Steganographic Techniques for High-Capacity Covert Communication in Images and Videos

Krishna Kadam, Sumit Tambe, Aniket Bomble, Sarthak Bora, Prof.K.T.Mohite

[1]*Krishna Kadam Computer Engineering ,SAE*
[2]*Sumit Tambe Computer Engineering, SAE*
[3]*Aniket Bomble Computer Engineering, SAE*
[4]*Sarthak Bora Computer Engineering, SAE*
[5] *prof.K.T.Mohite Computer Engineering, SAE*

ABSTRACT - Steganography is the art of concealing information within other data to obscure the transmission process. Digital photos are the preferred carrier files due to their ubiquity online. Various steganography techniques exist for hiding sensitive data in video frames, each with distinct strengths and weaknesses. Some applications require total invisibility for critical information, while others can accommodate larger secret messages. Our project conceals messages within visuals, enabling users to select replacement bits instead of employing less secure LSB substitution. Data transmission, the process of sending data from source to destination, often involves slower mediums like coaxial cables and twisted pair wires, which can result in data leaks or losses. To address these issues, fiber optics are employed. Fiber optics transmited data as light beams, minimizing data leakage and incorporating security measures. In our proposed system, we enhance fiber optic encryption through the use of images.

***Key Words*:** Steganography, data concealment, digital photos, steganography techniques, data invisibility, LSB substitution, data transmission, coaxial cables, twisted pair wires, fiber optics, data security, image encryption.

1.INTRODUCTION

In today's digital age, the protection and transmission of sensitive information have become paramount. Alongside the advancements in information security, techniques for concealing data have evolved as well. Among these, steganography, the art and science of hiding information within seemingly innocuous cover media, has gained prominence as a powerful tool for covert communication and information protection. Steganography finds its application not only in the realm of text but also in the concealment of data within images and videos. This introductory exploration delves into the fascinating world of image and video steganography, shedding light on its significance, methodologies, and real-world applications.

Image steganography involves the art of embedding data within digital images. These images serve as the canvas for concealing information. Various techniques exist, ranging from rudimentary methods like the Least Significant Bit (LSB) replacement to more sophisticated approaches that exploit the frequencies and transforms within the image. The primary challenge is to embed data in such a way that it remains visually imperceptible to the human eye, ensuring that the cover image appears unaltered to casual observers. The embedded data could be anything from text messages to multimedia files, making it a versatile tool in secure data transmission.

Extending the principles of image steganography, video steganography encompasses the practice of hiding data within video files. It introduces an added layer of complexity due to the temporal and spatial dimensions inherent in video content. Video steganography aims to ensure that the concealed information seamlessly integrates with the video frames, maintaining synchronization and preserving the video's integrity. Video steganography is particularly relevant in applications where data concealment within moving images is required, such as video watermarking and covert video communication.

2. LITERATURE REVIEW

1. Manohar N1,Peetla Vijay Kumar" Data Encryption Decryption Using Steganography" Video steganography is a method that processes secure communication. When we see the history of steganography, it was hidden in many ways such as tablets covered with wax, written on the stomachs of rabbits. Here in this paper, consider the video steganography methods to perform secure steganography communication. Many methods have been proposed for video steganography but there are no more different types of formats, and secured, quality, of the results. So here propose secure steganography methods i.e. Secure base LSB method, Neural Networks Fuzzy logic, and check their using PSNR and MSE data of the methods.

2. K. Jayasakthi velmurugan ,S.Hemavathi "Video Steganography by Neural Networks Using Hash Function" Video Steganography is an extension of image steganography where any kind of file in any extension is hidden in a digital video. The video content is dynamic in nature and this makes the detection of hidden data more difficult than other steganographic techniques. The main motive for using video steganography is that the videos can store large amounts of data in them. This paper focuses on security using the combination of hybrid neural networks and hash functions for determining the best bits in the cover video to embed the secret data.All experiments are done using Mat Lab 2016 a software.

3. Meenu Suresh1 ,Dr. I. Shatheesh Sam Single level Discrete Wavelet Transform based Video Steganography on Horizontal and Vertical coefficients APPLICATIONS" This paper proposes a single-level discrete wavelet transform based novel video steganography algorithm. Initially '' number of carrier frames are chosen to hide the data in this method. After estimating carrier frames, every frame is separated into each R, G and B components which are decomposed using single-level discrete wavelet transform (DWT). For embedding the watermark information the horizontal and vertical coefficients are selected as a small change in these coefficients has negligible effect on the quality of the video frame. The watermark image pixels is shuffled before embedding for which a key is required.The performance of the method proposed in view of video quality as well as embedding capacity outperforms other methods and is justified by the experimental results

4. Mohammad A. Alia , Khulood Abu Maria "An Improved Video Steganography: Using Random Key-Dependent" Steganography is defined as the art of hiding secret data in a non-secret digital carrier called cover media. Trading delicate data without assurance against intruders that may intrude on this data is a lethal. In this manner, transmitting delicate information and privileged insights must not rely on upon just the current communications channels insurance advancements. The improvement made by searching for exact matching between the secret text and the video frames RGB channels and Random Key –Dependent Data, achieving steganography performance criteria, invisibility, payload/ capacity and robustness.

5. RENUKA B, Dr. N MANJA NAIK Secure Video Steganography Technique using DWT and H.264Sharing of mixed media data has turned out to be brisk because of headway in data innovation. In any case, data security breaking has expanded by the innovation progression. The concealing limit and power against assaults are three principle prerequisites used in video steganography technique should think about. In this paper a secure video steganography calculation using Discrete wavelet transform (DWT) space dependent on the motion object detection calculation and H.264 is proposed utilizing Mat lab programming. The mystery message is pre-prepared by applying bit moving and H.264 utilized for encoding the mystery information. To begin with, motion object detection calculation is actualized on host recordings to recognize the locales of enthusiasm for the moving articles.Our test result improves the installing limit as well as upgrades its security against different assaults.

6. Optical Steganography to Enhance Speed of Analog Transmission with Security Enhancement through Image Encryption Amanpreet Kaur, Gaurav Soni Data transmission is the way through which data is sent from source to destination over a physical medium. In networking we use coaxial cable, twisted pair wires for transfer of data from source to destination. These medium of data transfer are slower in nature and data which is transferred may leak or lost during transmission and also there no security of data. It also uses some security mechanisms for secure transmission of data. The data which are transferred firstly encrypt and after that transferred to the destination in the form of light beams. In our proposed system we introduced encryption in fibre optics using image.

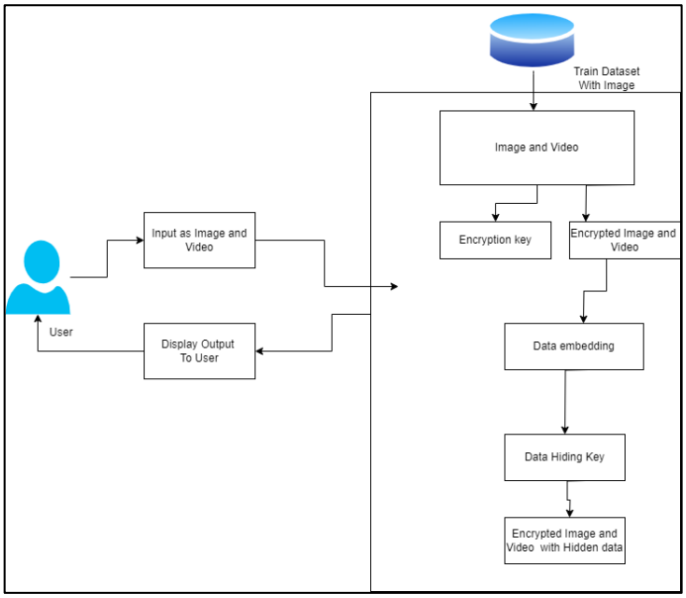
7. New Proposed Practice for Secure Image Combing Cryptography Steganography and Watermarking based on Various Parameters Rupesh Gupta, Dr.Tanu Preet Singh. Since the rise of usage of internet in the world security is becoming the major concern all over. So making this thing clear in mind developers are continuously working to make internet a safe environment for all the users. Many algorithm or techniques are proposed and they worked but as the intruders are acting smartly to hack information developers are also supposed to invent new techniques to stop hacker's intentions.PSNR and Embedding capacity still after the noise attack. The purpose this paper is to provide a new technique that will provide better security for hiding data in an image and watermarked video.

8. A Novel Approach to Hide Text Data in Colour Image Suraj Kumar1 , Santosh Kumar2 , Neeraj Kumar Singh3 , Anandaprova Majumder4 , Suvamoy Changder5 Steganography, unlike cryptography, is an art of hiding of information in such a manner that it does not attract attention. This ancient practice has been in use for a long time to hide and communicate sensitive data escaping the notice of prying eyes. This art in today's time in the context of image, is being exploited in digital world generically to hide digital signatures and watermarks. The experimental observations affirms the efficiency if this approach. The proposed method can be efficiently employed to add signature to the images without much affecting the natural behavior of the noise bed generated.

3. Reference architecture for image and video steganography:

A reference architecture for image and video steganography is a standardized or widely accepted framework that provides guidance on how to design, implement, and deploy steganographic systems. While there isn't a single universally recognized reference architecture for steganography, I can outline a generalized framework that can serve as a reference point for designing such systems. Keep in mind that the actual implementation and architecture may vary based

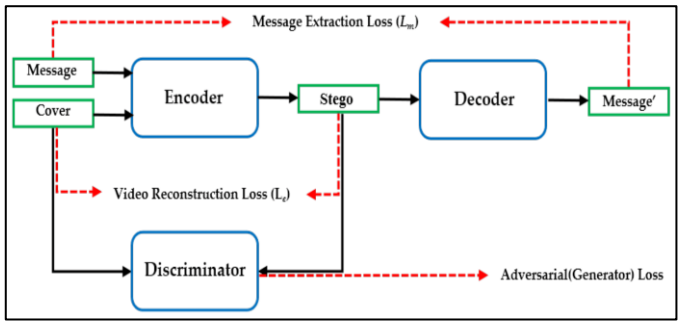
on specific steganographic techniques, applications, and security requirements. The original image or video content that will conceal the hidden information. The data you want to hide within the cover media. This can be text, images, files, or any other form of information .Responsible for hiding the message within the cover media while maintaining the visual or auditory quality.Used to recover the hidden message from the steganographic container. It reverses the embedding process.If security is a concern, a secret key may be used to control the embedding and extraction process.The resulting image or video after the message has been embedded. It should resemble the original cover media as closely as possible. Tools and metrics to assess the quality of the steganographic container,



ensuring it remains perceptually similar to the original media.

Additional steps to ensure synchronization, compatibility with video codecs, or other video-specific considerations. Additional security layers, such as encryption of hidden data or authentication mechanisms to protect against steganalysis and unauthorized extraction. Define the process for embedding the message into the cover media using the chosen embedding algorithm.

4. Design and Development



4. 1. Architecture Design:

Develop a modular and extensible architecture for your steganography system. Define the core components, including. Embedding and extraction modules. Security mechanisms like encryption and authentication.

Quality preservation techniques to ensure perceptual fidelity. User interface for user interaction.

4.2. Algorithm Selection and Integration:

Based on your requirements and objectives, select and integrate suitable embedding and extraction algorithms into the system. These could range from classic LSB substitution to more advanced frequency domain methods or even deep learning-based approaches.

4.3. Security Measures:

Implement security measures to protect against steganalysis and unauthorized data extraction. This might involve encryption of the hidden data, key management, and techniques to reduce detectability.

4.4. Future Development Roadmap:

Outline a roadmap for future development, indicating potential enhancements, additional features, and research areas for further exploration.

In summary, designing and developing an image and video steganography system involves careful planning, research, algorithm selection, security considerations, quality assurance, user-friendliness, documentation, and an eye toward responsible and ethical use. The result is a versatile tool that can be used in various applications,

from secure communication to copyright protection, while preserving the integrity of the cover media.

5. Performance and Effectiveness:

5.1. Data Capacity: One of the primary metrics of performance is the data capacity, i.e., the amount of hidden data that can be concealed within an image or video. Performance is enhanced when a steganography technique can hide larger volumes of data without significantly degrading the quality of the cover media. Capacity is measured in bits or bytes.

5.2. Visual and Auditory Quality: Effectiveness is closely linked to the perceptual quality of the steganographic container. A high-quality steganography technique ensures that the modified image or video remains visually and auditorily indistinguishable from the original. This is crucial for maintaining the integrity of the cover media and ensuring that hidden data goes unnoticed by unintended viewers or listeners. Common quality metrics include Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM).

5.3. Robustness: The effectiveness of a steganography method is gauged by its ability to withstand various transformations and attacks. Robustness testing involves subjecting the steganographic container to alterations such as compression, noise addition, cropping, and filtering. A robust technique can preserve hidden data even in the face of these challenges.

5.4. Security: Security is a fundamental measure of effectiveness in steganography. A successful steganography technique should be able to protect the hidden information from detection (steganalysis) and unauthorized extraction. Security features can include encryption of the hidden data and the use of authentication mechanisms.

RESULT AND EVALUATION:

The results and evaluation of image and video steganography are crucial aspects of assessing the effectiveness and performance of steganographic techniques. Researchers and practitioners use various metrics and criteria to evaluate the quality, security, and robustness of steganography methods. Embedding Capacity: Report the maximum amount of data that can be embedded in images and videos using the steganographic techniques employed. This includes both the payload size and the percentage of the cover media's capacity used. Perceptual Quality: Assess the visual and auditory quality of the stego-images and stego-videos. Use objective metrics like PSNR (Peak Signal-to-Noise Ratio) and subjective evaluations to determine the extent to which the quality has been preserved. Robustness:Evaluate the resilience of the steganographic method against common attacks, such as compression, filtering, and noise. Report how well the hidden data survives these processes. Detection Resistance: Measure the success of the steganographic technique in avoiding detection by various steganalysis methods. Discuss the ability to remain covert in the presence of adversaries.

CONCLUSION AND FUTURE SCOPE:

The proposed method in the paper, selectively feeds the pixels with secret data. The noise bed hence obtained is not so distorted as to arouse suspicion. The histogram of the stego image shows subtle variation from original cover image, hence affirming better visual quality in comparison to generic LSB approach. The PSNR ratio shows greater value than the generic LSB substitution method which signifies the low distortion of the image due to embedding of the secret data in it. This factor of embedded distortion would behaviourally be in alignment to the natural distortion gained by the image in the transmission channel. The concerned secret media is audio when this is extracted from the video, it will not be exactly same as the original embedded audio. The media may get distorted by rounding or processing steps and compression techniques so further processing of the

audio data will be necessary to get nearly same audio. So this method can find many applications in science and technology development. More efforts are needed in this area of secret and secure communication to improve the existing techniques and to find loopholes

REFRENCES:

1. Bhargava, S., Mukhija, M. (2019). HIDE IMAGE AND TEXT USING LSB,DWT AND RSA BASED ON IMAGE STEGANOGRAPHY. ICTACT Journal on Image Video Processing,9(3)

2.Srilakshmi, P., Himabindu, C., Chait anya, N.Muralidhar, S. V.,Sumanth, M. V.,Vinay,K.(2018). TEXT EMBEDDING USING IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN. International Journal of Engineering Technology, 7(3.6), 14.

3. Krishnaveni, N. (2018). IMAGE STEGANOGRAPHY USING LSB EMBEDDING WIT H CHAOS. International Journal of Pure and Applied Mathematics,118(8), 505-509.

4. Karanjit Kaur Baldip Kaur (2018). "DWTLSB Approach for Video Steganography using Artificial Neural Network". In International Advanced Research Journal in Science, Engineering and Technology, IARJSET.

5. Mehdi Boroumand, Mo Chen Jessica Fridich (2018). "Deep Residual Network for Steganalysis of Digital Images". 2018 IEEE.

6."Anamika Saini, Kamaldeep Joshi, Kirti Sharma Rainu Nandal (2017). "An Analysis of LSB Technique in Video Steganography using PSNR and MSE". In International Journal of Advanced Research in Computer Science. IJARCS.

7.Ramadhan J. Mstafa and Khaled M. Elleithy Eman Abdelfattah (2017). "Video Steganography Techniques: Taxonomy, Challenges and Future Directions. 2017 IEEE.

8.M. Dalal and M. Juneja, "A robust and imperceptible steganography technique for SD and HD videos," Multimed Tools Appl, vol. 78, no. 5, pp. 5769–5789, Mar.2019, doi:10.1007/s11042-018-6093-3

9.M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H.Jung, "Image steganography in spatial domain: A survey," Signal Processing: Image Communication, vol. 65, pp. 46–66, Jul. 2018, doi: 10.1016/j.image.2018.03.012.