Steganography Report

IT 360: Information Assurance and Security

by

Chahine Jebabli

Achref Mouelhi

Ahmed Nour

April 2023

Information Technology Major

Tunis Business School

2022-2023

Contents

Chapter 1

Introduction

1.1 What is Steganography

Steganography is the practise of concealing information within a medium, originating from the Greek words "steganos" (covered) and "graphial" (writing). This entails concealing the data so that only the intended recipient is aware of its presence. While archaic methods entailed concealing data on the backs of wax, writing tables, or even rabbit bellies, modern methods often involve transferring data in the form of text, images, video, and audio across numerous mediums. Multimedia items are frequently employed as cover sources to conceal sensitive data during transmission. Steganography's goal is to permit invisible communication while guaranteeing confidentiality between communicative parties. We intend to discuss several security and data concealment techniques that can be utilised in steganography, such as LSB and PVD, in this study. We will investigate the strategies' strengths and drawbacks, as well as their applicability in various circumstances. Our goal is to provide a thorough understanding of steganography and its potential applications. Readers will have a better knowledge of steganography and its function in facilitating secure communication by the end of this paper.

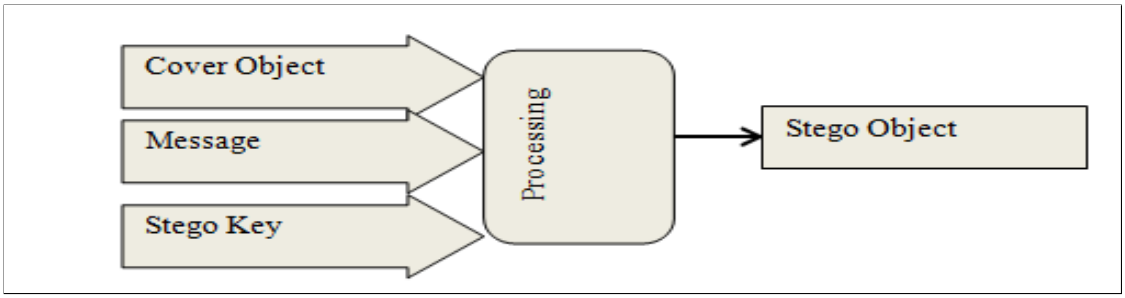

Figure 1.1: Steganography Action. Adapted from [1]

1.2 Process

The steganography process involves several steps:

1. Select and convert the secret data into a binary format.
2. Choose a cover object, such as an image or audio file.
3. Embed the secret data into the cover object using a steganographic algorithm.
4. Create a new file, known as the stego-object, which appears identical to the original cover object but contains the hidden secret data.
5. Transmit the stego-object over a chosen medium to the intended recipient.
6. Extract the secret data using a reverse steganographic algorithm.

By following these steps, steganography allows for the secure and discreet transmission of confidential information.

1.3 History

Steganography has an interesting history that dates back to ancient Greece. It has been used to disguise messages in a variety of methods, including ink and milk, as well as digital images, audio, and video files. Despite its growth, steganography's primary purpose remains the same: to keep information secret. This centuries-old strategy is still important in current communication.

1.4 Image steganography

Image steganography is a technique for concealing sensitive information within digital photographs. The secret information is encoded into the image pixels using a steganographic technique, resulting in a new image that appears identical to the original, known as the stego-image. The stego-image can be conveyed to the receiver via a specified medium, and the secret information can be extracted using a reverse steganographic technique. Despite the fact that image steganography is a common technique due to the popularity of digital photographs, it can be detected through statistical analysis or visual inspection.

Chapter 2

Basics

2.1 Cryptography Basics

Cryptography is a method of rendering information unintelligible to unauthorised individuals. This aids in the concealment of concealed information in steganography. Cryptography employs techniques to convert information into a secret code (ciphertext) that can be safely transferred. The recipient then decodes the information back into its original form (plaintext) using a key. Steganography employs several types of encryption, including symmetric key cryptography, public key cryptography, and hashing. Hidden information could be obtained by unauthorised parties if cryptography is not used.

2.2 Steganography Basics

Steganography is a method of concealing information within cover data in such a way that unauthorised users analysing the data are unable to find it. Unlike watermarking, steganography is designed to ensure that the hidden message is neither removed or altered by adversaries, but rather that it remains invisible. Steganography is very beneficial when encryption cannot be used to secure secret information during communication.

	Steganography	Cryptography
Definition	Depend on hiding the message existence	Depend on hiding the message meaning
Purpose	Keep communication secure.	Provide protection for data
Visibility	Never	Always
Failure	When discover the presence of a hidden message	When able to decrypt and read the message
Concern	Embedding capacity and detectability of cover object	Robustness against deciphering.
Carrier	Any type of digital media	Depend on text as a carrier
Key	Optional, but provide more security	Necessary

Figure 2.1: Steganography vs Cryptography. Adapted from [1]

Chapter 3

Main Concepts

Steganography is a method of hiding a hidden message within a cover image, audio file, or video file. The cover image acts as a vehicle for the hidden message, which is concealed within it via a steganography technique. To ensure safe communication, the algorithm defines how the secret message is encoded in the cover image, and a steganography key may also be employed. Understanding the fundamental fundamentals of steganography is essential for efficiently applying and employing this approach.

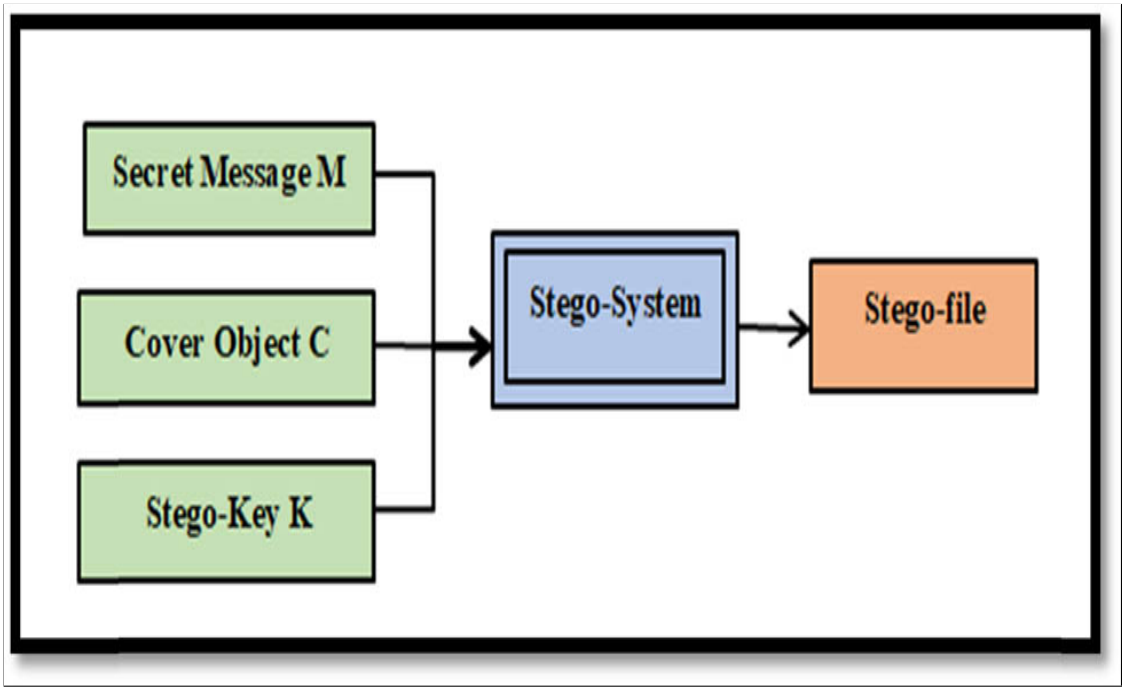

Figure 3.1: Steganography Main Concepts. Adapted from [2]

3.0.1 Cover Image

A cover image is the image in which the secret message is hidden. The cover image is chosen for its aesthetic complexity and resemblance to the original image. The cover image remains unmodified in image steganography, while the hidden message is embedded within it. The cover image can be in any format, including JPEG, PNG, and BMP.

3.0.2 Secret Message

The cover image's secret message is the message we want to conceal. The hidden message can take any form, including text, audio, video, or images. The secret message's size is determined by the capacity of the cover image to store it. To ensure confidentiality and integrity, the secret message is encrypted using a cryptographic technique.

3.0.3 Steganography Algorithm

The steganography algorithm is used to incorporate the hidden message into the cover image. Least Significant Bit (LSB), Pixel Value Differencing (PVD), and Spread Spectrum Steganography are several steganography algorithms. The LSB algorithm substitutes the least significant bit of each pixel in the cover image with the secret message's corresponding bit. The PVD algorithm embeds the secret message in the cover image by comparing the difference between neighbouring pixels. By spreading the hidden message across various frequency channels, the Spread Spectrum Steganography method embeds it.

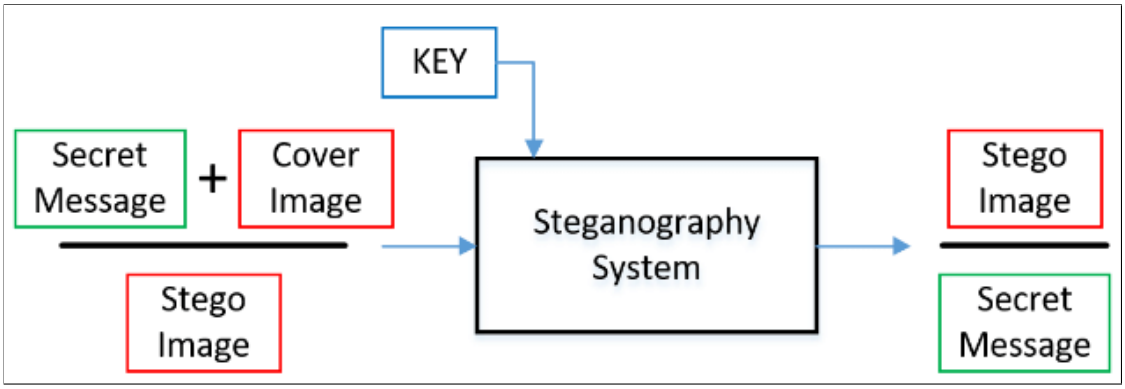

Figure 3.2: LSB-based image steganography system. Adapted from [3]

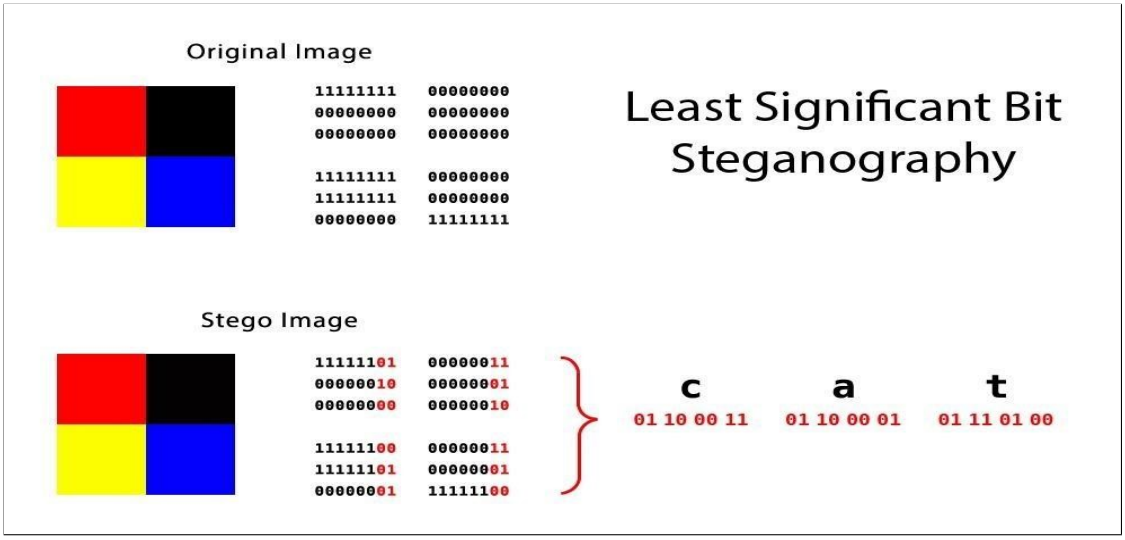

Figure 3.3: LSB Steganography [4]

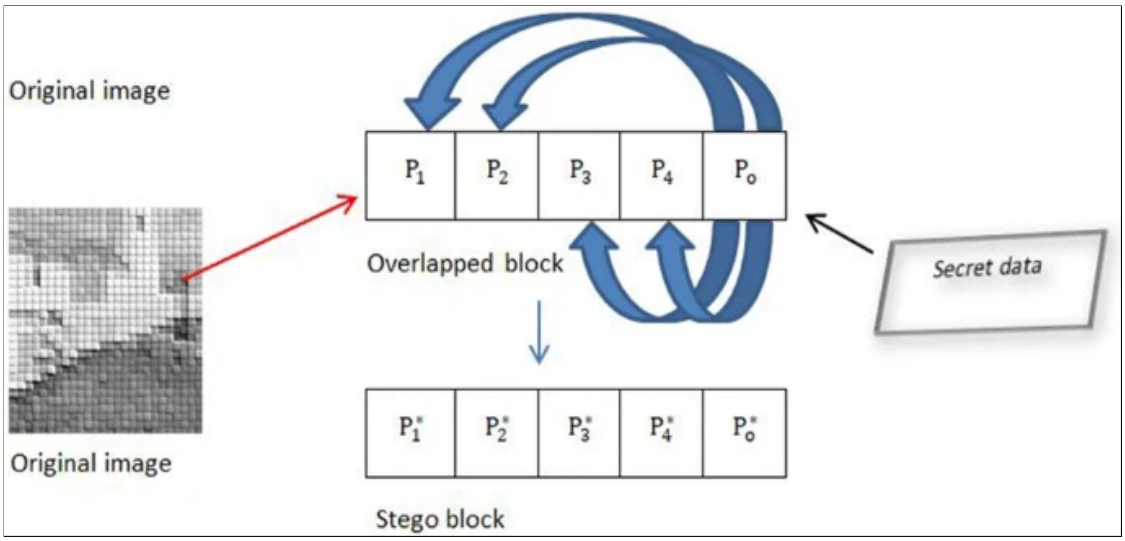

Figure 3.4: Pixel Value Differencing Image Steganography. Adapted from [5]

3.0.4 Steganography Key

A steganography key is a secret key that is used to encrypt the hidden message before it is included in the cover image. The steganography key is used to maintain the hidden message's confidentiality. Only the sender and intended recipient of the communication have access to the key. The hidden message is encrypted and decrypted using the steganography key. It is also used to choose which pixels in the cover image will contain the hidden message.

3.0.5 Key Takeaways

In summary, the cover picture, secret message, steganography algorithm, and steganography key are the essential ideas of image steganography. These ideas are crucial for understanding how image steganography works and how to use it safely.

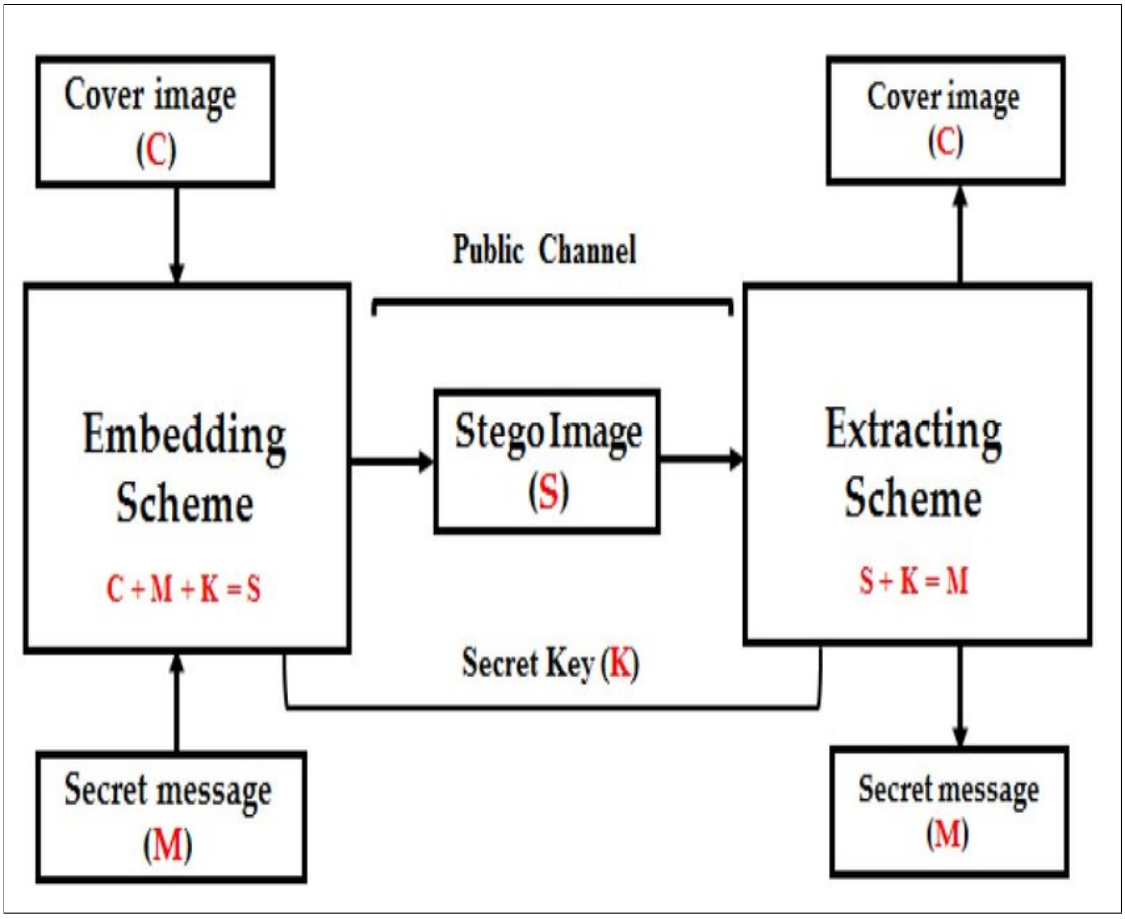

Figure 3.5: The basic concept of the steganography arrangement. Adapted from [6].

Chapter 4

Main Components

The four major components of steganography are embedding, extraction, cryptography, and user interface. The secret message is embedded, extracted, and encrypted using cryptography, and the user interface allows for system interaction. It is critical to grasp these crucial components in order to use steganography successfully and safely.

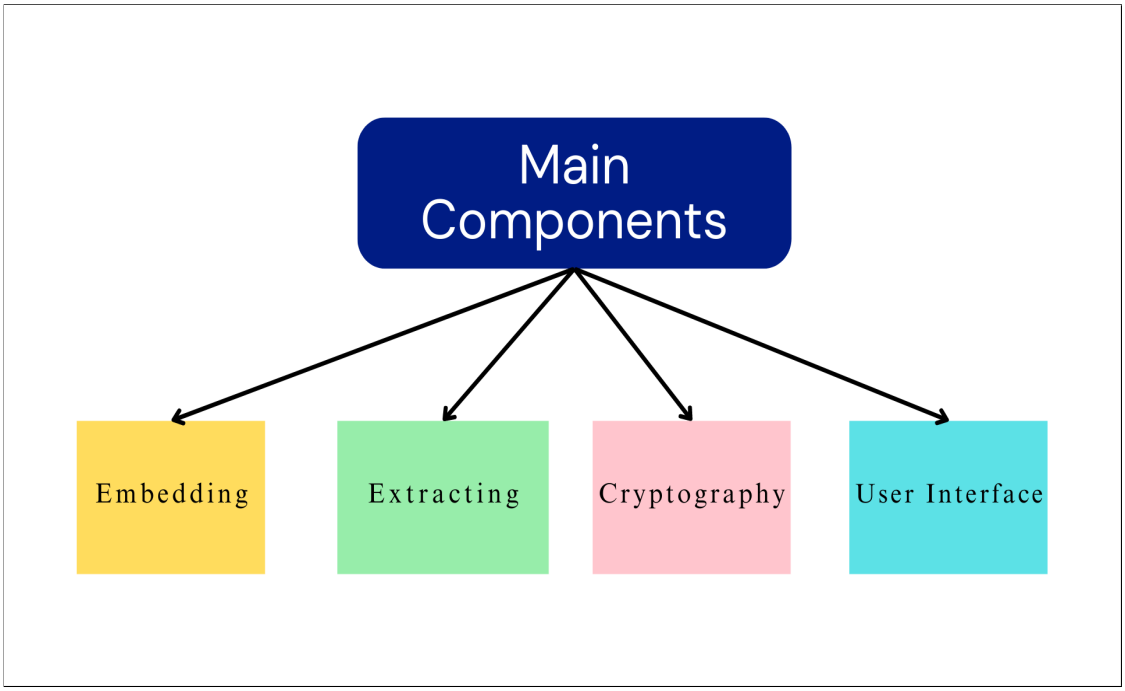

Figure 4.1: Steganography Main Components

4.0.1 Module for Embedding

Using techniques like as LSB and PVD, the embedding module conceals the hidden message in the image file. The least significant bit of each pixel is replaced with a bit from the secret message using LSB, whereas PVD alters the difference between pixel values in consecutive pixels. PVD can embed the message more effectively but may distort the image, whereas LSB has little influence on image quality but is open to assaults.

The embedding module usually consists of the following steps:

- Choose a carrier image and a hidden message.
- Convert the encrypted message to binary format.
- Disassemble the carrier image into individual pixels.
- Using the embedding procedure, replace the bits of the carrier picture with the bits of the hidden message.
- Save the changed image that contains the hidden message.

4.0.2 Extraction Module

The extraction module is in charge of obtaining the hidden message from the image file. The extraction procedure entails analyzing the image file and recovering the hidden message bits that were encoded in it. To retrieve the secret message, the extraction module employs the same procedures as the embedding module. To ensure that the extracted message is accurate and complete, the extraction module includes error correction methods.

The extraction module usually consists of the following steps:

- Load the carrier picture with the hidden message.
- Using the extraction algorithm, extract the bits of the secret message.
- Convert the extracted bits back to the secret message format.
- Using error correction methods, check the secret message's integrity.
- Show the user the extracted secret message.

A.LSB Embedding Algorithm

Input: photo cover (p) $\in P^L$, secret message (x) $\in \{0,1\}^m$, key (k)

Output: stego photo (g) with x implanted note bits

PRNG Seed with k

route = comb (l);

//comb (l) is a pseudo-random combination of {1,2,..l}

g = c;

z = min(x,n);

for j = 1 to z {

g[route[j]] = c[route[j]] + m[i] – c[route[j]] mod 2;

}

B.LSB Extracting Algorithm

Input: stego image (g) $\in P^L$, key (k)

Output: secret message (msg)

PRNG Seed with k

route = comb (l);

//comb (l) is a pseudo-random combination of {1,2,..l}

for i = 1 to m {

msg[i] = s[route[i]] mod 2;

}

Figure 4.2: LSB Embedding and Extracting Algorithms. Adapted from [2]

4.0.3 Module of Cryptography

The cryptography module is in charge of encrypting the secret message before embedding it in the picture file. The cryptography module ensures that the secret message is secure and that only the intended recipient has access to it. To encrypt the secret message, the cryptography module employs several encryption methods such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA).

Typically, the cryptography module includes the following steps:

- Choose a secret message to encrypt.
- Decide on a cryptography algorithm and create a key
- Using the key and the cryptography technique, encrypt the secret message.
- Using the embedding module, insert the encrypted message into the carrier image.
- Distribute the key to the appropriate recipient

4.0.4 User Interaction

The user interface gives the steganography tool a graphical user interface (GUI). The user interface allows the user to select the carrier image and the secret message, as well as to configure the encryption technique and key and to start the embedding and extraction operations. The user interface is user-friendly and intuitive, allowing even non-technical individuals to utilize the steganography programme with ease.

User interface features:

- An interface for picking the carrier image and the hidden message from files.
- An encryption configuration interface that allows you to configure the encryption algorithm and key.
- An embedding interface used to start the embedding process.
- Using the embedding module, insert the encrypted message into the carrier image.
- An extraction interface used to start the extraction process.
- The retrieved secret message is shown using a message display interface.

4.0.5 Key Takeaways

In summary, embedding, extraction, cryptography, and user interface are the four essential components of steganography. The embedding module hides the secret message within the carrier image, and the extraction module retrieves it. Before embedding the message, cryptography encrypts it, and the user interface allows users to engage with the steganography tool. Both the embedding and extraction modules require a number of processes, including error correction to ensure proper message retrieval. Overall, understanding these fundamental components is critical for using steganography efficiently and safely.

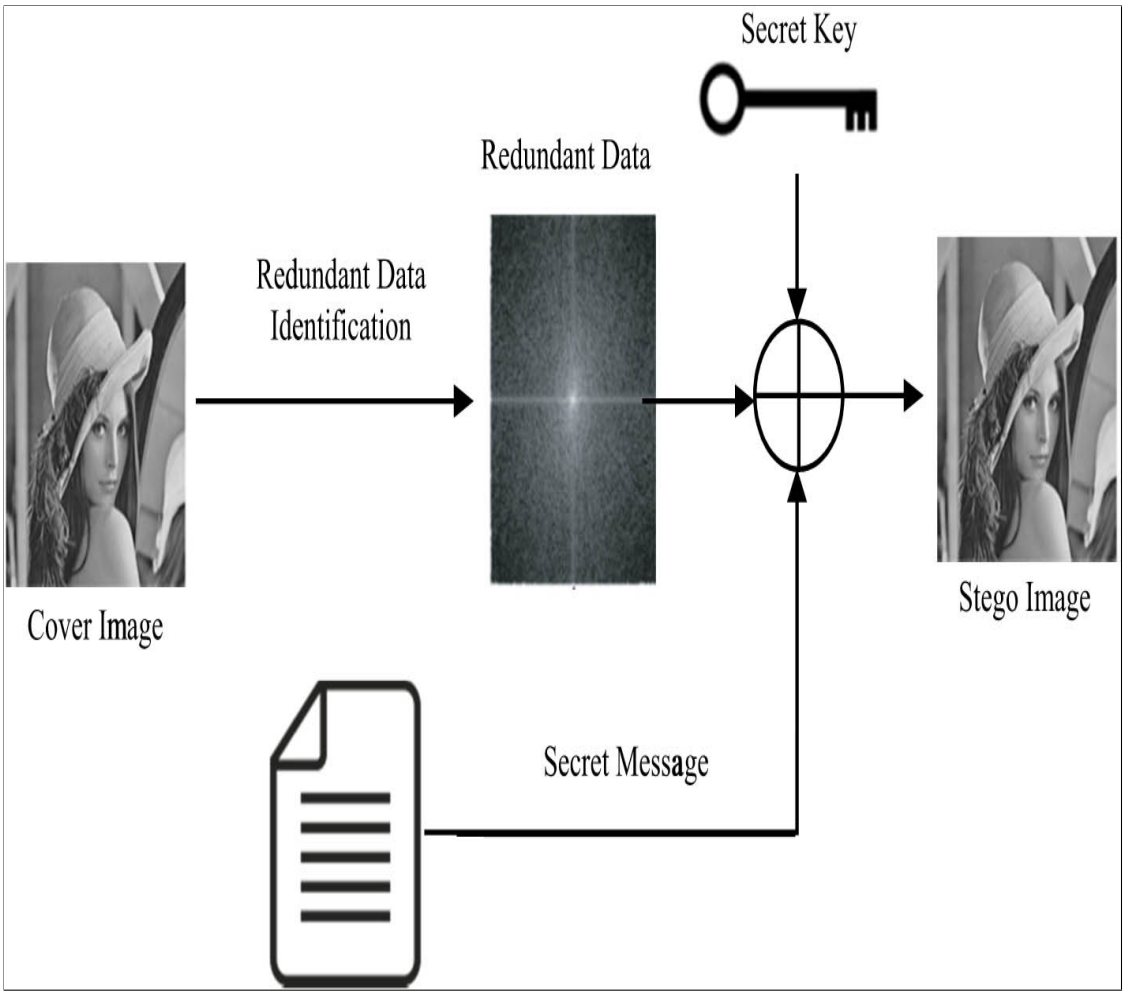

Figure 4.3: LSB System. Adapted from [2]

Chapter 5

Functional Flow

The step-by-step process of hiding a secret message behind a cover image to create a stego-image is referred to as steganography functional flow. Inputing the cover image and secret message, encrypting the secret message, embedding the encrypted message into the cover image, generating the stego-image, securely transmitting it, extracting the encrypted secret message, decrypting it, and displaying the hidden message are all common steps in this process. Understanding this functional flow is essential for using steganography for clandestine communication.

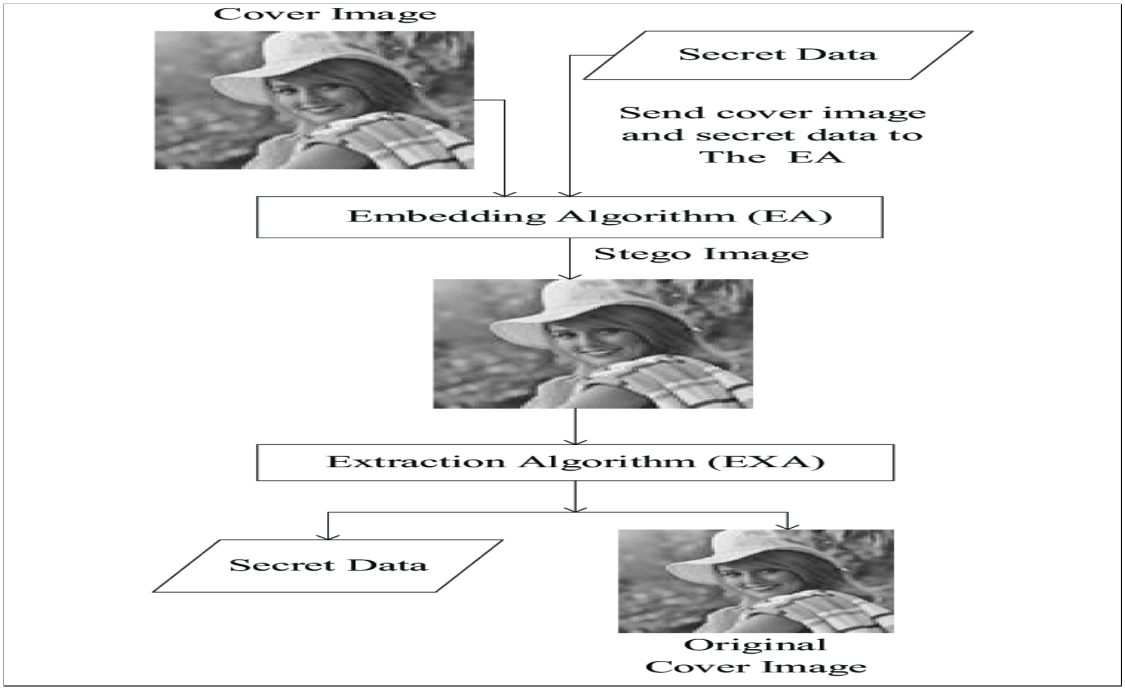

Figure 5.1: Steganography Functional Flow. Adapted from [7]

5.0.1 Input Cover Image and Secret Message

The cover image and secret message are entered into the system by the user: The user enters the input cover image and the secret message to be hidden in this phase. The cover picture can be any image that will be used as the carrier for the hidden message, such as a JPEG or PNG file. The secret message can be any data that needs to be kept private, such as text, audio, or video.

Here are some examples of cover images for an Image Steganography System:

- Image of natural scenery, such as a landscape or a beach view.
- Images of a creative nature, such as paintings or drawings.
- Photos of commonplace objects, such as a cup, a book, or a pen.
- Personal photographs, such as those of family members or pets.
- Images that are abstract, such as colourful patterns or textures.

The cover image for steganography should be carefully chosen to avoid suspicion. The chosen image should not raise any suspicions or appear suspicious. Following the submission of the cover image and secret message, the secret message is encrypted using a cryptographic technique to maintain confidentiality.

5.0.2 Secret Message Encryption

To guarantee confidentiality, the secret message provided by the user is encrypted in steganography. In the encryption process, a steganography key is utilised to generate a unique encryption pattern for each message. This key is a secret code known only to the sender and intended recipient, and it changes the arrangement of the message's bits, making deciphering difficult without it. Depending on the level of protection required and available processing power, many cryptographic methods can be used. Using a steganography algorithm, the encrypted message is subsequently inserted in the cover image.

5.0.3 Secret Message Embedding

A steganography algorithm is used to embed the encrypted secret message into the cover image. The algorithm is intended to obscure the message in an unnoticeable manner. Depending on the security level and type of cover picture, various methods such as LSB, PVD, and SS can be employed. The steganography algorithm alters particular parts of the cover image to include the encrypted message while retaining the image's aesthetic look. A stego-picture including both the original cover image and the concealed message is created. It can be viewed and sent to the intended recipient.

5.0.4 Generating the Stego-Image

A stego-picture is created by merging the cover image and changed pixels carrying the encrypted secret message. The user is then shown the stego-image to confirm that it appears natural and does not raise suspicion. To avoid unauthorised access, the stego-image should be transferred using a secure connection. The user has the option of keeping the stego-image for personal use or sending it to the intended recipient.

5.0.5 Transmitting the Stego-Image securely

The stego-image can be communicated to the receiver using secure methods such as email or messaging apps, and encryption techniques such as TLS or SSL can be used to protect the data while it is being transmitted. Password security can also be used to ensure that the stego-image is only accessible to the intended recipient. If an unauthorised entity gains access, the steganography technique and key can be utilised to extract the secret message. The recipient can utilise the extraction module to obtain the message after it has been transmitted.

5.0.6 Extracting the encrypted secret message

The recipient uses the extraction module to extract the secret message from the stego-image, which is then decrypted using the same technique and key as the cryptography module. To avoid security issues, the extracted message is displayed to the receiver, who should keep it secure and erase the stego-image.

5.0.7 Decrypting the encrypted secret message

The steganography key is used by the extraction module to decipher the embedded secret message that was encrypted by the cryptography module. The encryption and decryption modules share the same algorithm and key. The extracted message is then shown to the intended recipient, who must maintain the key secret in order for the message to be extracted from the stego-image. For the intended recipient to extract and read the buried secret message, the seventh step is critical.

5.0.8 Displaying the secret message

The original message is displayed to the receiver when the extraction module decrypts the secret message using the steganography key. The recipient can then take appropriate actions based on its contents. Because the decrypted message may contain critical information, it must be kept discreet and safe. The completion of the final step indicates that the secret message was securely transferred to the recipient and was not intercepted. The eighth and last phase of an Image Steganography System is critical for the recipient to access and interpret the secret message and take necessary actions as a result of it.

5.0.9 Key Takeaways

To summarise, the functional flow of steganography entails hiding a hidden message beneath a cover image to form a stego-image. To guarantee confidentiality, the input cover image and secret message are encrypted, and a steganography algorithm is employed to embed the encrypted message into the cover image in an imperceptible manner. Using encryption techniques and password security, the stego-image can be securely transferred to the intended recipient, and the receiver can extract and decrypt the concealed message using the steganography key. The original communication is shown to the receiver, who must keep it private and secure. Understanding the functional flow of steganography is critical for employing it for covert communication.

Chapter 6

Conclusion

In this study, we looked at the basics of steganography, such as the cover image, secret message, steganography algorithm, and key. We also talked about the main steganography components, such as the embedding and extraction modules, the cryptography module, and user interface. We also demonstrated the steganography functional flow, which includes entering the cover image and secret message, encrypting the secret message, embedding the message, generating the stego-image, securely transmitting it, extracting the encrypted message, decrypting it, and displaying the secret message.

Furthermore, we examined the importance of steganography in numerous domains, such as military and forensic investigations, as well as its limitations. To prevent unauthorised access to the secret message, we also highlighted the requirement for secure communication routes and encryption.

In conclusion, Finally,steganography is an effective approach for securely transferring information that is not limited to a certain field. However, it is critical to select appropriate steganography algorithms and keys to ensure the secret message's confidentiality. Future study could concentrate on the development of more robust steganography techniques and their use in other fields.

We would like to express our gratitude to our professor Mrs. Manel Abdelkader for providing us with the guidance and support that helped us reach this point. We extend a personal thank you to her for her invaluable contributions to our learning journey.

Bibliography

[1] M. Anbarasi and V. Karthikeyani, "A survey of steganography and steganalysis techniques in digital images," *International Journal of Computer Science Information Security*, vol. 1, pp. 1–6, 06 2009.

[2] F. A. Baothman and B. S. Edhah, "Toward agent-based lsb image steganography system," *Journal of Intelligent Systems*, vol. 30, no. 1, pp. 903–919, 2021.

[3] Q. Do and I. Koo, "Fpga implementation of lsb-based steganography," *Journal of Information and Communication Convergence Engineering*, vol. 15, pp. 151–159, 09 2017.

[4] WonderHowTo, "Steganography: Hide secret data inside image or audio file in seconds." `https://shorturl.at/EJX25`, accessed on 2023-04-22.

[5] S. Chauhan and G. Singh, "Pixel value differencing based image steganography: a review," *SN Computer Science*, vol. 9, pp. 321–326, 11 2018.

[6] M. Hashim, A. A.Mahmood, and M. Mohammed, "A pixel contrast based medical image steganography to ensure and secure patient data," *The International Journal of Nonlinear Analysis and Applications (IJNAA)*, vol. 12, pp. 2008–6822, 12 2021.

[7] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *Journal of King Saud University - Computer and Information Sciences*, vol. 31, 07 2019.