International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Safe Communication Using Steganography

Prof. Mrs. Seema Bandgar, Anand. D. Chougule, Shivam. R. Jadhav, Subodh. R. Patil, Aftab. F. Shaikh

Asst. Prof. Dept. Of Information Technology, Dr. J. J. Magdum College of Engineering, Jaysingpur

Student, Dept. Of Information Technology, Dr. J. J. Magdum College of Engineering, Jaysingpur

ABSTRACT

This research aims to propose a method of safe communication using steganography, which involves hiding information in other information to conceal the fact that communication is taking place. Digital images are one of the most popular file formats used for steganography due to their frequency on the internet. The project focuses on hiding secret information within images using steganography techniques. Different techniques have their respective strong and weak points, and their application requirements vary. The proposed technique allows users to choose the bits for replacement instead of using the least significant bit (LSB) replacement from the images. In this technique, the sender selects a cover image with the secret text or text file, hides it in the image, and sends it to the receiver through a private or public communication network. The receiver retrieves the secret text hidden in the stego-image using the software. This method provides a secure and user-friendly interface for individuals to exchange confidential messages. It leverages the power of image steganography to address the growing need for privacy and confidentiality in digital communication. By hiding messages within images, it ensures a covert and secure means of transmitting information while maintaining the visual appearance of harmless images.

Keywords: Encryption, decryption, steganography, safe communication.

INTRODUCTION

Steganography is derived from the Greek language, where "stegano" means covered and "graphical" means writing. It is a method of concealing secret data in another file in such a way that only the recipient knows about the existence of the communicated data, thus maintaining confidentiality. Steganography helps maintain secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into the cover image and generating a stego image. There are different types of steganography techniques, each with its strengths and weaknesses. This paper reviews different security and data-hiding techniques used to implement steganography, such as LSB, ISB, MLSB, and others. Communication is a basic necessity in every growing area, and everyone wants the secrecy and safety of their communicating data. In steganography, the process of hiding information content inside any multimedia content like image, audio, or video is referred to as embedding. Both techniques may combine to increase the confidentiality of communicating data. Steganography finds its application in confidential communication, protection of data alteration, and access control systems for digital content distribution.

LITERATURE REVIEW

A literature review on safe communication and steganography can provide valuable insights into the current state of research in this field. Here's an outline of what such a review might cover, along

with some key references you can explore.

Here is a literature review of some of the recent research on safe communication steganography:

- **Shahid Rahman, Jamal Uddin, Habib Ullah Khan, Hameed Hussain, Ayaz Ali Khan, And Muhammad Zakarya (2022)** "A Novel Steganography Technique for Safe Communication Using Image Processing" This paper proposes a new steganography technique for secure communication using image processing. The proposed technique is based on the use of a chaotic map to generate a secret key that is used to encrypt the secret data before it is embedded in the image. The experimental results show that the proposed technique is robust against a variety of steganalysis attacks.

- **S. Sharma et al. [2018]** "proposed a steganographic approach for safe communication on social media platforms". The authors used a combination of LSB and Discrete Cosine Transform (DCT) techniques to hide secret messages in images. They claimed that their approach was more secure and efficient than existing steganographic techniques.

- **Alsalehet al. [2020]** "proposed a novel steganographic technique for safe communication over the internet". Their approach used a hybrid embedding algorithm that combines the advantages of LSB and DCT techniques to hide secret messages in images. The authors demonstrated the effectiveness of their technique using various metrics such as PSNR, MSE, and BER.
- **Manoj Kumar B, Ravikumar K, Gopi Sailesh C, Ravi Kumar CV, (2020)** "Secure Data Communication With Cryptography and Steganography" This technique shows more efficiency with robustness in the image with a high-security system. It will be used in the health care application to hide the details of the patient and also in the e-commerce system with a high-security process.
- **Saurabh Agarwal, Cheonshik Kim, Ki-Hyun Jung (2022)** "Steganalysis Of Context-Aware Image Steganography Techniques Using Convolutional Neural Network"
- **Numrena Farooq, Arvind Selwal, (2023)** "Image Steganalysis Using Deep Learning: a Systematic Review and Open Research Challenges" Image steganography involves the process of concealing sensitive information in the cover image to achieve secret communication. The counterpart of steganography is image steganalysis, which is used to detect any hidden information that is being communicated among different entities., Journal of Ambient Intelligence and Humanized Computing, 14, 7761-7793.

LIMITATIONS OF EXISTING SYSTEM

Steganography has certain limitations and challenges that must be considered while using this technique for secure communication. Some of the main limitations of image steganography include the limited capacity of an image to hold data without significantly altering its appearance. This limits the size of the message that can be transmitted using steganography and thus reduces the usefulness of this technique for certain types of communication. Furthermore, while steganography can make it difficult for attackers to detect the presence of hidden information in an image, it is not foolproof. Skilled attackers can use specialized software to detect the presence of hidden information in an image, which could compromise the security of the

communication. Implementing steganography requires technical expertise, and it can be challenging to ensure that the steganography algorithm is implemented correctly. Additionally, the encryption and decryption processes must also be implemented correctly to ensure the security of the communication. Key management is another challenge in secure message transmission using steganography, as the encryption key or password used to encrypt and decrypt the message must be kept secure. If the key is compromised, an attacker could potentially gain access to the encrypted message, which could compromise the security of the communication. Compatibility is also a challenge in using steganography for secure communication. Both parties need to have compatible software to implement the algorithm used for embedding and extracting the message. This could be a limitation if one party is using an incompatible platform or software.

NECESSITY OF WORK

The increasing need for individuals and organizations to protect their confidential information from unauthorized access has driven the necessity of a website offering a safe communication method using image steganography. With the growing number of cyber threats and data breaches, it's more important than ever to have safe communication channels to protect sensitive information. Image steganography provides a unique method for safe communication by allowing users to hide their messages within image files, making it difficult for unauthorized parties to detect or decode the hidden message. This can be especially useful for individuals and organizations that need to send confidential messages, such as businesses, government agencies, or legal professionals. Our website provides an easy-to-use interface for users to encode and decode their messages using steganographic techniques, making it a convenient and reliable option for safe communication. By using steganography in combination with other security measures, we provide our users with a comprehensive solution for protecting their confidential information. In summary, our website is necessary because it offers a safe communication method that is easy to use, reliable, and effective at protecting sensitive information. With the increasing need for data privacy and security, our website provides a valuable tool for individuals and organizations that require safe communication channels.

SYSTEM DIAGRAM

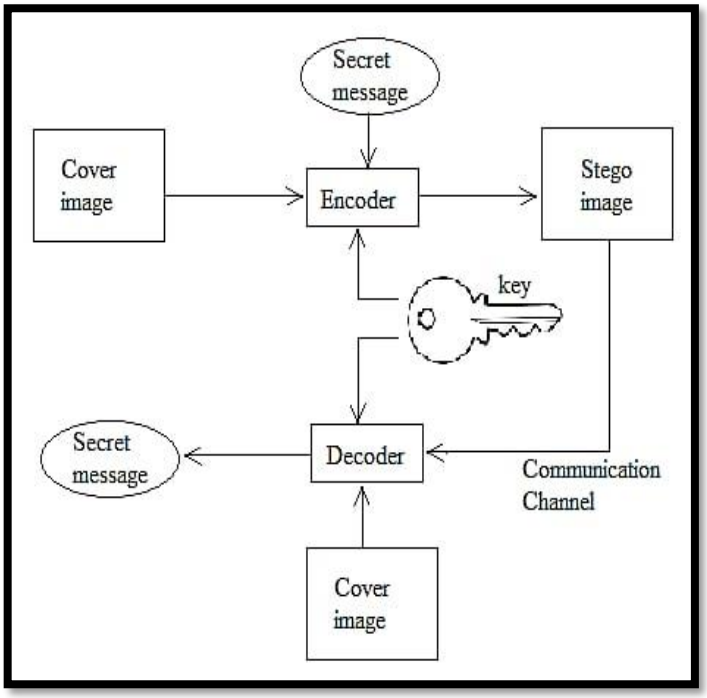


Fig1.- System Diagram

In the safe communication process of hiding a secret message within a cover image using steganography.

1. Cover Image: - This is the original image that you want to use to hide your secret message. It serves as a container for the hidden data. The cover image is usually a regular image that appears innocuous.

2. Encoder: - The encoder is responsible for embedding the secret message into the cover image. It takes both the cover image and the secret message as input. The encoder algorithm determines how the message will be hidden within the pixels of the cover image, making subtle changes that are difficult to detect by the naked eye.

3. Stego-Image: - After the encoder has done its work, the result is the stego-image. This is essentially the modified cover image with the secret message hidden within it. To most observers, it should still appear like the original cover image.

4. Decoder: - The decoder is the counterpart to the encoder. It takes the stego-image as input and extracts the hidden secret message. It does this by using a decoding algorithm that knows how to reverse the encoding process and retrieve the original message.

5. Secret Message: - This is the information you want to keep hidden within the cover image. It can be text, an image, or any other form of data. The secret message is typically encrypted or compressed before embedding it into the cover image to ensure data integrity and security.

The goal of this system is to transmit sensitive information covertly, using the cover image as a disguise. Steganography techniques aim to hide the existence of the secret message, making it difficult for unauthorized parties to detect or decipher the hidden data. However, it's important to note that the effectiveness of steganography depends on the chosen algorithms and the ability to resist various forms of analysis.

Least significant bit (LSB): In the LSB algorithm, the least significant bit in each byte of a multimedia file (e.g., an image or audio) is modified to convey a hidden message.

1.Text steganography

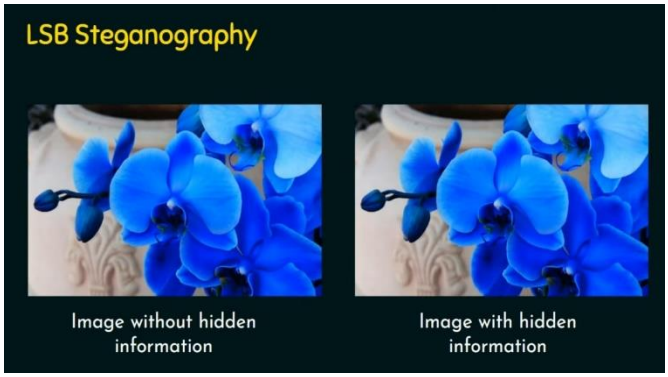
Text steganography conceals a mystery message inner a bit of text. The simplest version of text steganography might use the first letter in each sentence to form the hidden message. Other textual content steganography strategies may consist of including significant typos or encoding facts via punctuation.

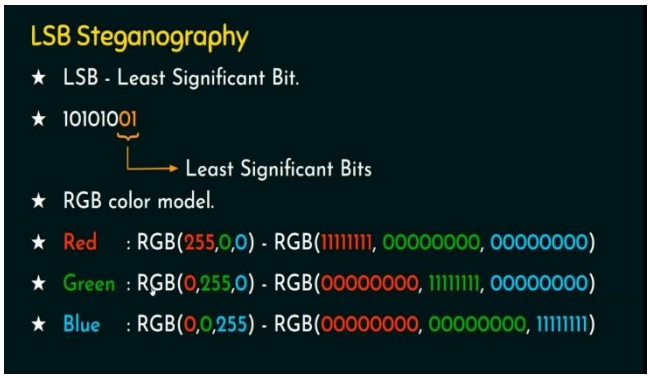
2. Image steganography

In photo steganography, mystery records is encoded inside a virtual photo. This method is based at the truth that small adjustments in picture colour or noise are very tough to discover with the human eye. For example, one photo may be hid inside some other through the use of the least full-size bits of every pixel withinside the photo to symbolize the hidden photo instead.

3. Video steganography

Video steganography is a more sophisticated version of image steganography that can encode entire videos. Because virtual motion pictures are represented as a chain of consecutive images, every video body can encode a separate image, hiding a coherent video in undeniable sight.





ADVANTAGES

• The main advantage of this system is Security that it provides security to your communications.
• Normal network junkies can't guess images.
• In steganography anyone cannot jump on a suspect by looking at images.
• It's Reliable.
• Easy to use.
• Easy preservation.
• System has been secured by countersign authentication.

DISADVANTAGES

• **Finding –** Steganography can be problematic to discover, but with the advancement of technology and methods, it becomes easier to uncover the secret information.
• **Limited data capacity –** Steganography has a limited capacity for data, meaning that only small measures of information can be hidden within a queue.
• **line size increase –** The process of hiding information within a column can bring the range size to increase, making it more potent and easier to determine.
• **Complexity –** Steganography can be a complex process, needing technical software and a certain standing of specialized skills.

USES

• Confidential Communication and Secret Data Storing.
• Protection of Data Alteration.
• Access Control System for Digital Content Distribution.
• Database Systems.
• Digital Watermarking.
• Secure data transmission.

HARDWARE AND SOFTWARE REQUIREMENTS

Recommended Operating Systems
• **Windows** 7 or newer
• **MAC OS** X v10.7 or high
• **Linux** Ubuntu or Kali

SOFTWARE REQUIREMENTS
Supported Browser

• Firefox
• Chrome

OTHER IMPORTANT SOFTWARE

• PHP
• XAMPP
• Database MySQL
• Visual Studio Code 2010

TACKLE DEMANDS

• **Processor Minimum 1 GHz;** Recommended 2 GHz or other
• **Ethernet connection** (LAN) OR a wireless accessory (Wi-Fi)
• **Hard Drive** Minimum 32 GB; Recommended 64 GB or further
• **Memory (RAM)** fewest 1 GB; Recommended 4 GB or ab

CONCLUSION

The LSB commutation steganographic methodology has shown affecting results in data secretion, as it takes advantage of the fact that any image can be broken up into individual bit-airplanes representing different places of information. This technique is effective only for bitmap images as they involve lossless contracting systems. still, it can be extended for use in color images by performing bit-airplane slicing separately for the top four bit-airplanes of each R, G, and B factor of the dispatch image. It's important to note that although steganography was onetime undetectable, with the multicolored styles today used, it isn't only easy to determine the presence of covert information but also to recover it. For prototype, there are simple systems to observe if an image range has been manipulated, corresponding as

1. **Size of the image** A steganographic image has a much larger warehouse size compared to a regular image of the same range. For representative, if the original image repository size is many KBs, the steganographic image could be several MBs in size. This can vary depending on the resolution and type of image used.

2. **Noise in the image** A steganographic image has more noise than a regular image. This is why primarily, a small volume of noise is added to the cover image so that the steganographic image doesn't appear too noisy compared to the original cover image.

REFERENCES

- **S. Sharma et al. (2018)** proposed a steganographic approach for Safe Communication on social media platforms.
- **Singh S, (2019)** "An inspection on steganography and steganalysis methods " Journal of Network and Computer Applications, Vol. 131, pp. 64- 93.
- **Al Saleh et al. (2020)** proposed an original steganographic f orm for Safe communication on the Internet.
- **Manoj Kumar B, Ravikumar K, Gopi Sailesh C, Ravi Kumar CV, (2020)** "Secure Data Communication With Cryptography and Steganography" International Journal of Electrical Engineering and Technology (IJEET), 11(3),pp.164- 172.
- **Saurabh Agarwal, Cheonshik Kim, Ki-Hyun Jung (2022)** "Steganalysis Of setting-conscious Image Steganography methods Usi ng Convolutional Neural Network" MDPI Appl.Sci..
- **DoaaA. Shehab, MohammedJ. Alhaddad (2022)** "Comprehensive Survey of Multimedia Steganalysis tacks, Evaluations, and Trends in Future Research" Symmetry, MDPI, 14, 117.
- **WafaM.Eid, SarahS. Alotaibi, HasnaM. Alqahtani, SaharQ. Saleh** "Digital Image Steganalysis Current Methodologies and Future Challenges" IEEE,10.1109.
- **Numrena Farooq, Arvind Selwal, (2023)** "Image Steganalysis Using Deep Learning: a Systematic Review and Open Research Challenges" Journal of Ambient Intelligence and Humanized Computing, 14, 7761-7793.