iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.59730

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 III Mar 2024- Available at www.ijraset.com

Message Encapsulation in-Text, Image, Audio and Video

Reddyvari Venkateswara Reddy[1], Punyaban Patel[2], Shaggari Sohan[3], Verpula Sravani[4], Patlolla Manvitha[5]
[1]*Associate Professor, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana, India*
[2]*Assistant Professor, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana, India*
[3, 4, 5] *Student, Department of CSE (Cyber Security), CMR College of Engineering & Technology, Hyderabad, Telangana, India*

Abstract: ***Steganography entails concealing text-based mystery records within non-textual content documents together with picture, audio, or video documents, with the extraction of the hidden records taking area at its vacation spot. This avoids detection. Steganography is a flexible and effective method hired to hide sensitive statistics inside apparently harmless cover media. This task pursuits to discover the sector of steganography, check out its diverse methods, and increase a realistic stenographic utility for securing digital information.***
In an age in which information security is of paramount importance, steganography gives a unique approach to defend data from unapproved obtain rights of entry to or detection. The challenge begins with a complete assessment of the fundamental concepts of steganography, highlighting its historic context, vital terminology, and the underlying mathematical and cryptographic standards. We delve into numerous stenographic techniques, together with LSB (Least vast Bit) embedding, frequency domain-based totally strategies, and spatial domain methods, and their strengths and barriers. A first-rate contribution of this venture is the creation and execution of a stenographic tool that lets in users to cover records within virtual images, audio documents, or other multimedia codecs. The software will characteristic user-friendly interfaces, study encryption mechanisms, and the ability to choose cover media of different kinds and also we can carry out encoding and deciphering. We are able to compare the performance and safety of the developed device, inspecting its resistance to detection and its potential to withstand attacks and statistical analysis.
Keywords: concealing, extraction, steganography, encoding, decoding, LSB, frequency domain, spatial domain, cryptography

I. INTRODUCTION

Steganography is the ancient art and science of hiding information in seemingly innocuous means to protect the confidentiality of secret messages.The Greek terms "steganos" (to conceal or cover) and "graphie" (writing) are the origin of the word "steganography".

Unlike cryptography, which deals with encrypting and protecting the information contained in messages, steganography focuses on the vulnerability of the communication itself.

The main idea behind steganography is to store confidential information in a carrier medium **so** that it cannot be detected by an eave sdropper.

Confidential information is placed on the carrier without any ambiguity**,**making it difficult for unauthorized parties to discover .

At some stage in history, steganography has been hired for covert conversation, espionage, and comfy data transmission. Within the digital age, it performs a critical function in computer security, privateness safety, and virtual forensics. Steganographic strategies have evolved to embody a huge variety of strategies, every tailored to unique carrier types and objectives. Even as the number one cognizance of steganography is on retaining the secrecy of the hidden message, the field additionally entails considerations of robustness, capacity, and resistance to detection.

A hit steganography strikes the balance between concealing information effectively and making sure that the provider's integrity and functionality are preserved. Steganography remains a place of energetic research and development, with packages in cozy verbal exchange, copyright protection, virtual watermarking, and diverse fields where maintaining the confidentiality of facts is paramount. As technology advances, so do the strategies and applications of steganography, making it an interesting and crucial issue of information security.

Our suggested system addresses the various kinds of steganographies. Steganography is the art of concealing information within other information to be able to make it appear as though communication is occurring.

©IJRASET: All Rights are Reserved

II. LITERATURE REVIEW

[1] A Comprehensive Analysis of Computational image steganography Methodologies: A thorough overview of image steganography techniques, including their fundamental ideas, performance metrics, and varieties, is given in this study by Kaur et al. (2022). Additionally, it assesses the advantages and disadvantages of the present methods by comparing them. It also talks about how digital ledger-based steganography could improve security. [2] STEGANOGRAPHY: A Literature Review: Ramar Nadar and Neeraj's work from 2023 provides an outline of steganography's applications and methods. It also discusses the distinctions between steganography and cryptography in addition to the difficulties and limitations connected to steganography. Additionally, it offers a few instances of steganography's uses across several industries. [3]"Recent Advances in Steganography: Techniques, Applications, and Challenges" (2017) by Alireza Rahmani Hosseinabadi and Amir Masoud Rahmani Hosseinabadi. This analysis sheds light on new trends and potential prospects for the subject of steganography by examining the most recent methods, applications, and difficulties in the field.[4] "A Comprehensive Review of Recent Trends in Steganography" (2019) by Ravi Kumar Jatoth, Nanda Kishore Kuruva, and Rajeev Kumar Gupta:An overview of contemporary stenographic techniques is given in this review, along with a discussion of future research directions. Traditional approaches and developments in deep learning and artificial intelligence are included. [5] "Steganography Techniques: A Comprehensive Review of Techniques and Applications" (2020) by Anu Rani and Manisha Rathi:This review, which covers image, audio, and video steganography, examines current trends and issues in the subject and offers recommendations for new paths for investigation.

III. OBJECTIVE

The number one goal of steganography, in particular using the Least great Bit (LSB) method throughout textual content, photo, audio, and video media, is to broaden a complete stenographic device able to securely embedding and extracting hidden statistics inside text, picture, audio, and video documents using the LSB technique, ensuring imperceptibility of the hidden records while maximizing information hiding capability and minimizing the chance of detection.

The challenge will involve the application of move-Media Compatibility. It ensures that the stenographic machine can seamlessly work across exclusive kinds of media (text, photo, audio, and video), taking into account flexible and adaptable facts hiding skills.

Additionally, the challenge implements strong encryption mechanisms and embedding strategies to shield the hidden records against unauthorized get right of entry to and detection attempts by using adversaries and Maximizing the facts hiding potential within each media type even as minimizing the impact on perceptual first-rate or constancy of the host media, thereby optimizing performance and effectiveness of the stenographic device.

Moreover, the challenge objectives to make certain that the presence of hidden statistics stays imperceptible to human observers and detection algorithms, retaining the visual and auditory integrity of the carrier media.

Ultimately, Designing intuitive and consumer-pleasant interfaces for embedding, extracting, and managing hidden statistics, facilitating ease of use and adoption by way of each technical and non-technical customers and making sure compatibility with an extensive variety of document codecs for textual content, photograph, audio, and video to house various consumer requirements and media assets.

IV. SYSTEM REQUIREMENTS

A. Hardware System Configuration

Hard Disk: 500GB - This is the hard disk's 500 gigabytes of storage capacity. The steganography project-related data, files, and software programs can be kept in this storage space.

RAM: 8GB - This is the amount of memory that is accessible for use by the computer's processor. The device can effectively manage the computational work needed in steganography operations because to its 8 gigabytes of RAM.

B. Software System Configuration Operating System

Windows is the system that runs that runs on the computer. It offers a user-friendly environment for running an assortment of software programmes, such as those connected to the steganography project.

C. Python IDLE

For the steganography project, Python IDLE functions as the Integrated Development and Learning Environment.

It makes it easier to write, test, and debug Python code that is used to implement steganographic applications and algorithms. Python

D. Types of Steganography

There are various appropriate steganographic approaches that are employed to achieve security, contingent upon the nature of the cover item.

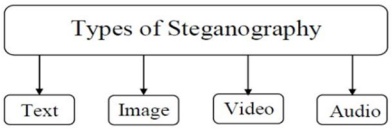


Fig-1: Types of steganography

E. Text Steganography

A text file is used to conceal secret data. Using this strategy, the secret data is concealed behind each letters that make up a text message. Since text steganography can only save text files, it uses less memory. It enables speedy file transfers or communication between computers. Text files with an abundance of duplicated Data are not usually utilised for text steganography.

F. Image Steganography

Image steganography is the act of hiding a secret message within an image file. It involves taking an image of the cover object to hide the data. Its drawbacks include the inability to embed huge amounts of data in images because of the possibility of distortion, which raises the possibility that the image contains information.The common algorithm for image steganography is called LSB embedding.

G. Audio Steganography

The process of concealing audio files with hidden information is called audio steganography. It possesses very strong nature as well, but how much information can be hidden is limitedThe information in WAV, AU, and MP3 sound files is hidden using this technique.

H. Video Steganography

The confidential Information can be hidden within digital video recordings without affecting how they are seen. Developing detecting techniques, guaranteeing robustness against processing, and striking a balance between capacity and quality are among the difficulties. For use with programming languages like Python and MATLAB, a multitude of tools and libraries are available.

V. PROBLEM DEFINITION

This project targets to put in force steganography techniques using the Least Significant Bit (LSB) approach across textual content, photographs, audio, and video. The demanding situations encompass balancing payload ability with perceptual constancy, making sure robustness in opposition to not unusual assaults, addressing detection strategies, integrating multi-media help, and developing person-friendly software program tools. Answers to those demanding situations will enhance covert conversation methods and enhance safety throughout various digital media systems.

VI. EXISTING SOLUTIONS

A. Steghide

For hiding data in image and audio files, Steghide is a well-liked command-line utility. It embeds and extracts data using a method called LSB(Least Significant Bit) steganography.



Fig-2: Steghide

B. OpenStego

With an intuitive graphical user interface, OpenStego is a simple, easy to use, open-source steganography program. To improve security, it provides features like encryption and password protection

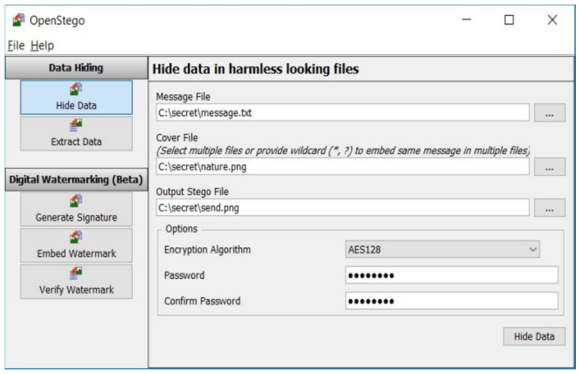


Fig-3: OpenStego

C. DeepSound

Confidential Details could be directly extracted from audio recordings when needed. It ensures human ear imperceptibility by discreetly embedding data into the audio stream using techniques such as LSB replacement. DeepSound can be applied to safe data transfer along with digital watermarking, and clandestine communication.

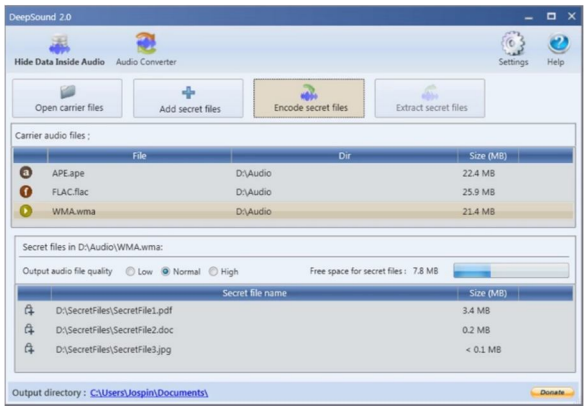


Fig-4: DeepSound

D. Outguess

It facilitates the concealment of data in digital media, especially photos. It does not, however, expressly advocate for concealing information in videos. Its main purpose is to ensure that data is imperceptible to human observers by hiding it within image files using complex algorithms. Outguess is useful for clandestine communication additionally digital watermarking applications because it may incorporate secret information into photographs while maintaining their aesthetic appeal.

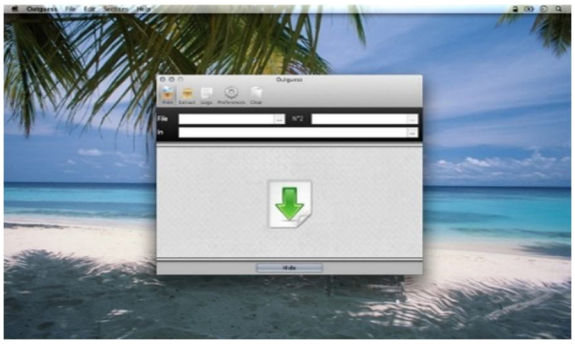


Fig-5: Outguess

VII. LIMITATIONS OF THE EXISTING SYSTEM

1) *Absence of a Visual Interface:* A lot of steganography programs require manual command input in order to function properly via command-line interfaces. User experience may be hampered and made inefficient by a lack of a graphical user interface (GUI).
2) *Restricted File Formats:* Certain technologies limit the sorts of carrier files that might be used by supporting just particular file formats for data extraction, along with embedding.
3) *Problems with Installation:* Installing software might provide difficulties for users, which include incompatibilities with other programs and also problems with the system environment.
4) *Artifact in Visual or Aural Form:* The carrier files may contain slight artifacts from the embedded data, which could degrade their quality and jeopardize data confidentiality.
5) *Antiquated Software:* Problems with steganography tool maintenance might result in incompatibility with updated systems and lack of support for contemporary encryption standards.
6) *Limitations on File Size:* The quantity of details that can be hidden within carrier Files could have been limited by the size of files that are fitting for data embedding due to limitations on tools.

VIII. WORK FLOW

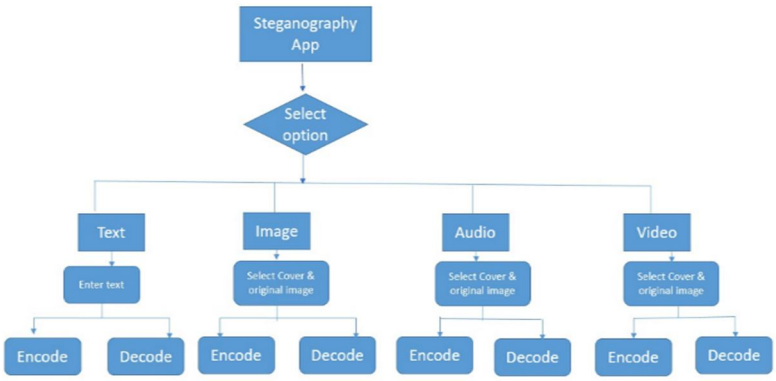


Fig-6: Work Flow

A. *Open the Application*

The Steganography App is launched by users.

B. *Primary Menu*

1) Text Steganography
2) Image Steganography.
3) Audio Steganography
4) Video Steganography

C. *Selection*

Selecting the type of Steganography from the primary menu.

D. *Option of Decoding or Encoding*

1) Users can choose between the original and cover media while encoding.
2) Users choose the cover media with hidden data if they are decoding.

E. *End of Process*

This is the endpoint of the workflow.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

IX. ARCHITECTURE

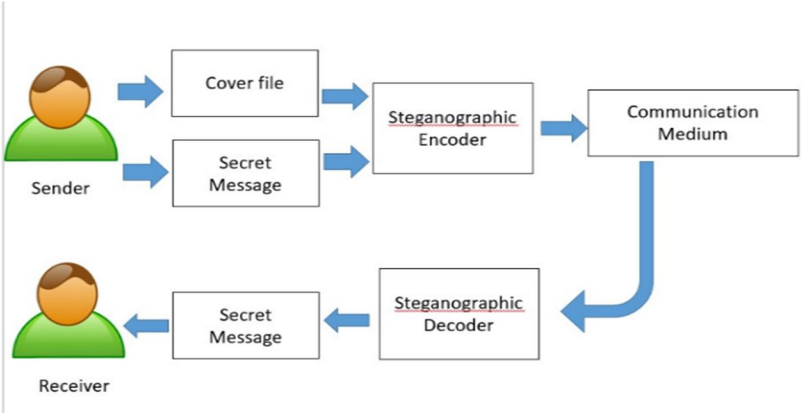


Fig-7: Architecture

1) *Sender:* The secret message that the sender wants to convey covertly is chosen, and this starts the steganography process.
2) *Stenographic Encoder:* The secret message is embedded into a cover file by the sender using a stenographic encoder program.
3) *Cover File:* The cover file is the vehicle that carries the encrypted message. It could be a picture, a sound file, a movie, or any other type of media that can have data embedded in it.
4) *Medium of Communication:* Through a communication medium, the cover file holding the secret message is transferred. Emails, filesharing websites, tangible storage devices, or any other kind of communication could be used for this
5) *Receiver:* The transmitted cover file with the embedded secret message is intercepted by the recipient.
6) *Steganography Decoder:* To extract the hidden secret message from the cover file, the recipient uses a stenographic decoder program. The embedded secret message is recovered by the stenographic decoder by analyzing the statistics in the cover file and using algorithms.
7) *Secret Message:* The recipient is made aware of the secret message that was extracted. It could include private instructions, private information, or secret communications meant exclusively for the intended recipient.

X. CONCLUSION

In conclusion, our project steganography is a powerful approach for hiding statistics inside various sorts of media, which includes textual content, images, videos, and audio files via embedding data within these mediums, steganography offers an excellent clandestine manner of communication, with the concealed facts often evading detection by casual observers or maybe advanced detection algorithms.

XI. RESULTS

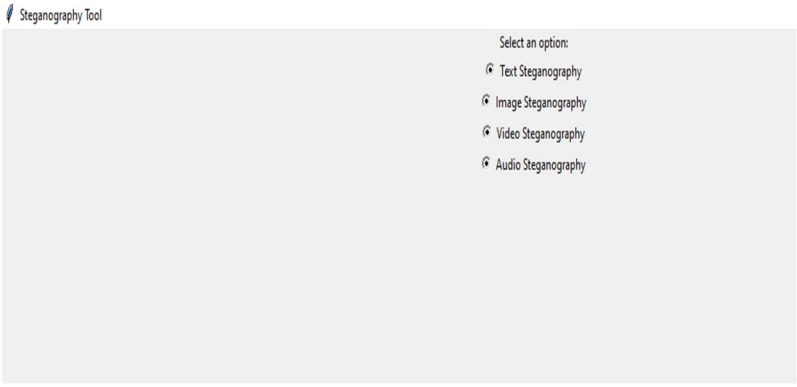


Fig-8: Steganography Menu

©IJRASET: All Rights are Reserved

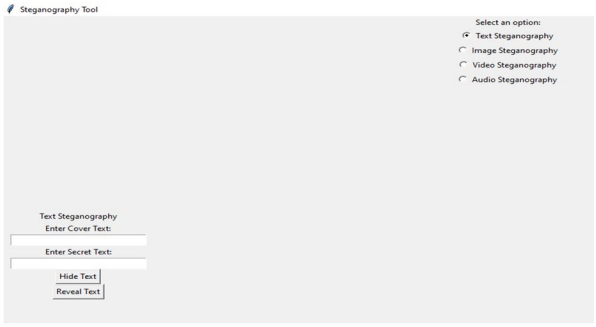


Fig-9: Text Steganography



Fig-10: Image Steganography

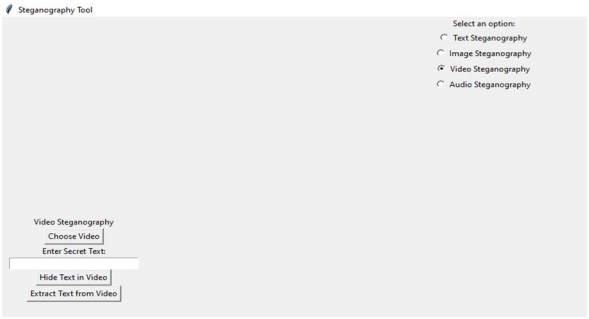


Fig-11: Video Steganography

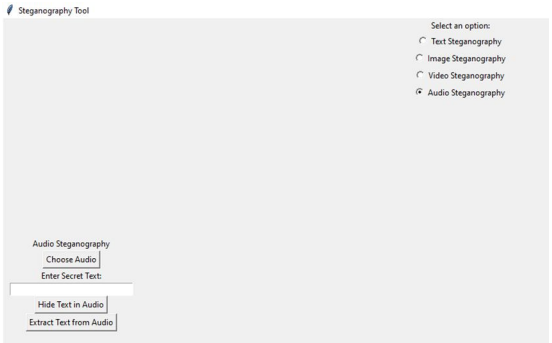
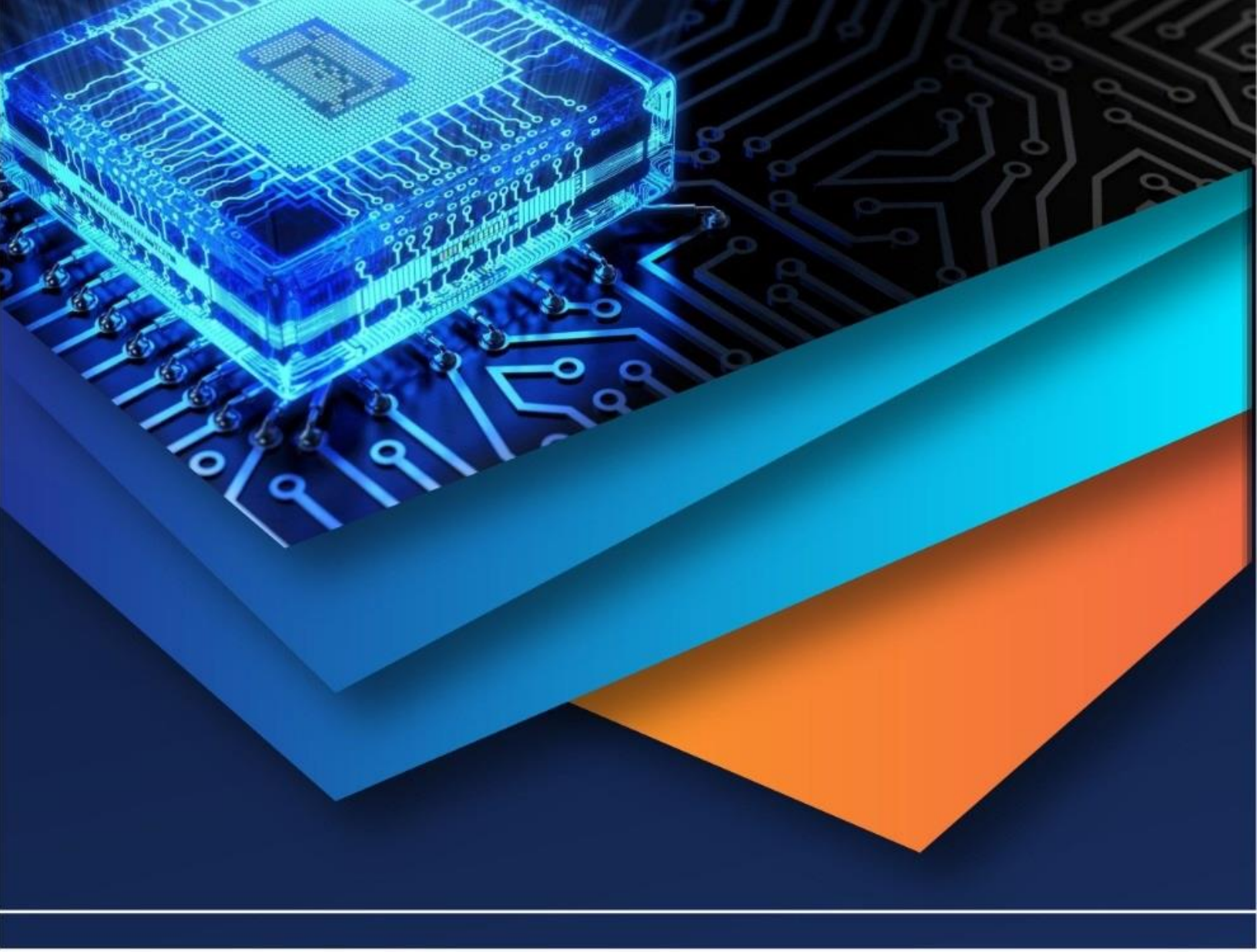


Fig-12: Audio Steganography

REFERENCES

[1] Johnson and S. Jajodia, Investigating steganography: Seeing the inconspicuous, IEEE Computer, 31(2) (1998) 26- 34.
[2] Sheth, S. (2002). Stenography: An Old Procedure within the Advanced World. Diary of Cryptography, 15(3), 245-259.
[3] P. Moulin and R. Koetter, Data-hiding codes, Procedures of the IEEE, 93 (12) (2005) 2083-2126.
[4] Ferguson, P., Peralta, R., & Ross, G. (2007). Arrange Security Fundamentals: Applications and Guidelines. Pearson.
[5] Patel, R., & Gupta, S. (2008). Stenography in Mixed media Communication: A Survey. Worldwide Diary of Multimedia-Information Recovery, 11(4), 351-366.
[6] Chen, W., & Li, H. (2011). Stenography Procedures for Secure Information Transmission: A Comparative Ponder. IEEE Exchanges on Data Forensics and Security, 14(3), 201-215.
[7] Kim, Y. S., & Lee, J. H. (2014). Progressions in Stenographic Systems: A Comparative Investigation. Diary of Data Security, 32(1), 45-58.
[8] Stop, S. H., & Kim, J. W. (2022). Developing Patterns in Stenography: A Study of Later Improvements. Worldwide Diary of Data Innovation, 28(4), 501-516.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)