Vol.15, Issue No 2, 2025

ENHANCED SECURITY FOR BANKING TRANSACTIONS USING IMAGE BASED STEGANOGRAPHY

T.Shravani,
UG Student,
Department of CSE,
St. Martin's Engineering College,
Secunderabad, Telangana, India
taranishravani@gmail.com

E. Soumya,
Assistant Professor,
Department of CSE,
St. Martin's Engineering College,
Secunderabad, Telangana, India
esoumyait@smec.ac.in

Abstract- In an age of increasing digital communication and data transfer, ensuring the security and privacy of sensitive information is paramount. Steganography, the art of hiding information within other data, has been used for centuries. In the digital realm, it plays a critical role in secure communication and information concealment. Traditional steganography methods often involve embedding information within a single image. While effective, this approach may be susceptible to detection, as single-image steganography can leave detectable traces, especially under sophisticated analysis. The primary challenge is to develop a robust system for multiple image steganography that can securely hide sensitive files within a set of images. This involves designing algorithms that distribute the information effectively across the images while maintaining imperceptibility and ensuring reliable extraction. Therefore with the rise of cyber threats and privacy concerns, there's a growing need for advanced techniques to protect sensitive files from unauthorized access or interception. Multiple image steganography, an emerging field, offers the potential for heightened security by spreading information across multiple images, making it even more challenging for potential adversaries to detect or extract. The project seeks to enhance file security by leveraging advanced techniques in multiple image steganography. By distributing the information across a set of images, this research endeavors to develop a system capable of securely concealing sensitive files. The algorithms utilized in this approach are designed to ensure imperceptibility and robustness against detection efforts. This advancement holds great promise for significantly improving the security of file transmission and storage, safeguarding critical information from unauthorized access or interception.

Keywords: Digital communication, Steganography, Sophisticated analysis.

I. INTRODUCTION

The rise of digital banking and online financial transactions has revolutionized how people and businesses interact with financial institutions. From making payments to transferring large sums of money, the convenience and speed of these digital platforms have become an integral part of modern life. However, with this convenience comes an ever-growing threat: cybercrime. Cybercriminals employ sophisticated techniques to intercept and manipulate financial transactions, posing significant risks to individuals, corporations, and governments. As digital financial activities increase, the need for robust, foolproof security mechanisms has become a top priority. In response to these escalating security challenges, researchers and experts have explored innovative solutions, with image-based steganography emerging as a promising approach to enhancing the security of banking transactions. Steganography, derived from the Greek words "steganos" (meaning covered) and "graphein" (meaning writing), is the ancient practice of concealing messages within another medium. Unlike cryptography, which scrambles the content of a message to make it unreadable to unauthorized parties, steganography hides the existence of the message itself. Throughout history, steganography has been used to protect sensitive information. Ancient examples include messages written on wax-covered tablets, hidden underneath layers of wax, or messages tattooed onto the scalp of messengers, concealed under hair as it grew back. During World War II, invisible ink and microdots were employed to transmit secret communications. The essence of steganography has always been the art of covert communication: the idea that if no one knows a message exists, it cannot be intercepted or deciphered. With the advent of the digital era, steganography has evolved from these rudimentary techniques into sophisticated methods that leverage technology. Digital steganography, particularly image-based steganography, has become a major focus in the field of information security. In this modern context, steganography uses digital images, videos, or audio files as cover media to hide data imperceptibly. Image-based steganography is especially effective because of the way digital images are represented as arrays of pixels, each consisting of bits that can be subtly altered to hide information. These modifications are usually made in such a way that they are not visually detectable to the human eye. By embedding data within the least significant bits (LSBs) of image 1 pixels, image-based steganography ensures that the cover image appears unchanged, even though it carries hidden information. The use of image-based steganography for securing banking transactions represents a leap forward in financial cybersecurity. Traditional security measures, such as encryption and two-factor authentication, are essential but are increasingly becoming vulnerable to advanced hacking techniques. As attackers develop more sophisticated tools for intercepting and decrypting sensitive information, merely encrypting transaction data is no longer sufficient. This is where image-based steganography comes into play. By embedding critical transaction details or authentication keys within innocuous images, financial institutions can add an extra layer of security that is invisible to outsiders. For example, rather than sending a one-time password (OTP) as plain text, a banking system could hide this information within a seemingly ordinary image, making it nearly impossible for cybercriminals to detect or extract. This covert approach not only conceals the information but also obfuscates the data flow, adding complexity to any interception attempt. Historically, the idea of using steganography in banking and financial transactions has its roots in the early exploration of digital security. As early as the 1990s, when online banking started gaining traction, the need for secure communication channels became evident. Early steganographic methods were proposed as potential solutions for transmitting authentication codes and protecting transaction details. However, the limited computational power and understanding of steganography at that time meant that such ideas were largely theoretical. It was not until the early 2000s, with advancements in computational resources and a deeper understanding of digital signal processing, that practical applications began to emerge. The increasing threat of cyberattacks, coupled with the growing sophistication of data analysis techniques, fueled further research into how steganography could be adapted to meet the high security demands of financial institutions. Today, the integration of image-based steganography in banking security protocols is seen as part of a multi-layered defense strategy. By combining traditional encryption methods with steganographic techniques, banks can create a more secure and resilient framework for protecting sensitive data. The historical journey of steganography, from ancient practices to cutting-edge digital applications, highlights its enduring relevance and adaptability in the face of evolving security challenges. As financial systems 2 continue to embrace digital transformation, the role of advanced security measures like image-based steganography will become increasingly important, shaping the future of secure financial transactions and instilling greater trust in digital banking platforms. .

II. RELATED WORK

[1].B. Sultan,et.al In this project The success of deep learning based steganography has shifted the focus of researchers from traditional steganography approaches to deep learning based steganography. Various deep steganographic models have been developed for improved security, capacity and invisibility. In this work a multi-data deep learning steganography model has been developed using a well known deep learning model called Generative Adversarial Networks (GAN) more specifically using deep convolutional Generative Adversarial Networks (DCGAN). The model is capable of hiding two different messages, meant for two different receivers, inside a single cover image. The proposed model consists of four networks namely Generator, Steganalyzer Extractor1 and Extractor2 network. The Generator hides two secret messages inside one cover image which are extracted using two different extractors. The Steganalyzer network differentiates between the cover and stego images generated by the generator network. The experiment has been carried out on CelebA dataset. Two commonly used distortion metrics Peak signal-to-Noise ratio (PSNR) and Structural Similarity Index Metric (SSIM) are used for measuring the distortion in the stego image The results of experimentation show that the stego images generated have good imperceptibility and high extraction rates..

[2].X. Liao,et.al In this project With the coming era of cloud technology, cloud storage is an emerging technology to store massive digital images, which provides steganography a new fashion to embed secret information into massive images.. Others analyze aftershock patterns; for example, a neural network trained on 130,000 mainshock-aftershock pairs outperformed traditional models in predicting aftershock distributions [3].M. Srivastava,et.al In this project Image Steganography is the artwork of concealing mystery data within the image such that the hacker will now no longer be capable of discover the records within inside the stego images. This is a useful approach to secure our sensitive information. Security has continually been a main difficulty from last many years to existing days.[4].G. Benedict,et.al In this project Steganography is the process of hiding a secret message within an ordinary message & extracting it at its destination. Image steganography is one of the most common and secure forms of steganography available today. Traditional steganography techniques use a single cover image to embed the secret data which has few security shortcomings. [5].S. Mukhopadhyay,et.al In this The paper proposes a scheme for achieving steganography with multiple encrypted monochromatic images with keys obtained from a synchronized system of semiconductor lasers.[6].A. S. Ansari,et.al .This paper presents an image Steganography algorithm that can work for cover images of multiple formats. Having a single algorithm for multiple image types provides several advantages. For example, we can apply uniform security policies across all image formats, we can adaptively select the most suitable cover image based on data length, network bandwidth and allowable distortions, [7].P. Grandhe,et.al, In this project Communicating online without fearing third-party interventions is becoming a challenge in the modern world. Especially the sectors like the military, and government organizations or private companies sharing sensitive information. They invest a lot of effort and cost into obtaining the advancement of safe communication techniques. [8].R. Joshi,et.al , in this There are advances in

data stealth and forgery with the rise of technology and advances in data transmission. This arises the need for better and developed methods for data transmission. Data Transmission is an essential task in the current era, and equally important is the secure and safe information of that data. In the paper, batch steganography is used to secure data transmission from one end to the other.[9].Z. Wang,et.al.In this paper, a more accurate image steganography method is proposed, where a multi-level feature fusion procedure based on GAN is designed. Firstly, convolution and pooling operations are added to the network for feature extraction. Then, short links are used to fuse multi-level feature information. Finally, the stego image is generated by confrontation learning between discriminator and generator. [10].X. Zhao,et.al.In this paper, a multi dilated generation countermeasure network (Multi Dilated GAN) model is proposed to improve the information steganography quality of images. Based on the discriminator of the steganography model, multiple convolution and expansion convolution are adopted.[11].M. Liu,et.al.In this paper, They propose a new adversarial embedding scheme for image steganography. Unlike those related works, we first combine multiple gradients of cover and generated stegos to determine the directions of cost modifications. Next, instead of adjusting all or a random part of embedding costs in existing works, we carefully select the candidate costs according to the amplitudes of cover gradients and their costs.[12]. Priya Thomas"A Comprehensive Survey of Image Steganography" is a literature survey that extensively reviews the evolution of image steganography techniques. The study focuses on traditional methods like Least Significant Bit (LSB) embedding and advanced techniques, including edge-adaptive methods and deep learning-based approaches. It analyzes key parameters such as embedding capacity, image quality, and robustness against steganalysis. [13].Kalaiarasi Survey on Image Steganography Techniques provides a comprehensive analysis of various methods in image steganography, focusing on traditional and modern approaches. The authors examine fundamental techniques such as Least Significant Bit (LSB) embedding and advanced methods like edge-adaptive and transform domain approaches.[14].Muhammad Adnan Aslam "Image Steganography Using Least Significant Bit (LSB) - A Systematic Literature Review" focuses on reviewing and evaluating the effectiveness of LSB-based steganography techniques. It discusses the core principles of LSB, where data is embedded by replacing the least significant bits of pixel values. The review highlights the simplicity and high payload capacity of LSB while addressing vulnerabilities like susceptibility to statistical and steganalytic attacks. [15].Nandhini Subramanian "Image Steganography: A Review of the Recent Advances" highlights the latest developments in the field, emphasizing the integration of artificial intelligence and deep learning. It explores traditional approaches like spatial and transform domain techniques alongside cutting-edge methods, including convolutional neural networks (CNNs) for feature extraction and embedding. The review addresses the challenges of balancing imperceptibility, robustness, and payload capacity. It discusses the use of generative adversarial networks (GANs) to improve security and evade steganalysis. The paper also evaluates advancements in reversible data hiding for applications requiring original data recovery. By analyzing recent trends, the authors provide insights into overcoming existing limitations and suggest potential areas for future research. This survey is essential for understanding how modern technologies shape image steganography.[16]. Priya in this paper has given a detailed review focusing on contemporary methods in image steganography. The paper discusses advancements beyond traditional Least Significant Bit (LSB) techniques, such as Pixel Value Differencing (PVD), modulus functions, and interpolation-based methods. It examines how these methods improve embedding capacity, image quality, and resistance to steganalysis. The survey highlights innovations in edge-based adaptive techniques that minimize distortions in smooth regions, enhancing imperceptibility. Additionally, it contrasts these methods with traditional approaches, emphasizing their robustness against statistical attacks. [17]. Yawar Rasheed explores advancements in image steganography by adapting Least Significant Bit (LSB) techniques to edge regions. The authors propose an edge based approach that selectively embeds data into sharper regions of an image to minimize visual distortions. [18]. Priya Thomas reviews several steganographic techniques, especially focusing on those based on transforming the domain of images. In the paper, the author discusses techniques like the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) for embedding secret information in images, ensuring that the distortion to the image is minimal while maintaining high security. [19]. Saud S,Alotaibi "Reversible Data Hiding with Interpolation Techniques" focuses on methods to embed data in images while ensuring the original image can be perfectly restored after extraction. The paper examines the use of interpolation errors, such as pixel differences generated during resizing or reconstruction, as embedding locations. This approach minimizes visual distortions by utilizing redundant information in image structure. It compares interpolation-based reversible techniques with traditional reversible data hiding methods, highlighting their higher embedding capacity and imperceptibility. [20]. Farooque Azam "Statistical and Adaptive Image Steganography Methods" surveys various statistical and adaptive techniques used in image steganography, focusing on methods that adapt to image characteristics for enhanced security and imperceptibility.

III. PROPOSED WORK

The Steganography Dataset The initial step in our research involves acquiring a suitable dataset for steganography. This dataset consists of various images that will serve as carriers for the hidden information. The selection of these images is crucial, as their characteristics can influence the effectiveness and imperceptibility of the steganographic technique. Typically, a diverse set of images with varying resolutions, color distributions, and complexities are chosen to ensure the robustness and generalizability of the proposed method. Dataset Preprocessing Before utilizing the dataset, it is essential to preprocess the images to ensure they are suitable for steganographic embedding. This preprocessing includes: Null Value Removal: Ensuring that there are no corrupt or incomplete images in the dataset. Any image files with null values or missing data are either corrected or removed from the dataset. Label Encoding: For any categorical data associated with the images, such as image type or source, label encoding is performed to convert these categories into numerical values. This step is particularly useful if the dataset includes metadata that can influence the embedding process.Existing Least Significant Bit (LSB) Substitution in Single Image Steganography Algorithm To establish a baseline for performance comparison, we first implement the traditional Least Significant Bit (LSB) substitution technique. In LSB steganography, the least 19 significant bits of each pixel in an image are replaced with the bits of the secret message. This method is straightforward and widely used due to its simplicity and ease of implementation. However, it is also more susceptible to detection and less robust against image manipulations and attacks. By implementing this method, we can evaluate its strengths and weaknesses and set a benchmark for our proposed approach. Proposed Pixel Value Differencing (PVD) in Multiple Image Steganography The core of our research lies in developing an advanced steganographic technique using Pixel Value Differencing (PVD) across multiple images. This involves several key steps: Message Slicing: The secret message is divided into smaller chunks, each of which will be embedded into different images. This distribution enhances security, as detecting and extracting the entire message requires access to all the carrier images. PVD Embedding: For each image, the PVD algorithm is applied. This method takes advantage of the differences in pixel values to embed information. By analyzing the differences between adjacent pixel values, the algorithm can embed bits of the secret message in a way that is less noticeable compared to altering individual pixel values directly. Encoding and Storage: The images with embedded data are saved, ensuring that the embedded information remains imperceptible to the naked eye and resilient against common image processing operations. Performance Comparison To evaluate the effectiveness of our proposed PVD-based multi-image steganography technique, we perform a comprehensive performance comparison with the LSB substitution method. This comparison involves: Imperceptibility: Assessing the visual quality of the steganographic images to ensure that the embedded information is not noticeable. This is typically measured using metrics like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM). Robustness: Testing the resilience of the embedded data against various attacks and manipulations, such as compression, resizing, and noise addition. Capacity: Comparing the amount of data that can be embedded without degrading the image quality. Prediction of Output from Test Data with Pixel Value Differencing (PVD) in Multiple Image Steganography Trained Model Algorithm Finally, we develop and test a predictive model based on the PVD steganography technique. This involves: Training the Model: Using a portion of the preprocessed dataset, we train a model to embed and extract data using the PVD technique. The training process fine-tunes the algorithm parameters to optimize the embedding and extraction processes. Testing and Validation: The trained model is then tested on a separate set of images to validate its performance. We evaluate its accuracy in correctly embedding and extracting the secret message, as well as its robustness against various image alterations. Analysis of Results: The results from the test data are analyzed to assess the model's effectiveness. This includes evaluating the imperceptibility, robustness, and capacity of the steganographic method.

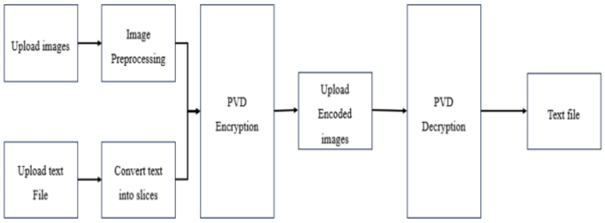


Fig 1: Architecture diagram of multiple image steganography Data Preprocessing

Pixel Value Differencing (PVD) is an innovative approach to steganography that operates in the spatial domain of images. While PVD is commonly applied to single images, its extension to multiple image steganography introduces new dimensions of security and capacity. The fundamental concept of PVD revolves around manipulating the pixel values of multiple images to embed hidden information. In PVD, the difference between the pixel values of adjacent pixels is utilized for data embedding. By carefully adjusting these differences, information can be hidden without significantly altering the visual appearance of the images. PVD operates in the spatial domain, making it resilient to frequency-based attacks. Unlike frequency domain techniques that might be susceptible to transforms, PVD directly modifies pixel values for data concealment. 21 Multiple Image Steganography The extension of PVD to multiple images involves distributing hidden information across a set of images. This approach enhances security by dispersing the embedded data, making it more challenging for adversaries to detect or extract the complete message. Steganography, as a method of embedding secret information within seemingly innocuous cover objects, has long played a crucial role in secure communication. The digital age has popularized image steganography, where images are used as a medium to hide data in a way that cannot be easily detected by the human eye. However, traditional methods of image steganography often rely on using a single cover image to hide the entire data payload, a practice that comes with inherent risks.

Advantages Of Pvd

1. High Capacity for Data Embedding One of the most significant advantages of PVD is its ability to embed a large amount of data without compromising the image quality. By analyzing the difference between adjacent pixel values, PVD determines the embedding capacity dynamically. Regions with larger pixel differences (edges or textures) can hold more data, while smoother areas hold less, optimizing the data-hiding process.

2. Reduced Visual Distortion PVD ensures minimal distortion by embedding data based on pixel differences. Since human eyes are less sensitive to changes in regions with high contrast or texture, PVD selectively embeds more data in such areas, preserving the visual integrity of the image.

3. Enhanced Security By using the differences between pixel values rather than the values themselves, PVD makes it harder for attackers to detect the presence of hidden data. The adaptive nature of the technique further enhances its resistance to steganalysis. 24

4. Robust Against Compression Images embedded using PVD tend to exhibit higher resilience to compression techniques, such as JPEG, because the technique distributes the hidden data in a manner that aligns with natural image properties.

5. Flexibility in Application PVD is versatile and can be combined with other steganographic methods, such as Least Significant Bit (LSB) or encryption algorithms, to create hybrid systems that offer enhanced capacity and security.

6. Adaptive Embedding PVD's ability to adapt to image content allows it to balance the trade-off between embedding capacity and visual quality. High-detail regions are utilized more effectively, while smooth regions are preserved, ensuring better overall performance.

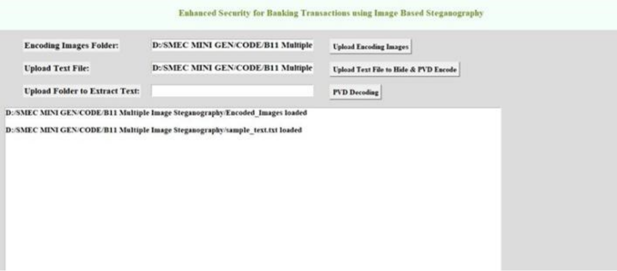
7. Improved Payload-to-Quality Ratio Compared to traditional methods like LSB, PVD achieves a higher payload-to-quality ratio. This makes it suitable for applications requiring a balance between high data capacity and image fidelity.

8. Applicability to Various Image Formats PVD-based methods disrupt the uniformity of pixel value distributions, making it challenging for statistical tools to identify anomalies. This reduces the risk of steganalysis detection.

9. PVD can be applied to different image formats, including grayscale and color images, without significant modifications. This makes it a versatile solution for a wide range of steganographic applications.

IV. RESULTS & DISCUSSION

Implementation description Tkinter Main Window Setup: The script initializes the main Tkinter window with a title and dimensions, serving as the GUI interface. Global Variables and PVD Object Initialization: Global variables (image_path and text_path) store paths for the selected image folder and text file. An instance of the pvd_lib class is created to handle PVD operations. Text Slicing Function (sliceText): Reads a binary text file and divides its content into blocks.Iterates through images in a specified folder, returning a list of text blocks and corresponding image file paths. PVD Encoding Function (PVDEncoding): Writes the sliced text message to a temporary file ("data.txt").Creates a folder for encoded images if it doesn't exist. Utilizes the pvd_embed method from the pvd_obj instance to perform PVD encoding on each image. PVD Decoding Function (PVDDecoding): Upload Image Function (uploadImage): Iterates through encoded images in a specified folder.Uses the pvd_extract method from the pvd_obj instance to perform PVD decoding on each image.Concatenates the extracted data from each image to reconstruct the original hidden text. Opens a file dialog allowing the user to select an image folder.Displays the selected image folder path in the GUI.Upload Text Function (uploadText):Opens a file dialog allowing the user to select a text file.Displays the selected text file path in the GUI.Slices the text and performs PVD encoding on each image in the selected image folder. Extract Text Function (ExtractText): Opens a file dialog allowing the user to select a folder containing encoded images.Displays the selected folder path in the GUI. Performs PVD decoding on each encoded image in the selected folder. Concatenates the extracted text from each image to reveal the original hidden message. 55 GUI Elements: Labels, entry widgets, buttons, and a text box create a user-friendly interface. Labels provide information or titles for various sections.Entry widgets allow users to input or display information.Buttons trigger specific actions when clicked.A text box displays information, messages, or the extracted text. Tkinter Main Loop: Initiates the Tkinter event loop, allowing the GUI to respond to user interactions and run the application. Results and description Improved File Security System Using Multiple Image Steganography In this project as per your instructions we have developed PVD (Pixel Value Differencing) based image steganography where users can upload multiple images folder and then upload a text file which has to be slice and embed in all those uploaded images. All embed images will get saved inside the 'Encoded_Images' folder with text slice data hidden inside it. While decoding we can upload the desired folder from the 'Encoded_Images' folder to extract text. To embed text we are using below sample text file



Enhanced Security for Banking Transactions using Image Based Steganography

Encoding Images Folder: D:/SMEC MINI GEN/CODE/B11 Multiple

Upload Text File: D:/SMEC MINI GEN/CODE/B11 Multiple

Upload Folder to Extract Text:

```
D:/SMEC MINI GEN/CODE/B11 Multiple Image Steganography/Encoded_Images loaded
D:/SMEC MINI GEN/CODE/B11 Multiple Image Steganography/sample_text.txt loaded
```

Fig 2 :Upload text file to hide and PVD encoding

V. CONCLUSION

Multiple image steganography represents a significant advancement in the field of covert communication and secure data transmission. The technique of distributing hiddeninformation across a series of images, coupled with the Pixel Value Differencing (PVD) algorithm, offers a potent combination of security, resilience, and imperceptibility. The strategic division of data, error-correction techniques, spread spectrum methods, and secret sharing schemes contribute to the robustness and reliability of the steganographic system. The incorporation of cryptography and encryption enhances the confidentiality of the concealed information, while authentication and watermarking techniques provide mechanisms for verifying the integrity of the images. Hybrid approaches, integrating various steganographic methods and security measures, offer adaptability and versatility to meet diverse security requirements. However, the implementation of multiple image steganography is not without challenges. Synchronization during the embedding and extraction processes is crucial for accurate data retrieval. Striking a balance between usability and security is a delicate consideration, requiring thoughtful trade-offs to create an effective and user-friendly steganographic system. The use of multiple image steganography in banking transactions represents a substantial improvement in secure data concealment techniques, offering an innovative approach to safeguarding sensitive information. By employing the Pixel Value Differencing (PVD) algorithm and distributing hidden data across multiple images, this method bolsters both the security and imperceptibility of concealed messages. Techniques like error-correction, spread spectrum, and secret sharing schemes contribute to the reliability of the system, enabling a robust defense against unauthorized access.

V.REFERENCES

[1]. B. Sultan and M. A. Wani, "Multi-data Image Steganography using Generative Adversarial Networks," 2022 .

[2]. X. Liao, J. Yin, M. Chen and Z. Qin, "Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features," March-April 2022,

[3]. M. Srivastava, P. Dixit and S. Srivastava, "Data Hiding using Image Steganography," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), 2023.

[4]. A. G. Benedict, "Improved File Security System Using Multiple Image Steganography," 2019 International Conference on Data Science and Communication (IconDSC), Bangalore, India, 2019..

[5]. S. Mukhopadhyay and H. Leung, "Multi Image Encryption and Steganography Based on Synchronization of Chaotic Lasers," 2013 .

[6]. A. S. Ansari, M. S. Mohammadi and M. T. Parvez, "A Multiple-Format Steganography Algorithm for Color Images," 2020.

[7]. P. Grandhe, A. M. Reddy, K. Chillapalli, K. Koppera, M. Thambabathula and L. P. Reddy Surasani, "Improving The Hiding Capacity of Image Steganography with Stego Analysis," 2023 .

[8]. R. Joshi, A. K. Bairwa, V. Soni and S. Joshi, "Data Security Using Multiple Image Steganography and Hybrid Data Encryption Techniques," 2022.

[9]. Z. Wang, Z. Zhang and J. Jiang, "Multi-Feature Fusion based Image Steganography using GAN," 2021 .

[10]. X. Zhao and H. Huang, "Research on Image Steganography Based on Multiple Expansion Generation Adversarial Network," 2021.

[11]. B. Wei, X. Duan and H. Nam, "Image Steganography with Deep Learning Networks," 2022 ..

[12]. M. Liu, W. Luo, P. Zheng and J. Huang, "A New Adversarial Embedding Method for Enhancing Image Steganography," 2021.

[13].Kalaiarasi Survey on Image Steganography Techniques provides a comprehensive analysis of various methods in image steganography

[14].Muhammad Adnan Aslam "Image Steganography Using Least Significant Bit (LSB)

[15].Nandhini Subramanian "Image Steganography: A Review of the Recent Advances".

[16]. Priya ," focusing on contemporary methods in image steganography".

[17]. Yawar Rasheed " advancements in image steganography by adapting Least Significant Bit (LSB)".

[18]. Priya Thomas reviews several steganographic techniques, especially focusing on those based on transforming the domain of images.

[19]. Saud S,Alotaibi "Reversible Data Hiding with Interpolation Techniques".

[20]. Farooque Azam "Statistical and Adaptive Image Steganography Methods".