IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11762

ADVANCED IMAGE STEGANOGRAPHY

DIMPU J[1], SOMYA MS[2]

Student, MCA, Bangalore Institute of Technology, Bengaluru, India[1]

Professor, MCA, Bangalore Institute of Technology, Bengaluru, India[2]

Abstract: This project tries to take the existing methods of patient administrative data security to another level by securing such data through the use of advanced steganographic techniques of data incorporation. The following report also contains a fully working the system's implementation providing for better management with enhanced security and more access to data in health care facilities through Python application and libraries. The principal facets data generation is one of this system's functions., well- known as data gen. py, total administration of the patient files at the clinic patient File management. txt, Steganography application—secret pixel. py files and the main application which is being referred to as 'app'. py. For encryption it uses AES while for hash, it uses SHA- 256; hence, the security aspect is done quite well.

I. INTRODUCTION

The word "steganography" itself is taken from the Greek words "steganos," meaning covered, and "graphia," meaning writing. Steganography means concealing a message inside some other medium to prevent its detection. In essence, this would imply that the information should get embedded into any chosen medium or channel in in a way that makes it imperceptible to any human eye, thus achieving hidden communication. This can be done through different media; however, digital images are more favored given their widespread usage, and the amount of redundant data they contain is huge, which may be exploited in the embedding process. On a fundamental level, image steganography involves an appropriate cover photo as well as embedding the confidential information within the pixels values. The two principal domains are the spatial and the frequency domains, in which data embedding takes place.

Spatial Domain Techniques: The techniques in the geographical area include the method of LSB modification. It typically involves the manipulation of the LSB of image pixels to encode the secret data. For instance, the cover image's pixel value can be 10010110, and changing the LSB to hide data can result in 10010111. Since only the least significant bit is changed, the net The image has changed quite a little. small and usually is not visible to the human eye.

Frequency Domain Techniques: In the frequency domain, discrete cosine transforms and Wavelet transforms that are discrete are applied to the image. These transforms take a different domain where data included into the transformed coefficients. For instance, in DCT-based steganography, the cover picture is separated into blocks, after which the DCT is applied to each block. After that, the secret data is embedded into the DCT coefficients; then, perform the inverse DCT to acquire the stego picture in the spatial domain. On the other hand, the methods of DWT have very similar approaches: an image will be divided into various frequency ranges to enable data embedding inside wavelet coefficients. Both domains have their advantages. Spatial domain techniques, like LSB, are simple and computationally efficient but more prone to image processing attacks like compression and noise addition. Although the methods in the frequency domain are more resistant to such, they are computationally complex.

Steganography offers a very secure means of data transmission by understanding and making use of these techniques, wherein the information remained hidden from unwanted observers. This capability is important to applications requiring a high level of confidentiality and security.

II. LITRATURE SURVEY

[1] The paper by Halim and Sani explores embedding techniques in image utilizing spread spectrum steganography methods within Galois Fields, aiming to enhance security and robustness of hidden data within digital images, presented at the 2010 IMT-GT-ICMSA conference..

[2] El-Emam's 2007 paper details a steganography algorithm capable of embedding large amounts of data into digital media. It focuses on achieving high security and maintaining data integrity, providing an effective method for secure data hiding in various digital formats. The research is significant in science.This review explores the use of deep

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11762

learning across various areas of modern astronomy, including exoplanet detection, astronomical object classification, and large survey data analysis. It evaluates the capabilities and limitations of deep learning approaches and their potential to significantly advance astronomical research through improved data processing and interpretation methods.

[3] Morkel, Eloff, and Oliver's 2005 paper provides a comprehensive overview of image steganography, discussing various techniques and their applications. The paper highlights the importance of image steganography in secure communication and presents a detailed analysis of existing methods and their effectiveness in concealing data within digital images.

[4] Chun-Shien's 2005 book delves into multimedia security, focusing on Cryptography and electronic watermarking techniques. It covers methods to protect intellectual property, offering a thorough analysis of how these technologies can secure digital media against unauthorized use and distribution, and discusses their practical applications and effectiveness.

[5] This review emphasizes the growing role of data-driven approaches in exoplanet astronomy, focusing on the challenges posed by noisy observational data and current developments in using data-driven techniques for exoplanet detection. It discusses future research directions, advocating for the enhanced use of advanced data analytics to improve exoplanet discovery and understanding.

III. PROPOSED SYSTEM

This study suggests an advanced method that will integrate the strength of spatial and frequency domain techniques with modern cryptographic practices to meet the challenges in image steganography. The suggested approach utilizes a use of a multi-layered approach to offer enhanced security, capacity, and imperceptibility to the steganographic system. In its framework, The suggested approach consists of the following components:

Encryption: Before it is embedded, the hidden message is encrypted by a cryptographically strong algorithm. Therefore, if the hidden data is extracted, without a decryption key, there is no meaning to the extracted hidden information. Contrasted with this, additional security through encryption embeds the content of the hidden message, apart from embedding itself, which safeguards against unauthorized access.

Hybrid Embedding: This method combines the frequency domain of the Discrete Wavelet Transform with the Least Significant Bit modification of the spatial domain. By using the strengths of both domains, this hybrid technique can boost embedding capacity without sacrificing cover picture quality. Huge capacity are supported using LSB modification with almost any noticeable deterioration. DWT offers defense against the majority of image processing exploits.

Key-Based Embedding: The pixel positions for data embedding are chosen based on a secret key. In this case, a key-based approach adds an extra line of defense to the security of the steganographic algorithm, where the positions of embedding become quite unforeseeable. Thus, application of the secret key will ensure the overall betterment of the security of the steganographic system where only the right people with the correct key can do the embedding and extraction of the hidden data properly.

Error Correction:Error-correcting codes are often added to increase the strength of the implanted data. Such codes are capable of recovering the hidden data from distortion or attacks on a cover image. In this respect, error correction provides resilience against degradations of an image, like compression, cropping, or even adding noise to it, and ensures that the implanted information remains intact.

In this covert communication, the proposed method will integrate these components to provide a secure, highcapacity, and imperceptible solution by resolving the major challenges of image steganography

IV. METHODOLOGY

There are four main modules in this system:

Data Generation (datagen.py): This generates artificial patient data for testing.
Patient Details Management (patient_details.txt): This stores patient details in a well-structured format. Steganography

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11762

Application (secret_pixel.py): This embeds and extracts the sensitive information within the images.

Main Application (app.py): The overall workflow is coordinated here by integrating data generation, management, and steganography.

Tools and Technologies Programming Language: Python

Libraries: OpenCV, NumPy, PyCryptodome Encryption Algorithm: AES Hashing Algorithm: SHA-256

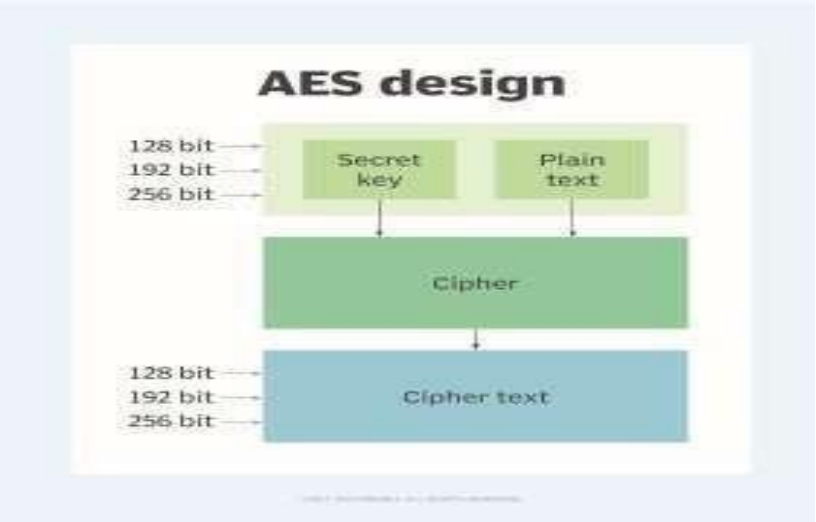

Figure .1 AES Encryption

AES stands for Advanced Encryption Standard. It is symmetric encryption that has gained worldwide acceptance in securing data. It was adopted by the United States NIST (National Institute of Standards and Technology) in 2001 after a competition among various encryption algorithms. AES has turned out to be very fast, secure, and efficient.

Some of the key things regarding AES encryption one should know are:

Symmetric Key Encryption: AES uses the same key for encryption and decryption. This means that the key should be kept secret since anyone with the key can decrypt the data.

Block Cipher: AES is a block cipher; it forms a block of bits, usually of fixed size, and encrypts them. The block size of this algorithm is 128 bits or 16 bytes.

Sizes of Keys: AES supports three sizes of keys: 128 bits, 192 bits, and 256 bits. The larger the key, the stronger is the encryption; however, this may also bring about slower performance.

Rounds: AES involves a number of transformation rounds to encrypt data. The number of rounds depends upon the key size.

V. IMPLEMENTATION

Data Generation (datagen.py)

The datagen.py script generates synthetic patient data, including names, ages, medical records, and other relevant information. This data simulates real-world patient records, providing a basis for testing the steganography application.

Patient Details Management (patient_details.txt)

The patient_details.txt file stores patient data generated by datagen.py. Each record is stored in a structured format for easy retrieval and processing.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024
DOI: 10.17148/IARJSET.2024.11762

Steganography Application (secret_pixel.py)

The secret_pixel.py script embeds encrypted patient data into images using least significant bit (LSB) steganography. It also provides functionality to extract and decrypt the hidden information.

Main Application (app.py)

The app.py script integrates all components, providing a cohesive interface for data generation, embedding, and extraction. It manages the workflow and ensures seamless interaction between the various modules.

VI. CONCLUSION

Thus, this project introduced an image steganography system that could easily address fundamental hindrances to secure data embedding by integrating appropriate encryption techniques and other forms of embedding alongside the error-correcting codes so that the concealed data is secret and visually indistinguishable with high practical interiority and resistance towards various assaults and distortions possible. Therefore, depending on its ultimate use, it will be an extremely efficient stealth communication means for various purposes and will guarantee the proper delivery of confidential information by achieving the best balance between security, capacity, and inconspicuousness when using this approach.

VII. ENHANCEMENT

Future Improvements in Advanced Image Steganography
There are a number of enhancements that can be done in the near future and as the field of image steganography continues to evolve in terms of its robustness, security, and usability. Some such improvements are as follows:

1. Additional Security Features
Quantum Cryptography: Quantum cryptography is one of the features that could be implemented in order to further the security of the encrypted data in images and make it more resilient against quantum computing attacks. Advanced Algorithms of Encryption: More advanced and effective encryption algorithms to be used for the protection of hidden data; post- quantum cryptography.

2. Steganographic Algorithms
Adaptive Algorithms: Development of adaptive steganographic algorithms that can dynamically choose the best method (LSB, DCT, DWT, etc.) depending on the content of the image and the type of data hidden.

Integration with Machine Learning: Using machine learning models to optimize the embedding process for minimal distortion and maximum data capacity.

3. More Capacity and Speed
Larger Capacity in Data: Develop algorithms to increase more data to be hidden without affecting the quality of the image.
Compression Technique: Include sophisticated data compression techniques to reduce the size of the hidden data. This would accommodate more information to be embedded.

4. Robustness and Imperceptibility
Resist Attack: The output of the resistance to steganalysis attack would be enhanced with more sophisticated techniques so that the hidden data is even more difficult to detect.

5. Cross-Platform Compatibility
Multi-Platform Support: Make the steganography system compatible on all platforms, including web-based, mobile, and desktop environments. Standardized APIs: Provide standardized APIs for integration with other applications and systems.

6. Usability Enhancements
More User-Friendly Interfaces: An interface that is more intuitive and user-friendly in embedment and extraction of steganography should be created. Automation: Inbuilt automation where both embedding and extraction are done with less intervention of the user.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 7, July 2024

DOI: 10.17148/IARJSET.2024.11762

7. Real-Time Applications

Live Streaming: Development of techniques for real-time data embedding and extraction, like live video streaming, to enhance secure communication.

Steganography and Instant Messaging: Steganography embedded in instant messaging for encrypted message transmission without suspicion.

8. Advanced Image Formats and Media

Newer Image Formats: The proprietary support of newer image formats and other media types, such as 3D images and videos, further expand the application area.

Augmented Reality: Exploring applications of steganography in AR for hiding data in augmented scenes.

REFERENCES

[1]. S.A. Halim and M.F.A Sani. "Embedding using spread spectrum image steganography with GF ( )," in Proc. IMT-GT-ICMSA, 2010, pp. 659-666.

[2]. N.N. El-Emam. (2007). "Hiding a large amount of data with high security using steganography algorithm." Computer Science. [On-line]. 3(4), pp. 223-232. Available:www.thescipub.com/pdf/10.3844/jcssp.2007. 223.232 [Dec., 2011].

[3]. T. Morkel, J.H.P. Eloff, and M.S. Oliver. "An overview of image steganography." in Proc. ISSA, 2005, pp. 1- 11.

[4]. L. Chun-Shien. Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. USA: Idea Group Publishing, 2005, pp. 1-253.

[5]. R.J. Anderson and F.A.P. Petitcolas. (1998, May). "On the limits of steganography." IEEE Journal of Selected Area in Communications. [On line]. 16(4), pp. 474-481. Available: http://www.cl.cam.ac.uk/~rja14/Papers/jsac98 -limsteg.pdf [Jun., 2011].

[6]. I.J. Cox, M.L. Bloom, J.A. Fridrich, andT. Kalkert. Digital watermarking and steganography. USA: Morgan Kaufman Publishers, 2008, pp. 1-591.

[7]. N.F. Johnson and S. Jajodia. (1998, Feb.). "Exploring steganography: seeing the