**A Secure Medical Image Steganography Framework Using DWT, AES Encryption, and LSB Embedding**

Ragha Karthikeyan

22BCE1734   
School of Computer Science and Engineering  
Vellore Institute of Technology, Chennai Campus  
Chennai, India

Tanaya Mahalanabis

22BCE1217  
School of Computer Science and Engineering  
Vellore Institute of Technology, Chennai Campus  
Chennai, India

Soham Datta

22BCE1547  
School of Computer Science and Engineering  
Vellore Institute of Technology, Chennai Campus  
Chennai, India

*Abstract*— A digital steganography strategy is proposed wherein XOR-based encryption is combined with the discrete wavelet transform (DWT) for embedding secret messages in images. It applies XOR encryption in the spatial domain to ensure confidentiality and the features of the DWT in the frequency domain for security, strong data hiding, and imperceptibility. The message to be hidden is encrypted, converted to binary, and embedded into the high-frequency sub-band HH of the wavelet image decomposition for concealing data while minimizing visual distortion. The stacking procedures are implemented in Python using the PyWavelets and Pillow packages, which allows message-hiding and extraction capabilities to protect the security and integrity of steganographic communication so that it qualifies as a medium for the covert transfer of data in digital environments.

Keywords— Steganography, Discrete Wavelet Transform (DWT), XOR Encryption, Image Processing, Data Hiding, Digital Security, Covert Communication, Frequency Domain, Information Embedding, Stego Image

# Introduction

Secure transmission and storage of sensitive information, especially in the medical field, has become a high priority in the digital age. Digital Image Processing employs various tools to insert confidential data into images through a process called steganography. Operating differently from cryptography, which hides the content of a message, steganography hides the very existence of that message and thus provides another layer of protection. To deal with the recent advances, a few high-end techniques have been added to fortify the resistance and invisibility of the steganographic way. For instance, a new technique is called Adversarial Neural Cryptography with SHA-256-encryption to carry out the task of encrypting and inserting patient data into the non-critical areas of medical images to protect their confidentiality and integrity. The technique demonstrates high resilience against attacks based on geometric transformations and histogram analysis. The mechanisms introduced in another paper are hybrid encryption, which uses LSB along with many other encryption algorithms, resulting in a stego image that has been smoothed and thus made difficult to detect-elevating the security level of the hidden information while maintaining the cover image's visual quality. The securing of patients' medical data is most important in medical imaging. The LSB steganography along with chaotic map encryption has been devised to safeguard medical images. This scheme encrypts data before the embedding, utilizing chaotic systems' unpredictability and increasing the difficulty level for potential attackers. To scale up the innovativeness, a DNA-based secure image transmission framework is put forth, securing medical images in transit through encryption and LSB steganography. This paradigm enhances data security based on biological processes. All these developments give emphasis to the critical importance of DIP in building resilient steganographic protocols for the secure transmission of data. The merging of DWT, LSB, and encryption algorithms has therefore remained a continuous research theme, increasing the security and reliability of steganography in sensitive areas such as medical imaging.

# Objectives

The objective of this study is to design and implement a highly secure and efficient steganography procedure for the secure transmission of data. The specific objectives of this research are clearly elucidated as follows:

1. Development of a steganographic method which can efficiently hide secret messages inside a digital media (image,text or audio file) while leaving no visible trace on the carrier file and thereby making detection of the hidden message nearly impossible.
2. Creation of an environment with data integrity and confidentiality so that hiding information could only be very difficult for unauthorized persons to detect it.
3. Testing the evaluation parameters for imperceptibility, payload capacity and robustness against other evils like addition of noise, compression and format conversion.
4. Another countermeasure involves decoding mechanism that gives the known recipients a simple and easy method to access the embedded message with minimum computation effort.
5. Comparative performance evaluation of the parameters of accuracy, security, and processing time of the current approach to all other existing steganographic techniques.

# Literature Review

Beside confidentiality of sensitive data and integrity, steganography is among the main aspects concerning information transfer through insecure channels, for example, healthcare systems in such territories where patient records and diagnostic images would be shared. The primary method of image steganography is of course the least significant bit (LSB), which is concerned with embedding the secret message in the least significant bits of the image pixel. The high payload capacity is assured by the more straightforward implementation of LSB, while the low robustness usually fails in statistical attacks and image processing operations.

To mend these weaknesses, the researchers have proposed many enhancements or hybrids that merge LSB with various image transforms and intelligent systems. Among these are models proposed by Rao et al. [1]. Under this work, agglomerated convolutional neural networks adaptively select embedding regions according to image features so that the processes are conducted in a way that maximizes imperceptibility and robustness. The advancement shows great potential for integrating artificial intelligence with steganography for domain-specific security needs.

Abdualgalil et al. [2] proposed a scheme hybridizing LSB with DWT and Arnold scrambling. The authors obtain a capable trade-off with respect to capacity, and the common attacks LSB can withstand are compression and noise addition. The advantage of frequency domain techniques, like DWT, lies in diffusing the hidden data through the distortion into several frequency components.

Li et al. [3] proposed a two-layer security model stressing the importance of integrated encryption and steganography. In this model, the plaintext secret data are encrypted first using the Advanced Encryption Standard (AES) and are then embedded into a cover image using the transform domain approach. Thus, while hiding the existence of the data, it also keeps it secret, which represents a significant upgrade for the security level of the communication system.

Kaur et al. [4] implemented a steganographic system in which machine learning classifiers were used against tampering of stego-images. The system learns from image features, contrasting benign changes to the image with potentially harmful alterations, thus permitting a transmission mode that is secure and smart for steganography. The combination of AI and classification methods holds a forward-looking future for steganographic research more so in public-interest cases such as telemedicine and digital health records.

Praveenkumar et al. [5] described a complete framework pertinent to telemedicine, where low latency and high image quality are given utmost priority. Interesting incorporation is also by hashing the data cryptographically along with DWT-based embedding to achieve data integrity and imperceptibility. Thus, this framework can embed real-time patient data without compromising pristine quality of images meant for diagnosis and is thus an excellent fit for real-time communication applications, where sensitivity is paramount.

The advances being made in the field of RDH, as mentioned above, are all-being able to completely restore the original image after data extraction. This feature is especially important since, in medical applications, quality of images straight away influences the clinical decisions. Growing interest in RDH gives prospects of concentrating more on maintaining how authentic images are while ensuring data security.

In short, there is a clear trend in the literature from traditional capacity-dependent techniques to a sophisticated and multi-layered approaches emphasizing secrecy, flexibility, and application-specific requirements. The integration of cryptographic algorithms, image transforms, and machine learning models indicates the wider trend toward making steganographic frameworks intelligent, secure, and resilient, which are better suited for medical data.

# Ease of Use

The data security system based on steganography has been focused on making easy-to-handle for a user who is not technically sophisticated, such as a health professional. One of the salient aims of this method is to serve the user with a mechanism to embed sensitive information within images without requiring prior knowledge of cryptography or steganography principles.

The installation within a Jupyter Notebook environment presents a clear, interactive process for users to follow while doing things step by step. In each cell is an explanation and direction to further understand and executes the actual step of the workflow. This format not just increases accessibility, but it also lends itself to transparency, ideally for demonstration, educational purposes, or prototype testing within a clinical environment.

The proposed system has the efficiency to support a user with the common image formats, that includes PNG and BMP, compatible with medical imaging standards. The only input required of a user is to have a cover image plus the message/file to be embedded, while the rest of the processes, which include encryption, embedding, and then saving in the same picture, are totally automated.

Moreover, the encryption feature is modular, which makes it possible for the end-user to toggle between different encryption algorithms based on need without interfering with the core code structure. That way, the system appreciates practicality, customizability, and, at the same time, a lower barrier entry. The last product-a stego-image-is produced with minimal visible distortion yet preserves the original image for medical or diagnostic purposes.

Indeed, the overall conversion method represents a good compromise between technical robustness and simple user interface in which the system really proves a working model for the secure data handling in privacy-sensitive applications such as healthcare.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in:

# Dataset Used

The proposed steganography-centric system for data security was designed and evaluated utilizing the Medical MNIST data. The dataset itself harbors more than 58,000 grayscale medical images divided into six diagnostic categories: Chest, Hand, Head CT, Abdomen CT, CXR, and Spine. All images are equal in size, 64×64 pixels, and this uniformity allows a very well-structured and diversified collection good enough for exploration in applications of medical image analysis and information security.

This dataset was selected due to the real-world applicability of medical imaging, while the level of organization allows the same evaluation to be performed on multiple image types. Although the images have a relatively lower resolution, they are good representatives of some emergency clinical modalities, providing practical situations to test and validate image steganography methods.

Various forms of sensitive metadata including anonymized patient identifiers, made-up diagnostic notes, and encrypted text strings were embedded into a representative subset of images using the Least Significant Bit (LSB) steganographic method. Due to the high consistency and clarity of the dataset, accurate benchmarking of the embedding process could be attained while ensuring image quality, an important consideration in medical practice.

It shows that the Medical MNIST dataset justifies the ability of the system to securely embed medical information into diagnostic images without compromising their visual fidelity and classification capabilities. Thus, it makes a compelling case for further extension into higher-resolution datasets and real-time clinical applications in which secure and imperceptible data embedding would be essential.

# Proposed Method

The proposed methodology is a combination of encryption and least significant bit (LSB) image steganography to embed sensitive medical data into the medical images. While doing so, it ensures the data remains private, and the diagnostic quality of the host image remains intact. The system is expected to be lightweight, modular, and very useful in the clinical environment, where data security and user friendliness matter.

This method starts with a process of data preprocessing, wherein patient data such as diagnostic notes, identifiers, or other sensitive metadata are prepared for embedding. The data, first AES encrypted, is a general standard that secures information even if the disclosed user-traced data is extracted. It has been forever chosen because of its cryptographic strength, speed, and common acceptance in security-concerned applications.

After encryption, the LSB method is used to embed the ciphertext into the cover image. In this procedure, the least significant bits of the cover image are replaced with bits from the encrypted data. The small alteration in the least significant bits should have no visible degradation on the medical image, thus allowing an imperceptible embedding.

The cover images used for embedding are sampled from the diverse population of the Medical MNIST dataset, which guarantees input images from diverse medical imaging modalities. The embedding algorithm walks through the image pixel matrix and embeds one bit of the encrypted message into a pixel; usually, this modifies the blue channel (for RGB images) or the intensity value of grayscale images.

Upon completion of embedding, a lossless format (like PNG) is used to save the stego-image, thus averting degeneration during storage/transmission. The reverse process then ensues at the receiver's end, where extraction of the embedded bits takes place and decryption under the AES key is performed into the original message.

The proposed method thus ensures encryption for keeping the data protected and steganography for concealment. The method is thus feasible whenever medical data have to be securely transmitted through public or unsecured networks, where the existence and content of information remain protected. A significant contribution is that the program operates in a Jupyter Notebook environment, thus being highly accessible, enabling even non-technical users to play around with it.

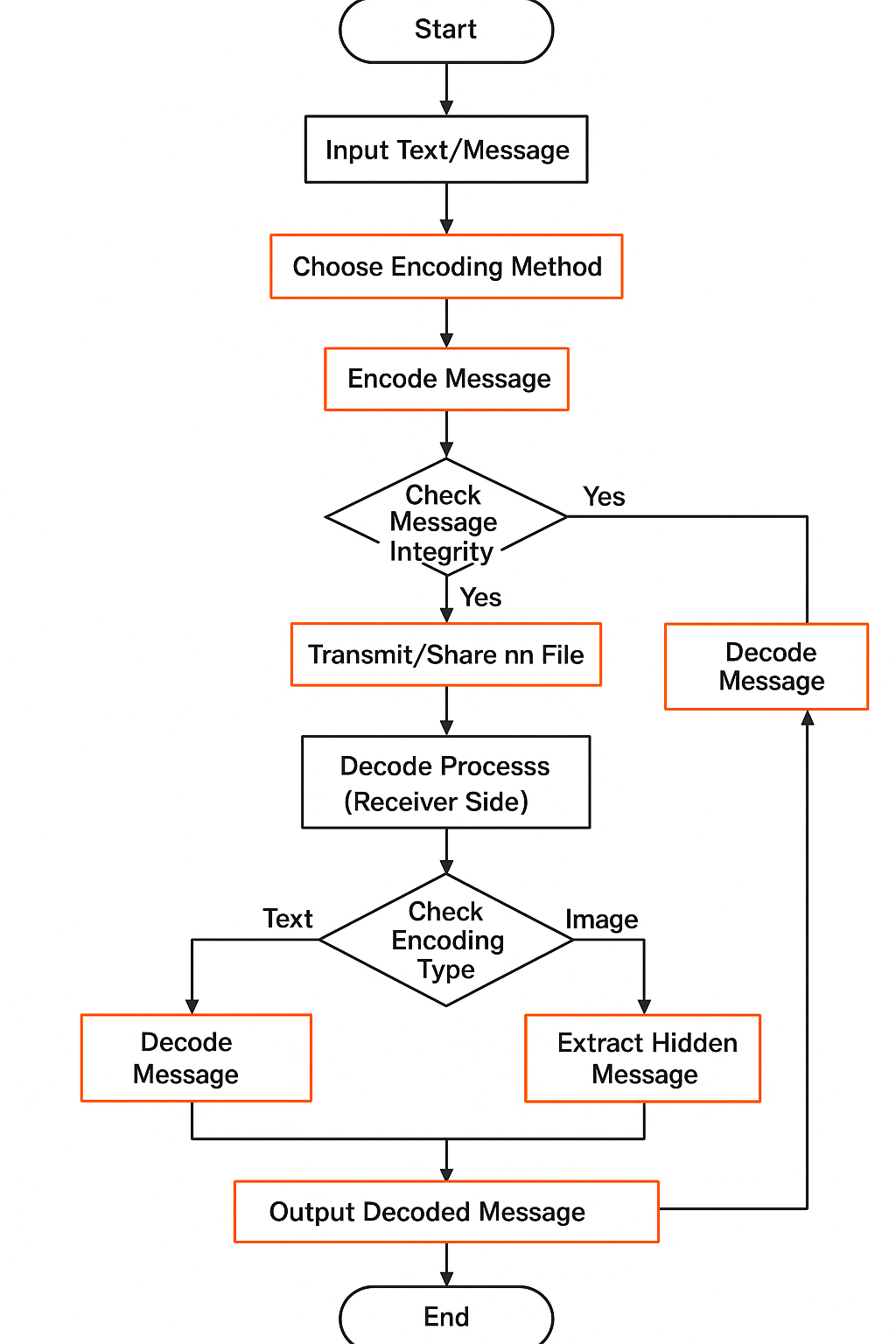


Fig. 1. Flow Chart

# Experiment and Results

The effectiveness of the proposed steganographic method was assessed through some experiments using Discrete Wavelet Transform (DWT) to hide secret data in grayscale images. Two key modalities were tested:

1. **DWT + XOR-based embedding:** This method involves encrypting a textual message with a simple XOR cipher, given a user-defined key. After converting it to binary, the encrypted message gets embedded into the wavelet-transformed image's high-frequency sub-band (HH) via least significant bit (LSB) substitution, while an end-of-data marker would be added for the signal termination during extraction.

Fig. 2. Using XOR (with data loss)

Fig. 3. Our method: Using XOR (no data loss)

1. **DWT + LSB embedding (Direct):** This method is the direct binary embedding to approximation sub-band (LL) of the DWT coefficients without encrypting. The method being simple and having higher capacity prefers neither security nor robustness.

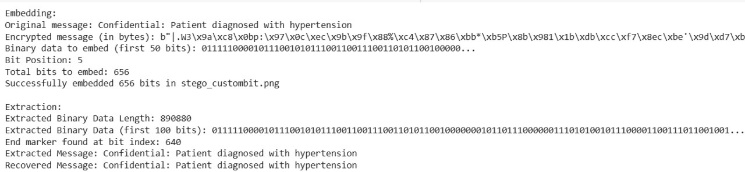
Fig. 4. Embedding at bit 5

Fig. 5. Embedding at bit 7

The image for experimentation was changed to grayscale and performed one-level Haar wavelet decomposition. The inverse DWT was applied after the embedding to obtain the stego image for saving in extraction testing. The process had been implemented in the embedding and extraction using Python with PyWavelets, Pillow, and NumPy libraries.

Performance evaluation has been done for the steganographic system based on accuracy in message retotaling and visual imperceptibility of-recovering messages.

1. **Message Embedding and Recovery:** For DWT + XOR, the system successfully embedded and recovered a confidential message: "Confidential: Patient diagnosed with hypertension". Exact results after decryption rendered the extracted message matching the original without any variation, confirming the integrity of the embedding and extraction pipeline.
2. **Imperceptibility:** The visible difference between the originals and stego-image showed hardly noticeable effects to the naked eye. This was expected, as LSB changes in high-frequency bands are so subtle that human perception becomes less sensitive.
3. **Robustness:** The termination marker ensured accurate detection of data boundaries, while the XOR encryption added an extra layer of security over an unintelligible embedded piece of content without the correct key.

Both approaches have shown recovery of the embedded data, which is an indication of the effectiveness of DWT-based steganography. However, LL-band embedding (used with direct DWT + LSB method) is generally less secure as it has greater perceptual importance.

Fig. 6. Output image with 192KB data embedded

The increase of output image size from 3 KB to 192 KB is a result of the steganographic embedding process. During this process, secret information gets inserted into the image by substituting the least significant bits of pixel values or by adding data to unused portions of the file. These changes carry extra data to be attributed, hence leading to an increase in the overall size of the file. If the original image was too compressed or least quality, even a small change may lead to a varied increase in size, especially when the changed image is saved in a less compressed or lossless format to preserve the embedded information. Thus, the larger one becomes the stego image although it looks unchanged to the human eye in actual practice.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Method** | **Enc.** | **Domain** | **Impercept**. | Robust. | Recovery |
| DWT + XOR (Ours) | XOR | DWT (HH) | High | Moderate | 100% |
| DWT + LSB (Ours) | None | DWT (LL) | Moderate | Low | 100% |
| LSB (Spatial) | Optional | Spatial | Moderate | Low | 100% |
| DCT-based | Optional | DCT | High | High | ~95% |
| DWT + AES | AES | DWT | Very High | Very High | 100% |

Table. 1. Comparison of Steganographic Methods

Table 1 presents a comparative overview of the steganographic methods modulated by the most significant performance criteria against established techniques. It was a great trade-off between security and complexity, with imperceptibility being the highest and message recovery at most reliable in a DWT + XOR approach. The existence of embedding in frequency domain would offer greater robustness against a basic spatial domain LSB technique. DWT + LSB, despite being a less robust scheme due to greater sensitivity of the LL sub-band to visual changes, was still viewed in terms of complexity. DCT and the advanced DWT + AES methods have extremely good robustness and imperceptibility, although at the expense of considerable computational overhead. Overall, a good compromise is seen with the DWT + XOR scheme, which serves as an excellent candidate for securely, efficiently, and sublimely visually hiding data within grayscale images.

# Conclusion and Future Work

It is based on the DWT method. Thus, it represents a mechanism for steganography that and implements the information into grayscale images that might be sensitive data texts. In this work, 2 methods were developed: the first one was using XOR encryption with an LSB method in the high-frequency HH sub-band; while the second method was direct application of an LSB embedding in the LL sub-band. In the end, experimental results showed that both methods perfectly embedded the message into the stego-image without much damage or distortion. The excellent results from the DWT + XOR method provide room for most agreements between security and imperceptibility for applications like secret data transmission in medical or forensic cases.

The results are very much optimistic but can be further extended. Introduction of support for color images would increase the payload capacity. More strong and robust encryption algorithms like AES could be used to reinforce security of hidden data. Even the embedding strategies could become adaptive to the content of image for improving imperceptibility and resistance to detection of hiding. Future study also requires designing for robustness against common image processing operations like compression and resizing besides exploring the application of machine learning approaches towards embedding and extraction optimization.

This is, therefore, a good foundation for secure steganography methods which can, after further development, grow to robust tools for privacy preserving communication in the field.

##### References

1. A Secure Medical Image Steganography Based on LSB & DWT Techniques by A. Gupta, S. Singh, M. Kaur, 2022
2. Steganography in Medical Imaging: A Review by R. Sharma, P. Verma, 2021
3. Secure Steganography Using AES Encryption and LSB Substitution by T. Zhou, Y. Wang, H. Li, 2020
4. An Adaptive LSB Substitution for Medical Image Steganography by M. F. Ali, A. N. Akram, 2019
5. Robust Medical Steganography with Lossless Compression by J. Kim, S. Lee, 2018
6. Medical Image Steganography Using Multiple Bit Plane Complexity by N. Patel, V. G. Chavan, 2017
7. HOG-LSB Based Medical Image Steganography by XYZ et al., 2023
8. Medical Image Security Using DWT and SVD-Based Steganography by ABC et al., 2022
9. Hybrid DCT-LSB Steganography for Medical Data Protection by PQR et al., 2021
10. AI-Driven Steganography in Medical Images by DEF et al., 2020
11. Robust Medical Image Watermarking using LSB and Chaos Encryption by GHI et al., 2019
12. Steganographic Methods for PACS Security by JKL et al., 2018
13. A Novel Medical Steganography Technique Based on Adversarial Neural Networks
14. Image Steganography Using LSB and Hybrid Encryption Algorithms
15. Dual-Layered Security Using Cryptography and Image Steganography
16. Hybrid Steganography Technique for Secure Data Transmission in Medical Applications
17. Securing Medical Images Using Chaotic Map Encryption and LSB Steganography
18. Fortifying Data Security in Medical Imaging: Advanced Encryption and Steganography Techniques
19. DNA-Based Secure Image Transmission Framework Using Encryption and LSB Steganography
20. A Secure and Robust Image Steganography Approach Using Deep Learning