VISVESVARAYA TECHNOLOGICAL UNIVERSITY
Jnana Sangama, Belagavi, Karnataka–590014

Mini-Project Report

On

“ENHANCING SECURITY OF DATA USING IMAGE STEGANOGRAPHY AND ENCRYPTION”

Submitted in partial fulfillment of the requirements for the award of degree of

BACHELOR OF ENGINEERING

In

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted by

SHASHIDHARA	**(1BI20EC131)**
SOUJANYA S	**(1BI20EC147)**
VARSHA V	**(1BI21EC169)**
VIVEK D	**(1BI20EC174)**

Under the guidance of

BHAVYA K B
Assistant Professor
Dept. of ECE, BIT

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING
BANGALORE INSTITUTE OF TECHNOLOGY
K.R. Road, BANGALORE – 560004
2022-2023

BANGALORE INSTITUTE OF TECHNOLOGY

K.R. Road, V .V Puram, Bangalore 560004

www.bit-bangalore.edu.in

Department of Electronics and Communication Engineering

CERTIFICATE

Certified that the mini-project work entitled **"ENCHANCING SECURITY OF DATA AND USING IMAGE STEGANOGRAPHY AND ENCRYPTION"** carried out by **SHASHIDHARA** USN:(1BI20EC131), **SOUJANYA S** USN:(1BI20EC147), **VARSHA V** USN:(1BI20EC169) and **VIVEK D** USN:(1BI20EC174) a bonafide student of Bangalore Institute Of Technology in partial fulfillment for the award of Bachelor of Engineering/ Bachelor of Technology in Electronics and Communication Engineering of the Visvesvaraya Technological University, Belgaum during the year 2020- 2021. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the Report deposited inthe departmental library. The Mini-project report has been approved as it satisfies the academic requirements in respect of Mini-Project work prescribed for the above said Degree.

BHAVYA K B
Assistant Professor
Dept. of ECE, BIT

Dr. HEMANTH KUMAR A.R
Professor & Head
Dept. of ECE, BIT

External Viva

Name of the examiners &Signature with date

1.

2.

ACKNOWLEDGEMENT

We would like to thank my guide **Bhavya K B**, Assistant Professor, Electronics and Communication Department, Bangalore Institute of Technology, Bengaluru for guiding untiringly all through my tenure.

We would like to thank the Mini Project Coordinator **J.C.Narayana Swamy**, Associate Professor, and, **Dr. Vidyasaraswathi H.N**, Assistant Professor, Electronics and Communication Department, Bangalore Institute of Technology, Bengaluru for their guidance.

We would like to thank **Dr. Hemanth Kumar A.R**, Head of the Department Electronics and Communication Department, Bangalore Institute of Technology, Bengaluru for this opportunity to present this **Mini Project** on “**ENHANCING SECURITY OF DATA USING IMAGE STEGANOGRAPHY AND ENCRYPTION**” of our choice and interest.

We extend my gratitude to **Dr. Aswath M U**, Principal, Bangalore Institute of Technology, Bengaluru, for his encouragement and support.

We are fortunate for being part of Bangalore Institute of Technology, the institution that stood by our side and assisted us towards successfully completing the **Mini Project**. We also take this opportunity to thank the Department of Electronics and Communication, Bangalore Institute of Technology for their tremendous help and guidance.

SHASHIDHARA	**(1BI20EC131)**
SOUJANYA S	**(1BI20EC147)**
VARSHA V	**(1BI21EC169)**
VIVEK D	**(1BI20EC174)**

ABSTRACT

Image steganography is a technique used to conceal secret information within digital images, ensuring the privacy and security of data transmission. This abstract explores the fusion of Advanced Encryption Standard (AES) and Least Significant Bit (LSB) algorithms for robust and efficient image steganography. The AES algorithm, known for its strength in encryption, provides a secure mechanism to protect the confidentiality of the embedded data. It employs symmetric key encryption to convert the secret information into cipher text using a key known only to the authorized parties.On the other hand, the LSB algorithm focuses on modifying the least significant bit of the image pixels to embed the hidden data without significantly affecting the visual quality of the image. By substituting the least significant bits with the secret message bits, the algorithm achieves imperceptible alterations in the image.In combining AES and LSB algorithms, this proposed steganography technique offers both encryption and hiding capabilities, ensuring the secure transmission and inconspicuousness of the embedded data. The AES algorithm acts as an additional layer of protection, making the hidden information resistant to various attacks. Experimental results demonstrate the effectiveness of the combined AES-LSB approach in terms of security and robustness against various steganalysis techniques. The proposed technique successfully achieves a balance between data hiding capacity, image quality preservation, and encryption strength. In conclusion, the integration of AES and LSB algorithms presents a powerful method for image steganography, providing enhanced security and confidentiality while maintaining the visual integrity of the carrier image. This technique finds potential applications in secure communication, digital watermarking, and covert data transmission.

.

TABLE OF CONTENTS

LIST OF FIGURES

BANGALORE INSTITUTE OF TECHNOLOGY

VISION

To establish and develop the Institute as a center of higher learning, ever abreast with expanding horizon of knowledge in the field of engineering and technology, with entrepreneurial thinking, leadership excellence for life-long success and solve societal problem.

MISSION

- Provide high quality education in the engineering disciplines from the undergraduate through doctoral levels with creative academic and professional programs.
- Develop the Institute as a leader in Science, Engineering, Technology and management, Research and apply knowledge for the benefit of society.
- Establish mutual beneficial partnerships with industry, alumni, local, state and central governments by public service assistance and collaborative research.
- Inculcate personality development through sports, cultural and extracurricular activities and engage in the social, economic and professional challenges.

LONG TERM GOALS

- To be among top 3 private engineering colleges in Karnataka and top 20 in India.
- To be the most preferred choice of students and faculty.
- To be the preferred partner of corporate.
- To provide knowledge through education and research in engineering.
- To develop in each student mastery of fundamentals, versatility of mind, motivation for learning, intellectual discipline and self-reliance which provide the best foundation for continuing professional achievement.
- To provide a liberal; as well as a professional education so that each student acquires a respect for moral values, a sense of their duties as a citizen, a feeling for taste and style, and a better human understanding.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION

VISION

Imparting **Quality Education** to achieve **Academic Excellence** in Electronics and Communication Engineering for **Global Competent Engineers**.

MISSION

- Create **state of art infrastructure** for quality education.
- Nurture innovative concepts and problem solving skills.
- Delivering Professional Engineers to meet the societal needs.

PROGRAM EDUCATIONAL OBJECTIVES

- Prepare graduates to be **professionals**, Practicing engineers and entrepreneurs in the field of Electronics and communication.
- To acquire sufficient knowledge base for **innovative techniques** in design and development of systems.
- Capable of competing globally in **multidisciplinary** field.
- Achieve personal and professional success with awareness and commitment to **ethical and social responsibilities** as an individual as well as a team.
- Graduates will maintain and improve technical competence through **continuous learning process**.

PROGRAM SPECIFIC OUTCOMES

PSO1: Core Engineering: The graduates will be able to apply the principles of Electronics and Communication in core areas.

PSO2: Soft Skills: An ability to use latest hardware and software tools in Electronics and Communication engineering.

PSO3: Successful Career: Preparing Graduates to satisfy industrial needs and pursue higher studies with social-awareness and universal moral values.

CHAPTER 1
INTRODUCTION

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

In today's era of digital communication and information exchange, ensuring the security and confidentiality of sensitive data has become paramount. With the ever-increasing risks of cyberattacks and unauthorized access, it is crucial to employ robust security measures to protect valuable information. The rapid advancement of technology has significantly transformed the way we communicate and share information. However, concerns about data privacy and confidentiality have arisen due to the knowledge that email service providers may sell user data to third-party companies. This realization has led to a growing need for individuals to take control of their own data security and protect their confidential information.

Image steganography is a technique used to hide sensitive information within digital images, enabling covert communication and secure data transmission. The integration of the AES (Advanced Encryption Standard) and LSB (Least Significant Bit) algorithm enhances the effectiveness and security of this process. AES is a widely adopted symmetric encryption algorithm known for its robust cryptographic properties. It ensures that the hidden data remains confidential by encrypting it before embedding it into the carrier image. AES employs a strong key-based encryption system, making it highly resistant to decryption attacks. The LSB algorithm, on the other hand, takes advantage of the least significant bits of pixel values in an image. These bits are modified to represent the hidden data, causing minimal visual distortion to the human eye. By altering these bits, the LSB algorithm provides a method of hiding information within the image without significantly altering its appearance.

The combination of AES and LSB algorithm offers a powerful solution for image steganography. The hidden data is not only encrypted but also seamlessly embedded within the image, making it difficult for unauthorized individuals to detect or access the concealed information. This approach provides a secure and efficient means of transmitting sensitive data while maintaining the visual integrity of the carrier image.

1.2 MOTIVATION

In today's digital age, email has become an indispensable tool for communication, both in personal and professional spheres. However, the widespread use of email has raised concerns about the privacy and confidentiality of the information transmitted through this medium. Users often share highly sensitive and confidential data via email, such as financial information, personal details, trade secrets, or legal documents. The realization that email service providers may sell user data to third-party companies for targeted advertising or other purposes has further exacerbated these concerns. The potential compromise of sensitive data poses a significant risk to individuals and organizations. Unauthorized access or interception of email communication can lead to identity theft, financial fraud, corporate espionage, or the leakage of personal and proprietary information. It is imperative to address these concerns and take proactive measures to ensure the confidentiality and security of data transmitted via email.

The motivation behind this project arises from the need to empower individuals to protect their own data and regain control over their privacy. By implementing a combination of steganography and encryption techniques, the project aims to provide users with a higher level of data confidentiality in email communication.

1.3 NEED FOR IMPROVEMENT IN DATA SECURITY

- Data security systems must focus on robust authentication mechanisms such as multi-factor authentication (MFA) to strengthen access controls and mitigate the risk of unauthorized access
- Compliance with data privacy regulations such as GDPR or CCPA is essential in protecting user data and maintaining trust with stakeholders.
- Continuous monitoring and incident response capabilities are vital to detect and respond swiftly to security incidents, minimizing potential data loss.
- The efficient use and responsible handling of resources become more important as data breaches can lead to significant financial and reputational damages.
- The rise in data breaches and unauthorized access highlights the importance of implementing advanced encryption techniques to protect sensitive information.
- User awareness and training programs play a critical role in reducing human error, which is often a major factor in data breaches.

1.4 PROBLEM STATEMENT

The problem statement addresses the concern of email service providers selling user data to third-party companies for their own financial gain. This practice raises security concerns as traditional network security measures are often inadequate in protecting sensitive information from increasing cybercrimes. To mitigate these risks, alternative techniques must be employed

for secure data transmission over networks. The project aims to explore various security techniques that can be combined to achieve higher levels of data security. By doing so, the project seeks to address the pressing need for improved security measures to safeguard data from unauthorized access, ensuring the privacy and confidentiality of users' information.

1.5 OBJECTIVES

- To develop a robust and secure image steganography technique by combining the AES encryption algorithm and the LSB embedding algorithm.
- To ensure the confidentiality and integrity of hidden information by leveraging the strength of AES encryption.
- To achieve imperceptible embedding of secret data within the image using the LSB algorithm, minimizing any visible changes to the image.
- To enhance the resistance against steganalysis techniques by employing AES encryption, making it difficult for unauthorized parties to detect and extract the hidden information.
- To evaluate the performance and effectiveness of the proposed AES-LSB steganography technique through experimentation and analysis, considering factors such as data hiding capacity, image quality preservation, and encryption strength.
- To explore potential applications of the AES-LSB technique in secure communication, digital watermarking, and covert data transmission, demonstrating its practicality and utility in real-world scenarios and digital watermarking.

CHAPTER 2
LITERATURE SURVEY

CHAPTER 2

LITERATURE SURVEY

1. The paper titled "A Hybrid Approach for Image Security by Combining Encryption and Steganography" by Jaspal Kaur Saini and Harsh K Verma proposes a hybrid approach for enhancing image security. The approach combines encryption using a modified version of the Advanced Encryption Standard (AES) algorithm and steganography. The AES algorithm is employed to encrypt the original image into a cipher image, and then steganography is utilized to hide the encrypted image within a cover image. The authors demonstrate through experimental results that this hybrid approach provides improved security against various attacks. The paper discusses the image encryption scheme, the image steganography technique used, and presents the proposed hybrid approach in detail. The experimental results and analysis, as well as the performance evaluation of the algorithm, are also included. The paper concludes by highlighting the effectiveness of the hybrid approach for image security..
2. The paper titled "Secure LSB Steganography over Modified Vigenère-AES Cipher and Modified Interrupt Key-AES Cipher" by Priya Paresh Bandekar1 and Suguna G C proposes two novel techniques for secure information hiding. The paper combines LSB-based image steganography with two newly proposed cryptography techniques: Vigenère-AES Cipher Steganography and Modified Interrupt Key-AES Cipher Steganography. These techniques aim to enhance the security of information hiding by using stego-keys and incorporating encryption algorithms such as AES. The paper discusses various related concepts and techniques. It explains the use of LSB steganography, which exploits the least significant bit of pixel intensities to hide information in digital images. The Vigenère cipher and AES encryption algorithm are introduced as cryptographic techniques to secure the message image. The paper also mentions the Diffie-Hellman key exchange algorithm for secure key transmission. Additionally, it provides an overview of the Advanced Encryption Standard (AES), highlighting its symmetric key algorithm and iterative block-based encryption process. the paper proposes a two-tier security approach by combining image steganography with cryptography techniques. It presents the working principles of the proposed techniques, discusses their advantages, and provides experimental results to demonstrate their efficiency.
3. The paper titled "A Performance Analysis of StegoCrypt Algorithm based on LSB-AES 128-bit in Various Image Sizes" by Eko Hari Rachmawanto, Rofi’ Syaiful Amin, De Rosal Ignatius Moses Setiadi and Christy Atika Sari provides a comprehensive on the combination of LSB and AES algorithms for data security. The authors highlight the increasing significance of data security

in internet transactions and the vulnerabilities that can lead to unauthorized access. They acknowledge previous studies that have proposed similar combinations, showcasing the growing interest in this research area. Various approaches, such as LSB-based filtering, AES encryption, and integration with random pixels, have been explored. The focus of the report is on analyzing the performance of the LSB-AES algorithm in relation to different cover image sizes. The authors evaluate the algorithm's imperceptibility using metrics like PSNR, MSE, and histogram analysis. The results demonstrate high imperceptibility values, indicating that the embedded message remains undetectable to human vision. The cryptographic performance of the algorithm is also evaluated in terms of time and entropy, with results showing strong cryptographic quality and effective encryption and decryption processes.. Overall, the LSB-AES algorithm proves effective in ensuring data security and maintaining image quality.

4. The paper titled “Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard” by Adit Pabbi, Rakshit Malhotra and Manikandan K proposes a method to increase the security of message sent using steganography along with AES encryption. The paper proposes a unique technique of image steganography by using discrete wavelet transformation and singular vector decomposition techniques where the focus is on changing the HH band. The algorithm’s SVD technique ensures hiding secret information without degradation in quality of the image. The experimental results for testing potency of attacks on the image suggest that the algorithm is quite resistant to image processing and geometric attacks. The PSNR, RMSE, MSSIM, FSIM and NCC values obtained in the experiments were also impressive suggesting that algorithm could be used in image steganography. There are as such no disadvantages of the algorithm apart from the complexity. This paper offers a way to use the LSB method of steganography while at the same time concurrently employing RSA, AES, DES and Blowfish algorithms in order to analyse them on several factors such as histogram equalization, encryption to decryption time and signal to noise ratio. Further, in this paper the encrypted information is hidden with the usage of LSB technique. This proposed methodology presents multiple layers of data security and this makes it difficult for the intruders to find out the original data. This paper uses a unique way of the usage of mixture of cryptography with steganography to encrypt and protect the data. It similarly analyses the experimental outcome to expose the quality of the final image.
5. The paper titled “Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm” by Nurhayati, Syukri and Sayyid Ahmad explores the use of steganography, specifically the Least Significant Bit (LSB) method, combined with the Advanced Encryption Standard (AES) algorithm for secure communication. The authors highlight

the increasing importance of data security in the face of cybercrime and the need to protect valuable and confidential information. They propose steganography as an alternative method to secure electronic messages, emphasizing its ability to hide secret messages within other data without arousing suspicion. The paper discusses the fundamentals of cryptography and steganography, distinguishing between the two techniques. It explains how cryptography transforms plaintext into unreadable ciphertext, while steganography focuses on concealing messages within a file without altering its appearance. The authors utilize the LSB method, which involves replacing the least significant bit of data in a digital image with the secret message. They combine this technique with the AES algorithm to encrypt the message before embedding it, enhancing the security of the hidden data.The research includes several experiments and analyses to evaluate the effectiveness of the proposed method. They assess imperceptibility by ensuring that the embedded message remains indistinguishable to the human eye. Fidelity tests confirm that the image quality is minimally affected after the insertion process. The authors also demonstrate successful message recovery, highlighting the application's ability to retrieve the hidden data. They conclude that the LSB-AES approach offers a reliable and relatively safe means of concealing and securing secret messages within digital images. The paper suggests further research to explore alternative steganographic methods and stronger encryption algorithms for improved security.

CHAPTER 3
METHODOLOGY

CHAPTER 3

METHODOLOGY

This chapter explains about the various components being used in the project and even description of the project. The system analysis includes block diagram and the software implementation of the complete project and its working.

3.1 EXISTING SYSTEM

Various systems are available for information hiding in an image, but they have some drawbacks i.e., they either do not encrypt the message or use a very weak algorithm in order to perform cryptography. They use the same key for encryption and decryption making it easy for the intruder to get access of the information. In some other cases the technique used may not be very efficient that is, the original image and the resulting image will be easily distinguishable by naked human eyes. For example DES algorithm, an encryption algorithm, used keys of smaller sizes (64 bit key) hence it was easy to decode it using computations. Algorithms using keys of these sizes are easily cracked by any intruder. So it is better if one goes for algorithms using keys of larger size which are difficult to decrypt and provide better security. Where stitching is concerned, multiband blending, gain compensation, automatic straightening makes the images smooth and more realistic.

3.2 PROPOSED SYSTEM

The proposed system aims to enhance data security in digital communication. It integrates advanced encryption and image steganography techniques to protect sensitive information during transmission. By utilizing robust encryption algorithms and LSB-based image steganography, the system ensures the confidentiality of the secret image and message. It also utilizes a cover image to conceal the existence of the hidden data. To prevent unauthorized access and data loss, the system splits the stego image into parts and indexes them for secure transmission. On the receiver's side, the sub-images are merged, decrypted, and the secret message is extracted using LSB extraction. The proposed system has real-world applications in financial services, defense, detective agencies, and secure document transportation, addressing the critical need for enhanced data security in today's digital landscape.

3.3 BLOCK DIAGRAM

The entire workflow is broken down into four phases. Initially the secret image is broken into multiple parts.

1. **Encryption phase** – In this phase AES algorithm is used to encrypt the secret message.
2. **Embedding phase** – Cipher text is hidden inside the image using LSB based image steganography algorithm.
3. **Hiding phase** – Kekre's Median Codebook Algorithm is used for image steganography. Image is segmented into parts and each part converted into vectors in this step. Part of secret image is hidden behind the cover image using steganography and the resulting image is sent across to the receiver's end.
4. **Stitching phase** - K-nearest neighbour supervised algorithm is used. SIFT features are extracted from all sub images. KNN is found for each feature using k-d tree. RANSAC is used to find geometrically consistent feature matches. Later connected components of image matches are found out.

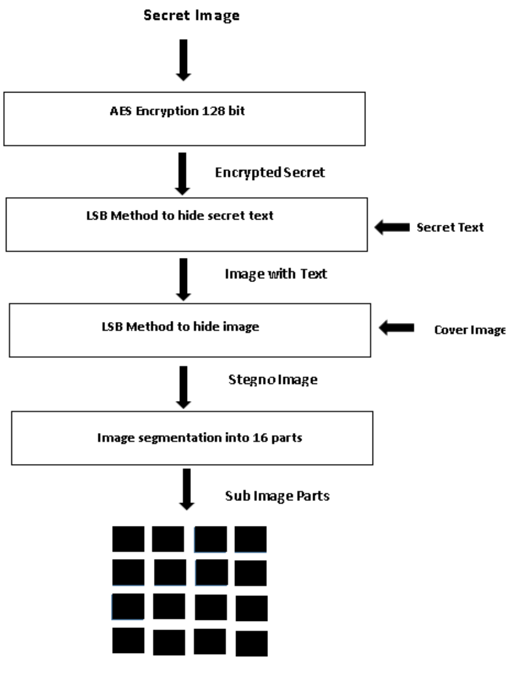


Figure 3.1: Sequence of steps performed by sender

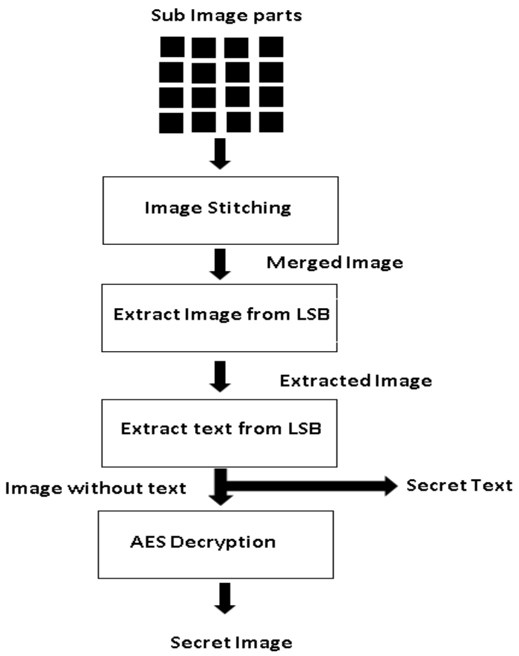


Figure 3.2: Sequence of steps performed by the receiver

3.4 IMPLEMENTATION AND RESULTS

Image encryption and decryption was implemented using the AES algorithm. Firstly, the given image was resized to a known size (480 x 480). Then the image was divided into Nx16 blocks. The sender and receiver use a key of 128 bits. This key must be shared between the sender and the receiver in a secure manner. The key can be imagined as blocks x[0],x[1]...x[15], where each block is 8 bits long.

AES Encryption is done in rounds, where we process 16 pixels in each round. The AES algorithm uses a round function that is composed of four different byte related transformations:

- **SubBytes step:** Each value in the state matrix (original image) is replaced with a subbyte using an 8-bit substitution box (S-box). This ensures non-linearity in the cipher. The S-box is constructed by combining the inverse function with an invertible affine transformation. An 8-bit lookup table is used to replace each byte in the state S as, b[i,j]= S(a[i, j]).
- **Shift Rows step:** The bytes in each row are shifted by a certain offset to the left that increases iteratively. The first row is left unchanged. Each byte of the second row is moved one byte to the left cyclically. Similarly, the third and fourth rows are moved by offsets of two and three accordingly.
- **Mix Columns step:** The four blocks of each column of the state are joined using an invertible linear transformation like multiplication followed by bitwise XOR. This function takes four bytes as input and outputs four bytes. Addition is a simple XOR operation. Multiplication is modulo irreducible polynomial. Each column of the state is multiplied with a fixed polynomial c(x).
- **Add Round Key step:** The state and sub key are combined. Using the main key, a sub key is found. The sub key is added by XORing a byte from the state with its respective byte form the sub key.

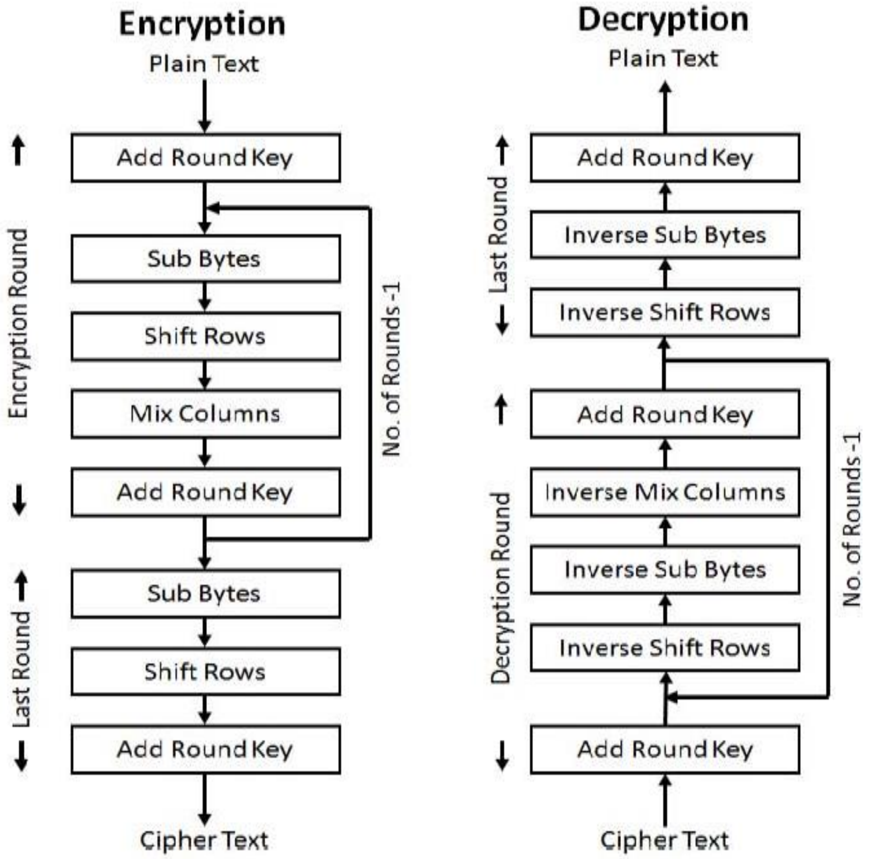


Figure 3.3 Block diagram of AES algorithm

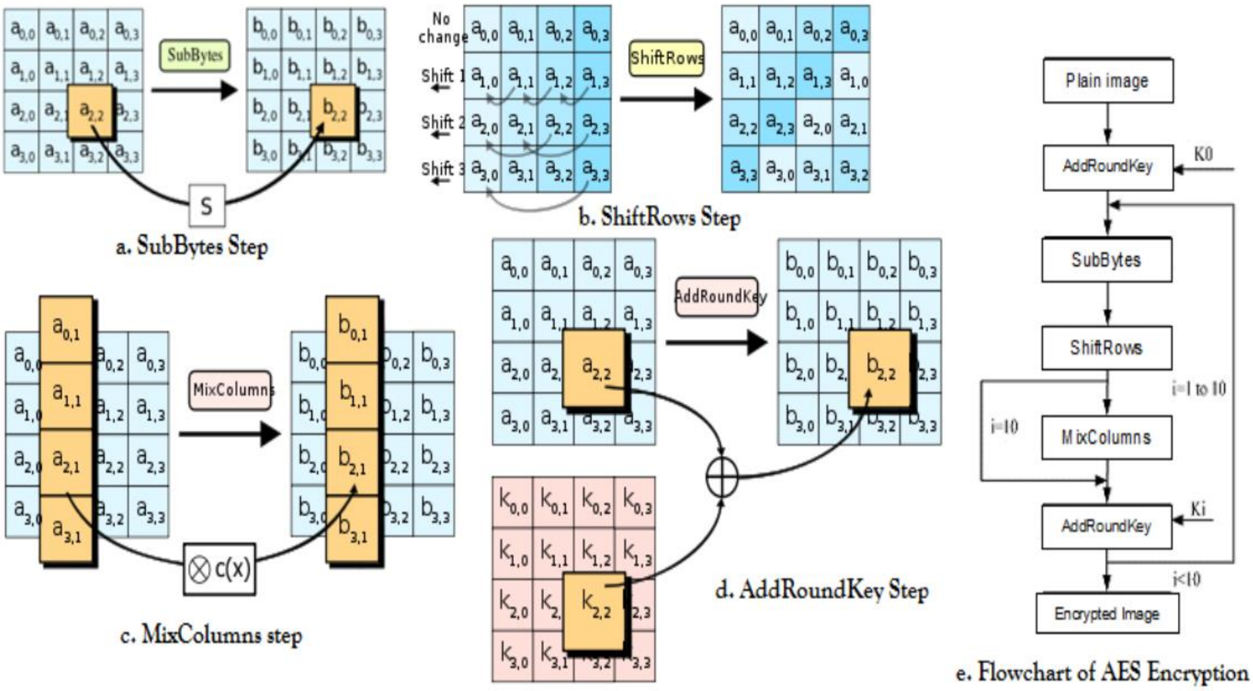


Figure 3.4 AES algorithm sub blocks diagram

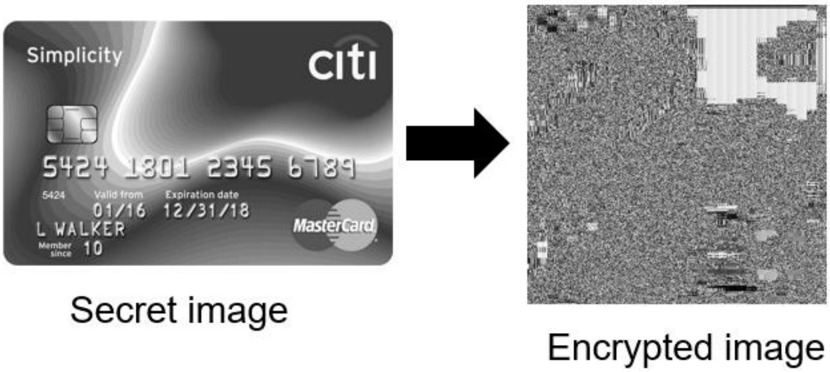


Figure 3.5 AES algorithm performed on the secret image

After encrypting the secret image, least significant bit based image steganography is performed to hide the secret message in the secret image. We append a null character with the secret text to denote the end-of-text. LSB based image steganography involves hiding data in the least significant bits of an image as it contains the least amount of information in an image and flipping them will not cause a significant change in the appearance of the image. The secret message is converted into its ASCII representation. These ASCII values are converted into their 8-bit binary representation. The least significant bits of the pixel values of the secret image are replaced with these bits in order. Hence the secret text is successfully hidden inside the secret image.

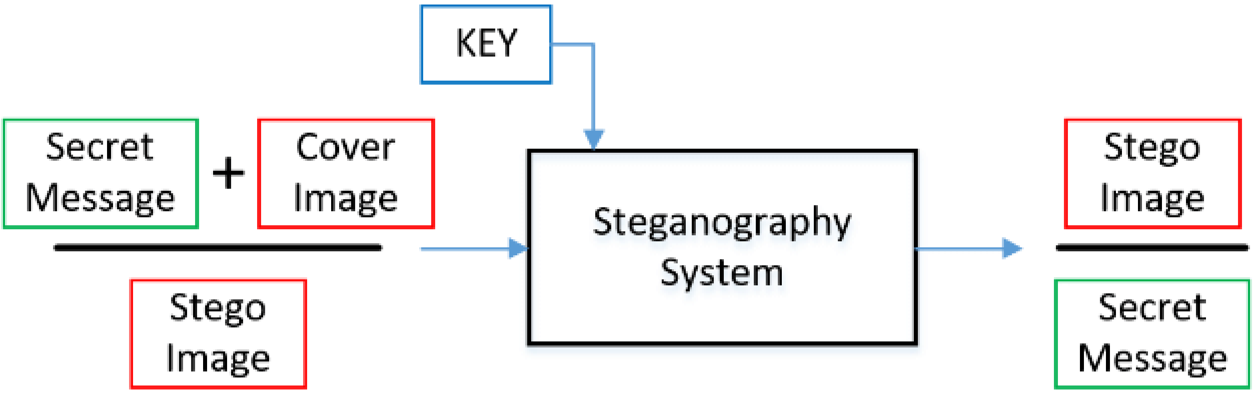


Figure 3.6: LSB based image steganography block diagram

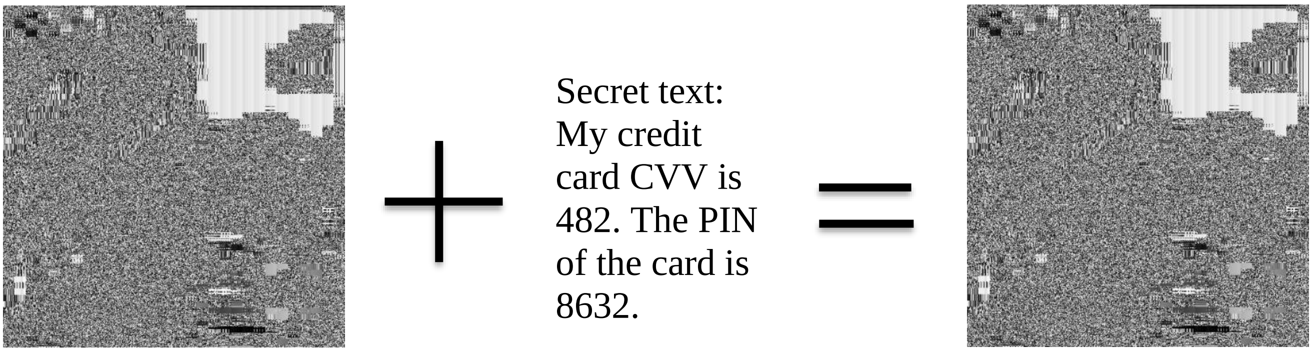

Secret text: My credit card CVV is 482. The PIN of the card is 8632.

Figure 3.7: Hiding of secret key inside the encrypted secret image

Similar to the method of LSB based image steganography that involved hiding the secret message into the secret image, the encrypted secret image containing the secret text is hidden inside the cover image using the same technique. The binary representation of the pixel values of the encrypted image with the secret text in it is hidden first in the red component, followed by the blue and the green components of the cover image.

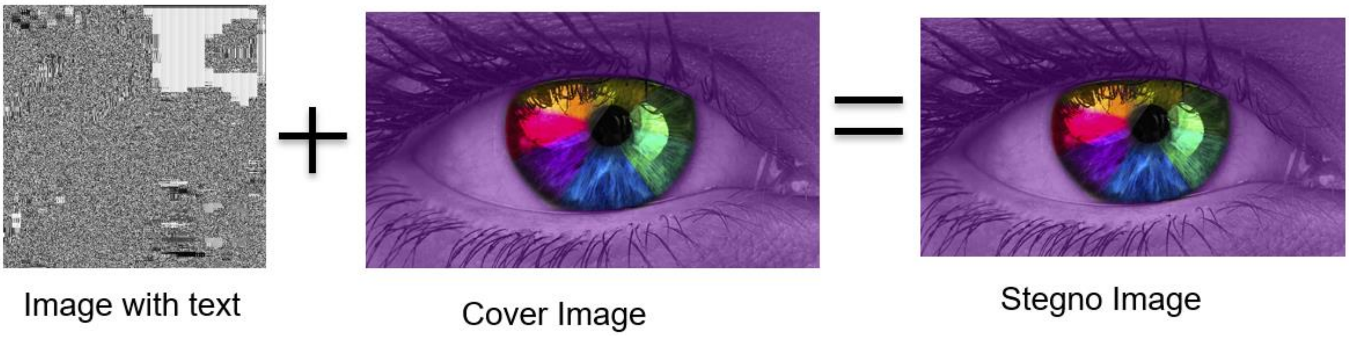


Image with text

Cover Image

Stegno Image

Figure 3.8: Hiding of encrypted image containing the secret text inside the cover image

Next, we divide the cover image with the encrypted secret image and the secret text embedded in it into multiple parts (16 to be specific). Each part is then separately sent to the recipient.

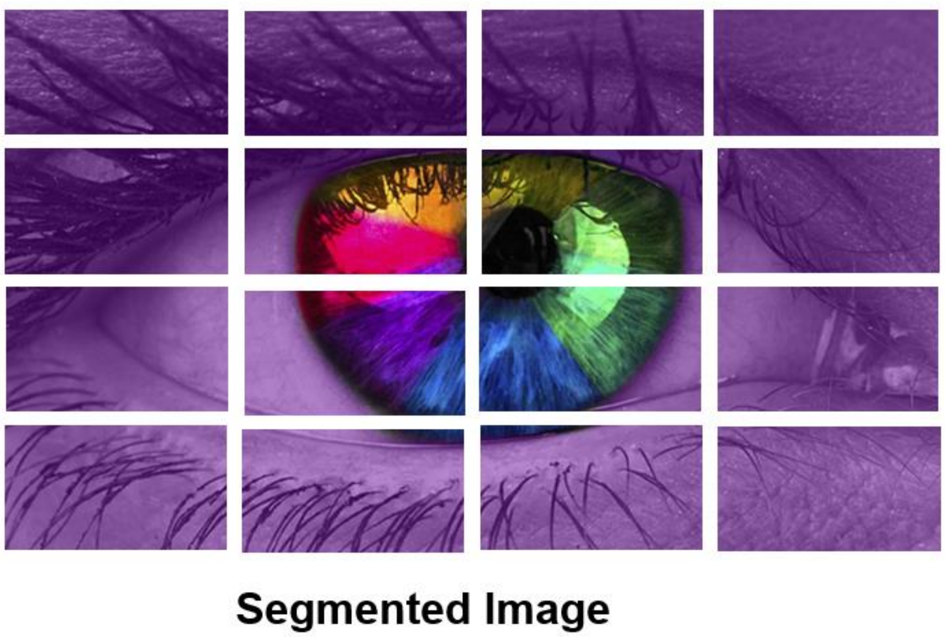


Figure 3.9: Segmentation of the stego image

On the receiver's end, the sub images are stitched back based on their index values (0 to 15) to regain the original cover image.

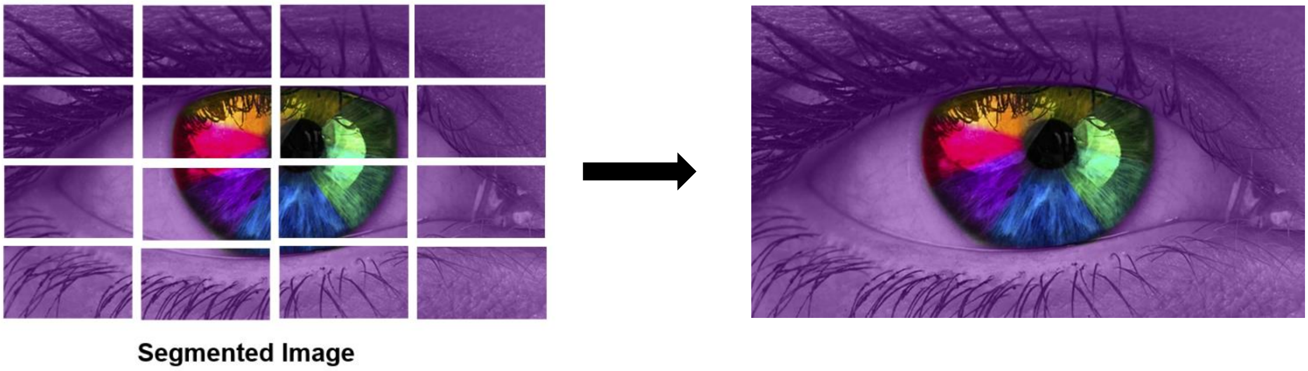
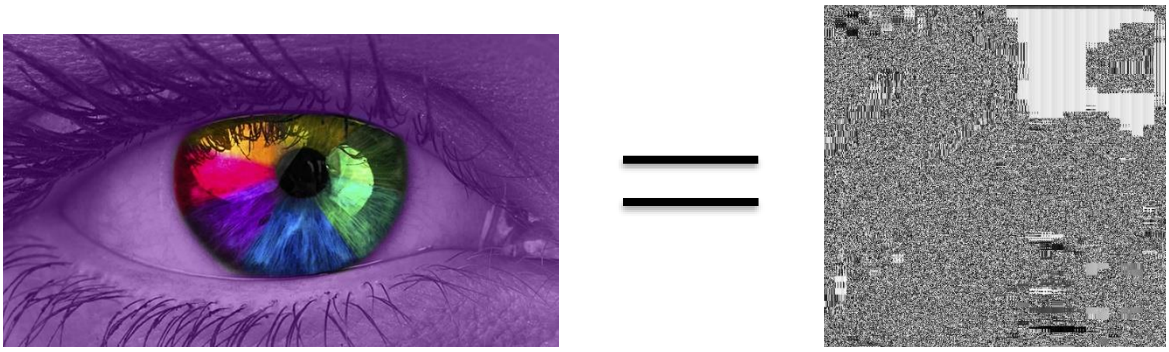


Figure 3.10: Stitching of sub images into a single image

The least significant bits of the red, blue and the green components are extracted 8-bits at a time for the entire size of the secret image. Now, we obtain the encrypted secret image with the secret text embedded in it.



Merged Image Containing Information

Encrypted Image + Secret Text in it

Figure 3.11: Extracting the encrypted image from the least significant bits of the stego image

From this secret image, the least significant bits are extricated, 8 bits at once, until we hit a number representing a zero. These 8 bit binary numbers obtained are converted to their decimal representation. These decimal representations represent the ASCII values of the characters. They are then converted back to their character representation to obtain the secret message.

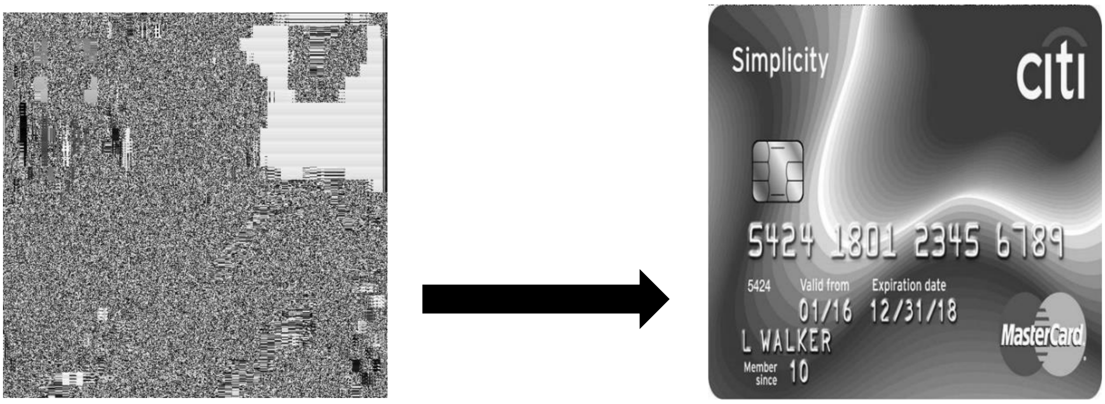
Secret text: My credit card CVV is 482. The PIN of the card is 8632.

Secret text

Encrypted Image + Secret Text in it

Figure 3.12: Extracting the secret text from the encrypted image

After the inverse substitution, the decryption process moves on to the final step, which is the Inverse Shift Rows. In this step, the rows of the image are shifted back to their original positions, undoing the row shifting applied during encryption. This ensures that the image is restored to its original layout. Once the Inverse Shift Rows step is completed, the process moves to the last round of the decryption. This round consists of the Add Round Key operation, where the round key used for encryption is applied again to the image. This step effectively undoes the XOR operation performed during encryption, restoring the original pixel values of the secret image. By performing these reverse operations in the decryption process, the receiver is able to obtain the secret image that was encrypted using the AES algorithm by the sender.



Encrypted image Decrypted image

Figure 3.13: Decrypting the encrypted image using AES Algorithm

CHAPTER 4
CONCLUSION

CHAPTER 4

CONCLUSION AND FUTURE WORK

4.1 CONCLUSION

In conclusion, the proposed system combines AES encryption, image steganography, and image stitching to provide a highly secure method for data and image encryption. By leveraging these techniques, the system ensures that transmitted data remains protected from unauthorized access. The AES encryption conceals the original content, enhancing confidentiality. The LSB-based image steganography further hides the secret message within the encrypted image, making it difficult for potential attackers to detect its existence. The inclusion of a cover image as a decoy adds an extra layer of camouflage, making the hidden information even more elusive.

Moreover, breaking down the stego image into multiple parts and transmitting them separately enhances security. Even if an intruder intercepts a subset of the sub-images, they would lack the complete information required to decipher the secret message or image. The system's ability to embed the secret image and message within the cover image using LSB-based steganography provides an added layer of protection against data interception. In the event of an interception, the hidden information remains intact and secure, minimizing the risk of unauthorized access. These features make the proposed technique valuable in industries dealing with confidential data, such as defense, finance, or research.

Overall, the integration of AES encryption, image steganography, and image stitching offers a comprehensive solution to address the challenges of data security and privacy. The system provides a highly secure and efficient method for secure communication and data transmission. It finds practical applicability in various sectors and can safeguard sensitive information, making it a valuable tool in combating cybercrimes and ensuring data confidentiality in today's interconnected world. By protecting confidential images and messages, the system contributes to the overall goal of safeguarding sensitive data and maintaining privacy in an increasingly digital landscape.

Furthermore, the proposed system not only focuses on data security but also ensures a visually appealing and seamless output through image stitching. By leveraging invariant local features and probabilistic models for image matching, the system automatically recognizes and stitches multiple panoramas, providing users with a visually coherent result. This feature enhances the overall user experience and demonstrates the system's versatility in handling both security and aesthetic aspects of image encryption.

In addition, the integration of AES encryption, image steganography, and image stitching in a single system offers a streamlined and efficient approach to secure data transmission. Users can benefit from the convenience of a unified solution that incorporates multiple layers of protection, minimizing the need for separate tools or complex integration processes. This further strengthens the practicality and effectiveness of the proposed system in various domains where data confidentiality and visual presentation are equally crucial.

4.2 APPLICATION

1. Secure Communication: The system can be used to ensure secure communication in various industries, including finance, healthcare, legal services, and government sectors.
2. Banking and Financial Services: It can be implemented to protect sensitive financial data during online transactions, securing customer information, and preventing unauthorized access to financial systems.
3. Defense and Military: The system's robust encryption and steganography techniques can assist defense organizations in transmitting classified information securely, enhancing national security measures.
4. Detective Agencies: Investigators and detective agencies can utilize the system to securely share sensitive case-related information, maintaining the privacy and integrity of their investigation.
5. Digital Rights Management: The system can support digital rights management by protecting copyrighted content from unauthorized access and distribution.
6. Secure Password and Key Exchange: The project can be used to securely exchange passwords, encryption keys, and other sensitive authentication information, strengthening overall system security.
7. Healthcare Industry: The system can ensure the secure transmission of sensitive patient data and medical records between healthcare providers, safeguarding patient privacy and compliance with data protection regulations.

4.3 FUTURE WORK

- **Robustness Analysis:** It emphasizes the need for a comprehensive analysis of the proposed technique's robustness. This analysis involves conducting thorough testing against various attacks and potential vulnerabilities. It includes evaluating the system's resilience against steganalysis techniques designed to detect hidden data, cryptographic attacks aimed at breaking the encryption, and image processing algorithms that could potentially compromise the hidden information. The objective is to ensure that the system maintains its security under different threat scenarios, providing confidence in its ability to protect the concealed data and withstand potential attacks from adversaries.

- **Optimal Image Fragmentation:** Investigate and develop algorithms to optimize the fragmentation of the stego image for transmission. This includes studying the trade-off between the number of sub-images and the transmission efficiency, as well as exploring techniques to ensure efficient and reliable reassembly of the sub-images at the receiver's end.
- **Network Security Integration:** Integrate the proposed technique with existing network security measures, such as secure transmission protocols (e.g., SSL/TLS) or intrusion detection systems (IDS), to create a comprehensive security framework. Evaluate the performance and compatibility of the system in real-world network environments, considering factors like latency, throughput, and scalability.
- **Usability and User Interface Enhancements:** Pay attention to the usability aspects of the system by improving the user interface and overall user experience. Conduct user studies to gather feedback on the system's ease of use, intuitiveness, and efficiency, and implement necessary enhancements to make it more user-friendly

REFERENCES

[1] Nandhini Subramanian, Omar Elharrouss, Somaya AlMaadeed and Ahmed Bouridane, *“Image Steganography: A Review of the Recent Advances”*, (2021)

[2] Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, *“An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography”*, (2019)

[3]Vikas Singhal, Yash Kumar Shukla, Navin Prakash, *“Image Steganography embedded with Advance Encryption Standard (AES) securing with SHA-256”,* (2020)

[4] Mustafa S. Abbas, Suadad S. Mahdi and Shahad A. Hussien, *“Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography”*, (2020)

[5]Gurpreet Singh and Supriya proposed a paper *“A Study of Encryption Algorithms (RSA,DES, 3DES and AES) for information security”*, 2015.

[6] Qi Zang and Qunding proposed paper byname *“Digital Image Encryption based onAdvanced Encryption Standard [AES] algorithm”,*2015 fifth international conferenceon instrumentation and measurement,computer, communication and control.

[7]Harpreet Kaur and Ajay Kakkar proposed a paper *“Comparison of different image formatsusing LSB steganography”,* 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC).

[8] S.M Masud Karim, Md.Saifur Rahman, Md.Ismail Hossain presented a paper *“A new approach for LSB based image steganography using secrete key”,*14 th international conference on computer and information technology, December,2011.

[9] Aman Arora, Manish Pratap Singh, Prateek Thakral, Naveen Jarwal proposed a paper by name *“Image steganography using Enhanced LSB substitution technique”*,2016 fourth international conference on Parallel, Distributed and Grid Computing.

[10]Priya Deshmukh presented a paper on *“An image encryption and decryption using AES algorithm”*, International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016.

[11] Z. Y. Al-Omari and A. T. Al-Taani, *“Secure LSB steganography for coloured images using character-colour mapping,”* 2017 8th International Conference on Information and Communication Systems (ICICS), 2017, pp. 104-110.

[12] D. Samidha and D. Agrawal, *“Random image steganography in spatial domain,”* 2013 International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), 2013, pp. 1-3.

[13] Ali K. Hmood B. B. Zaindan, *“An overview on hiding information techniques in images,”* journal of applied sciences, vil. 10, no. 18, 2010.

[14] *“Automatic Panoramic Image Stitching using Invariant Features”,* Matthew Brown and David G. Lowe of Computer Science,University of British Columbia, Vancouver, Canada.

[15] *“High payload using mixed codebooks of Vector Quantization”*, H. B. Kekre, Tanuja K. Sarode, ArchanaAthawale, KalpanaSagvekar.

APPENDIX

CODE

We are implementing the proposed system on MATLAB R2023a software. MATLAB is a powerful software environment widely used in scientific and engineering fields for data analysis, algorithm development, and numerical computation. It provides a user-friendly programming language that allows users to solve complex mathematical problems, visualize data, and create interactive plots and graphs. MATLAB offers a vast array of built-in functions and toolboxes, making it convenient for tasks such as signal processing, image and video processing, machine learning, and control systems design. Its intuitive interface and extensive documentation make it accessible for both beginners and experienced programmers, enabling efficient prototyping and development of applications in various domains.

Figure 4.1: MATLAB R2023a

SENDER PART CODE

1. SENDER

```
%% Adding path of libraries
addpath('C:\Users\Varsha\Desktop\Image-Steganography\Sender\Library');
%% Reading the secret image and cover image
secret_img = imread('C:\Users\Varsha\Desktop\Image-
Steganography\Sender\secret_img.jpg');
cover_img = imread('C:\Users\Varsha\Desktop\Image-
Steganography\Sender\cover_img.jpg');

cov_size = size(cover_img);
sec_size = size(secret_img);
if(sec_size(1)*sec_size(2) * 8 > cov_size(1)*cov_size(2)*cov_size(3))
    disp('Cover image too small for the secret image');
    return;
```

```
end

%% Setting the secret message to be send to the receiver
secret_msg = 'My credit card CVV is 482. The PIN of this card is 8632.';

%% Step 1 - AES Encyption of secret image
encrypted_img = aes_encryption(secret_img);

if((length(secret_msg)+1)*8 > sec_size(1)*sec_size(2))
    disp('Secret message too long to be fit into the secret message');
    return;
end
%% Step 2 - LSB based steganography to hide secret message in the encrypted
secret image
img_with_text = lsbstego(encrypted_img, secret_msg);
%% Step 3 - LSB based steganography to hide encryped secret image with text
into the cover image
stego_img = embedding(cover_img, img_with_text);
%% Step 4 - Split the images to be sent to the receiver
splitimage(stego_img);
% Create a new figure window
figure;
imshow(secret_img);
title('Secret Image');
figure;
imshow(cover_img);
title('Cover Image');
figure;
imshow(encrypted_img);
title('Encrypted Image');
figure;
imshow(uint8(img_with_text));
title('Image with Text');
figure;
imshow(stego_img);
title('Stego Image');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img0.tif');
title('Image 0');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img1.tif');
title('Image 1');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img2.tif');
title('Image 2');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img3.tif');
title('Image 3');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img4.tif');
title('Image 4');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img5.tif');
title('Image 5');
figure;
```

```
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img6.tif');
title('Image 6');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img7.tif');
title('Image 7');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img8.tif');
title('Image 8');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img9.tif');
title('Image 9');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img10.tif');
title('Image 10');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img11.tif');
title('Image 11');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img12.tif');
title('Image 12');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img13.tif');
title('Image 13');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img14.tif');
title('Image 14');
figure;
imshow('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img15.tif');
title('Image 15');
% The images that have been split and saved as img[0-15].tif must be
% shipped to the receiver.
```

2. AES Encryption

```
function [encrypt_o] = aes_encryption (input_img)
%% SD Dimension
SD_Rw = 480;
SD_Cl = 480;
%% Image Read
image_in = imresize(input_img, [SD_Rw SD_Cl]);
%% Divide image in to Nx16 block
image_x_16 = double(reshape(image_in', 16,(SD_Rw*SD_Cl/16))');
%% Key
key = 0:15;
key = mod(key, 256);
key_i = repmat(key, size(image_x_16,1), 1);
%% Encryption
s_box_o = s_box_fun(image_x_16);
shift_rows_o = shift_rows_fun(s_box_o);
mix_col_o = mix_column_fun(shift_rows_o);
xor_key_o = bitxor(mix_col_o, key_i);
encrypt_o = uint8(reshape(xor_key_o', SD_Cl, SD_Rw)');
imwrite(encrypt_o, 'C:\Users\Varsha\Desktop\Image-Steganography\Sender\1-
encrypted.tif'); %Write the input to the disk
```

3. Embedding

```
function [newimg] = embedding(cov_img, secret_img)
%%Embedding image inside images
size_sec = size(secret_img);
secret1d = reshape(secret_img, 1, size_sec(1)*size_sec(2));
%Declaration of variables to control the insertion of encrypted image into
%the cover image
[siz1, siz2, ~] = size(cov_img);
plane = 1;
colplane = cov_img(:,:,plane);
newimg = []; %Output image - cover image with secret image embedded in it
c1 = 1; c2 = 1;

%% Embedding the secret image in the least significant bits of the cover image
for i = 1:length(secret1d)
    temp = de2bi(secret1d(i), 8);
    for j = 8:-1:1
        val = colplane(c1, c2);
        val = floor(double(val)/2) * 2;
        colplane(c1, c2) = bitor(val,temp(j));
        c2 = c2+1;
        if c2 > siz2
            c2 = 1;
            c1 = c1 + 1;
            if c1 > siz1
                c1 = 1;
                c2 = 1;
                newimg = cat(3, newimg, colplane);
                plane = plane + 1; %Embedding it in the next plane on exhaustion
of current plane
                colplane = cov_img(:,:,plane);
            end
        end
    end
end
newimg = cat(3, newimg, colplane);
%Inserting back the remaining color plains into the output image
for i = plane+1:3
    newimg = cat(3, newimg, cov_img(:,:,i));
end

imwrite(newimg, 'C:\Users\Varsha\Desktop\Image-Steganography\Sender\3-
embedded_image.tif');
```

4. LSB stego

```
function [secret_img] = lsbstego(secret_img, text)
%% Data Hiding
secret_img=double(secret_img);
val = [double(text) 0]; %Coverting secret text to ASCII representation
[~, siz2] = size(secret_img);
i = 1; j = 1;
for y = 1:length(val)
    data = val(y); %data is the character in the secret text to be hidden
    bit = 128; %Counter variable
    while bit > 0 %Clearing the LSB of a pixel
        secret_img(i, j) = floor(secret_img(i, j)/2);
        secret_img(i, j) = secret_img(i, j)*2;
        if bitand(data, bit) > 0 %Setting the LSB of pixel to the information bit
            secret_img(i, j) = secret_img(i,j)+1;
        end
        j = j+1;
        if j > siz2
            i = i+1;
            j = 1;
        end
        bit = floor(bit/2);
    end
end
imwrite(uint8(secret_img), 'C:\Users\Varsha\Desktop\Image-Steganography\Sender\2-
image_with_text.tif'); %writing the stego image into a new file
```

5. Mix coloumn function

```
function [mix_column_out] = mix_column_fun (mix_column_in)

idx_1 = 1:16;
idx_2 = [idx_1(5:16) idx_1(1:4)];
idx_3 = [idx_2(5:16) idx_2(1:4)];


idx_4 = [idx_3(5:16) idx_3(1:4)];

data_in_mul_2 = mix_column_in * 2;
mask = bitget(data_in_mul_2, 9)*27;
mul_2 = bitxor(mod(data_in_mul_2, 256), mask);

data_in_mul_3 = bitxor(data_in_mul_2, mix_column_in);
mask = bitget(data_in_mul_3, 9)*27;
mul_3 = bitxor(mod(data_in_mul_3, 256), mask);

mix_column_out = bitxor(bitxor(mul_2(:,idx_1), mul_3(:,idx_2)),
bitxor(mix_column_in(:,idx_3), mix_column_in(:,idx_4)));
```

6. S box function

```
function [s_box_out] = s_box_fun(s_box_in)

rw = size(s_box_in, 1);
cl = size(s_box_in, 2);

s_box_in = reshape(s_box_in', rw*cl, 1)';

s_box_table = [ 99,124,119,123,242,107,111,197,48,1,103,43,254,215,171,118 ...
                202,130,201,125,250,89,71,240,173,212,162,175,156,164,114,192 ...
                183,253,147,38,54,63,247,204,52,165,229,241,113,216,49,21 ...
                4,199,35,195,24,150,5,154,7,18,128,226,235,39,178,117 ...
                9,131,44,26,27,110,90,160,82,59,214,179,41,227,47,132 ...
                83,209,0,237,32,252,177,91,106,203,190,57,74,76,88,207 ...
                208,239,170,251,67,77,51,133,69,249,2,127,80,60,159,168 ...
                81,163,64,143,146,157,56,245,188,182,218,33,16,255,243,210 ...
                205,12,19,236,95,151,68,23,196,167,126,61,100,93,25,115 ...
                96,129,79,220,34,42,144,136,70,238,184,20,222,94,11,219 ...
                224,50,58,10,73,6,36,92,194,211,172,98,145,149,228,121 ...
                231,200,55,109,141,213,78,169,108,86,244,234,101,122,174,8 ...
                186,120,37,46,28,166,180,198,232,221,116,31,75,189,139,138 ...
                112,62,181,102,72,3,246,14,97,53,87,185,134,193,29,158 ...
                225,248,152,17,105,217,142,148,155,30,135,233,206,85,40,223 ...
                140,161,137,13,191,230,66,104,65,153,45,15,176,84,187,22];

s_box_out = s_box_table(s_box_in + 1);


s_box_out = reshape(s_box_out', cl, rw)';
```

7. Shift rows function

```
function [shift_rows_out] = shift_rows_fun (shift_rows_in)

idx = [1 2 3 4 6 7 8 5 11 12 9 10 16 13 14 15];

shift_rows_out = shift_rows_in(:, idx);
```

8. Split image

```
function [] = splitimage(out_img)
%% Splitting of image into 16 sub images for transmission of data
%Initializing the required variables
[s1, s2, ~] = size(out_img);
i = 1;
j = 1;
in = 0;
cond = true;

%Running a while loop to split the image into sub-images as required
while (cond)
    img = out_img(i:i+(s1/4)-1, j:j+(s2/4)-1,:); %Splitting the image into 16
equal parts using s1/4 and s2/4
    j = j+(s2/4);
    if j > s2
        i = i+(s1/4);
        j = 1;
        if i > s1
            cond = false;
        end
    end
    imwrite(img, strcat('C:\Users\Varsha\Desktop\Image-Steganography\Sender\img',
num2str(in), '.tif')); %write every image into the disk as img(num).tif
    in = in + 1;
end
```

RECEIVER PART CODE

1. Receiver

```
%% Adding path of libraries
addpath('C:\Users\Varsha\Desktop\Image-Steganography\Receiver\Library');
%% Merge images received by the receiver
merged_img = mergeimg();
%% Extract encrypted image from the merged image
encrypted_img = extract_img(merged_img);
%% Extract secret text from the encrypted image
secret_text = extract_text(encrypted_img);
disp(strcat('Secret Text : ', secret_text));
%% Extract original secret image from encrypted secret image
secret_img = decryption(encrypted_img);
imwrite(secret_img, 'C:\Users\Varsha\Desktop\Image-
Steganography\Sender\SECRET_IMAGE.jpg');

figure;
imshow(merged_img);
title('Merged Image');
figure;
imshow(uint8(encrypted_img));
title('Extracted Secret Image');
figure;
imshow(secret_img);
title('Secret Image Received');
```

2. Decryption

```
function [decrypt_o] = decryption (encrypt_o)
%% SD Dimension
SD_Rw = 480;
SD_Cl = 480;

%% Key
key = 0:15;
key = mod(key, 256);
key_i = repmat(key, SD_Rw*SD_Cl/16, 1);

%% Divide image in to Nx16 block
image_x_16 = double(reshape(encrypt_o', 16, (SD_Rw*SD_Cl/16))');

%% Decryption
xor_key_o = bitxor(image_x_16, key_i);
inv_mix_col_o = inv_mix_column_fun(xor_key_o);
inv_shift_rows_o = inv_shift_rows_fun(inv_mix_col_o);
inv_s_box_o = inv_s_box_fun(inv_shift_rows_o);
decrypt_o = uint8(reshape(inv_s_box_o', SD_Cl, SD_Rw)');

%% Write output to disk
imwrite(decrypt_o, 'C:\Users\Varsha\Desktop\Image-Steganography\Sender\5-
decrytped_img.tif');
```

3. Extract image

```
function [sec_img] = extract_img(newimg2)
%% Extracting the secret image
secsiz1 = 480;
secsiz2 = 480;
condition = true;
[siz1, siz2, ~] = size(newimg2);
plane = 1;
pix = 0;
npix = secsiz1 * secsiz2;
sec_img = [];
colplane = newimg2(:,:,plane);
c1 = 1; c2 = 1;
one = 1;

%Extracting the data in every pixel from the least significant bit
while condition
    num = 0;
    %Extracting one pixel of secret image
    for i = 1:8
        bit = bitand(colplane(c1, c2), one);
        num = (num * 10) + double(bit);
        c2 = c2 + 1;
        if c2 > siz2
            c2 = 1;
            c1 = c1 + 1;
            if c1 > siz1
                c1 = 1;
                plane = plane + 1;
                colplane = newimg2(:,:,plane);
            end
        end
    end
    pix = pix + 1;
    num = bin2dec(num2str(num));
    sec_img = [sec_img num];
    if pix >= npix
        condition = false;
    end
end

%sec_img is a linear array. Hence, we will need to reshape it back to it's
%original dimensions
sec_img = reshape(sec_img, secsiz1, secsiz2);
imwrite(uint8(sec_img), 'C:\Users\Varsha\Desktop\Image-Steganography\Sender\4-
extract_secret_image.tif');
```

4. Extract text

```
function [secret_text] = extract_text(stego_img)
%% Extracting hidden data from the stego image
data=[]; %Extracted secret information
[~, siz2] = size(stego_img);
condition = true;
```

```
i = 1;
j = 1;
while condition
    k = 8;
    num = 0;
    while k > 0 %Obtaining the binary representation of a character in the hidden
text
        num = (num*10) + bitand(stego_img(i, j),1);
        k = k - 1;
        j = j+1;
        if j > siz2
            i = i+1;
            j = 1;
        end
    end
    data = [data num]; %Adding the obtained binary representation of character of
the secret information
    if num == 0 %Checking if the last character read was a 'null character'
        condition = false;
    end
end
secret_text=[];
for i = 1:length(data)
    secret_text = [secret_text bin2dec(num2str(data(i)))]; %Converting the binary
numbers to ASCII values
end
secret_text = char(secret_text); %Coverting the ASCII value to characters
```

5. Inverse mix column function

```
function [inv_mix_column_out] = inv_mix_column_fun (inv_mix_column_in)

idx_1 = 1:16;
idx_2 = [idx_1(5:16) idx_1(1:4)];
idx_3 = [idx_2(5:16) idx_2(1:4)];
idx_4 = [idx_3(5:16) idx_3(1:4)];

data_in_mul_2 = inv_mix_column_in * 2;
mask = bitget(data_in_mul_2, 9)*27;
mul_2 = bitxor(mod(data_in_mul_2, 256), mask);

data_in_mul_4 = mul_2 * 2;
mask = bitget(data_in_mul_4, 9)*27;
mul_4 = bitxor(mod(data_in_mul_4, 256), mask);

data_in_mul_8 = mul_4 * 2;
mask = bitget(data_in_mul_8, 9)*27;
mul_8 = bitxor(mod(data_in_mul_8, 256), mask);
mul_9 = bitxor(mul_8, inv_mix_column_in);
mul_b = bitxor(bitxor(mul_8, mul_2), inv_mix_column_in);
mul_d = bitxor(bitxor(mul_8, mul_4), inv_mix_column_in);
mul_e = bitxor(bitxor(mul_8, mul_4), mul_2);
inv_mix_column_out = bitxor(bitxor(mul_e(:,idx_1), mul_b(:,idx_2)),
bitxor(mul_d(:,idx_3), mul_9(:,idx_4)));
```

6. Inverse S – box function

```
function [inv_s_box_out] = inv_s_box_fun(inv_s_box_in)

rw = size(inv_s_box_in, 1);
cl = size(inv_s_box_in, 2);
inv_s_box_in = reshape(inv_s_box_in', rw*cl, 1)';

inv_s_box_table = [ 82,9,106,213,48,54,165,56,191,64,163,158,129,243,215,251 ...
                    124,227,57,130,155,47,255,135,52,142,67,68,196,222,233,203
...
                    84,123,148,50,166,194,35,61,238,76,149,11,66,250,195,78 ...
                    8,46,161,102,40,217,36,178,118,91,162,73,109,139,209,37 ...
                    114,248,246,100,134,104,152,22,212,164,92,204,93,101,182,146
...
                    108,112,72,80,253,237,185,218,94,21,70,87,167,141,157,132 ...
                    144,216,171,0,140,188,211,10,247,228,88,5,184,179,69,6 ...
                    208,44,30,143,202,63,15,2,193,175,189,3,1,19,138,107 ...
                    58,145,17,65,79,103,220,234,151,242,207,206,240,180,230,115
...
                    150,172,116,34,231,173,53,133,226,249,55,232,28,117,223,110
...
                    71,241,26,113,29,41,197,137,111,183,98,14,170,24,190,27 ...
                    252,86,62,75,198,210,121,32,154,219,192,254,120,205,90,244
...
                    31,221,168,51,136,7,199,49,177,18,16,89,39,128,236,95 ...
                    96,81,127,169,25,181,74,13,45,229,122,159,147,201,156,239 ...
                    160,224,59,77,174,42,245,176,200,235,187,60,131,83,153,97 ...
                    23,43,4,126,186,119,214,38,225,105,20,99,85,33,12,125];

inv_s_box_out = inv_s_box_table(inv_s_box_in + 1);

inv_s_box_out = reshape(inv_s_box_out', cl, rw)';
```

7. Inverse shift rows function

```
function [inv_shift_rows_out] = inv_shift_rows_fun (inv_shift_rows_in)

idx = [1 2 3 4 8 5 6 7 11 12 9 10 14 15 16 13];
inv_shift_rows_out = inv_shift_rows_in(:, idx);
```

8. Merging image

```
function [out] = mergeimg()
%% Merging of input image files back to the original image on the receiver's end
for i = 0:3
    for j = 0:3
        temp = imread(strcat('C:\Users\Varsha\Desktop\Image-
Steganography\Sender\img', num2str(4*i + j), '.tif'));
        if j == 0
            img = temp;
        else
            img = [img temp];
        end
    end
    if i == 0
        out = img;
    else
        out = [out; img];
    end
end
imwrite(out, 'C:\Users\Varsha\Desktop\Image-Steganography\Sender\1-
merged_image.tif');
```