IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Hiding Secrets In Images

Sneha C. Raut , Vaishnavi R. Bhalerao , Anisha V. Tatte , Yash A. Thakare

Prof. Shubhangi A. Gulhane

Computer Science And Engineering

P. R. Pote College Of Engineering and Management , Amravati , India

Abstract: Steganography is the method of hiding message in a cover object for cover communication. The article deals with the steganography system which hides text inside images without losing of data (BMP, PNG, TIFF and GIF). The secret message is hidden in the cover image using Last Significant Bit (LSB) method. Paper presents functionalities of the developing software, using LBS methods. Visual and statistical analysis of LBS method indicate the good results of its application

Keywords: steganography, cover image, data hiding, stego image, LSB

I. Introduction

Hiding secrets in images, a practice known as steganography, is the art of concealing information within image files without altering their perceptual quality. By embedding data in the least significant bits or exploiting the color palette, steganography enables the covert transmission of sensitive information. This technique serves as a discreet means of communication, offering a layer of secrecy beyond traditional encryption methods.

Hiding secrets in images involves combining cryptography and steganography to secure information within image files. Cryptography ensures the confidentiality of the data, while steganography conceals it within the image without arousing suspicion. This dual-layered approach enhances data security by making it challenging for unauthorized parties to detect or access the concealed information.Image steganography is the practice of concealing a message within an image without effecting its visible characteristics. The cover source can be changed in the pixels that have significant variations in colors, which will make the modifications less obvious.

II. FUNCTIONAL COMPONENT

1.Carrier Image: The image in which you want to hide the secret information. A carrier image, in the context of steganography, is an image that contains hidden data within it. This technique involves embedding information, such as text or another image, into the pixels of the carrier image in a way that is imperceptible to the human eye. The hidden data can be extracted using specific algorithms or software, revealing the concealed message or content. It's often used for covert communication or digital watermarking.

2.Secret Data: The information you want to conceal within the image. Secret data must be preprocessed for security reasons. Encrypting the hidden data prevents them from being illegally accessed or unscrambled. Some existing encryption techniques, such as DES and RSA others can be used to encrypt hidden data. Secret data also can be compressed in advance using lossless compression techniques to reduce the amount of hidden data and increase the visual quality of stego-image, and thus deceive potential grabbers.

3.Embedding Algorithm: A method to embed the secret data into the carrier image without significantly altering its appearance. Data-embedding algorithms may be used to establish ownership and distribution of data. In fact, this is the application of data embedding or watermarking that has received most attention in the literature. Unfortunately, most current watermarking schemes are unable to resolve rightful ownership of digital data when multiple ownership claims are made, i.e., when a deadlock problem arises.

4.Extraction Algorithm: A method to retrieve the hidden information from the image. The counterpart to the embedding process, this component extracts the hidden data from the stego-image. It must accurately recover the original secret data without introducing errors.

5. Key or Password: In some cases, a key or password may be required to encode or decode the hidden information. This adds an additional layer of security to the steganographic process.

6. Security Measures: Depending on the sensitivity of the hidden information, additional security measures may be implemented, such as encryption of the secret data before embedding or digital watermarking to detect unauthorized modifications.

III. Methodology

In the concrete realization the method consists of several main steps:

1. Embedding a confidential message:
   - Enter the text which must be hidden;
   - Choose the image which must be hidden;
   - Create a key (password);
   - Choose the settings-choose number of bits;
   - Embed the message;
   - Save the stego image.

2. Extracting the confidential message:
   - Load the stego file;
   - In order to extract information the user must input a key;
   - The extraction of information is executed;
   - After completing the information the message is stored in a file.

Embedding a confidential message using steganography involves several key steps. Initially, format your confidential message appropriately, choosing plaintext or encrypted text. Select a cover image with visual complexity to avoid suspicion, and then use a steganography tool like Steghide or OpenStego to embed the message into the image. Adjust settings for encryption or strength based on security needs. Optionally, add a password for extra security.

Extract the confidential message, use the same steganography tool and follow the reverse process. Input the steganographic image, apply the tool to extract the hidden data, and, if necessary, provide the password. Verify the extracted message against the original to ensure accuracy. Always adhere to ethical and legal standards when using steganography, respecting privacy and applicable laws.

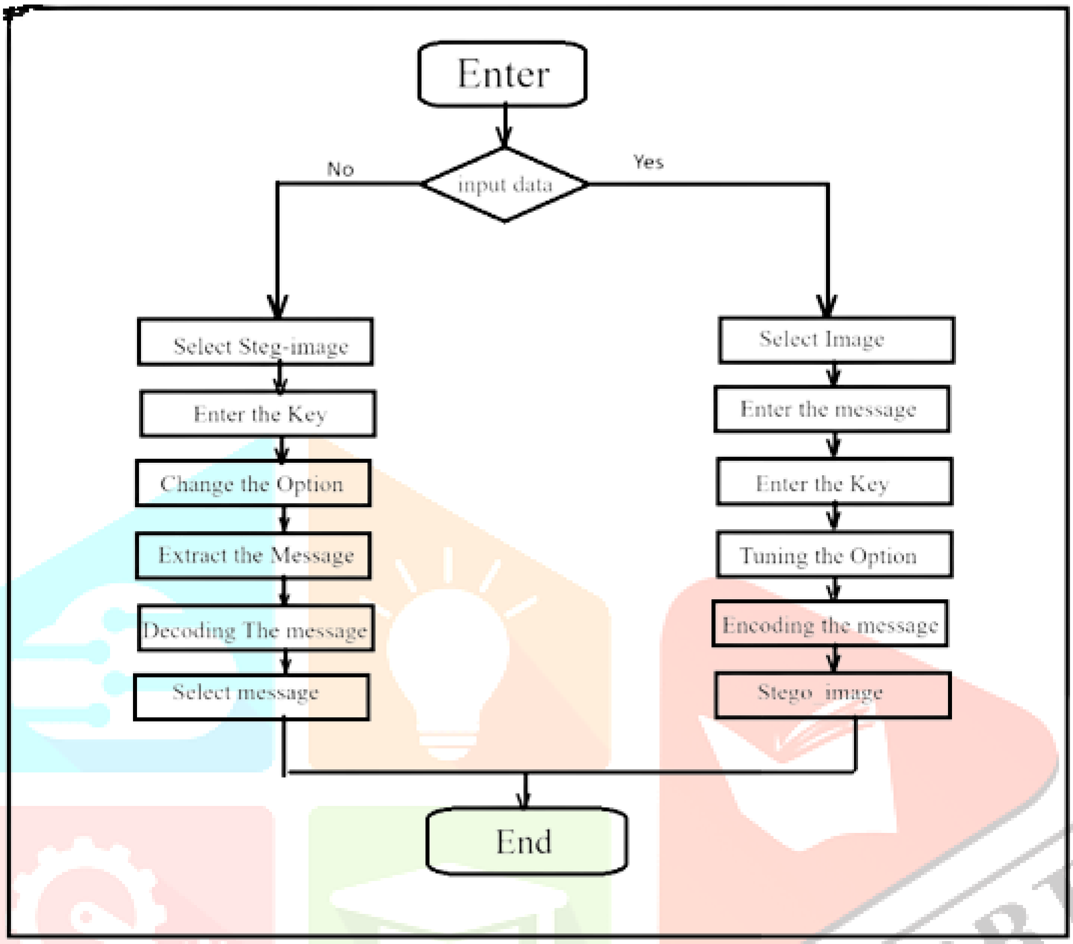

Fig.01 Block Scheme of the Program System

IV. BENEFITS OF IT SECRETS IN IMAGES

1. Security through Obscurity: Provides an additional layer of security by relying on the obscurity of the hidden data, making it less likely to be detected.

2. Data Smuggling: Facilitates the smuggling of small amounts of data past security measures without raising suspicion.

3.Enhanced Privacy: Enhances privacy for confidential messages or files, particularly in situations where traditional encryption methods might be more conspicuous.

4.Stealthy File Transfer: Allows for covert file transfer, as steganographic images can be shared openly without indicating the presence of hidden information.

5.Digital Watermarking: Supports positive applications like digital watermarking, helping protect intellectual property and verify the authenticity of content.

6.Creative Security Measures: Introduces a creative and non-conventional security measure, making it more challenging for unauthorized individuals to detect and access sensitive information.

V. CONCLUSION

This method hides more number of bytes of secret data into cover image compare to other existing method. Steganography can be used for hidden communication. The speed of embedding the data into the image is also high in the proposed approach such that the image is protected and the data to the destination is sent securely.

VI. REFERNCES

- G. R. Aishwarya and K. R. Aishwarya's "A Study on Image Steganography Techniques"2021.
- I. M. ,. G. P. ,. B. C. Pratap Chandra Mandal.""Digital image steganography: A literature survey",2022.
- I. Aljazaery, and M. Aziz, "Combination of hiding and encryption for data security," hj,hk., vol. 10, no. 15, pp. 10-20, 2020.
- P. S. Ritu Sindhu, “Information Hiding using Steganography,” Vols. Volume-9,(2020).
- M. H. Mahdi, A. A. Abdulrazzaq, M. S. Mohd Rahim, M. S. Taha, H. N. Khalid, and S. A. Lafta. (2019) ‘Improvement of Image Steganography Scheme Based on LSB Value.
- R. Singh and P. Kaur's article "A Comprehensive Review on Image Steganography Techniques" 2019.
- Z. S. L. Y. Wu S., “ Deep residual learning for image steganalysis, Multimedia tools and applications,” pp. 2018.
- A. B. A. M. &. A. M. Zeki, “PSW statistical LSB image steganalysis,” 2017.
- A. H. K. Masoud Nosrati, “Steganography in Image Segments Using Genetic Algorithm,” 2015.
- Morgan Kaufmann, “Digital Watermarking and Stegnography: Fundamentals and Techniques” 2007.

VII.AUTHOR

- Prof. Shubhangi A. Gulhane
- Sneha C. Raut
- Vaishnavi R. Bhalerao
- Anisha V. Tatte
- Yash A. Thakare