EasyChair Preprint

№ 6019

Digital Steganography

Rishitha Gudipati

July 5, 2021

"DIGITAL STEGANOGRAPHY"

(Rishitha Gudipati,

Computer Science and Engineering

Kakatiya Institute of Technology and Science, Warangal)

Abstract--Maintaining confidentiality of data is very crucial in large corporations because there is lot of chance to hack the data by the hackers. So securing information is very important. For exchanging secret information we already have cryptography which is successfully transmitting this information to the required destination. But, it will give a suspicion to the hackers and it affects unintended users. This project Digital Steganography overcomes this factor and provides a solution for exchanging the secret information without affecting the unintended users. This Steganography uses multimedia data for covering secret information. By using this, data which is the secret information can hide within multimedia data such as image. This can be sent anywhere and transfers the message easily without giving any suspicion to others.

***Keywords*--** *Steganography, multimedia, secret information.*

I. INTRODUCTION

Steganography is one of the most trusted methods to transfer data without giving any indication to the unintended user. This process basically includes hiding of data under any multimedia such as images, video etc.

This steganography can be performed in different ways such as text steganography, audio steganography, video steganography, image steganography. In text steganography secret information is covered by some other text. Next in audio steganography information is covered by audio, in video steganography under video, under image steganography under image.

In this project we focus on digital steganography. In this the secret information is hidden under any image.

II. SYSTEM ANALYSIS

Existing System:

In the existing system we already have cryptography to transmit secret information from sender to receiver but this gives indication to the hackers as the structure of the message is scrambled, the hacker can easily identify that the sender is transmitting some secret information. So this fails to transmit secret information successfully from sender to receiver.

Proposed System:

This project Digital Steganography gives the solution to the problem of sharing secret information without giving any hint to the hackers. This method uses multimedia data (here image) to cover the secret information. This multimedia data acts as the covering medium for this information. By this we can transfer any data without giving any suspicion to the hackers. The features of this proposed system is it is user friendly and very flexible.

III. SYSTEM ARCHITECTURE

This architecture consists of two modules:

1. Creating stegano medium

This module includes making of stegano medium. This medium mainly focuses on hiding of the secret information under an image. For this we need to make a stegano medium. In this firstly we choose a image and select a key. This key is used by receiver to extract secret information for the stegano file. Then enter the information you want to share with the receiver. After entering all these a image will be generated under which the information is hidden. Now this image is sent to the user.

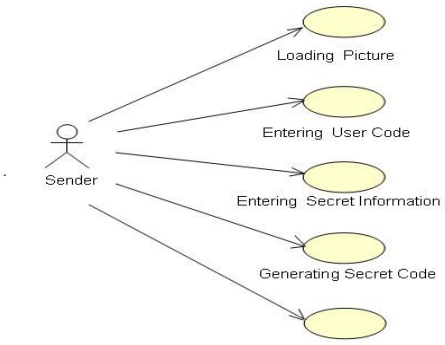
2. Extracting secret information from the stegano medium

After receiving the image from the sender the receiver must extract the secret information from that image. For this the receiver should enter the steganographic medium. Then they should enter the key selected by the sender. After entering the key the receiver goes into the stegano medium where they can see the secret information sent by the sender.

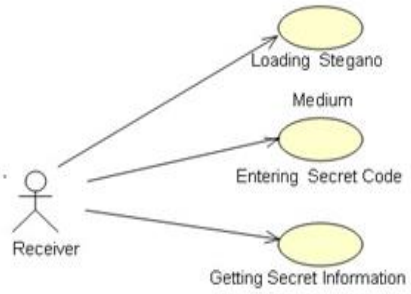
These are the two modules for sending and receiving the secret information without giving suspicion to others.

SOFTWARE MODELING

Sender Case Diagram:

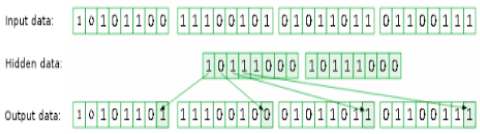


Receiver case diagram:



IV. LEAST SIGNIFICANT BIT(LSB) ALGORITHM

In this project we use least significant bit algorithm. In this the last bit of the pixel is called least significant bit. Let us consider the size of pixel as 1 byte. This 1 byte equals to 8 bits. The last bit of this is called a least significant bit because changing the last bit data shows less effect on the entire data.



So taking this into consideration the last bit of the pixel stores the data bit which is to be transmitted to the receiver.

V. CONCLUSION AND FUTURE SCOPE

Digital steganography provides a user friendly environment for sharing of data without giving any clues to the hackers where this data is hidden under image. Thus we can say that the user can transfer any type of data to the receiver. In future this may overcome all its drawbacks and provides best security. For this one idea is to include all four types of steganographic methods into one which in trun increases the security. The data hidden under image should also be encrypted so even though if anyone knows the key cannot know the information.

VI. REFERENCES

1. **"**Information Hiding in Images Using Steganography Techniques" Ramadhan J. Mstafa, Christian Bach(2013)

2. "Image based steganography" A Gutub, M Ankeer, M Abu-Ghalioun(2009)

MERITS AND DEMERITS

As the structure of the message is not changed the hacker cannot identify that the image contains secret data. So this reduces the chances of data getting hacked. By this the security of data increases. As every coin has two sides even this has disadvantages. One disadvantage is if anyone other than receiver knows the key they can easily extract the information and there are so many chances of misusing this and also if anyone knows the algorithm used for this they can also extract information easily. But advantages are more compared to disadvantages.