VIETNAM NATIONAL UNIVERSITY
HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY
Faculty of Computer Science and Engineering

CRYPTOGRAPHY AND NETWORK SECURITY (CO3069)

Assignment

STEGANOGRAPHY

Advisor: Nguyen Duc Thai
Students: Doan Viet Tu - 1952521
Tran Trung Hieu - 1952684
Vu Tien Giang - 1952240

HO CHI MINH CITY, SEMESTER 2022 - 2023

Contents

Contents **1**

1 INTRODUCTION **2**

2 BACKGROUND STUDY **3**
2.1 STEGANOGRAPHY 3
2.1.1 Definition 3
2.1.2 Applications 4
2.1.3 Steganography vs Cryptography 5

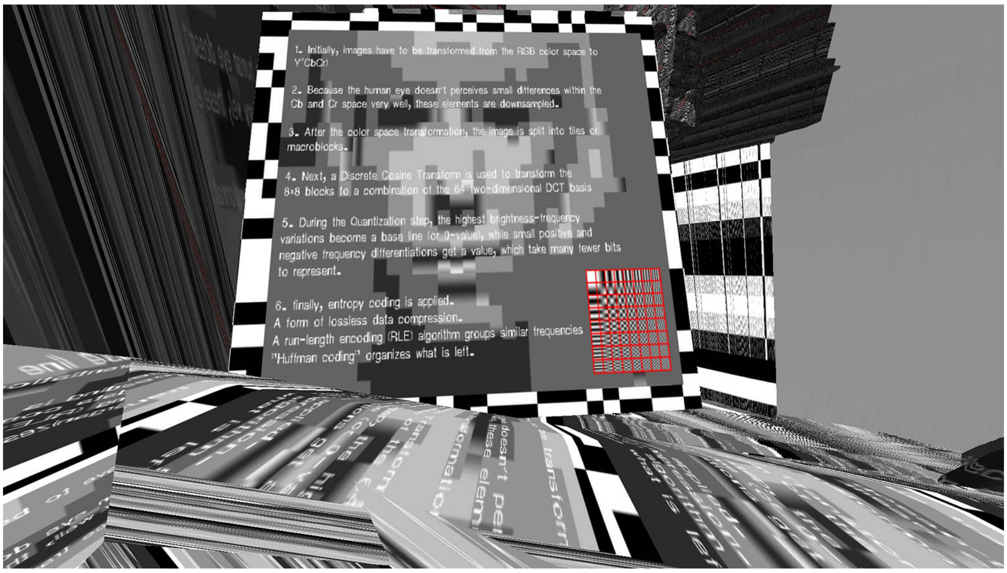
3 IMPLEMENTATION **7**
3.1 Image Steganography 7
3.2 Pixel 7
3.3 Least Significant Bit (LSB) algorithm 7
3.4 How our tool works 8
3.4.1 Installation 8
3.4.2 Demo 8

4 CONCLUSION **10**
4.1 Final words 10

References **11**

1 INTRODUCTION

"Who owns the information, he owns the world", a famous phrase of Rothchilds has a bit different meaning nowadays but still accurate. Information or data is very decisive resource to us as the development of the internet increased rapidly. Sensitive data can lead to the collapse of information systems, organizations or even countries as well. Securing information is becoming a bigger concern. Cryptogrphy is used in most cases with wide range of encrypting and decrypting methods to secure the message. Due to the increase of technology, people sometimes requires more than just cryptography. Steganography is used to secure the information by hiding it inside other information. It works like a camouflage of secret data and combine with cryptography to increase security level.



1. Initially, images have to be transformed from the RGB color space to Y'CbCr)

2. Because the human eye doesn't perceives small differences within the Cb and Cr space very well, these elements are downsampled.

3. After the color space transformation, the image is split into tiles of macroblocks.

4. Next, a Discrete Cosine Transform is used to transform the 8x8 blocks to a combination of the 64 two-dimensional DCT basis

5. During the Quantization step, the highest brightness-frequency variations become a base line (or 0-value), while small positive and negative frequency differentiations get a value, which take many fewer bits to represent.

6. finally, entropy coding is applied.
A form of lossless data compression.
A run-length encoding (RLE) algorithm groups similar frequencies
"Huffman coding" organizes what is left.

Figure 1: Steganography.

We will study about steganography, its types and examples, to see how different between steganography and cryptography, to know how this techniques helps to overcome the problems of data security and to test and evaluate the quality by performing image steganography.

2 BACKGROUND STUDY

2.1 STEGANOGRAPHY

2.1.1 Definition

Steganography is a technique for hiding secret information by enclosing it in a regular, non-secret file or communication and the information is extracted at the intended location, thus avoiding detection. The word steganography is combined from the Greek words steganos (meaning hidden or covered) and the Greek root graph (meaning to write).

There are several types and forms of steganography but only a few are interesting and commonly used:

- **Physical:** one does not involve the use of digital mediums or files, for example:
  - Writing messages with invisible ink, which can be read by applying certain chemical techniques.
  - Using ciphering techniques to hide information within textual information.
- **Microdots:** shrinking messages to such tiny dimensions, they are made almost invisible. These also involve placing tiny dots within a message to convey a specific message.
- **Digital:** uses digital mediums to hide secret information such as:
  - **Text Steganography:** Text files can contain steganography, which involves discreetly storing information. With this technique, each word's letter contains an encoded version of the concealed data.
  - **Image Steganography:** Concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography. In digital steganography, images are frequently used as a cover source since the computer description of an image contains multiple bits. Change
    There are various term in image steganography:
    - Cover image: unique picture that can conceal data.
    - Message: Real data that can mask within pictures. Message can be in form of standard text or image.
    - Stego image: an image contains a hidden message.
    - Stego-key: with this key, messages can be embedded in cover images and stego-images but they also can be derived from the photos themselves.
  - **Audio Steganography:** It is the study of how to conceal data in sound. It safeguards against illegal reproduction when used digitally. Using the watermarking technique, the message is encrypted within another piece of data (the "carrier"). Media playback, primarily audio clips, is what it is typically used for.
  - **Video Steganography:** Using video steganography, data or other files can be covertly included in video files on a computer. The "carrier" in this design can be video (a compilation of still images). The discrete cosine transform (DCT), which is invisible to the naked eye, is frequently used to insert values that can be utilized to obscure the data in each image in the movie. H.264, MP4, MPEG, and AVI are the most frequently used file formats for video steganography.

  - **Network or protocol Steganography:** hiding data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

2.1.2 Applications

Some common Steganography examples in real life are:

- **Invisible ink:** It is a substance used for writing, which is invisible either on application or soon thereafter, and can later be made visible by some means, such as heat or ultraviolet light. This is the most common method that people will see in some detective films.

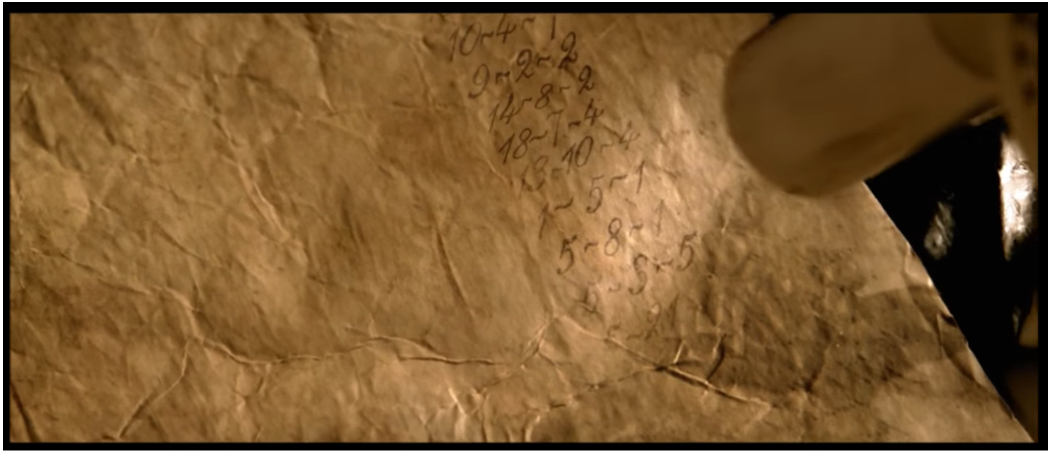


Figure 2: Invisible ink used in the film National Treasure

- **Backward masking:** Backmasking is a method of recording a message backward onto a track that is intended to be played forward. This is most common seen in some songs but the most common one is Revolution 9 by The Beatles. The link below is the backward masking of that song in the first 40 seconds.
  https://www.youtube.com/watch?v=n7QZNZx2QKA
  We can hear something that is close to *"Turn me on dead man"*. This may relate to the background of the song but we are only using it on steganography aspect.

- **Embedding text in a picture:** Just like the title, this method modifies the image pixels for hiding secret information. In the 2 images below, we do not see any difference between the original picture and the stego image because this method commonly needs tools to encrypt the messages into the images and what we are seeing below is just the result.

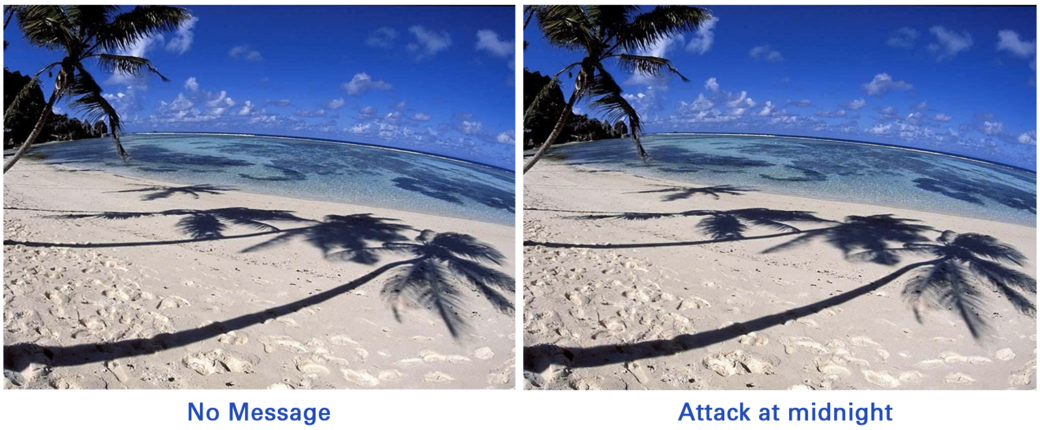


Figure 3: Hidden message inside a normal image

Sometimes, to see the hidden messages in this method, people need to use different lights such as green, blue, or red light.

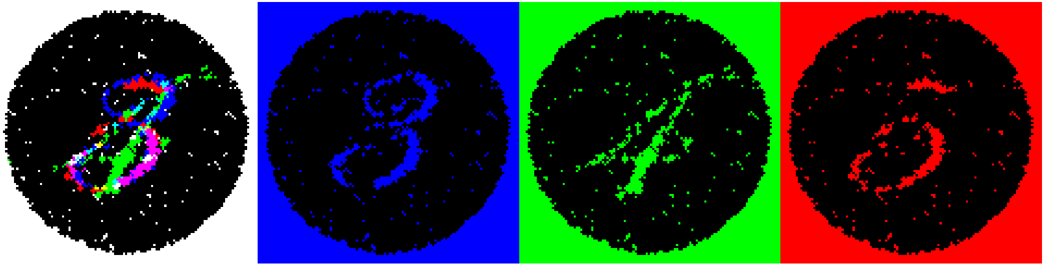


Figure 4: Number is shown when using different lights

2.1.3 Steganography vs Cryptography

At their most basic level, steganography and cryptography work to hide communications and data from prying eyes. It may immediately occur to us that this is similar to cryptography, but it is not. Cryptography focuses on keeping information secret while steganography aims for making information existence secret.

Below is the table to compare the main factors of steganography and cryptography:

Properties	**Steganography**	**Cryptography**
Definition	A method to hide a secret communication	A method to make the information unintelligible
Purpose	Maintain communication security	Protect the data
Key	Optional but boots security when used	Essential requirement
Data visibility	No	Yes
Risk	Once secret information has been unlocked, anyone can use the data	If you have access to the decryption key, you can decipher the ciphertext and retrieve the original message.
Data order	Does not change the data's general order	Change the data's general order

Steganography is different from cryptography, but combining the two can increase the security of the data that is being safeguarded and keep the covert communication from being discovered.

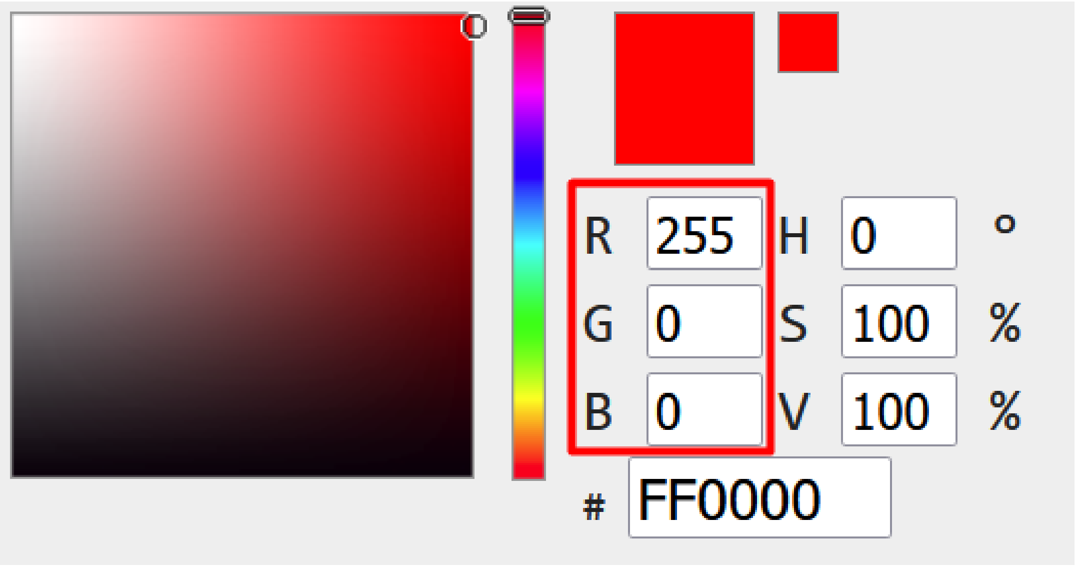
3 IMPLEMENTATION

3.1 Image Steganography

As mentioned above in the applications of steganography, image steganography needs tools or softwares to encrypt the data into the picture. Therefore, in this assignment, we will implement the tool used for **image steganography**.

3.2 Pixel

First, it is critical that we need to understand pixels and colour models. The pixel is the smallest portion of an image or display that a computer is capable of printing or displaying. For grayscale photographs, an 8-bit data value (with a range of 0 to 255) or a 16-bit data value (with a range of 0 to 65535) is frequently used. While for color images, there are 8-bit, 16-bit, 24-bit, and 30-bit colors available. The 24-bit colors having 3 8-bit pixels, one for each of the red, green, and blue intensities, are considered as real colors. For example, a pixel with a value of 255, 0, and 0 is a red pixel.



R 255 H 0 °
G 0 S 100 %
B 0 V 100 %
FF0000

Figure 5: RGB value for a red pixel

As mentioned above, the 24-bit colours are considered as real colours, we will work with it on this assignment. Each 8-bit colour contains 8 digits (0 or 1) for each. The smallest number would be 00000000 in 8 digits representation, which is 0 and the largest number would be 11111111 in 8 digits representation, which is 255. Any pixels in 8-bit case could accommodate anything between 0 to 255 as a value for each of the colors.

3.3 Least Significant Bit (LSB) algorithm

In computing, the **least significant bit (LSB)** is the bit position in a binary integer representing the binary 1s place of the integer. Similarly, the **most significant bit (MSB)** represents the highest-order place of the binary integer. The LSB is sometimes referred to as the low-order bit or right-most bit, due to the convention in positional notation of writing less significant digits further to the right. The MSB is similarly referred to as the high-order bit or left-most bit.

In this assignment, we will implement the LSB algorithm.

3.4 How our tool works

According to the 2 topics above, we will now apply them to the project.

For example, we have a red pixel RGB(255,0,0) with the 8-bit value of each colour is 11111111, 00000000 and 00000000 respectively and a letter B with 8-bit value is 01000010. Now, we will replace 2 LSB of the 8-bit value of each colour by 2 MSB of the B character by from left to right. In the example above, after replacing, the 8-bit colours will have the values of 000000**01**, 000000**00** and 000000**00** respectively. The 8-bit value of letter B still has 10 but it will replace the next red pixel's 8-bit value.

That is how our tool encodes the message into an image. For decoding, we will just need to reverse the process.

3.4.1 Installation

For this tool to work, the installation of **OpenCV** library is required.

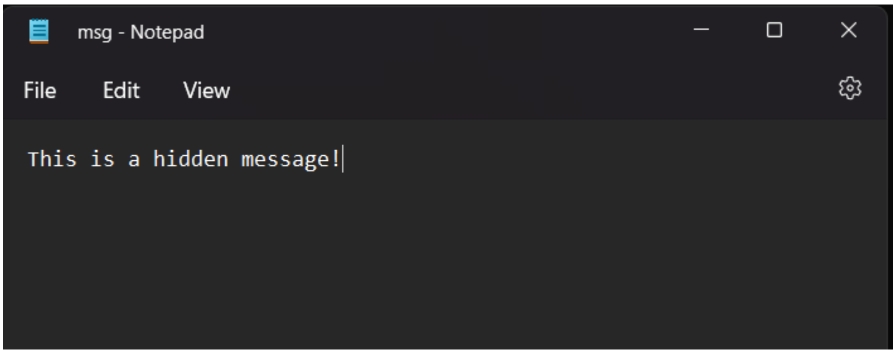
- Linux: Install on Linux
- Windows: Install on Windows

Folder arrangment:

- Place your picture inside 'image' folder.
- Place your text inside 'message' folder.

3.4.2 Demo

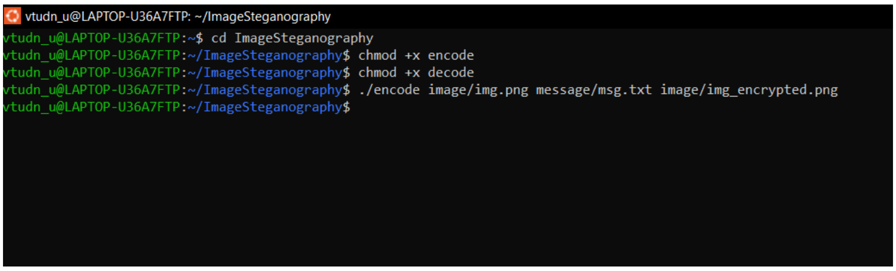
Now we will try to hide a message inside the picture.



This is a hidden message!

Figure 6: The text file.

Firstly, let's move to the directory of the tool. Here, we will use the command 'chmod +x' to give permission to the executable programs. Then we should start the encoding process.



```
vtudn_u@LAPTOP-U36A7FTP: ~/ImageSteganography
vtudn_u@LAPTOP-U36A7FTP:~$ cd ImageSteganography
vtudn_u@LAPTOP-U36A7FTP:~/ImageSteganography$ chmod +x encode
vtudn_u@LAPTOP-U36A7FTP:~/ImageSteganography$ chmod +x decode
vtudn_u@LAPTOP-U36A7FTP:~/ImageSteganography$ ./encode image/img.png message/msg.txt image/img_encrypted.png
vtudn_u@LAPTOP-U36A7FTP:~/ImageSteganography$
```

Figure 7: Encrypting.

Now the message is already embedded to the picture. Note that the encrypted picture may not look so diffrent from the original because of the LSB algorithm.

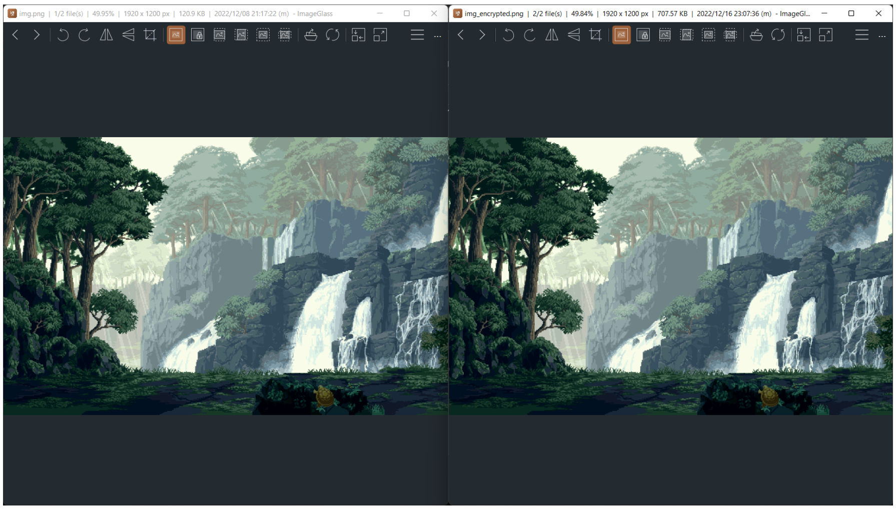
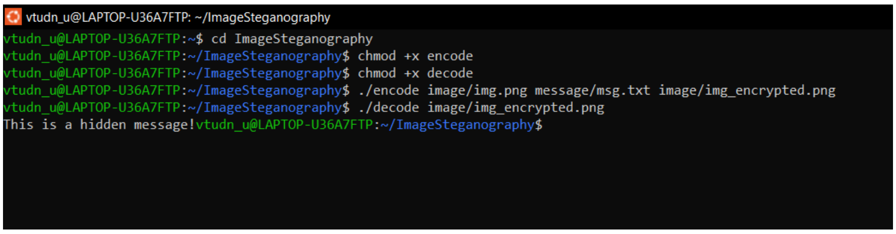

img.png | 1/2 file(s) | 49.95% | 1920 x 1200 px | 120.9 KB | 2022/12/08 21:17:22 (m) - ImageGlass
img_encrypted.png | 2/2 file(s) | 49.84% | 1920 x 1200 px | 707.57 KB | 2022/12/16 23:07:36 (m) - ImageGl...

Figure 8: The output picture.

Finally, let's decode to see the hidden message.



```
vtudn_u@LAPTOP-U36A7FTP: ~/ImageSteganography
vtudn_u@LAPTOP-U36A7FTP:~$ cd ImageSteganography
vtudn_u@LAPTOP-U36A7FTP:~/ImageSteganography$ chmod +x encode
vtudn_u@LAPTOP-U36A7FTP:~/ImageSteganography$ chmod +x decode
vtudn_u@LAPTOP-U36A7FTP:~/ImageSteganography$ ./encode image/img.png message/msg.txt image/img_encrypted.png
vtudn_u@LAPTOP-U36A7FTP:~/ImageSteganography$ ./decode image/img_encrypted.png
This is a hidden message!vtudn_u@LAPTOP-U36A7FTP:~/ImageSteganography$
```

Figure 9: Decrypting.

4 CONCLUSION

4.1 Final words

This project already finished all the assignment's requirements. Source code will be submitted together with this report to the university site.

References

[1] W. Stallings, *Cryptography and network security, principles and practice*, 2020.