THE ART OF SECRET COMMUNICATION: EXPLORING STEGANOGRAPHY METHODS

A Project Report

Submitted in the partial fulfillment of the requirements for the

award of the degree of

Bachelor of Technology in

Department of Computer Science and Engineering

By

2010030364_K.YASHWANTH
2010030501_G.PAVAN REDDY
2010030502_G.VIPUL REDDY
2010030508_S.PADMASHREE
2010030512_L.KEERTHANA

under the supervision of

Panduraju Pagidimalla

Department of Computer Science and Engineering

K L University Hyderabad,

Aziz Nagar, Moinabad Road, Hyderabad – 500 075, Telangana, India.

March, 2023

Declaration

The Project Report entitled "**THE ART OF SECRET COMMUNICATION: EXPLORING STEGANOGRAPHY METHODS**" is a record of bonafide work of Mr.K.Yashwanth(2010030364),Mr.G.PavanReddy(2010030501),Mr.G.VipulReddy(2010030502), Ms.S.Padmashree(2010030508),Ms.L.Keerthana(2010030512)., submitted in partial fulfillment for the award of B.Tech in the Department of Computer Science and Engineering to the K L University, Hyderabad. The results embodied in this report have not been copied from any other Departments/University/Institute.

Signature of the Students

K.YASHWANTH

G.PAVAN REDDY

G.VIPUL REDDY

S.PADMASHREE

L.KEERTHANA

Certificate

This is to certify that the Project Report entitled "**THE ART OF SECRET COMMUNICATION: EXPLORING STEGANOGRAPHY METHODS**" is being submitted by K.YASHWANTH,G.PAVANREDDY,G.VIPULREDDY,S.PADMASHREE,L.KEERTHANA submitted in partial fulfillment for the award of B.Tech in CSE to the K L University, Hyderabad is a record of bonafide work carried out under our guidance and supervision.The results embodied in this report have not been copied from any other departments/ University/Institute.

Signature of the Supervisor

Panduraju Pagidimalla
Assistant professor

Signature of the HOD

Signature of the External Examine

ACKNOWLEDGEMENTS

It is great pleasure for me to express my gratitude to our honorable President **Sri. Koneru Satyanarayana**, for giving the opportunity and platform with facilities in accomplishing the project based laboratory report.

I express the sincere gratitude to our Principal **Dr. A .RamaKrishna** for his administration towards our academic growth.

I express sincere gratitude to our Coordinator **Mr.Panduraju** for his leadership and constant motivation provided in successful completion of our academic semester. I record it as my privilege to deeply thank for providing us the efficient faculty and facilities to make our ideas into reality.

I express my sincere thanks to our project supervisor **Mr.Panduraju** for his/her novel association of ideas, encouragement, appreciation and intellectual zeal which motivated us to venture this project successfully.

Finally, it is pleased to acknowledge the indebtedness to all those who devoted themselves directly or indirectly to make this project report success.

INDEX

PROJECT ABSTRACT

- Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information.

- The purpose of steganography is to keep the communication secret, whereas cryptography focuses on keeping the content of the communication secret. Steganography techniques include using least significant bit (LSB) insertion, where the message is inserted into the least significant bit of each pixel in an image, and using spread spectrum techniques, where the message is spread out across multiple pixels or frequencies in a signal.

- The effectiveness of steganography depends on the strength of the algorithm used to hide the message, as well as the quality of the carrier medium used. Steganography has various applications, including in military communications, digital watermarking, and digital forensics.

- 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 some are more complex than others and all of them have respective strong and weak points.

- For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This project hides the message with in the image. For a more secure approach, the project it allows user to choose the bits for replacement instead of LSB replacement from the image. sender select the cover image with the secret text or text file and hide it in to the image with the bit replacement choice, it help to generate the secure stego image .the stego image is sent to the destination with the help of private or public communication network. on the other side i.e. receiver.

INTRODUCTION

- **Confidentiality:** Steganography helps ensure that confidential information remains private by embedding it within a seemingly innocuous message or image. This makes it difficult for unauthorized individuals to intercept or decode the secret information.

- **Security:** Steganography can be used to protect sensitive data from theft or tampering. By concealing information within another file or message, it is more difficult for hackers or cybercriminals to locate and exploit vulnerabilities.

- **Covert Communication:** Steganography enables covert communication between parties, allowing them to communicate secretly without detection. This can be especially useful in situations where open communication is not possible or safe.

- **Deniability:** Steganography can provide a level of deniability for individuals or organizations who may be communicating sensitive information. If discovered, the existence of the hidden message can be denied, making it difficult to prove wrongdoing.

- The paper proposes a steganography algorithm to hide data within images to protect data privacy. The proposed system is called Steganography Imaging System (SIS), which allows users to input images and texts and hide the data within the image. The paper discusses the importance of data security and privacy, particularly in the age of the internet, and how steganography can be used as a security tool when combined with encryption. The paper also compares steganography to watermarking and fingerprinting, which are technologies used for intellectual property protection. The paper explains the different types of steganography, the properties that measure steganographic system performance, and the popular carrier file formats for steganography, particularly digital images. Finally, the paper outlines the organization of the rest of the paper, which includes a review of related work, a presentation of the proposed algorithm, implementation of the system, and results obtained from testing the system with various sizes of data.
-

LITERATURE SURVEY

- **A Cautionary Note On Image Downgrading:-** The results of an experiment that shows that it is very simple to contaminate digital images with information that can later be extracted are presented. This contamination cannot be detected when the image is displayed on a good quality graphics workstation. Based on these results, it is recommended that image downgrading based on visual display of the image to be downgraded not be performed if there is any threat of image contamination by Trojan horse programs.
  https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=A+Cautionary+Note+On+Image+Downgrading+&btnG=
- **A Multiresolution Watermark for Digital Images:-** a new multiresolution watermarking method for digital images. The method is based on the discrete wavelet transform (DWT). Pseudo-random codes are added to the large coefficients at the high and middle frequency bands of the DWT of an image. It is shown that this method is more robust to often proposed methods to some common image distortions, such as the wavelet transform based image compression, and image halftoning. Moreover, the method is hierarchical. The computation load needed to detect the watermark depends on the noise level in an image.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=+A+Multiresolution+Watermark+for+Digital+Images+&btnG=

- **Techniques for Data Hiding:-** Data hiding, a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions, e.g., lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party. We explore both traditional and novel techniques for addressing the data-hiding process and evaluate these techniques in light of three applications: copyright protection, tamper-proofing, and augmentation data embedding.
  https://ieeexplore.ieee.org/abstract/document/5387237
- **DIGITAL IMAGE WATERMARKING TECHNIQUE FOR COPYRIGHT PROTECTION OF MULTIMEDIA DATA:-** The rapid expansion of multimedia technology has offered several facilities in the data transmission, manipulation and reproduction. This advance has brought some critical issues like copyright protection. Digital watermarking is one of the promising tool for copyright protection of multimedia data. Many algorithms and techniques have been developed for watermarking,t his paper introduces an efficient digital image watermarking technique for copyright protection. The proposed technique developed by integrating Lifting Wavelet Transform (LWT) with the Artificial Neural Network (ANN).LWT based technique has more robust to several attacks than least significant bit and discrete wavelet transform based approaches. PSNR and NCC are the performance measure parameters employed to evaluate the efficiency of the proposed fusion technique. Simulation results are provided to demonstrate that the proposed watermarking technique can withstand for many image manipulation operations and also maintain its imperceptibility.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=+DIGITAL+IMAGE+WATERMARKING+TECHNIQUE+FOR+COPYRIGHT+PROTECTION+OF+MULTIMEDIA+DATA+&btnG

- **Document marking and identification using both line and word shifting**:-Continues a study of document marking to deter illicit dissemination. An experiment performed reveals that the distortion on the photocopy of a document is very different in the vertical and horizontal directions. This leads to the strategy that marks a text line both vertically using line shifting and horizontally using word shifting. A line that is marked is always accompanied by two unmarked control lines one above and one below. They are used to measure distortions in the vertical and horizontal directions in order to decide whether line or word shift should be detected.
  https://ieeexplore.ieee.org/abstract/document/515956

SYSTEM REQUIREMENTS SOFTWARE

REQUIREMENTS:

- Language: JAVA
- Web Server: Apache Tomcat server

- **HARDWARE REQUIREMENTS:**

- core 2 duo Clock speed: 2GhZ
- Hard Disk 20GB RAM: 2GB
- Cache Memory: 512KB

METHODS

A.IMAGE FILES:

Steganography is commonly used with image files to hide messages. The message is embedded in a way that is hard to detect by the naked eye, often in the least significant bits of the image pixels or the frequency domain of the image. Despite the potential image quality degradation caused by the process, image files remain popular due to their wide usage, easy shareability, and large data storage capacity.

B. STEGANOGRAPY ALGORITHM TO HIDE SECRETMESSAGE INSIDE AN IMAGE

- accuracy of data.
- A framework for the system process is shown in Fig. 1, which includes data hiding and retrieval from images.
- Prior to data hiding, the user is required to log in with a username and password, and a secret key is needed to retrieve the hidden data.
- A novel steganography algorithm is used to embed data with minimal distortion to the original image.
- Fig. 2 shows the algorithm for embedding secret messages in the image, which requires a secret key for retrieval.
- The secret message is first transferred to a text file, compressed into a zip file for security, and converted into binary codes.
- Data hiding is then applied by encoding binary codes into pixels in the image.
- The secret key plays an essential role in the proposed steganography algorithm.

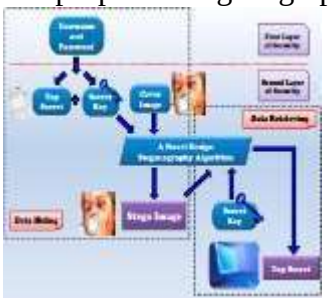


Fig:1 the frame work of the system

```
Begin Input: Cover_Image, Secret_Message, Secret_Key;
Transfer Secret_Message into Text_File; Zip Text_File;
Convert Zip_Text_File to Binary_Codes;
Convert Secret_Key into Binary_Codes;
Set BitsPerUnit to Zero;
Encode Message to Binary_Codes;
Add by 2 unit for bitsPerUnit;
Output: Stego _ image
End
```

Fig2: algorithm for embedding data inside image

- The steganography algorithm involves transferring the secret message into a text file, compressing it into a zipfile, converting it into binary codes, and using data hiding to encode the binary codes into the pixels of theimage.
- The secret key acts as a locker to lock and unlock thesecret message, and each last two bits of the binary codes are encoded into each pixel of the image to minimize changes to the original image.

- To extract the secret message from the stego image, asecret key is needed for verification, and the binary codes are decoded to form a zipped text file, which isthen unzipped to retrieve the original secret message.
- Fig. 3 presents the algorithm for extracting the hiddenmessage from the stego image.
- A secret key is required to extract the message correctlyfrom the image for verification purposes.
- The data extraction method shown in Fig. 3 also requiresa secret key to check if it matches the key that decodes from the binary code sequence.
- Once the key is verified, the binary code is converted into a zipped text file.
- The text file is then unzipped, and the secret message istransferred from the file to retrieve the original message.

Fig 3.Algorithm for extracting data from stego image.

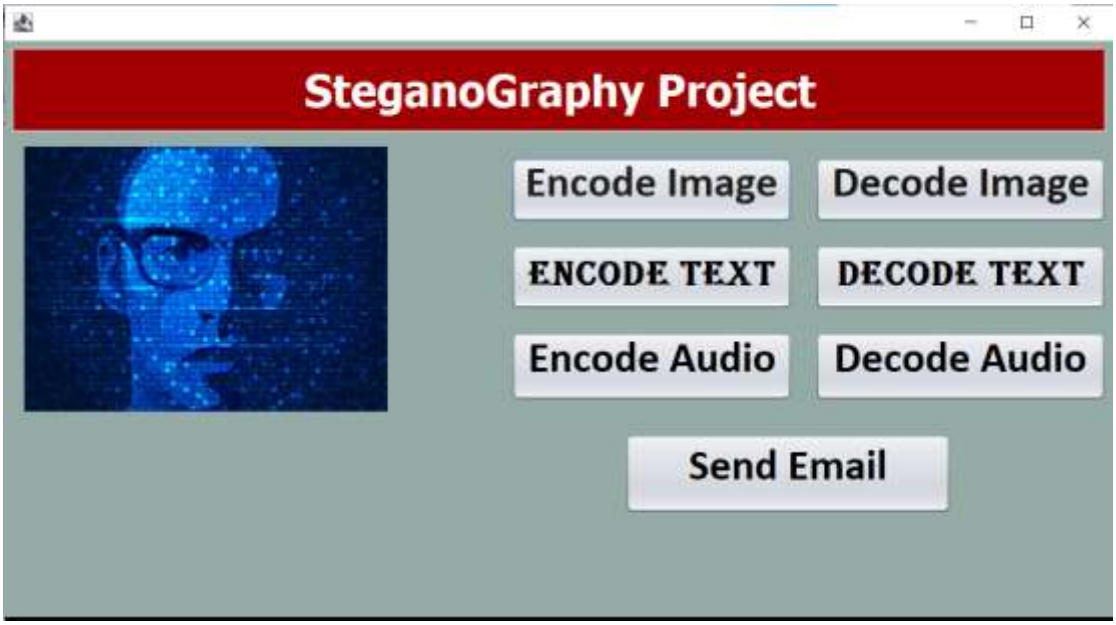
- The proposed steganography algorithm focuses on several key techniques, including transferring the secret message to a text file, zipping the file, converting the file and key into binary codes, and encoding those codes into the pixels of an image.
- Despite these techniques, the image quality remains robust with minimal distortion and color changes.
- The secret message is difficult to steal through steganalysis, which makes it a secure way to protect data from unauthorized access.
- The algorithm uses two image embedding techniques, namely data hiding and data retrieving methods.
- Data hiding is used to hide the secret message and keyin the cover image, while data retrieval is used toextract the key and hidden secret message from the stego image.
- Overall, this steganography algorithm provides a secure way to protect data, especially secret messages,within an image without revealing them to unauthorized parties.

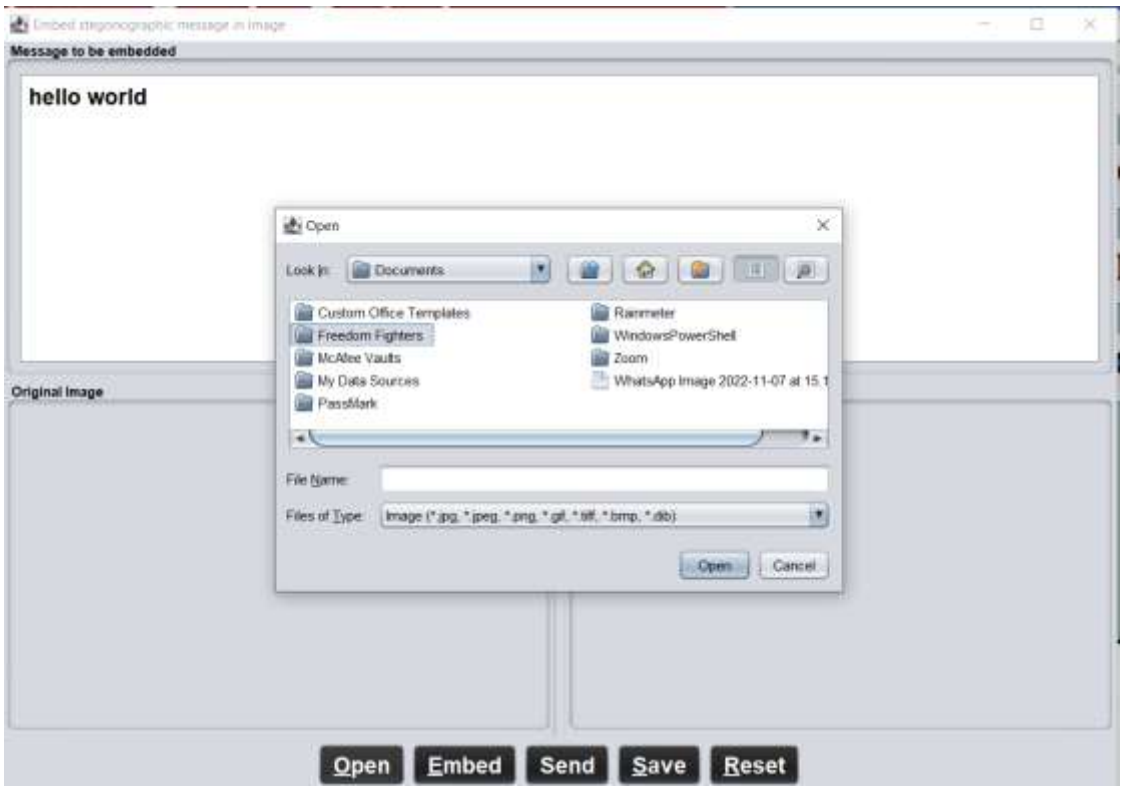
IMPLEMENTATION

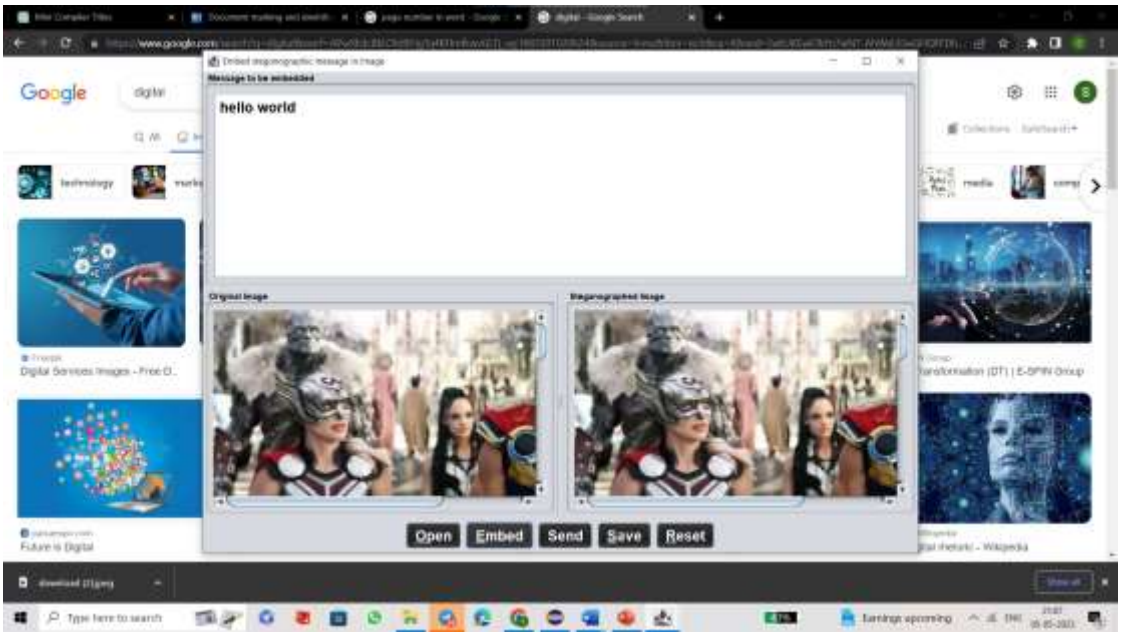
```
package Coding;

import Audio_Steganography.Decode_Audio;

/**
 *
 * @author Hadi
 */
public class HomePage extends javax.swing.JFrame {

    /**
     * Creates new form MainMenu
     */
    public HomePage() {
        initComponents();
    }
    /**
     * This method is called from within the constructor to initialize the form.
     * WARNING: Do NOT modify this code. The content of this method is always
     * regenerated by the Form Editor.
     */
    @SuppressWarnings("unchecked")
    // <editor-fold defaultstate="collapsed" desc="Generated Code">//GEN-BEGIN:initComponents
    private void initComponents() {

        jButton3 = new javax.swing.JButton();
        jPanel1 = new javax.swing.JPanel();
        jButton2 = new javax.swing.JButton();
        jButtonDecodeAudio = new javax.swing.JButton();
        jPanel2 = new javax.swing.JPanel();
        jLabel1 = new javax.swing.JLabel();
        jLabel2 = new javax.swing.JLabel();
        jPanel3 = new javax.swing.JPanel();
        jLabel3 = new javax.swing.JLabel();
        jButton5 = new javax.swing.JButton();
        jButton6 = new javax.swing.JButton();
        jButtonEncodeAudio = new javax.swing.JButton();
        jButton7 = new javax.swing.JButton();
```

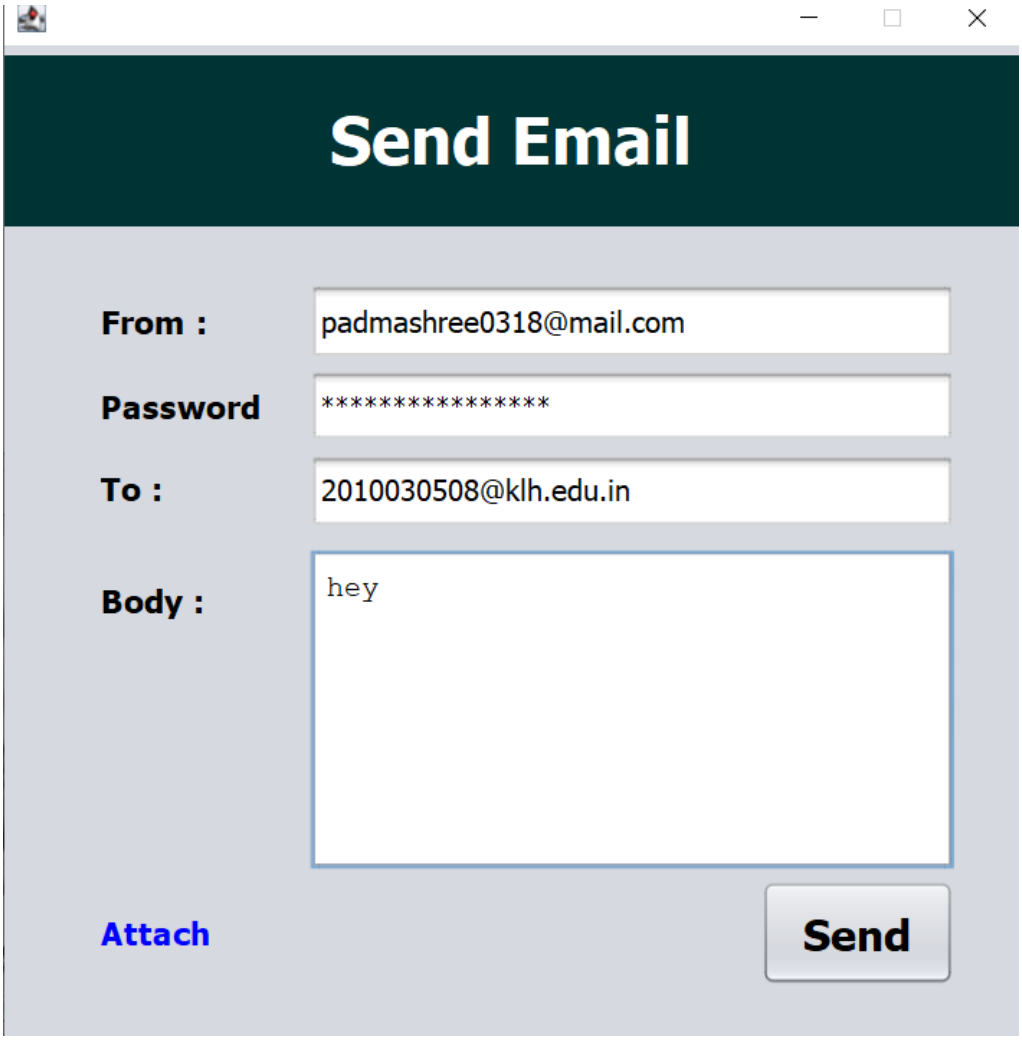
```
package Coding;

import java.awt.Color;

public class LoginForm extends javax.swing.JFrame {

   String MyAppPassword = "xxxx";

    public LoginForm() {
        initComponents();
        this.setLocationRelativeTo(null);

    }

    /**
     * This method is called from within the constructor to initialize the form.
     * WARNING: Do NOT modify this code. The content of this method is always
     * regenerated by the Form Editor.
     */
    @SuppressWarnings("unchecked")
    // <editor-fold defaultstate="collapsed" desc="Generated Code">//GEN-BEGIN:initComponents
    private void initComponents() {

        jPanel1 = new javax.swing.JPanel();
        jTextUserName = new javax.swing.JTextField();
        jPassword = new javax.swing.JPasswordField();
        jLabel1 = new javax.swing.JLabel();
        jSeparator1 = new javax.swing.JSeparator();
        jButton1 = new javax.swing.JButton();
        jButton2 = new javax.swing.JButton();
        jLabel7 = new javax.swing.JLabel();

        setDefaultCloseOperation(javax.swing.WindowConstants.EXIT_ON_CLOSE);
        setUndecorated(true);
        setResizable(false);
        addWindowListener(new java.awt.event.WindowAdapter() {
```

RESULTS


SteganoGraphy Project
Encode Image
Decode Image
ENCODE TEXT
DECODE TEXT
Encode Audio
Decode Audio
Send Email


Message to be embedded
hello world
Original Image
Open
Look in: Documents
Custom Office Templates
Freedom Fighters
McAfee Vaults
My Data Sources
PassMark
Rainmeter
WindowsPowerShell
Zoom
File Name:
Files of Type:
Open
Cancel
Open
Embed
Send
Save
Reset


hello world
Open
Embed
Send
Save
Reset


Send Email
From :
padmashree0318@mail.com
Password
****
To :
2010030508@klh.edu.in
Body :
hey
Attach
Send

CONCLUSION

Steganography is a technique that involves hiding a message or data within another message, image, or file. It can be used for various purposes, including secure communication, covert communication, and protection against censorship.

Steganography offers several advantages, such as enhanced security, versatility, and preservation of message integrity. However, it also has several limitations and potential drawbacks, such as detection, capacity limitations, complexity, compatibility issues, potential for misuse, and a false sense of security.

It is important to carefully evaluate the risks and benefits before using steganography, and to ensure that it is used in a responsible and ethical manner.

Ultimately, steganography is just one of several tools and techniques available for secure communication and data protection, and should be used in conjunction with other methods to provide robust security.

REFERENCES

- M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source– Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450
- [4] E. Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Indianapolis: Wiley Publishing, 2003.
- [5] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf
- [6] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001
- [7] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999
- [8] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10,
- October 2004
- [9] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998