e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

EMBEDDING SECRET KEYS WITH PYTHON AND LSB STEGANOGRAPHY IN IMAGES

Jaya Surya.A*1, Viji Vinod*2, V. Sarala Devi*3

*1MCA Student, Department Of Computer Applications Dr. M.G.R. Educational And Research Institute, Chennai, India.

*2Professor, Department Of Computer Applications Dr. M.G.R. Educational And Research Institute, Chennai, India.

*3Assistant Professor, Department Of Computer Applications Dr. M.G.R. Educational And Research Institute, Chennai, India.

DOI : https://www.doi.org/10.56726/IRJMETS52713

ABSTRACT

This project investigates the Incorporation of LSB (Least Significant Bit) steganography into images and secret key embedding techniques using Python. The main goal is to find out if it is possible to hide private data, like cryptographic keys, in the least important bits of picture pixels. The project embeds secret keys into image files using the LSB steganography algorithm. In order to encode the sensitive data with the least amount of visual impact possible, this technique manipulates the least important bits of each pixel's RGB channels. The integrity of communication channels is largely dependent on the secure transmission of cryptographic keys, which is a common practice in current security procedure. However, when exchanging keys, vulnerabilities could appear. These keys might not have an extra layer of security in the current system, leaving them vulnerable to interception or unwanted access. By directly embedding cryptographic keys into picture files via LSB steganography, the suggested method presents a revolutionary approach.This technique aims to enhance key transmission security by introducing a low-key layer of security. The project looks into the potential benefits and challenges of this approach. This discovery is significant because it has the potential to improve current security methods by utilising LSB steganography to add an additional layer of secrecy.

Keywords: LSB Steganography , Secret Key Embedding Techniques, Python, Private Data, Cryptographic Keys, Image Files, RGB Channels, Visual Impact, Communication Channels, Secure Transmission, Vulnerabilities, Interception, Security Procedure.

I. INTRODUCTION

The "Embedding Secret Keys with Python and LSB Steganography in Images" project combines the features of the PyQt framework, LSB (Least Significant Bit) steganography, and Python programming to offer a novel method of secure data transfer and storage. The main goal of this project is to use the PyQt framework to build a graphical user interface (GUI) that is robust and easy to use.This GUI will serve as a platform for users to seamlessly embed and extract secret keys or confidential information within digital images using LSB steganography. LSB steganography involves subtly altering the least significant bits of pixel data within images to conceal encrypted information, ensuring that the changes are imperceptible to the human eye.[1]

By harnessing Python's versatility and simplicity along with PyQt's powerful GUI development features, the project seeks to empower users with a user-friendly tool. This tool will enable them to encode sensitive data into images securely and retrieve it when needed, providing a straightforward and accessible solution for data protection.[2]

The combination of PyQt, LSB steganography, and Python is intended to provide a useful and effective way to secure data contained in images, along with the added advantage of an easy-to-use interface. Because of its emphasis on security and usability, the project is applicable to a wide range of domains, including as information exchange, data privacy, and secure communication. It serves the needs of both individual users and businesses looking for dependable ways to safeguard their sensitive data.[3]

By combining these technologies, the project endeavors to create a cohesive system that not only conceals keys within images effectively but also enhances the user experience through a visually appealing and user-friendly

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

interface. This amalgamation represents a step towards providing a versatile, accessible, and robust solution for securing information within digital images.[4]

II. LITERATURE SURVEY

According to OSAMA HOSAM, Cloud technology is gaining immense popularity due to its parallel and flexible services, revolutionizing the IT field. However, addressing security concerns is crucial. We propose a hybrid solution: AES encryption with a 256-bit key, further encrypted with ECC, and embedded in images using LSB steganography for efficient key management and distribution, ensuring strong security for cloud data.[5]

According to MD AL AMIN HOSSAIN, Cloud computing is rapidly evolving in the ICT sector, but the challenge of information security persists. This study focuses on enhancing information privacy using ElGamal ECC for encryption and masking/filtering steganography for robust protection of internet-based data. Results show improved data privacy and reliability compared to other encryption schemes like RSA, with reduced computational power requirements and enhanced defense against lossy compression algorithms.[6]

According to NUTHALAPATI PAULINE ANGEL, This project focuses on secure data exchange using LSB-based steganography, concealing information within images. It employs Tkinter and Stegano modules in Python, with functions for encoding and decoding messages. The report outlines security key-based steganography for images, integrating cryptography for enhanced security, and demonstrates the implementation and functionality of the image steganography algorithm.[7]

According to Adee, R., & Mouratidis, H, Authors integrate cryptography and steganography for enhanced cloud data security. AES-256 and RSA encryption combine in a four-step model, concealing data in images using LSB steganography. Identity-based encryption enables secure data sharing. Reduced picture distortion increases data concealment. Methodology suits diverse company needs, ensuring data integrity and privacy in cloud, financial, and healthcare sectors. Future research should focus on enhancing security for multimedia data.[8]

According to Kumar, V., Pathak, V., Badal, N., Pandey, P. S., Mishra, R., & Gupta, S. K,A modified version of the Arnold Cat algorithm is a suitable encryption method for securing digital documents, especially when it comes to pixel security. Other techniques are primarily designed to secure files or text. The Modified Arnold Cat algorithms make it easy to protect the image without sacrificing its significance or fine features. Therefore, the essential medical imaging data may be safeguarded using the suggested plan. The medical image can be saved in a large database in the future with the development of an interface or program, guaranteeing that the encrypted image is safely preserved before transmission. We may conclude that this method works well for tasks like securely transferring internet content and encrypting medical photographs.[9]

According to, Edwar, J. G., & Holman, M. A ,The PRESENT encryption technique is lightweight and suitable for low power consumption applications. Its performance across platforms was evaluated, leading to the creation of four fixed-hardware microcontroller implementations. Understanding cryptographic algorithms and finite field arithmetic is crucial for such implementations. This study aimed to optimize implementations for 8, 16, 32, and 64-bit platforms, achieving lower computational costs compared to previous efforts. Notably, this work includes the first documented implementation of the algorithm on 32-bit microcontrollers, distinguishing it from previous studies.[10]

According to, Rajesh, P., Alam, M., Tahernezhadi, M., Kumar, T. R., & Rajesh, V. P, Data Science analysis enhances business profitability by selecting players for positions based on various features using a novel Pseudo code Algorithm. Machine learning helps in player selection for ambassadorship and club formation while reducing costs. The approach reduces player selection risk factors by 50% and minimizes time and cost discrepancies in market values. It can be applied to manage sports analytics' financial profit. Future directions involve incorporating AI solutions for decision-making enhancements, considering factors like player injuries, GPS data, and video performance extraction.[11]

According to, Osakwe, U. O. Data Protection Using Fibonacci Series Encryption And Text-In-Image Steganography. This study demonstrates how methods for steganography and encryption can be developed to safeguard data and information by using steganography to conceal sensitive data within an image and cryptography to render sensitive data unreadable. It is safe to say that the technique has been effectively

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

implemented given the findings, which indicate that the image is still intact and that the encrypted file has been correctly decrypted to its original condition.[12]

EXISTING SYSTEM:

Various steganographic techniques and methods exist for hiding information within different media types, such as images, audio, and videos. Some of the commonly used steganography methods include.

Spread Spectrum Technique: This method spreads the secret information across multiple pixels or audio samples, making it harder to detect and extract. The secret bits are distributed using mathematical operations like Discrete Cosine Transform (DCT) or Discrete Fourier Transform (DFT).

Palette-based Steganography: This method involves hiding information by modifying the color palette of an image. The color indices are modified to carry the hidden data without noticeably altering the image's appearance.

Phase Encoding: In audio steganography, this technique exploits the phase component of the audio signal rather than modifying the amplitude. The phase differences between audio samples are altered to encode the hidden information.

Distortion Techniques: These methods introduce intentional distortions in images, videos, or audio files to encode the secret information. For example, altering the noise level or introducing slight geometric transformations to encode the data.

Transform Domain Techniques: Some methods embed data in the transformed domain of the media, such as the frequency domain (e.g., Discrete Cosine Transform) for images and audio or the wavelet domain for images.

Text Steganography: Instead of hiding text inside an image, text steganography hides information within the text itself by using techniques like word spacing, invisible characters, or modified letter formatting.

DISADVANTAGES:

1) Key Management Complexity.
2) Limited Protection Against Advanced Attacks.
3) Increased Overhead.
4) Dependence on Algorithmic Security.

III. PROPOSED SYSTEM

The proposed system aims to enhance the existing text steganography implementation by incorporating more advanced techniques to ensure secure and efficient information concealment. The system will employ encryption algorithms to obfuscate the text message before embedding it into the image, providing an additional layer of security. This encryption will make it significantly harder for unauthorized parties to extract the hidden information, even if they manage to detect the presence of steganography. To improve the capacity of hiding information within an image, the proposed system will use more sophisticated image manipulation methods that go beyond simply modifying the LSB of pixel color channels. Advanced techniques such as spatial domain and transform domain steganography will be explored to increase the payload capacity while maintaining imperceptibility. These methods will carefully distribute the embedded information across the image to avoid suspicious patterns that might arise from the modification of LSBs. Moreover, the suggested system would include redundancy methods or error correcting codes to strengthen the steganography's robustness. By reducing the effects of potential image modifications like noise or compression, these strategies will make sure that the hidden data is preserved and accessible even under difficult circumstances.

ADVANTAGE:

1. It provides more precision.
2. Good performance .
3. The ability to attain greater accuracy as the system analyses.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

SYSTEM DESIGN:

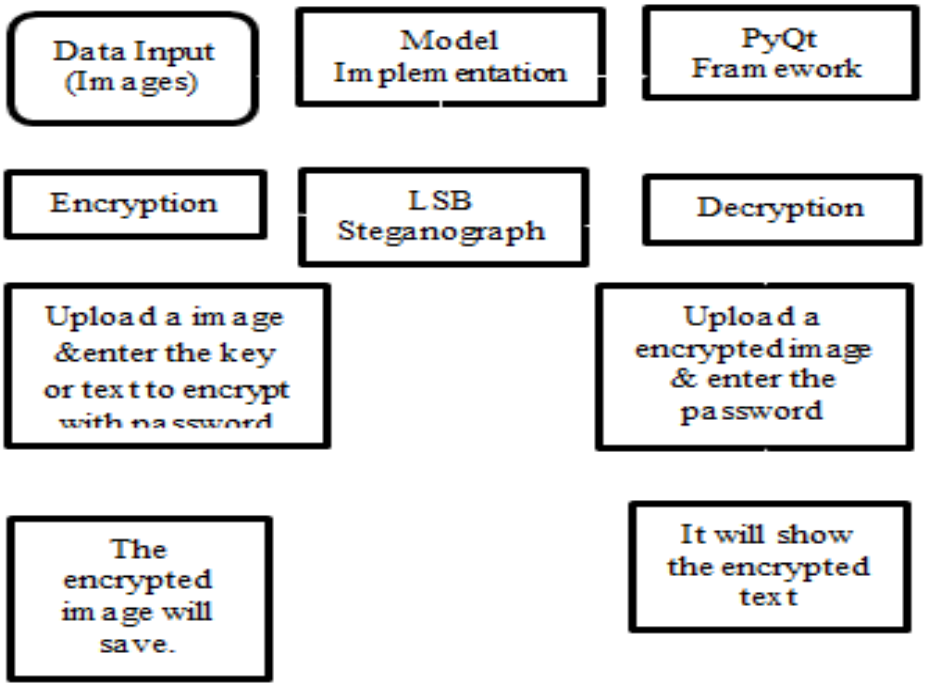


Figure 1: System Design

MODULE DESCRIPTION

1) Image Upload Module:

This module enables users to upload images through the PyQt GUI, providing a straightforward mechanism to select and load image files.

2) Encryption Module:

Responsible for encrypting sensitive information (e.g., secret keys or text) with a user-provided password before embedding it into the image using LSB steganography.

3) Decryption Module:

Manages the extraction and decryption of hidden information from an encrypted image using the specified password.

4) Output Module:

Handles the display or storage of results, including generating and showing the encrypted image and presenting the decrypted information.

GRAPH

Histogram images of before and after encryption (a)original image, (b) stegano image. The graph under are histograms.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:04/April-2024 Impact Factor- 7.868 www.irjmets.com

Figure 2

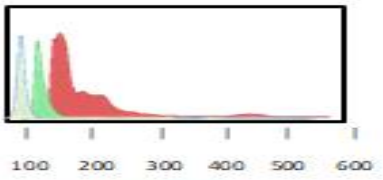
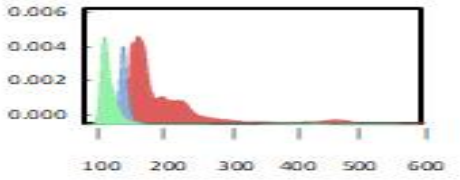


Figure 3



In figure 2and 3 are shows the image histogram in RGB channels .Then ,the accuracy, performance, and capacity of the suggested system are improved by the employment of the LSB algorithm. The accuracy rate grew as a percentage, performance improved as well, the capacity displayed a lower graph, and the loss of image data was 0.00078%.

IV. CONCLUSION

In conclusion, the "Secure Pixel Secrecy" project presents a comprehensive solution for secure communication through a user-friendly Python application with a PyQt GUI. By integrating LSB steganography and encryption, the project addresses the critical need for discreet and protected information exchange in the digital landscape. The proposed method ensures stealthy communication by embedding encrypted data within image pixels, fortified by an additional layer of security through password-based encryption. The practical advantages, including a versatile and accessible interface, make the project well-suited for real-world applications where privacy and data security are paramount. As technology continues to advance, "Secure Pixel Secrecy" stands as a practical and effective tool for individuals seeking a secure means of communication, exemplifying the fusion of cryptographic techniques within a user-friendly environment.

V. REFERENCES

[1] Hosam, O., & Ahmad, M. H. (2019). Hybrid design for cloud data security using combination of AES, ECC and LSB steganography. International Journal of Computational Science and Engineering, 19(2), 153-161.

[2] HOSSAIN, M. A. A. Enhancing Performance of Data Privacy on the Cloud Using Cryptography with Steganography in Python.

[3] Angel, N. P., Rexie, J. A. M., & Mythily, M. (2023, April). Security Key-Based Steganography for Images. In 2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT) (pp. 1-7). IEEE.

[4] Mayilsamy, K., Ramachandran, N., & Raj, V. S. (2018). An integrated approach for data security in vehicle diagnostics over internet protocol and software update over the air. Computers & Electrical Engineering, 71, 578-593.

[5] Pabbi, A., Malhotra, R., & Manikandan, K. (2021, March). Implementation of least significant bit image steganography with advanced encryption standard. In 2021 international conference on emerging smart computing and informatics (ESCI) (pp. 363-366). IEEE.

[6] Shashidhar, R., Kumar, M. S., Arunakumari, B. N., Santhosh kumar, R., & Patilkulkani, S. (2022). Novel Approach for Steganography to Camouflage Digital Information Using Least Significant Bit. In Computational Intelligence in Pattern Recognition: Proceedings of CIPR 2021 (pp. 551-562). Springer Singapore.

[7] Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors, 22(3), 1109.

[8] Parmar, V., Gandhi, D., Srivastava, A., & Sharma, S. (2022, April). Stego Dog: Image Steganography Tool for Confidentiality and Integrity. In 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) (pp. 1658-1666). IEEE.

[9] Kumar, V., Pathak, V., Badal, N., Pandey, P. S., Mishra, R., & Gupta, S. K. (2022). Complex entropy based encryption and decryption technique for securing medical images. Multimedia Tools and Applications, 81(26), 37441-37459.

[10] Edwar, J. G., & Holman, M. A. (2022). Enhanced Security: Implementa

[11] Adebayo, O. S., Ganiyu, S. O., Osang, F. B., Salawu, S. A., Mustapha, K., & Abdulazeez, L. (2022). Data Privacy System Using Steganography and Cryptography.

[12] Gutiérrez-Cárdenas, J. M. (2014, July). Secret key steganography with message obfuscation by pseudo-random number generators. In 2014 IEEE 38th International Computer Software and Applications Conference Workshops (pp. 164-168). IEEE.

[13] Rajesh, P., Alam, M., Tahernezhadi, M., Kumar, T. R., & Rajesh, V. P. (2020). Secure communication across the internet by encrypting the data using cryptography and image steganography. International Journal of Advanced Computer Science and Applications, 11(10).

[14] Kedia, R., Kumar, B., Banerjee, P., Jha, P., Kundu, T., & Dehury, M. K. (2023, April). Analysis and Implementation of Image Steganography by Using AES Algorithm. In 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 537-544). IEEE.

[15] Osakwe, U. O. Data Protection Using Fibonacci Series Encryption And Text-In-Image Steganography.