Explore the Nature of Steganography

# Steganography

Steganography, derived from the Greek words "steganos" (meaning hidden) and "graphia" (meaning writing), is the art and science of concealing information within seemingly innocuous carriers such as images, audio files, or text. Unlike cryptography, which focuses on encrypting messages to prevent unauthorized access, steganography aims to hide the existence of the message itself. This clandestine communication technique has been used throughout history, dating back to ancient civilizations where messages were concealed within wax tablets or tattooed on messengers' scalps. The allure of steganography lies in its ability to covertly transmit sensitive information under the radar of surveillance or interception. By embedding secret data within a cover medium, whether it's altering the least significant bits of an image or subtly manipulating the structure of a sentence, steganography enables parties to communicate without arousing suspicion. In today's digital age, where vast amounts of data are exchanged daily across various channels, steganography presents both challenges and opportunities for digital forensics and cybersecurity professionals.

By examining a hypothetical scenario and hands-on demonstrations, we'll uncover the intricacies of steganographic methods, discuss the ethical and legal considerations surrounding its use, and highlight its relevance in the context of modern information security. As we journey through the hidden realms of steganography, we'll gain insights into its role in covert communication, its detection challenges, and its impact on forensic investigations.

## How it Works and Techniques

Steganography operates on the principle of embedding secret data, known as the "payload," within a cover medium, also called the "carrier," in such a way that the alteration is imperceptible to an observer. There are several techniques employed to achieve this covert communication:

1. **LSB Substitution**: One of the most common techniques involves altering the least significant bits (LSBs) of digital files such as images, audio, or video. Since LSBs contribute minimally to the overall perception of the content, modifying them to encode hidden information usually goes unnoticed. For example, in an image file, the RGB values of each pixel can be modified to represent binary data, with the LSBs serving as storage for the secret message.
2. **Whitespace Steganography**: This technique exploits the spaces, tabs, and line breaks within text documents or HTML code to conceal information. By strategically inserting extra spaces or modifying formatting elements, a hidden message can be encoded without visibly altering the appearance of the text. Whitespace steganography is particularly effective in online communication, where text-based platforms are prevalent.
3. **Spread Spectrum Technique**: Inspired by the spread spectrum communication technology used in wireless communication, this method involves spreading the secret data across a broader frequency range within an audio signal. By modulating the amplitude or phase of the carrier signal with the secret message, the embedded data becomes imperceptible amidst the background noise. This technique is commonly used in audio steganography to hide information within music or speech recordings.
4. **Digital Watermarking**: While not strictly steganography, digital watermarking is a related technique used to embed imperceptible marks or signatures within multimedia content for purposes such as copyright protection or authentication. Watermarks are typically designed to be robust against common signal processing operations while remaining invisible to the human eye or ear.

# Scenario

As you admired Drew's new exotic car, a sense of curiosity and suspicion began to gnaw at you. Drew's sudden acquisition of such a luxurious vehicle seemed incongruent with his purported profession as a stock market professional. Despite his claims of financial success, you couldn't shake the feeling that something was amiss. Intrigued by Drew's extravagant lifestyle, you decided to strike up a conversation with him, hoping to glean some insight into his apparent wealth. When you asked him about his secret to afford such a high-end car, he casually attributed it to his success in the stock market. However, upon further probing, you discovered that Drew had never pursued formal education in finance, nor had he ever participated in any investment discussions or workshops. As the days passed, your suspicions only grew stronger. You couldn't shake the feeling that Drew was hiding something, and you made a mental note to keep a close eye on his activities.

One day, an opportunity presented itself when you needed to pass a document to Drew for review. As you approached his desk, you noticed him engrossed in a conversation with others on his computer. Curiosity getting the better of you, you peered over his shoulder and caught a glimpse of the chat window. To your surprise, you saw that Drew and his recipient were communicating in vanish mode, a feature that automatically removes chat history after closing the application or after a certain period. Your suspicions peaked when you observed Drew's behavior during the conversation. He seemed unusually secretive and guarded, exchanging cryptic messages with his contacts. Your attention was drawn to the images being sent to Drew by the other participants. Without hesitation, Drew downloaded them to his PC and quickly responded with a message: "LET'S TAKE DOWN THE COMPANY." The gravity of the situation hit you like a ton of bricks. It was clear that something nefarious was afoot, and you knew you had to take action to prevent any harm from occurring. With a sense of urgency, you made your way to the IT department to report your findings and request further investigation into Drew's activities. As you recounted the details of the encounter to the IT professionals, you couldn't help but feel a sense of unease. What dark secrets lay hidden beneath Drew's facade of success? And what role did steganography play in his sinister plot to "take down the company"? With the investigation underway, only time would tell what truths would be uncovered and what consequences would ensue.

## Principles and Rules Violated

1. **Ethical Standards**: Drew's behavior of engaging in covert communication and potentially illicit activities goes against ethical standards expected in a professional environment. Ethical guidelines dictate honesty, transparency, and integrity in all interactions, especially within the workplace. By participating in clandestine communication and potentially plotting to harm the company, Drew breaches ethical norms.
2. **Privacy Policies**: The use of steganography to exchanging potentially sensitive information without proper encryption or security measures violates privacy policies within the organization. Employees are typically expected to adhere to company policies regarding communication channels and the handling of confidential information. Drew's actions may compromise the privacy and security of company data.
3. **Legal Regulations**: Drew's alleged plan to "take down the company" may violate various legal regulations, including those related to corporate espionage, insider trading, or conspiracy to commit unlawful acts. Engaging in activities that harm the company's interests or infringe upon the rights of stakeholders could lead to legal consequences for Drew and potentially other individuals involved.
4. **Corporate Governance**: Drew's behavior contradicts principles of corporate governance, which emphasize accountability, transparency, and responsible decision-making within organizations. Engaging in clandestine activities that threaten the stability and reputation of the company undermines the principles of good governance and may erode trust among stakeholders.

## Relation to Other Topic Discussed in Class

The scenario of Drew's suspicious behavior and potential involvement in covert activities intersects with several concepts and topics discussed in digital forensics and cybersecurity:

1. **Covert Communication**: Drew's use of steganography to exchange hidden messages exemplifies covert communication techniques. This relates to discussions about covert channels and steganography, which are methods used to conceal information and evade detection.
2. **Digital Forensics**: The scenario underscores the importance of digital forensics in investigating suspicious activities and uncovering evidence of wrongdoing. Digital forensic techniques, such as network analysis, data recovery, and steganalysis, would be essential in examining Drew's digital footprint and uncovering hidden messages or illicit activities.
3. **Incident Response**: The scenario demonstrates the need for effective incident response procedures to address security incidents and mitigate potential risks to the organization. Discussions about incident detection, response planning, and forensic analysis methodologies are relevant in handling situations like the one involving Drew.

## Backstory

By having completed a minor degree in cybersecurity, you've developed a keen interest in digital forensics and steganography. Your knowledge and skills in these areas have caught the attention of the IT department, who have enlisted your help to investigate suspicious activity within the company. The recent acquisition of an exotic car by your colleague, Drew, has raised eyebrows among the staff. Despite Drew's claims of success in the stock market, there are lingering doubts about the source of his newfound wealth. Your familiarity with steganography makes you the ideal candidate to assist the IT department in uncovering any potential wrongdoing.

Given your expertise, you're tasked with leading the investigation into Drew's activities and determining whether steganography is being used to conceal illicit communication. The stakes are high, as the company's reputation and security may be at risk if malicious intent is uncovered. With access to the necessary tools and resources, you set out to gather evidence and piece together the puzzle surrounding Drew's behavior. Your goal is clear: to identify any hidden messages or covert communication channels and to take swift action to protect the company's interests.

As you delve deeper into the investigation, you find yourself drawn into a web of secrecy and intrigue. The discovery of vanish mode chats and cryptic messages exchanged between Drew and unidentified individuals only serves to heighten your suspicions. With each piece of evidence uncovered, the urgency of the situation becomes increasingly apparent. Armed with your knowledge of steganography and digital forensics, you're determined to get to the bottom of the mystery surrounding Drew's activities. The fate of the company hangs in the balance, and it's up to you to ensure that justice is served and the truth is revealed.

# Demonstration

In this demonstration, I will walk through all the steganography techniques I used in this project.

Before I start the demonstration, here’s the development environment setup:

1. Install Visual Studio Code
2. Git Bash
3. OpenStego
4. Python 3.12.3
5. JDK 22

Requirements (Python Packages):

1. blinker == 1.7.0
2. click == 8.1.7
3. colorama == 0.4.6
4. Flask == 3.0.3
5. itsdangerous == 2.2.0
6. Jinja2 == 3.1.3
7. joblib == 1.4.0
8. MarkupSafe == 2.1.5
9. numpy == 1.26.4
10. pillow == 10.3.0
11. pip == 24.0
12. scikit-learn == 1.4.2
13. scipy == 1.13.0
14. threadpoolctl == 3.4.0
15. Werkzeug == 3.0.2

Let’s get the demonstration started,

1. Launch cpre436\_Win\_Final\_Project virtual machine. It is located under iselab01.ece.iastate.edu/ISELAB01/cpre436/isehost26.ece.iastate.edu/cpre436/cpre436\_kaiheng9. Username: Drew, Password: cpre436
2. Once successfully log in, you will see Drew’s Desktop with a Porsche 911 wallpaper.



1. On Drew’s Desktop, you can find the ‘Work’ folder, Autofire, openstego-Shortcut, and MrZ.png. This is important information for you to find out what Drew was working on.
2. First, you open up the Work folder. You will see two text files, CheckList.txt and ‘Project Proposal.txt’. Open both text files and read the content. You might find CheckList.txt a bit suspicious. Take note of this file.

A screenshot of a computer

Description automatically generated

1. In the CheckList.txt, you saw Drew mentioned a person called Mr.Z. On this desktop, there is an image file called MrZ. You open it and find no suspicious on this file. But, you have some knowledge of steganography. You become more suspicious of this file. Why is the image file named as MrZ? Then, you can try your luck by using OpenStego.

A screenshot of a computer

Description automatically generated

1. Congratulation! You found a piece of information. A text file was hidden in the image, information.txt.

A computer screen shot of a message

Description automatically generated

1. You will find that information.txt has been added to Drew’s Desktop. You open up information.txt. Take note of this text file.

A white background with black text

Description automatically generated

1. You find this information.txt mentioned a website and AudioStego. Look back to your note. In CheckList.txt, it mentioned a website, OpenStego, and AudioStego. And these three aspects are the program to conceal his secret messages. But remember, these three don’t share the same algorithms of concealing messages.
2. Now, on Drew’s Desktop, there is an application named Autofire. You double-click it and open up that webpage. It will show you the homepage of the website. Then, you click around the website and find out this is a normal beta webpage showing cars. But it is not. Look at the address bar of the website. This website is not published yet; you can find its HTML files in the file system.

A screenshot of a computer

Description automatically generated

1. “C:/Users/Drew/.MyWeb/” is the file directory you are looking for. And you went to that directory but you couldn’t find “.MyWeb”.

A screenshot of a computer

Description automatically generated

1. In Linux OS, the file or folder name starting with ‘.’ will not appear in the user interface. Take this as a hint. Drew purposely put ‘.’ in front of ‘MyWeb’, which means he wanted to hide this folder. Now, you want to check whether there is a hidden file. In File Explorer, find and click ‘view’ -> ‘Options’ -> “Change folder and search options.” The system will pop up a “Folder Options” window. In the “Folder Options” window, find and click ‘view’ -> “Show hidden files, folders, and drives,” apply changes and click ‘OK.’

A screenshot of a computer

Description automatically generated

1. Now, you will be able to see ‘.MyWeb’. Open the folder. You saw the HTML files, Python files, and folders. Now, let’s open up ReadME. The content shows how Drew plan to create AutoFire website. You will see “login.html – Hidden page only available for Mr.Z and me when successfully logged in.” Also, the content mentioned LSB steganography with images. You learned about this in class. Let’s find out what Drew was hiding.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. To make sure the website is working properly, start the Flask server. Open up Git Bash from Drew’s Desktop. To check if the Flask server is running, use ‘ps’. The image below shows Flask server is not running.

A screenshot of a computer

Description automatically generated

If the Flask server is not running, run this command: “python /c/Users/Drew/.MyWeb/flaskserver.py &”. The Flask server will run in the background. When you run ‘ps’ command again, you will see PID 1475, Flask server, running in the background. Keep that Git Bash open.

A computer screen shot of a program

Description automatically generated

1. Now go back to the website and click ‘Login’ in the navigation bar. Here are the valid users:

Username: elon Password: mars

Username: jack Password: ripper

Username: mrm Password: thesmartest

Username: mrz Password: thegreatest

Try out those usernames and corresponding passwords. You will find something. Recall back to the ReadME file in .MyWeb. It mentioned only Mr.Z and Drew are able to access the hidden page. And yes, mrz is Mr.Z’s username, and mrm is Drew’s username. Now, you know Mr.M is Drew.

Once you successfully log in with either Mr.Z or Drew credentials, you will be redirected to the hidden page. This is where Mr.Z and Drew will conceal and exchange their secret messages.

A screenshot of a computer

Description automatically generated

1. Let’s test it out the program. Choose any picture from Drew’s desktop and upload it.

A screenshot of a computer

Description automatically generated

1. You will find a folder called Favorite created in C:\Users\Drew. And in it, there is an image called “Bugatti Chiron.png”. To reveal the secret message, go back to .MyWeb folder, right-click and open Git Bash in the directory. Enter the following command: python extractor.py <Your Processed Image Path>. You have successfully revealed the message.

A computer screen shot of a computer

Description automatically generated

1. Since you know how to use the extractor.py, let’s find out the secret messages hidden by Drew. Go back to ‘.MyWeb’ folder to see which folder contains images. The ‘Cars’ folder contains some images. Some images are duplicated, such as car6, car6\_1, car12, car12\_1, car14, and car14\_1.

A screenshot of a computer

Description automatically generated

1. Let’s investigate the images. You will find secret messages were revealed from car6\_1.png, car12\_1.png, and car14\_1.png. One secret message shows that Drew will use audio to secure their conversation.

A computer screen shot of a black screen

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Let’s find out what Drew does with audio. First, you need to find out where the audio files are located at. The audio files are stored in the ‘C:\Users\Drew\Music\Audio’ directory. You will find duplicated audio files: original\_audio, original\_audio\_1, sample-15s, sample-15s\_1. You open up original\_audio and original \_audio\_1 are almost the same. Your instinct tells you something is hidden in those audio files. You wanted to prove you are right, but you must find the AudioStego first.
2. At ‘C:\IYKYK’ folder, you will find a zip file named AudioStego. Extract the zip file. You will find two Python files in the extracted folder.

A screenshot of a computer

Description automatically generated

1. It is time to prove. Right-click in the folder and open Git Bash here.

If you want to reveal the message, use this command: python audioDecoder.py <Suspicious Audio File> <Original Audio File>

If you want to conceal the message, use this command: python audioEncoder.py <Audio File> <Text File> <Output Directory>

Enter “python audioDecoder.py /c/Users/Drew/Music/Audio/original\_audio\_1.wav /c/Users/Drew/Music/Audio/original\_audio.wav” in Git Bash. You will get the secret message.

A computer screen shot of a program

Description automatically generated

Enter “python audioDecoder.py /c/Users/Drew/Music/Audio/sample-15s\_1.wav /c/Users/Drew/Music/Audio/sample-15s.wav” in Git Bash. You will get the secret message. This secret message is important. You could stop other companies from lossing.

A computer screen shot of a program

Description automatically generated

1. There is one piece of information that hasn’t been found yet. This information will prove Drew is guilty. Navigate to ‘C:\Users\Drew\Pictures\Saved Pictures,’ and you will find images and Dream\_car\_list.txt. Open up Dream\_car\_list.txt; you will see Drew mentioned, “The classic the best. Lovin’ it”. In the ‘Saved Pictures’ folder, you will see a duplicate image named Lovin’it. Open the OpenStego from Drew’s Desktop and extract the message.

A screenshot of a computer error message

Description automatically generated

1. The ‘pplan\_03272024.txt’ was extracted from the Lovin’it.png. You read the content of the text file; you found out Drew was planning to take down the company you are working with. Congratulations, you have avoided the bad things that will happen to the company. A white screen with black text

   Description automatically generated

# Conclusion

This project has provided me with deeper understanding of steganography techniques, applications, and ethical implications. Through a hypothetical scenario involving suspicious behavior and covert communication, I have illustrated the practical relevance of steganography in digital forensics and cybersecurity. This scenario highlights the ethical and legal considerations that arise when dealing with clandestine communication methods for conducting espionage activity, emphasizing the importance of upholding ethical standards, privacy policies, and legal regulations.

This project also offers valuable insights for both companies and law enforcement agencies into the realm of steganography, shedding light on covert communication techniques and their implications for security. By exploring various steganographic methods such as LSB substitution and spread spectrum technique, organizations gain a deeper understanding of how hidden messages can be concealed within seemingly innocuous carriers like images and audio files. Understanding these techniques is crucial for identifying potential vulnerabilities in communication channels and developing effective countermeasures to detect and prevent steganographic attacks.

One of the key takeaways from this project is the importance of remaining vigilant and proactive in addressing security threats. Companies and law enforcement agencies must prioritize incident response planning, digital forensic capabilities, and employee awareness training to mitigate risks associated with covert communication and clandestine activities effectively. By adopting proactive security measures, organizations can better protect their assets, preserve the integrity of their operations, and safeguard sensitive information from unauthorized access or manipulation.