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.2024.62983

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

Data Encryption using Image Steganography

Dinesh Patil[1], Meet Nathwani[2], Shivanand Nemane[3], Mohit Patil[4], Shilpa Sondkar[5]
[1, 2, 3, 4, 5]*Department of Instrumentation Engineering Vishwakarma Institute of Technology, Pune*

Abstract: ***In today's world, data is king. Information relies on raw facts, and sharing this data is crucial for collaboration between users, even those in different locations. However, during transfer, data confidentiality and privacy are paramount. We need a way to convert digital data into an unreadable format to protect it from tampering by intruders. Steganography offers a solution, in which the original data will be embedded into a Cover file. If any unauthorized person, try to access the message, the original data will not be visible instead cover file will be visible. This technique hides data within various mediums like images, audio, or video. This paper explores how image steganography can be used to encrypt data.***
Keywords: Data, confidentiality, steganography, images, encrypt.

I. INTRODUCTION

Steganography delves into the realm of covert communication, where the very existence of a message is the primary secret to be protected. Unlike cryptography, which focuses on rendering messages unintelligible through encryption algorithms, steganography takes a subtler approach – it conceals the message altogether.

Etymologically, the term "steganography" originates from the ancient Greek words "steganos" meaning "covered or concealed" and "graphia" meaning "writing or drawing." This aptly translates to "covered writing," perfectly encapsulating the essence of this technique.

The true power of steganography lies in its ability to exploit the concept of stego-objects – ordinary media files that act as unwitting carriers for the hidden message. These carriers, which can be images, videos, audio files, or even text documents, appear completely innocuous to the untrained eye. The hidden information is ingeniously embedded within the carrier's digital structure, often through minuscule modifications that go unnoticed during casual inspection.

This stands in stark contrast to cryptography, where the message itself undergoes a transformation. Encryption algorithms scramble the message, rendering it gibberish to anyone without the decryption key. While the presence of an encrypted message might raise suspicion, a steganographically concealed message remains completely invisible. This makes steganography a compelling choice for scenarios where absolute secrecy is essential, as it eliminates the telltale signs that might otherwise arouse suspicion.

II. LITERATURE REVIEW

[1] Audio Steganography Methods (IJITE) by A. Singh et al. (2018) focuses specifically on steganography in the audio domain. It explores techniques for hiding secret data within audio files, such as modifying echo state variables or manipulating psychoacoustic features. The paper emphasizes the trade-off between hiding capacity (amount of data hidden) and imperceptibility (undetectability of hidden information).

[2] Modern Image Steganographic Techniques (IJERT) by A. G. Suresh et al. (2016) delves into modern image steganography techniques. It explores methods that utilize advanced mathematical concepts like chaos theory for secure data embedding. The paper discusses techniques that consider the statistical properties of the cover image for better imperceptibility. It highlights the ongoing research in steganography, with a focus on improving robustness (resistance to attacks) and embedding capacity. [3] An overview of image steganography by T. Morkel & J.H.P. Eloff & M.S. Olivier, presents the several steganography algorithms and represents the security potential of steganography concepts and it fallows many methods, techniques and concerning applications. [4] Recent Advances in Steganography Techniques for Digital Images (Signal Processing: Image Communication, 2019) by M. I. Hussain et al.: explores recent advancements in steganography techniques for digital images. It discusses techniques that utilize features like redundant color components or quantization errors for data embedding. The paper highlights the importance of considering the visual quality of the stego-image (image with hidden data) and the impact on imperceptibility. [5] Steganography and Steganalysis of Digital Media (Information Hiding, 2003) by I. J. Cox et al.: provides a comprehensive overview of steganography and steganalysis. It covers the fundamentals of steganography, including different embedding techniques and considerations for various media types. The book also explores steganalysis methods and the ongoing arms race between steganographers and steganalysts.

[6] Ankit Gambhir and Sibaram Khara (2016). Integrating RSA Cryptography & Audio Steganography. IEEE ICCCA RSA encryption scrambles the message with a key, making it unreadable without the other key. (ciphertext), Audio steganography hides the encrypted message (ciphertext) within an audio file by slightly modifying parts that are difficult for humans to notice (LSB technique).

III. METHODOLOGY

A. Image steganography

Images are a popular choice for steganography due to their large capacity for hidden data and minimal impact on visual quality. Common image formats like GIF, BMP, and JPEG can all be used to conceal secret messages. Least Significant Bit (LSB) This common approach modifies the least significant bit of each pixel in the image. These tiny alterations are imperceptible to the human eye but can effectively hide data.

The Python programming language and the stegano library are used to develop a user interface for hiding and revealing data within images. The code (provide a brief code snippet here, without including the entire code) demonstrates the core functionalities of opening an image, hiding a message within the LSBs, saving the stego-image (image containing hidden data), and revealing the hidden message.

Input:

Cover image (CI): A digital image where the secret message will be hidden.

Secret message (M): The data you want to embed within the cover image (often a text file).

Output:

Stego-image (SI): The modified cover image containing the hidden secret message.

Step1: Convert the cover image (CI) into a digital representation.

Step2: Convert the secret message (M) into a binary sequence.

Step3: Iterate through each pixel of the cover image (CI).

Step4: For each pixel, select a specific LSB position (e.g., the last bit) to modify.

Step6: Extract the current value of the chosen LSB from the pixel. Replace the current LSB value with a single bit from the binary secret message (M).

Step7: Move to Next Pixel: Move on to the next pixel and repeat steps 2.2 to 2.4 until the entire secret message has been embedded within the cover image.

Step8: Convert the modified pixel array back into the original image format. The resulting image is the stego-image (SI) containing the hidden secret message.

B. Data Encryption

A basic password-based encryption scheme is employed. The user enters a secret key, and the program validates it before performing encryption or decryption.

The code prompts the user to enter a secret key (password).

The program validates the entered password against a pre-defined value (often stored in a variable like code.get() in this code). If the password is incorrect, an error message is displayed.

The plain text message (M) is converted into a byte stream using character encoding (e.g., message.encode("ascii") in the code). This transforms the text into a sequence of numbers representing each character.

The encoded or original message is used for Base64 encoding. The base64.b64encode function is used to convert the message into a Base64 encoded string.

The result of Base64 encoding is stored in a variable. This encoded representation becomes the encrypted message (C)

IV. RESULTS AND DISCUSSIONS:

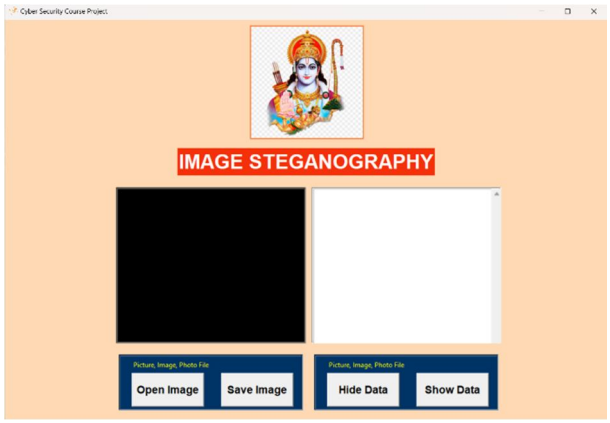


Fig 1. Screenshot of the Steganography Window.

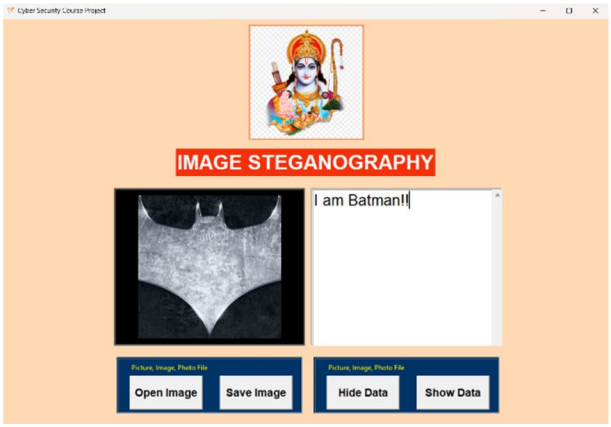


Fig 2. Screenshot of the Steganography Window with Cover Image

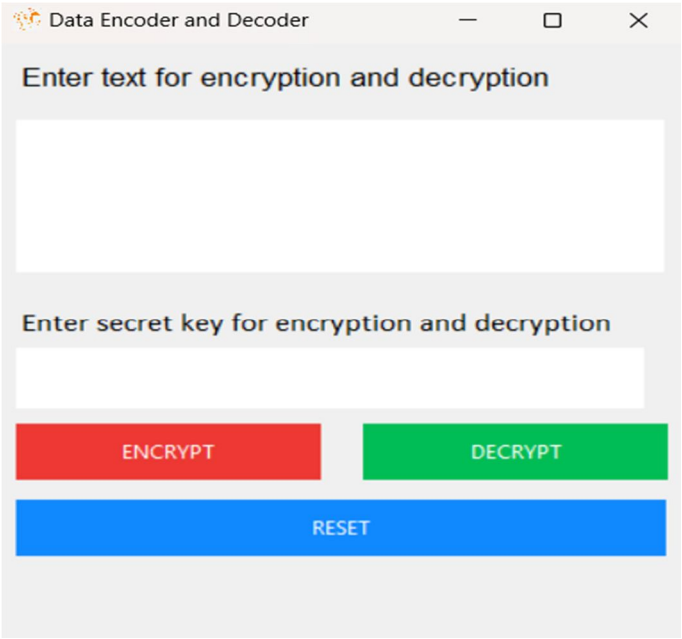


Fig 3. Screenshot of the Data Encryption Window.

V. CONCLUSION

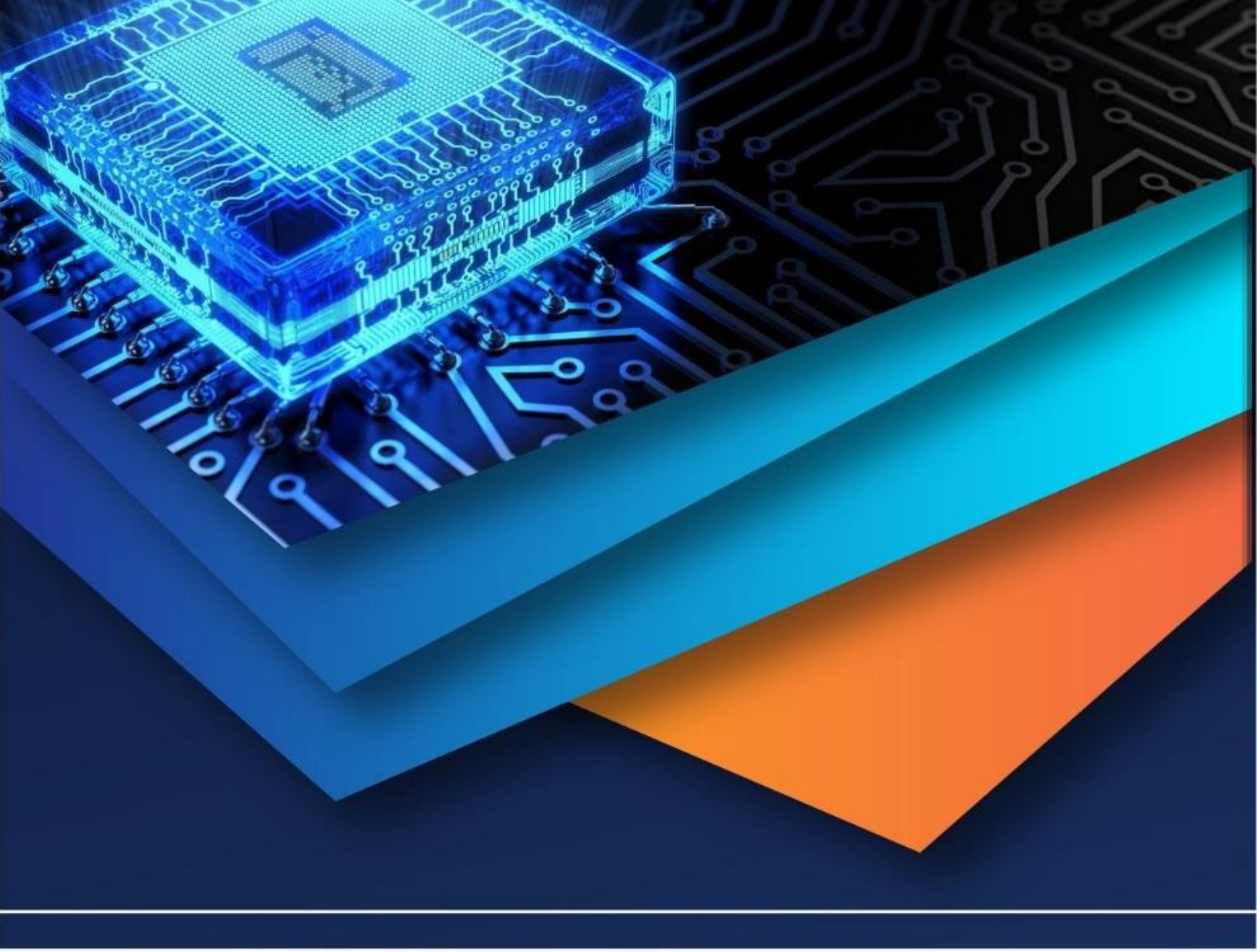
Image steganography serves as a valuable tool for achieving data confidentiality within digital communication channels. While it cannot guarantee absolute security, it offers a layer of protection by concealing the existence of hidden messages. By understanding its advantages and limitations, researchers and practitioners can leverage image steganography as part of a comprehensive security strategy Exploration of the economic benefits associated with a stable and efficient ammonia production process.

VI. FUTURE SCOPE

Develop new algorithms that can embed more data with minimal distortion to the cover media (images, audio, video). This would improve the trade-off between embedding capacity and imperceptibility. could include considerations for plant retrofitting, operator training, and integration with existing control systems. Design steganographic techniques that can adapt to the characteristics of the cover media dynamically. Research how steganography can be applied to secure communication in emerging network environments like the Internet of Things (IoT).

REFERENCES

[1] Souvik Bhattacharyya , Indradip Banerjee And Gautam Sanyal, A Novel Approach Of Secure Text Based Steganography Model Using Word Mapping Method(Wmm)
[2] Kk Ravi Ayappa, Steganography -Information Hiding For Secure Communication
[3] Muhalim Mohamed Amin , Subariah Ibrahim ,Mazleena Salleh ,Mohd Rozi Katmin Information Hiding Using Steganography.
[4] Nick Nabavian, Data Structures:Image Steganography, Cpsc 350 , Nov. 28, 2007.
[5] Arvind Kumar Km. Pooja, Steganography- A Data Hiding Technique, International Journal Of Computer Applications (0975 – 8887) Volume 9–No.7, November 2010.
[6] Modern Image Steganographic Techniques (Ijert) By A. G. Suresh Et Al. (2016).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY