Securing Military Communications

Using LSB Steganography

Project submitted for the partial fulfillment of the requirements for the course

CSE 337L: Cryptography Lab

Offered by the

Department of Computer Science and Engineering

School of Engineering and Sciences

Submitted by

1) Kumar Sashank Ganta | AP20110010229

2) Solleti Krishna Chaitanya Subhash | AP20110010232

3) D.Yogesh | AP20110010240

4) Kancharla Prahlad Reddy | AP20110010242

SRM University–AP

Neerukonda, Mangalagiri, Guntur

Andhra Pradesh – 522 240

[December, 2022]

Contents:

Introduction

Steganography is a technique used by military personnel to securely communicate without leaving any trace of their activity. This method of communication involves hiding data within other data, such as text, images, or audio.

This allows the user to send a message without anyone knowing the true content of the message. By using this method, military personnel can securely transmit sensitive information without the risk of it being intercepted or compromised. Steganography can also be used to verify the authenticity of a message, as it is much more difficult to forge a message that has been encoded using steganography.

Overall, this technique allows military personnel to securely and covertly communicate with one another, ensuring that their information remains confidential.

Background

The military uses steganography in a variety of ways, including covert communication, secure data storage, and hiding classified information.

For example, a soldier may use steganography to securely communicate a message to another soldier by hiding it in a seemingly innocent image or audio file. Similarly, classified data can be hidden within an image or audio file, making it difficult to detect without the proper tools.

Overall, steganography is a powerful and important tool for the military, allowing it to securely communicate and store sensitive and classified information.

Other Possibilities:

Other possibilities or future improvements include encrypting the text using more secure encryption algorithms such as AES or RSA and then hiding the encrypted text in an image. Then the image can be encrypted and sent to the receiver.

Proposed Approach

➢ Flow Chart

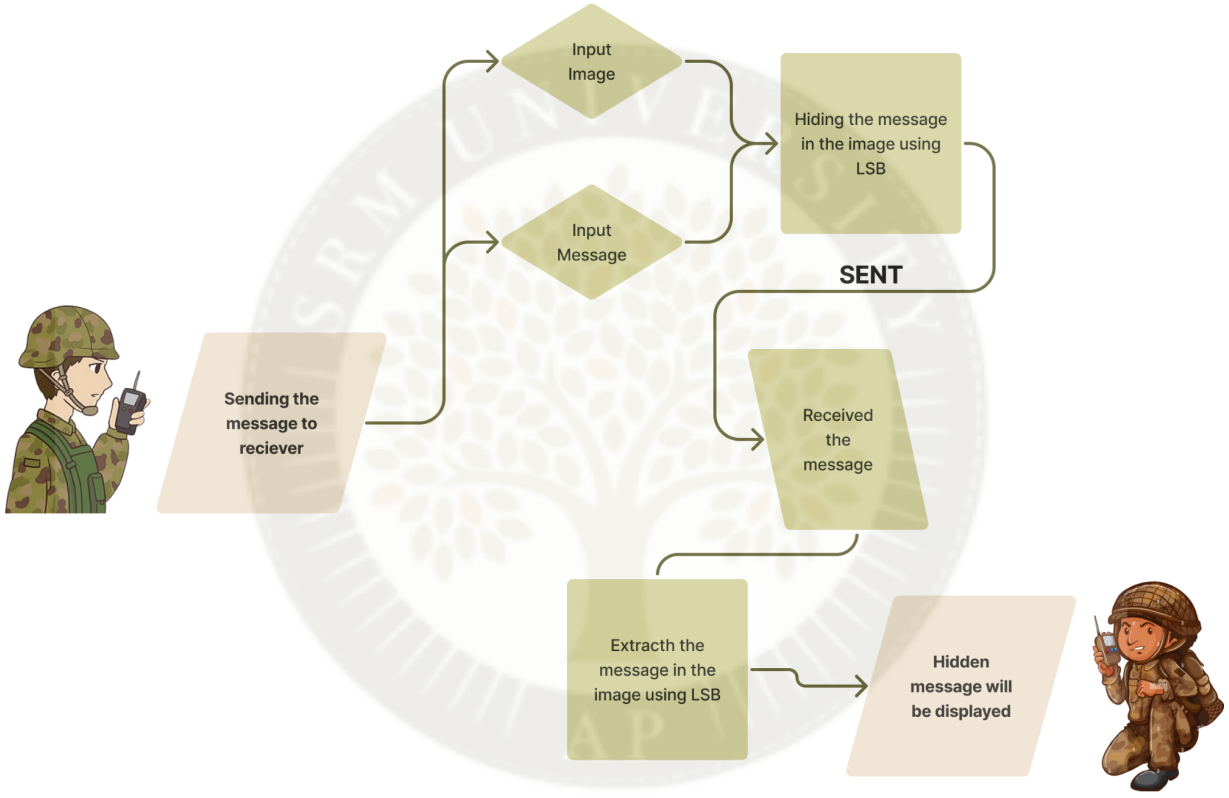

fig:1 flow diagram (communication between army personnel)

➢ System Design

Image Steganography is a technique used to hide secret information in an image. The system design of Image Steganography consists of the following steps:

1. Data Embedding: This process involves selecting the secret data to be embedded, choosing an appropriate algorithm, and encoding it into a suitable format such as ASCII or binary.

2. Steganography: This is the process of hiding the secret data inside the image. It can be done by replacing some of the least significant bits in the image with the secret data.

3. Data Extraction: This is the process of extracting the secret data from the image. It is done by reading the least significant bits of the image and decoding the secret data.

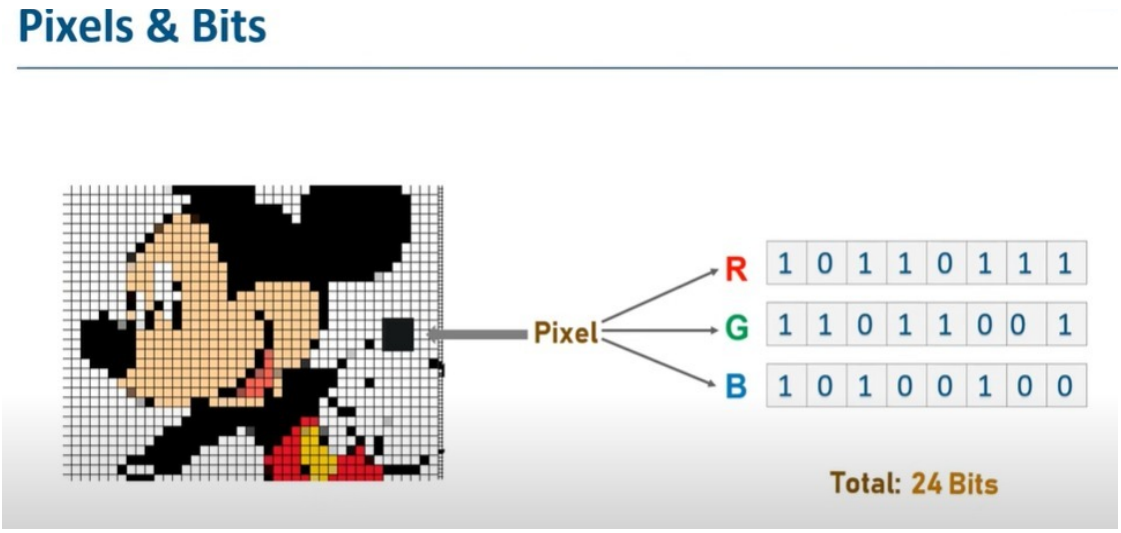

fig.2: Pixel RGB description

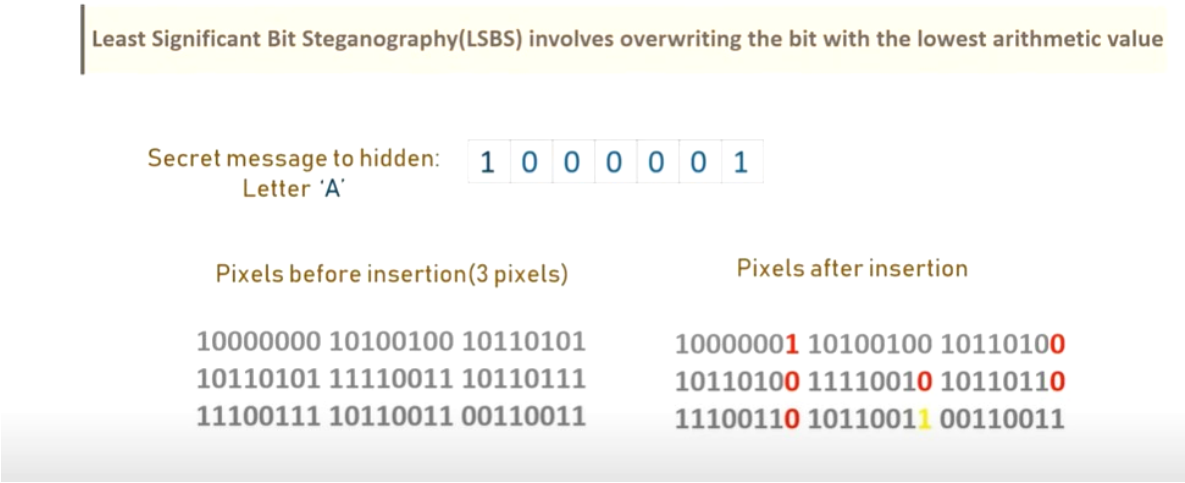

fig.3: Insertion of message bits

Results & Discussion:

- In this program, two interfaces are utilized: one to hide information and another to access it from the image.
- Through running hideGUI Matlab program, a GUI appears to interact with the user, allowing them to select the image file by typing the filename in the image name box and entering the message in the text input box.
- Once the hide button is clicked, the image with the information is produced as a secret.bmp file.
- To access the information, the user needs to initiate the retrieveGui Matlab program. By selecting the secret.bmp file, the information is retrieved and stored in the secret.txt file.

- **Sample Input Output:**

Hiding:

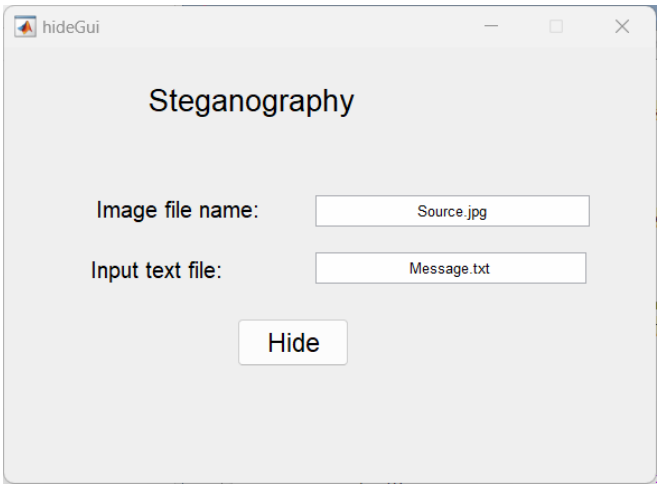

fig.4: hideGui dialog box

The HideGUI displays an image file and a plain text file as inputs. When the Hide button is clicked, the program generates a hidden image.

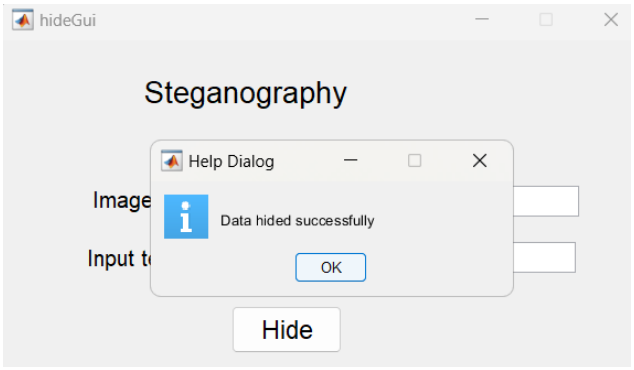

fig.5: data hiding

Retrieving:

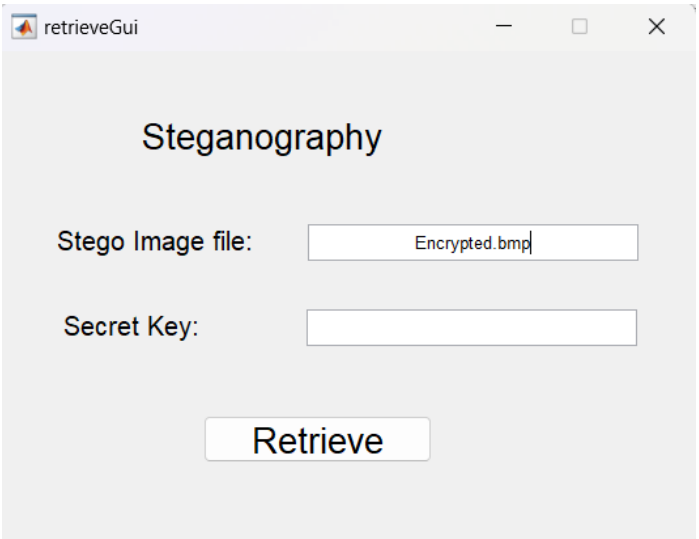

fig.6: data extraction

Once the retrieveGui is initiated, it prompts us to enter the encrypted file. Upon doing so, the retrieve button is clicked which then generates the decrypted image and plain text file.

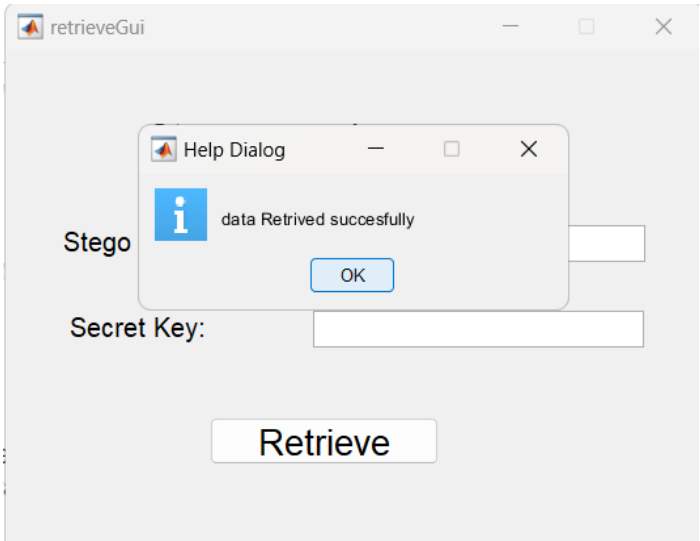

fig.7: secret text file generation

Conclusion

In conclusion, steganography is a powerful tool for secure communication and data hiding. It allows for secure data exchange and storage by hiding data in plain sight. It has many applications in both commercial and military contexts and can be used in a wide variety of ways. Steganography is an important component of any information security strategy, as it allows for secure communication and data storage that is undetectable by conventional methods of detection. As technology continues to evolve, the uses of steganography are sure to expand.

Limitations:

1. Capacity: Steganography has limited capacity for hiding data due to the fact that it can only hide limited amounts of data in a given medium.

2. Detectability: Steganography is not completely secure as there are various ways to detect hidden messages.

3. File size: Steganography usually increases the size of the file, thus making it more obvious that something is hidden in the medium.

4. Complexity: It can be quite complex to hide data in a medium, and it requires specific software or tools to successfully complete the task.

5. Cost: Steganography requires additional hardware or software, which may add additional costs.

References

https://en.wikipedia.org/wiki/Steganography

https://www.youtube.com/watch?v=xepNoHgNj0w&t=1067s

https://www.youtube.com/watch?v=JeV-WKK1A9Y&ab_channel=Pranjalkalal

https://github.com/anuragiiits/Image-and-Video-Steganography/blob/master/Image%20Steganography/hideGui.m

https://www.google.com/imgres?imgurl=https://www.researchgate.net/publication/345267201/figure/fig3/AS:954017823875088@1604466982933/Traditional-LSB-Image-Steganography.png&imgrefurl=https://www.researchgate.net/figure/Traditional-LSB-Image-Steganography_fig3_345267201&tbnid=cTz6NFjZe0aplM&vet=1&docid=OWqd2NTy3EmtCM&w=850&h=683&itg=1&source=sh/x/im