art of hiding an information within other such that the change in the cover information cannot be detectable. In this paper we have provided security for an image using the concept of video steganography. A secret information is to be hidden in the randomly chosen unique video frame. Here we use the LSB method to hide that image into multiple video frames. Here frames are generated by some pseudo random number generator. Eight bits of secret images are divided into 8 bit-planes .As we first resize the image equal to the cover frame along with the bit-slicing method ,exactly 8 cover frames are needed to embed the secret image. An application of this technique is also presented here.

HISTORY: A steganography project typically falls under the category of information security, specifically within the subfield of data concealment or covert communication. It involves the implementation and study of techniques to hide secret information within various types of digital media, such as images, audio files, videos, or text. Steganography projects often involve researching and developing algorithms, tools, or methodologies for embedding and extracting hidden data, as well as analyzing the security and effectiveness of steganographic techniques.

The phenomenal growth in e-commerce applications through the Internet in the past few years has led to a genuine need, as well as a sense of urgency, for both small office and home office (SOHO) and corporate users to protect their data transactions through the Internet. The data transactions may include sensitive document transfer, digital signature authentication, digital watermarking for copyright protection, and digital data storage and linkage.

I.INTRODUCTION

Steganography is a method of concealing messages between senders and receivers. The term "steganography" combines "stego," meaning covered or concealed, with "graphy," meaning writing and drawing. It is a technique used to prevent the detection of communication. In steganography, messages are hidden within other files, such as images, audio files, or videos. The hidden data can be text, images, audio, or even videos. Two methods for hiding data within other files are cryptography and steganography.

Steganography is the practice of concealing messages, while cryptography focuses on encrypting data for protection. Steganography enables easy secret communication by hiding the existence of the message. In many cases, encryption can be combined with steganography to enhance security, making it like cryptography.

II. MAIN OBJECTIVE OF THE PROJECT:

- Design and implement a steganography system capable of hiding secret data within image, audio, and video files while maintaining a high level of imperceptibility and robustness against various attacks.
- The system should support both embedding and extraction processes, ensuring secure and reliable communication of hidden information.
- The hidden information should be imperceptible to human senses, ensuring that the carrier media appears unchanged and natural to casual observers.
- The project aims to provide a secure means of transmitting sensitive data by concealing it within cover objects.

III. LITERATURE SURVEY

[1] IMAGE STEGANOGRAPHY

In this type of steganography, secret data is hidden in the image as a cover object. Images are used in this process as a cover source due to the number of bits in the images' digital representation. Images can be used in three different ways as cover objects to hide information; these are spatial domain, frequency domain, and adaptive domain. Various studies have used images as cover objects to hide secret data; for instance, Yang et al proposed contrast enhancement of

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305378 |

medical images which had hidden data inside them. The proposed method could hide the data into a smooth region of images with improvement in the visual quality of the stego-image. The prime step of the proposed method was the use of the histogram shifting method for hiding information in the texture area of the image and the use of a contrast enhancement method for improving the visual quality of the image. The authors compared the proposed method with the other reversible data hiding method that also used histogram shifting. The authors used the peak signal to noise ratio as an objective parameter. From the results, it was clear that the proposed method performed better in comparison to the other methods. Punidha et al used the concept of integer wavelet transform for sending audio speech signals through the steganography technique. The authors used the well-known Haar wavelet method with the integer wavelet transform for hiding secret messages. The authors used various objective parameters, such as signal-to-noise ratio, MSE, PSNR, and structural similarity index to evaluate the performance of the proposed method.

[2] AUDIO STEGANOGRAPHY

In this type of steganography, secret data is hidden in the image as a cover object. Images are used in this process as a cover source due to the number of bits in the images' digital representation. Images can be used in three different ways as cover objects to hide information; these are spatial domain, frequency domain, and adaptive domain. Various studies have used images as cover objects to hide secret data; for instance, Yang et al. proposed contrast enhancement of medical images which had hidden data inside them. The proposed method could hide the data into a smooth region of images with improvement in the visual quality of the stego-image. The prime step of the proposed method was the use of the histogram shifting method for hiding information in the texture area of the image and the use of a contrast enhancement method for improving the visual quality of the image. The authors compared the proposed method with the other reversible data hiding method that also used histogram shifting.

[3] VIDEO

STEGANOGRAPHY video steganography technique for secure communication has been proposed by Hanafy et al. [48]. This technique is used in the spatial domain. Furthermore, the secret data is divided into nonoverlapping pieces and then hidden (using a secret key) within the video frames. The secret data is constantly randomized within each video frame to prevent an intruder from locating the exact location of the secret data. The data embedding process was accomplished by using the two least significant bits (LSB) from each RGB color channel to hide six bits in each pixel frame of the secret message. Confidential information is protected in this technique by utilizing a secret key. However, this approach conceals the hidden information by using the spatial domain. The video quality for different resolutions varied based on the PSNR for each cover. The PSNR value ranges from 51.57 to 53.58 dB when using text as the secret information; 50.44–65.56 dB when using an image; 50.86–59.3 dB when using audio; and 50.94–52.58 dB when using video as the secret message. The noise and compression levels are significantly reduced. Tadiparthi et al. [49] proposed a steAganography technique that uses animations as the cover object. different resolutions varied based on the PSNR for each cover. The PSNR value ranges from 51.57 to 53.58 dB when using text as the secret information; 50.44–65.56 dB when using an image; 50.86–59.3 dB when using audio; and 50.94–52.58 dB when using video as the secret message. The noise and compression levels are significantly reduced. Tadiparthi et al. [49] proposed a steganography technique that uses animations as the cover object**.**

IV. METHODOLOGY

A. Spatial Domain: In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms

Least Significant Bit (LSB):

This is the most common, simple approach for embedding data in a cover image. The least significant bit (8th bit) of one or all of the bytes inside an image is changed to a bit of the secret message. When we use 24-bit image, three color bits components are used which are red, green, blue, each byte store 3 bits in every pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305378 |

(10100110 11000101 00001100)
(11010010 10101100 01100011)

The number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be visible by the human eye due to the message hidden. In these consecutive bytes of the image data – from the first byte to the end of the message – are used to embed the information. And easy to detect, more secure system for the sender and receiver to share a secret key that specifies only some pixels to be changed in its simplest form, LSB makes use of BMP images, since they use lossless compression. It hide a secret message inside a BMP file, one would require a very large cover image. In BMP images of 800 × 600 Pixels are not often used on the Internet and might arouse suspicion. For this reason, LSB steganography has also been developed for use with other image file formats. It is a simple method for embedding data in a cover image. This is the simplest algorithm in which information can be inserted into every bit of image information. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (least significant bit) of selected pixels of the image proposed a simple data hiding technique by simple LSB substitution. In this technique last bit of host data is randomly changed and produce the watermarked data at output. The cover LSB media data are used to hide the message.

Pixel Value Differencing:
It provides both high embed-ding capacity and outstanding imperceptibility for the stego-image; this segments the cover image into non overlapping blocks containing two connecting pixels and it modifies the pixel difference in each pair for data embedding.

Pixel Indicator:
This method gives the stego images of better quality than the traditional method while maintaining a high embedding capacity and it also uses concept of hiding the data using the difference between the pixel values. It's more complex way of hiding information in an image. Transformations are used on the image to hide information in. Transform domain embedding can be termed as a domain of embedding techniques in frequency domain; image is represented.

B) **Frequency Domain:**

- **Discrete Cosine Transformation:** These methods convert the uncompressed image into JPEG compressed type. It is based on data hiding used in the JPEG compression algorithm to transform successive 8x8pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain. The main advantage of this method is its ability to minimize the block like appearance resulting when boundaries between the 8x8 sub-images become visible (known as blocking artefact).
- **Discrete Wavelet Transformation:** It gives the best result of image transformation.it splits the signal into set of basic functions . There are two types of wavelet transformation one is continuous and other is discrete This is the new idea in the application of wavelets, in this the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. It also performs local analysis and multi-resolution analysis. DWT transforms the object in wavelet domain and then processes the coefficients and performs inverse wavelet transform to show the original format of the stego object.

V. EXISTING SYSTEM

- Pixel Value Differencing (PVD): PVD is a technique that takes advantage of the differences between consecutive pixel values in an image. The secret data is embedded by modifying these differences while keeping the overall visual appearance intact.
- Masking and Filtering: This technique involves creating a mask or a filter image that specifies which pixels in the cover image will be modified to hide the secret data. The secret information is embedded by altering the selected pixels according to the mask or filter image.
- Spatial Domain Techniques: Spatial domain techniques involve directly modifying the pixel values of the image to embed the secret data. This can be achieved through methods like altering the intensity of selected pixels or rearranging the pixel values based on a specific pattern.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305378 |

VI. PROPOSED SYSTEM

This Steganography technique is more popular in recent year than other steganography possibly because of the flood of electronic image information available with the advent of digital cameras and high-speed internet distribution. It can involve hiding information in the naturally occurred noise within the image. Most kinds of information contain some kind of noise. Noise refers to the imperfections inherent in the process of rendering an analog picture as a digital image. In Image steganography we can hide message in pixels of an image. An imagesteganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method. Someone can then use a proper decoding procedure to recover the hidden message from the image. The original image is called a cover image in steganography, and the message-embedded image is called a stegoimag

VII. APPLICATIONS

• Military and Defense: Morse code can be used for secure communication between military personnel, and AI algorithms can enhance encryption and decryption processes, ensuring message integrity and confidentiality.

• This authentication can be implemented in IoT devices to prevent unauthorized access and control. AI can manage authentication processes and detect anomalies in device communication.

VIII. CONCLUSION

Throughout this project, we have explored and implemented various modules that make up a steganographic system. The carrier selection module allows users to choose the carrier file in which they want to hide the secret information. The secret information input module enables users to input the data they wish to hide within the carrier file. The encryption module applies steganographic techniques to embed the secret information, while the decryption module extracts the hidden information from the carrier file. These modules employ different algorithms and methods, such as LSB manipulation, spread spectrum, or transform domain techniques, to ensure the hidden information remains undetectable.

REFERENCES

[1] https://ieeexplore.ieee.org/document/8343528
[2] http://www.jetir.org/papers/JETIR1703020.pdf
[3] A Munasinghe ,Anuja Dharmaratne and Kasun De Zoysa,“Video Steganography”, 2013“International Conference on Advances In ICT for Emerging Regions.
[4] Tanmay Bhowmik, Pramatha Nath Basu "On Embedding of text in Audio- A case of Stegnography" International conference on recent trends in information, Telecommunication and computing, IEEE 2010.
[5] Nedeljko Cvejic ,Tapio Seppben " Increasing the capacity of LSB Based audio Steganography", IEEE 2002.
[6] RehanaBegumR.D.andSharayuPradeep,“BestApproachforLSBbasedvideo steganography using Genetic Algorithm and visual Cryptography for secured data hiding and transmission over networks”, International Journal of Advanced Research in Computer Science and Software Engineering,2014.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details