iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.62552

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

Image Steganography

Rashmeet Kaur[1], Shivani Agarwal[2], Dr. Sadhana Rana[3]
Department of Computer Science and Engineering, Shri Ramswaroop Memorial College of Engineering and Management, Lucknow, Uttar Pradesh, India

Abstract: Steganography is the art of hiding the fact that communication is taking place, by hiding by information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of stenographic techniques some are more complex than others and all of them have respective strong and weak points. This project intends to give an overview of image steganography, its uses and techniques. It also supports steganography in Audio files. For a more secure approach, the project encrypts the message using secret key and then sends it to the receiver. The receiver then decrypts the message
Keywords: Encryption and Decryption, LSB Algorithm

I. INTRODUCTION

Steganography is the art of hiding the fact that communication is taking place, by hiding by information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of stenographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden.

This project intends to give an overview of image steganography, its uses and techniques. It also supports steganography in Audio files. For a more secure approach, the project encrypts the message using secret key and then sends it to the receiver. The receiver then decrypts the message to get the original one.

Image steganography is a technique used to hide secret information within an image file without altering its perceptual quality. This method ensures the confidentiality and integrity of the hidden data, making it imperceptible to the human eye and various forms of analysis. In the context of computer security and privacy, image steganography plays a vital role in secure communication.

.

II. LITERATURE SURVEY

A. Encryption and Decryption

The user needs to run the application. The user has two tab options: encryption and decryption. When the user selects Encrypt, the application displays a screen for selecting image files, information files, and options for saving image files. When the user selects Decrypt, the application throws the screen to select only the image file and asks the user for the path to save the secret file.

There are two methods for this project: encryption and decryption.

With encryption, confidential information is hidden in all types of image files. Confidential information is retrieved from the image file during decryption.

A new technique for steganography was presented, implemented and analyzed. The proposed method hides the secret message based on a search for the same bit between the secret message and the image pixel value.The goal of steganography is secret communication. The basic requirement of this steganography system is to ensure that the hider messages sent by Stegomedia are not perceived by humans.

Another reason for steganography is to not suspect the existence of hidden messages. This approach to information hiding technology has recently become important in many application areas.

The purpose of this project is to: Develop security tools based on steganography technology.

1) Explore techniques for hiding data using the encryption module of this project.

2) Find out methods for retrieving private data using the decryption method.

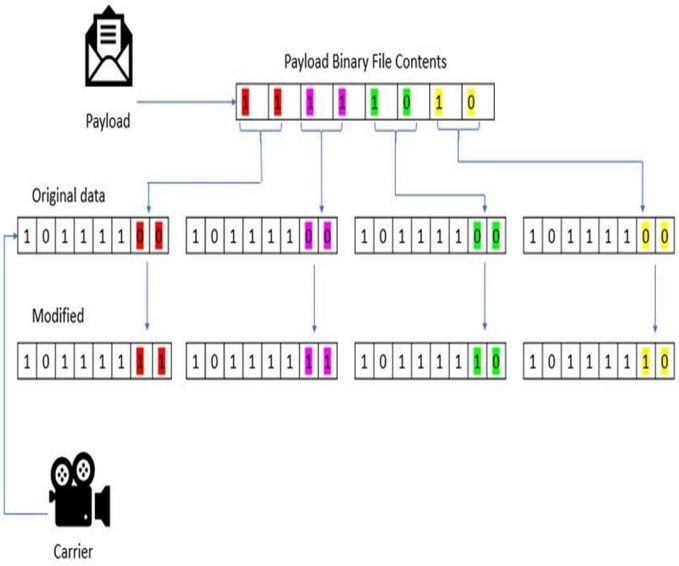
Steganography may be used if encryption is not allowed.

Or, more commonly, steganography is used to complement encryption. Encrypted files can use steganography to hide information, so when an encrypted file is decrypted, the hidden message is not displayed.

B. LSB ALGORITHM

LSB embedding is the most common technique for embedding message bits. DCT coefficient. This technique is also used in spatial domains where the least significant bit value of a pixel is changed and a 0 or 1 is inserted. A

The recipient then extracts the hidden message bits by reading the coefficients in the same sequence and decoding them according to the coding techniques performed on them. The advantage of LSB embedding is that it has a high embedding ability and is usually inconspicuous to the human eye On the other hand, there is almost 1 bit per pixel for each color component, which can provide larger spatial domain embedding capacity. However, sending a raw image, such as a bitmap (BMP), to the recipient makes it suspicious in itself, unless the image file is very small.



III. PROPOSED METHODOLOGY

The proposed approach for designing a frameworkto illustrate the functionality of an algorithm can be summarized as follows:

1) The user has two tab options: encryption and decryption.
2) When the user selects Encrypt, the application displays a screen for selecting image file in which the message is to be embedded.
3) When the user selects Decrypt, the confidential information is retrieved from the embedded image.

IV. MODULE DESCRIPTION

The module description for a image steganography project could outline the various components and functionalities of the software system :-

A. Authentication

Authentication Form is used to provide permission to view this project. The following details needed for Authentication Form

1) Username
2) Password

The following operations are carried out in this form:

Ok

It consists of the username and the password fields. If these fields are valid then only it's possible to view this project. If these fields are invalid it's prompt out the error message like "Invalid String".

Cancel

It's used to cancel the user action.

B. Embedding A Message In A Picture

FILE: This module is used to hide message in picture files. Image Location, Save File Location, Encryption Key are provided by the user to hide message in the save file location.

1) Image location-The Image file, which is already, exists in the system. User has to open the file from the open dialog box. IMAGE STEGANOGRAPHY 161
2) Save the file -This is also an Image file, which is generated by the user. User has to save this new file in any location according to their wish. This file is used to embed the message in the image file.
3) Encryption Key-This key is the private key. This is confidential key between sender and receiver. This is also embedded in picture with message.
4) Validation code-This is actual file size of the image location. This is in bytes. The message is added to the saved image location after this last byte.
5) Hide-It is used to hide the message into saved image file. Messages are encrypted in unknown format and then embed in the saved image file.
6) Send-The user to another user uses this button to send the saved image file, which contains the message hided.

C. Retriving The Embedded Message From The Picture File

1) Extract Messages- This module is used to extract messages.
2) Image Location-Downloaded images by the user are given as input in this text box.
3) Encryption key- The key used to extract the message. This a secret key. Receiver should know this key to retrieve message.
4) Validation Code-This is the offset of the file where actually the message is reside.
5) Extract message- When receiver clicks this button the message is shown to the receiver. Encrypted messages are decrypted and then shown in the text box.

V. IMPLEMENTATION

This part gives subtle elements of the sensible prerequisites, non-utilitarian necessities, asset prerequisites, equipment necessities, programming necessities then on. Again the non-utilitarian prerequisites thus contain item necessities, authoritative prerequisites, client prerequisites, fundamental operational necessities so on.

1) Limitations of the Software: This project has an assumption that's both the sender and receiver must have shared some secret information before imprisonment. Pure steganography implies that there is none prior information shared by two communication parties.
2) Detecting Steganography: The art of detecting Steganography is spoken as Steganalysis.

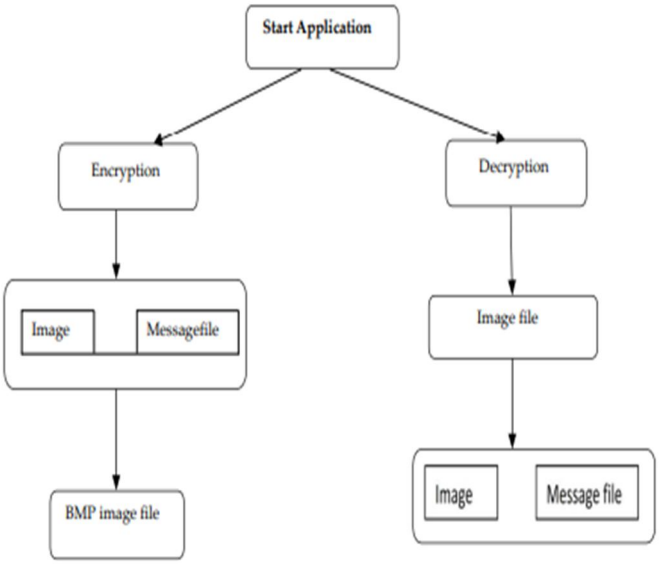
To put is simply Steganalysis involves detecting the use of Steganography within a file. Steganalysis doesn't cater to trying to decrypt the hidden information inside a file, just discovering it.

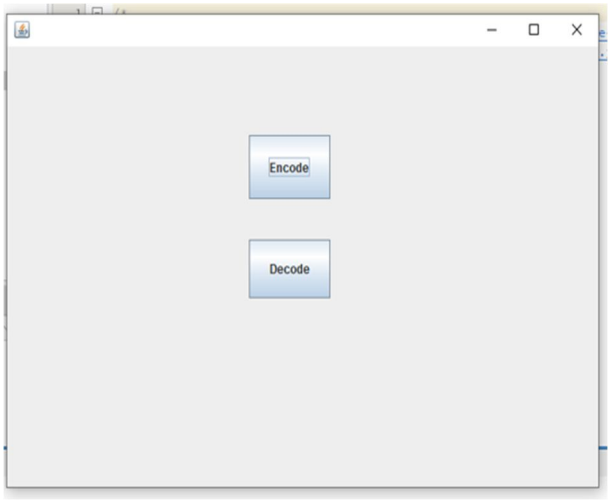
There are many methods which is ready to be accustomed detect Steganography such as:

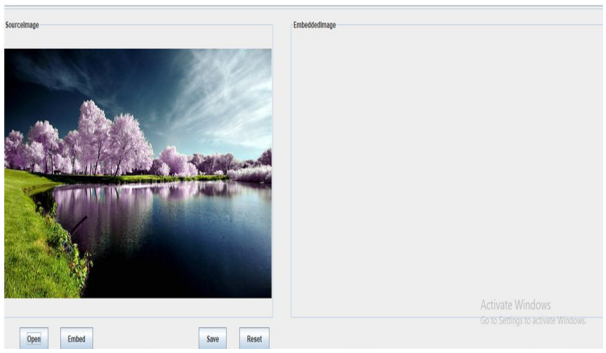
“Viewing the file and comparing it to a special copy of the file found on the online (Picture file). There are usually multiple copies of images on the net, so you may want to seem for several of them and take a glance at and compare the suspect file to them. as an example if you download a JPEG and your suspect file is additionally a JPEG and therefore the 2 files look almost identical apart from the actual fact that one is larger than the alternative, it's most probable you suspect file has hidden information within it.

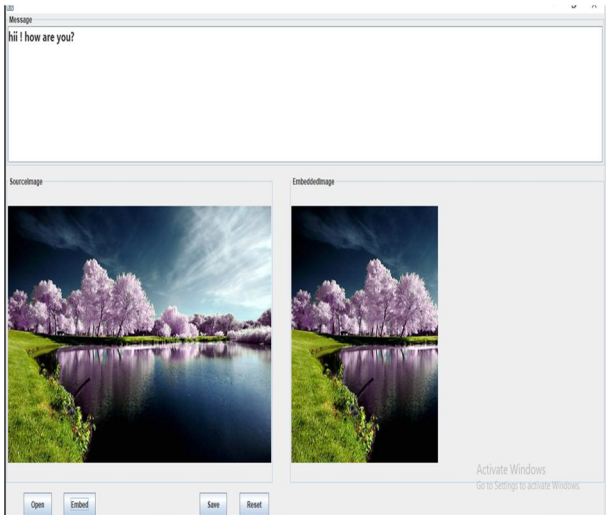
VI. RESULT

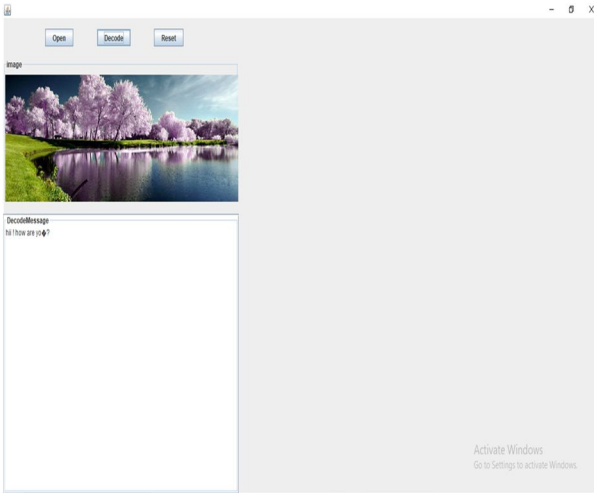
Steganography systems need to hide all types of image files and information or messages. There are two modules for encryption and decryption. The algorithm used for encryption and decryption in this application is to use multiple layers instead of using the LSB layer of the image. Writing data begins at the last layer (8th or LSB layer). This layer is the least important, as each upper layer doubles the importance of the lower layer. Each time you go to a higher image level, the image quality will be degraded and you will see a retouch of the image. The encryption module is used to hide the information in the image. No one can see this information or files. This module requires any type of image and message and only specifies the image file as the target. Decryption module is used to get the hidden information in the image file. Receives an image file as output and outputs two files to the destination folder. One is the same image file and the other is a message file hidden inside. Before you can encrypt a file in an image, you need to save the name and size of the file in a specific location in the image. You can save the file name before the file information in the LSB layer, and save the file size and file name size in most pixels in the lower right corner of the image.


Start Application
Encryption
Decryption
Image
Messagefile
Image file
BMP image file
Image
Message file


Encode
Decode


SourceImage
EmbeddedImage
Open
Embed
Save
Reset





VII. CONCLUSION AND FUTURE SCOPE

Steganography is a really interesting topic that goes beyond the basic encryption and system administration that most of us deal with on a daily basis. Steganography can be used for covert communication. We explored the limitations of the theory and practice of steganography. To provide a secure means of communication, we printed enhancements to our image steganography system using an LSB approach. Stego-key was put on to the system while encrypting the data in the cover image.

This steganography application software is designed to use image format to hide any type of file inside. The main and most important work of this system is in supporting all types of pictures without necessarily converting it in bitmap, and also reducing limitation on the size of file to hide, as it uses maximum space of memory to hide file inside a picture.Since long ago man has a desire to fine something from which he can secretly communicate.

In the recent time with the vast research in watermarking to protect intellectual property is proof that steganography is not only limited to military or surveillance applications. Like cryptography steganography will also play an increasing role in future to secure the communication in the world which is digitally growing.

In terms of future scope of project, some points are mentioned below :

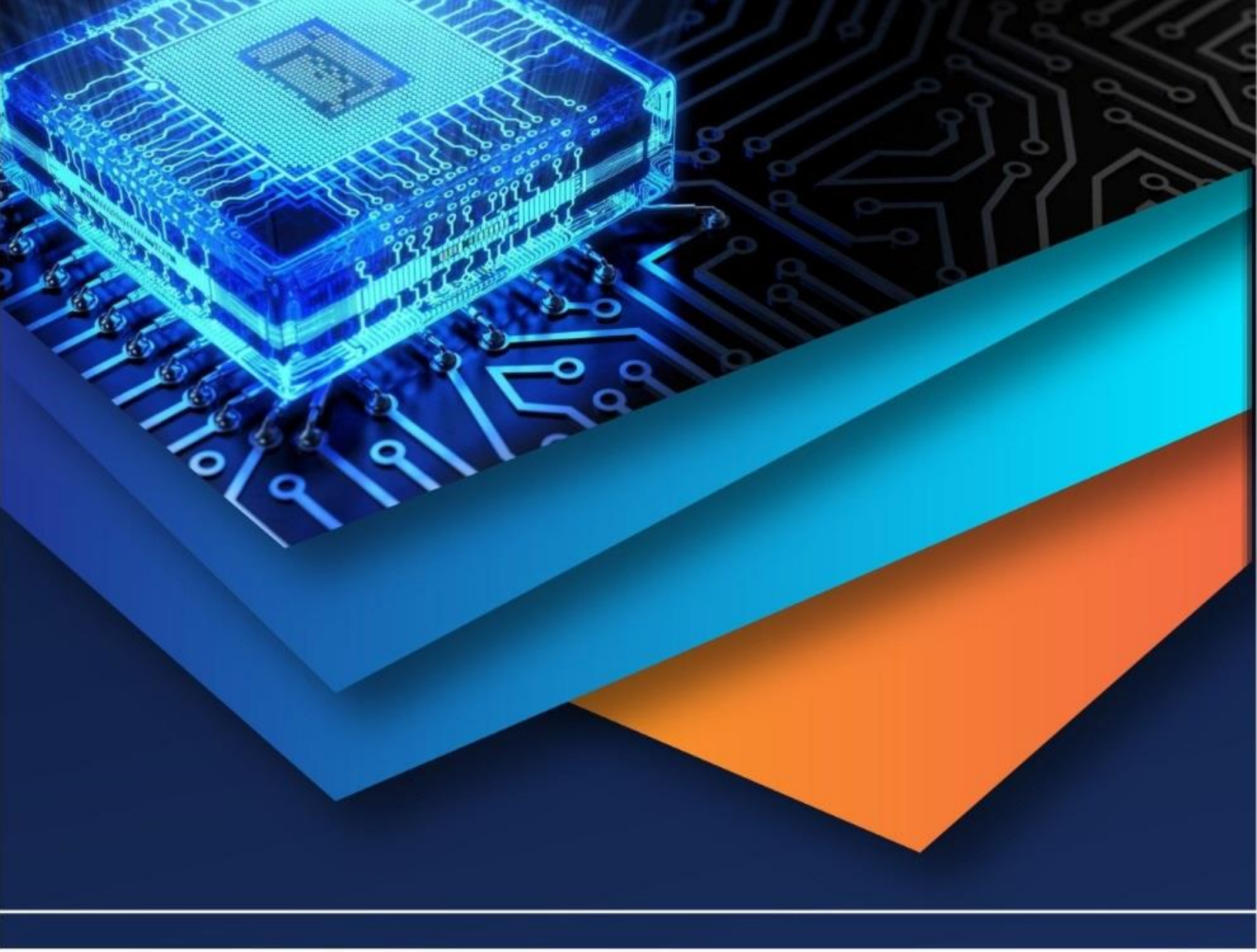
1) An ideal steganographic algorithm should have high precision, a higher level of security with good embedding capacity.

2) The concepts of steganography through PVD, weighted matrix, graph neighbourhood, DCT, and DWT are well known. But the idea of combining weighted matrix with graph neighbourhood, DCT, or DWT is quite new.

In the future, the researchers may give attention to this area and explore how to use .Future Scope spatial domain techniques in transform domain to solve some reallife problems. A variety of optimization schemes can be used to improve the cost of the steganographic algorithm and enhance the quality of the stego image. These include particle swarm optimization (PSO), ant colony optimization (ACO), neural networks (NN), fuzzy logic, hybrid network and genetic algorithm (GA), etc. These optimization algorithms may help to embed a secret message within a cover image in such a way that it improves stego image quality, embedding capacity, and imperceptibility.

REFERENCES

[1] Pahati, Omar J. "Confounding carnivore: How to protect your online privacy." AlterNet. Archived from the original on (2007): 07-16.
[2] Hariri, Mehdi, Ronak Karimi, and Masoud Nosrati. "An introduction to steganography methods." World Applied Programming 1.3 (2011): 191-195.
[3] Pal, Pabitra, Partha Chowdhuri, and Biswapati Jana. "Weighted matrix based reversiblewatermarking scheme using color image." Multimedia Tools and Applications 77.18 (2018): 23073-23098.
[4] Ahmad, Mostafa A., et al. "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images." Alexandria Engineering Journal 61.12 (2022): 10577-10592.
[5] Rostam, Habib Esmaeelzadeh, Homayun Motameni, and Rasul Enayatifar. "Privacy- preserving in the Internet of Things based on steganography and chaotic functions." Optik 258(2022): 168864.
[6] Kurane, S., H. Harke, and S. Kulkarni. "TEXT AND AUDIO DATA HIDINGUSINGLSBAND DCT A REVIEW APPROACH."Natl. Conf."Internet Things Towar. a Smart Futur."Recent Trends Electron. Commun. 2016.
[7] https://ieeexplore.ieee.org/document/6516338
[8] https://www.geeksforgeeks.org/image-steganography-in-cryptography/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY