Presented to the Department of Electronics and Computer Engineering
De La Salle University - Manila
Term 2, A.Y. 2022-2023

In partial fulfillment
of the course Signals, Spectra and Signal Processing Laboratory
In LBYEC4A-EK2

A Steganographic Text Encryption and Decryption Application in MATLAB

BELANDRES, Rocelle Andrea S.
LACA, Jean Lenard
SULIT, Keane Dwight A.

Submitted to:
Ruiz, Ramon Stephen

Submitted on:
April 18, 2023

Abstract

Privacy and security have been a big issue in the 21st century given the advancements of the society's technology. With this it has been a priority that the users will be ensured that their data and information will be kept private and safe from the anomalies that will try to use it against them. Thus, the proponents got the inspiration of the project from digital image processing wherein the image is altered to hide messages. The process is called steganography which uses least significant bit to manipulate the object, the image in this instance, to hide and encrypt the message which can only be decrypt using the same key used in the encryption process. The proponents decided to also utilize a log in and registration process wherein the keys are different for each user. The system uses Message Digest Algorithm Hashing, also known as MD5, to create a username and password system. The credentials are used as a key and save in a text file. Moreover, the application is only compatible with MATLAB, can load certain types of images, and has a limited text length which will depend on the image size. Further study and improvements on this application is advised before it can be commercially available.

I. Introduction

Today, privacy and security are one of the top priorities in ensuring the welfare of the users. The methods in which the one's information is accessed and used against the person is evolving with how the technology is evolving, thus the level of security is also required to evolve and improve. 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.

Steganography is a form of data protection in which information and data is concealed within another form of data or physical object to avoid detection and data breaching [1]. 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) [1].

With this, the proponents have decided 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 objective specifically aims:

- To be able to be proficient in using MATLAB and to apply the concepts of signal processing from the lecture and laboratory exercises.
- To create a user interface wherein the user will be able to encrypt and decrypt the message.
- To create registration process using MD5 Hashing wherein the encryption key is unique to every user.

II. Theoretical Consideration

The project is inspired with the security systems found online and the topic of cryptography thus the concepts of digital image processing and the surrounding ideas on the manipulation of such variable into security application will used. Furthermore, a log in system will be implement in such that each user will have a uniquely different key when encrypting and decrypting their messages. With this, the proponents deem it vital to have the concept stated below as a precursor to the project:

i. 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 [2]. 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 [2].

ii. Steganography

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 [1] [3]. 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].

iii. Least significant bit

Steganography works why concealing information that avoids suspicion and one of the most used techniques is called least significant bit (LSB) [1]. 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 [1][3].

iv. Message Digest Algorithm Hashing

Message Digest Algorithm (MD5) is a cryptographic protocol that is used for authenticating messages and content verification [4]. Message digests, also known as hash functions, are one-way functions; they accept a message of any size as input and produce as output a fixed-length message digest. MD5 is the third message-digest algorithm Rivest created. MD2, MD4 and MD5 have similar structures, but MD2 was optimized for 8-bit machines, in comparison with the two later algorithms, which are designed for 32-bit machines. The MD5 algorithm is an extension of MD4, which the critical review found to be fast but potentially insecure. In comparison, MD5 is not quite as fast as the MD4 algorithm but offered much more assurance of data security. Ronald Rivest, founder of RSA Data Security LLC and professor at Massachusetts Institute of Technology, designed MD5 in 1991 as an improvement to a prior message-digest algorithm, MD4 [4].

v. Graphical User Interface

As the name suggests, graphic user interface or GUI, is a form of interface that allows the user to interact with the electronic device or window through graphical icons and menus [5]. Each icon manages a specific task with regards to the interaction with the system. Its goal is to let the user decide on how the task is to be executed while limiting the purpose of each interface [5].

III. Methodology and Project Overview

The project was created and performed using Matrix Laboratory (MATLAB) 2022b/2023a. The application can be used to hide text messages in images and can also be used to extract hidden text messages from images. The main algorithm used in the project is described using a flowchart (see Figure 3.1) wherein the application is unique to a specific user, as it uses MD5 hashing to hash the user's credentials as a key to encrypt and decrypt the text. 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. 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.

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. Further discussion will be provided in the succeeding sections.

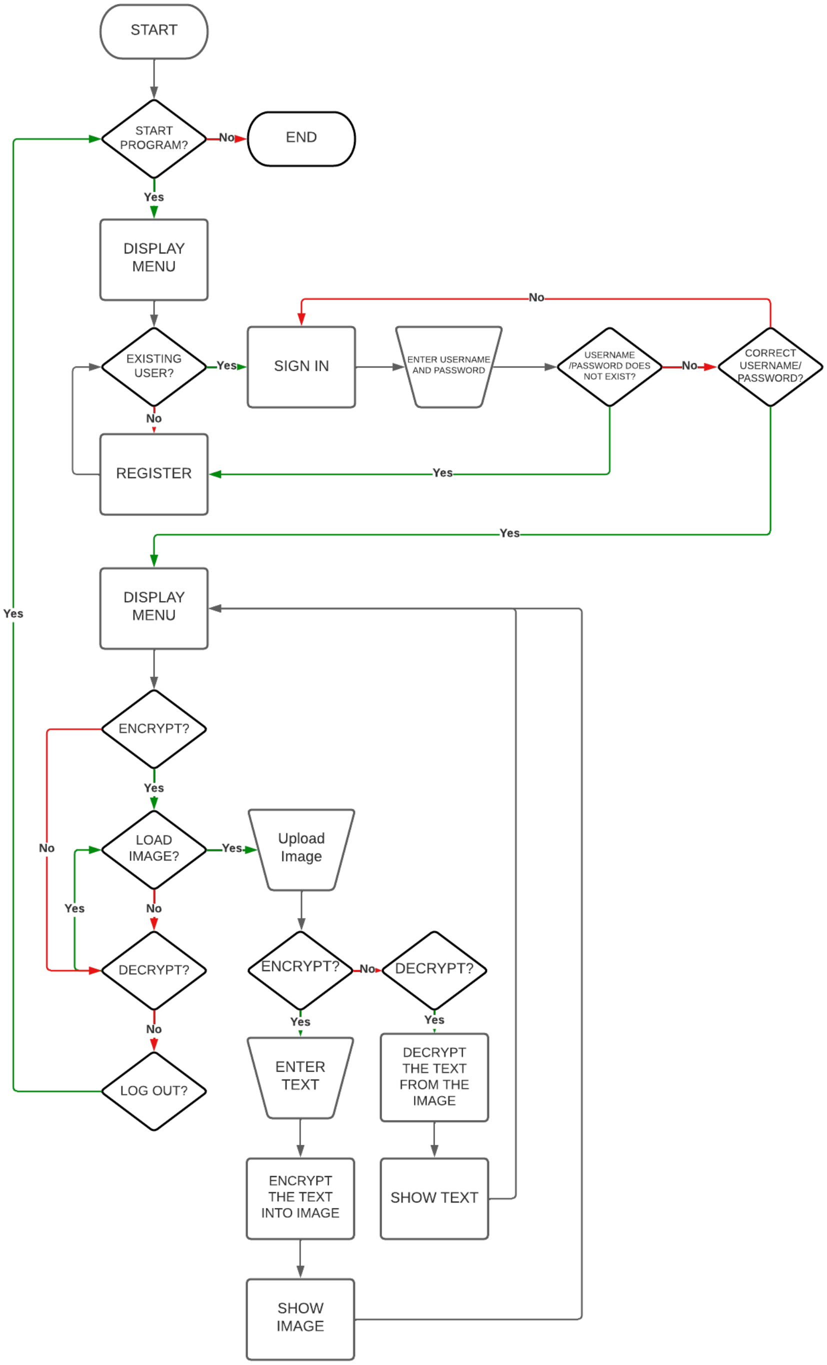


Figure 3.1 Flowchart of the Steganography Application

IV. Results

As described by the flowchart, there will be a log in/registration is utilized and will start the whole system. The system is run by the main.m script, which its input will be the login credentials of the user. The process blocks can branch out into two. The output of the main is the main steganography application. Basically, it serves as a security measure on the application's accessibility. Figure 4.1 shows the login menu and registration page.

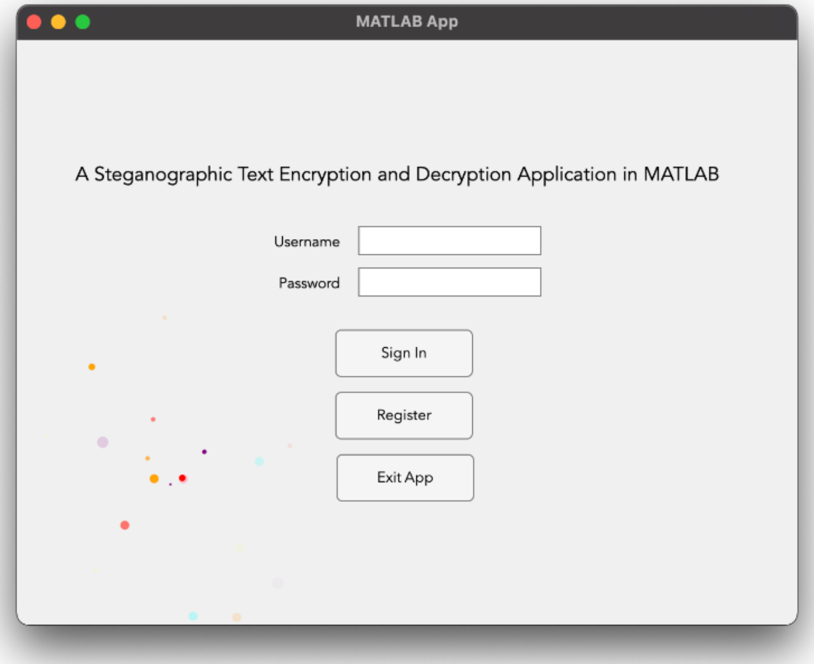
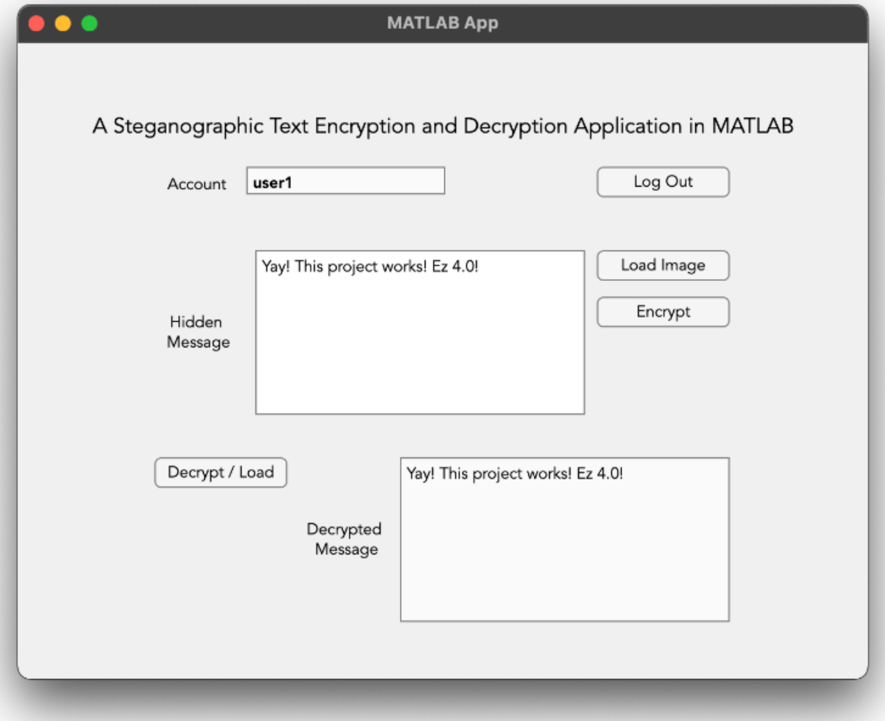

A Steganographic Text Encryption and Decryption Application in MATLAB

Figure 4.1 Log in Menu System

Found in Figure 4.2 is the user interface when the use successfully registered or logged in. The use has the ability to encrypt a message into an image or decrypt the message from the image loaded. As said in the sections beforehand, each user has a unique key code which is based on the user's credentials which is inputted into the registration menu.

Moreover, the length of the allowable message is based on the loaded image size. Exceeding the limit will immediately show and error in terms of encrypting the message while loading the wrong image will show an error message. Furthermore, the system will only show if the image that is being decrypted matches the key each user has and if the image indeed has a message.



A Steganographic Text Encryption and Decryption Application in MATLAB

Account: user1

Hidden Message: Yay! This project works! Ez 4.0!

Decrypted Message: Yay! This project works! Ez 4.0!

Figure 4.2 Encryption and Decryption Menu

The user also can log out of the system which will direct to the log in menu and once again asked for a new registration or a new account log in. As seen in Figure 4.1, the user also has the option to exit the application for good.

V. Discussion

It is important to take note that MATLAB is based on Python and C language which has the advantage in utilizing the external data set and analyzing them into what the proponents plan to do. With this, the creation of GUI is easier as compared to how it will be done if it is purely code based and without the help of extensions. With this, the codes must be discussed to fully understand the application.

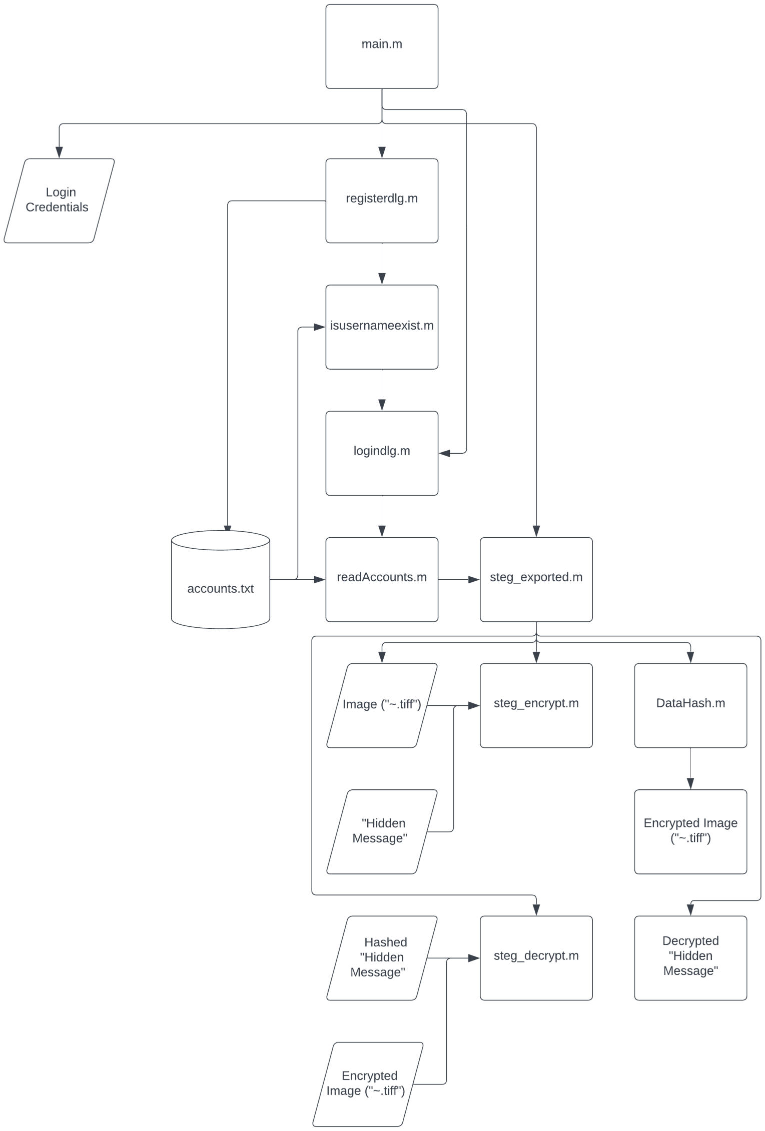


Figure 5.1 Hierarchy Chart of the Application based on the Files in the Repository

As stated in the sections, the processes are described in the flowchart from Figure 3.1, thus the files used will be discussed. To start off, the registerdlg.m takes into consideration the database of accounts, `accounts.txt`. The processes involved here is to check if the username exist. The output of the `registerdlg.m` is to proceed into the `logindlg.m` which is the other process of the main application. The `logindlg.m` proceeds to read the user credentials and pass it into the `readAccounts.m` function, which outputs whether the user is authenticated to access the steganography application. For the steganography application, `steg_exported.m`, branches out into two different processes which is steg_encrypt.m and steg_exported.m.

The first one, involves the `steg_encrypt.m` function. This function has the following inputs — the image, and the hidden message. When these are both satisfied, it would proceed into hashing the user data by MD5 hashing, and later on encrypts the text inside the least significant bit of the image. The second process of `steg_exported.m` is the `steg_decrypt.m` function. This takes into consideration the hashed hidden message and the encrypted image. If the hashed information matches to the user's data, it then proceeds to decrypt the hidden message.

VI. Conclusion and Recommendation

As discussed in the sections beforehand, the application was able to handle the encryption and decryption of text using steganography. The login and registration page works as the proponents hoped it to be, and provides a unique key for every user registration, while the main program encrypts and decrypts the message as how it was tasked to do. Overall, the proponents were able to use the concepts and lectures from the subject and was able to make use of MATLAB upon the creation of the application. Furthermore, the application provided seamless graphic user interface in where the user can interact with the program.

Due to the lack of time, it is recommended that the future developers and researchers perform and more in dept study and improvement of the bugs found in the said application. It is also recommended to improve on the user registration and login system where in the user is able to change their password in case they forgot their password, to delete the past encryptions, and to delete their account entirely. It is also recommended that the future developers improve the GUI even more as the application uses the default dialog boxes.

VII. Authors' Contributions

Belandres – Flow Chart, Abstract, Introduction, Theoretical Considerations, Results, Conclusion, and Poster

Laca - Hierarchy Chart, Methodology, Recommendations, and Code Proper

Sulit - Hierarchy Chart, Discussion, Recommendations, and Code Proper

VIII. References

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

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

[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.

[4] “Definition of GUI (Graphical User Interface) - Gartner Information Technology Glossary,” Gartner. https://www.gartner.com/en/information-technology/glossary/gui-graphical-user-interface#:~:text=A%20graphics%2Dbased%20operating%20system

[5] “What is MD5 (MD5 Message-Digest Algorithm)?,” SearchSecurity. https://www.techtarget.com/searchsecurity/definition/MD5