STEGANOGRAPHIC TECHNIQUES IN DIGITAL IMAGES

## A PROJECT REPORT FOR J COMPONENT

**INFORMATION SECURITY ANALYSIS AND AUDIT (CSE3501)**

# BY:

# JATIN KUMAR (18BCB0072)

# FACULTY NAME:

RAMANI S

Assistant Professor, Scope, VIT Vellore

**FALL SEMESTER 20-21**



**ABSTRACT**

We the students of VIT, Vellore have made a project on “**STEGANOGRAPHIC TECHNIQUES IN DIGITAL IMAGES**” as our Image Processing project for the fourth semester. Our goal was to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganographic techniques are more suitable for which applications. Steganography is the process of hiding one file inside another such that others can neither identify the meaning of the embedded object, nor even recognize its existence. 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 steganography techniques. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. The techniques have been used to create the watermarks that are in our nation’s currency, as well as encode music information in the ever- popular mp3 music file. Copyrights can be included in files, and fingerprints can be used to identify the people who break copyright agreements. However, this technology is not always used for good intentions; terrorists and criminals also use it to convey information. According to various officials and experts, terrorist groups are “hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards, and other Websites”.

**REVIEW 3**

TABLE OF CONTENTS OF PROJECT

1. **INTRODUCTION**
2. **LITERATURE SURVEY**
3. **BACKGROUND OF YOUR PROJECT WORK**
   1. Various components of your work
4. **PROPOSED WORK**
   1. Block Diagrams and Architectures of your Project
5. **EVALUATION AND RESULT DISCUSSIONS(Grouped in one)**
   1. Should have Tables, diagrams, snaps
   2. Every Table and diagram should be explained
   3. Use proper caption for diagrams/snaps/tables
6. **TABULAR COMPARISON WITH EXISTING WORKS.**
7. **CONCLUSION**
8. **REFERENCES**

**INTRODUCTION**

Steganography is an ancient technology that has applications even in today’s modern society. A Greek word meaning “covered writing” steganography has taken many forms since its origin in ancient Greece. During the war between Sparta and Xerxes, Dermeratus wanted to warn Sparta of Xerxes pending invasion. To do this, he scraped the wax off one of the wooden tablets they used to send messages and carved a message on the underlying wood. Covering it with wax again, the tablet appeared to be unused and thereby slipped past the sentries inspection. However, this would not be the last time steganography would be used in times of war.

In World War II, the Germans utilized this technology. Unlike the Greeks, these messages were not physically hidden; rather they used a method termed “null ciphering” Null ciphering is a process of encoding a message in plain sight. For example, the second letter of each word in an innocent message could be extracted to reveal a hidden message.

Although its roots lay in ancient Greece, steganography has continually been used with great success throughout history. Today steganography is being incorporated into digital technology. The techniques have been used to create the watermarks that are in our nation’s currency, as well as encode music information in the ever-popular mp3 music file. Copyrights can be included in files, and fingerprints can be used to identify the people who break copyright agreements. However, this technology is not always used for good intentions; terrorists and criminals also use it to convey information. According to various officials and experts, terrorist groups are “hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards, and other Websites”.

The above aspect of steganography is what sparked the research into this vast field. Education and understanding are the first steps toward security. Thus, it is important to study steganography in order to allow innocent messages to be placed in digital media as well as intercept abuse of this technology.

#### What is Steganography?

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information.

What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file.

1. **History of Steganography:**

Throughout history Steganography has been used to secretly communicate information between people. Some examples of use of Steganography is past times are:

1. During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just being blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances are heated they darken and become visible to the human eye.
2. In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secrete message.
3. Another method used in Greece was where someone would peel wax off a tablet.

#### Why This Steganography?

This technique is chosen, because this system includes not only imperceptibility but also un- delectability by any steganolysis tool.

**LITERATURE SURVEY**

#### Sumedha Sirsikar, Jagruti Salunkhe , “Analysis of data hiding using Digital Image Signal Processing”,2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies[2]

In this paper, many different image processing techniques are elaborated for data hiding related to pixel value differencing. There has been implementation of Steganographic tool and analyzed all evaluation metrics like MSE, PSNR and SSIM for data hiding methods such as Hamming, OPAP, Zig-Zag, Modified and Adaptive. Comparison of all the methods show that Adaptive data hiding method gives the better result as compared to any other methods.

#### Shreyank N Gowda, “Using Blowfish Encryption to Enhance Security Feature of an Image”, 2016 6th International Conference on Information Communication and Management[3]

In this paper, an algorithm is proposed that significantly enhances the security of the algorithm. The proposed algorithm increases the capacity of hiding data since we use more images. The proposed algorithm takes a little more time to execute than the standard LSB. The most important aspect here is that the LSB is easily decoded. By using the proposed algorithm it can increase the security factor of an image.

#### Hiding Secret Message in Edges ofthe Image Kh. Manglem Singh, L Shyamsudar Singh, A. Buboo Singh and Kh. Subhabati Devi[4]

The paper proposes a new least significant bit embedding algorithm for hiding the secret messages in non-adjacent pixel locations of the edges in the images. The purpose of steganography is to hide the very existence of a message from a third party. The author ensures in this way a better security against eavesdroppers. It has been shown experimentally that the blind LSB detection technique like the gradient energy method couldn’t estimate the exact length of the secret message bits very accurately for the proposed algorithm.

#### Studying of Stability of the Information Hiding Methods in Still Images AndriyAstrakhantsev, OleksiyDoroghan, OleksandrPoponin, NataliyaShostak[5]

The paper proposes that Steganography is hiding messages (by embedding) in the digital data, like speech, image, audio or video, text files. The main advantage of steganography to cryptographically protect information is provided that hides the very existence of our confidential information during transmission, storage or processing. In this paper, the comparative analysis of the two information hiding methods (LSB and Kutter) characteristics is presented. The authors analyzed the resistance to intentional attacks and noise in the communication channel. They were also able to obtain the values of SNR depending on the number of re-embedding and embedding energy.

#### Wei Liu, “Data Hiding in JPEG 2000 Code Streams”,2004 International Conference on Image Processing (ICIP) [6]

This paper proposed an integrated data embedding and image compression scheme to hide secret messages into JPEG 2000 code streams. Its high embedding capacity, progressive extractability and visual transparency have been proven by the experiments. This paper proposed a new steganography scheme which is supposed to be more robust, progressively extractable, and of high visual fidelity.

#### L.Jani Anbarasi and S.Kannan, “Secured Secret Color Image Sharing With Steganography” [7]

This paper proposed that in the existing methods, the reconstructed shadows are meaningless and the distortions are large. The proposed reversible image sharing approach for color image reveals the secret image without loss and preserves the cover image. The generated shadows are meaningful with better PSNR value compared with the previous methods. Based on (t, n) threshold scheme, any t authorized recipients can recover the secret by using the reversible process. This methodology can be further enhanced for 3D images and can be used for embedding text.

#### TushinaBedwal and Mukesh Kumar, ”An Enhanced and Secure Image Steganographic Technique using RGB-Box Mapping”, Computer Science & Engineering Department [8]

In this paper a new image steganographic scheme for RGB image is proposed which provides improved security and improved image quality as evident from PSNR values. Further, use of key-boxes as stego key and concept of mapping enhances the security, as no one could extract the embedded secret image from cover image without the knowledge of mapping technique being used. The proposed scheme, pixels of secret RGB image are embedded in only 3 LSB bits of channels of cover image using mapping. It is a modified least significant- bit (LSB) method, resulting in improve perceptibility.

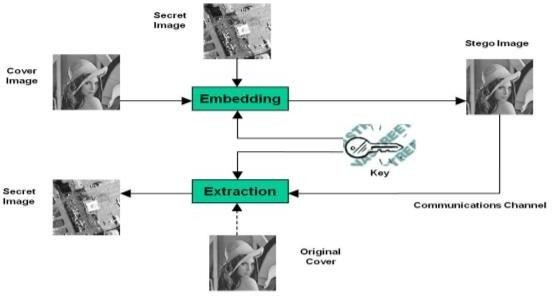
#### “Digital Steganography: Hiding data within a data”, Donovan Artz [9]

This paper proposed that Steganography and steganalysis are beginning to receive increased attention as their applications become more relevant to the needs of governments, businesses, and individuals. As privacy concerns continue to develop along with the digital communication domain, steganography will undoubtedly play a growing role in society. For this reason, it is important that we are aware of digital steganography technology and its implications. Using steganographic techniques, software can easily transmit private user information without the user’s permission or knowledge. Steganography, as mentioned, enhances rather than replaces encryption. Messages are not secure simply by virtue of being hidden.

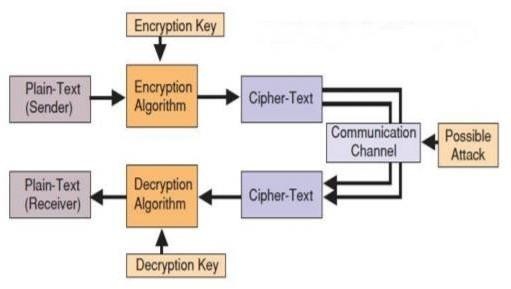
**BACKGROUND WORK OF OUR PROJECT**

User needs to run the application. The user has two tab options – encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file. This project has two methods – Encrypt and Decrypt. In encryption the secret information is hiding in with any type of image file. Decryption is getting the secret information from image file.

There are many techniques for performing STEGANOGRAPHIC techniques and each one has its own benefits and disadvantages.



Encryption is a method or a process for protecting information from undesirable attacks by converting it into a form non recognizable by the attackers. Data encryption is mainly the scrambling of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or incomprehensible during transmission.



**PROPOSED WORK**

* 1. **Encryption Process:**

During first phase of the algorithm:-

1. Generating the random strings and saving it into text file (in this case, creating 1000 random string)
2. Input the Text message for the encryption.
3. Generating the key for the text.

a) Getting all the lines from the entered text and inserting them into the arrLines string array. b) Lines will be separated by the "." operator.

1. From the arrLines array, arrWord array will be filled by all the words of the specific lines.
2. By working on specific lines and on all the words of the lines, start the encryption process.
3. Getting the character of the word one by one for the processing.
4. Filling the arrSeq array that have the range for all the character (symbols, integers, alphabets)
5. Convert the incoming character into its asciivalue.
6. Find the range corresponding to the incoming char. Ascii value by using arrSeq array.
7. By using the range, generate a random integer between that range and fetch thats no’s position random string from the random string txt file. Ex – for the asciii value 65, 651 – 660 is the range. Let 653 is the random no. generated, then find the random string placed on the 653th place in the random string text file.
8. After getting the random ascii string of that character, add four parameter in that.

Four parameters are:

* 1. linoNo (line number frm which that word relates),
  2. posOfW (position of the word in that line),
  3. lengthOfW (length of that word) and
  4. posInWo (position of character in that word).

In 2nd phase, apply some mathematical operation in that encoded string.

1. Now key comes into play, store the entire individual integer in the arrKey array and all the individual ascii value into the arrCodes array.
2. In this case here using 5 length long integer value and performingrespective mathematical operation on each value:
3. Ascii + first integer
4. Then multiplied by second integerc. Then Ascii – third integer \* 20
5. Then Ascii- fourth integer\*5 e.ThenAscii-fifth integer

# Decryption Process:

Following is the decryption process which involves the use of same key as generated during encryption process.

1. Using the key of length 5 (here used), apply the following mathematical operations which are performed.
2. Ascii - fifth integer
3. Then Ascii +fourth integer\*5
4. Then Ascii + third integer \* 20
5. Then Ascii- second integer
6. Then Ascii- first integer
7. Inserting the changed value of code in array 3.Inserting the decrypted code value

The random string generated is shown by considering and processing the four parameters taken.

1. From the random string generated, the particular character is retrieved.
2. The outputted text is the original message.

**EVALUATION AND RESULT DISCUSSION**

# OUTPUT:

## INPUT IMAGE:

## C:\Users\jatin\Pictures\9.jpg

## EMBEDDING MESSAGE:

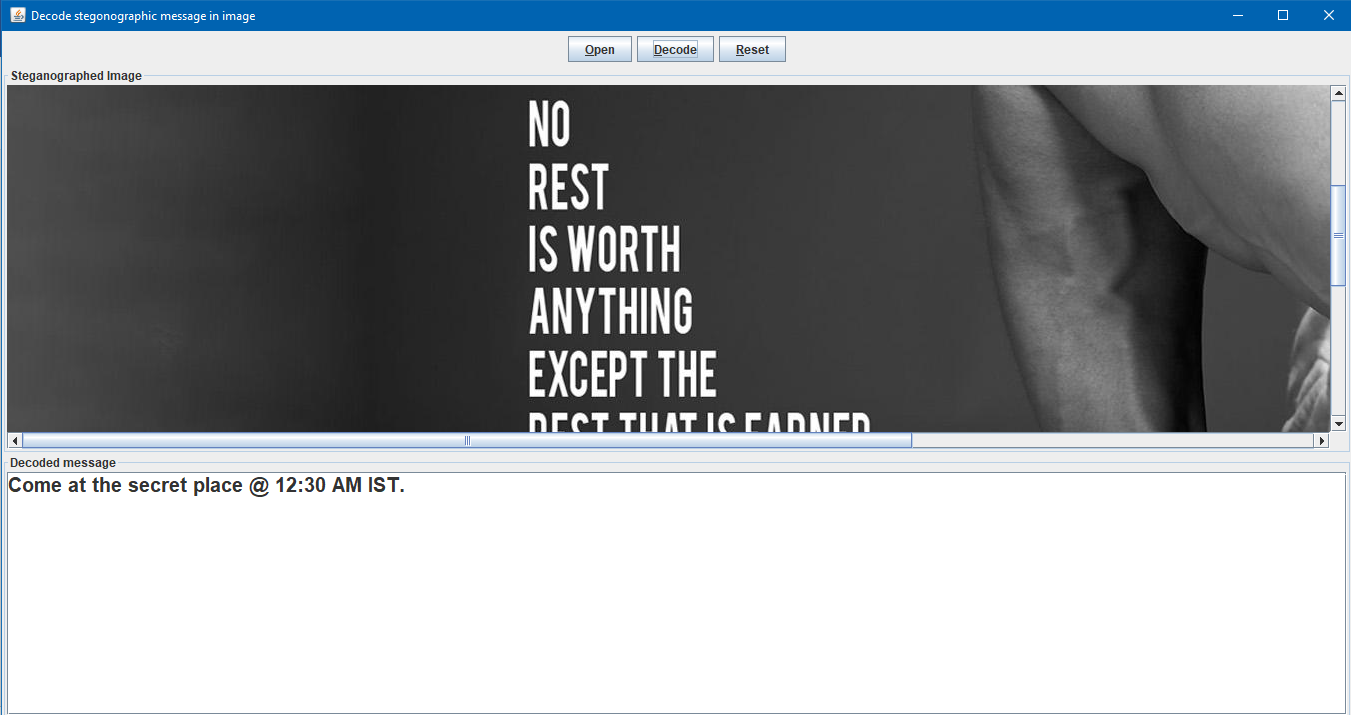
## 

**AFTER ENCRYPTION:-**

ENCRYPTED\_IMAGE:



DECODING MESSGAE:



**COMPARISON WITH EXISTING WORKS**

Already discussed in Literature Survey but also presented here in a tabular form:

|  |  |  |
| --- | --- | --- |
| Info about the Paper | Methodology used in the paper | Why is our approach better |
| Sumedha Sirsikar, Jagruti Salunkhe , ”Analysis of data hiding using Digital Image Signal Processing”,2014 International Conference on Electronic Systems, Signal Processing and Computing  Technologies | In this paper, many different image processing techniques are elaborated for data hiding related to pixel value differencing. There has been implementation of Steganographic tool and analyzed all evaluation metrics like MSE, PSNR and SSIM for data hiding methods such as Hamming, OPAP, Zig-Zag, Modified and Adaptive. | In this paper only the various methods have been discussed. We have applied the result of this and used adaptive data hiding method which gives us the better results than most of the above things. |
| Shreyank Gowda,”Using Blowfish Encryption to Enhance-Security Feature of an Image”, 2016 6thInternational Conferenceon Information Communication and Management. | In this paper, an algorithm is proposed that significantly enhances the security of the algorithm. The proposed algorithm increases the capacity of hiding data since we use more images | The proposed algorithm takes a little more time to execute than the standard LSB. The most important aspect here is that the LSB is easily decoded. By using the proposed algorithm it can increase the security factor of an image. |
| Hiding Secret Message in Edges of the Image Kh. Manglem Singh, L Shyamsudar Singh, A. Buboo Singh and Kh. Subhabati Devi | The paper proposes a new least significant bit embedding algorithm for hiding the secret messages in non-adjacent pixel locations of the edges in the images. The purpose of steganography is to hide the very existence of a message from a third  party. The author ensures in this way a | It has been shown experimentally that the blind LSB detection technique like the gradient energy method couldn’t estimate the exact length of the secret message bits very accurately for the proposed algorithm. |

|  |  |  |
| --- | --- | --- |
|  | better security against eavesdroppers. |  |
| L. Jani Anbarasi and S. Kannan, ”Secured Secret Color Image Sharing With Steganography” | This paper proposed that in the existing methods, the reconstructed shadows are meaningless and the distortions are large. The proposed reversible image sharing approach for color image reveals the secret image without loss and preserves the cover  image. | The generated shadows are meaningful with better PSNR value compared with the previous methods. Based on (t, n) threshold scheme, any t authorized recipients can recover the secret by using the reversible process. |
| “A PSNR-Controllable Data Hiding Algorithm: Based on LSBs Substitution”, Huaibo Sun, Hong Luo, Tin-Yu Wu, Mohammad S. Obaidat | In this paper a new image steganographic scheme for RGB image is proposed which provides improved security and improved image quality as evident from PSNR values. Further, use of key-boxes as stego key and concept of mapping enhances the security, as no one could extract the embedded secret image from cover image without the knowledge of mapping  technique being used. | The proposed scheme, pixels of secret RGB image are embedded in only 3 LSB bits of channels of cover image using mapping. It is a modified least significant- bit (LSB) method, resulting in improve perceptibility. |

# CONCLUSION

Interest in the usage of steganography in our current “digital world” can be attributed to both the desire of the man to communicate in a covert manner, to hide communication through the medium rife with the potential listeners, or in the case of the digital watermarking, the necessity of maintaining the control over a person’s ownership and the data integrity as it passes through that medium. This recent explosion of the research in watermarking to protect the property which is intellectual is the evidence that the applications of steganography is not limited only to the military or the espionage. Steganography, just like cryptography, will definitely play an increasing role in future of the secure communication in this digital world.

# REFERENCES

* 1. Steganography - A new technique to hide information within image file - by Mr. AtanuMaity.
  2. SumedhaSirsikar, JagrutiSalunkhe , ”Analysis of data hiding using Digital Image Signal Processing”,2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.
  3. Shreyank N Gowda,”Using Blowfish Encryption to Enhance Security Feature of an Image”, 2016 6thInternational Conference on Information Communication and Management.
  4. Hiding Secret Message in Edges ofthe Image Kh. Manglem Singh, L Shyamsudar Singh,

A. Buboo Singh and Kh. Subhabati Devi.

* 1. Studying of Stability of the Information Hiding Methods in Still\_ImagesAndriyAstrakhantsev, OleksiyDoroghan, OleksandrPoponin, NataliyaShostak.
  2. L.JaniAnbarasi and S.Kannan, ”Secured Secret Color Image Sharing With Steganography”
  3. TushinaBedwal and Mukesh Kumar, ”An Enhanced and Secure Image Steganographic Technique using RGB-Box Mapping”, Computer Science & Engineering Department
  4. “Digital Steganography: Hiding data within a data”, Donovan Artz
  5. “A PSNR-Controllable Data Hiding Algorithm: Based on LSBs Substitution”, Huaibo Sun, Hong Luo, Tin-Yu Wu, Mohammad S. Obaidat
  6. [www.ieeexplore.ieee.org](http://www.ieeexplore.ieee.org/)
  7. https://image.slidesharecdn.com/steganoppt-121026131532-phpapp01/95/steganography- 34-638.jpg?cb=135125740