iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** V **Month of publication:** May 2024

DOI: https://doi.org/10.22214/ijraset.2024.62639

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue V May 2024- Available at www.ijraset.com

Unified Steganography for Concealing and Extracting Secret Messages

Mohammed Yasir[1], Havi Gowda R[2], Rukhiya Bee[3], Dr. Rama Krishna K[4]
[1, 2, 3]*Students, Dept of AI&ML Impact college of Engineering and applied Sciences, Bangalore, Affiliated to VTU*
[4]*Professor and Head, Dept of AI&ML Impact college of Engineering and applied Sciences, Bangalore, Affiliated to VTU*

Abstract: ***With the increasing significance of data security in the digital age, steganography has emerged as a crucial technique for concealing information within various forms of media. This paper presents a unified steganographic framework designed to embed and extract secret messages in images, audio, and text files. Utilizing the Least_Significant_Bit (LSB) method, our approach ensures minimal distortion of the host media while maintaining high security and robustness of the hidden messages. The system is implemented in Python, featuring an intuitive graphical user interface (GUI) to facilitate user interaction. Comprehensive experiments and analyses demonstrate the effectiveness of our method in maintaining the imperceptibility and integrity of the steganographic media. This unified solution offers a versatile and efficient tool for secure communication, digital watermarking, and protection of intellectual property. Our findings underline the potential of integrating steganographic techniques across different media formats to enhance data security and privacy.***

Keywords: ***Steganography, Data Security, Least_Significant_Bit (LSB), Image_Steganography, Audio_Steganography, Text_Steganography, Digital Watermarking, Secure Communication, Data Hiding, Information Concealment, Steganalysis, Cryptography, Information Security, Data Embedding, Digital Steganography, Secret Message Extraction, Image Processing, Audio Processing, Text Encoding, Steganographic Techniques.***

I. INTRODUCTION

Steganography, derived from the Greek words "steganos" (meaning hidden) and "graphy" (meaning writing), is an ancient technique that is used to conceal secret information within innocent-looking carriers such as images, audio files, or text documents. This clandestine nature makes steganography a vital tool in various fields, including cybersecurity, espionage, and digital forensics. The digital era has witnessed a significant surge of steganographic techniques of digital media and the increasing requirement for secure communication channels. With the vast amount of new data transmitted over networks daily, the required ability to conceal sensitive information within seemingly innocuous files has become indispensable. Consequently, researchers and practitioners alike are continuously innovating and refining steganographic methods to enhance their effectiveness while mitigating detection risks. The Unified Steganography project presented herein addresses the growing demand for robust and versatile steganographic solutions across different media types. By providing a comprehensive framework for concealing and extracting secret messages from images, audio files, and text documents, the project aims to streamline the steganographic process and facilitate secure communication in diverse scenarios. In this paper, we elucidate the design, implementation, and functionalities of the Unified Steganography system. We delve into the underlying principles of steganography, explore existing techniques employed in concealing and extracting secret messages, and introduce novel methodologies devised to highly improve the concealment capacity and robustness of the system. Furthermore, we assess the performance of the Unified Steganography system through rigorous testing and benchmarking, demonstrating its efficacy in real-world scenarios. Through the culmination of extensive research, innovative design, and rigorous testing, the Unified Steganography project endeavors to advance the steganography and contribute to the ongoing efforts aimed at securing digital communications in an increasingly interconnected world. Steganography has changed significantly since its inception, driven by advancements in digital technology and the perpetual cat-and-mouse game between concealment and detection techniques. Traditional steganographic methods, such as Least_Significant_Bit (LSB) and masking, have paved the way for more sophisticated approaches, including transform domain techniques and adaptive embedding strategies. These advancements have enabled steganography to transcend mere data_hiding and evolve into a multifaceted discipline encompassing covert communication, authentication, and digital watermarking. The Unified Steganography project represents a culmination of these advancements, offering a unified platform for concealing and extracting secret messages across multiple media formats. By improving the strengths of various steganographic techniques and integrating them into a cohesive framework, the project seeks to discourse the inherent limitations and fragmentation present in existing steganography tools.

Through a blend of modular design, extensibility, and user-friendly interfaces, the Unified Steganography system empowers users to conceal sensitive information with ease while ensuring robustness and resilience against detection. Furthermore its practical applications in secure communication and data protection, the Unified Steganography project holds promise in advancing research in steganography and related areas. The system's open architecture and extensible design provide a fertile ground for experimentation and innovation, encouraging researchers to explore new avenues in steganography.

II. LITRETURE SURVEY

Image_Steganography: A_Review_of_the-Recent-Advances: The paper provides a comprehensive review of recent improvements in image steganography. It focuses on deep learning techniques, categorizing them into traditional ways, Convolutional_Neural_Network (CNN)-based methods, and Generative Adversarial Network (GAN)-based methods. The paper details the datasets used, experimental setups, and evaluation metrics. It aims to assist researchers by compiling current trends, challenges, and future directions in the field. [2]. Steganography Techniques Using Convolutional Neural Networks: The paper explores modern steganography techniques, aiming to hide digital messages within images using deep learning methods. The study employs Convolutional_Neural_Networks (CNNs) along with traditional LSB encoding to achieve minimal distortion in the hidden message, making it invisible to the naked eye while ensuring its integrity. These networks effectively encode and decode messages without significant changes to the cover image, offering a secure method of information concealment that resists standard steganalysis techniques. The research demonstrates the effectiveness of using CNNs for image steganography, enhancing security through obscurity. The integration of LSB encoding and deep learning techniques provides a robust method for hiding and revealing messages with minimal distortion. [3]. Recent_Advances_of_Image_Steganography_with-Generative-Adversarial-Networks: Generative_Adversarial_Networks (GANs), introduced in 2014, have achieved significant success in computer visioning and natural-language processing. Image-steganography, a way for hiding secret-messages within digital images for covert communication, has given great-potential with the incorporation of GANs. The paper shows the advancements in GAN-based image steganography, focusing on different data hiding strategies: cover-modification, cover-selection, and cover-synthesis. The paper discusses the characters and evaluation metrics of these strategies, summarizes current challenges, and explores future research directions. The integration of GANs into image steganography has enabled new research avenues, combining computer vision with information security. While GAN-based methods offer innovative solutions, they also present unique challenges. Continued research will focus on improving capacity, evaluation methods, and steganalysis, aiming to develop more secure and efficient steganography techniques. [4]. Research on Coverless Image Steganography: The paper titled "Research on Coverless-Image-Steganography" by Kurnia Anggriani, Nan-I Wu, and Min-Shiang Hwang investigates the evolution and advancements in Coverless Image Steganography (CIS) over the past five years. CIS, introduced in 2015, represents a departure from traditional steganography-methods by concealing information within images without directly modifying the cover-image. Instead, CIS employs a mapping operation to select a stego-image, thereby avoiding any visible alterations to the cover_image and enhancing resilience against steganalysis tools. [5]. Review on feature-based method performance in text_steganography: The paper titled "Review on feature-based method performance in text steganography" discusses the importance of text steganography as a means to hide essential messages in text formats to avoid detection by intruders. It specifically focuses on the feature-based method within text_steganography and reviews previous research efforts in this area over the last decade. The paper aims to explore the performance of methods used in the making of feature-based text steganography methods and highlights related issues. [6]. Generative Text Steganography Based on LSTM Network and Attention Mechanism with Keywords: The paper titled "Generative Text Steganography Based on LSTM Network and Attention Mechanism with Keywords" introduces a approach to text steganography leveraging deep_neural-networks (DNNs), specifically long-short-term-memory (LSTM) networks. Given the widespread use of text in online social networks, the paper addresses the necessity for efficient and secure steganographic communication methods in this context. [7]. Logistic_Tan-Map-Based Audio-Steganography: The paper titled presents an innovative approach to audio steganography, combining both cryptography and steganography-techniques to enhance communication security. The proposed method utilizes both AES-128 encryption for scrambling the secret-message and steganography_techniques to embed the scrambled-message into an audio_cover file using the Least_Significant_Bit (LSB) method. [8]. A Comparative Study of Audio Steganography Schemes: The paper titled "A Comparative Study of Audio Steganography Schemes" introduces a double-layer that combines cryptography-way and steganography_techniques for secure communication. [9]. A_New_Steganography_Method for Hiding-Text into RGB_Image: The paper introduces method for encrypting-secret_messages in RGB images, aiming to enhance data security. The proposed method employs Huffman encoding to compress the secret message, reducing its dimensionality, and utilizes XOR and XNOR logic gates for encryption to enhance message security. [10].

Steganography Techniques – A Review Paper: The paper titled "Steganography Techniques – A Review Paper" provides an overview of various steganography methods employed for securing communication by hiding data within cover images. The importance of maintaining confidentiality between communicating parties and highlights various techniques and methods used for data embedding and extraction.

III. AIM AND OBJECTIVES

The purpose and aims outlined entail:

A. Aim

The aim is to build a unified steganography system capable of effectively concealing and extracting secret messages within various types of cover media, including images, audio files, and text documents. The model aims to enhance the advanced-security of communication channels by providing a robust and versatile method for covert data transmission.

B. Objectives

1) Develop a Comprehensive Steganography Framework: The primary objective is to implement a unified_steganography framework that can seamlessly embed and extract secret messages across different kinds of digital media.
2) Enhance Security and Robustness: Implement advanced encryption and embedding techniques to ensure the safekeeping and strength of the steganography system against detection and attacks.
3) Support Multiple Types of Cover Media: Enable the steganography system to work with various types of cover media, including images, audio files, and text documents, to accommodate diverse communication requirements.
4) Optimize Embedding_Capacity and Fidelity: Optimize the embedding_capacity of the system while maintaining high fidelity of the cover_media to minimize perceptible changes and maximize the content of hidden information.
5) Evaluate Performance and Effectiveness: Conduct extensive performance evaluations to assess the effectiveness, efficiency, and safety of the developed steganography system under various scenarios and conditions.
6) Provide User-Friendly Interface and Integration: Develop a user-friendly interface for seamless integration of steganography_system into existing communication platforms, ensuring betterment for end-users.
7) Explore Real-World Applications and Use Cases: Explore potential real-world applications and use cases of the unified steganography system across different domains, including cybersecurity, data privacy, and covert communication.

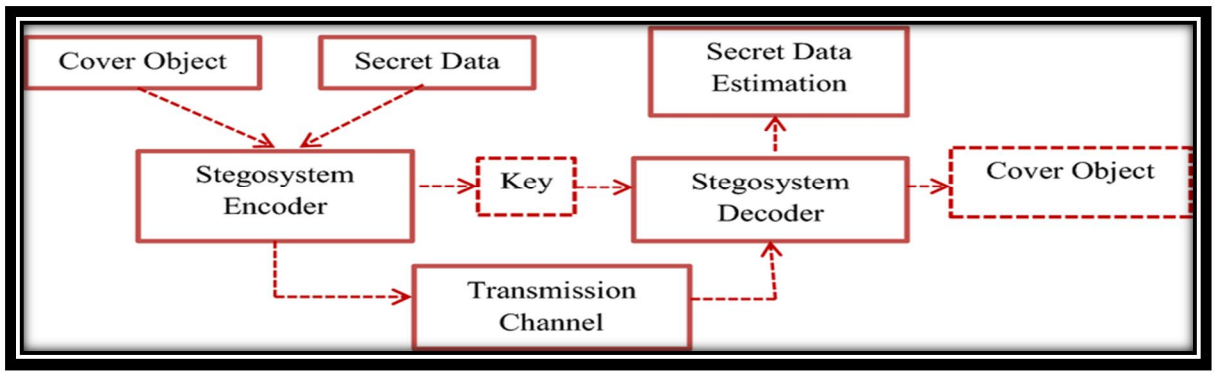


Fig 1: Working of Steganography Model

IV. DESIGN AND IMPLEMENTATION

A. Proposed System

The proposed steganography_system is build to provide a comprehensive solution for concealing and extracting secret messages across multiple types of digital media. The system architecture comprises several interconnected modules responsible for different tasks, including encryption, embedding, extraction, and user interface interaction. The system leverages advanced encryption algorithms and embedding techniques to ensure the safety and strength of hidden data transmission. Additionally, it supports various types of cover media, such as images, audio files, and text documents, offering flexibility and versatility in covert communication.

B. Modules

1) Module 1: LSB (Least Significant Bit) Embedding and Extraction

- Embedding: The module includes functions to embed secret_messages into cover_images by replacing the least_significant_bits of selected pixels with the bits given of the message.
- Extraction: It provides functions to extract hidden messages from stego-images by retrieving the least_significant_bits of specific pixels.
- The LSB way of technique is straightforward to implement and understand, making it accessible for developers.
- While LSB is susceptible to detection by advanced steganalysis techniques, it remains effective against basic inspection methods.
- The LSB module can be applied to various types of digital images, including grayscale and color images, without significant modification.

2) Module 2. Front-end Components

➢ Front-end GUI Design using PyQt

- Graphical user interfaces (GUIs) play a significant role in improving the user experience using software.
- GUIs provide an intuitive way to interact with complex systems.
- The integration of PyQt offers flexibility and scalability for future development.
- Using PyQt's features and functionalities, the aim is to create a GUI that meets system requirements and improves user experience.
- Various aspects of the GUI will be explored to facilitate interaction with the underlying system.

3) Module 3. Integrated Development Environments (IDEs)

➢ PyCharm:

- PyCharm provides intelligent code completion, syntax highlighting, and code navigation features, facilitating faster coding and reducing errors.
- It offers context-aware code suggestions and auto-import capabilities, making it easier to work with Python libraries and modules.
- The IDE includes powerful refactoring tools for renaming variables, extracting methods, and restructuring code.
- It ensures code maintainability and readability by automatically updating references across the project.
- PyCharm's built-in debugger allows for seamless debugging of Python code, enabling developers to set breakpoints, inspect variables, and step through code execution.
- It provides real-time debugging feedback and supports both local and remote debugging scenarios.
- PyCharm is highly customizable, allowing developers to tailor the IDE to their preferences and workflow.
- It supports plugin development and offers a rich ecosystem of third-party plugins to extend its functionality further.

V. METHODOLOGY

A. Data Collection

Data collection involved sourcing sample and demo images which are publicly available in datasets and creating custom datasets for performance evaluation. Challenges in data collection were mitigated through thorough validation and selection processes.

B. Experimental Setup

The experimental setup comprised high-performance computing hardware, including Intel Core i7 processors and ample RAM, to support intensive computational tasks. PyCharm, a robust Integrated Development Environment (IDE) for Python development, was utilized for software implementation.

C. Methodological Framework

Developed a comprehensive framework integrating various steganographic techniques, including Least_Significant_Bit (LSB) embedding, to meet project objectives. Emphasis placed on robustness and efficiency in concealing and extracting secret messages.

D. Evaluation Metrics

Evaluated system performance using established metrics such as Mean_Square_Error (MSE), Peak_Signal-to-Noise Ratio (PSNR), and embedding capacity. The given metrics were chosen based on their relevance to measuring the effectiveness and efficiency of the steganography_system.

E. Experimental Procedure

Conducted experiments involving preprocessing of input data, embedding secret_messages into cover_images using LSB embedding techniques, and the extraction of hidden_messages from stego-images. Rigorous analysis of evaluation metrics ensured reproducibility and validation of experimental results.

VI. CONCLUSION

In conclusion, "Unified Steganography for Concealing and Extracting Secret Messages" presents a comprehensive approach to secure communication through the concealment and the extraction of secret_messages within digital media. Through the integration of various steganographic techniques and cryptographic algorithms, the given proposed system offers a robust and versatile solution for protecting sensitive information. By leveraging techniques and ways such as LSB embedding, AES encryption, and advanced encoding methods, the system ensures both security and efficiency in data concealment. The modular design allows for flexibility in adapting to different requirements and scenarios, while making the use of established evaluation metrics such as the MSE,_ PSNR_, and embedding capacity provides quantitative measures of system performance. Furthermore, the utilization of PyCharm as the Integrated Development Environment (IDE) streamlines the development process, enhancing productivity and code quality. The meticulous design and implementation of the system's modules, alongside thorough testing and validation, attest to its reliability and effectiveness in real-world applications. Overall, "Unified Steganography for Concealing and Extracting Secret Messages" represents a significant advancement in the field of information_security, offering a unified framework for secure communication across various digital platforms. With its robust features and comprehensive approach, the system stands poised to provide the evolving challenges of modern data protection and privacy.

VII. ACKNOWLEDGMENT

We gratefully acknowledge the invaluable contributions of individuals and institutions who played pivotal roles in the completion of this assignment.

We extend our heartfelt gratitude to Impact College of Engineering and Applied Sciences for providing a conducive environment for our academic pursuits.

Special thanks to our mentor, Dr. Rama Krishna K, Professor and Head of the Department of Artificial Intelligence and Machine Learning at Impact College of Engineering and Applied Sciences, for his dedicated guidance and insightful feedback on various aspects of our work.

We are indebted to Dr. Rama Krishna K, Professor and Head of the Department of Artificial Intelligence and Machine Learning, for his unwavering support and encouragement throughout the project.

Our appreciation also goes to Dr. Jalumedi Babu, our esteemed Principal, and the Management team for their continuous support and encouragement.

We express our gratitude to the faculty members and support staff of the Department of Artificial Intelligence and Machine Learning at ICEAS for their assistance and cooperation.

REFERENCES

[1] Image_Steganography: A_Review_of_the_Recent_Advances. Nandhini Subramanian, Somaya Al-Maadeed, Ahmed Bouridane. Department_of_Computer _Science_and _Engineering, Qatar University, Doha, Qatar.

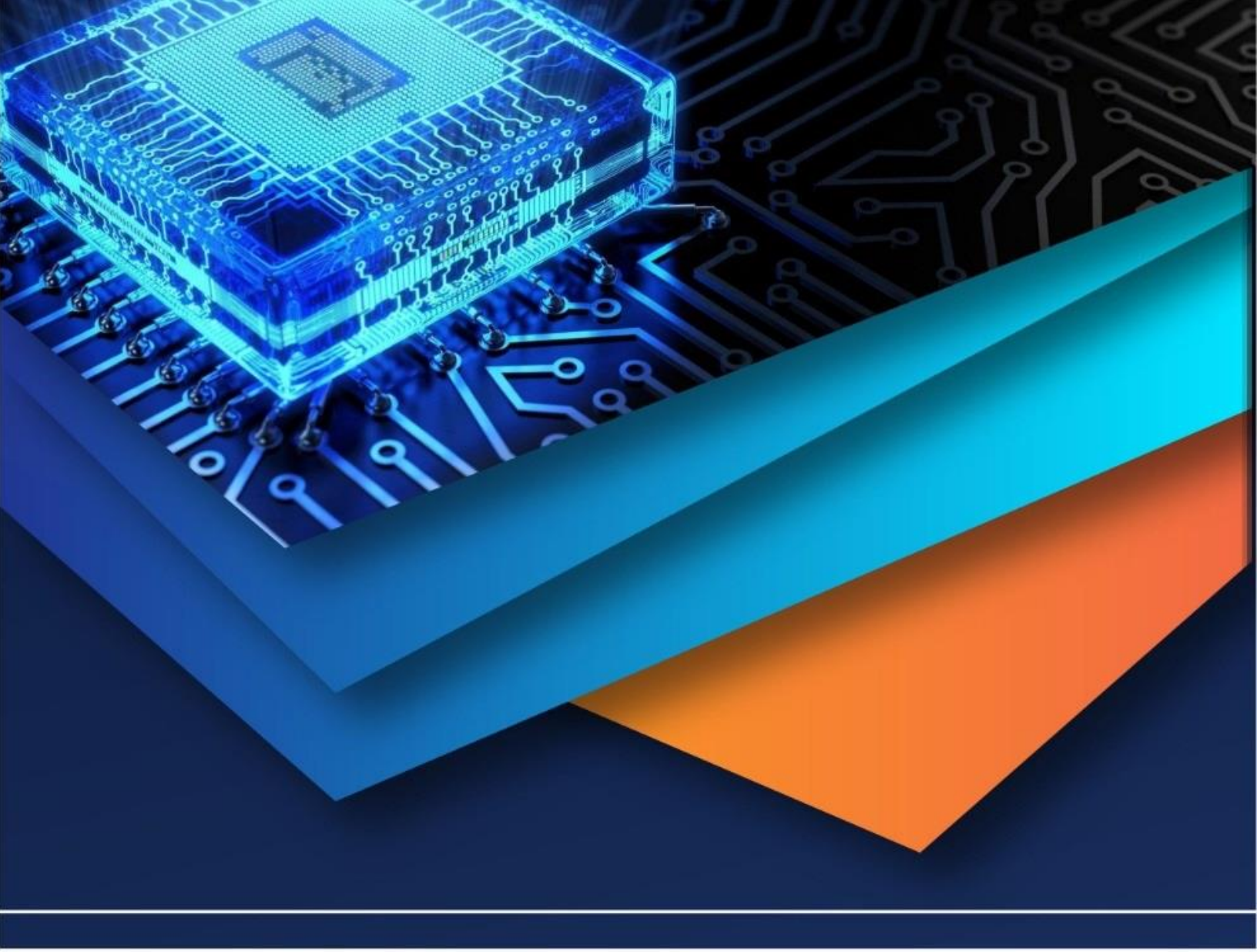
[2] Steganography_Techniques Using_Convolutional_Neural Networks. Vijay Kumar, Saloni Laddha, Aniket, Nitin Dogra. Computer Science and Engineering, NIT Hamirpur, H.P. 177005, India.

[3] Recent _Advances_of_Image_Steganography_with_Generative-Adversarial Networks. Jia Liu_, _Zhuo Zhang, _Yu Lei, _Yan Ke, Minqing_ Zhang, Jun Li and Xiaoyuan Yang. Laboratory of Network and Information Security, Engineering University of People Armed Police Force, Xi'an 710086, China.

[4] Research on Coverless Image Steganography. Kurnia Anggriani, Nan Wu, and Min-Shiang Hwang. Department_of_Computer_Science & Information_Engineering, Asia University.

[5] Review on Feature-Based Method Performance in Text Steganography. Hanizan Shaker Hussain, Mohd Hilal Muhammad, Roshidi Din, Hafiza Samad, Sunariya Utama. Department of Computing & Management Sciences, Universiti Islam Antarabangsa Sultan Abdul Halim Mu'adzam Shah, Malaysia, SP Intellect Resources, Malaysia.

[6] Generative Text_Steganography_Based on LSTM Network and Attention Mechanism with Keywords. Huixian Kang, Hanzhou Wu, and Xinpeng Zhang. School_of_Communication_and_Information_Engineering, Shanghai University, Shanghai 200444, China.
[7] Logistic_Tan_Map_Based_Audio_Steganography. Marwa Tarek Elkando, Wassim Alexan. The_Faculty_of IET, The German_University in Cairo, Cairo, Egypt.
[8] A_Comparative_Study of Audio_Steganography Schemes. Farah_Hemeida, Wassim Alexan, and Salma Mamdouh. Faculty_of_Information_Engineering_and_Technology, The_German University in Cairo, Cairo, Egypt.
[9] A New _Steganography_ Method for Hiding _Text into RGB_Image. Al-Hasan Amer Ibrahim, Ruaa_Shallal Abbas_Anooz. Department_of_Electronic_and Communication-College of_Engineering, Al Muthanna University, Iraq.
[10] Steganography Techniques – A Review Paper. Jasleen Kour, Deepankar Verma. M-Tech_Student, Computer- Science, Assistant-Professor, Computer-Science, _R.B.I.E.B.T_, India_,_ R.B.I.E.B.T_,_ INDIA.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY