VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Steganography- Secure Data Hiding

(Information Security Analysis and Audit- CSE 3501)

Under the Guidance of

Mr. SIVA SHANMUGAM

Submitted by

PARAG SINGH - 19BCE0633

SURABHI VENKATA PHANI KUMAR - 19BCE0512

Abstract

Steganography is a form of security technique through obscurity, the science and art of hiding the existence of a message between sender and intended recipient. Steganography has been used to hide secret messages in various types of files, including digital images, audio and video. The three most important parameters for image steganography are imperceptibility, payload, and robustness. Different applications have different requirements of the steganography technique used. This report intends to give an overview of image steganography, its uses and techniques.

Introduction

Steganography is the art of hiding secret data, by implanting it into an audio, video, image or text file, which is identified as a carrier or data carrier, more precisely. It is one of the approaches used to guard secret or sensitive data from malicious attacks. Cryptography and steganography are two methods used to defend secret data.

The difference is that cryptography makes the data unreadable, or hides the meaning of the data, while steganography hides the existence of the data. In steganography, on the other hand, we have sensitive data concealed inside some usual carrier data, which is undoubtedly just an image file, or another text file. That is the advantage of steganography; the data cannot be recovered if the hacker does not even know that there is some data fixed in something that seems unimportant like the carrier data. Image Steganography refers to the process of hiding the information within an image file. The image nominated for this purpose is called the cover-image and the image gained after steganography is called the stego-image.

In this project, we deal with encrypting text in an image file using BPCS technique. The BPCS algorithm is applied in a three-dimensional domain in which the payload bits are rooted into the least significant bits of cover image to originate the stego- image ordinal images, sound clips, and even implemental files. Most BPCS Steganography Experimental Program places use duplicate data for the vessel of the secret data. We have proposed a new technique to hide secret information in a color image. It is not built on a programming technique, but is created on the property of the human vision system. Its information hiding volume can be as large as 50% of the unique image data.

Survey report

Title: A Novel Technique for Data Steganography

Author: Amjad Y. Hindi, Majed O. Dwairi, Ziad A. AlQadi

Idea of Paper: In this paper, a novel stego-method will be introduced, which can be used to hide any secret message in any holding color image. The proposed method will be implemented and tested and the calculated parameters will be compared with the LSB method parameters. It will be shown that the proposed method provides a high-security level by using two keys to extract the secret message from the holding image, making it very difficult to hack.

Advantage/Disadvantage: The obtained results were acceptable when compared with the results of the LSB method. LSB method suffers from low security level. The proposed stego-method provides a high security level, because it needs two keys to extract the secret message from the holding image, each of these keys consisting of eight decimal digits making the process of penetration very difficult.

Title: Image Steganography: A Review of the Recent Advances

Author: NANDHINI SUBRAMANIAN, SOMAYA AL-MAADEED, OMAR ELHARROUSS, AHMED BOURIDANE

Idea of Paper: The main goal of this paper is to explore and discuss various deep learning methods available in the image steganography field. Deep learning techniques used for image steganography can be broadly divided into three categories -traditional methods, Convolutional Neural Network-based and General Adversarial Network-based methods. Along with the methodology, an elaborate summary on the datasets used, experimental set-ups considered and the evaluation metrics commonly used are described in this paper

Advantage/Disadvantage: This paper has elaborated on the techniques used in the recent times for image steganography, the current trends. Along with it, details on the datasets and evaluation metrics are detailed. Challenges faced some discussions on the gaps and the scopes for future direction are evaluated in this paper. It can be concluded that deep learning has tremendous potential in the image steganography field taking into consideration that all the challenges and gaps are filled.

Title: Image Steganography Using Mid Position Value Technique

Author: Srilekha Mukherjee, Subhajit Roy, Goutam Sanyal

Idea of Paper: This paper presents a stenographic approach of concealing the secret data to facilitate secure communication. Arnold transformation has been imposed on the chosen cover image in the first stage. This results in the scrambling of the data bits, thereby disrupting the normal pixel orientation.

Advantage/Disadvantage: In this paper, a stenographic approach in image medium which masks the secret data bits that we want to communicate without any third party intervention. Application of Arnold Transform on the host image layers a level of security in the beginning of the procedure itself. The MPV technique follows a conditional strategy while embedding secret data bits. Thus, the overall security is endorsed. This methodology promotes high embedding capacity of the carrier image. The experimental results affirm that the generated stego is imperceptible. Therefore, it does not attract the attention of unwanted sources. This work can be extended to accommodate more secret data bits within the carrier medium. Alongside, there must be no chances of introducing any kind of distortion within the generated stego.

Title: An Algorithm for Security Enhancement in Image Transmission Using Steganography

Author: M. Saravanan, A. Priya

Idea of Paper: In this paper, a novel method for the hiding of image information by converting into another format thereby reduces the computational complexity.

Advantage/Disadvantage: A novel algorithm for improving the level of security in image transmission is proposed. Here instead of encrypting the image directly, the input image is scaled and converted into audio format and then transmitted as an audio file. At the receiver side the audio file is once again scaled back to restore the input image. Since the information is in the form of an audio signal, it is much more difficult to recognize the data hidden in the audio signal. Thus the image information is hidden in the audio medium which makes it more robust and secure especially when the transmission takes place in public communication.

Title: Feature Extraction and Analysis using Gabor Filter and Higher Order Statistics for the JPEG Steganography

Author: Swagota Bera, Dr. Monisha Sharma, Dr. Bikesh Singh

Idea of Paper: In the proposed work the efficiency of JPEG steganalysis is tried to increase with the implementation of higher order statistics.

Advantage/Disadvantage: It is having wide applications in smart id generation, forgery detection in forensic department and also to suspect the terrorist activities. Increase in the detection efficiency will be helpful to have prior information about any antisocial act. The work is concerned with the universal steganalysis for the grayscale images. The detection technique highlights the variations in the statistical feature derived from the transformed image. The analysis parameter of the proposed technique is compared with the recent existing JPEG steganalysis DCTR and conventional GFR technique and it is the finding that efficiency of the proposed technique gives the better results.

Title: - Colour Image Steganography Using SHA-512 and Lossless Compression

Link: - https://www.researchgate.net/publication/322331105_Colour_Image_Steganography_

Author: - Ke-Huey Ng, Siau-Chuin Liew, Ferda Ernawan

Year of published: - 2018

Summary: - In the proposed method, image compression is used to compress a message before embedding process starts if the message provided is too large to be embedded into cover image. This enhances the embedding capacity of cover image. A secret key has been utilized to hide secret information into cover image by deciding the position of bits to be substituted. This process provides a new dimension for image steganography. It is very difficult for third party to recover the secret information without knowing the secret key. Another technique which is called the hash function is used to hash the hidden information before embedded into the cover image. At the end of extraction process, original hash value will be compared with the hash value obtained after hashing on extracted message. If there is no difference between both hash values, it means the extracted message is correct. As a conclusion, the proposed method provides better security and ease of use in terms of capacity. For future enhancement, lossy image compression will be carried out to see if it affects the embedding capacity of cover image as compared to lossless image compression. Every stego image should produce a message for user even if it has been tampered. The extraction process will be improved so that user can extract something out of the stego image with or without tampering.

Advantages: -

1. The same size of original image and message image is embedded due to the help of lossless compression, so there is better PSNR for 100% of data embedding.

2. Hash function ensures the security of information so user can determine whether the message obtained is genuine.

3. Three-level security which checks whether:

· The stego-image has been tampered

· The secret key entered is correct

· The extracted message is correct

Title: - A NEW COMBINED METHOD WITH HIGH SECURITY FOR DIGITAL IMAGES STEGANOGRAPHY BASED ON IMPERIALIST COMPETITIVE ALGORITHM AND SYMMETRIC ENCRYPTION ALGORITHM

Link: - https://www.ijrcar.com/Volume_6_Issue_1/v6i101.pdf

Author: - Mohammad Tahghighi Sharabyan, Hamid Ghorbani

Year of published: - 2018

Summary: - Today, with the growing expansion of information and communication technology, the world, through digital data, is moving to the digital world and communications. Meanwhile, the role of internet as a public communication channel is becoming more and more important in the world of communication every day. In addition, maintaining security and creating confidential communications are of particular importance regarding the general structure of this communication channel. Cryptography and information steganography are two important issues in security systems. Both encryption and steganography techniques are not effective for high security information alone, but combining these two methods can greatly improve the confidentiality and security of confidential information. Recently, new hybrid algorithms have been proposed using cryptography and steganography. However, in these methods, attempts have been made to increase the security of censorship by using random factors and hidden keys, most of these methods are broken by examining the statistical components of the images. In this paper, a high-security hybrid approach is proposed to digital images steganography based on the Imperialist Competitive Algorithm and Symmetric Cryptography Algorithm. The proposed method, by considering the Imperialist Competitive Algorithm, creates a high quality, high-security image. Prior to data insertion, symmetric encryption of information takes place, and then encrypted information is embedded in the cover image. The results of the implementation of the proposed method show that in addition to enhancing the image quality of the steganography, it is more secure than other methods

Advantages: - In this paper, they propose a secure method for the secrecy information steganography using the Imperialist Competitive Algorithm and symmetric cryptography in the location area. In the presented method, first, the confidential information was encrypted, then the encrypted information in the cover images was embedded using the Imperialist Competitive. Embedding information in the image pixels was done by considering the LSB method. The results indicate that the use of the proposed scheme increases the security of confidential information and improves the quality of the steganography image and also renders it resistant to attacks. Steganography image is visually recognizable from the corresponding host image. That the proposed algorithm can create a high-quality hidden image and the demand for embedded capacity by satisfying users are satisfactory. Our proposed method is simple and practical for steganography applications. According to the implementation results, the use of cryptographic and steganography configurations can be of great help in increasing the efficiency of security systems. Our next task is to focus on improving the efficiency of the proposed method, especially by using other meta-heuristic algorithms such as Firefly Algorithm, Queen Bee Honey Algorithm.

Title: - Implementation of Secure Steganography on Jpeg Image Using LSB Method

Link: - http://www.ripublication.com/ijaer18/ijaerv13n1_60.pdf

Author: - Danny Adiyan Z, Tito Waluyo Purboyo and Ratna Astuti Nugrahaeni

Year of published: - 2018

Summary: - Image Files are one of the most widely used file types today. This paper describes the use of JPEG image files in Steganography. Steganography is the technique of hiding a message in an image file (cover image) so as not to be known by people who do not have permission to access. This insertion utilizes the smallest bit of pixel units in an image file (Least Significant Bit). In this journal, steganography will be combined with vigenere cipher. Steganography utilizes the weakness of the human eye in viewing the image file, steganography also uses mathematical calculations in inserting messages into the image file. This type of insertion uses the binary of the ASCII code of a character. This paper also compare the size of an image file to the size of the information that can be inserted. Future research is expected to use cryptography not only limited to one method only. Rather it can be applied some cryptographic methods that make messages or information more secure even though messages embedded in a media can be extracted by irresponsible parties, but the information they actually get is not actual, but the encrypted information.

Advantages: - From all the experiments that have been made to JPEG image by using LSB can be listed the conclusion as follows: a. LSB is one technique that can be used to insert information in an image. b. The size of the message does not exceed the size of the cover image. c. The larger image resolution, the larger message or information can be inserted. d. RGB images can hold more information or messages than with Grayscale images of the same resolution. e. The data previously encrypted using vigenere after extracted from the stego image will then be processed again. f. Differences in the use of vigenere cipher encryption is when the message before it is inserted (plaintext) and after it is extracted (ciphertext). In the insertion process is the same as the usual LSB method.

Title: - IMAGE STEGANOGRAPHY USING SECURED FORCE ALGORITHM FOR HIDING AUDIO SIGNAL INTO COLOUR IMAGE

Link: - https://www.irjet.net/archives/V5/i2/IRJET-V5I2263.pdf

Author: - B.G.AAGARSANA, ANJALI, T.K.KIRTHIKA, Mr. S. SIVAKUMAR

Year of published: - 2018

Summary: - The increasing growth of internet application, create the need for secured transmission of secret message, data or information. There exist several methods for providing secured transmission of information. The most attractive and latest approach for information security is steganography. Steganography is the practice of hiding any text data, image, audio or video within another image, audio or video. The main aim of this paper is to hide audio signal into colour image using AES algorithm and circular LSB algorithm. And this embedded output is secured using secured force algorithm which provide another layer of security. At decryption side ADS algorithm provides decrypted output. This image steganography provides hiding of data more effective and efficient manner with help of circular LSB and secured force algorithm. This paper present a more efficient way for hiding secret data into an image and also provides a more secure way of secret communication. Also a novel way of hiding an audio signal into colour image and transmitting through more secured way. This also prevent attackers from hacking the hidden data into the cover medium because only using password the decryption process can be carried out on stego image.

Advantages: - Increasing the layer of security in communication of data using secured force algorithm. The algorithms used in encryption side are

· Advance Encryption Standard Algorithm

· Circular LSB Algorithm

· Secured Force Algorithm And towards the decryption side the algorithms used are

· Advance Decryption Standard Algorithm In this paper both AES algorithm along with Circular LSB algorithm hide the audio in form of data into lsb bit of pixel of image and this encrypted image is further secured it using a password. At the decryption side the if the entered password is correct then ADS algorithm reverse the process of AES algorithm and separate the cover image and hidden data independently.

Title: - PERFORMANCE ANALYSIS OF TEXT AND IMAGE STEGANOGRAPHY WITH RSA ALGORITHM IN CLOUD COMPUTING

Link: - https://aircconline.com/ijsea/V9N1/9118ijsea06.pdf

Author: - Ismail Abdulkarim Adamu and Boukari Souley

Year of published: - 2018

Summary: - The increased demand and use of cloud resources by various users such as institutions, organizations and individuals has drawn so much attention from cloud service providers to provide strong security mechanisms to secure and protect user's data from attacks or unauthorized access by malicious users and intruders. The use of hybrid security techniques such as steganography and cryptography provide strong security techniques to guarantee safety of user data in the cloud. The major advantage of combining cryptography and Steganography to secure user data in the cloud is to make the data difficult to access, modify by unauthorized users, and guarantee secure communication of the data over the cloud without drawing the attention of intruders. The analysis of the two adopted techniques Image steganography and RSA as digital signature and Text steganography and RSA algorithm in this research work shows that, image steganography and RSA as digital signature consumes less resource, executes data faster and provide more robust security compare to text steganography with RSA algorithm. Image steganography and RSA as digital signatures can handle and hide both text, audio, video and image data types as compared to text steganography with RSA algorithm that can only handle and hide text data. Finally, the concept discussed in this research will help to build a strong architecture for security in the field of cloud computing. This kind of structure of security will also be able to improve customer satisfaction to a great extent and will attract more investors in this cloud computation concept for industrial as well as future research farms. In the future, we intend to carry out more simulations on the system in order to evaluate its performance with different image steganography techniques proposed by other researchers.

Advantages: - Text steganography and RSA algorithm perform better than Image Steganography and RSA as Digital Signature in terms of memory used when extracting data with performance difference of -5.09 mb because of the bit size of the image data when extracted. This research work recommends the use of image steganography and RSA as digital signature to cloud service providers and users since it can secure major data types such as text, image, audio and video used in the cloud and consume less system resources.

Existing System

The existing system, which is most commonly used, is cryptography for the sake of data hiding. Cryptography is the science of using mathematics to encrypt and decrypt data to keep messages secured by transforming intelligible data form (plaintext) into unintelligible form (cipher text). The term cryptography has a cryptosystem consisting of plaintext, encryption algorithm, decryption algorithm, Cipher text, and Key. Plaintext is message or data which are in their normal, readable (not encrypted) form. Encryption is the process of converting plaintext to cipher text by using a key. Cipher text results from encryption by applying the encryption key on the plaintext. Decryption is the process of retrieving the plaintext back from the cipher text. The key is used to control the cryptosystem (cipher system), and it is known by the sender and receiver only. While cryptography is very powerful for securing data, the cryptanalysts could succeed in breaking the ciphers by analyzing the contents of cipher text to get back the plaintext.

Gap Analysis

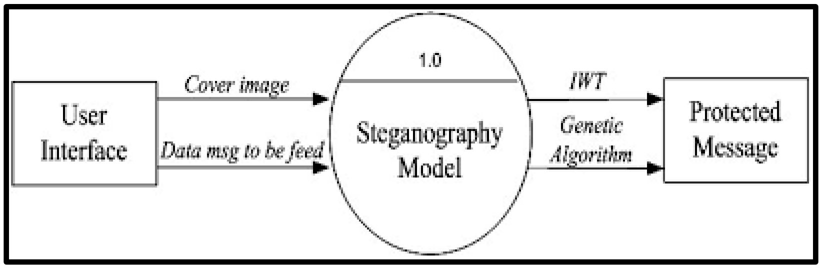
Steganography is considered the art and science of hiding information in other information. The messages are embedded directly into the Least Significant Bits (LSBs). Image steganography system comprises two algorithms, one for embedding and one for extraction. The embedding process hides a secret message within a cover media (cover image), and the result of the embedding process is stego image. The main issue is that the secret message will not be unnoticed if a third party tries to intercept the cover, media (cover image). The extraction process is simply because it is the inverse of the embedding process, where the secret message is revealed at the end.

Drawbacks & Solution

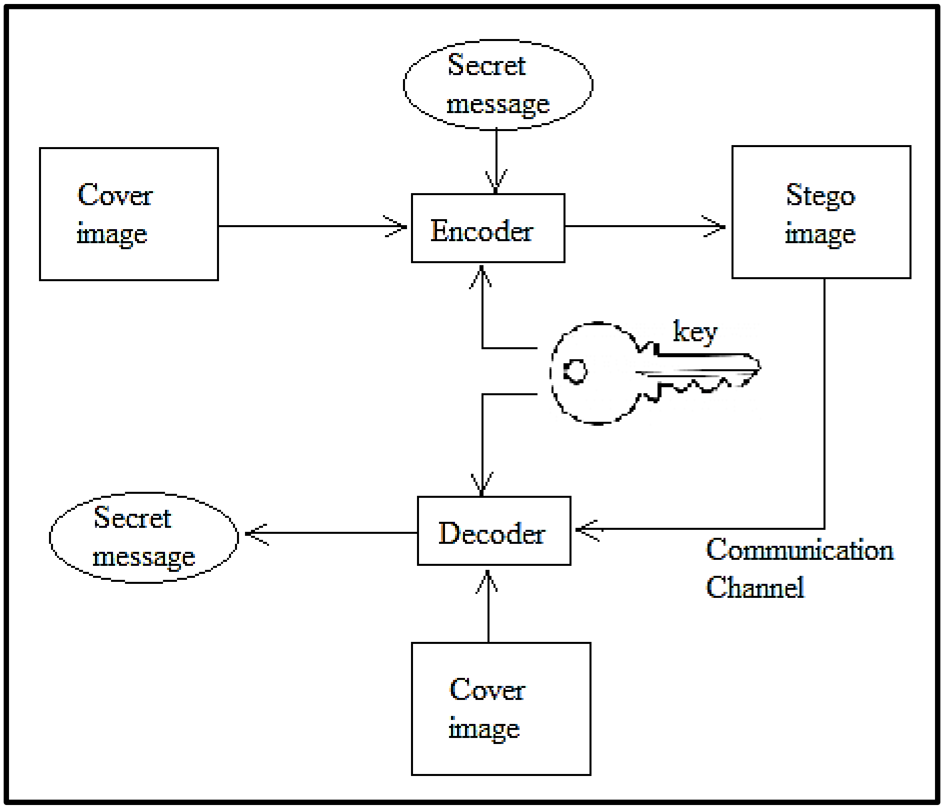
Cryptography prevents unauthorized parties from discovering the content of communication but Steganography prevents discovery of the existence of communication for example Cryptography makes data gibberish and knows the message passing while Steganography tends to conceal presence of hidden data and unknown the message passing. Cryptography alters the structure of secret messages while Steganography does not alter the structure of secret messages. Most algorithms of Cryptography are well known, but the algorithms of Steganography are still being developed that's why it is better to use.

Proposed System

a. Architecture Diagram

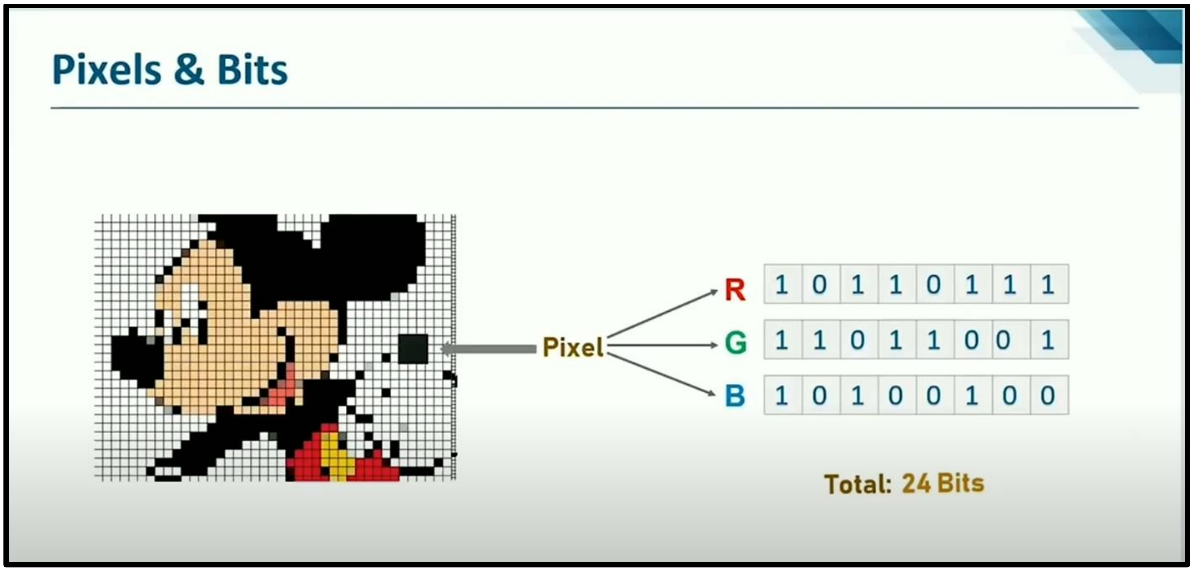


b. Flow Diagram



c. Detailed paragraph explanation

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called the Least Significant bit as its value will affect the pixel value only by “1”. So, this property is used to hide the data in the image. If anyone has considered the last two bits as LSB bits as they will affect the pixel value only by “3”. This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which the least significant bit of the image is replaced with a data bit. As this method is vulnerable to steganalysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple. In this method the least significant bits of some or all of the bytes inside an image are replaced with bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains – for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today.

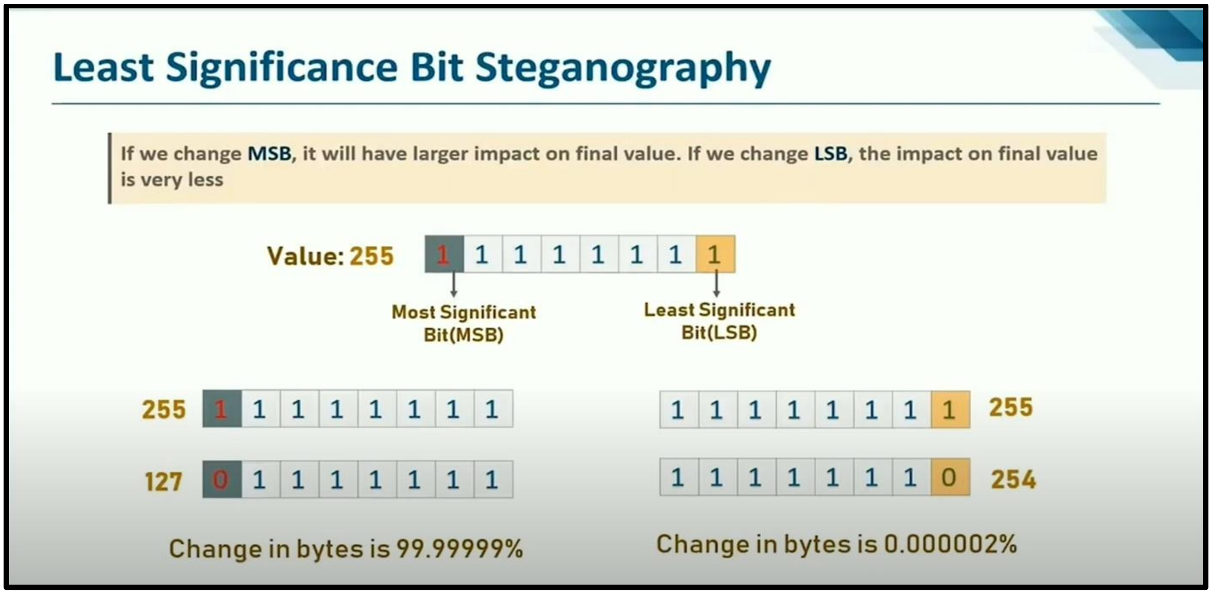


Pixels & Bits

Pixel

R	1	0	1	1	0	1	1	1
G	1	1	0	1	1	0	0	1
B	1	0	1	0	0	1	0	0

Total: 24 Bits



Least Significance Bit Steganography

> If we change **MSB**, it will have larger impact on final value. If we change **LSB**, the impact on final value is very less

Value: 255 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1

Most Significant Bit(MSB)

Least Significant Bit(LSB)

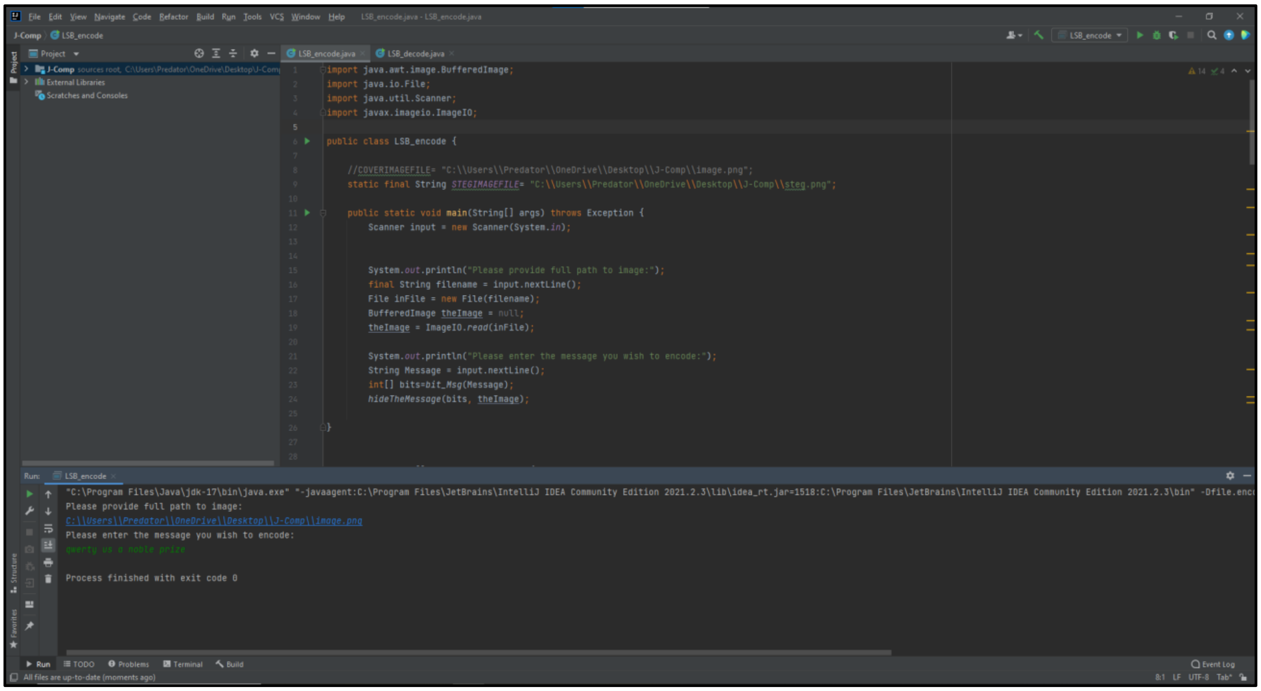
255	1	1	1	1	1	1	1	1
127	0	1	1	1	1	1	1	1

Change in bytes is 99.99999%

1	1	1	1	1	1	1	1	255
1	1	1	1	1	1	1	0	254

Change in bytes is 0.000002%

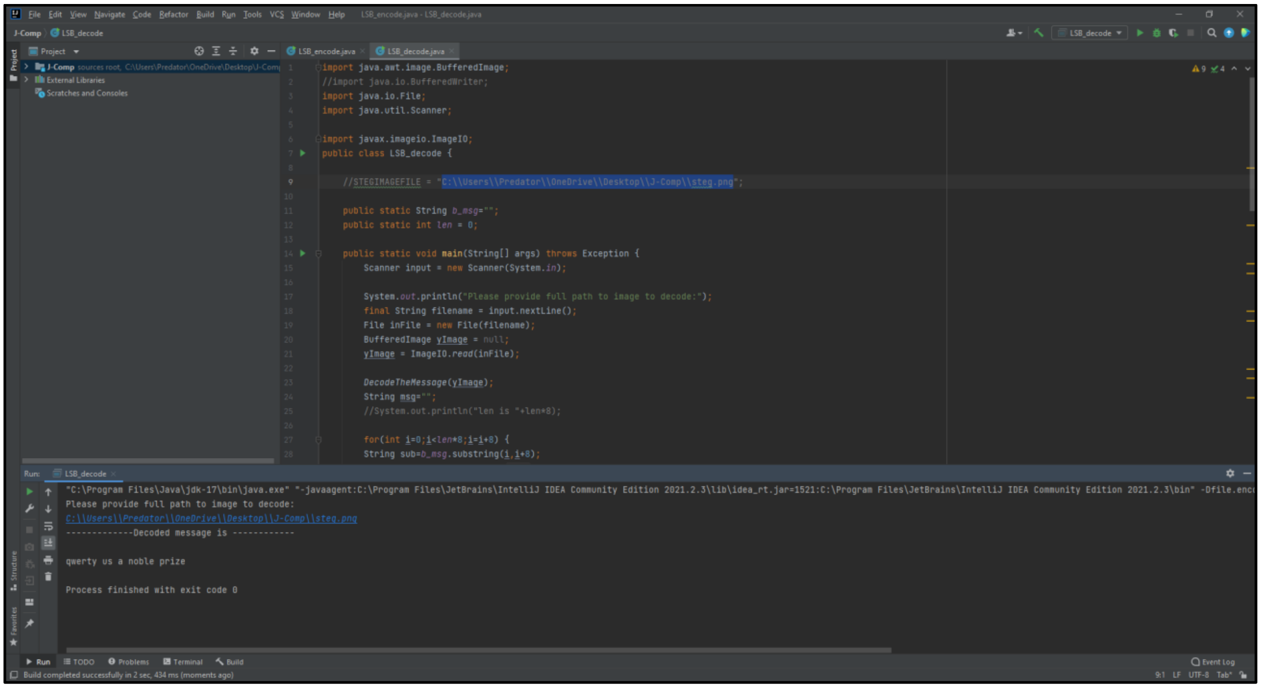
d. Screenshot with explanation of each window


File Edit View Navigate Code Refactor Build Run Tools VCS Window Help LSB_encode.java - LSB_encode.java
J-Comp LSB_encode
Project
J-Comp sources root, C:\Users\Predator\OneDrive\Desktop\J-Comp
External Libraries
Scratches and Consoles
LSB_encode.java
LSB_decode.java
Run: LSB_encode
Run TODO Problems Terminal Build
All files are up-to-date (moments ago)
Event Log
8:1 LF UTF-8 Tab*

```java
import java.awt.image.BufferedImage;
import java.io.File;
import java.util.Scanner;
import javax.imageio.ImageIO;

public class LSB_encode {

    //COVERIMAGEFILE= "C:\\Users\\Predator\\OneDrive\\Desktop\\J-Comp\\image.png";
    static final String STEGIMAGEFILE= "C:\\Users\\Predator\\OneDrive\\Desktop\\J-Comp\\steg.png";

    public static void main(String[] args) throws Exception {
        Scanner input = new Scanner(System.in);


        System.out.println("Please provide full path to image:");
        final String filename = input.nextLine();
        File inFile = new File(filename);
        BufferedImage theImage = null;
        theImage = ImageIO.read(inFile);

        System.out.println("Please enter the message you wish to encode:");
        String Message = input.nextLine();
        int[] bits=bit_Msg(Message);
        hideTheMessage(bits, theImage);

}
```

```
"C:\Program Files\Java\jdk-17\bin\java.exe" "-javaagent:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2021.2.3\lib\idea_rt.jar=1518:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2021.2.3\bin" -Dfile.enc
Please provide full path to image:
C:\\Users\\Predator\\OneDrive\\Desktop\\J-Comp\\image.png
Please enter the message you wish to encode:
qwerty us a noble prize

Process finished with exit code 0
```

In this screen, the code for encryption is executed where a user-defined message is encoded in a png file using LSB technique explained above.


File Edit View Navigate Code Refactor Build Run Tools VCS Window Help LSB_encode.java - LSB_decode.java
J-Comp LSB_decode
Project
J-Comp sources root, C:\Users\Predator\OneDrive\Desktop\J-Comp
External Libraries
Scratches and Consoles
LSB_encode.java
LSB_decode.java
Run: LSB_decode
Run TODO Problems Terminal Build
Build completed successfully in 2 sec, 434 ms (moments ago)
Event Log
9:1 LF UTF-8 Tab*

```java
import java.awt.image.BufferedImage;
//import java.io.BufferedWriter;
import java.io.File;
import java.util.Scanner;

import javax.imageio.ImageIO;
public class LSB_decode {

    //STEGIMAGEFILE = "C:\\Users\\Predator\\OneDrive\\Desktop\\J-Comp\\steg.png";

    public static String b_msg="";
    public static int len = 0;

    public static void main(String[] args) throws Exception {
        Scanner input = new Scanner(System.in);

        System.out.println("Please provide full path to image to decode:");
        final String filename = input.nextLine();
        File inFile = new File(filename);
        BufferedImage yImage = null;
        yImage = ImageIO.read(inFile);

        DecodeTheMessage(yImage);
        String msg="";
        //System.out.println("len is "+len*8);

        for(int i=0;i<len*8;i=i+8) {
        String sub=b_msg.substring(i,i+8);
```

```
"C:\Program Files\Java\jdk-17\bin\java.exe" "-javaagent:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2021.2.3\lib\idea_rt.jar=1521:C:\Program Files\JetBrains\IntelliJ IDEA Community Edition 2021.2.3\bin" -Dfile.enc
Please provide full path to image to decode:
C:\\Users\\Predator\\OneDrive\\Desktop\\J-Comp\\steg.png
------------Decoded message is -----------

qwerty us a noble prize

Process finished with exit code 0
```

In this screen, the code for decryption is executed where an encoded png file is decoded and the secret message is retrieved.

e. Conclusion

Still efforts have to be made to increase the embedding capacity and maintain secrecy. In this method, we can hide a text file equal to the size of the image. Efforts can be made to hide text files having more size than image size. If Steganography is used with Cryptography, it will prove to be an unbeatable tool in secure communication links. Security of the scheme can be improved by using advanced cryptography techniques and also improve the efficiency by using data compression techniques.

References

1. Wendzel', 'Steffen; Mazurczyk', 'Wojciech; Haas', 'Georg': "Information Hiding In Cyber Physical Systems Using Smart Buildings". Proceedings of the 2017 IEEE Security & Privacy Workshops. IEEE.

2. 'Krzysztof Szczypiorski '(4 November 2003). "Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System – HICCUPS". Institute of Telecommunications Seminar. Retrieved 17 June 2010

3. Mazurczyk, Wojciech; Wendzel, Steffen; Zander, Sebastian; Houmansadr, Amir; Szczypiorski, Krzysztof (1 February 2016). Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications(1 ed.). Wiley- IEEE. ISBN 978-1-118-86169-1.

4. "Secret Code in Color Printers Lets Government Track You; Tiny Dots Show Where and once you Made Your Print". Electronic Frontier Foundation. 16 October 2005.

5. "Criminal complaint by agent Ricci against alleged Russian agents" . United States Department of Justice B. Saha and S. Sharma, “Steganographic Techniques of knowledge Hiding using Digital Images”,in Defence Science Journal, vol. 62, no. 1,2012 January,pp. 11-18.

6. Diego De Luca Picione , Federica Battisti , Marco Carli ,Jaakko Astola , and Karen Egiazarian,”A FIBONACCI LSB DATA HIDING TECHNIQUE”,14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006.

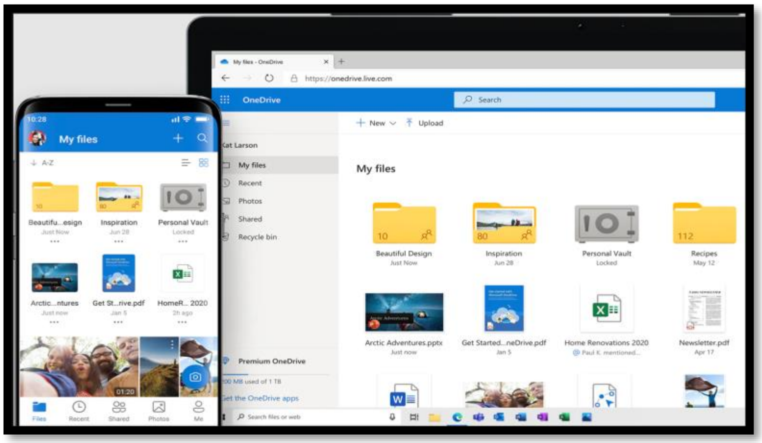
7. http://imagelpcmatlab.blogspot.in/2013/12/matlab-implementation-of-steganography.html

8. http://www.asciitable.com/ [12] http://www.viprefect.com/application-areas

Audit Report:

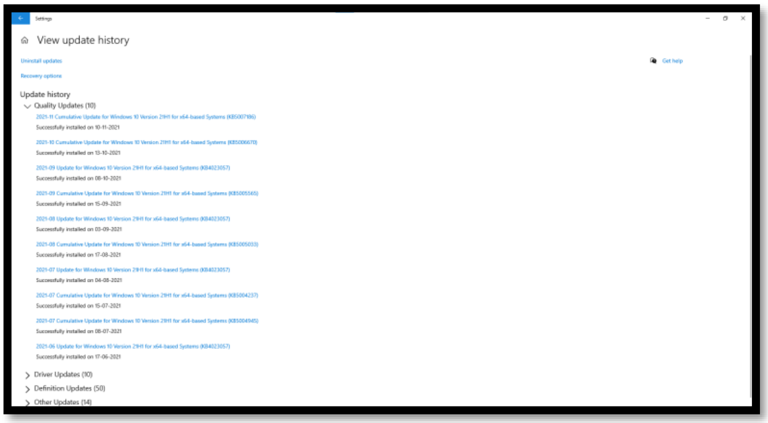
1. Risk Assessment:
    - A virus can infect the system and corrupt all the files.
    - Offline storage may crash.
    - Unauthorised user can access and do malicious activities.

2. Backup procedures: Using Microsoft One-Drive & Backup Hard drive



3. Password Policy Section: My system consists of Username & password. My password complexity includes uppercase, lowercase and a special character.

4. Change Control Section:


Settings

View update history

Uninstall updates

Recovery options

Get help

Update history

Quality Updates (10)

2021-11 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5007186)
Successfully installed on 10-11-2021

2021-10 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5006670)
Successfully installed on 13-10-2021

2021-09 Update for Windows 10 Version 21H1 for x64-based Systems (KB4023057)
Successfully installed on 08-10-2021

2021-09 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5005565)
Successfully installed on 15-09-2021

2021-08 Update for Windows 10 Version 21H1 for x64-based Systems (KB4023057)
Successfully installed on 03-09-2021

2021-08 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5005033)
Successfully installed on 17-08-2021

2021-07 Update for Windows 10 Version 21H1 for x64-based Systems (KB4023057)
Successfully installed on 04-08-2021

2021-07 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5004237)
Successfully installed on 15-07-2021

2021-07 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5004945)
Successfully installed on 08-07-2021

2021-06 Update for Windows 10 Version 21H1 for x64-based Systems (KB4023057)
Successfully installed on 17-06-2021

Driver Updates (10)

Definition Updates (50)

Other Updates (14)

Last update on 10 Nov 2021.

OS Ver: Win-10 Pro (21H1)

Antivirus: Windows Defender

5. Incident Response Section: N/A

6. Security Posture: N/A

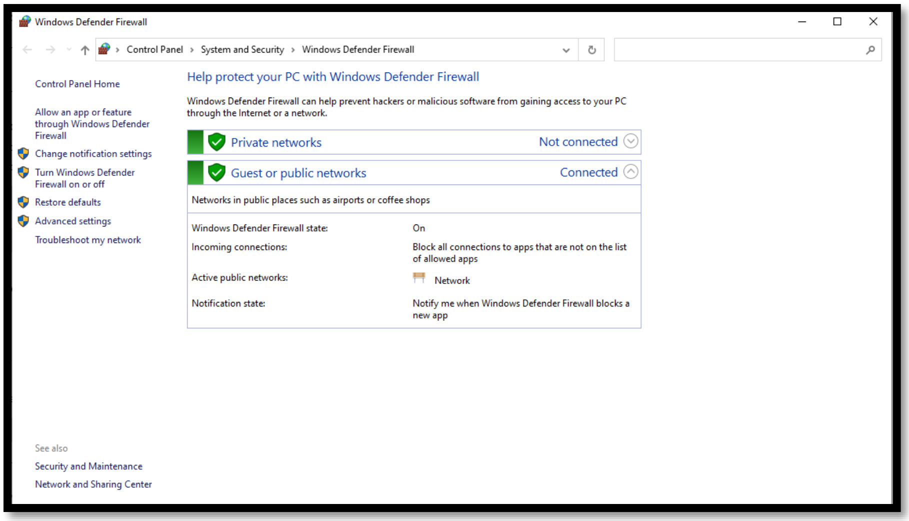
7. Report:

a. Network Security Audit:

Possibilities of attack: **Yes**

System able to forecast: **Yes**

Firewall: Enable


Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

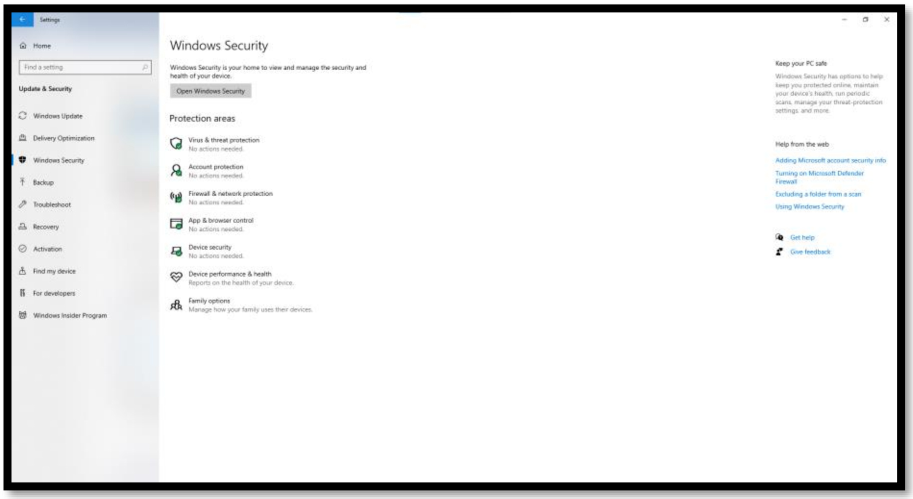
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

b. Cyber Security Audit: Windows Defender



Windows Security

Windows Security is your home to view and manage the security and health of your device.

Protection areas

Virus & threat protection
No actions needed.

Account protection
No actions needed.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health
Reports on the health of your device.

Family options
Manage how your family uses their devices.

Keep your PC safe

Windows Security has options to help keep you protected online, maintain your device's health, run periodic scans, manage your threat-protection settings, and more.

Help from the web

c. Web Application Security: N/A

d. Compliance Audit

d.1) Your environment under protection of Disaster Management: Yes

d.2) Peoples Involved are educated: Yes

d.3) All the components involved are following Indian Standards: Yes

d.4) All Components are MADE IN INDIA: No

d.5) Regular Internal Audit was covered: Yes

VERDICT: **It is safe to run application in our place.**