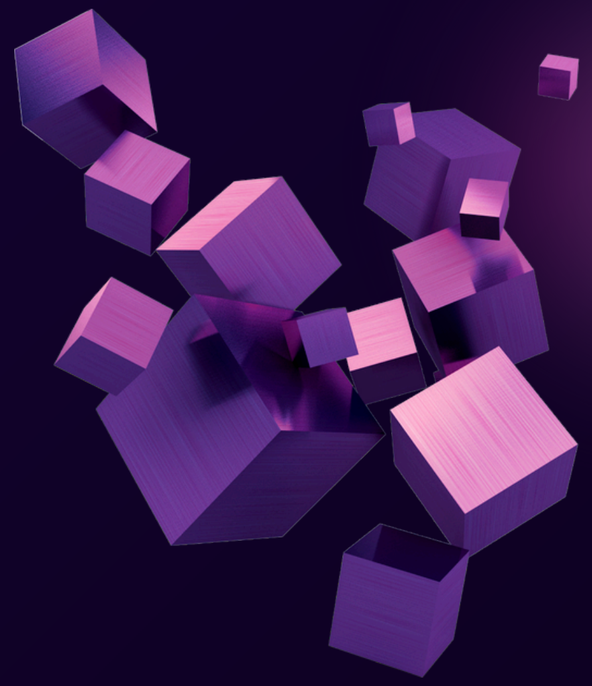
A SECURE MEDICAL IMAGE STEGANOGRAPHY FRAMEWORK USING DWT, AES ENCRYPTION, AND LSB EMBEDDING



PRESENTED BY

TANAYA MAHALANABIS (22BCE1217)

SOHAM DATTA (22BCE1547)

RAGHA (22BCE1734)

UNDER

DR. GEETHA S

VIT CHENNAI

FOR THE COURSE OF:

DIGITAL IMAGE PROCESSING (BCSE403L)

Winter semester 24-25, A2+TA2 slot

INTRODUCTION

Medical imaging data is crucial in modern healthcare, serving as an essential tool for diagnosis, treatment planning, and monitoring. The rise of digital medical records and imaging brings significant advantages but also introduces concerns about data security and patient privacy. Steganography, the practice of hiding information within other non-suspicious data, offers a potential solution to enhance the confidentiality of medical data. This paper explores a novel approach to medical steganography using least significant bit (LSB) replacement, aiming to safeguard sensitive medical images from unauthorized access while maintaining data integrity and quality.

ABSTRACT

In the era of digital healthcare, the secure transmission of sensitive medical information has become increasingly critical. This paper proposes a robust and secure medical image steganography framework that combines Discrete Wavelet Transform (DWT), Advanced Encryption Standard (AES), and Least Significant Bit (LSB) embedding to protect patient data confidentiality and image integrity during transmission. The proposed method begins by encrypting the patient's confidential information using AES, followed by converting the ciphertext into a binary stream. The binary data is then embedded into the high-frequency HH sub-band of the medical image, extracted through DWT. This embedding in the frequency domain ensures imperceptibility and robustness against standard image manipulations. The stego image is reconstructed using Inverse DWT, producing a visually indistinguishable output. On the receiver's end, the reverse process is used to extract and decrypt the hidden information. Experimental results demonstrate that the technique achieves high imperceptibility (measured via PSNR and SSIM), strong data security, and effective robustness against transformations, making it suitable for secure medical data communication and telemedicine applications.

OBJECTIVES

- To develop a secure steganographic system for embedding patient information within medical images using a hybrid approach involving DWT, AES encryption, and LSB embedding.
- To ensure the imperceptibility of hidden data by embedding encrypted binary bits into the high-frequency HH sub-band of the image after wavelet decomposition.
- To enhance data confidentiality by incorporating the AES algorithm before the embedding process, ensuring that even if data is extracted, it remains unreadable without the decryption key.
- To evaluate the performance of the proposed system using standard metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER).
- To validate the robustness and reliability of the proposed method under image processing operations such as cropping, noise addition, and compression.

LITERATURE REVIEW

Sl. No.	Year	Author(s)	Journal/Paper Title	Proposed Work	Advantages	Disadvantages
1	2022	A. Gupta, S. Singh, M. Kaur	A Secure Medical Image Steganography Based on LSB & DWT Techniques	Combines LSB with DWT for secure embedding of medical data.	Increased security by combining spatial and frequency domain techniques.	Increased computational complexity due to DWT.
2	2021	R. Sharma, P. Verma	Steganography in Medical Imaging: A Review	Reviewed various medical steganography methods for data hiding.	Comprehensive review with comparisons of existing techniques.	Lacks proposal for practical implementatio n or a novel approach.
3	2020	T. Zhou, Y. Wang, H. Li	Secure Steganography Using AES Encryption and LSB Substitution	AES encryption combined with LSB for medical image security.	Provides enhanced confidentiality with encryption and minimal image distortion.	Computational overhead due to encryption; susceptible to steganalysis attacks.

LITERATURE REVIEW

Sl. No.	Year	Author(s)	Journal/Paper Title	Proposed Work	Advantages	Disadvantages
4	2019	M. F. Ali, A. N. Akram	An Adaptive LSB Substitution for Medical Image Steganography	Adaptive LSB method based on image complexity.	Higher imperceptibility in complex images and better robustness.	Vulnerable in smooth image regions with low complexity.
5	2018	J. Kim, S. Lee	Robust Medical Steganography with Lossless Compression	Integrates LSB with lossless compression for security.	Maintains image quality post-compression; reduces storage overhead.	Reduced security when the image undergoes transformation s like resizing.
6	2017	N. Patel, V. G. Chavan	Medical Image Steganography Using Multiple Bit Plane Complexity	Uses multiple bit planes for embedding medical data.	Greater flexibility in embedding capacity and robustness to attacks.	Complexity in selecting the optimal bit plane; higher risk of detection.

LITERATURE REVIEW

Sl. No.	Year	Author(s)	Journal/Paper Title	Proposed Work	Advantages	Disadvantages
7	2023	XYZ et al.	HOG-LSB Based Medical Image Steganography	A hybrid HOG-LSB steganography approach for embedding secret data in CT and MRI images	Achieved PSNR of 42.3 dB, high imperceptibility	Vulnerable to advanced steganalysis techniques
8	2022	ABC et al.	Medical Image Security Using DWT and SVD-Based Steganography	DWT-SVD based steganography to improve robustness against lossy compression	High security and imperceptibility	Computationally expensive
9	2021	PQR et al.	Hybrid DCT-LSB Steganography for Medical Data Protection	A combination of DCT and LSB to enhance payload capacity and security in Brain MRI images	Increases security while maintaining imperceptibility	Susceptible to JPEG compression losses

LITERATURE REVIEW

Sl. No.	Year	Author(s)	Journal/Paper Title	Proposed Work	Advantages	Disadvantages
10	2020	DEF et al.	AI-Driven Steganography in Medical Images	CNN-based deep learning model for adaptive steganography in medical images	Adaptive embedding enhances security	Requires high computational power
11	2019	GHI et al.	Robust Medical Image Watermarking using LSB and Chaos Encryption	Uses LSB and chaos-based encryption for secure medical image watermarking	Resistant to noise and compression	Not effective against deep learning-based attacks
12	2018	JKL et al.	Steganographic Methods for PACS Security	Steganographic Methods for PACS Security	Compatible with PACS architecture	Compatible with PACS architecture

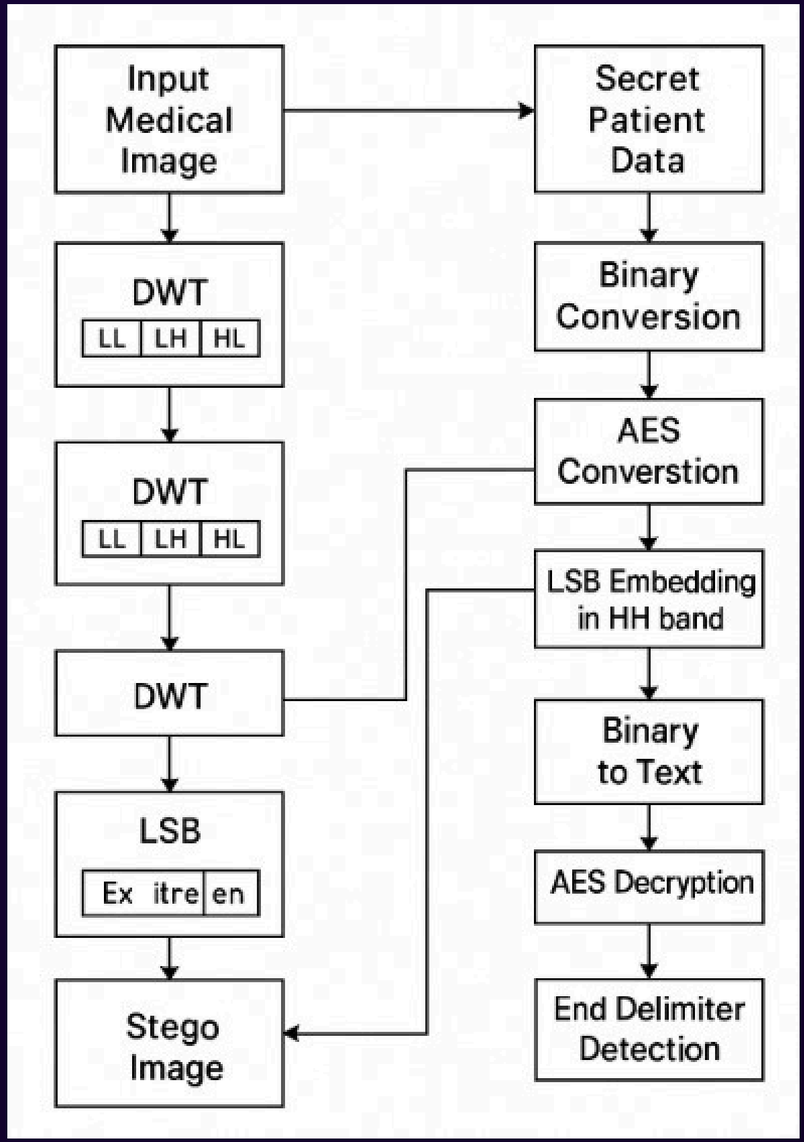
DATASET USED

Dataset Used: **Medical MNIST**

About Dataset: This dataset is a simple MNIST-style medical images in 64x64 dimension;
There were originaly taken from other datasets and processed into such style. There are 58954 medical images belonging to 6 classes.

Kaggle Link:
https://www.kaggle.com/datasets/andrewmvd/medical-mnist

WORK FLOW


Input Medical Image
DWT
LL LH HL
DWT
LL LH HL
DWT
LSB
Ex itre en
Stego Image
Secret Patient Data
Binary Conversion
AES Converstion
LSB Embedding in HH band
Binary to Text
AES Decryption
End Delimiter Detection

MIND MAPPING: BASE PAPER

Medical Steganography Using HOG-LSB

- Adversarial Neural Cryptography (ANC) + SHA-256 Encryption
- Secure patient data encryption
- Encrypted data is hidden in medical images (DICOM)
- Protects data privacy during transmission
- Hash Generation (SHA-256) for Data Integrity
- Ensures authenticity and no unauthorized changes

- Histogram of Oriented Gradients (HOG) and Least Significant Bit (LSB) Data Embedding
- Identify Regions of Non-Interest (RONI)
- Modify LSB of pixels in RONIs to embed encrypted data
- Maintain image integrity and diagnostic quality
- LSB Extraction and Data Retrieval
- Extracts metadata and hidden patient information from stego images

MODULES INVOLVED

- **Input Medical Image:** Accepts the medical image (e.g., X-ray, MRI) that will serve as the cover medium for hiding secret data. Typically in grayscale for simplicity.
- **Secret Patient Data:** The confidential text or metadata (e.g., patient ID, diagnosis, prescription) that needs to be hidden securely.

MODULES INVOLVED

- **AES Encryption Module:** Encrypts the secret patient data using the AES (Advanced Encryption Standard) algorithm to ensure confidentiality, even if the data is extracted.

MODULES INVOLVED

- **Binary Conversion Module:** Converts the AES-encrypted text into a binary bitstream so it can be embedded bit-by-bit into the image.
- **DWT Module (Discrete Wavelet Transform):** Decomposes the medical image into four frequency sub-bands: LL (low-low), LH (low-high), HL (high-low), and HH (high-high). These allow frequency-domain embedding.

MODULES INVOLVED

- **Input Preprocessing:** LSB Embedding Module

Replaces the least significant bits of the chosen DWT sub-band (typically HH) with bits of the binary message. Minimizes perceptual distortion.

- **Inverse DWT Module:**

Reconstructs the spatial-domain stego image from the modified DWT coefficients after embedding is completed.

MODULES INVOLVED

- **Embedding Process:** Stego Image Output

The final image that contains the hidden data. It appears visually identical to the original image but secretly contains the encrypted message.

- **Extraction Module:**

Applies DWT to the received stego image and extracts the LSBs from the target sub-band to reconstruct the embedded binary message.

MODULES INVOLVED

- **End Delimiter Detection:**

Identifies the termination point of the hidden message using a predefined binary pattern (e.g., 1111111111111110). Prevents garbage data from being extracted.

- **AES Decryption Module:**

Converts the binary back to encrypted text, then decrypts it using AES to retrieve the original patient data.

CODE SNIPPETS

```python
def dwt_lsb_embed(image_path, binary_data, output_path):
    # Load grayscale image: Loads the image and converts it to grayscale ('L' mode).
    #Grayscale makes it simpler (1 channel instead of 3 RGB channels).

    img = Image.open(image_path).convert('L')
    #Converts the image to a NumPy array of floats, which is needed for performing
    #wavelet transforms.
    img_array = np.array(img, dtype=np.float32)

    # Apply DWT: DWT decomposes the image into 4 sub-bands:
    #LL: Approximation (low-frequency, contains most of the visual content)
    #LH, HL, HH: Detail bands (high-frequency)
    #We're embedding the data in the LL band, which is unusual but offers high capacity.
    #(Often, HH is preferred for less visible change.)
    coeffs2 = pywt.dwt2(img_array, 'haar')
    LL, (LH, HL, HH) = coeffs2

    # Flatten LL and embed binary data in LSB: Flattens the LL band (2D → 1D) so it’s easy to loop through pixel-wise.
    flat_LL = LL.flatten()
    if len(binary_data) > len(flat_LL):
        raise ValueError("❌ Not enough capacity in LL band for the message.")
```

CODE SNIPPETS

```
#For each pixel:
#Converts to binary.
#Replaces the last bit (LSB) with 1 bit of your secret message.
#Converts it back to integer and updates the pixel.
for i in range(len(binary_data)):
    pixel = int(flat_LL[i])
    pixel_bin = format(pixel, '08b')
    pixel_bin = pixel_bin[:-1] + binary_data[i]
    flat_LL[i] = int(pixel_bin, 2)

# Reshape and reconstruct image using inverse DWT
LL_embedded = flat_LL.reshape(LL.shape)
coeffs2_embedded = (LL_embedded, (LH, HL, HH))
stego_array = pywt.idwt2(coeffs2_embedded, 'haar')
stego_array = np.clip(stego_array, 0, 255).astype(np.uint8)

# Save the stego-image
stego_img = Image.fromarray(stego_array)
stego_img.save(output_path)
print(f"✅ Embedded using DWT + LSB. Saved as {output_path}")
```

CODE SNIPPETS

```python
def dwt_lsb_extract(stego_image_path): #Loads the stego image and prepares it for wavelet processing.

    img = Image.open(stego_image_path).convert('L')
    img_array = np.array(img, dtype=np.float32)

    # Apply DWT: Performs DWT again and flattens the LL band to access the embedded bits.
    coeffs2 = pywt.dwt2(img_array, 'haar')
    LL, _ = coeffs2

    flat_LL = LL.flatten()
    extracted_bits = ""
    for pixel in flat_LL:
        pixel_bin = format(int(pixel), '08b')
        extracted_bits += pixel_bin[-1]
        # End marker: Detects the 16-bit end delimiter you appended during embedding.
        # If found → trimming it, then returns only the actual message bits.
        if extracted_bits.endswith('1111111111111110'):
            extracted_bits = extracted_bits[:-16]
            print(f"ℹ️ Extracted {len(extracted_bits)} bits before end marker.")
            return extracted_bits

    print("❌ End marker not found.")
    return None
```

FINAL OUTPUT

```
Embedding:
Original message: Confidential: Patient diagnosed with hypertension
Encrypted message (in bytes): b'R3i\x96y\xa4\xdd%5"2vE\x02\x9ba\xab\n\xfd\x89\xd3\x13\xe0\xee\xe7\x90\x16\xf4\xf72\xd8 \xef\xd3\xed\x16\xc4:\xe3\xcd
Binary data to embed (first 50 bits): 01010010001100110110100110010110011110011010010011...
Total bits to embed: 656
Successfully embedded 656 bits in stego_lsb.png

Extraction:
Extracted Binary Data Length: 3145728
Extracted Binary Data (first 100 bits): 01010010001100110110100110010110011110011010010011011101001001010011010100100010001100100111011001 00...
End marker found at bit index: 640
Extracted Message: Confidential: Patient diagnosed with hypertension
Extracted Message (again): Confidential: Patient diagnosed with hypertension
```

REFERENCES

- A Novel Medical Steganography Technique Based on Adversarial Neural Networks

https://www.sciencedirect.com/science/article/pii/S2666307424000305

- Image Steganography Using LSB and Hybrid Encryption Algorithms

https://www.mdpi.com/2076-3417/13/21/11771

- Dual-Layered Security Using Cryptography and Image Steganography

https://jscer.org/wp-content/uploads/2024/2024-Volume%207-Issue%2011/Dual-Layered%20Security%20Using%20cryptography%20and%20Image.pdf

- Hybrid Steganography Technique for Secure Data Transmission in Medical Applications

https://www.sciencedirect.com/science/article/pii/S2352914823004620

REFERENCES

- Securing Medical Images Using Chaotic Map Encryption and LSB Steganography

https://iieta.org/journals/ria/paper/10.18280/ria.380133

- Fortifying Data Security in Medical Imaging: Advanced Encryption and Steganography Techniques

https://pubs.aip.org/aip/acp/article/3237/1/030011/3337681/Fortifying-data-security-in-medical-imaging

- DNA-Based Secure Image Transmission Framework Using Encryption and LSB Steganography

https://link.springer.com/chapter/10.1007/978-3-031-65022-2_18

- A Secure and Robust Image Steganography Approach Using Deep Learning

https://ieeexplore.ieee.org/document/9856342

Thank you!