ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 11 Issue 7 July 2024

Developing a Secure Multimedia Communication System Using Steganography

[1] Prof. Megha S, [2] Manogna M S, [3] Meda Veerendra Charan Tej, [4] Meghana S, [5] Neha Vastrad G

[1] [2] [3] [4] [5] School of CSE Reva University Karnataka, India
Corresponding Author Email: [1] s.megha@reva.edu.in, [2] msmanognagnk@gmail.com, [3] charantej677@gmail.com, [4] meghanasg56@gmail.com, [5] neha.gv2@gmail.com

***Abstract*— This project focuses on applying steganography methods across different media formats by utilizing the Least Significant Bit (LSB) algorithm. The three main functions are video steganography, which hides text within video clips, audio steganography, which embeds information within audio files, and image steganography, which conceals text within images. The procedure combines a description method that uses a secure key with encryption for added security. The tkinter library was used in the development of the user interface, which offers a simple graphical user interface for smooth steganography features. This extensive project combines cutting-edge cryptography methods with intuitive design to disguise data effectively and securely across many media forms.**

***Index Terms*— steganography, Least Significant Bit, encryption, tkinter library, interface, cutting-edge.**

I. INTRODUCTION

In today's landscape, the transfer of sensitive data over the internet has become a precarious endeavor. With hackers constantly monitoring networks and launching assaults to pilfer valuable information, reliance on online data transfer has been restricted. Despite securely storing data on local systems, online transmission remains susceptible to breaches. The proliferation of digital formats, propelled by rapid advancements in information technology, has led to a significant increase in knowledge distribution via the interconnected network, or internet. However, ensuring information security to safeguard private data from dishonest individuals has emerged as a paramount concern in this environment of heightened vulnerability. Steganography and cryptography have emerged as crucial information security techniques in response to the vulnerabilities associated with data transfer. The program integrates both steganography and encryption within multimedia files, such as digital audio and video, to enhance the security of information exchange for both senders and recipients. Given the persistent threat landscape, communication processes must prioritize information security to mitigate risks effectively. The objective of this project is to create software allowing users to conceal a previously encrypted text message within a multimedia file. By leveraging a combination of Blowfish and RSA Public Key encryption techniques, the text message undergoes encryption to ensure confidentiality and facilitate efficient communication between the sender and the destination. This endeavor seeks to enhance

data security and privacy by embedding encrypted messages within multimedia files, thereby enabling secure transmission and storage. Additionally, the project incorporates the DES encryption method to encrypt the RSA Private Key File, requiring an eight-character password for added security. Introducing steganography into the software becomes imperative to further obscure the encrypted data. The program is designed to execute both splitting and decryption processes, enabling users to access and view the encrypted data seamlessly. This comprehensive approach enhances the security and concealment of sensitive information within multimedia files. The article establishes its focus on developing software aimed at concealing text messages within multimedia files through the integration of steganography and encryption techniques. It highlights the utilization of several cryptography techniques, including the Least Significant Bit (LSB) method for steganography, the Blowfish Encryption-Decryption algorithm for text message security, the RSA Public-Private Key algorithm for encrypting and decrypting the Blowfish Secret Key, and the DES algorithm for encrypting and decrypting the RSA Private Key File. By combining these cryptographic methods with injection steganography, the article aims to provide a comprehensive solution for securing data within multimedia files. Steganography is a technique that entails concealing data within an ordinary and non-secret message or file, rendering it undetectable until it reaches its intended recipient. When combined with encryption, steganography enhances data hiding and safeguarding. The English word" steganography" originates from the Greek words" steganos," meaning" hidden or covered," and" graph," meaning" to write." This amalgamation of techniques and their underlying principles underscores the importance of ensuring data security and confidentiality in digital communication. Steganography provides the capability to conceal nearly any type of digital content, ranging from text and photos to movies and audio files. Virtually all forms of digital content can serve as carriers for hiding sensitive information. When incorporating content into a seemingly innocuous cover text file or data stream, steganography, also known as hidden text, frequently encrypts the content to be concealed. In cases where the hidden text is not encrypted, alternative methods are often employed to complicate the decoding process, thereby enhancing the security of the secret information. Various forms of steganography exist, each tailored to specific types of digital media, including:

A. Image steganography: Image steganography involves using an image as the cover object, with information hidden based on pixel intensities. This method utilizes various terms, such as stego-image (which refers to the combination of the message and cover image), cover image (which serves as the carrier for confidential information), and sensitive information (which is the data to be concealed within the graphics). [1].

B. Audio steganography Audio steganography employs audio files as the cover object, utilizing digital audio formats such as WAVE, MPEG, and others to conceal information. This method provides a robust means of safeguarding privacy and is considered one of the most effective ways to ensure data confidentiality. [2]

C. Video steganography Video steganography utilizes a video file as the cover object, which can be in formats such as MP4, MPEG, or others. Information is concealed within the video, leveraging the abundance of frames available. Due to the numerous frames, it becomes straightforward to conceal information within a movie. Compared to digital images, videos offer a deeper embedding capability, making video steganography a powerful method for hiding information securely. [3]

D. Network steganography Network steganography involves the utilization of network protocols like TCP, UDP, IP, among others. This technique operates by implementing a single network protocol change to conceal information. This approach enables the covert transmission of data within network communications, making it difficult for unauthorized parties to detect the hidden information.

E. Text steganography Text steganography utilizes text as the cover object, employing various techniques to conceal information within textual data. It can be categorized into three main approaches: 1. Format-based methods: These methods involve altering the format or structure of the text to embed hidden information. Examples include modifying whitespace, punctuation, or formatting elements. 2. Random and statistical generation: This approach involves generating random or statistically manipulated text to embed hidden information. Techniques may include altering word frequencies, sentence lengths, or using pseudo-random generators. 3. Linguistic approaches: Linguistic steganography techniques exploit linguistic properties of the text, such as semantic meanings, syntactic structures, or grammatical rules, to conceal information. This may include using synonyms, homophones, or linguistic anomalies to encode hidden messages. Each category offers distinct methodologies for concealing information within textual data, catering to different requirements and preferences in text steganography. [4].

In an era marked by heightened concerns regarding privacy and data security, the importance of information concealment has surged. Steganography emerges as a pivotal technique for secure communication, offering protection for private information from unauthorized access. This paper delves into the intricate domain of steganography, with a specific focus on implementing the Least Significant Bit (LSB) algorithm. The LSB technique presents an imperceptible method for embedding data within digital media, ensuring that the altered content closely resembles its original form. To cater to diverse requirements and digital formats, this research leverages the versatility of the LSB methodology across three different media formats: photos, audio, and video. Through this investigation, the aim is to provide a robust and adaptable approach to text hiding, bolstering data security in various digital contexts. This project is built upon a systematic process of information extraction and embedding, ensuring a structured approach to data concealment. Encryption plays a crucial role in enhancing the security of hidden data, requiring an encryption key for both embedding and extraction procedures. This security measure ensures that only authorized users have access to the concealed data, thereby safeguarding its confidentiality. Moreover, the project includes the development of a graphical user interface (GUI) using the tkinter library. This GUI provides an intuitive platform for users to interact with steganography capabilities, making it easy and accessible to conceal text across various digital media formats. By integrating state-of-the-art cryptographic techniques with a user-friendly interface, the project aims to create a dependable and approachable platform for text concealment, thereby enhancing data security in diverse digital environments.

II. LITERATURE SURVEY

In the process described in [5], data is concealed within another image using steganography techniques. Initially, the final bits of the original image are replaced with an encrypted version of the data to be hidden. Subsequently, the bits in the encrypted cover picture disperse in a zigzag pattern, rendering it extremely challenging to recover the concealed data, even in the event of an attack, owing to the encryption and scattering techniques employed. The encrypted cover photo, containing the concealed data, can be transmitted via communication channels such as WhatsApp or email over the internet. To ensure secure access to the hidden data, a stego key is generated, allowing only the sender and recipient to decrypt and access the secret information. This methodology proves particularly beneficial in defensive contexts when transmitting sensitive material and holds high statistical requirements for ensuring data security.

In [6], the technique described for concealing data within an image file is known as image steganography, employing the Least Significant Bit (LSB) Algorithm. This method involves substituting hidden data bits for the least significant color values in the image pixel values. By doing so, the operation typically results in minimal changes to the pixel values, which are often imperceptible to the human eye, rendering the concealed data virtually invisible. The LSB algorithm is acknowledged as the most straightforward and commonly used method for image steganography. However, due to its ease of data recovery, it is also considered one of the least secure methods available. Despite its simplicity and widespread usage, the vulnerability to data extraction makes it necessary to consider more robust steganographic techniques for applications requiring higher levels of security.

In [7], the process of preprocessing images is highlighted as a crucial step in making the image suitable for steganography. Preprocessing plays a significant role in the digital image processing phase, particularly when working with high-resolution images. The post emphasizes the use of high-resolution photos and the integration of grayscale image conversion within the image coding network. To streamline the algorithmic complexity, the technique involves converting a 3-channel, high-resolution color image into a 1-channel grayscale image. This conversion simplifies the image representation while retaining essential visual information, making it suitable for subsequent steganographic embedding processes. By reducing the complexity through grayscale conversion, the preprocessing step enhances the efficiency and effectiveness of the steganographic techniques applied to the image.

In [8], an understanding of cryptography is deemed essential to comprehend the nuances of steganography. The passage elucidates the fundamental differences between these two theories of information concealment. While steganography focuses on concealing the mere existence of a message within a medium, cryptography is concerned with obfuscating the meaning of the hidden message itself. Additionally, cryptography relies on keys for both encryption and decryption processes. Unlike cryptography, steganography employs various types of mediums, each with its distinct implementation techniques, as coverings to conceal secret messages. This diversity allows steganography to conceal information within a wide array of digital mediums, enhancing its versatility and applicability across different contexts.

In [9], the discussion revolves around the efficiency and effectiveness of different LSB (Least Significant Bit) techniques for embedding data into images. It is stated that modifying the final two bits of each pixel in the cover image allows for a significantly larger amount of data to be embedded compared to the 1-bit LSB method, all while maintaining the original image's quality. The two-bit LSB technique offers the advantage of storing four different values using 2 bits (00, 01, 10, 11), thereby enabling the storage of more information per unit of data. This approach allows for greater text embedding capacity while minimizing the impact on the perceived quality of the carrier medium. Moreover, when compared to three- and four-bit LSB approaches, changes made using the two-bit LSB method are less visible to the human eye and have a lesser effect on the overall quality of the image. Theoretically, the two-bit LSB technique combines the benefits of increased data embedding capacity with improved image quality preservation, making it a favorable choice for steganographic applications.

In [10], visual cryptography is acknowledged for its superior security and resilience due to its creation of shares that can only be decoded when overlaid. However, a hybrid model combining LSB steganography and AES cryptography technology introduces an additional layer of security by encrypting the data before embedding it into the image. This hybrid approach ensures that even if the steganography is detected, the encrypted data remains protected. While this hybrid model may not match the reliability of visual cryptography, it offers a trade-off between security and robustness. The effectiveness of the chosen strategy depends on the specific requirements and uses case. Therefore, the ideal approach involves considering the balance between security and robustness to meet the desired level of data protection in practical applications.

In [11], the quality of the encoded image is influenced by several factors, with the embedding position of the message being a crucial determinant. Embedding a message into complex texture sections of an image is essential to ensure a higher level of consistency between the embedded message and the image contour. To achieve this, the encoder must possess the capability to accurately extract image features, enabling reliable embedding while preserving the visual integrity of the image. This emphasis on selecting appropriate embedding positions within the image contributes significantly to maintaining the overall quality and effectiveness of the encoded message.

In [12], the stego-only attack is described as a type of attack where the attacker possesses only the stego-image, without access to the original cover image. To mitigate this attack, it's crucial to ensure that no blocking artifacts related to message embedding are present in the stego-image, as attackers could exploit these artifacts to uncover the hidden message. The stego-image, modified using the CAS (Complexity Adaptive Steganography) method, undergoes subtle changes in pixel values to insert messages based on the local characteristics of image blocks. Consequently, the stego-image maintains excellent fidelity and closely resembles the cover image, making it less suspicious to casual attackers who are unaware of its concealed message. Even in the event of unintentional attacks such as rotation or scaling, the embedded message may become unretrievable but remains intact within the stego-image. Ultimately, the encoded message can still be extracted by synchronizing the stego-image with the original cover image, thereby preserving the security and integrity of the hidden message despite potential attacks.

In [13], audio steganography is highlighted as a method for transmitting covert battlefield information using an innocuous cover audio signal. The success of this technique hinges on ensuring that the resulting stego signal, after embedding the covert message, remains perceptually indistinguishable from the original host audio signal. This seamless integration is essential for effectively concealing the covert message within the audio file. Moreover, beyond concealing the message, it is imperative that the embedded message can be accurately recovered by the intended recipient. This ensures the reliability and effectiveness of the communication process. Depending on the specific application requirements, additional considerations may include the ability to retrieve data without access to the original cover signal and the need for robust embedding techniques to withstand potential signal distortions or attacks. These factors underscore the importance of designing audio steganographic systems that meet the diverse needs of covert communication scenarios, especially in sensitive environments such as battlefield operations.

In [14], the extraction phase involves retrieving the original message from the stego-image, which is the reverse process of embedding. The suggested technique prioritizes security by utilizing symmetric key sharing and dual-level security measures, enhancing the overall safety of the system. This approach ensures that only authorized parties with access to the symmetric key can extract the hidden message, bolstering the confidentiality of the communication process. In the context of colored image steganography, the suggested algorithm demonstrates superior performance compared to existing methods, particularly in terms of invisibility. By optimizing the embedding process, the suggested algorithm achieves a higher level of stealthiness, making the embedded message less perceptible to unintended viewers. This improved invisibility enhances the covert nature of communication, making it more effective for clandestine purposes.

In [15], the least significant bits (LSB) method is high-lighted for its high payload capacity and simplicity as a steganography technique. This method involves replacing the final bits of the stego-image with secret data, effectively concealing information within the image. By utilizing LSB, it becomes challenging for humans to visually distinguish between the original and stego-image through simple visual inspection. Furthermore, hybrid edge detectors, which are based on LSB, are mentioned as another steganography technology aimed at increasing capacity and invisibility. According to this approach, secret bits are predominantly placed in edge pixels rather than smooth pixels. This strategy is employed because edge pixels are less prone to modifications after the hiding of secret data, thereby enhancing the invisibility of the embedded information within the image.

In [16], In this scenario, an MP3 file serves as the cover object for steganography. The Advanced Encryption Standard (AES) technique is employed to encrypt the secret message, ensuring its confidentiality. To generate the encryption key, the MD5 hash function is utilized. Within the MP3 files, an integrated key code and the encrypted data are embedded, facilitating the secure transmission and retrieval of the hidden message.

In [17], The process of injecting information into carrier files, it’s essential to note that each multimedia file can only serve as a carrier for concealed information once. This limitation arises from the fact that any data appended after the multimedia portion within the file remains embedded in the background after the initial injection operation. As a result, attempting a second injection of concealed information within the same Stegano File using the software would be unsuccessful. Users would encounter an error message prompting them to choose a different cover file to proceed with the concealment process. This constraint underscores the importance of careful selection and planning when utilizing carrier files for steganographic purposes.

In [18], concerns regarding phishing attacks and unauthorized access to multimedia data or content, potentially by individuals such as service provider employees, are highlighted. These risks underscore the importance of safeguarding sensitive information stored within multimedia files. Measures such as encryption, access controls, and secure transmission protocols may be necessary to mitigate the threat of unauthorized access and data breaches in multimedia environments.

In [19], the process involves embedding hidden messages into various types of cover media such as audio, video, and images. Subsequently, thorough testing is conducted from multiple perspectives to evaluate the efficacy of the steganographic process. These evaluations encompass several aspects:

1. Quality comparison of the cover media before and after steganography to assess any perceptible changes or degradation in quality.
2. Recovery test of the embedded secret message to ensure successful extraction.
3. Assessment of the size of the secret message both before and after steganography to determine any changes in data size. 4. Evaluation of the size of the cover media before and after steganography to ascertain any alterations in file size.
4. Human perception tests to gauge the visibility or detectability of the embedded message by human observers. These comprehensive evaluations help assess the effectiveness and reliability of the steganographic techniques employed, ensuring that hidden messages can be securely embedded and extracted without compromising the integrity or quality of the cover media.

In [20], the safest method for transmitting confidential data over the internet via steganography involves utilizing digital images. These images are captured using a camera, which detects the subject and displays it on the camera's screen. Digital images consist of pixels, with each pixel determining the resolution of the picture. Pixels, the smallest units of light on a display screen, are imperceptible to the human eye. A pixel comprises three components: Red, Green, and Blue (R, G, and B), each represented by a single byte, totaling 24 bits or 3 bytes per pixel. The combination of these components produces various colors, with each component's byte value ranging from 0 to 255. The color displayed depends on the bit values, where 0 signifies the darkest shade and 255 indicates the brightest.

III. SYSTEM ARCHITECTURE

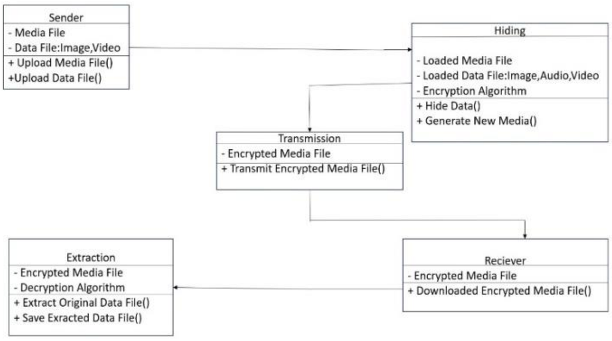


Figure 1. Steganography system Architecture

IV. ER DIAGRAM

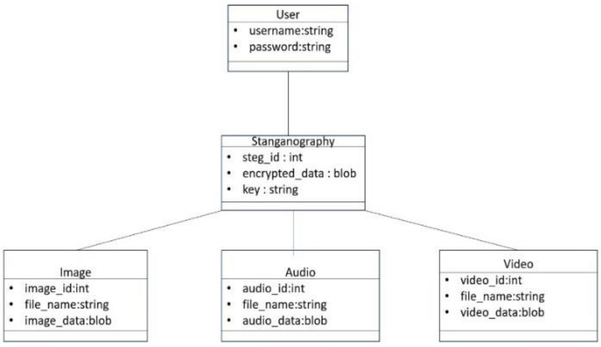
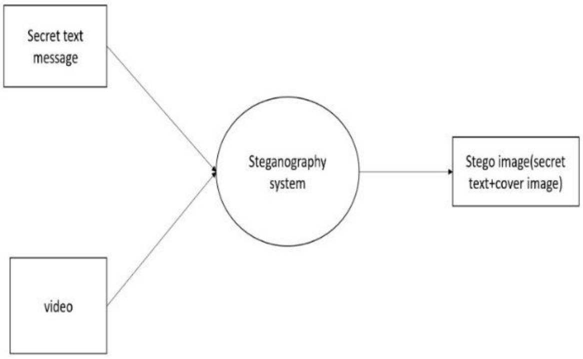


Figure 2. Steganography entity relationship model

V. FLOWCHART



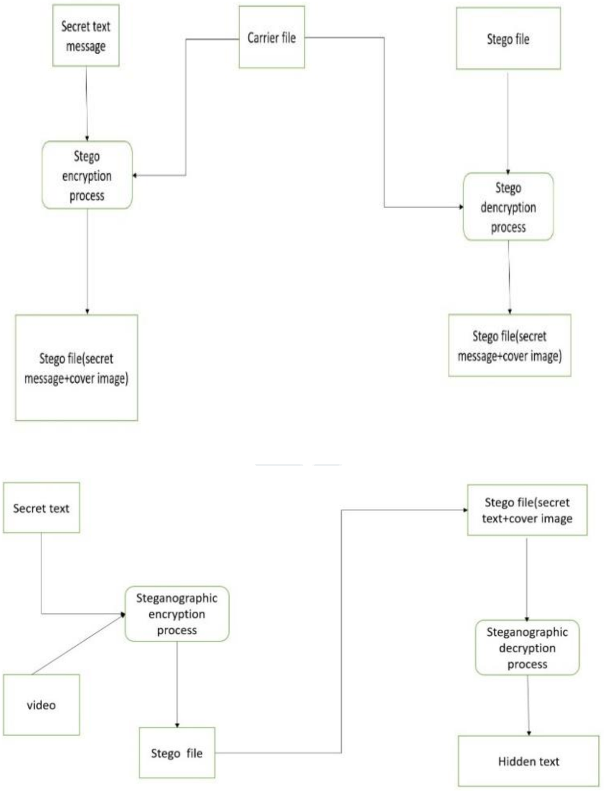

Secret text message
Carrier file
Stego file
Stego encryption process
Stego dencryption process
Stego file(secret message+cover image)
Stego file(secret message+cover image)
Secret text
video
Steganographic encryption process
Stego file
Stego file(secret text+cover image
Steganographic decryption process
Hidden text

Figure 3. Steganography framework

VI. METHODOLOGY

The methodological framework outlines a systematic approach and sequential process to effectively execute the steganography project. It includes several phases: 1. Requirement Analysis and Specification: This initial phase involves a comprehensive examination of requirements, user expectations, and intended outcomes. Stakeholders are interviewed, and user needs are compiled to define specific features such as LSB-based image, audio, and video steganography, encryption integration, and GUI development using tkinter. Requirements document detailing functionalities and specifications is created. 2.Research and Literature Review: In this stage, an extensive analysis of existing knowledge, scholarly works, and relevant materials related to steganography, the LSB algorithm, encryption methods, and tkinter GUI development is conducted. Informed decisions regarding design and implementation are based on this research, including reviewing scholarly literature on steganography techniques and examining cryptographic algorithms and their integration with steganography. 3.Algorithm Design and Implementation: The selected steganography algorithms, particularly the Least Significant Bit (LSB) algorithm, are implemented in this phase. Distinct modules for image, audio, and video steganography are developed to ensure precise data embedding and extraction procedures. The LSB algorithm is applied to steganography of images, audio steganography module is created using LSB, and a video steganography module integrated with LSB is built. 4.Encryption Integration: This phase focuses on enhancing data security by incorporating encryption techniques. Steganography is combined with symmetric key encryption, such as AES, which requires a secure key for data extraction. The objective is to implement AES encryption for secure data hiding and create encryption and decryption key management systems. 5.Graphical User Interface (GUI) Development: Using the tkinter library, the GUI development phase aims to create an intuitive and user-friendly interface. Features for user interaction, including file selection, input of encryption keys, and output display, are implemented to facilitate easy engagement with the steganography toolbox. This methodological framework ensures a thorough and dependable execution of the steganography project, encompassing requirement analysis, research, algorithm design, encryption integration, and GUI development.

VII. CONCLUSION

Steganography, a captivating data hiding technique with a rich historical background, has found its place in modern data protection strategies. It offers a means to safeguard critical information like passwords and defence-related data transfers, complementing other storage methods such as watermarking. As our understanding of its features and functionalities grows, steganography becomes increasingly accessible for various applications. This paper delves into the utilization of wavelet transformation within the Least Significant Bit (LSB) approach to embed one image into another. The focus lies on steganalysis of the LSB approach, particularly concerning security applications in the defence industry. The study assesses the effectiveness of steganography in scenarios with and without noise, noting that in noisy images, Peak Signal-to-Noise Ratio (PSNR) values typically fall between 30 dB to 50 dB. The method discussed in this paper achieves a PSNR of 37 dB for noisy images and infinity for noise-free ones. However, a limitation of this technique is identified: it struggles to handle decryption of fuzzy images accurately during encryption, resulting in some data loss when encrypting hazy photos. Nonetheless, there is potential for further development. Future research could explore ways to enhance the image-to-text compression ratio and devise advanced algorithms capable of transmitting multiple hidden audio, video, and image files over a single carrier, expanding the scope and efficacy of steganographic methods.

REFERENCES

[1] Mehdi Hussain and Mureed Hussain - “A Survey of Image Steganography Techniques” International Journal of Advanced Science and Technology Vol. 54, May 2013.

[2] Fatiha Djebbar and Beghdad Ayad and Karim Abed Meraim and Habib Hamam - “Comparative Study of Digital Audio Steganography Techniques”.

[3] R. Balaji, G. Naveen - “Secure data transmission using video steganography”.

[4] Monika Agarwal - “Text Steganographic Approaches: A comparison” International Journal of Network Security and Its Applications (IJNSA).

[5] “Image Steganography for confidential data communication”- S. Sravani Department of Electrical and Electronics Engineering Amrita School of Engineering, Coimbatore Amrita Vishwa Vidyapeetham, India, R. Ranjith Department of Electrical and Electronics Engineering Amrita School of Engineering, Coimbatore Amrita Vishwa Vidyapeetham, India, 2021.

[6] “Secure File Sharing System using Image Steganography and Cryptography Techniques”- U A Solomon Raj Computer Science and Engineering Karunya Institute of Technology and Sciences Coimbatore, India, Dr. C P. Maheswaran Computer Science and Engineering Karunya Institute of Technology and Sciences Coimbatore, India,2023.

[7] “Generative Image Steganography Scheme Based on Deep Learning”- Jingyi Qiu Tongda College of Nanjing University of Post and Telecommunications, Yangzhou, Jiangsu, China,2022.

[8] “A Novel Steganography Approach to Embed Secret Information into a Legitimate URL”- Kholood Ayed Almalki College of Computer Science and Engineering Jeddah University Jeddah, Saudi Arabia, Roshayu Mohammed College of Computer Science and Engineering Jeddah University Jeddah, Saudi Arabia, Roshayu Mohammed College of Computer Science and Engineering Jeddah University Jeddah, Saudi Arabia, Jan,2022.

[9] “LSB Steganography mechanism to hide texts within images backed with layers of encryption”-Ishaan Shukla Pune Institute of Computer Technology Pune, India, Atharva Joshi Pune Institute of Computer Technology Pune, India, Prof. Shital Girme Pune Institute of Computer Technology Pune, India,2023.

[10] “Exploring the Effectiveness of Steganography Techniques: A Comparative Analysis”-Dr. Sowmya K. S Department of Information Science and Engineering B.M.S College of Engineering Bengaluru, India, Sumith Hegde Department of Information Science and Engineering B.M.S College of Engineering Bengaluru, India, Sunag P Department of Information Science and Engineering B.M.S College of Engineering Bengaluru, India, Varun R P Department of Information Science and Engineering B.M.S College of Engineering Bengaluru, India,2023.

[11] “An image steganography method based on texture perception”- Lianqiang Niu School of Software, Shenyang University of Technology Shenyang, China, Jing Zhang School of Information Science and Engineering, Shenyang University of Technology Shenyang, China,2004.

[12] “A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem”- Der-Chyuan Lou and Chia-Hung Sung ,2004.

[13] “Audio Steganography using Bit Modification”- Kaliappan Gopalan Department of Engineering, Purdue University Calumet, Hammond, IN 46323.

[14] “An Improved Method for Reversible Data Hiding Steganography Combined with Cryptography” -Ms. Rashmi N Dr Jyothi K Dept. of ISE, Professor and Head, Dept. of ISE, NMAM Institute of Technology, Nitte JNNCE, Shimoga Karnataka, India Karnataka, India,2018.

[15] "Image Steganography Based on Hybrid Edge Detector to Hide Encrypted Image using Vernam Algorithm"- Zainab F. Yaseen Department of Computer Science University of Technology - Iraq Baghdad, Iraq, Abdulameer A. Kareem Department of Computer Science University of Technology - Iraq Baghdad, Iraq,2019.

[16] "Secure Data Transfer Through Internet Using Cryptography and Image Steganography"- Krishna Chaitanya Nunna, Ramakalavathi Marapareddy School of Computing Sciences and Engineering, The University of Southern Mississippi, Hattiesburg, USA, 2020.

[17] "Steganography Software with Combination of Encryption Algorithms for Multimedia Files"- Nur Hadisukmana Faculty of Computing President University Bekasi, Indonesia, Yosua Kristianto Faculty of Computing President University Bekasi, Indonesia,2011.

[18] "Analysis of Secure Multimedia Communication in Cloud Computing"- Sharath M N Research Scholar Dr. Rajesh Asst. Professor, T M Dr. Mallanagouda Patil Associate Professor, Department of Computer Science, Dayananda Sagar University,2019.

[19] "Human Perception Evaluation toward End of File Steganography Method's Implementation Using Multimedia File (Image, Audio, and Video)"- Rini Indrayani Faculty of Computer Science, Universitas Amikom Yogyakarta Yogyakarta, Indonesia,2019.

[20] "Secret Communication using Multi-Image Steganography for Military Purposes"-Pratik Wani1, Anuja Nanaware 2, Sneha Shirode3, Aishwarya Suram 4, Prof. Archana Jadhav5 Students, Department of Informa- tion Technology1,2,3,4 Associate Professor, Department of Informa- tion Technology5 JSPM'S Rajarshi Shahu College of Engineering, Tathawade, Pune, Maharashtra, India,2022.