IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secretum Communication System

1Pardip Mane, 2Rupesh Verma , 3Amit Sahu ,4Amit Gujar, 5Aniket Harker
[1]Professor, [2]Student, [3]Student, [4]Student, [5]Student
[1]Information Technology
[1] Vasantdada Patil Prathishtan College of Engineering, Mumbai, India

Abstract: With the proliferation of Windows-based devices, ensuring secure communication has become paramount for various applications. This report delves into the creation of a secure communication system for Windows platforms using diverse cryptography techniques. It provides an overview of different cryptographic methods, highlighting their respective strengths and weaknesses, and explores their implementation within a Windows environment. The report further details the development of the secure communication system for Windows and evaluates its efficacy in terms of security and performance.Our analysis demonstrates that the system can offer robust security and optimal performance by employing techniques such as symmetric encryption, asymmetric encryption, hashing, and digital signatures.

Index Terms - Secure communication, Windows system, cryptography techniques, symmetric encryption, asymmetric encryption, hashing, digital signatures.

INTRODUCTION

In recent times, the ubiquitous presence of computer systems has intertwined with our daily routines. As the number of these devices escalates, so does the imperative for secure communication. The susceptibility of computer systems to security breaches underscores the necessity of employing cryptographic methods to fortify security measures. This report delves into the development of a Secretum Communication System focused on secure communication, leveraging diverse cryptographic techniques. We delve into an array of cryptographic methodologies, dissecting their merits and demerits, and elucidating their integration into computer systems. Furthermore, we scrutinize the execution of the secure communication system and scrutinize its efficacy in terms of security and performance.

2. Literature Survey

A. Arrangement using Multidirectional Pixel-Value Differencing

PyungHan Klim et al, described the following methodology in their paper [5] as mentioned below. In this strategy, the shading picture is separated into non-covering 2 X2 blocks. Leave C alone in the square. And afterward, deteriorate the shading picture into R G B tones. Refocus the decayed RGB pixel esteems in square C. Track down the base pixel esteems. And afterward, produce the sets in two ways or three ways Construct and perform two sets in two ways dependent on the base worth and in the subsequent stage develop sets in the three ways dependent on the base worth. Conceal more privileged information in the edge. Appropriate the pixels in two sets or three sets of two pictures. The privileged information is inserted in one or the other a few headings dependent on the base worth. Create two stego-shaded picture and use blend capacity to join R, G and B to deliver a shading cover picture. Also, send the shading cover picture through the web. [1]

On the recipient side, during the extraction cycle of privileged information from the hued cover picture following advances are followed. Split the hued cover picture into noncovering squares and afterward decay each shading picture into R, G, and B. Then, at that point, partition the two stego shading pictures into 2 X2 blocks. Concentrate privileged information from the shading cover picture.

B. Real-Time error Free Reversible Data Hiding in Encrypted Images Scheme Kaimeng Chen et al, explained in the paper [9] explained their methodology as following steps.

Produce a mistake expectation map for the first picture, and afterward scramble the picture utilizing key by utilizing cryptographic calculation. Nonmodifiable eight pseudo-irregular pieces are produced by utilizing the picture encryption key. Again the encoded picture was scrambled for mistake expectation map encryption and most huge piece replacement by utilizing encryption key and perform bit insightful XOR. Presently the mysterious message is hidden in the encoded picture which is called a cover picture. For inserting the restricted information in the picture, all modifiable pixels are isolated into seven-pixel bunches even
pieces. The seven-piece hamming code is separated from the most un-critical piece of all pixels in the gathering. With the assistance of an equality check, the 7-piece hamming codeword is named one of the eight kinds of 7-piece hamming codeword. What's more, in the second least critical piece privileged information is implanted. And afterward, send the cover picture to the beneficiary. If any unapproved individual attempts to get to the message, they aren't ready to remove the information that is hidden in the picture. Presently at the collector side, unscramble the cover record and concentrate the privileged information inserted in the beneficiary side. Afterward, separate the inserted information and recuperate the first picture using decoding and information-concealing keys. Decode the scrambled picture and mistake the expectation map. Ascertain the expectation mistake. Assuming a blunder isn't anticipated in the beneficiary side, the privileged information is extricated from the cover picture.

C. Separable Reversible Data Hiding in Encrypted Signals Wei-Liang Tai et al, described in their methodology in the paper as mentioned below.

Three unique modules are clarified in this approach. In the main module, a unique cover picture record is encoded by the proprietor by utilizing a public key and sending it to the information hider. Leave every pixel alone xi, j, and convert xi, j to x1i, j and x2i, j, where xi, j = x1i, j + x2i, j. Pick an irregular whole number r1, and encode e public every pixel utilizing a public key. Furthermore, send the scrambled picture to the information hider. In the second module, Data Hider gets the encoded message from the proprietor and installs the information in the scrambled cover document by utilizing the information concealing key and extra information. Install the secret piece into an encoded unit. Leave the encryption unit alone EUi. On the off chance that the mysterious piece is 1 and EU1 EU2, trade EU1 and EU2. Produce a stamped signal, when every one of the signs is installed. Presently the scrambled cover document with an implanted message is shipped off to the beneficiary. In the third module, the beneficiary gets the encoded cover document with installed information. Develop a non-rehashed irregular implanting succession by utilizing the information-concealing key. The beneficiary concentrates the mysterious key from the checked scrambled unit. Leave the checked encoded unit alone MEUi. On the off chance that MEU1> MEU2, extricate bit 1 in any case separate piece 0. The collector extricates every one of the information by utilizing the information-concealing key and unscrambles the first picture by utilizing the private key of the recipient. The collector will recuperate the first picture when all stamped encoded units are recuperated

D. Goldreich, Oded [3, 13] J2ME plays a vital role in software development (Java 2 Micro Edition). J2ME is employed for devices that have limited display, memory, and processing power. Mobiles are extremely useful for the National Security Agency Department for exchanging secret information. Cryptography secures the messages so that unauthorized users intruders or hackers cannot read it, only the authorized person can read it and access it [7, 8]. From the literature review, it is understood that the algorithms are not used to secure the SMS. The algorithms are used for secured data communication over networks.

E. AES encryption was carried out by Muttaqin and Rahmadoni with their research entitled

"Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based ". In this study, AS uses the Rijndael algorithm which can encrypt and decrypt data blocks of more than 128 bits with a key length of 128 bits. Its application is to encrypt files. In system testing, testing is carried out on all files with different file sizes and for the results of the encryption process (ciphertext) in the form of files with the *.encrypted extension file format.

3. Architectural Design

Implementation Phase

Steganography is cloaking a hidden message inside an image or cover message. One way to achieve this is to use the Least Significant Bit (LSB) approach, which entails swapping out the least significant bits of the cover picture with those from the hidden message. **Figure 1** depicts the Least considerable method. We have a 480×480 480×480 colour image with the dataset, and we want to hide a secret message of 100 bits within the image using LSB steganography. The LSB approach replaces the least significant bit of each pixel in the image with a bit from the secret message. This results in a slight change in the pixel values that is not easily noticeable to the human eye, but the difference is sufficient to hide the message. To ensure the secret message's confidentiality, we encrypt it using AES encryption. For example, AES operates on data in bytes rather than bits. The cipher processes 128 bits of the incoming data at a time because each block is 128-bit long. The embedding process can be described mathematically as using Equation (**1**

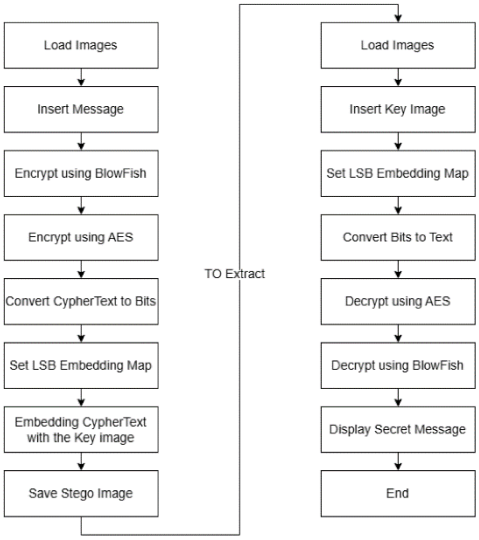


Fig. 1. Least significant approach encryption and decryption process.

We let the original pixel value of the ith pixel be denoted by Pi,and we let the modified pixel value after embedding the secret message be represented by $P'i$. The modified pixel value can be calculated using Equation (**1**),

$$P'i=Pi+(2n*mi),$$

where n is the number of least significant bits used for embedding (for example, n = 1 for LSB), mi is the ith bit of the secret message, and the addition is performed in modulo 28(since each colour component of a pixel is typically stored as an 8-bit value). The process is similar for grayscale images, but the pixel values are 8-bit values instead of 24-bit values. Similarly, if we want to use Blowfish encryption instead of AES, the secret message would be encrypted using Blowfish, and the encrypted ciphertext would be hidden within the image using LSB steganography. This example shows how LSB steganography and encryption algorithms can be used together to hide a secret message within an image, providing both confidentiality and imperceptibility to the hidden message. Steganography and cryptography are commonly used to manipulate information and mask their presence. Intentionally, cryptography messages up to make it understood.

On the other hand, steganography masks or dissimulates the text and renders it unnoticed. Steganography is very useful if it is forbidden to use cryptography, where strong encryption is usually prohibited. Steganography can, therefore, stop these laws and transfer a text anonymously. Our research focuses on the ways a strong defensive mechanism can be developed. In cryptanalysis and steganalysis, a great effort has been made to overcome the hiding skills, so our role is to create a new technique that is more difficult to discover or defeat. The proposed model has two main functions, Embedding the Message into Cover Image and Extraction the Message from the Cover Image. The following processes are discussed: The data are securely embedded into the cover image at multiple levels using compress and encryption algorithms AES and BlowFish. The final output image combines a secret message and an image created using a dynamic transfer model.

This model adapts the key image method to calculate a cipher key and implements various data-hiding techniques to enhance security. The result is a smoothed stego image that is difficult to detect, ensuring the confidentiality of the hidden information.

The stego image accompanies a key idea as the decryption key. Upon successful upload, the decryption phase commences, followed by the decoding process, revealing the hidden message. An integrity check ensures that any changes to the image, such as an attack, did not alter the mask value and compromised the key for decryption. This helps to ensure the accuracy and security of the recovered information. The flow diagram of embedding images is shown in **Fig 2**. The LSB Approach:

The LSB approach is an essential and widely used technique in steganography.

It involves replacing the least significant bits of the cover media with secret data to embed information. The altered bits are typically invisible to the human eye or ear, making it difficult to detect the hidden message. Supposing we have an image with pixel values ranging from 0 to 255, we can modify the least significant bit of each pixel to hide a secret message using the LSB approach. For instance, if the pixel value is 110 (in binary: 01101110), and we want to embed a bit of 1, we can change the LSB to 1 (01101111). This slight modification is often visually indistinguishable, especially with large cover media such as images or audio files

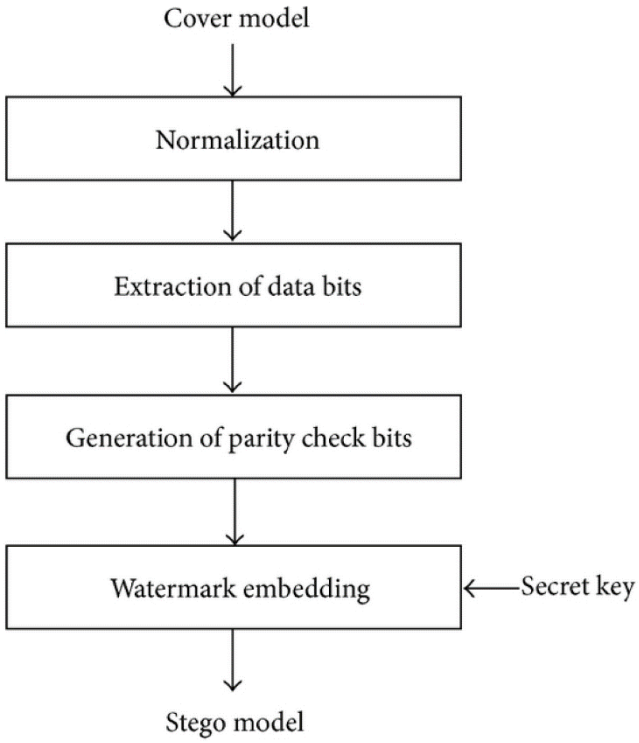


Fig. 2 Flow diagram of embedding images.

4. Project Planning

4.1 Roles and Responsibilities

SR. No	Name of Member	Role	Responsibilities
1	Rupesh Verma	Team Leader	Libraries, Model Design
2	Amit Gujar	Member	Frontend, UI Design
3	Amit Sahu	Member	Data flow, Backend Connectivity
4	Aniket Harker	Member	Model Training and Design

4.2Assumptions and Constraints

- Users of this Desktop App can use this system.
- Users of this Desktop not required to have active internet.
- Users should provide a Password to get the result.
- This system will work for 24/7 at the Devices.
- Highest accuracy is provided to the user based on the Length of Text provided
- We have to work with the available resources.

• We need to manage the entire project within the team of developers.

4.3 Project Management Approach

We will be working in an agile project management approach. As Agile is a project management methodology that uses short development cycles called "sprints" to focus on continuous improvement in the development of a product or service. We will be using the following principles while working:

• Changing environments are embraced at any stage of the process to provide the customer with a competitive advantage.
• We will deliver a product or service with higher frequency.
• Our Stakeholders and developers collaborate closely on a daily basis.
• All stakeholders and team members remain motivated for optimal project out- comes, while teams are provided with all the necessary tools and support, and are trusted to accomplish project goals.
• Face-to-face meetings are deemed the most efficient and effective format for project success.
• A final working product is the ultimate measure of success.
• Sustainable development is accomplished through agile processes whereby development teams and stakeholders are able to maintain a constant and ongoing pace.
• Agility is enhanced through a continuous focus on technical excellence and proper design.
• Simplicity is an essential element.
• Self-organizing teams are most likely to develop the best architectures and designs and to meet requirements. Regular intervals are used by teams to improve efficiency through fine-tuning behaviors.

4.4 Ground Rules for the Project

• Be on time for all team meetings.
• Team leader must create and disseminate agendas for each team meeting.
• Team leader must create and disseminate minutes after each team meeting.
• Attend full duration of all team meetings unless a case of emergency.
• Avoid informal/social talk during team meetings.
• Avoid apathetic/passive decision making (e.g., "whatever you all think is right").
• Inform team leader if unable to complete work on time.
• Set deadlines for each deliverable in advance of due date to allow for collaborative revisions.
• Rotate responsibilities so each person gets experience with several aspects regardless of quality or qualifications.
• Make criticisms constructive with suggestions for improvement and non-judgmental language.
• Confront issues directly and promptly.
• Promptly relay all interpersonal concerns/conflicts to team leader.
• Keep a positive attitude toward the team, individual members, projects and course.
• Take initiative by offering ideas and volunteering for tasks.
• Play an equal role in the team by contributing equally to every task.
• Be honest with any team member who is not pulling her/his weight.
• Help one another with difficult or time-consuming deliverables.
• Ask for help from the team or other resources if "stuck" or falling behind.
• Treat each other with respect.
• Accept responsibility and accountability along with the authority given.

4.5 Project Budget

• It is cost efficient Project.
• Easily deployable across compatible devices.

5. Software Requirements Specification

5.1 Overall Description

5.1.1 Product Features

The following are the main features that are included in our Secretum Communication System:

1. Hide your private messages in images, audio & text files.
2. Forgot password in case you forget.
   (Click on the 3 dots in main window to know more)

3. Access info about any button just by hovering on it.

5.1.2 Characteristics

Using Secretum Communication System people can hide their important information in Text, Image, and Audio. This hidden message will be only open by the password.

5.1 .3 Operating Environment

The application is developed using the languages like Python, and Python Libraries to enable the creation of a Desktop based Application, which can be accessed from any Device.

5.1.4 Design and Implementation Constraints

a. The application should run in a latest Python version.
b. The application might take a few seconds to load the information for the user
c. This system is highly flexible.

5.2 External Interface Requirements

5.2.1 User Interfaces

a. Front-end software: Tkinter and Dear PyGui
b. Back-end software: sqlite3

5.2.2 Hardware Interfaces

a. Windows or Mac operating systems
b. Devices not necessary to have the Internet.

5.2.3 Software Interfaces

a. The user's System should be latest Python version and libraries compatible for all the functionalities to work.

5.3 Nonfunctional Requirements

5.3.1 Performance Requirements

a. The dashboard page is displayed to the user immediately. It takes few seconds to display the output to the user weather it is providing image to text , text to audio result.
b. The Secretum Communication System is flexible and smooth so that it does not consume any time of the user.

6. Implementation

This Python-based GUI tool, developed using Tkinter, implements a simple steganography technique known as the Least Significant Bit (LSB) method. It facilitates the concealment and extraction of text data within images and audio files, as well as the hiding of one image behind another. The LSB method operates by altering the least significant bit of each pixel's RGB components, ensuring minimal perceptible change to the human eye. In cases where data exceeds the capacity of the first bit of every pixel, subsequent bits are utilized, with caution exercised to avoid conspicuous alterations to the image. This tool leverages basic image processing concepts, treating digital images as matrices of pixels, each representing the brightness of a color. Through this methodology, users can communicate covertly while maintaining a semblance of normalcy within their multimedia files

7. Screenshots of Project

Home Page :

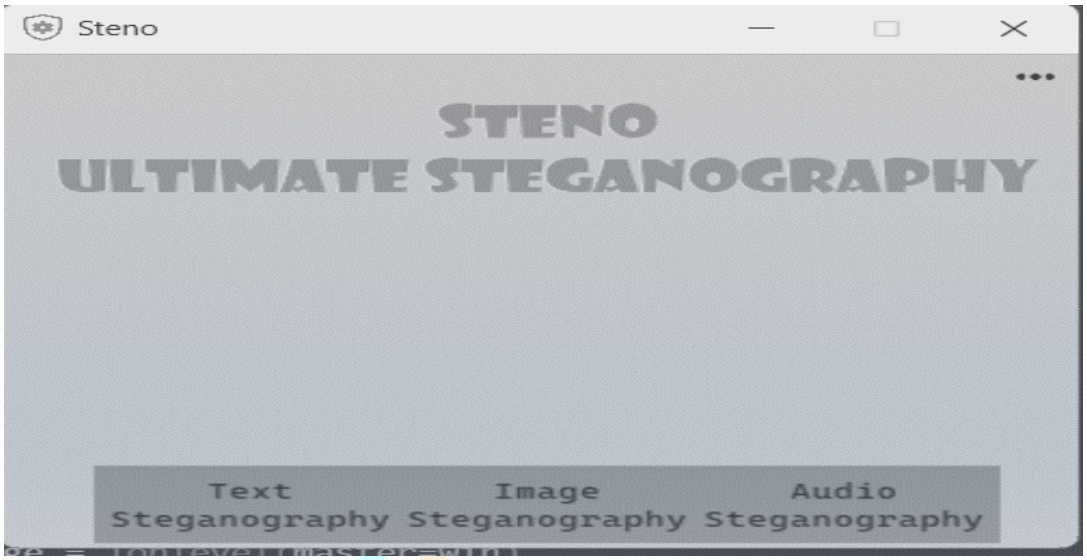
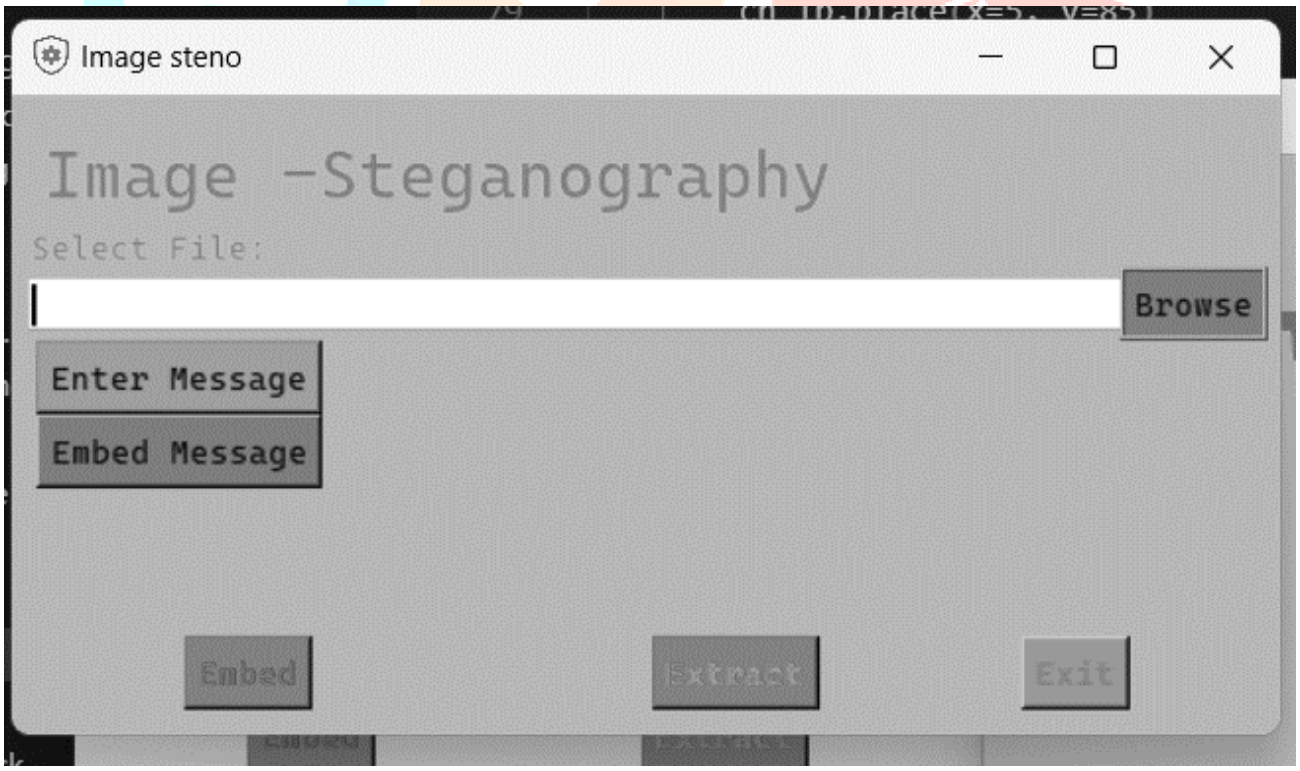
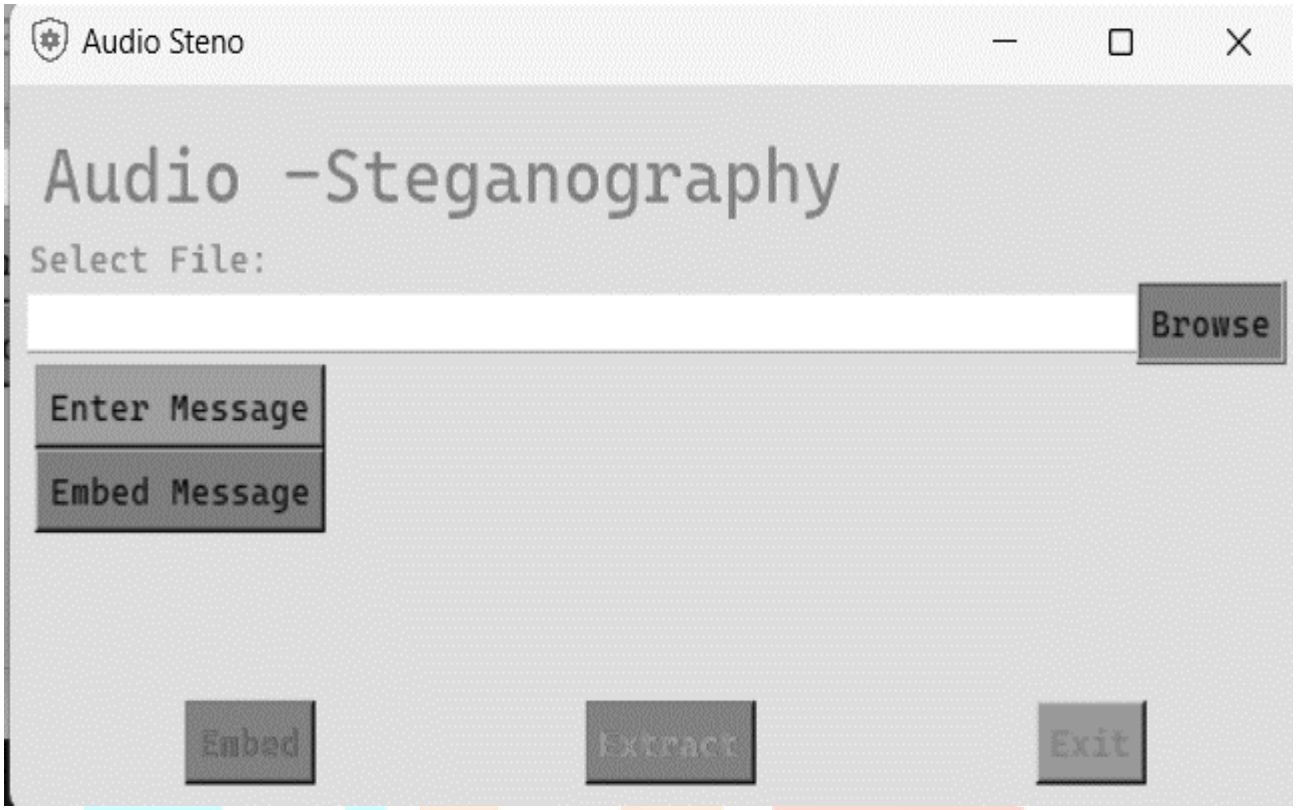


Image section :



Audio section:



8. Conclusion and Future Scope

8.1 Conclusion

The main aim of this investigation was to create a messaging system that employs cryptography to deliver top-tier security and privacy while maintaining user-friendliness. The study underscores the significance of crafting a user-friendly interface to streamline the system's usability without compromising security and privacy standards. Through the exploration of various cryptography techniques such as end-to-end encryption, digital signatures, and public-key cryptography, the study unveils avenues to fortify the app's security and privacy features.

The study underscores the pivotal role of intuitive interface design in ensuring the success of cryptography-driven messaging Secretum Communication System. It emphasizes the critical nature of end-to-end encryption in furnishing robust security and p–rivacy layers. Furthermore, the study advocates for the integration of digital signatures and public-key cryptography to augment the system security measures

8.2 Future Scope

Given the existing groundwork laid out for a GUI-based steganography tool using the LSB method in Python with Tkinter, the future scope for enhancement and expansion is vast. Firstly, the tool can be extended to support more advanced steganographic techniques beyond just LSB, such as LSB matching or frequency domain methods, to increase the capacity and security of hiding data within images and audio files. Additionally, the tool can be optimized for performance, especially when dealing with larger files or batches of files. This could involve implementing multithreading or multiprocessing techniques to improve speed and efficiency. Furthermore, the GUI can be enhanced to provide a more intuitive and user-friendly experience, with features like drag-and-drop functionality, real-time previews, and error handling for invalid inputs.

In terms of functionality, the tool can be expanded to support hiding data in other types of media, such as videos or documents, and also incorporate encryption techniques to further enhance security. Moreover, the tool can be made more versatile by adding support for different file formats and compression methods, as well as incorporating error correction mechanisms to ensure data integrity during extraction. Overall, the future scope for the steganography tool is promising, with opportunities for enhancing functionality, performance,

and usability to meet the evolving needs of users in the realm of secure communication and data concealment.

9. References

1. Pyung-Han Klim, Eun-Jun Yon, Kwan-Woo Ryo and Hi-Hyun Jung, “Data-Hiding Scheme Using Multidirectional Pixel-Value Differencing on Colour Images”, Hindawi Security and Communication Networks, 11, 1-12 (2019)
2. Kaimeng Chen 1 and Chin-Chen Chang, “Real-Time Error-Free Reversible Data Hiding inEncrypted Images Using (7, 4) Hamming Code and Most Significant Bit Prediction”, MPDI Symmetry, 10, 51(2019)
3. Wei-Liang Tai 1 and Ya-Fen Chang, “Separable Reversible Data Hiding in Encrypted Signals with Public Key Cryptography”, MPDI Symmetry,10,23 (2018)
4. IBM Knowledge Center, "uuencode() function," IBM, 15 August 2015. [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSULQD_7.2.1/com.ibm.nz.sqltk.doc/r_sqlext_uuencode.html. [Accessed 26 September 2018]
5. D. R. I. M. Setiadi and J. Jumanto, "An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection," Cybernetics and Information Technologies, vol. 18, no. 2, pp. 74-88, 2018.
6. R. P. Naik, "Optimising the SHA256 Hashing Algorithm for Faster and More Efficient Bitcoin Mining," Department cf Computer Science University College London, London , 2013.
7. Yufeng Wang, Qun Jin, jianhuawang, “A Wi-Fi Direct based P2P application prototype for mobile social networking in proximity (MSNP)”, IEEE 12th International Conference on Dependable, 2014
8. Bo Zhao,Yu Xiao,Yuqing Huang,Xiaoyu Cui.A Private User Data Protection Mechanism in TrustZone Architecture Based on Identity Authentication[J].Tsinghua Science and Technology,2017,22(02):218 225.
9. Xuhong Peng, Ju Ren*, Liang She, Deyu Zhang, Jie Li, Yaoxue Zhang, "BOAT: A Block-Streaming App Execution Scheme for Lightweight IoT Devices", IEEE Internet-of-Things Journal, vol. 5, no. 3, pp. 1816 1829, 2018.
10. Behrouz A. Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, 2nd Edition, Tata McGraw Hill, 2012. [Date of access: 20 February 2016]