LBYEC4A – EK3

Signals, Spectra and Signal Processing Laboratory

Final Project Proposal

A Steganographic Text Encryption and Decryption Application in MATLAB

Rocelle Andrea S. Belandres
Jean Lenard P. Laca
Keane Dwight A. Sulit

PROJECT DESCRIPTION

In the world of technology, data and privacy can often be used against one person especially if the data is personal or private, thus security plays an important role into one's everyday life. It is critical to ensure that everything is protected from hackers and threats as data can be downloaded and manipulated in just one click. With this, the proponents decided to create an application which encrypts and decrypts data using steganography.

The goal of this project is to create a MATLAB application that allows users to encrypt and decrypt text data using steganography. The program lets the user enter a secret message that will be hidden in an image using steganography techniques. The intended application of the project is to provide a secure and covert method for communicating sensitive information using digital images.

The MATLAB application contains several graphical user interface (GUI) components, including a text box for entering the message to be hidden, a text box for displaying the decrypted message, and buttons for loading the image, encrypting the message, and decrypting the encoded image. The encryption algorithm used is a custom steganography algorithm. When encrypting a message, the algorithm hides the message within the image by modifying the least significant bit (LSB) of each pixel value.

The following theoretical concepts must be studied by the proponents and will be utilized in the implementation of the project:

A. Digital Image Processing

Images are represented using dimensions based on the density and number of pixels present. These pixels are the points on the image that takes on a specific code and shade, opacity, and color. These pixels are also the ones being manipulated through image processing.

Image processing is the process wherein the image is transformed into a digital form and processes are performed to it wherein useful data and information are extracted. Image processing treats all images as two-dimensional signals (2D) when applying certain predetermined signal processing methods [1]. Software and applications are widely available to perform this type of manipulation. This may include enhancement, restoration, compression, and recognition.

It is also important to take note of the magnitude and phase of the image as Fourier Transform and its reverse may be applied to enhance the image or restore the image into its original form [1].

B. Steganography

The protection of data is one of the important things to do which is why concealing information within another message or physical object to avoid detection and to protect the user from harm is essential. The process of concealing is called steganography [2]. Most commonly, steganography included encryption within another file format to protect the data or it is processed in such a way that

it is hard to detect. It is often confused with cryptography; however, they are not the same since steganography does not involve scrambling data upon sending or using a key to decode it upon receipt. The term ‘steganography’ comes from the Greek words ‘steganos’ (which means hidden or covered) and ‘graphein’ (which means writing) [2].

C. Least Significant Bit Technique

Steganography works why concealing information that avoids suspicion and one of the most used techniques is called least significant bit (LSB). This involves embedding the secret information in the least significant bits of a media file. In an image file, each pixel is made up of three bytes of data corresponding to the colors red, green, and blue. Some image formats allocate an additional fourth byte to transparency, or ‘alpha’. LSB alters the last bit of each of the bytes to hide one bit of data. The same method can be applied to other digital media, such as audio and video, where data is hidden in parts of the file that result in the least change to the audible or visual output [2].

D. Applications of Steganography

This method is widely used for various applications, including covert communication, copyright protection, and authentication. One of the most significant advantages of steganography is that it can operate without drawing attention to the communication channel, which makes it an attractive option for covert communication in military, intelligence, and criminal contexts. Furthermore, steganography can be used in conjunction with other security measures, such as encryption and digital signatures, to provide an extra layer of protection against unauthorized access and tampering [3].

Steganography has been widely studied in the literature, and many techniques and algorithms have been proposed to improve its performance and security. For instance, a popular approach is based on the Least Significant Bit (LSB) embedding, where the secret message bits are inserted in the least significant bits of the cover media pixels. Other techniques include the use of error-correcting codes, spread-spectrum modulation, and frequency domain transformations. Despite the increasing popularity of steganography, it also raises some ethical and legal concerns, as it can be used for illegal purposes, such as terrorism and cybercrime. Therefore, it is important to regulate the use of steganography and to develop countermeasures to detect and prevent its misuse [3].

E. Rivest-Sharmir-Adleman Algorithm

The Rivest-Shamir-Adleman (RSA) algorithm is a popular public-key encryption algorithm that was created in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is based on the computationally difficult mathematical problem of factoring large integers into their prime factors. RSA encryption uses two keys: a public key for encryption and a private key for decryption. The difficulty of factoring large numbers into their primes, which is considered a difficult problem for classical computers, underpins the security of RSA encryption. Many applications use

RSA encryption, including secure communication protocols, digital signatures, and online banking [4].

METHODOLOGY

The main algorithm used in the methodology is configuration of the LSB to create a visually identical image. The image is first initialized in MATLAB in the RGB color space. In accessing the LSB of the RGB values, this requires converting the RGB values from decimal to 8 – bit binary. Before any modification is performed on the array of RGB values, the message is provided by the user. This message will then be converted to ASCII in terms of binary reshaped into a matrix with the bits generated stored into 1 cell at a time. Moreover, from this message public and private keys will be generated based on the Rivest-Sharmir-Adleman algorithm. These will be verified first before returning the generated keys to the user, if invalid the program generates another set of keys until it is validated and returned. The binary values are then stored into the least significant bit of the RGB values, converted back to 8-bit, and then saved as an image.

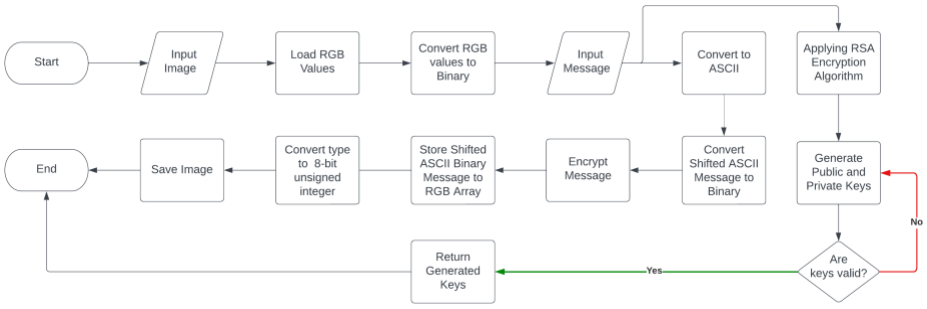

Figure 1. Flowchart of Encryption Method

In decrypting, the user dictates first the private key to be used as a basis for decrypting the message provided after encrypting. The image is first initialized in MATLAB in the RGB color space. The RGB values from decimal to 8 – bit binary and the LSB of the RGB values are stored into MATLAB. Every 8 LSBs are combined to create an 8 – bit binary number and converted to decimal for decrypting the messaged based on the key provided by the user.

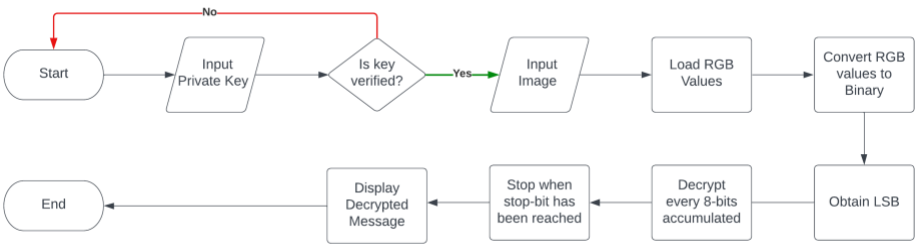

Figure 2. Flowchart of Decryption Method

SCHEDULE OF ACTIVITIES

The activities are divided into 4 stages, namely Phase 1: Project Proposal, Phase 2: Final Project Proposal, Phase 3: Project Review, and Phase 4: Presentation.

Phase 1 includes the brainstorming of ideas and proposal of topics that would be feasible to be the executed as a project.

Activity	Feb 27	Feb 28	Mar 1	Mar 2	Mar 3	Mar 4	Mar 5	Mar 6	Mar 7	Mar 8	Mar 9	Mar 10	Mar 11	Mar 12	Mar 13	Mar 14
Creation of Links (Trello and GitHub)																
Brainstorming																
Proposal																
Presentation																

Phase 2 includes the final proposal paper, the research and creation of prototypes that is deemed essential to the creation of the project. This phase also includes the finalization of process to be implemented.

Activity (March)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Research																											
Prototyping																											
GUI and design																											
Added Features																											
Finalization of Final Proposal																											

Phase 3 includes the review and improvements that will be made throughout the project. Research should be an ongoing process as this will be about solving bugs and finalization of the project.

Activity (March)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Research																														
Improvements																														
Review Files																														
Updating databases and Progress																														

Activity (April)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Research															
Improvements															
Review Files															
Updating databases and Progress															

Lastly, Phase 4 includes the finalization and recording of the simulation. This will also cover the creation of final paper, the recording of the presentation itself, and the submission of the project.

Activity (April)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Finalization																		
Creation of Presentation																		
Recording																		
Presentation																		
Submission																		

REFERENCES

[1] Simplilearn, "What Is Image Processing : Overview, Applications, Benefits, and More," *Simplilearn.com*, Apr. 29, 2021. Available: https://www.simplilearn.com/image-processing-article. [Accessed Mar. 14, 2023].

[2] Kaspersky, "What is steganography? Definition and explanation," *www.kaspersky.com*, Feb. 10, 2023. https://www.kaspersky.com/resource-center/definitions/what-is-steganography. [Accessed Mar. 14, 2023].

[3] R. Doshi, P. Jain, L. Gupta, "Steganography and Its Applications in Security," *IJMER. International Journal of Modern Engineering Research,* vol. 2, no. 6, pp. 4634-4638. [Online]. Available: http://www.ijmer.com/papers/Vol2_Issue6/EN2646344638.pdf. [Accessed Mar. 14, 2023].

[4] GeeksForGeeks, "RSA Algorithm in Cryptography," *GeeksforGeeks*, Apr. 22, 2017. https://www.geeksforgeeks.org/rsa-algorithm-cryptography/. [Accessed Mar. 14, 2023].