WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Steganography Using Python

Dr. N. Kalaivani[1], Mr. M. Chandru[2], Mr. R. Arun Prasath[3]

[1]Assistant professor, Department of Information Technology, Sri Krishna Adithya College of Arts & Science, Coimbatore.
[2]III B.Sc. IT, Department of Information Technology, Sri Krishna Adithya College of Arts & Science, Coimbatore
[3]III B.Sc. IT, Department of Information Technology, Sri Krishna Adithya College of Arts & Science, Coimbatore.

ABSTRACT

Steganography is the practice of concealing secret data within an ordinary file, such as an image or audio file, to avoid detection. This project explores the use of Python for implementing a simple and effective steganographic technique for embedding and extracting hidden messages in image files. The proposed method utilizes the Least Significant Bit (LSB) algorithm, where the secret message is embedded in the least significant bits of the image pixels. The system allows users to input a message, which is then encoded into an image, and provides functionality to extract the hidden message from the modified image. Python libraries such as Pillow (for image manipulation) and numpy (for handling pixel data) are used to perform the encoding and decoding operations. The results demonstrate that the system can successfully hide and retrieve messages without noticeable degradation in image quality, showcasing the potential for secure communication through steganography..

Keyword: *Steganography, Techniques, Algorithm*

I. INTRODUCTION

The topic that is selected is Steganography Using Python, one reason that interlopers can be fruitful is the majority of the data they obtain from a framework is in a structure that they can peruse and understand. Gatecrashers may uncover the data to other people, adjust it to distort an individual or association, or use it to dispatch an assault. One answer for this issue is, using steganography. Steganography is a method of concealing data in computerized media. As opposed to cryptography, it isn't to shield others from knowing the concealed data yet it is to shield others from imagining that the data even exists. Steganography is a technique used for hiding secret information within an ordinary, non-suspicious medium, such as images, audio, or video files. Unlike encryption, which transforms data to be unreadable, steganography conceals data in a way that makes it indistinguishable from normal content. This method is often used for secure communication, as it allows sensitive information to be hidden in plain sight, reducing the chances of detection.. Due to propel in ICT, the vast majority of data is kept electronically. Therefore, the security of data has become a principal issue. Other than cryptography, steganography can be utilized to make sure about data.In recent years, with the rapid growth of digital media and the increasing need for secure communication, steganography has become a vital tool in the field of cybersecurity. Other than concealing information for privacy, this methodology of data stowing away can be reached out to copyright insurance for advanced media: sound, video and pictures.

II. LITERATURE STUDY

This project demonstrates the use of steganography techniques to hide secret messages within digital media files, such as images and audio, using Python. The primary method used in this implementation is **Least Significant Bit (LSB)** steganography, where the least significant bit of the image's pixel values is altered to embed the hidden information. The message is first converted into binary form, then systematically embedded within the image without noticeably altering its appearance. A Python script is developed using libraries such as Pillow for image processing and numpy for efficient data manipulation. The project also includes functions for extracting the hidden message from the altered media file, making it a simple and effective way to secure information using commonly available digital formats.

Drawbacks

- **LSB-based methods**, while simple, are often vulnerable to detection through statistical analysis. Since the least significant bits are altered, there may be patterns or anomalies in the image or audio that can be detected by steganalysis tools.
- Advanced detection algorithms, including machine learning-based methods, can easily identify whether an image or audio file contains hidden data if they know what to look for.

- The amount of data that can be hidden in a medium without significantly altering its appearance or quality is limited. In the case of LSB, the hidden message is typically constrained to a small size due to the limited number of bits that can be changed without being noticed.

III. Steganography using python

This venture gives subtleties how to share information utilizing steganography. The developing prospects of current interchanges need the unique methods for security particularly on PC arrange. The system security is getting progressively significant as the quantity of information being traded on the web increments. In this manner, the classification and information respectability are requiring to ensure against unapproved access and use. This has brought about a touchy development of the field of data covering up Information covering up is a rising exploration territory, which includes applications, for example, copyright insurance for advanced media, watermarking, fingerprinting, and steganography. In watermarking applications, the message contains data, for example, proprietor distinguishing proof and a computerized time stamp, which normally applied for copyright assurance. Fingerprint, the proprietor of the informational index inserts a sequential number that remarkably recognizes the client of the informational index. This adds to copyright data to makes it conceivable to follow any unapproved utilized of the informational collection back to the client.

In this tutorial, we'll explore how to implement a simple steganography system using Python, specifically embedding and extracting hidden messages in image files using the Least Significant Bit (LSB) method. The LSB method embeds the secret message into the least significant bits of the image pixels, which results in minimal distortion that's not noticeable to the human eye.

Benefits:

1. Enhanced Security: Hides information without detection, ensuring confidential communication.

2. Easy to Implement: Python libraries like Pillow and NumPy make it simple and efficient.

3. Minimal Distortion: Changes to media (images, audio, etc.) are barely noticeable.

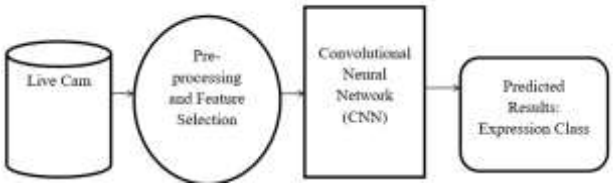
4. Covert Communication: Hides messages in normal files, avoiding suspicion.

5. Wide Applications: Used in digital watermarking, secure messaging, and data integrity.

6. Low Risk of Detection: Hidden messages are undetectable by standard security tools.

7. Flexible Media Use: Works with images, audio, and video files

SYSTEM FLOW DIAGRAM:



MODULE DESIGN:

1. Image Loading Module:

   - load_image(image_path): Loads the image.

   - prepare_image(img): Converts image to RGB for manipulation.

2. Message Encoding Module:

   - message_to_binary(message): Converts message to binary.

   - embed_message(image, binary_message): Embeds the binary message using LSB.

3. Message Decoding Module:

   - extract_binary(image): Extracts the binary hidden in the image.

   - binary_to_message(binary_message): Converts binary back to text.

4. File I/O Module:

   - save_image(image, output_path): Saves the encoded image.

   - load_image_from_file(image_path): Loads an image for decoding.

5. Utility Module:

- add_delimiter(binary_message): Adds an end delimiter to the message.

- validate_image_format(image): Ensures the image is in a correct format.

IV. RESULT AND DISCUSSION

To conclude, in this paper, explained the process of Steganography and different techniques in steganography. Discussed the advantages and disadvantages of steganography over cryptography. Also discussed the process of steganalysis which is a process of identifying the use of steganography. Finally, selected 5 different steganography tools and compared them by the quality of stego images generated by each tool. The steganography tools are CryptaPix, Steg, VSL, Hide N Send, QuickStego. Two carrier images are selected, and two secret files are selected, one is an image, and another is a text file which are hided in the carrier images. The final output images also known as stego images are further analyzed using Imatest software in Matlab for calculating the SSIM and PSNR values. After observing the PSNR values of the stego images generated by all five steganography tools, they produced the images of high quality and SSIM values conclude that almost all the tools produced the images that are similar to original image.

Stage of Development of a System

- Feasibility assessment
- Requirement analysis
- External assessment
- Architectural design
- Detailed design
- Coding
- Debugging
- Maintenance

Feasibility Assessment

In Feasibility this stage problem was defined. Criteria for choosing solution were developed, proposed possible solution, estimated costs and benefits of the system and recommended the course of action to be taken.

Requirement Analysis

During requirement analysis high-level requirement like the capabilities of the system must provide in order to solve a problem. Function requirements, performance requirements for the hardware specified during the initial planning were elaborated and made more specific in order to characterize features and the proposed system will incorporate.

External Design

External design of any software development involves conceiving, planning out and specifying the externally observable characteristic of the software product. These characteristics include user displays, report formats, external data source and data links and the functional characteristics.

Internal Design Architectural and Detailed Design

Internal design involved conceiving, planning out and specifying the internal structure and processing details in order to record the design decisions and to be able to indicate why certain alternations were chosen in preference to others. These phases also include elaboration of the test plans and provide blue prints of implementation, testing and maintenance activities. The product of internal design is architectural structure specification.

The work products of internal design are architectural structure specification, the details of the algorithm, data structure and test plan. In architectural design the conceptual view is refined.

Detailed Design

Detailed design involved specifying the algorithmic details concerned with data representation, interconnections among data structures and packaging of the software product. This phase emphasizes more on semantic issues and less synthetic details.

Coding

This phase involves actual programming, i.e, transacting detailed design into source code using appropriate programming language.

Debugging

This stage was related with removing errors from programs and making them completely error free.

Maintenance

During this stage the systems are loaded and put into use. They also get modified accordingly to the requirements of the user. These modifications included making enhancements to system and removing problems.

V. CONCLUSION AND FUTURE ENHANCEMENT

To conclude, This Paper Steganography using python which has been developed using Python. This paper helps users to hide data inside another image file. Which provides Easy implementation. Thus, the paper entitled above should include all the above-mentioned features and it is confirmed that it is up to the specifications entitled for the project..

SCOPE FOR FUTURE ENHANCEMENT

Future work could focus on developing more **robust steganographic techniques** that are harder to detect using modern steganalysis tools. This includes methods that minimize detectable patterns in the altered data, improving the security and privacy of hidden messages. To enhance the **security** of hidden messages, future versions of the project could incorporate **encryption algorithms** to ensure that even if an attacker detects hidden data, they cannot easily extract or understand the information without the correct decryption key.