DECLARATION

We the undersigned solemnly declare that the project report "**STEGANOGRAPHY BASED WEB PROJECT**" is based on my own work carried out during the course of our study under the supervision of **Asst. Professor Bharti Dubey, CSE PIT, Vadodara**.

We assert the statements made and conclusions drawn are the outcomes of my own work. I further certify that

1. The work contained in the report is original and has been done by us under the general supervision of our supervisor.
2. The work has not been submitted to any other Institution for any other degree / diploma / certificate in this university or any other University of India or abroad.
3. We have followed the guidelines provided by the university in writing the report.

Whenever we have used materials (data, theoretical analysis, and text) from other sources, we have given due credit to them in the text of the report and giving their details in the references.

AAYUSH RAJ THAKUR **SIGNATURE:-**

JITESH N. SONWANE **SIGNATURE:-**

TEJAS SANDIP BORASE **SIGNATURE:-**

YASH SHAH **SIGNATURE :-**

ACKNOWLEDGEMENT

In this semester, we have completed our project on “STEGANOGRAPHY BASED WEB PROJECT”. During this time, all the group members collaboratively worked on the project and learnt about the industry standards that how projects are being developed in IT Companies. We also understood the importance of teamwork while creating a project and got to learn the new technologies on which we are going to work in near future.

We gratefully acknowledge for the assistance, cooperation guidance and clarification provided by “Asst Prof. Bharti Dubey” during the development of our project. We would also like to thank our Head of Department Prof. Sumitra Menaria and our Principal Dr. Swapnil Parikh Sir for giving us an opportunity to develop this project. Their continuous motivation and guidance helped us overcome the different obstacles for completing the Project.

We perceive this as an opportunity and a big milestone in our career development. We will strive to use gained skills and knowledge in our best possible way and we will work to improve them.

AAYUSH RAJ THAKUR	**SIGNATURE:-**
JITESH N. SONWANE	**SIGNATURE:-**
TEJAS SANDIP BORASE	**SIGNATURE:-**
YASH SHAH	**SIGNATURE :-**

LIST OF FIGURES

INDEX

CHAPTER 1: INTRODUCTION

1.1 Context:

Steganography is a method of hiding secret information within a non-secret message, image, or other medium in such a way that the very existence of the secret information is not evident. When done correctly, anyone viewing the image file should not see a difference between the original image file and the altered file; this is accomplished by storing the message with less significant bits in the data file. This process can be completed manually or by using a steganography tool. There are five main types of steganography: text steganography, image steganography, video steganography, audio steganography, and network steganography. Each type involves hiding information within a specific medium, such as text files, image files, audio signals, or digital video formats. Steganography can be detected using stegoanalytical algorithms, which can be categorized according to the information available and the purpose sought. These algorithms can be used to identify and extract hidden information from steganographic messages.

1.2 Problem Statement:

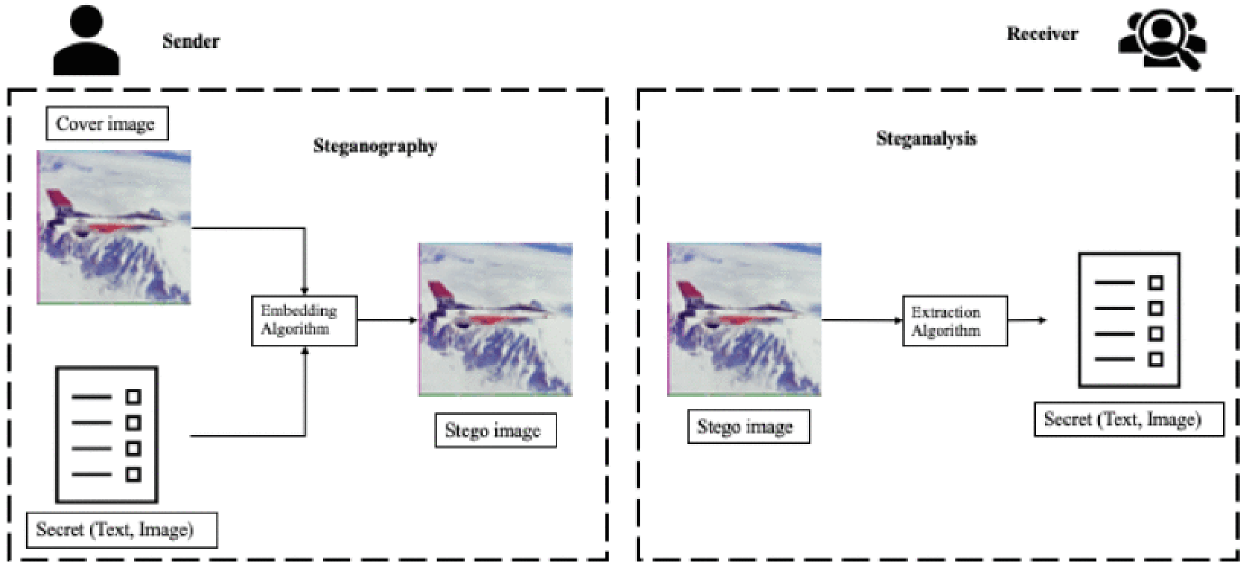
In today's digital age, the exchange of sensitive information over the internet is vulnerable to cyber threats and unauthorized access. Despite advancements in cryptography, the mere detection of encrypted data can alert malicious actors, increasing the risk of interception and decryption. To address this issue, there is a need for a more covert method of securing information that can blend seamlessly into innocuous digital content. Steganography, the practice of concealing messages within other non-sensitive data, offers a potential solution by allowing the hidden transmission of sensitive information without drawing attention to its existence.

1.3 Objectives:

The objectives of this project are:

- To design and develop a steganography-based web project that enables secure communication over the internet
- To implement steganographic algorithms for hiding secret information within image files
- To evaluate the performance of the steganography-based web project in terms of security, robustness, and efficiency

1.4 Functions:

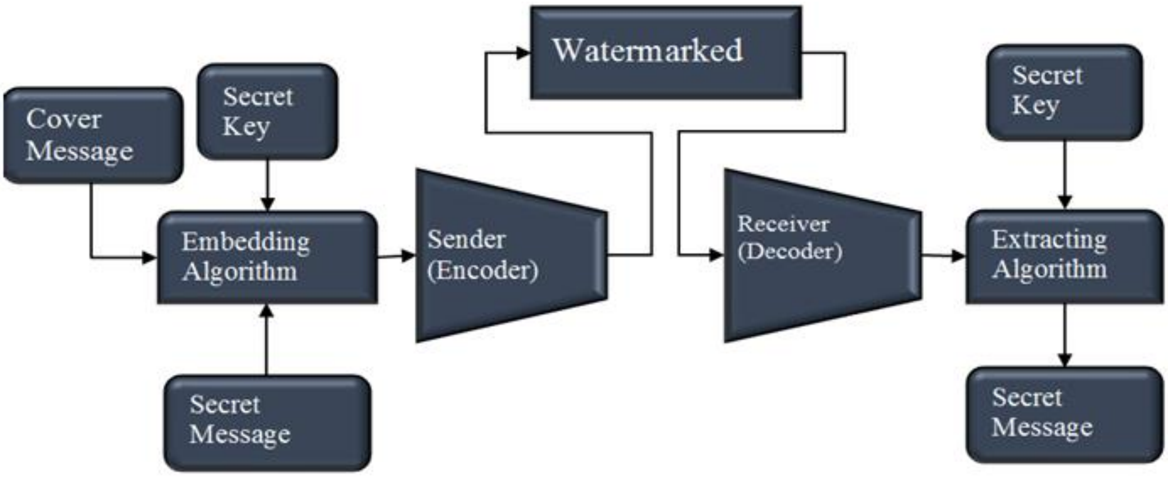


1.4.1 Fig 1: Functionalities of the Project

The steganography-based web project will have the following functions:

- Image upload: users can upload images to be used as cover media
- Secret message input: users can input secret messages to be hidden within the cover image
- Steganographic algorithm selection: users can select from various steganographic algorithms to hide the secret message
- Stegotext generation: the system will generate a stegotext by embedding the secret message into the cover image
- Stegotext transmission: the stegotext will be transmitted over the internet to the intended recipient
- Secret message extraction: the recipient can extract the secret message from the stegotext using the corresponding steganographic algorithm Here is an example of a simple steganography algorithm using Least Significant Bit (LSB) substitution:

1.4.2 Understanding the functionalities with figures:



1.5 LSB Steganography Algorithm Embedding Algorithm:

1. Input:

    a. Cover image (CI): the original image in which the secret message will be hidden

    b. Secret message (SM): the messag**e** to be hidden in the cover image

    c. Key (K): a random key used to encrypt the secret message

2. Preprocessing:
    a. Convert the cover image to a binary representation (e.g., 8-bit grayscale)
    b. Convert the secret message to a binary representation (e.g., ASCII code)
    c. Encrypt the secret message using a symmetric encryption algorithm (e.g., AES) with the key K
3. Embedding:
    a. Iterate through each pixel of the cover image
    b. For each pixel, extract the least significant bit (LSB) of each color component (R, G, B)
    c. Replace the LSB of each color component with the corresponding bit of the encrypted secret message
    d. If the secret message is shorter than the number of pixels in the cover image, repeat the message to fill the remaining pixels
4. Output:
    a. Stegotext (ST): the resulting image with the hidden secret message

1.6 Extraction Algorithm:

1. Input:
    - Stegotext (ST): the image containing the hidden secret message
    - Key (K): the same key used to encrypt the secret message
2. Preprocessing:
    - Convert the stegotext to a binary representation (e.g., 8-bit grayscale)
    - Convert the stegotext to a binary representation (e.g., 8-bit grayscale)
3. Iterate through each pixel of the stegotext
    - For each pixel, extract the LSB of each color component (R, G, B)
    - Combine the extracted bits to form the encrypted secret message
4. Decryption:
    - Decrypt the extracted secret message using the same symmetric encryption algorithm (e.g., AES) with the key K
5. Output:
    - Secret message (SM): the original secret message

1.7 Performance:

The performance of the steganography-based web project will be evaluated in terms of:

- Security: the ability of the system to resist unauthorized access to the secret message

- Robustness: the ability of the system to withstand attacks and tampering
- Efficiency: the speed and computational resources required to perform steganographic operations

Chapter 2: Literature Review

1. INTRODUCTION

Recently, several methods are developed to protect important information. The developed methods may be classified into two categories: steganography and watermarking. Both steganography and watermarking are data embedding methods. Steganography aims to embedding huge amount of secret data in multimedia carrier such as text, image, audio, and video. On the other hand, watermarking, that may be mainly used for proving copyright, aims to hiding small amount of secret data in multimedia carrier. Although steganography and cryptography have a common goal and are related concepts, the usage and the way of both are somewhat different. Steganography is hiding the message existence completely whereas cryptography is securing the sent message. Steganography's main factors are un detectability, robustness, and capacity. These factors separate steganography from other related techniques e.g. cryptography and watermarking

This paper concerns with steganography-based information hiding. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. In other words, steganography is the process of embedding a file, message, image, or video within another file, message, image, or video. The expression steganography combines the Greek word "stego" which means "cover" and the Greek word "grafia" which means "writing", resulting "covered writing".

The idea of steganography was first presented in at 1983. Figure [1.4.1] presents the scenario of steganography system [8]. Steganography scenario can be summarized in two different phases: encoding (embedding) phase with the help of secret key and decoding (extracting) secret data phase with the manner of preserving information invisible. In the embedding phase, the secret message is embedded in an actual/original multimedia carrier (cover message) by using an embedding algorithm and a secret key. The key is used to aid in encryption and to decide where the information should be hidden in the multimedia carrier. After hiding the secret message, one can call it stegomedium and the key which is used for hiding process is called stego-key. In the extracting phase, the secret message is extracted from the multimedia carrier by using an extracting algorithm and the same secret key.

2. History

Few instances of historical incidents on steganography:

1. Harpagus' Hare Message:

- Harpagus hid a message inside a hare's body and sent it with a messenger pretending to be a hunter.

- Demonstrates the use of animals to conceal messages in ancient times.

2. Histaieus' Tattooed Message:

- Histaieus shaved the head of a trusted slave, tattooed the message on his head, and waited for his hair to grow back before sending him.

- Shows the extreme lengths to which people went to hide messages, even using human bodies as carriers.

3. Demeratus' Wax Tablets:

- Demeratus concealed a message under wax writing tablets by removing the wax, writing on the wood, and re-covering it with wax.

- Illustrates a clever method of hiding messages in plain sight, relying on the recipient to uncover the hidden message.

4. Aeneas' Astrogal:

- Aeneas invented the astrogal, a ball or cube with drilled holes representing letters, to pass thread through for spelling out messages.

- A creative and intricate method of secret communication, resembling a toy to avoid suspicion.

5. Invisible Ink and Pin Pricks:

- Germans used invisible ink and pin pricks above letters in innocuous messages, requiring heating or careful inspection to reveal the hidden message.

- Demonstrates the use of hidden markings and substances to convey covert information, even in modern times.

6. Porta's Dog Message:

- Giovanni Batista Porta suggested feeding a message to a dog and killing the dog to retrieve the message.

- Shows a more extreme and brutal method of retrieving hidden messages, indicating the lengths to which people went for secrecy

3. LITERATURE REVIEW

In the year of 2013 Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier transform (FrFT), investigated on as a generalization of the classical Fourier transform, introduced years ago in mathematics literature. The enhanced computation of fractional Fourier transform, the discrete version of FrFT came into existence DFrFT. This study of illustrates the advantage of discrete fractional Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The result shows same PSNR in both domain (time and frequency) but DFrFT gives an advantage of additional stego key. The order parameter of this transform.

In the year of 2013 Akhtar, N.; Johri, P.; Khan, S., implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit-inversion technique. LSB method improving the PSNR of stegoimage. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving the robustness of steganography, RC4 algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message. The presented method shows good enhancement to Least Significant Bit technique in consideration to security as well as image quality.

In the year of 2013 Prabakaran, G.; Bhavani, R. and Rajeswari P.S. Investigated on Medical records are extremely sensitive patient information a multi secure and robustness of medical image based steganography scheme is proposed. This methodology provides an efficient and storage security mechanism for the protection of digital medical images. Authors proposed a viable steganography method using Integer Wavelet Transform to protect the MRI medical image into a single container image. The patient's medical diagnosis image has been taken as secret image and Arnold transform was applied and scrambled secret image was obtained. In this case, the scrambled secret image was embedded into the dummy container image and Inverse IWT was taken to get a dummy secret image. It has been observed that the quality parameters are improved with acceptable PSNR compared to the existing algorithms.

In the year of 2012 Thenmozhi, S. and Chandrasekaran, M., presented the novel scheme embeds data in integer wavelet transform coefficients by using a cropping function in an 8×8 block on the cover image. The optimal pixel change process has been applied after embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoid the floating point precision problems of the wavelet filter. Result shows that the method outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity.

In the year of 2012 Das, R. and Tuithung, T. proposed a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of Huffman encoded bit stream and Huffman Table are alsoembedded inside the cover image, in order that the Stego Image becomes standalone information to the receiver. Results show that the algorithm has a high capacity and a good invisibility. Moreover Peak Signal to Noise Ratio (PSNR) of stego image with cover image shows better result in comparison with other existing steganography approaches. The satisfactory security is maintained in this research.

In the year of 2012 Hemalatha, S, Acharya, U.D. and Renuka [6] presented integer Wavelet Transform (IWT) is used to hide the key thus it is very secure and robust because no one can realize the hidden information and it cannot be lost due to noise or any signal processing operations. Result shows very good Peak Signal to Noise Ratio, which is a measure of security. In this method the secret information is hidden in the middle bit-planes of the integer wavelet coefficients in high frequency sub-bands. In the 2012 Reddy, H.S.M., Sathisha, N. and Kumari, A. [7] worked on the steganography is used to hide. Secure Steganography using Hybrid Domain Technique (SSHDT). The cover image of different formats and sizes are considered and resized to dimensions of power of 2. The Daubechies Lifting Wavelet Transforms (LWT) is applied on cover image to generate four sub bands XA, XH, XV and XD. The XD band is considered and divided into two equal blocks say upper and lower for payload embedding. The payload of different formats are considered and resized to dimensions of power of 2. The payload is fragmented into four equal blocks. The Decision Factor Based Manipulation (DFBM) is used to scramble further stego object to improve security to the payload. Dubechies Inverse LWT (ILWT) is applied on XA, XH, XV and XD stego objects to obtain stego image in spatial domain. It has been observed that PSNR and embedding capacity of the proposed algorithm is better compared to the existing algorithm.

With the rapid development of internet and wide application of multimedia technology, people can communicate the digital multimedia information such as digital image, with others conveniently over the internet. In numerous cases, image data, transmitted over a network are expected not to be browsed or processed by illegal receivers. Consequently, the security of digital image has attracted much attention recently and many different methods for image encryption have been proposed, such as Optical systems are of growing interest for image encryption because of their distinct advantages of processing 2-dimensional complex data in parallel at high speed. In the past, many optical methods have been proposed in . Among them the most widely used and highly successful optical encryption scheme is double random phase encoding proposed in [4]. It can be shown that if these random phases are statistically independent white noise then the encrypted image is also a stationary white noise. In some schemes, chaos based functions are used to generate random phase mask. Such as the generalization of the conventional Fourier transform

4. CONCLUSIONS

In this paper, a literature survey of digital image steganography information hiding techniques is presented. first, a classification of watermarking algorithms based on embedding domain is shown. These domains are spatial domain, transform domain, Spread Spectrum steganography, Model Based steganography. All these algorithms try to satisfy three most important factors of steganographic design i.e. un-detectability, robustness, and capacity. then, some hybrid techniques are discussed. Finally, a comparative study between the different methods is introduced. It is clearly observed that the embedding procedure is easy in spatial domain techniques compared to complex transform domain techniques. Also, Spatial domain techniques are simple and have high stego visual quality, but transform domain techniques are more robust and less exposure to image processing attacks. From the paper, it can be concluded that every technique has advantages and disadvantages if compared with other techniques of steganography. Which mean that it is not fair to call any method 'the best or the worst of all'. So determining the suitable method is chosen based on the wanted purpose.

5. REFERENCES

1. Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform," Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on, vol., no., pp.97,100, 1-2 March 2013.

2. Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, vol., no., pp.385,390, 27-29 Sept. 2013.

3. Das, R.; Tuithung, T., "A novel steganography method for image based on Huffman Encoding," Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on, vol., no., pp.14,18, 30-31 March 2012.

4. Hemalatha, S.; Acharya, U.D.; Renuka, A.; Kamath, P.R., "A secure image steganography technique using Integer Wavelet Transform," Information and Communication Technologies (WICT), 2012 World Congress on, vol., no., pp.755,758, Oct. 30 2012-Nov. 2 2012.

5. 2012-Nov. 2 2012. Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image-based steganography scheme," Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on, vol., no., pp.1188,1193, 20-21 March 2013.

6. Thenmozhi, S.; Chandrasekaran, M., "Novel approach for image stenography based on integer wavelet transform," Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on, vol., no., pp.1,5, 18-20 Dec. 2012.

7. Reddy, H.S.M.; Sathisha, N.; Kumari, A.; Raja, K.B., "Secure steganography using hybrid domain technique," Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on, vol., no., pp.1,11, 26-28 July 2012.

8. 2012. Masud Karim, S.M.; Rahman, M.S.; Hossain, M.I., "A new approach for LSB based image steganography using secret key," Computer and Information Technology (ICCIT), 2011 14th International Conference on, vol., no., pp.286,291, 22-24 Dec. 2011.

9. Tataru, R.L.; Battikh, D.; Assad, S.E.; Noura, H.; Deforges, O., "Enhanced Adaptive Data Hiding in Spatial LSB Domain by using Chaotic Sequences," Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on, vol., no., pp.85,88, 18-20 July 2012.

10. Keshari, S.; Modani, S.G., "Weighted fractional Fourier Transform based image Steganography," Recent Trends in Information Systems (ReTIS), 2011 International Conference on, vol., no., pp.214,217, 21-23 Dec. 2011.

11. Madhusudan Joshi, Chandrashakhar, Kehar Singh, “Color image encryption and decryption using fractional fourier transform”, Optics communications, Vol. 279 Issue 1, pp 35-42, 1 November 2007.

12. Narendra Singh, Alok Sinha, “Optical image encryption using fractional fourier transform and chaos”, Optics and Lasers in Engineering”, Vol. 46 Issue 2, pp 117 – 123, February 2008.

13. Lin Zhang, Jianhua Wu, Nanrun Zhou, “Image Encryption with Discrete Fractional Cosine Transform and Chaos”, Fifth International Conference on Information Assurance and Security 2009 IAS '09, pp 61 – 64, 2009.

Chapter 3: Methodology

3.1 Waterfall Model for Steganography Based Web Project :

The Waterfall Model is a linear and sequential approach to software development, which is suitable for a Steganography Based Web Project. Here's how the model can be applied to this project:

3.2 Phases of Waterfall Model

Phase 1: Requirements Gathering:

- Collect requirements from stakeholders and users about the Steganography Web Application.
- Identify the functional and non-functional requirements, such as:
- Hiding secret messages within images
- Encoding and decoding algorithms
- User authentication and authorization
- Web application security
- User interface and user experience

Phase 2: Analysis :

- Analyze the requirements gathered in the previous phase.
- Break down the project into smaller components, such as:
- Image processing module
- Steganography algorithm module
- User authentication module
- Web application framework
- Create a detailed analysis document outlining the project's scope, timelines, and resources.

Phase 3: Design :

- Create a detailed design document outlining the architecture of the Steganography Web Application.
- Design the user interface and user experience, including wireframes and prototypes.
- Plan the database schema and data models.
- Choose the programming languages, frameworks, and tools for the project.

Phase 4: Implementation (Coding) :

- Start coding the Steganography Web Application based on the design document.

- Implement the image processing module using a programming language such as Python or Java.
- Develop the steganography algorithm module using a library such as OpenCV or PySteg.
- Implement user authentication and authorization using a framework such as Flask or Django.
- Develop the web application framework using a framework such as React or Angular.

Phase 5: Testing :

- Test the Steganography Web Application to ensure it meets the requirements and works as expected.
- Conduct unit testing, integration testing, and system testing.
- Test the application's security and performance.

Phase 6: Deployment:

- Deploy the Steganography Web Application to a production environment.
- Configure the server and database settings.
- Perform any necessary migrations or updates.

Phase 7: Maintenance:

- Maintain the Steganography Web Application to ensure it continues to work as expected.
- Fix any bugs or issues that arise.
- Update the application to adapt to changing requirements or new technologies.

Fix bugs and issues: Monitor the web application for errors and fix them promptly Update the web application: Add new features or functionality Improve performance or security Perform regular security audits: Identify and address potential security vulnerabilities

By following the Waterfall Model, you can develop a Steganography-based Web Project in a structured and sequential manner, ensuring that each phase is completed before moving on to the next one. This approach helps to ensure that the project is completed on time, within budget, and meets the required specifications. The Waterfall Model provides a structured approach to the development of the Steganography Based Web Project, ensuring that each phase is completed before moving on to the next one. This approach helps to ensure that the project is completed on time, within budget, and meets the required specifications.

3.3 Figure of Waterfall Model

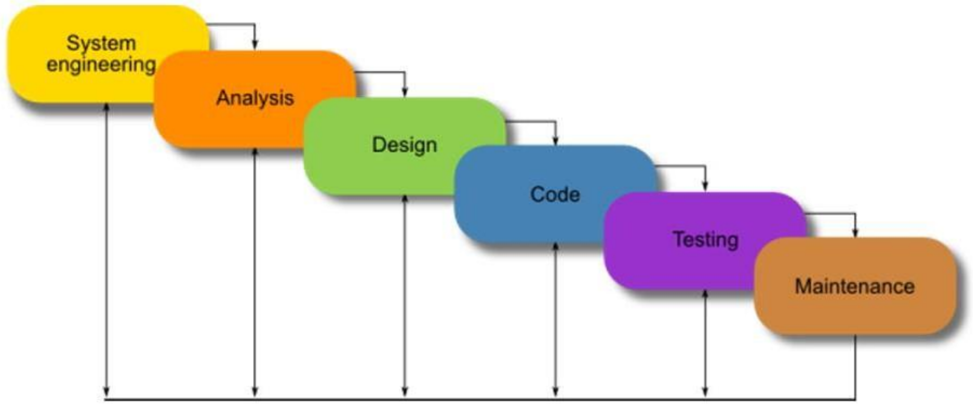


Fig : Waterfall Model.

3.4 Possibilities of choosing others model:

V- Model

Similar to the Waterfall Model, but with a focus on testing and validation Each phase has a corresponding testing phase Emphasizes early testing and validation to catch defects early

Pros:

Ensures thorough testing and validation of each phase Helps to catch defects early, reducing overall project risk Provides a clear, structured approach to development and testing

Cons:

Can be rigid and inflexible, making it difficult to adapt to changing requirements May lead to a longer development cycle due to the emphasis on testing and validation

Prototyping Model

Develop a working prototype of the web application Refine and iterate on the prototype based on user feedback and testing Emphasizes rapid prototyping and testing to validate assumptions and requirements

Pros:

Allows for rapid prototyping and testing of ideas Encourages user feedback and involvement Enables early detection and fixing of defects

Cons:

May lead to a lack of clear requirements and scope Can be resource-intensive, especially if multiple prototypes are developed May not be suitable for complex or large-scale projects

Spiral Model

Combines elements of the Waterfall and Prototyping Models Develops the web application in a series of iterative cycles, with each cycle focusing on a specific aspect of the project Emphasizes risk management and flexibility

Pros:

Allows for flexibility and adaptability to changing requirements Enables early detection and fixing of defects Provides a clear, structured approach to development and testing

Cons:

Can be complex and difficult to manage, especially for large projects May lead to scope creep or feature bloat Requires significant resources and expertise

Ultimately, the choice of SDLC model depends on the project's specific needs, constraints, and goals. The Waterfall Model may be suitable for projects with well-defined requirements and a f ixed scope, while Agile or Prototyping Models may be more suitable for projects with changing requirements or uncertain scope.

3.5 Conclusion:

Ultimately, the choice of SDLC model should align with the project's specific needs, constraints, and goals. The Waterfall Model may be appropriate for projects with well-defined requirements and a fixed scope, while Agile, Prototyping, or Spiral Models may be more suitable for projects characterized by changing requirements or uncertain scope. Careful consideration of the pros and cons of each model will help ensure a successful development process.

Chapter 4: Use Case Diagram | ER Diagram | Flow Diagram

4.1 System Analysis

Before we dive into the system design, let's break down the requirement specification into its functional and non-functional requirements.

4.1.1 Functional Requirements:

- What are the main functions of the steganography-based web project?
    - Hiding secret messages within images
    - Extracting hidden messages from images
    - User authentication and authorization
    - Image upload and download
- What are the inputs and outputs of the system?
    - Input: Image files, secret messages, user credentials
    - Output: Steganographed images, extracted secret messages
- What are the processing steps involved in the system?
    - Image processing (encoding and decoding)
    - Message hiding and extraction
    - User authentication and authorization

4.1.2 Non-Functional Requirements:

- What are the performance, security, and usability requirements of the system?
    - Performance: Fast image processing and message extraction
    - Security: Secure user authentication and authorization, encryption of secret messages
    - Usability: User-friendly interface for image upload, message hiding, and extraction
- Are there any specific constraints or assumptions that need to be considered?
    - Limited image size and format support
    - Limited message size and format support

4.2 System Design

4.2.1 DFD (Data Flow Diagram):

A DFD is a graphical representation of the flow of data through a system. It consists of processes, data stores, and data flows.

Here is a high-level DFD for the steganography-based web project:

Level 0 DFD:

- Process: Steganography System
- Data Stores: Image Database, User Database, Message Database
- Data Flows:
    - User -> Steganography System -> Image Database
    - Image Database -> Steganography System -> Message Database
    - Message Database -> Steganography System -> User

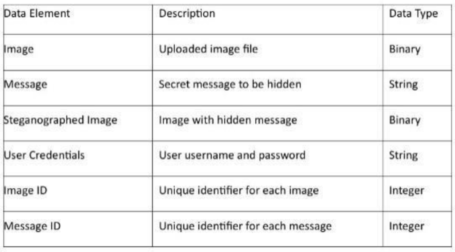
Level 1 DFD:

- Process 1: Image Upload
- Process 2: Message Hiding
- Process 3: Steganography
- Process 4: Message Extraction
- Process 5: Image Download
- Data Stores: Image Database, Message Database, Steganographed Image Database
- Data Flows:
    - User -> Process 1 -> Image Database
    - Image Database -> Process 2 -> Message Database
    - Message Database -> Process 3 -> Steganographed Image Database
    - Steganographed Image Database -> Process 4 -> Message Database
    - Message Database -> Process 5 -> User

4.2.2 Data Dictionary:

A data dictionary is a collection of data elements and their descriptions.

Here is a sample data dictionary for the steganography-based web project:

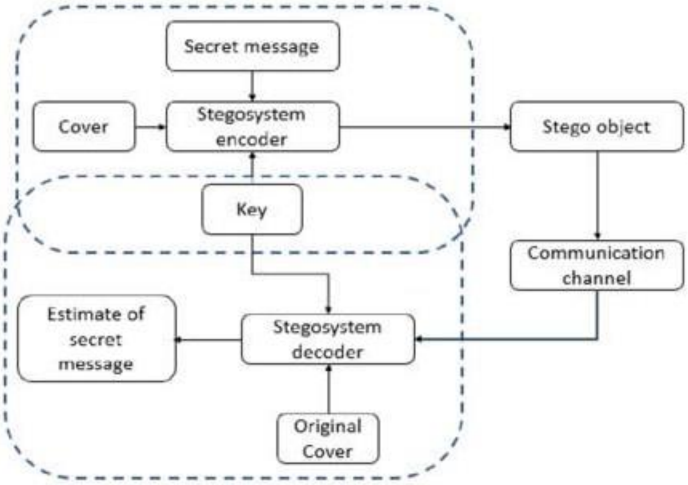


Data Element	Description	Data Type
Image	Uploaded image file	Binary
Message	Secret message to be hidden	String
Steganographed Image	Image with hidden message	Binary
User Credentials	User username and password	String
Image ID	Unique identifier for each image	Integer
Message ID	Unique identifier for each message	Integer

4.3 Structure Chart:

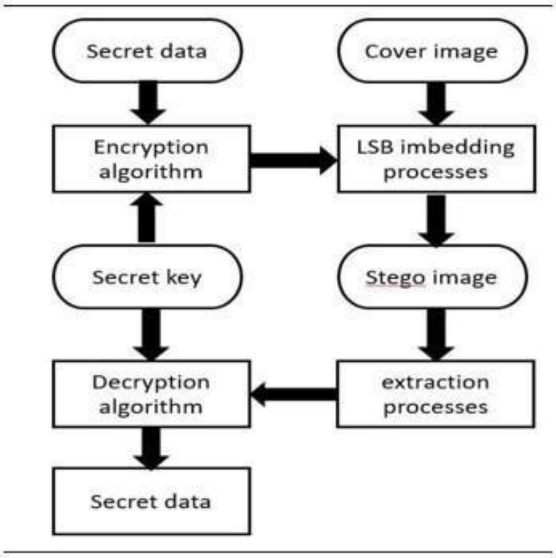
A structure chart is a graphical representation of the hierarchical structure of a system.

Here is a sample structure chart for the steganography-based web project:



Level 1 DFD:

The Level 1 DFD represents the decomposition of the Steganography System into smaller sub processes.



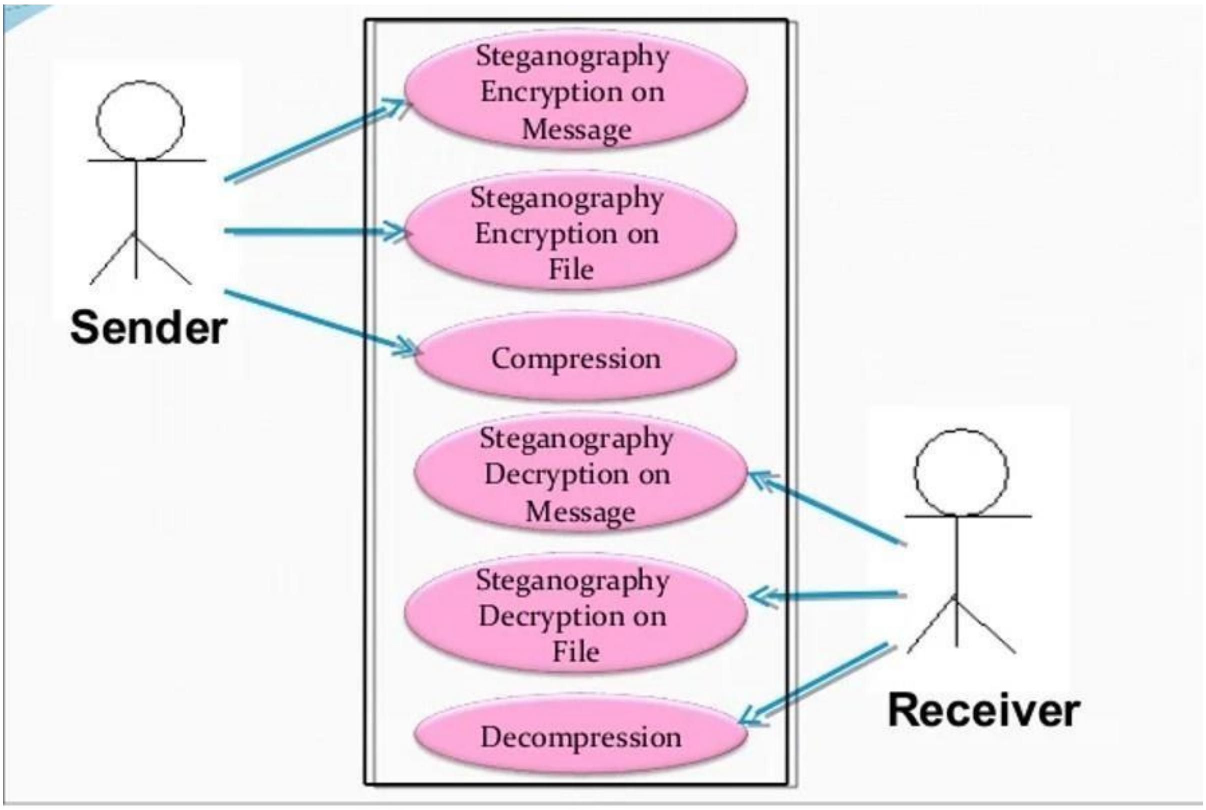
4.3.1 Data Dictionary:

Here's a sample data dictionary for the Steganography-based Web Project:

Data Element	Description	Data Type
Image ID	Unique identifier for each image	Integer
Image File	Image file uploaded by the user	Binary
Message ID	Unique identifier for each message	Integer
Message Text	Secret message to be hidden	String
Stego-Image ID	Unique identifier for each stego-image	Integer
Stego-Image File	Stego-image file generated by the system	Binary
Algorithm Type	Type of steganography algorithm used	String
User ID	Unique identifier for each user	Integer
User Credentials	User authentication credentials	Struct

4.4 Use Case Diagram with Scenarios:

Here is a possible use case diagram for the Steganography-based Web Project:


Sender
Steganography Encryption on Message
Steganography Encryption on File
Compression
Steganography Decryption on Message
Steganography Decryption on File
Decompression
Receiver

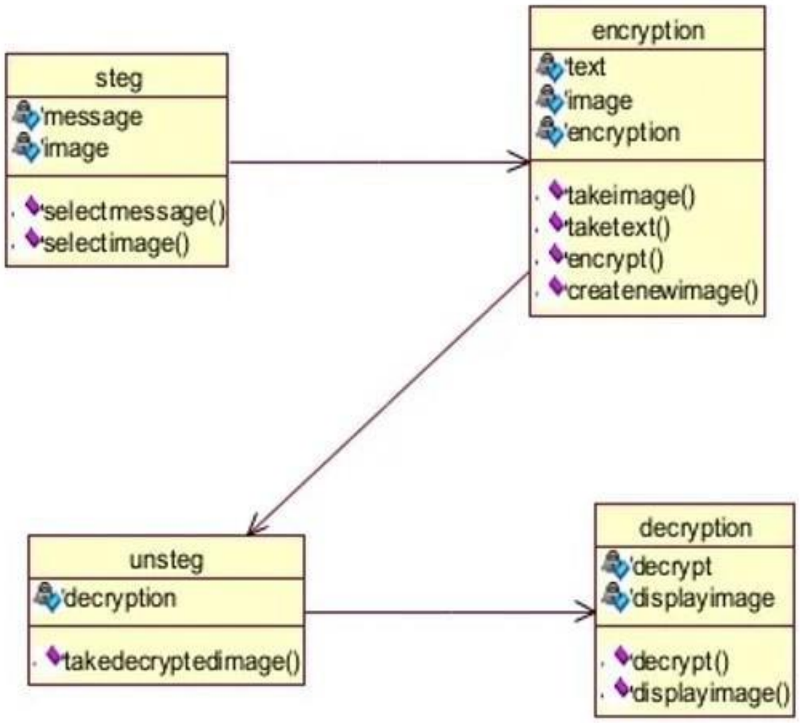
Scenarios:

1. **Upload Image Scenario:**
    - The user uploads an image to the system.
    - The system validates the image and stores it in the image repository.
2. **Upload Message Scenario:**
    - The user uploads a secret message to the system.
    - The system validates the message and stores it in the message repository.
3. **Hide Message Scenario:**
    - The user selects an image and a message to hide.
    - The system uses a steganography algorithm to hide the message within the image.
    - The system generates a stego-image and stores it in the stego-image repository.
4. **Retrieve Message Scenario:**
    - The user uploads a stego-image to the system.
    - The system uses a steganography algorithm to retrieve the hidden message.
    - The system displays the retrieved message to the user.
5. **Download Stego-Image Scenario:**
    - The user requests to download a stego-image.
    - The system retrieves the stego-image from the repository and sends it to the user.

4.4.1 Class Diagram

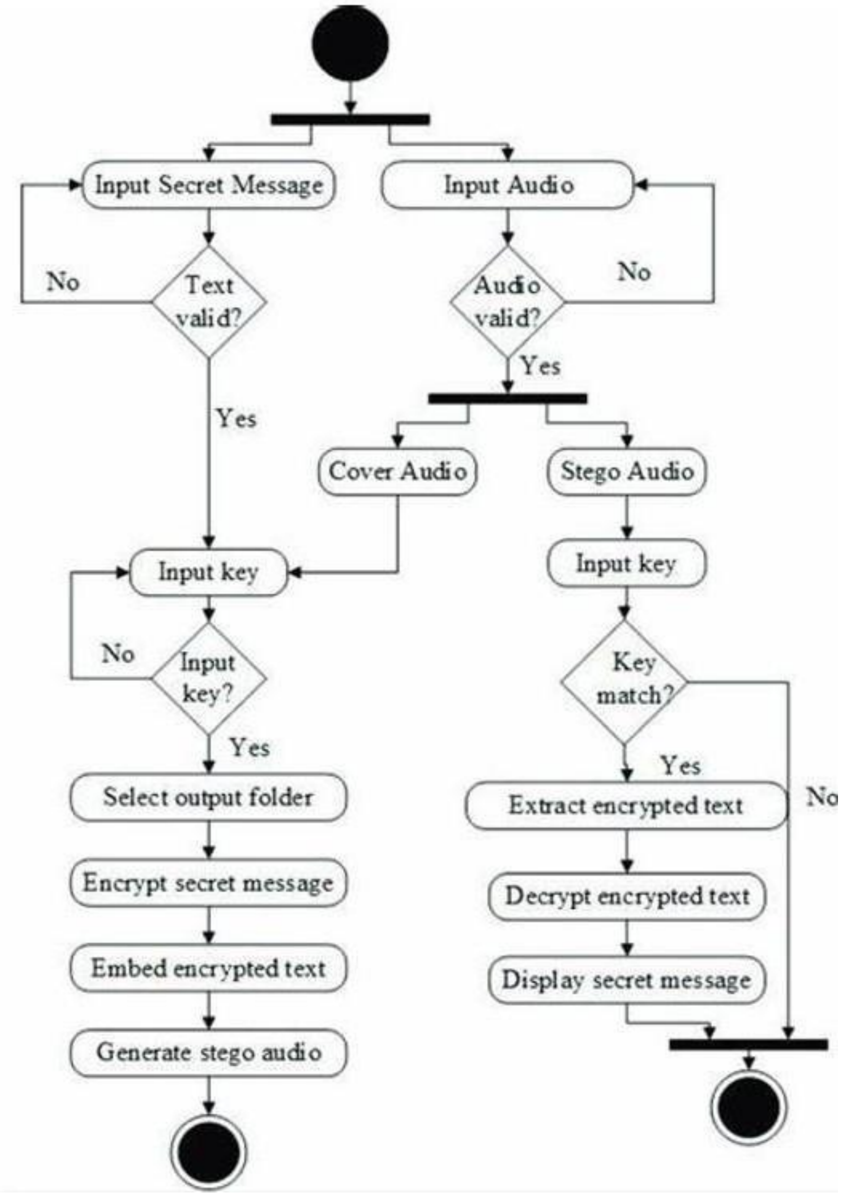
Here is a possible class diagram for the Steganography-based Web Project:

Class diagram of steganography



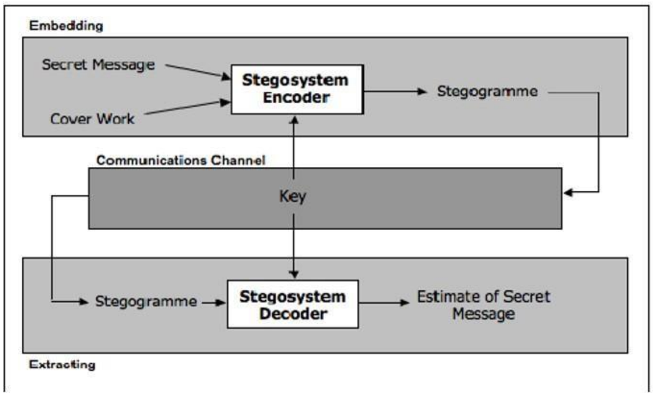
4.4.2 State Diagram:

The state diagram for the Steganography class is as follows:



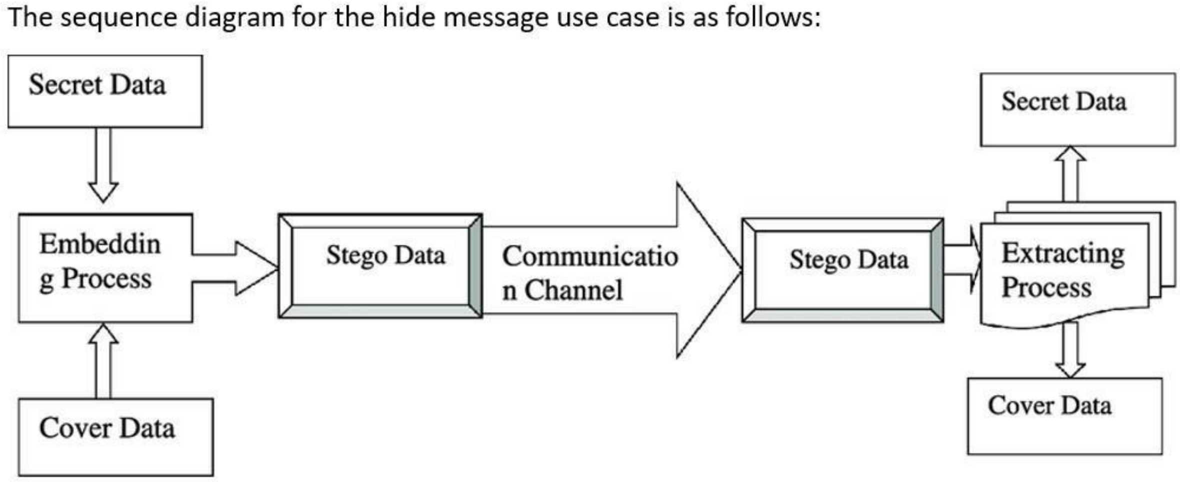
4.4.3 Collaboration Diagram:

The collaboration diagram for the steganography-based web project is as follows:



4.4.4 Sequence Diagram:

The sequence diagram for the hide message use case is as follows:



The sequence diagram for the hide message use case is as follows:

4.4.5 Conclusion:

The steganography-based web project designed using an object-oriented approach incorporates various diagrams to visualize and understand the system's behavior. The use case diagram highlights the primary actors and their interactions with the system. The class diagram illustrates the relationships between classes and their attributes and methods. The state diagram demonstrates the different states of the Steganography class. The collaboration diagram shows the interactions between objects, and the sequence diagram illustrates the sequence of events for the hide message use case.

Chapter 5: Hardware and Software Requirements

5.1 Project Overview:

Secure Image is a web-based platform that utilizes Steganography to securely share images over the internet. Steganography is the practice of hiding secret information within a non-secret message, image, or other medium. In this project, we will develop a web application that allows users to hide secret messages within images and share them securely with others.

5.2 Functional Requirements:

➢ **User Registration:**

- The system shall allow users to register with a unique username and password.
- The system shall validate the user's email address and password during registration.

➢ **Login:**

- The system shall allow registered users to log in with their username and password.
- The system shall authenticate the user's credentials during login.
- later retrieval.

➢ **Image Upload:**

- The system shall allow users to upload images in various formats (e.g., JPEG, PNG, GIF).
- The system shall validate the uploaded image to ensure it meets the required format and size constraints.

➢ **Steganography:**

- The system shall use a Steganography algorithm to hide secret messages within the uploaded images.
- The system shall support various Steganography techniques (e.g., Least Significant Bit (LSB) substitution, Spread Spectrum).
- The system shall encrypt the secret message using a secure encryption algorithm (e.g., AES).

➢ **Secret Message Hiding:**

- The system shall allow users to enter a secret message to be hidden within the image.
- The system shall validate the secret message to ensure it meets the required length and format constraints.

➢ **Image Sharing:**

- The system shall allow users to share the steganographed images with others via a unique URL or QR code.
- The system shall provide options for users to set access controls (e.g., password protection, expiration date) for the shared images.

➢ **Secret Message Extraction:**

- The system shall provide a mechanism for authorized users to extract the hidden secret message from the steganographed image.

5.3 Non-Functional Requirements :

- **Security:**
  - The system shall ensure the confidentiality, integrity, and authenticity of the secret messages hidden within the images.
  - The system shall protect against common web vulnerabilities (e.g., SQL injection, cross-site scripting).
- **Performance:**
  - The system shall respond to user input within 2 seconds.
  - The system shall handle a minimum of 100 concurrent users.
- **Usability:**
  - The system shall provide an intuitive user interface for easy navigation.
  - The system shall provide help and support resources for users

- **User Interface Requirements:**
  - The system shall provide a user-friendly interface for users to upload images, enter secret messages, and share the steganographed images.
  - The system shall provide a dashboard for users to view their uploaded images and shared steganographed images

- **System Interfaces:**
  - The system shall interface with a database management system (e.g., MySQL, MongoDB) for storing user data and image metadata.
  - The system shall interface with a file storage system (e.g., Amazon S3) for storing uploaded images.
- **Performance Requirements:**
  - The system shall respond to user input within 2 seconds.
  - The system shall handle a minimum of 100 concurrent users.
- **Design Constraints:**
  - The system shall be developed using a server-side programming language (e.g., Java).
  - The system shall use a JavaScript library (e.g., jQuery) for client-side scripting.

- **Assumptions and Dependencies:**
  - The system shall assume that users have a basic understanding of Steganography and image sharing.
  - The system shall depend on a reliable internet connection for image uploading and sharing.

Chapter 6: Expected Outcomes of the Project (with GUI)

6.1 Expected Outcomes Based on Functionalities and Features

When implementing a steganography solution, the expected outcomes should align with the functionalities and features that the system is designed to provide. Below are the anticipated outcomes categorized by key functionalities and features:

6.1.1. Robustness and Security

- **Outcome:** The steganography tool should effectively conceal sensitive information within various media types (text, images, audio, video) without compromising the integrity of the host file.
- **Feature:** Use of advanced algorithms to embed data in a way that is imperceptible to human observation and resistant to detection by stegoanalytical methods.

6.1.2. Ease of Use

- **Outcome:** Users should be able to easily navigate the steganography tool, allowing for straightforward embedding and extraction of hidden messages.
- **Feature:** A user-friendly interface that simplifies the process of selecting files, embedding messages, and retrieving hidden information.

6.1.3. Versatility

- Outcome: The tool should support multiple media formats, enabling users to choose the most suitable medium for their specific needs.
- Feature: Compatibility with various file types, including but not limited to JPEG, PNG, WAV, MP3, and MP4, allowing for diverse applications.

6.1.4. Detection Resistance

- Outcome: The embedded information should remain undetectable by common steganalysis techniques, ensuring that the existence of the hidden data is not revealed.
- Feature: Implementation of techniques such as least significant bit (LSB) manipulation, masking, and filtering to enhance the stealth of the hidden data.

6.1.5. Data Integrity and Quality

- Outcome: The quality of the host medium should remain intact post-embedding, ensuring that the original content is preserved and indistinguishable from the altered version.
- Feature: Algorithms that minimize distortion or degradation of the host file, maintaining visual and auditory fidelity.

6.1.6. Performance and Efficiency

- Outcome: The tool should operate efficiently, allowing for quick embedding and extraction processes without significant delays.
- Feature: Optimized algorithms that ensure minimal processing time and resource usage, enabling real-time applications.

6.1.7. Scalability

- Outcome: The solution should be scalable to accommodate varying amounts of data, from small messages to larger files, without compromising performance.
- Feature: Support for different payload sizes and the ability to handle multiple simultaneous

operations.

6.1.8. User Education and Support

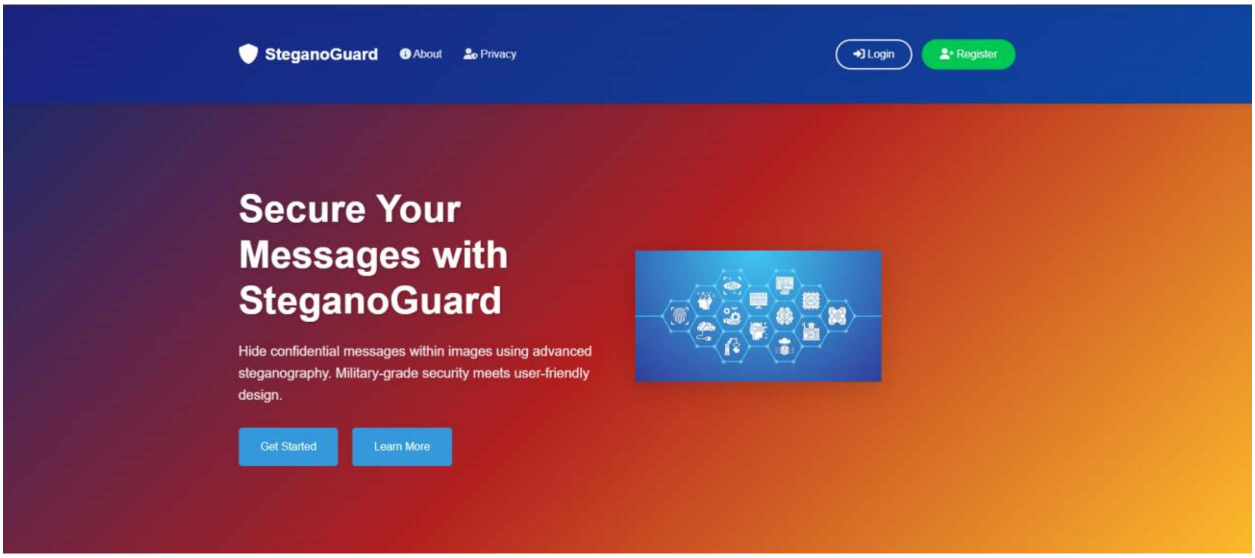
- Outcome: Users should have access to resources that educate them on the effective use of the tool and the principles of steganography.
- Feature: Comprehensive documentation, tutorials, and customer support to assist users in understanding and utilizing the tool effectively.

6.1.9. Legal and Ethical Compliance

- Outcome: The tool should promote responsible use and comply with legal standards regarding data privacy and security.
- Feature: Built-in guidelines and disclaimers to inform users about the ethical implications and legal considerations of using steganography.

6.2 Project Outcomes

1. Landing page of the SteganoGuard

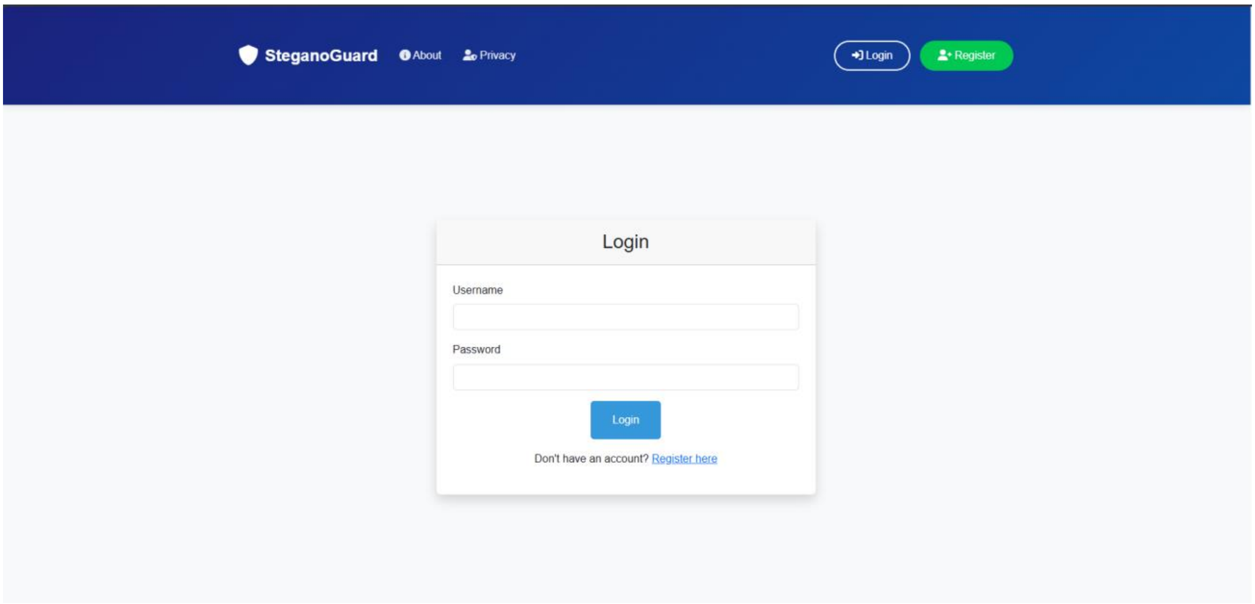


Secure Your Messages with SteganoGuard

Hide confidential messages within images using advanced steganography. Military-grade security meets user-friendly design.

6.2.1 Fig 1 : Homepage

2. Login page of SteganoGuard



Login

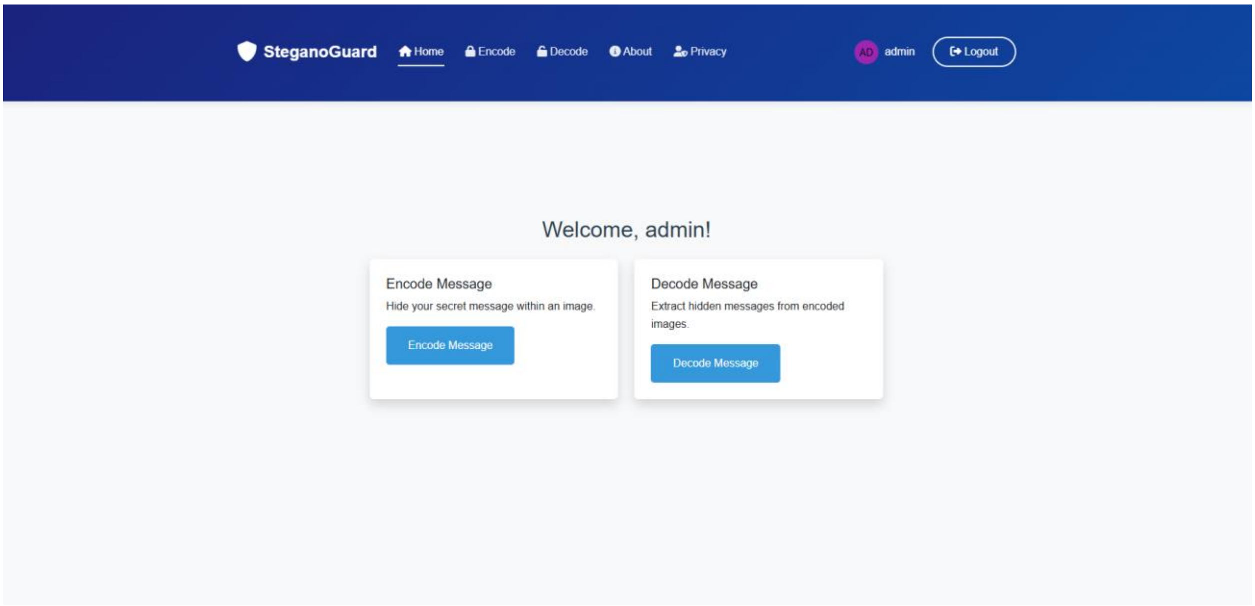
Username

Password

Don't have an account? Register here

6.2.2 Fig 2: Login Page

3. User Dashboard of the SteganoGuard



Welcome, admin!

Encode Message

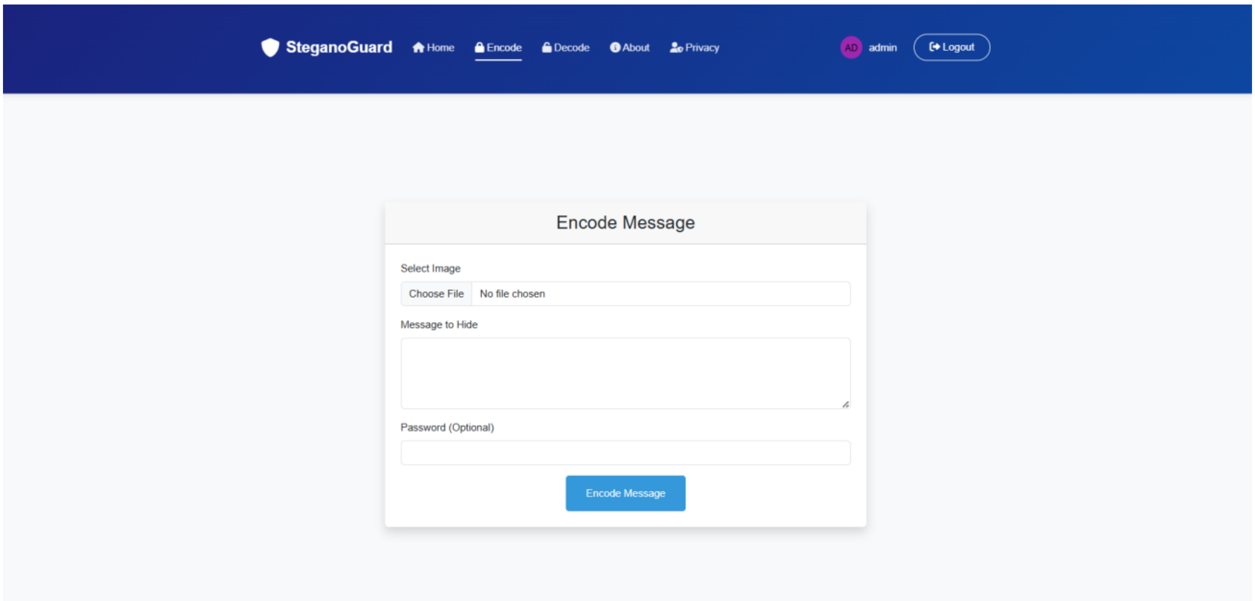
Hide your secret message within an image.

Decode Message

Extract hidden messages from encoded images.

6.2.3 Fig 3: Dashboard Page

4. Encode Page of the SteganoGuard



Encode Message

Select Image

Choose File No file chosen

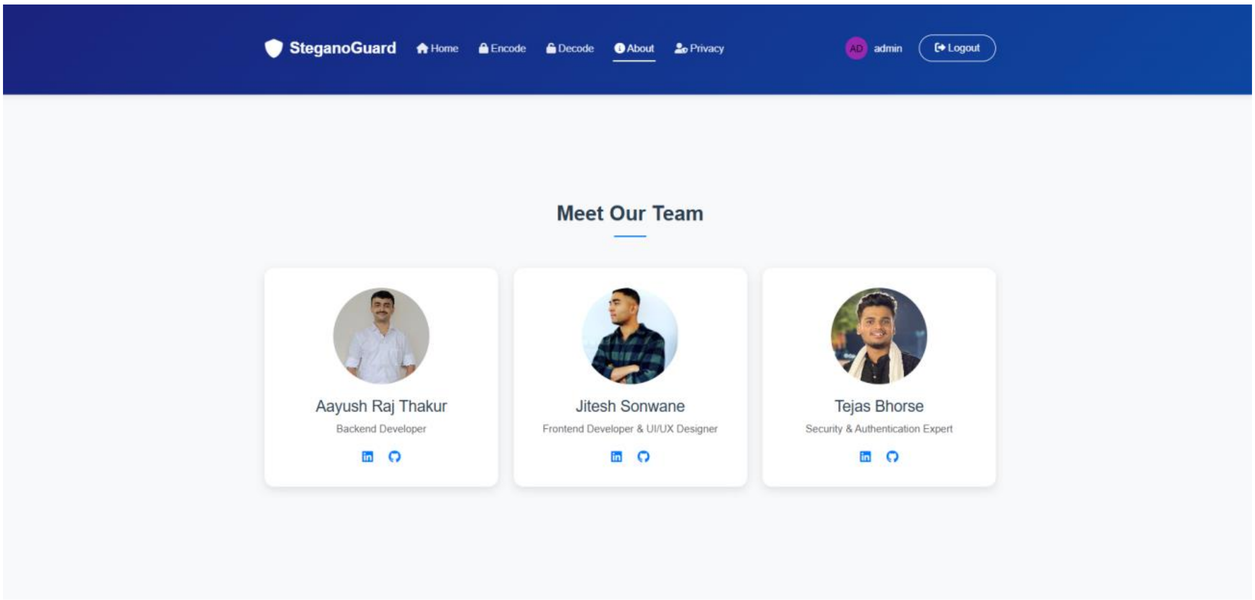
Message to Hide

Password (Optional)

Encode Message

6.2.4 Fig 4: Encode page

5. Our Team Panel



Meet Our Team

Aayush Raj Thakur
Backend Developer

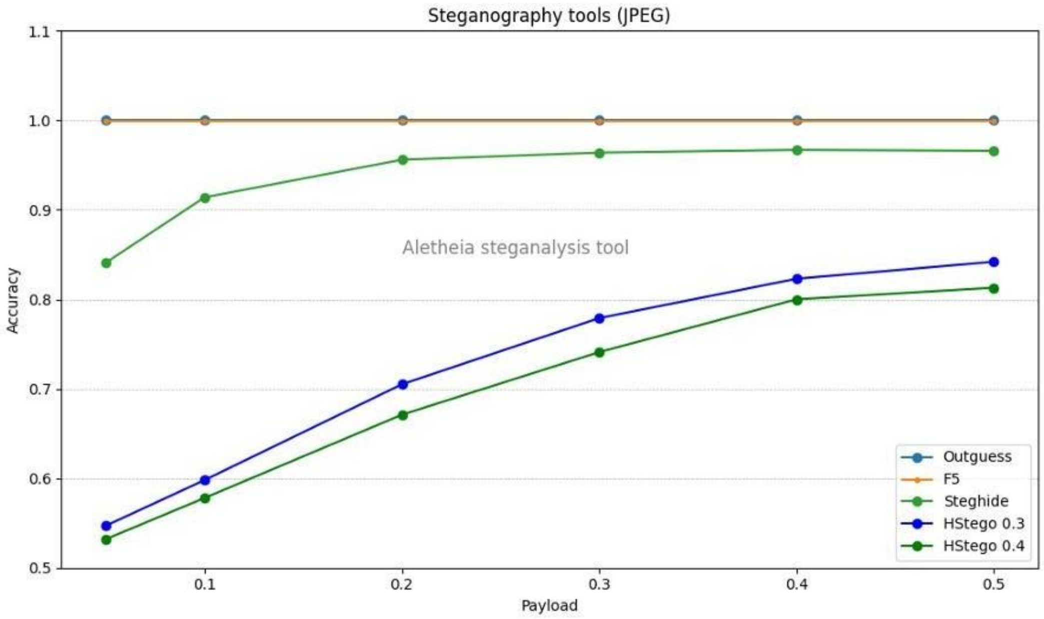
Jitesh Sonwane
Frontend Developer & UI/UX Designer

Tejas Bhorse
Security & Authentication Expert

6.2.5 Fig 5: About Us page

6.3 Performance Metrices:

6. Payload Usage of the algorithm while Working



6.3.1 Fig 1: Performance Metrices

6.4 Conclusion: By focusing on these expected outcomes based on the functionalities and features of a steganography solution, developers can create a robust, user-friendly, and effective tool that meets the needs of users seeking to securely transmit sensitive information in a covert manner. The successful implementation of these outcomes will enhance the overall effectiveness of steganography as a method of information security in the digital age.

Chapter 7: Future works and Limitations

7.1 Future of Steganography:

Given the nascent nature of this technology, the scope of the business issues that are affected and the continuing impact of Moore’s law on the power of computing it is difficult to predict with any certainty where we will be in 5 years. Nevertheless, the following predictions are presented as a reasonable set of possibilities:

- Steganographic techniques will become more common and increasingly sophisticated.
- Steganalysis tools will also become more complex but will typically be behind their steganographic counterparts.
- A stego process will be developed to embed Trojans, worms and viruses in media such as images or audio files and have they become active by viewing or listening to the files. In 2001, the Nimda worm demonstrated that it was possible to get a virus just by visiting an infected web site. In January of 2002, viruses were being delivered by Macromedia flash images. One day, merely viewing a bitmap image might cause a virus attack on your PC.
- Intrusion Detection Systems (IDS) will include images as part of their attack signatures. Anti-virus software will be developed with steganalytical capabilities to detect viruses in audio and image files.
- A strong tamper-resistant, economically viable digital watermark will be developed.

The rapid evolution of digital communication has underscored the need for innovative solutions to secure sensitive information. As highlighted, the development of advanced steganographic techniques, particularly Dual Steganography, which combines steganography with cryptography, presents a compelling opportunity for addressing the challenges of data security in the digital age.

7.2 Limitations of Steganography

Steganography, while a powerful tool for covert communication, is not without its limitations. The following sections outline key challenges and considerations that impact the effectiveness and security of steganographic techniques.

A. What If Perfect Compression Existed?

The hypothetical existence of perfect compression presents a significant challenge for steganography. If perfect compression were achievable, it would imply that any ciphertext could be efficiently hidden within compressed data without detection. This scenario raises two critical implications for steganography:

1. **Triviality or Impossibility:** If compression is highly efficient, steganography may become trivial, as hiding messages would be straightforward. Conversely, if compression is perfect, it could render steganography impossible, as any attempt to embed data might be easily detected.
2. **Bridging Information Theory and Steganography:** This situation underscores the necessity of integrating concepts from information theory with steganographic practices. Practical steganography may only be relevant in contexts where compression is inefficient, highlighting the importance of understanding the limitations imposed by data compression techniques.

B. Entropy

Entropy plays a crucial role in the security of steganographic systems, particularly when the embedded data is indistinguishable from random noise. Key considerations include:

1. **Entropy Calculation:** The entropy of the stegotext is the sum of the entropy of the cover text and the entropy of the embedded material. To maintain security against detection, it is essential to manage the uncertainty in the opponent's measurements.
2. **Challenges in Measurement:** The opponent's ability to accurately measure the entropy of the cover text is uncertain, complicating security proofs. Increasing the amount of stegotext available to the opponent may enhance their capacity to estimate the cover text's statistics, potentially limiting the safe rate of data embedding.
3. **Empirical Evidence:** Despite these challenges, empirical studies indicate that positive rates of ciphertext insertion are achievable in certain channels, suggesting that effective steganographic methods can still be developed.

C. Selection Channel

The concept of a selection channel, inspired by Shannon's correction channel, is integral to the security of steganographic systems that utilize a shared one-time pad. Key points include:

1. **Plausible Ciphertexts:** The use of a one-time pad allows for a large number of plausible ciphertexts, making it difficult for an adversary (e.g., Willie) to accuse the sender (e.g., Alice) of transmitting stegotext.
2. **Book Cipher Analogy:** Similar to a book cipher, where messages are encoded as pointers to words in a shared book, the security of this approach relies on the secrecy of the pad and the avoidance of word reuse. However, repetitive cover texts or those with unusual statistical properties may limit the capacity for secure message embedding.

D. The Power of Parity

In steganographic systems that filter out locations where embedding would significantly alter relevant statistics, the selection channel approach can be enhanced by using parity:

1. **Embedding as Parity:** By selecting a set of pixels using a one-time pad and embedding the ciphertext bit as their parity, the impact of the embedding process on the overall statistics can be minimized, keeping it below a predetermined threshold.
2. **Pseudorandom Number Generators:** The selection channel can be implemented using pseudorandom number generators, which can facilitate the hiding of more bits within the cover text. However, there are inherent limits to the amount of information that can be securely hidden, dictated by the characteristics of the cover text and the encoding rules employed.

7.3 Conclusion

In conclusion, our exploration of steganography highlights its enduring significance as a clandestine communication tool that has adapted to the evolving landscape of information security. From ancient methods of concealing messages in wax tablets to contemporary digital techniques embedded within multimedia files, steganography has continually evolved to meet the demands of covert communication in various contexts.

Our review has examined multiple facets of steganography, including its diverse techniques, detection methods, evaluation criteria, and practical applications. We have discussed the intricacies of steganalysis, which aims to detect hidden messages, and evaluated the robustness of different steganographic algorithms. Furthermore, we explored the concept of time-sensitive steganography, emphasizing the critical balance between detection and decoding times and the operational lifespan of covert channels.

Historically, steganography has played a pivotal role in espionage, warfare, and clandestine communication. While some academic circles focus on developing steganographic methods that are immune to detection, practitioners often recognize the pragmatic necessity of temporary concealment. Historical cases illustrate that even rudimentary steganographic methods can effectively serve their purpose if they can securely hold secrets for the required duration.

Looking ahead, steganography remains a dynamic field ripe for further exploration and innovation. As digital communication continues to evolve, so too will the techniques and tools employed in covert communication. By fostering a deeper understanding of steganography and its implications, we can better navigate the intricate landscape of information security and privacy in the digital age.

Ultimately, our review underscores the enduring relevance of steganography as both an art and a science, shaping the contours of covert communication in an ever-changing world. As we advance into the future, the continued study and application of steganographic techniques will be essential in addressing the challenges of securing sensitive information against an increasingly sophisticated array of threats.

Chapter 10: References

1. N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," in Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998, doi: 10.1109/MC.1998.4655281.
keywords: {Steganography;Image coding;Cryptography;Digital images;Graphics;Transform coding;Ink},

2. R. Das and T. Tuithung, "A novel steganography method for image based on Huffman Encoding," 2012 3rd National Conference on Emerging Trends and Applications in Computer Science, Shillong, India, 2012, pp. 14-18, doi: 10.1109/NCETACS.2012.6203290. keywords: {Airplanes;PSNR;Boats;Computer languages;Receivers;Robustness;Digital images;Steganography;Huffman Encoding;LSB;DCT;PSNR},

3. A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2015, pp. 1-4, doi: 10.1109/ICECCT.2015.7226122. keywords: {Image color analysis;Steganography;least significant bit;RGB;image quality;PSNR;data hiding},

4. N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography," 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), Dehradun, India, 2016, pp. 1-5, doi: 10.1109/ETCT.2016.7882955. keywords: {Image color analysis;Cryptography;Silicon;Cascading style sheets;Aerospace electronics;Receivers;Carrier Image (CI);Secret Image (SI);Pseudo Noise Sequence;Seed Value Propagation;Key Rotation;Image Steganography},

5. O. Elharrouss, N. Almaadeed and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2020, pp. 131-135, doi: 10.1109/ICIoT48696.2020.9089566. keywords: {Entropy;Image quality;Image resolution;Image coding;Digital images;Watermarking;Decoding;Image steganography;LSB;k-LSB;Entropy filter},

6. R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," in IEEE Access, vol. 5, pp. 5354-5365, 2017, doi: 10.1109/ACCESS.2017.2691581.
keywords: {Robustness;Encoding;Discrete cosine transforms;Discrete wavelet transforms;Distortion;Encryption;Video steganography;multimedia security;data hiding techniques;multiple object tracking;DWT;DCT;ECC;imperceptibility;embedding capacity;robustness},

7. K. A. Al-Afandy, O. S. Faragallah, A. Elmhalawy, E. -S. M. El-Rabaie and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, Morocco, 2016, pp. 400-404, doi: 10.1109/CIST.2016.7805079. keywords: {Agriculture;Image color analysis;Color;Security;PSNR;Monitoring;Degradation;Steganography;Least Significant Bit (LSB);Cropping},

8. R. D. Rashid and T. F. Majeed, "Edge Based Image Steganography: Problems and Solution," 2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Sharjah, United Arab Emirates, 2019, pp. 1-5, doi: 10.1109/ICCSPA.2019.8713712.

keywords: {Image edge detection;Color;Image color analysis;Detectors;Payloads;Receivers;Indexes;Steganography;Edge;LSB;Color image},

9. W. Lu, Y. Xue, Y. Yeung, H. Liu, J. Huang and Y. -Q. Shi, "Secure Halftone Image Steganography Based on Pixel Density Transition," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1137-1149, 1 May-June 2021, doi: 10.1109/TDSC.2019.2933621. keywords: {Histograms;Visualization;Security;Image edge detection;Gray-scale;Distortion;Media;Halftone image steganography;pixel density histogram (PDH);pixel density transition;pixel mesh Markov transition matrix (PMMTM)},

10. X. Duan, K. Jia, B. Li, D. Guo, E. Zhang and C. Qin, "Reversible Image Steganography Scheme Based on a U-Net Structure," in IEEE Access, vol. 7, pp. 9314-9323, 2019, doi: 10.1109/ACCESS.2019.2891247. keywords: {Neural networks;Decoding;Gallium nitride;Feature extraction;Receivers;Image coding;Transforms;Information security;reversible image steganography;deep learning;U-Net structure},

11. T. P. Van, T. H. Dinh and T. M. Thanh, "Simultaneous convolutional neural network for highly efficient image steganography," 2019 19th International Symposium on Communications and Information Technologies (ISCIT), Ho Chi Minh City, Vietnam, 2019, pp. 410-415, doi: 10.1109/ISCIT.2019.8905216. keywords: {Image steganography;information security;deep learning;convolutional neural network},