**INFO 2411: Foundations of Computer Security**

**Final Project:**

**Student Names:** Harmanpreet Kaur

Suneet Kaur

Ahmad Al-samarrai

Harman Mehla

**Email addresses:**[**harmanpreetkaur19@student.kpu.ca**](mailto:harmanpreetkaur19@student.kpu.ca)

[**suneetkaur@student.kpu.ca**](mailto:suneetkaur@student.kpu.ca)

[**ahmad.alsamarrai@student.kpu.ca**](mailto:ahmad.alsamarrai@student.kpu.ca)

[**harman.mehla@student.kpu.ca**](mailto:harman.mehla@student.kpu.ca)

**Student numbers:** 100421083

100347924

100398918

100400396

July 29, 2023

Table of Contents

[**1.** **Understanding Steganography Algorithms:** 3](#_Toc141814640)

[**1.** **Different Steganography Algorithms:** 3](#_Toc141814641)

[**2.1. LSB (Least Significant Bit) Steganography:** 3](#_Toc141814642)

[2.1.1 Explanation: 3](#_Toc141814643)

[2.1.2 Strengths: 3](#_Toc141814644)

[2.1.3 Weaknesses: 4](#_Toc141814645)

[2.1.4 Capacity: 4](#_Toc141814646)

[2.1.5 Imperceptibility: 4](#_Toc141814647)

[2.1.6 Security Characteristics: 4](#_Toc141814648)

[2.1.7 Real-World applications: 4](#_Toc141814649)

[**2.2 DCT (Discrete Cosine Transform) Steganography:** 4](#_Toc141814650)

[2.2.1 Explanation: 4](#_Toc141814651)

[2.2.2 Strengths: 4](#_Toc141814652)

[1.2. 3 Weaknesses: 5](#_Toc141814653)

[2.2.4 Capacity 5](#_Toc141814654)

[2.2.5 Imperceptibility: 5](#_Toc141814655)

[2.2.6 Security Characteristics: 5](#_Toc141814656)

[2.2.7 Real World Application 5](#_Toc141814657)

[**2.3 Spread Spectrum Steganography:** 6](#_Toc141814658)

[2.3.1 Explanation: 6](#_Toc141814659)

[2.3.2 Strengths: 6](#_Toc141814660)

[2.3.3 Weaknesses: 6](#_Toc141814661)

[2.3.4 Capacity: 7](#_Toc141814662)

[2.3.5 Imperceptibility 7](#_Toc141814663)

[2.3.6 Security Characteristics: 7](#_Toc141814664)

[2.3.7 Real-World Application 7](#_Toc141814665)

[**3. Technical Implementation** 8](#_Toc141814666)

[**1.1** **Stegosuite** 8](#_Toc141814667)

[3.1.1 Purpose: 8](#_Toc141814668)

[3.1.2 Procedure: 8](#_Toc141814669)

[**1.2** **QuickStego** 10](#_Toc141814670)

[3.2.1 Purpose: 10](#_Toc141814671)

[3.2.2 Procedure: 10](#_Toc141814672)

**1.3 OpenStego**

[3.3.1 Purpose: 10](#_Toc141814671)

[3.3.2 Procedure: 10](#_Toc141814672)

**1.4 Silent Eye**

[3.4.1 Purpose: 10](#_Toc141814671)

[3.4.2 Procedure: 10](#_Toc141814672)

[**4. Potential Risks Associated with Steganography: 19**](#_Toc141814673)

[**4.1 Mitigation Measures: 19**](#_Toc141814674)

[**5. Practical Applications of Steganography: 20**](#_Toc141814675)

[**5.1 Data Protection: 20**](#_Toc141814676)

[**5.2 Watermarking: 20**](#_Toc141814677)

[**5.3 Authentication: 20**](#_Toc141814678)

[**5.4 Covert Communication: 20**](#_Toc141814679)

[**6. Potential Misuse or Illegal Activities: 21**](#_Toc141814680)

[**6.1 Data Theft and Espionage: 21**](#_Toc141814681)

[**6.2 Cybercrime and Malware Delivery: 21**](#_Toc141814682)

[**6.3 Online Terrorism and Covert Communication: 21**](#_Toc141814683)

[**7.Responsible Usage of Steganography: 21**](#_Toc141814684)

[**7.1 Legal and Ethical Compliance: 22**](#_Toc141814685)

[**7.2 Obtain Consent: 22**](#_Toc141814686)

[**7.3 Promote Awareness: 22**](#_Toc141814687)

[**7.4 Legitimate Purposes: 22**](#_Toc141814688)

[**8. Conclusion 22**](#_Toc141814689)

[**9.References: 23**](#_Toc141814690)

# **Understanding Steganography Algorithms:**

Steganography algorithms are smart methods used to hide secret information within pictures, music, or videos securely. The algorithms embed secret data in carrier files such as photo or audio files and later the hidden data can be extracted using appropriate algorithms.

Steganography can be helpful for secure communication and protecting copyrights. But it can also be misused for hiding messages that shouldn’t be hidden. It is essential to use steganography responsibly and legally, following the rules and not doing anything harmful or illegal.

# **Different Steganography Algorithms:**

There are different types of steganography algorithms, each with its own approach to hiding data. Each algorithm varies in its complexity and effectiveness in concealing information. Some popular algorithms are as following:

## **2.1. LSB (Least Significant Bit) Steganography:**

### **2.1.1 Explanation:**

LSB steganography is a simple method to hide secret messages in pictures, music, or videos. It takes advantage of the fact that changing the least significant bit of a pixel’s color value has minimal visual impact. It slightly changes the last bit of pixel values in the media to encode the hidden information.

### **2.1.2 Strengths:**

* It is easy to use and apply to different media types.
* It does not need much computer power to work.
* It is very simple to use as it only requires modifying the least significant bit of pixel values.
* It also has a relatively high capacity for hiding data, as each pixel can potentially carry a bit of information.

### **2.1.3 Weaknesses:**

* It can only hide a small amount of data without affecting the media appearance.
* It can be detected by specialized tools looking for LSB changes.

### **2.1.4 Capacity:**

* The capacity of LSB steganography depends on the number of pixels in the image being used. Each pixel can potentially carry one bit of hidden information.

### **2.1.5 Imperceptibility:**

* When only a few bits are altered, it usually stays invisible to the human eye.

### **2.1.6 Security Characteristics:**

LSB steganography is considered to have lower security compared to other steganography methods. While it can be effective in concealing data from casual observers, it may not withstand advanced steganalysis techniques used by experts. If a higher security level is required, it’s recommended to explore more advanced steganography algorithms.

### **2.1.7 Real-World applications:**

* Sending Secret Messages: People can hide confidential messages in images to share secretly.
* Copyright Protection: Companies can use it to add hidden marks in images for copyright protection.

## **2.2 DCT (Discrete Cosine Transform) Steganography:**

### **2.2.1 Explanation:**

DCT steganography hides secret information in images by working with their frequency patterns. It alters specific frequency coefficients to encode the hidden data. It involves manipulating the DCT coefficients of an image to embedded hidden information. DCT steganography can provide higher security and better resistance to image compression compared to LSB steganography.

### **2.2.2 Strengths:**

* It can hide more data as compared to LSB, as it uses frequency patterns.
* The hidden information is distributed across multiple coefficients, making it harder to detect.
* It also achieves higher embedding capacity while maintaining good visual capacity while maintaining good visual quality of image as it does not distort the image’s appearance.

### **3 Weaknesses:**

* it is more complex to use compared to LSB steganography.
* It has limitations in terms of the amount of hidden information that can be embedded without significantly degrading the visual quality of the image.
* It can be detected by some advanced steganalysis methods.

### **2.2.4 Capacity**

The capacity of DCT steganography depends on various factors, such as the size and complexity of the images, the chosen embedding algorithms, and the desired level of imperceptibility. Generally, DCT steganography can achieve higher embedding capacity compared to LSB steganography.

### **2.2.5 Imperceptibility:**

- Generally, maintains a good visual quality as it works in the frequency domain.

### **2.2.6 Security Characteristics:**

DCT steganography offers certain security characteristics. By distributing the hidden information across multiple DCT coefficients, it becomes more resistant to detection by steganalysis techniques. Additionally, the use of DCT helps in maintaining the visual quality of the image, making it harder to detect any alterations. However, it’s important to note that advanced steganalysis methods can still uncover the presence of hidden data in DCT steganography.

### **2.2.7 Real World Application**

* Digital Watermarking: Companies can add hidden watermarks in images for copyright protection.
* Image Authentication: Ensuring the authenticity of images with hidden signatures.
* It can also be used for data hiding for forensic purposes.
* It also secures messages and confidential information exchange where the hidden data needs to be protected from unauthorized access.

## **2.3 Spread Spectrum Steganography:**

### **2.3.1 Explanation:**

Spread spectrum steganography is a technique that spreads hidden information across a wide range of frequencies. It can be used to embed data in audio, video, or other types of signals. This method is often secure data transmission and anti-forensic purposes. By spreading the hidden data across a broad spectrum, it becomes more resistant to detection and can be more robust against noise or signal interference.

### **2.3.2 Strengths:**

* It provides robustness against signal interference and noise, making the hidden data more resistant to detection.
* It can also offer a high level of security by spreading the hidden information across a wide range of frequencies, making it difficult for unauthorized parties to detect or extract the data.
* Additionally, spread spectrum steganography can be applied to various types of signals, such as audio, video, or wireless communication, making it versatile in different scenarios.

### **2.3.3 Weaknesses:**

* It has potential for increased computational complexity, as the spreading process requires additional processing power.
* Embedding a significant amount of data using spread spectrum techniques may result in a noticeable degradation of signal quality, which could raise suspicion.
* It Cannot hide as much data as LSB or DCT.
* It needs careful code selection for better invisibility.
* Advanced steganalysis techniques still potentially detect the presence of hidden data, especially if the steganographic algorithm is known or suspected.

### **2.3.4 Capacity:**

The capacity of spread spectrum steganography depends on various factors such as the bandwidth of the signal, the desired level of Imperceptibility, and the specific spread spectrum technique used. Generally, spread spectrum steganography can achieve moderate to high data capacity, allowing for the hiding of significant amount for the hiding of a significant amount of information within the signal. However, it’s important to strike a balance between capacity and the ability to maintain the covert nature of the hidden data.

### **2.3.5 Imperceptibility**

- If the code is carefully chosen, it can remain undetectable.

### **2.3.6 Security Characteristics:**

The security characteristics of spread spectrum steganography include its ability to provide a high level of security and resistance against detection. By spreading the hidden data across wide range of frequencies, it becomes more difficult for unauthorizes parties to detect or extract the information. Additionally, spread spectrum technique can offer robustness against noise and signal interference, further enhancing the security of the hidden data.

### **2.3.7 Real-World Application**

* It can be used to hide sensitive data within audio or video signals, providing a covert and secure means of transmitting information.
* This can also be useful in scenarios such as military communication, intelligence operations, or confidential business communication where maintaining the confidentiality and integrity of the data is crucial.
* Spread spectrum steganography can also be applied in digital watermarking to embed copyright information or ownership details within multimedia content.

# **3. Technical Implementation**

There is different open-source steganography available that offer multiple algorithms. The following are the results from the experiments done with different algorithms by using these tools to hide and extract data from various types of media files.

* 1. **Stegosuite**

**3.1.1 Purpose:**

Stegosuite is a tool that we can use to embed a secret message in an image using Least Significant Bit steganography algorithm. We can also use it to discover the message hidden in the image.

**3.1.2 Procedure:**

We click on a new file and browse the image we want to embed the secret message in, then we enter the message in the message box and then we must choose a password so that when we share the embedded image to someone, they can see the message when we share the password with them and then we click on embed and the image gets embedded with the message as it processes the image and converts the least significant bits of the image to the bits of the message and as it is the least significant bits that are being converted, there is close to none difference in both images and message can’t be easily seen and then at last, it gets automatically saved.

If we want to discover a message hidden in an image, then we just upload the image and enter password and click on extract and it will reverse the process and detects the bits of the message hidden in the image and we can see the message in the message box.

A screenshot of a computer

Description automatically generated

The message is INFO 2411 S11 and it has been embedded in the image of the forest and as we can see at the left bottom, the new image has been saved in the computer.

A screenshot of a computer

Description automatically generated

Upon uploading the image and entering the password that is 07July2001, we can extract the message from the image, and we can see it in the message box, and we can see in the left bottom, it says extraction completed means it has extracted the full message from the image.

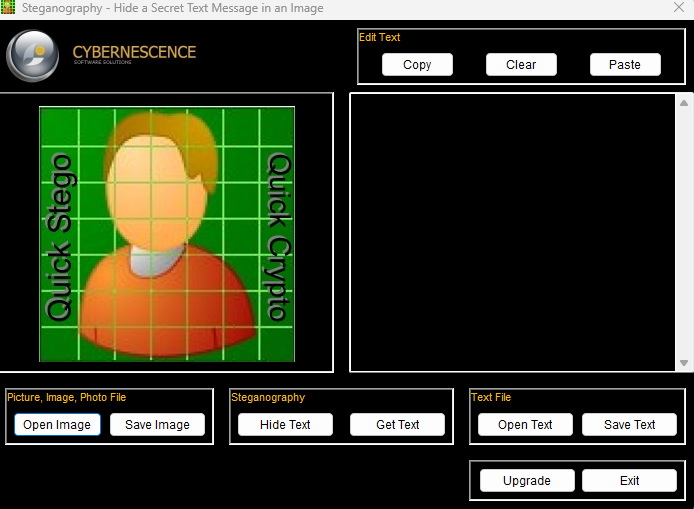
* 1. **QuickStego**

**3.2.1 Purpose:**

QuickStego is a popular tool that can be used for experimenting with DCT steganography. It provides a user-friendly interface to hide and extract data within the DCT coefficients of image files. It provides simple user friendly software that provides a simple interface where we can select an image file and embed a secret data within the DCT coefficients of the image.

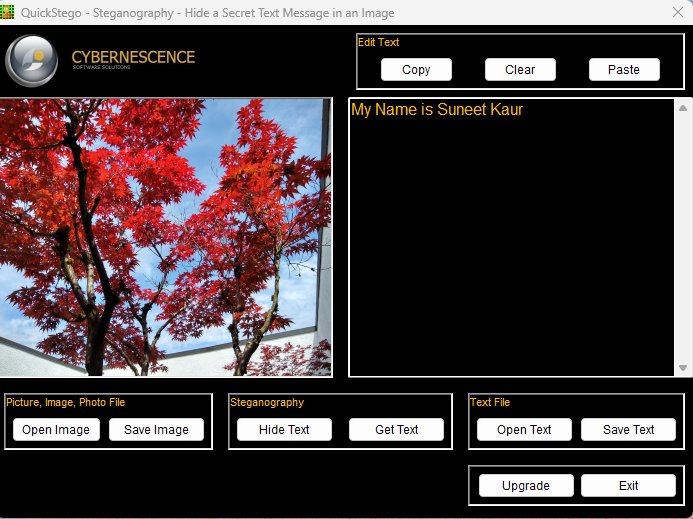
**3.2.2 Procedure:**

**Step 1**- Download QuickStego software and install it. Screenshot below shows the interface of QuickStego tool.



**Step 2 –** Click on ‘Open image’ and upload an image in which you want to hide the data. It will also show a preview of the inserted image. Also, click on ‘open text’ and upload a text file containing the confidential text that you would like to hide in the image.

The screenshot below displays the interface of QuickStego, previewing the image inserted to hide text and also, displays the text (“My name is Suneet”) that needs to be stored in the image.

****

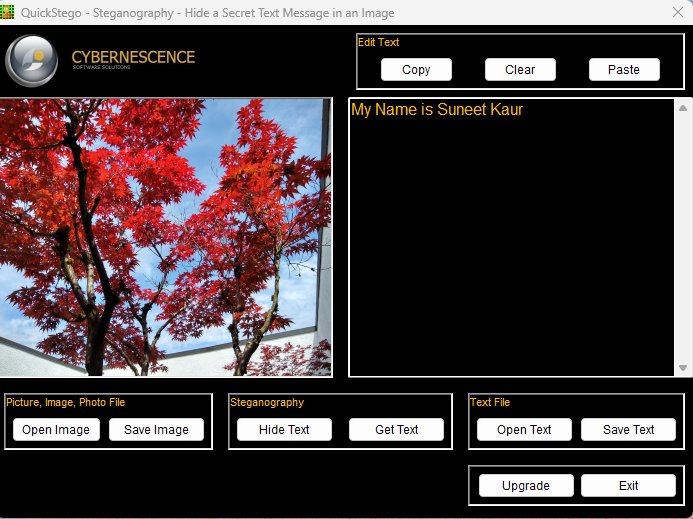
Step 3 – Click on ‘Hide text’ to hide the text in the image. As shown in the screenshot below the tool displays a message stating that the text is now hidden in the image.

A screenshot of a computer

Description automatically generated

Step 4- Click on the save image button to save the image with hidden text stored in it. The image will only be saved in BMP format although one can open an image in GIF, JPEG, JPG and BMP format.

Step 5– Extract the data by opening the image with hidden text and it will display the hidden message on the screen. As shown in the screenshot below, when image is opened in the tool, it displays the hidden text in the image.



* 1. **OpenStego**

A steganography tool called OpenStego can be used to hide any data in an image file. To use the OpenStego app, follow these steps:

2. Download OpenStego from the organization's website and install it. 1.

2. After installation, run the app.

**Hiding data:**

3. Select "Hide Data" from the menu.

4. Specify the location of your secret message document under the "Message File" option.

A screenshot of a computer

Description automatically generated

5. Specify the location for the cover image file in the "Cover File" option where you want to hide your data.

6. Select the location where you want to save your stego image from the "Output Stego File" option.

7. Set up an encryption password to prevent anyone from reading the stego file. This is optional.

8. After checking that everything is configured properly, press the "Hide Data" button to start the steganography procedure.

Output image after hiding message:

**A screenshot of a computer

Description automatically generated**

Output image after hiding message:

A purple flower with a yellow center

Description automatically generated

**Extracting data**

Run the OpenStego application and select "Extract Data" to extract data from the stego image. Then, specify the location of your stego picture under the "Input Stego File" option, and under the "Output Folder for Message File" option, specify the location where you wish to extract the data. Finally, enter the secret password if you used to encrypt the file and press "Extract Data".

A screenshot of a computer error message

Description automatically generated

A screenshot of a computer

Description automatically generated

* 1. **Silent Eye**

Silent Eye is a steganography software that allows to hide messages in an image file.

The steps are

1. Install the application
2. Go through the set up wizard

A screenshot of a computer

Description automatically generated

1. Drag the image you want to change.

A screenshot of a computer

Description automatically generated

1. Encode the message you want for that image.
2. Than pick the password to get that message.
3. Press encode.

A screenshot of a computer

Description automatically generated

1. To check if it is done properly select decode to see the message.

A screenshot of a computer

Description automatically generated  
and as you can see I have successfully encoded a message in that image.

# **4. Potential Risks Associated with Steganography:**

When it comes to Steganography there are few potential risks to aware of:

1. Information Leakage: Sensitive data can unknowingly leak through media files, putting the confidentiality of information at risk.
2. Covert Communication: Criminals can secretly communicate using steganography, making it hard for authorities to monitor their activities.
3. Data Exfiltration: Attackers can hide stolen data in innocent media files and sneak it out of an organization without detection.
4. Insider Threats: Malicious insiders can use steganography to bypass security controls and leak sensitive data unnoticed.
5. Evasion of Detection: Attackers can escape traditional security tools like antivirus by using steganography.
6. Malware Delivery: Steganography can be used to deliver malware by concealing malicious code in regular files, making it easier for infections.
7. Censorship Circumvention: In restricted environments, steganography may be employed to bypass censorship and share restricted information.
8. Legal Risks – The use of steganography to conceal illegal content, such as copyrighted material or malicious payloads, can result in legal consequences.
9. Detection Risks- While steganography aims to be undetectable, advanced forensic tools and hidden techniques can potentially uncover hidden information, especially in high security environments.

## **4.1 Mitigation Measures:**

1. To combat the risks of steganography, organizations should take certain steps.
2. Use advanced threat detection systems that can spot steganographic techniques and hidden data.
3. Conduct regular security training to raise awareness among employees about steganography risks and encourage reporting suspicious activities.
4. Deploy data loss prevention (DLP) solutions that can identify and stop data exfiltration through steganography.
5. Employ strong encryption to safeguard sensitive data, making it harder for attackers to exploit hidden information.

# **5. Practical Applications of Steganography:**

Steganography has practical applications in various domains for enhancing security and protecting data.

Let’s explore some of these applications as following:

**5.1 Data Protection:**

Steganography can safeguard sensitive information by hiding it within innocent-looking media files. This technique ensures that data remains safe during transmission or storage. For example, in the financial sector, steganography can be used to protect customer records and transactions details from unauthorized access.

* 1. **Watermarking:**

Digital watermarking is another application of steganography. It helps protect copyright and intellectual property rights by embedding invisible markers into images, videos, or audio files. This way, content creators are credited, discouraging unauthorized use.

**5.3 Authentication**:

Steganography plays a role in authentication by embedding secret codes or digital signatures into files. This helps verify the authenticity and integrity of digital documents, making sure they have not been altered without authorization.

**5.4 Covert Communication**:

Steganography can be used for secret communication, especially in espionage and military operations. Hidden encrypted messages can be sent within media files, allowing secure and undetected communication.

# **6. Potential Misuse or Illegal Activities:**

However, it’s essential to understand that steganography can also be misused for illegal activities:

* 1. **Data Theft and Espionage:**

Criminals may use steganography to hide stolen data, like confidential corporate information or intellectual property. They can then secretly extract and use this information without detection.

* 1. **Cybercrime and Malware Delivery:**

Cybercriminals can exploit steganography to conceal harmful software, viruses, or ransomware within regular files. This allows them to deliver these malicious programs and avoid antivirus detection.

**6.3 Online Terrorism and Covert Communication:**

Terrorist organizations or malicious groups might use steganography for covert communication, making it challenging for law enforcement to monitor and prevent potential threats.

# **7.Responsible Usage of Steganography:**

To ensure steganography is used responsibly, we need to follow these guidelines:

**7.1 Legal and Ethical Compliance**:

Always adhere to the laws and regulations regarding steganography avoid engaging in activities that infringe on privacy, copyright, or intellectual property rights.

* 1. **Obtain Consent**:

Obtain proper authorization and consent before embedding hidden data into media files. This applies to both the content creator and the recipient.

* 1. **Promote Awareness**:

Raise awareness about steganography, its benefits, and potential risks encourage responsible usage and discourage its misuse for illegal activities.

* 1. **Legitimate Purposes**:

Use steganography for legitimate purposes like data protection, watermarking and authentication. ensure that its application aligns with intended objectives and ethical guidelines.

By promoting responsible usage and understanding the risks, steganography can be a valuable tool for enhancing data security, protecting intellectual property, and facilitating secure communication in various domains.

# **8. Conclusion**

In this report we researched different steganography algorithms. Each of these algorithms and tools has its own strength and features so can be used according to one’s needs and preferences. DCT can achieve a good balance between hiding capacity and visual quality. Whereas LSB steganography achieves high capacity but may result in noticeable visual artifacts. Whereas spread spectrum steganography offers robustness against attacks and provides a high level of security and can also have good balance between hiding capacity and visual/audio quality.

Each technique has its own advantages and disadvantages. The choice of which depends on factors such as the desired hiding capacity, robustness against detection, and specific requirement of application.

Using Steganography algorithms can be a fascinating way to hide information within digital media. It offers a creative and intriguing approach to conceal data. However, it’s crucial to approach it responsibly and ethically.

# **9.References:**

<https://www.tutorialspoint.com/exploring-the-basics-of-image-steganography-in-cryptography>

<https://repository.stcloudstate.edu/msia_etds?utm_source=repository.stcloudstate.edu%2Fmsia_etds%2F75&utm_medium=PDF&utm_campaign=PDFCoverPages>

<http://article.nadiapub.com/IJAST/vol60/5.pdf>

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7913304/>

[ttps://commons.erau.edu/cgi/viewcontent.cgi?article=1039&context=jdfsl](https://commons.erau.edu/cgi/viewcontent.cgi?article=1039&context=jdfsl)

<https://achorein.github.io/silenteye/>

[Simple/Basic Steganography Algorithms and Methods | Saturn Cloud Blog](https://saturncloud.io/blog/simplebasic-steganography-algorithms-and-methods/)