cognizancejournal.com
Sayed Ehsan Shamsi *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.4, Apr 2024, pg. 272-282
(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)
ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

Securing Messages and Files Using Integrated Steganography and Asymmetric Encryption Techniques

Sayed Ehsan Shamsi[1*]; Bebe Wajiha Nasrat[2*]

[1]Department of Information Systems, Balkh University, Mazar e Sharif, Afghanistan
[2]Department of Software Engineering, Balkh University, Mazar e Sharif, Afghanistan
[1]Email: shamsi@ba.edu.af; [2]Email: wajiha.nasrat2016@gmail.com

DOI: 10.47760/cognizance.2024.v04i04.019

Abstract- ***Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. As we know, after the improvement of internet, the security or privacy of information and data are the most important factors of Information Technology and communication. Every day, large quantities of data are transferred via the internet, file sharing site, social networking sites and etc. simultaneously, the number of internet users are also increases. This article aims to develop a user-friendly program that would address the security concerns in message delivery to authorized parties safely, at least to some extent. We applied C# language in order to make the application work fast and by the time the user selects the file and image, immediately after pressing the Encryption button within few seconds the process will complete. This evaluation showed that users fund this application easy to use and likely to be useful during message passing through steganography and cryptography methods.***

Keywords- ***Stego-image, Hiding, Plain text, Steganography, Cryptography.***

I. INTRODUCTION

Since the rise of the Internet we know that the biggest and one of the most important factors of IT and communication has been the security or privacy of information and data[1]. Everyday tons of data are transferred through the Internet through e-mail, file sharing sites, social networking sites and more. By the time the number of Internet users increase, the concept of Internet security has also become important[2]. The great competitive nature of the computer industry forces web services and technologies to the market at an immediate pace, leaving slight or no time for audit of system security, while the tight labour market causes Internet project development to be staffed with less experienced staffs, who may not have any training in

* Corresponding Author

security. Overall we can say that the market pressure, low unemployment, and rapid growth create an environment rich in machines to be unused, and malicious users to misuse those machines.

Cryptography is a technique for securing the secrecy of communication or information exchange and many different methods and ways are there that have been developed to encrypt and decrypt data in order to keep the message secret and secure[3]. Even though, it is sometimes not enough to keep the contents of a message secret and hidden, it may also be necessary to keep the existence of originality of the message secret[3]. The technique we have used or generally are using to implement this is called steganography.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc. also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing[4].

As a result, Steganography and cryptography are the methods we have chosen to utilize to secure messages since they are both relatively new in the realm of data security and safety and because we believe they will have a significant future influence.

II. LITERATURE REVIEW

Steganography, the art of concealed communication, continues to evolve in response to the escalating demand for secure data transmission and communication. This literature review delves into recent advancements in steganographic techniques, with a particular focus on statistical analysis, performance evaluation, and practical implementations spanning various domains. Alia et al. (2020) introduce a scheme that underscores statistical security and performance analysis, demonstrating its viability through FPGA implementations. Sing & Verma (2019) contribute insights into diverse steganographic algorithms, elucidating the trade-offs between payload capacity and susceptibility to attacks. Ansari (2019) conducts an exhaustive performance analysis of image steganography methods, covering a decade's worth of research. Additionally, Mangayarkarasi & Suganya (2019) present a strategy aimed at bolstering mobile industry security through steganography, with a primary focus on user privacy and data protection. This review amalgamates these contributions to furnish a comprehensive comprehension of the dynamic landscape of steganography and its implications for secure data communication. Steganography is a field that has garnered significant attention due to its potential applications in secure data transmission and communication. Alia et al. (2020) proposed a scheme focusing on statistical and performance analysis. They emphasized the generation of key values statistically secure against attacks. Unlike traditional methods, their approach does not rely on cover images, ensuring unlimited hiding capacity. Their implementation achieved notable running frequencies, showcasing its feasibility.

[5] contributed by reviewing various steganographic algorithms, including those based on LSB (Least Significant Bit) methods. They highlighted the trade-offs between payload capacity and susceptibility to statistical attacks. Sing & Verma also compared the performance of embedding-encryption and decryption-extraction modules, providing insights into FPGA resource utilization and running frequencies

Ansari (2019) conducted performance analysis on Bitmap, JPEG, and PNG steganography algorithms, evaluating their effectiveness through PSNR (Peak Signal-to-Noise Ratio) comparisons and technical properties assessment. Their review spanned over a decade of publications, offering a comprehensive understanding of the evolution of image steganography methods[6]. Mangayarkarasi & Suganya (2019) proposed a method to enhance the security of mobile industry transactions through steganography. By concealing data within images, they aimed to increase the confidentiality of transmitted information, particularly in m-banking systems. Their approach prioritized user privacy and data protection, addressing concerns regarding secure data communication in mobile environments[1].

Generally, these studies contribute to the advancement of steganographic techniques, offering insights into performance analysis, algorithm comparisons, and practical implementations across various domains, including image transmission, mobile industry security, and FPGA-based systems.

III. METHODOLOGY

To accomplish data security, the technique for this system was developed via significant study and analysis. This study was conducted to demonstrate various strategies and processes utilized in the protection of image files and documents. The system "Securing Messages & Files Using Integrated Steganography and Asymmetric Encryption Techniques" is created in the form of application that improved file security by integrating the technique of steganography and encryption with the additional feature of compression using the concepts of LSB[1], RSA[2] and 3DES[3] Algorithm for encryption. The application used the LSB Algorithm in hiding the secret file in a cover media. The integration was done by modifying the binary value of the cover media through the least significant bit where in every eighth bit representation of a cover media is replaced by every bit of the secret file[7]. The user will supply the single stego-key (up to 128-bit key length), which will be utilized for both encryption and decryption of the stego-photo.

3.1 ANALYSES of the SYSTEM

The application interface is simple and requires just one type of user (general user) who is conversant with the basics. The regular user can do all of the operations listed after installing the application on his PC. The program requires a Microsoft.NET framework 4.0/4.5 or above to execute.

3.1.1) Use Case Specification: In Fig. 1, a visual representation of the encryption and decryption process is provided, illustrating each step described below.

Sender side

- Select the desired encryption algorithm
- Import image to convert it into stego-image
- Select text file to encrypt
- Enter key for encryption
- Apply for Encrypt operation.
- Save the stego-image
- Send the stego-image to receiver

Receiver Side

- Receive the stego-image form sender
- Select the desired decryption algorithm
- Select stego-image to split the encrypted message and orginal image
- Select text file path to save
- Enter key for decryption
- Apply for decrypt operation.
- Save the splited text file from stego image

[1] Least-significant bit
[2]Rivest, Shamir, and Adleman
[3] Triple Data Encryption Standard

cognizancejournal.com
Sayed Ehsan Shamsi *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.4, Apr 2024, pg. 272-282
(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)
ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

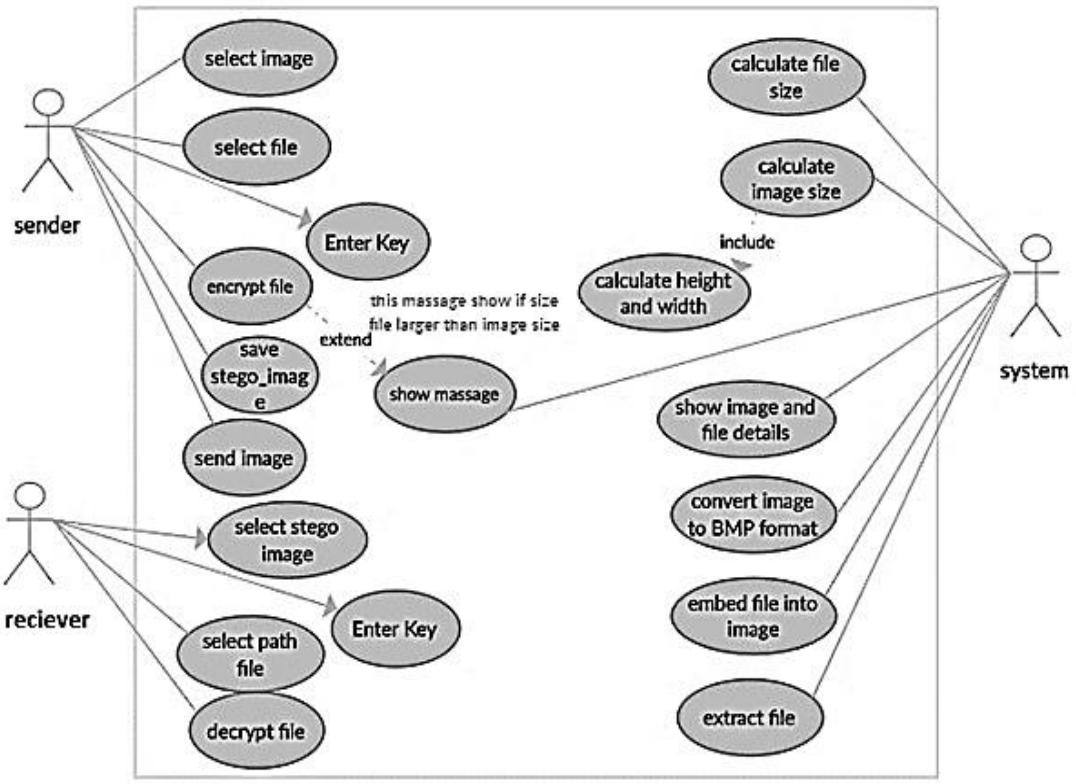

Fig. 1Use Case Diagram (Shamsi, 2024)

*3.1.2) Non-Functional Requirements: When selecting an image for encryption, it's essential to ensure its size falls within the appropriate range (200*200 pixels to 1000*1000 pixels), as images that are too small or too large may not be suitable. Additionally, the image should be free from distortion caused by any factors. Another consideration is that the operation may be halted until a proper key length, with a maximum of 128 bits, is applied.*

The application is designed to operate swiftly. Moreover, incorrect key lengths or incompatible picture formats should not cause the program to stop functioning abruptly; instead, appropriate notifications should be displayed as suggestions for resolving the issue.

Upon installation of the generated (.exe) file, the program we've developed should be capable of running and being installed on any computer running the Windows operating system. Users will require only the single (.exe) file to properly execute and install the application on any Windows machine.

3.1.3) The Activity Diagram: Once all encryption steps are finished—such as selecting the encryption technique (3DES, LSB, AES), choosing the file or text, and entering the secret key—the primary task involves selecting the text file and the image, embedding the text into the image, and encrypting it. The encrypted image acts as a carrier for the subsequent decryption phase. During decryption, the carrier image is decrypted using the same method and key which is shown in Fig.2. Upon completion, the original text file is retrieved along with the unencrypted image, which can be stored locally for future use.

cognizancejournal.com
Sayed Ehsan Shamsi *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.4, Apr 2024, pg. 272-282
(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)
ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

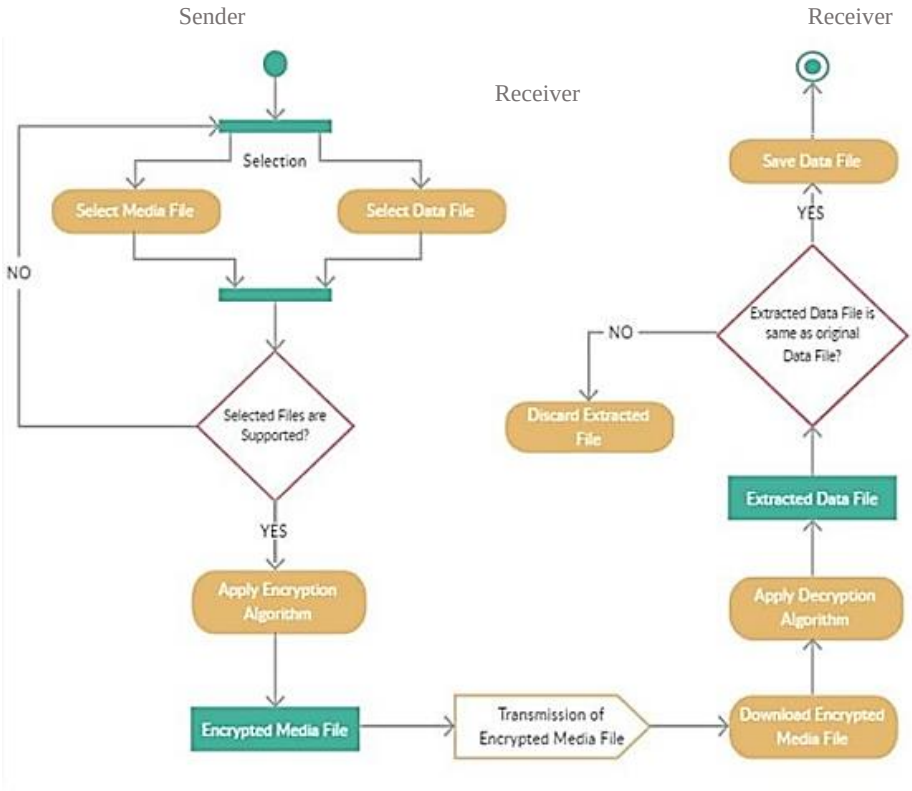

Fig. 2 Activity Diagram (Shamsi, 2024)

3.1.4) Class Diagram: The structure of the system is represented by a class diagram, which can highlight its classes' properties, functions, relationships, and interconnections with other entities. This article covers five phases of the classes: the source and the destination (also known as the Sender and the Receiver), hiding, transmission, and extraction. Each class has unique objects and methods, as seen in Fig. 3.

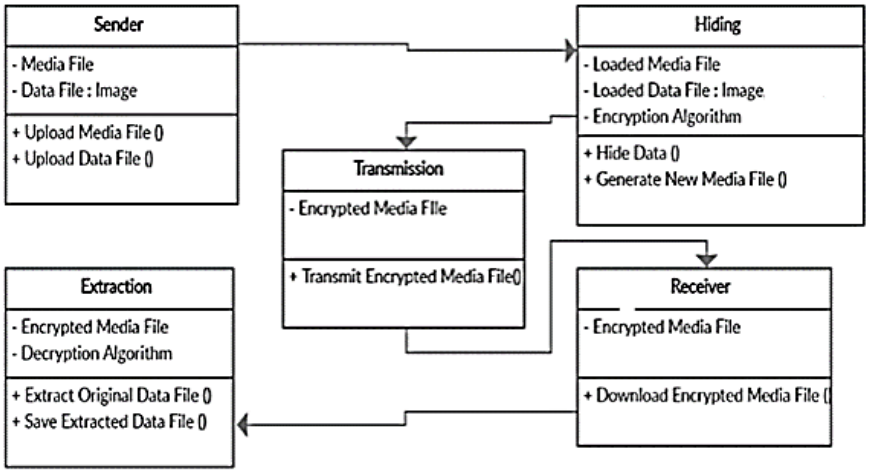

Fig. 3 Class Diagram(Sah & Gupta, 2017)

3.1.5) System Design: As previously noted, this study work is intended to use several steganographic approaches. The three steganographic techniques were used to try to create an application that would allow

cognizancejournal.com
Sayed Ehsan Shamsi *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.4, Apr 2024, pg. 272-282
(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)
ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

users to embed text or files with images (in this case, bmp). For improved security and encryption, the secret key the algorithm (3DES, LSB, AES) are utilized.

3.1.6) System Architecture: The (Fig. 4) demonstrates the overall architecture of the system.

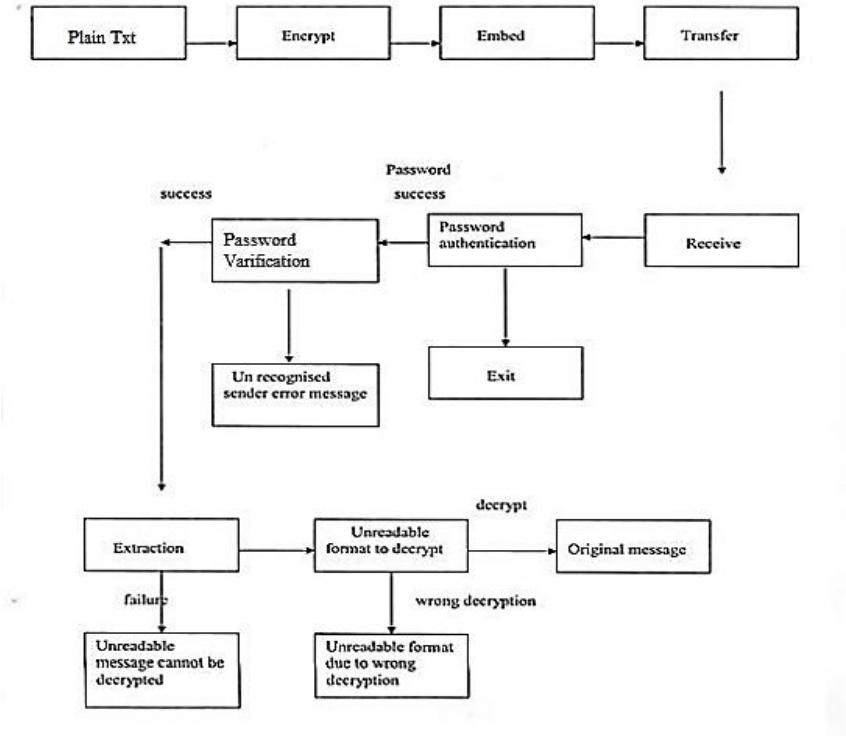

Fig. 4 System Architecture

3.1. Thoughts and Considerations

We have tried to make the end product in such a way that can help the users in the field of steganography. Meanwhile, beginner to expert users who are interested in installing the application may be among those who are using it. Therefore, the GUI[1] is offered so that this research project can be used as an application program by all user kinds.

However, C# programming was used to create the application in order to make it operate quickly, firstly in sender side once the user has chosen a file and an image, the procedure will be finished shortly after pushing the Encryption button, which is advantageous for stego-analyser. Gradually, decrypting the picture on the destination side proceeds with the same speed.

The primary focus is not only on the performance but also on improving the application's appearance and usability by including textboxes for entering the secret key and radio buttons to select the algorithms, among other features. Although, if additional functionality is needed in the future to increase the application's usefulness and security, it is simple to add it. The application's stability and durability are also given attention.

3.2. Development Tools

For developing the application, Microsoft .NET Framework is used, because it is good and user friendly that is developed by Microsoft. The main purpose of the .Net Framework is to make a user friendly GUI[1] which made the product more attractive and useful[8].The .Net Framework is the language that enabled us to make the application so easily and in a better way.

By using the security identifiers and also the control list, the applications which are made in .NET Framework are more secure and it also makes us able to build the web applications according to our needs[9]. In

[1] Graphical User Interface

cognizancejournal.com
Sayed Ehsan Shamsi *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.4, Apr 2024, pg. 272-282
(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)
ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

the current article Microsoft .NET Framework is used to make the application on steganography. the .NET module Visual Studio 2012 is main module to make the application.

3.3. Proposed Method Features

This research project's primary objective is to attempt to improve security while transmitting data from source to destination. The application's main benefit is its ability to conceal transferred data or information inside an image.

To safely deliver the message to the intended recipient, the image with the secret data is in the carrier. The encrypted image could be manipulated by malevolent or unauthorized users if any changes to the image's transparency or resolution occur during the encryption process. As a result, we must use extreme caution when doing image encryption. The coding part this project is available in [10] thesis.

IV. Result and Discussion

4.1 Software Interface

4.1.1) The Main Interface of the Application: The main interface is highly user-friendly and appealing. users can choose from five different tabs which are consecutively File Image Encrypt, File Image Dec, Image Message Enc, Image Message Dec and information, each of them explained by the interface in below. in addition, the last tab contains information about the software, as you can see bellow in (Figure 5) all operations are user friendly everyone with the basic knowledge can use it.

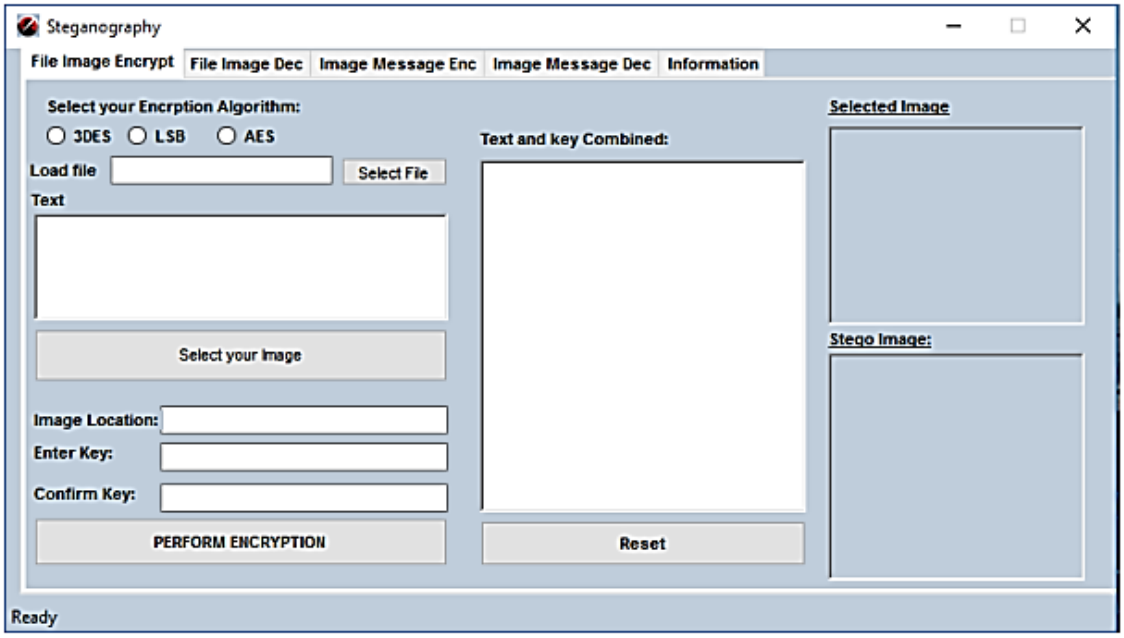

Fig. 5. The Main Interface (Image source: Author)

4.1.2) Interface One (File Image Encryption): In addressing the encryption aspect, the steps are detailed alongside corresponding figures

- Users initiate by selecting the desired encryption algorithm using the appropriate radio options. Following this, they can click "Select File" to choose the file for encryption, and its location will be displayed in the "image location area".
- Upon clicking "Select your Image," users are prompted to select the image intended for steganography and encryption. This image can be in bmp, JPEG, PNG, or GIF format, with bmp being the recommended format.
- The subsequent step involves entering the "Secret Key," utilized for encrypting the file's message, which is then displayed in the rich textbox. Users should note that the required key length varies based on the selected

algorithm (e.g., AES requires a key of more than six characters, 3DES necessitates a key of more than sixteen characters, while the LSB algorithm doesn't require a key at all). Furthermore, the encryption key must be entered twice for accuracy.

- Clicking the "Perform Encryption" button generates the encrypted message in the rich textbox and displays the stego picture in its designated image box. Users also have the option to save the stego image to the system storage for future use, such as sending it via email or social media.
- A confirmation message is displayed after selecting the directory and saving the stego image, ensuring successful saving. Users are then provided access to both the stego image and the encrypted message.
- The reset button restores the interface to its original state, clearing all buttons and textboxes after the encryption process, allowing for a fresh encryption or other purposes.

4.1.3) Interface Two (File Image Decryption): The phases and associated figures are explained for the objective of addressing the File Image Decryption side as shown in Fig. 6.

- The user should first select the decryption algorithm from the available radio buttons.
- The user is then led to the system storage by selecting Load Encrypted image, afterwards they must open the stego-image[1] in order for it to be displayed in the image box.
- After uploading the stego-image, the user must provide the secret key for image decryption in a textbox provided for that purpose.
- The "Save Decrypted Text File" button will appear after the user inserts the key, and it will display the path where the user wants to save the decrypted text. depicted in.
- After selecting the "Perform Decryption" button, the user will see the decrypted text file and image in their appropriate locations on the program interface.

Fig. 6. File Image Decryption

4.1.4) Interface Three (Image Message Encryption): The methods discussed above employ text files for encryption, while this method requires the user to enter text directly onto an application's interface in a designated location. although, there is no encryption procedure for plain text, or to put it another way, no encryption technique is employed for plain text; instead, plain text is only embedded in an image to create a stego-image as shown in Fig.7. the following are the steps for using Image Message Encryption

1. The user can enter text of her/his deciding on, choose "load image" as the next step, and then perform steganography on the text and image.

[1]Stego-image is the output of the embedding process. Stego-image contain the hidden message either in pixel values or in optimally selected coefficients[11]

2. The user is instructed to choose the image (plain text must be provided in the textbox field) in order to perform steganography on it by clicking the "Load Image" button.
3. After choosing an image and typing the text, we will click the "Perform Steganography" button to begin the steganography operation. A new window will then open, allowing users to save the stego-image before sending it to the recipient side.
4. Once the stego-image has been saved, a prompt message will show up to indicate that the action was successful in hiding the text and saving the image.
5. There is a reset option to undo all operations and restore the application to its original state after the completion of the text to image steganography process.

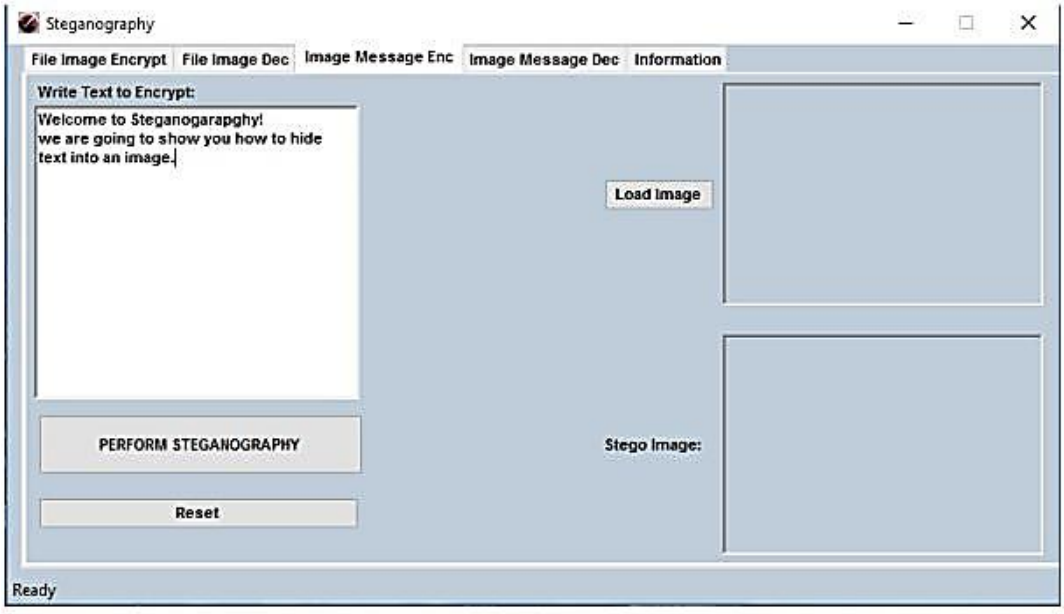

Fig. 7. Image Message Encryption

4.1.5) Interface four (Message Text Decryption): There is no decryption process to obtain the plain text, however; rather, the plain text is simply split from the stego-image to obtain the actual text from the stego-image as shown in Fig. 8. The procedures for using Image Message Decryption are as follows.

- Users are instructed to access the plain text from stego-image in the message text decryption section by selecting the load Encrypted Image button on the program.
- The user must obtain the plain text from the stego-image after it has loaded. The Decrypt button is used to carry out this action. The stego image will be divided into two parts: an image and plain text that will appear in readable form, allowing users to read the content that is concealed in the stego-image.
- The reset button returns the interface to its default state, allowing users to launch their new action. The application is open for new operations and all the buttons and textboxes have been released.

cognizancejournal.com
Sayed Ehsan Shamsi *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.4, Apr 2024, pg. 272-282
(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)
ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

Fig. 8. Message Text Decryption

V. CONCLUSION

As we can see, internet usage is growing daily, and consumers are particularly keen in using the internet to transfer confidential things like corporate documents, military information, and so on. The security of the data or information that users share is one of the main problems with using the internet to convey sensitive or critical information. It is possible that during the transfer of the information, users may lose secret data or that it may be acquired by unauthorized individuals who could misuse it. This could happen while internet users are sending secret information to authorized people. the confidential data may be obtained by hackers or online fraudsters, who may also change it before resending it to the original recipient parties. in order to safely transmit information. The application is set up to employ the Stego image technology, which conceals text-based information inside an image. LSB, 3DES, and AES algorithms are used to boost the security level of the stego image, and a secret key is also added when text is being hidden inside the image. So, by utilizing the application, users may securely exchange their information and are ensured that no unauthorized individuals will access their data. the created program performs steganography on the stego-image while maintaining its originality. Therefore, it is much safer and more secure to send the image to the authorized recipient since hackers cannot access the information due to encrypted text is concealed within the stego-image, so even if someone has accessed the stego image, he or she may not be able to tell whether it's the stego-image or image. Despite the text being separated from the image by a hacker, it is in encrypted form. this article has given readers a good opportunity to learn about dealing with data security challenges from a technical and theoretical standpoint. the program, which is a component of the.NET Framework and deals with security issues, was created using Visual Studio. Although the application is designed to work with a variety of image formats, including BMP, PNG, GIF, and JPEG, it suggests using a (.bmp) format image as a carrier image for better performance and security.

REFERENCES

1. S. Mangayarkarasi and K. Suganya, "IMAGE STEGANOGRAPHY BASED IMPROVING M-SECURITY," *Int. J. Manag. Technol. Eng.*, vol. IX, no. I, pp. 1000–1006, 2019.
2. M. T. Gençoğlu, "Combining of Cryptography and Steganography for Improving of Security," vol. 2, no. 6, pp. 77–85, 2018.
3. M. Kulkarni, P. Jagtap, and K. Kulkarni, "An Efficient Data Hiding Scheme Using Steganography and Cryptography Technique," vol. 5, no. 4, pp. 1–4, 2015.
4. G. N. Reddy and G. J. U. Reddy, "A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES".
5. A. Sing and C. Verma, "Image Steganography of Multiple File Types with Encryption and Compression Algorithms," *Int. J. Eng. Sci. Res. Technol.*, vol. 7, no. 7, pp. 1–4, 2019, doi: 10.5120/1238-1714.
6. A. S. Ansari, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats," *I. J. Comput. Netw. Inf. Secur.*, vol. 1, no. January, pp. 11–25, 2019, doi: 10.5815/ijcnis.2019.01.02.
7. A. Kaur, R. Kumar, and K. Kainth, "Review Paper on Image Steganography," vol. 6, no. 6, pp. 499–502, 2016.
8. S. Rajvanshi, S. Sawant, V. Tiwari, A. Waghmare, and M. Gogate, "Image Steganography," vol. 7, no. Xi, pp. 408–410, 2019.
9. S. Fraser, "Overview of the .NET Framework," 2009. doi: 10.1007/978-1-4302-1054-2_1.
10. M. Sharma and S. E. Shamsi, "SECURING MESSAGES & FILES USING INTEGRATED STEGANOGRAPHY AND ASYMMETRIC ENCRYPTION TECHNIQUES," LOVELY PROFESSIONAL UNIVERSITY in, 2019. [Online]. Available: https://drive.google.com/file/d/1BvaA29ny8calheFNdRydG2GJnfto5nTg/view?usp=sharing
11. M. Kalita and S. Majumder, "Steganography Using Biometrics," 2019, pp. 326–347. doi: 10.4018/978-1-5225-7492-7.ch026.
12. S. E. Shamsi, "Diagram." 2024. [Online]. Available: www.creately.com

