National College of Ireland

Using cryptography and image steganography to securely transfer data. (REPORT)

MSc Research Project
M. Sc. In Cybersecurity

Yash Lathigara
Student ID: 20182384

School of Computing
National College of Ireland

Supervisor: Professor Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Yash Mahesh Lathigara		
Student ID:	20182384		
Programme:	M. Sc. In Cybersecurity	**Year:**	2021
Module:	M. Sc. Research Projects		
Supervisor:	Professor Imran Khan		
Submission Due Date:	16th December 2021		
Project Title:	Using cryptography and image steganography to securely transfer data.		
Word Count:	4422	**Page Count:**	18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Yash Lathigara

Date: 15th December 2021

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Using cryptography and image steganography to securely transfer data.

Yash Lathigara
20182384

Abstract

When Computer apps were built to deal with financial and personal information, the need for security grew. Data on PCs is a very important aspect of front-line life. Today, security is so important that we must safely transfer information from one location to another. There is a big hacker and spire on the other side of the heavy security. Cryptography is one of the concepts that is concerned with security and plays a significant role in today's secure communication environment. However, the difficulty with cryptography is that an intruder will be aware that the data is encrypted and may attempt to decrypt it using a specific set of keys.

One of the reasons attackers are so effective is that most of the data they hack or extract from a system is in a format that they can read, update, and change. Intruders may disclose the information to others, modify it to misrepresent an individual or organization, or use it to conduct an attack. The use of steganography is one solution to this problem.

1 Introduction

CRYPTOGRAPHY:

Cryptography, often known as cryptology, is a term derived from the ancient Greek word kryptos, which meaning "hidden secrets." It is the act of researching strategies for secure communication in the presence of third parties such as users, intruders, or hackers. Cryptography, in general, is the act of modelling and evaluating procedures that prohibit third parties or people from accessing private messages. It deals with different areas of information security, such as data confidentiality, integrity, authentication, and non-repudiation. Nowadays, cryptography is utilized in a wide range of applications, including electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communication.

Cryptography employs a collection of techniques known as cryptographic algorithms, or ciphers, that execute data encryption and decryption to secure communications between two parties who may be utilizing computers, devices such as smartphones, and applications. One algorithm is used for encryption, another for message authentication, and still another for key exchange in a cipher system.

TYPES OF CRYPTOGRAPHY:

- Single-key cryptosystem or symmetric-key cryptosystem algorithms that use just one key for encryption and decryption.
- Public-key cryptography, also known as asymmetric-key cryptography, is a type of method that employs two keys: public and private.

- Hash Functions: A mathematical change is used to irrevocably "encrypt" information, allowing for digital authentication. It is one method for ensuring the data's integrity.

THE FOLLOWING ARE THE PRIMARY FUNCTIONS OF CRYPTOGRAPHY THAT ARE CURRENTLY IN USE:

- For Secrecy: Ensuring that the message being sent cannot be viewed by anybody other than the intended recipient.
- Authentication: One method of authenticating or verifying a user's identity.
- Integrity: Assuring the recipient that the received communication has not been tampered with in any manner from the original.
- Non-repudiation: A mechanism that confirms the sender is the person who transmitted the communication.
- Key exchange: The technique through which sender and recipient share crypto/secret keys.

I begin with the decoded information, also known as plaintext. Plaintext is jumbled into ciphertext, which is then decoded back into readable plaintext. The sort of cryptography strategy used, and the type of key used determine the encryption and decryption. For those who enjoy equations, this technique is sometimes written as:

Ciphertext, C = Ek(P)
Plaintext, P = Dk(C)

Where P represents plaintext, C represents ciphertext, E represents the encryption approach, D represents the decryption method, and k represents the key.

SECRET KEY OR SYMMETRIC CRYPTOGRAPHY:

Symmetric key cryptography employs a single/single key for both encryption and decoding. As shown in Figure below, the sender encodes the plaintext and transmits the cipher text to the collector. To decode the message and recover the plaintext, the collector employs a similar key. Because a single key is used for both functions, mystery key cryptography is also known as symmetric encryption.

With this sort of encryption, the key must plainly be known to both the sender and the receiver; this, in fact, is the mystery. Obviously, the most difficult aspect of this process is the transmission of essential information (more on that later in the dialog of open key cryptography). Symmetric key cryptography schemes are often classified as either stream ciphers or block ciphers.

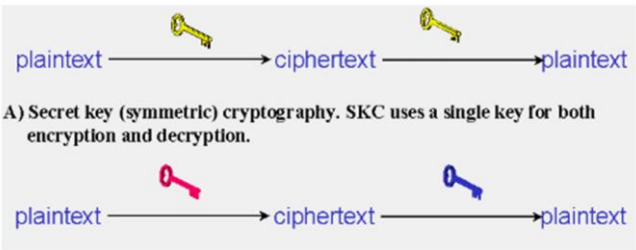

FIGURE 1: SYMMETRIC CRYPTOGRAPHY WORKING.

STEGANOGRAPHY:

Steganography is a Greek term that meaning "hidden composition." The term steganos refers to a safe and graphical method of data composition. As a result, steganography is more than simply the art of concealing information; it is also the art of concealing the true presence of transmission of secret information.

Steganography primarily conceals the mysterious information in another sort of data and transports it via a media such that only the receiver is aware of the message's presence. Previously, information was safeguarded by concealing it on the back of wax, composition tables, the stomachs of rabbits, or the scalps of slaves. However, the majority of people today communicate information like content, photos, video, and sound via the medium. To securely transmit secret information, visual and auditory items such as music, video, and photographs are used as a variety of sources to disguise the content.

The exploration of undetectable communication is referred to as steganography. Steganography generally deals with ways for disguising the presence of communicated information in order to keep it secret. It maintains secrecy between two imparting parties. Picture steganography conceals information by inserting it into a distributed picture and creating a stego-picture. There are several types of steganography systems, each with its own set of advantages and disadvantages. In this research, I employed an LSB-based steganography approach with a stego key to hide data.

PROJECT OBJECTIVE:

The goal of this project is to encrypt the data first and then hide a secret message behind a cover-media-like picture in such a manner that the presence of the hidden message is not suspected and safe data transmission between the two parties is achieved. In layman's terms, "this project will execute encryption and data concealment within an image, therefore protecting the presence of secret data."

PROJECT SOCPE/NEED:

The project's purpose is to prevent unwanted access and improve security during message delivery. To achieve the criteria, I employ a simple and straightforward technique of cryptography and steganography. In this research, the suggested technique identifies the best algorithm for encrypting and embedding data in a picture combining cryptography and steganography, resulting in a superior security pattern for transferring messages over a network.

The Java framework is used to realistically implement the functions of the discussed algorithms.

2 Related Work

Cryptography is used to ensure the privacy and integrity of messages. Encryption, decoding, and cryptographic hashing are some of the most important functions of cryptography. The sender and receiver must exchange a secret key to secure a communication using encryption and decryption. This key is used by both the sender and the recipient to encrypt and decode messages. This can be done on a pre-existing message, such as an email, or on a communications stream, such as a TCP/IP connection. Cryptographic hashing is a method for generating a fixed-length string from a variable-length message. If the sender includes a cryptographic hash with the message, the receiver can validate its authenticity. Cryptography is built on complicated scientific correlations and forms. Let's look at the common cryptography benchmarks (ccs) that are used to protect computer communications and how they may be used.

The three basic forms of cryptography are symmetric key, asymmetric (public) key systems, and cryptographic hash capabilities, which are widely used. Typically, the length of the key is directly connected to the quality of a crypto system. This assumes that there is no inherent flaw in the computation and that the keys are picked in a fashion that fully utilizes the key space (the number of conceivable keys) . The transactions will be extremely safe if we use public algorithms with no known weaknesses, use reasonable key lengths, and use excellent keys.

Cryptographic Technique Types:

1) Compact Key in Symmetric-Key Encryption:

An encryption algorithm [2] that was first designed for sending many keys in a broadcast situation.

2) Compact Key in Identification-Based Encryption (IBE):

IBE [3][4] is a sort of public-key encryption in which a user's public-key can be configured as the user's identity string. In IBE, there is a trusted party known as the private key generator, which possesses a master-secret key and gives a secret key to each user based on the user's identification. To encrypt a communication, the user encrypting the data can utilize the user's public data and a user identification. This encrypted data may be decrypted by the receiver using his secret key.

3) ABE (attribute-based encryption):

ABE [5] allows each ciphertext to be associated with an attribute, from which the master-secret key holder can extract a secret key for a policy of these attributes, such that encrypted data, i.e., ciphertext, can be decrypted by this key if its connected attribute complies to the policy.

4) proxy re-encryption (PRE):

A handy basic for delegating the decryption capability of some ciphertexts without passing the secret key to the delegate is proxy re-encryption (PRE)[6]. A PRE plan allows the

sender to delegate to the server (intermediary) the ability to convert ciphertexts encrypted under her open key into ones for the receiver.

Drawbacks of Cryptography:

Aside from the four key components of data security, there are other aspects that impact data use success:

- A securely encrypted, true, and precisely tagged material might be tough to access for a genuine user during a critical decision-making period. An intruder can attack the network or the computer framework and render it inoperable.
- High accessibility, one of the fundamental aspects of data security, cannot be ensured using encryption. Other techniques are necessary to guard against threats such as rejection of benefit or total collapse of data framework.
- Another basic requirement of data security of specific get to control cannot be met using cryptography. Regulatory controls and mechanisms must be developed for the same.
- Cryptography does not defend against the weaknesses and risks that arise because of a haphazard design of frameworks, protocols, and methodologies. These must be resolved by careful planning and the establishment of a solid basis.
- Cryptography is not free. The cost is measured in terms of both time and money. Expansion of cryptographic techniques during data preparation causes delays. The use of open key cryptography necessitates the establishment and funding of an open key foundation, which necessitates a nice-looking financial budget.
- The cryptographic procedure's security is dependent on the computational difficulty of numerical problems. Any advancement in addressing such scientific concerns or growing computing control might leave a cryptographic process vulnerable.

Steganography:

The goal of steganography is to conceal data in cover information in such a way that non-participants are unable to recognize the secret message behind the data. Unlike watermarking, steganography is not meant to prevent opponents from deleting or modifying the secret message that is contained in the cover data, but rather to keep it invisible. Steganography is especially appealing for applications where encryption cannot be utilized to protect the transmission of secret information.

LSB based Steganography:

Pixels are large enough to store one message byte. The rest of the pixels' bits stay unchanged. Steganography is the art and science of communicating in such a way that the presence of the message is concealed. It is the art of communicating invisibly by masking data inside other information. Steganography is taken from Greek and literally means "secured writing." A Steganography system is made up of three components: the cover image (which conceals the secret message), the secret message, and the Steganography image (which is the cover object with the message inserted inside it).

A digital image is characterized by a 2-D network of colour within each grid point (i.e., pixel). Grayscale images typically use 8 bits, whereas coloured images use 24 bits to define

the colour model, such as the RGB model. There are numerous techniques to conceal data inside the cover-image in the Steganography system, which employs a picture as the cover. To implant the mysterious information, techniques regulate the cover-image pixel bit values. The secret bits are directly added to the pixel bytes of the cover image. As a result, spatial domain approaches are basic and straightforward to execute. The Least Significant Bit (LSB) is one of the most often used techniques in spatial domain image Steganography. It takes use of the fact that the degree of accuracy in many image groups is far more than that perceivable by typical human eyesight. As a result, a changed image with minor colour alterations will be unrecognizable from the original simply by glancing at it. In the traditional LSB method, eight bytes of pixels are required to store one byte of mysterious information.

3 Research Methodology

Every computer in a Connected network may function as both a client and a server at the same time. Although today's linked networks have a variety of advantages in terms of efficiency and fault-tolerance, there are extra security dangers. Security and preventative measures should be implemented to protect against any potential leaking of sensitive data and security breaches. One of the reasons intruders/hackers are effective is that the majority of the information they obtain from a system is in a format that they can read and interpret. Even if the data is encrypted, intruders will readily get it and may attempt to decode it using mechanisms such as the brute force approach, and may even be successful in doing so, revealing the information to others. One answer to this problem is to employ the recommended strategy. The presented project model investigates the use of steganography and cryptography methods for safe data exchange in any network.

The project is divided into three major processes:

1) Encryption of data to be transferred using the AES Cryptography method.
2) Use of an image-based steganography method to embed secret data into a cover picture, resulting in a steganography image that may be conveyed to the destination party.
3) The destination party or receiver will get the steganography picture and will first execute steganography decoding to obtain encrypted data from the image, followed by AES decryption to obtain the original message.

4 Design Specification

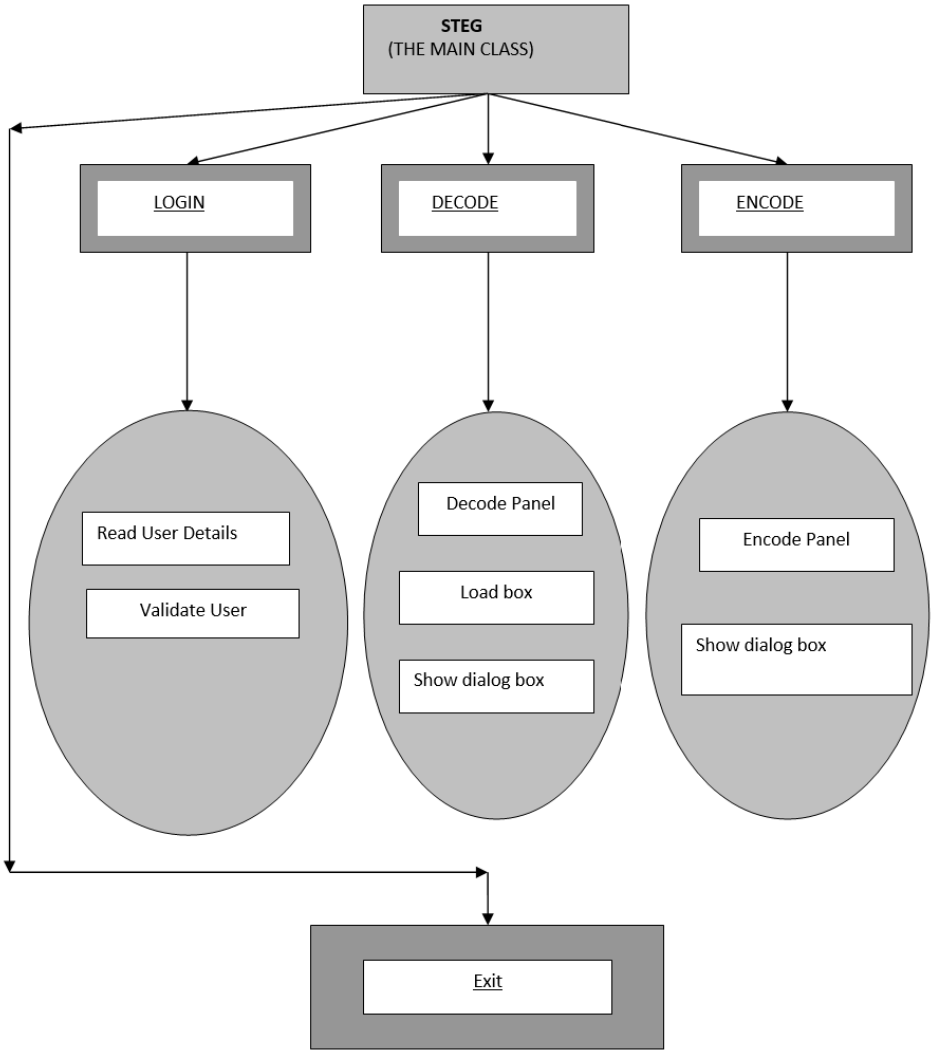

FIGURE 2: SYSTEM DESIGN

FUNCTIONAL REQUIREMENTS:

Functional requirements are those that primarily define the system's behaviour or functionalities.

- Login: To validate the user's authentication by confirming the username and password.
- Secret Message: This is the sender's sensitive message that must be safely conveyed.
- Cryptography Key: A secret key known only to both communication parties that will be used in the encryption and decryption of secret material to produce cipher text using cryptography.
- Cover Picture: The sender will choose an image in which the ciphertext will be buried.
- Steganography Key: A steganography key that is known by both communication parties and is utilized in the execution of steganography LSB. Steganography

Encryption with LSB is done on a cover picture to conceal a secret text message (cipher text) by changing bits of the cover image with message bits.

- Sender: In this case, the sender will transmit the steganography picture file to the designated recipient with whom he wishes to speak.
- Receiver: This receiver gets the steganography picture and opens it in decryption mode to obtain the ciphertext contained inside it.

NON-FUNCTIONAL REQUIREMENT:

- Safety Requirements: Communicating parties must ensure that they use the same software to encrypt and decode data included inside an image. Both must ensure the software's secrecy.
- Requirements for security: Only the sender and recipient should be aware of the encrypted picture file. The user should not expose any information about the sent image or the receiver's data.
- Software Quality Attributes: The product's quality is maintained such that a single sender and collector may communicate through image. There is no way of knowing the mystery image.

SYSTEM DESIGN:

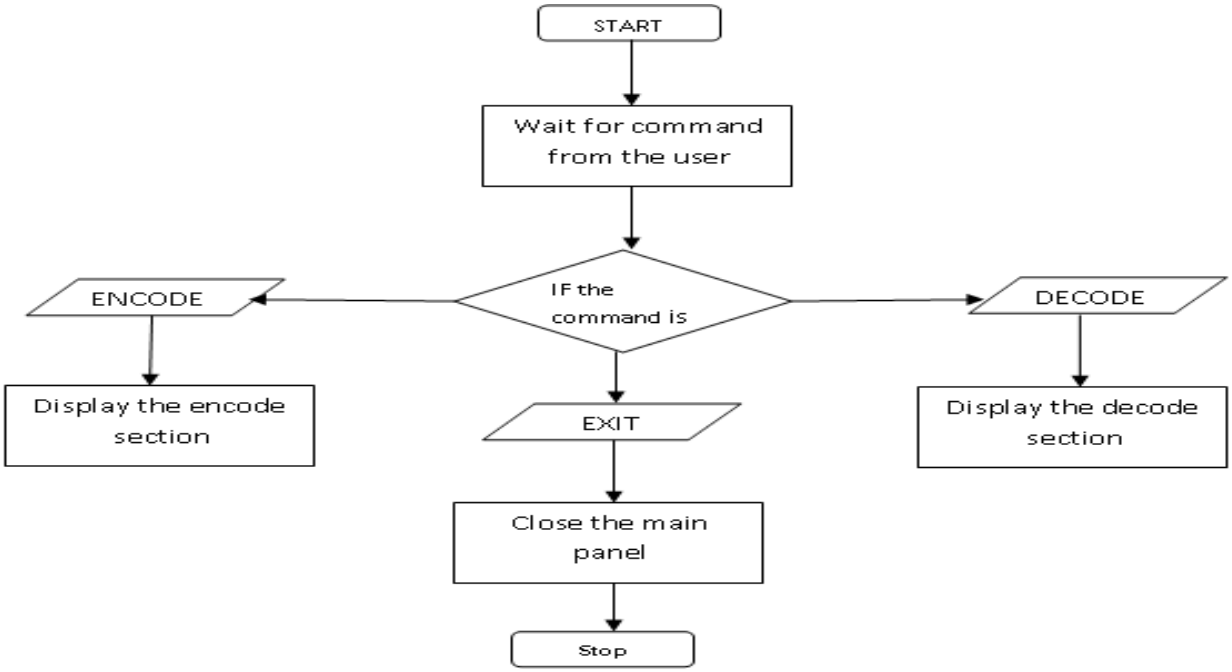

FIGURE 3: MAIN INTERFACE DIAGRAM

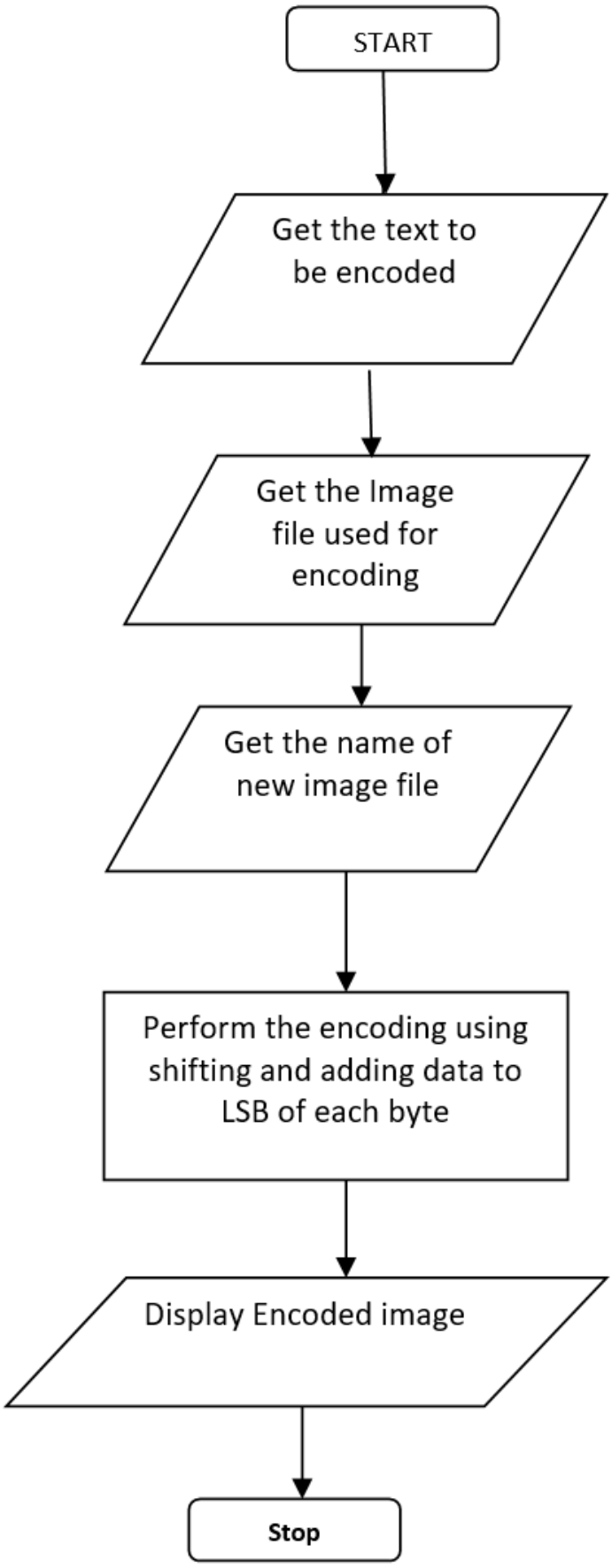

FIGURE 4: ENCRYPTION PROCESS

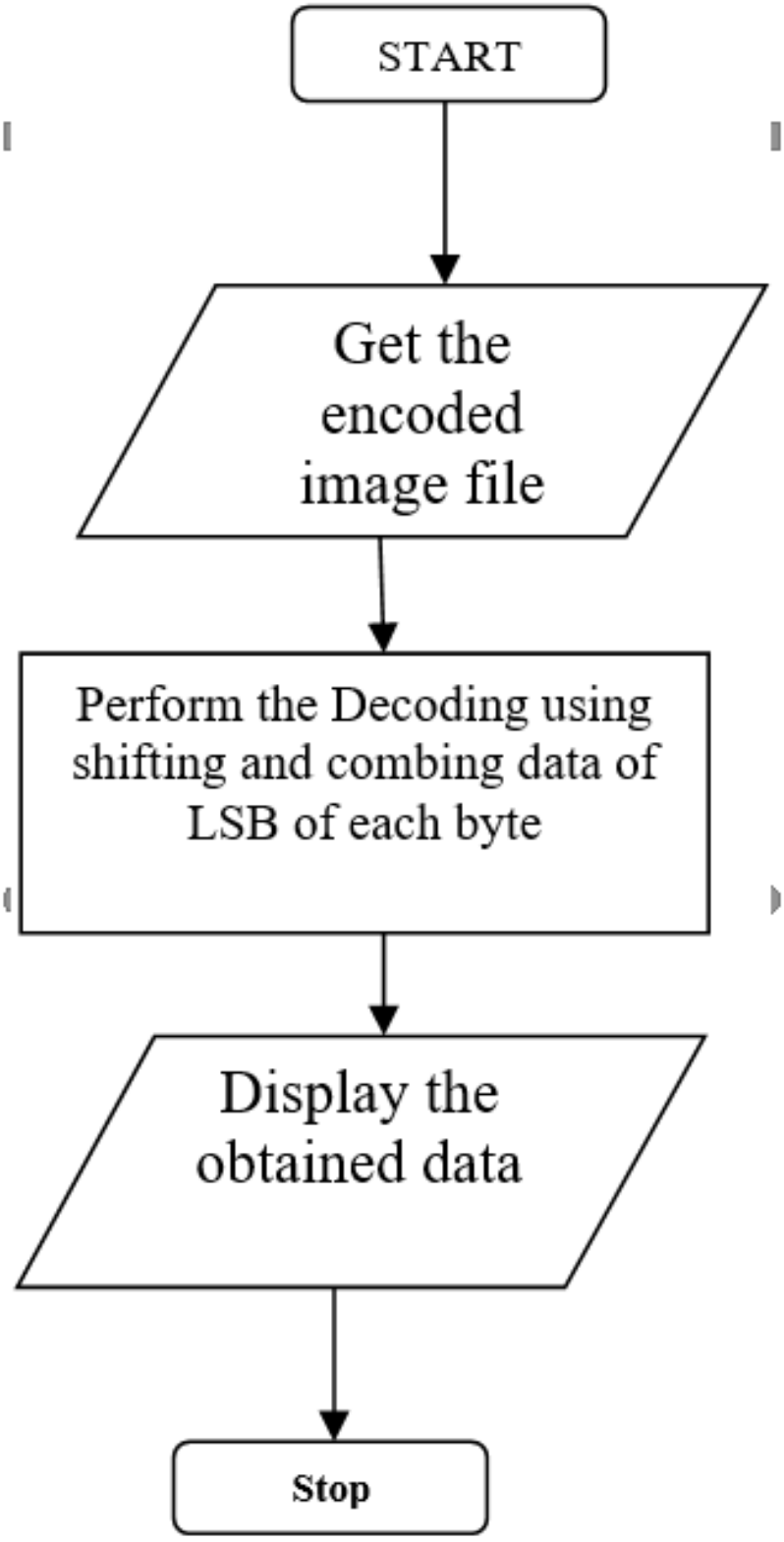

FIGURE 5: DECRYPTION PROCESS

FIGURE 6: SOFTWARE UI (LOGIN PAGE)

Step 1: The user will be prompted to provide a login detail. If the user's credentials are correct, the system authenticates the user.

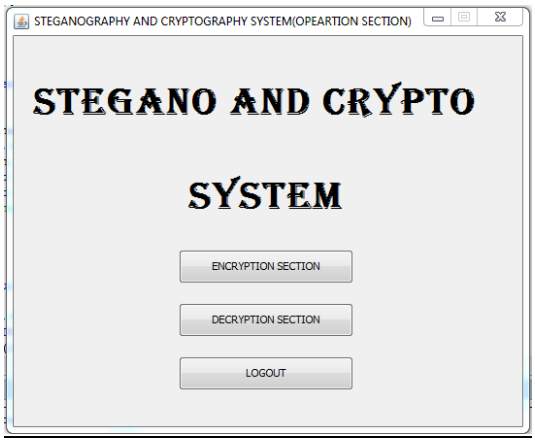

FIGURE 7: SOFTWARE UI (OPREATION SELECTION PAGE)

Step 2: Once the user has been verified, he will be led to the options where he may choose to encryption, decryption, or logout options.

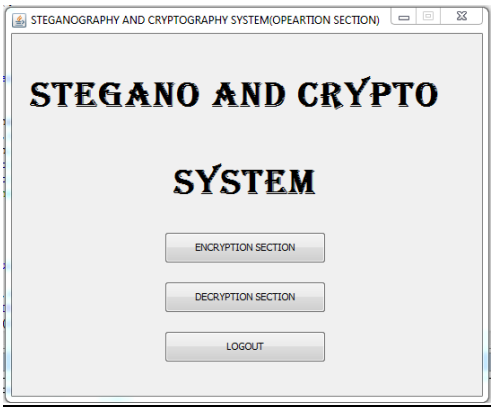

FIGURE 8: SOFTWARE UI (OPERATION SELECTION PAGE)

Step 3: The above image depicts the system's encryption part, where the user may enter information such as a secret message and other details to make a stego image.

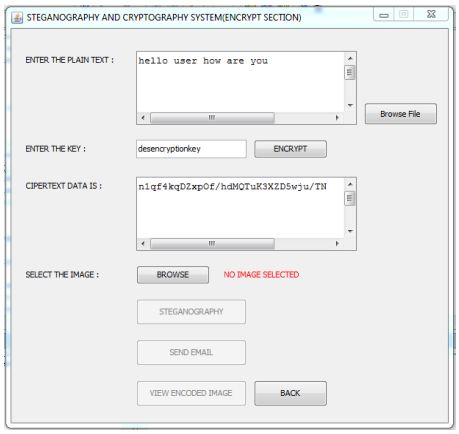

FIGURE 9: SOFTWARE UI (ENCRYPTION PAGE)

Step 4: In the above image, the user is in the encryption area, where he entered the data to be concealed as well as the AES secret key and executed AES encryption, the result of which is shown in the second picture.

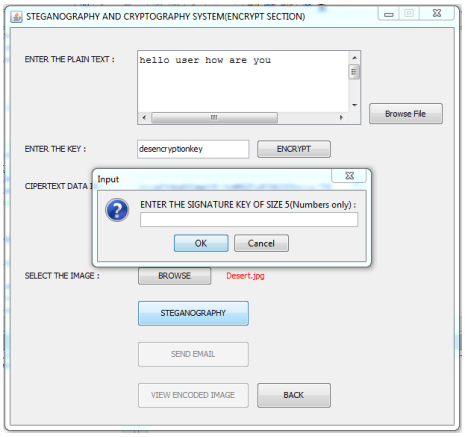

FIGURE 10: SOFTWARE UI (AES KEY PAGE)

Step 5: The above image presents a scenario where sender/user is asked for a stegokey to perform steganography encryption.

FIGURE 11: SOFTWARE UI (ENCRYPTION PREVIEW)

Step 6: The final output.

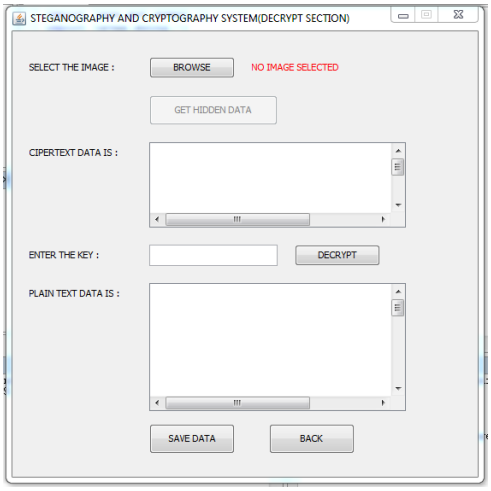

FIGURE 12: SOFTWARE UI (DECRYPTION PAGE)

Step 7: Decryption section.

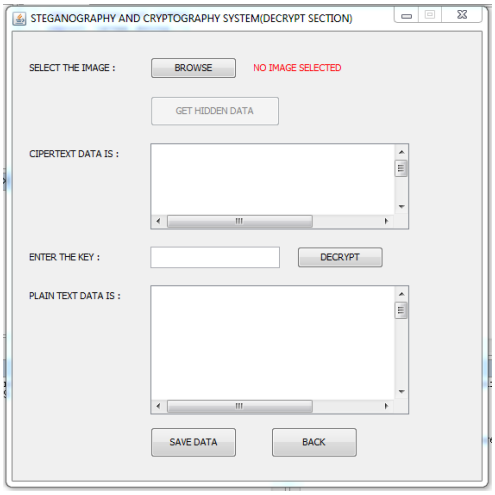

FIGURE 13: SOFTWARE UI (DECRYPTION PAGE)

Step 8: The above graphic depicts a situation in which the receiver picks the stegoimage supplied by the sender, enters the stegokey to obtain cipher data, and then enters the AES secret key to obtain the secret data hidden by the sender.

5 Implementation

System Implementation:

The project is divided into five major modules.

1. Plaintext encryption with the Cryptography AES algorithm.
2. The steganography section, which performs steganography analysis on a certain picture.
3. Encode portion, which does real data and picture encoding.
4. The decode part, which decodes the data from the picture.
5. The main panel, which contains all the preceding three parts.

For encryption and decryption, I have utilized AES algorithms and for steganography I have utilized LSB algorithm.

Following that, the following lines offer a simple and brief description of the steganography technique employed in this project:

Stegoimage = Cover image + Encrypted Data to be Hidden + Stegokey

The cover picture in this instance refers to the file in which we will hide the encrypted data, which may also be encrypted with the stegokey. The resulting file is called the stegoimage. I'll concentrate on picture files, thus I'll use the cover image and stegoimage.

Technical details of the incorporated algorithms is in the configuration manual.

Class diagram:

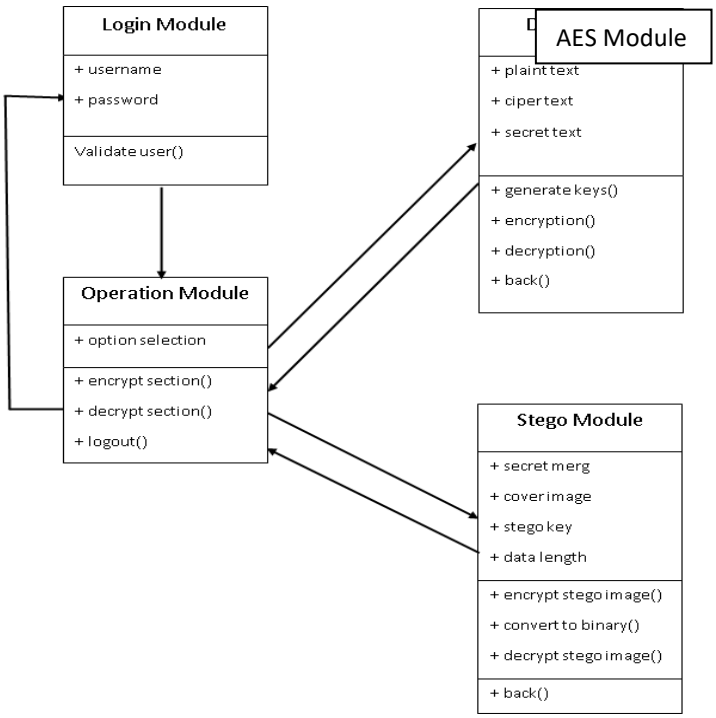

FIGURE 14: CLASS DIAGRAM

There are four major types:

1. Login Module: It has two characteristics, username and password, as well as one operation, validate user. It handles user authentication.

2. Operation Module: It offers one user attribute choice that allows the user to go to a specified portion of the software.

3. AES Module: It consists primarily of three attributes: plaintext, cipertext, and secret key, as well as three important operations: random key generation, AES encryption, and AES decryption. It is in charge of all AES implementation.

4. Stego Module: It is made up of five attributes: stegokey, cipertext, stegoimage, and message length, as well as four fundamental actions. createStegoImage makes a stego image, decryptStegoImage retrieves ciperdata from the image, convertToBinary does binary conversion, and back function returns the user to the operation area. It is in charge of all Steganography implementation.

Data Flow Diagram:

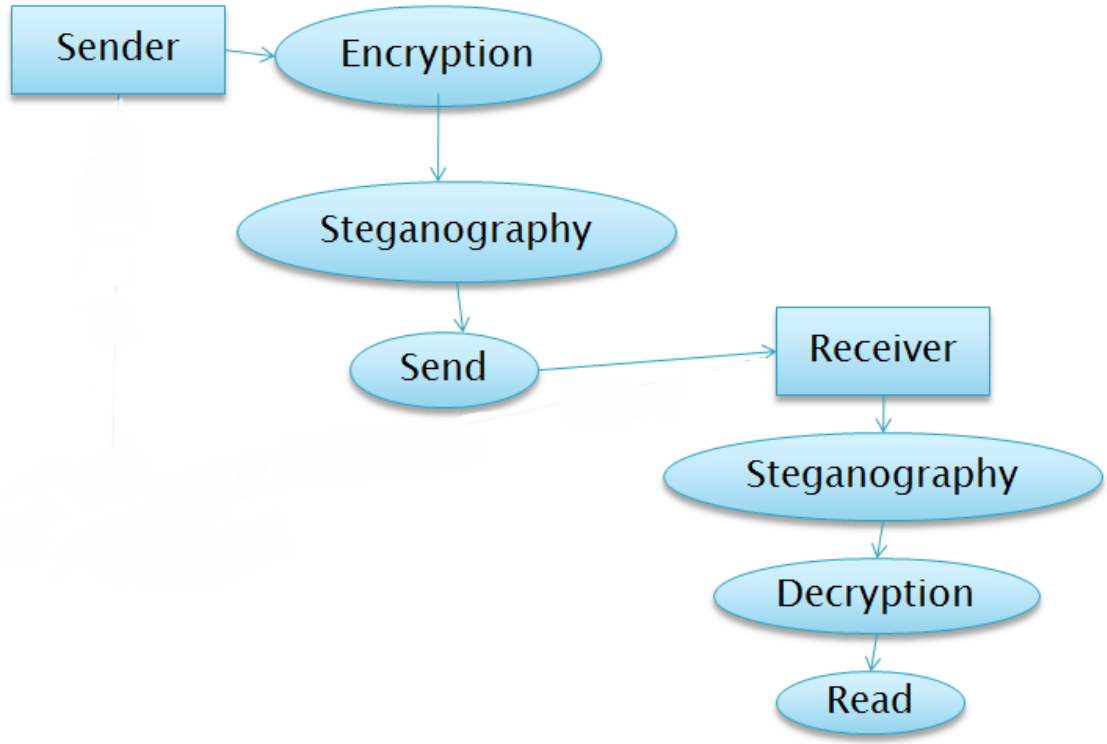

FIGURE 15: DATA FLOW DIAGRAM

Above is the data flow diagram of the functioning of the proposed system.

6 Evaluation

THE SYSTEM'S APPLICATIONS:

ADVANTAGES:

- One of the main reasons of interest of this framework is security since it provides security to your data.
- Messages sent to third parties without their knowledge, such as invaders or hackers.
- The number of bits has been replaced by the client or sender, thus a third party cannot guess the password.
- A normal user could even suspect that the image delivered contains data.
- Even if a user detects the presence of data in a picture, he will not know the true amount of the data or even the data itself because it will be encrypted.
- It adds an extra layer of protection by utilizing cryptography and a stego key.
- Simple to use and maintain.
- Software is protected by authentication.

DISADVANTAGES:

- Not appropriate for large amounts of data because data concealing is mostly determined by image size.
- As data size grows, it may take longer to produce a concealed picture.
- More computing power is required.
- If the stego picture is tampered with or compressed, part of the secret data will be lost.

APPLICATIONS:

- It is suitable for usage in Confidential Data Communications.
- Secure Data Storage.
- Data protection against tampering.
- Media in the E-Commerce Network.
- Can be utilized for secure data transport in military applications.
- Watermarking (Digital)

OBJECTIVE METRICS:

This system was created to provide secrecy so that 2 different clients or entities can safely communicate with each other. These entities can be government, secret services, the military, the banking sector, and normal people.

Things examined for the proper functioning of this system:

- The encryption and decryption process (AES algorithm).
- The image steganography process (LSB algorithm).
- The credentials of the users.
- Reliability, Security, Portability, Maintainability and Availability of the system were checked.

All this check made sure that the system if functioning well.

7 Future Work and Conclusion

Future Work:

There are continual advances in the PC area, suggesting advancements in the realm of steganography. All things considered, there will be increasingly proficient and advanced methods for Steganalysis soon long. Consider how difficult it is to identify the proximity of a truly huge book record inside a picture, and then consider how difficult it is to distinguish merely a handful of phrases inserted in a picture! It's like looking for a small needle in a large pile. It is expected that the Steganalysis approach will advance in the future, making it much simpler to detect even minor information inside an image. This study explores only a small portion of the science of steganography. As another discipline, there is a lot more research and development to be done. The accompanying segment depicts study areas that were comparable to the core objectives.

1. Distinguishing Steganography in Image Files:

Can steganography be differentiated in image files? This is a difficult question. It may be possible to identify a simple Steganographic approach by just studying the low request bits of the image bytes. However, if the Steganographic computation becomes increasingly random and scatters the implanted information throughout the image in an arbitrary manner or encodes the information before implanting, it may be impossible to detect.

2. Steganography on the WWW:

The World Wide Web (www) makes use of inline graphics. There are truly a significant number of images on various web pages all across the world. It could be possible to construct an application that acts as an internet browser in order to recover information embedded in site page Pictures. This Steganography-web might operate over the present WWW and provide a technique of transmitting info invisibly.

CONCLUSION:

The subject of how to preserve user data privacy is a hot topic these days. Cryptographic methods are becoming more adaptable as new mathematical tools become available, and they frequently now incorporate the usage of several keys in a single application development. In this study, we encrypt the plaintext with the Cryptography AES technique, then perform steganography on specific picture. Image and data encoding and decoding are carried out. Data hiding in images is said to be more versatile and secure.

LINK TO THE VIDEO PRESENTATION/DEMONSTRATION:

https://web.microsoftstream.com/video/e5270ac6-d228-42b9-a50e-fdd7d64047f

References

[1] Simmons, G. J., "The Prisoners' Problem and the Subliminal Channel," in Advances in Cryptology, Proceedings of CRYPTO '83, Plenum Press, pp. 51–67, 1984.

[2] J. Benaloh, “Key Compression and Its Application to Digital Fingerprinting,” technical report, Microsoft Research, 2009.

[3] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” Proc. 22nd Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT ’05), vol. 3494, pp. 457-473, 2005.

[4] S.S.M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, “Practical Leakage-Resilient Identity-Based Encryption from Simple As-sumptions,” Proc. ACM Conf. Computer and Comm. Security, pp. 152-161, 2010

[5]T. Furon, F. Cayre, G. J. Doërr, and P. Bas, editors, “Information Hiding,” Preproceedings of the 9th Int Workshop, No. 4567 in Saint Malo, France, June 11-13, Springer. ISBN 978-3-540-77369-6, 2007.

[6]Hai-Dong Yuan, “Secret sharing with multi-cover adaptive steganography,” Information Sciences Elsevier Vol. 254, P.P 197–212, 2013.

[7] R.J. Anderson and F. Petitcolas, “On the Limits of Steganography," IEEE Journal on Selected Areas of Communications, special issue on Copyright and Privacy Protection, April 1998.

[8] Anonymous Wikipedia link preffered (2004) “Steganography” Available at: http://en.wikipedia.org/wiki/Steganography (Nov 2004)

[9]Katzenbeisser, S. and Petitcolas, F.A.P (1999) Information hiding techniques for steganography and digital watermarking. Artech House, Norwood, MA 02062, USA.

[10]Backes, B. and Cachin, C. (2004) “Public key steganography with active attacks” IBM Research Report, Zurich Research Laboratory, Switzerland.

[11]Von Ahn, L. and Hopper, N.J. (2004) “Public key steganography” University Research Paper, Computer Science Department, Carnegie Mellon University, Pittsburgh, USA.