A Wavelet-Based Approach for Authenticating Medical Images and Extracting Patient Information

RAMAKRISHNA MISSION RESIDENTIAL COLLEGE(AUTONOMOUS),
NARENDRAPUR, KOLKATA - 700103

B.Sc. Sixth Semester Examination, 2024

Subject: Computer Science

Paper: DSE04 (Project)

Submitted by:

Arnab Ghosh (Registration No: A03-1112-0181-21, Roll no: 6R24CMSA2002)

Jit Malla (Registration No: A03-1122-0183-21, Roll no: 6R24CMSA2006)

Raihan Uddin (Registration No: A03-1142-0188-21, Roll no: 6R24CMSA2009)

Supervised by:

Sri Bibek Ranjan Ghosh

Submitted on: May 21, 2024

Index

Acknowledgment

We extend our deepest gratitude to our esteemed Supervisor, Sri Bibek Ranjan Ghosh, for his invaluable and constructive academic advice, continuous encouragement, and astute guidance at every critical juncture of our project. His expertise and thoughtful supervision were crucial in enabling us to successfully prepare our project report. Additionally, we are profoundly thankful to our respected Head of the Department, Dr. Siddhartha Banerjee, for allowing us the use of departmental facilities, which significantly facilitated our research. We would also like to express our appreciation to our lab assistant, Shyamaprasad Chakravorty, and all the teachers in our department for providing us with this enriching opportunity to engage in a project that has been a pivotal part of our DSE-4 curriculum, enhancing both our practical and theoretical knowledge in the field.

Certificate

I hereby certify that the project report titled "A Wavelet-Based Approach for Authenticating Medical Images and Extracting Patient Information," submitted by Arnab Ghosh (Registration No.: A03-1112-0181-21, College Roll No.: CSUG/111/21), Jit Malla (Registration No.: A03-1122-0183-21, College Roll No.: CSUG/113/21), and Raihan Uddin (Registration No.: A03-1142-0188-21, College Roll No.: CSUG/182/21), to the faculty of the Computer Science Department of Ramakrishna Mission Residential College, is a record of the project work carried out by the students under my supervision in complete fulfilment of the requirements for the Degree of Bachelor of Science (Honours) in Computer Science during the final semester (Semester VI) of the academic session 2023-2024.

(Signature of Head of the Department)   (Signature of Supervisor)

Problem Description

This project is dedicated to ensuring the authenticity and integrity of medical images shared online. The objective is to embed hidden markers, called watermarks, within these images to verify their genuineness and prevent unauthorized alterations. This process, known as digital watermarking, employs various techniques to seamlessly integrate imperceptible information into the images. Methods such as Discrete Wavelet Transform (DWT), Histogram shifting and Arnold Cat Map are being explored for their effectiveness in this context. By incorporating these techniques, the project aims to enhance the security and trustworthiness of medical images used for diagnostic purposes, treatment planning, and research. Once the watermarks are embedded, they serve as covert signatures that can be later extracted to verify the originality of the images. This verification process acts as a safeguard against potential tampering or malicious modifications, ensuring the reliability of the images in medical settings. Ultimately, the project seeks to provide healthcare professionals and researchers with a robust tool for verifying the authenticity of digital medical images, thereby contributing to improved patient care and medical research outcomes.

Chapter 1: Introduction

1.1 Steganography:

Steganography is about hiding a secret message inside a regular file like an image or audio using a special key. This key can encrypt the message and help mix it into the file. This process creates a medium, which looks normal but secretly carries hidden information that only people with the key can find. This method is great for keeping messages private and hidden [1].

The word "steganography" comes from two Greek words: "steganos," which means hidden or covered, and "graph," which means to write. So, steganography literally means "hidden writing." [2]

In digital steganography, the main goal is to make sure that an image with hidden information (stego-image) looks so normal that nobody suspects it's been altered [3]. Basically, we slightly change a regular image (cover object) to include the hidden data. Typically, those trying to detect such images (wardens) look for unusual patterns or statistics that differ from normal images.

1.2 Watermarking:

Digital watermarking is the process of embedding specific information, like text, logos, or codes, into a digital medium (such as images, videos, or audio) primarily to prove ownership, verify authenticity, or ensure the integrity of the content [4]. This embedded data is not meant to be a secret; instead, it serves as a digital signature to identify the creator or owner of the content, check if the content has been altered in any way, and possibly repair any damages. Watermarking is used extensively in copyright protection, helping to manage rights and prevent unauthorized use of digital media. Unlike steganography, which is used for covert communication, the purpose of watermarking is open and focused on protection and authentication. Watermarks can sometimes be visible, depending on their intended use, and don’t necessarily need to carry large amounts of data.

Digital watermarking adds a logo or code to an image to indicate ownership or verify integrity, using methods that modify the image's pixels (spatial domain) or its data after mathematical transformation (frequency domain) [5]. In the spatial domain, subtle color changes can embed watermarks, though these can be lost if the image is heavily edited or compressed. The frequency domain offers more security by embedding watermarks in transformed image data, making them harder to remove without damage

1.3 Characteristics of Steganography:

In steganography, the message to be hidden inside the cover media must consider several critical features to ensure effectiveness and security. These features include hiding capacity, perceptual transparency, robustness, and imperceptibility [6,8]. Here's an overview of these.

1.3.1 Hiding Capacity:

Hiding capacity refers to the amount of information that can be concealed within the cover file. A larger hiding capacity is advantageous because it allows a smaller cover media to be used, thereby reducing the bandwidth required for transmitting the stego media. For instance, in an RGB image measuring 200 x 200 pixels, there are 120,000 color values available for embedding the secret message (200 pixels in width x 200 pixels in height x 3 color channels: Red, Green, Blue). By embedding one bit of the secret message per color channel, the hiding capacity is 120,000 bits, or 15,000 bytes. If two bits per color channel are used, the capacity doubles to 30,000 bytes. Alternatively, if only one color channel and one bit per pixel are used, the capacity is reduced to 40,000 bits, or 5,000 bytes [7].

1.3.2 Perceptual Transparency:

Perceptual transparency is a vital feature in steganography. It ensures that the cover media remains visually or audibly unchanged even after embedding the secret message. Each cover media has a specific limit to how much data it can hide without noticeable degradation. Exceeding this limit can cause visible or audible distortions, making the stego media appear different from the origin al cover media. If such distortions are detectable, the steganographic method fails, as it might alert an attacker to the presence of hidden information, risking extraction or damage to the original message [7].

1.3.3 Robustness:

Robustness in steganography refers to the ability of the stego-image to keep the hidden message intact, even after the image undergoes various modifications like sharpening, rotation, cropping, blurring, scaling, and adding noise. This ensures that the secret data remains safe and retrievable despite these changes [8].

1.3.4 Imperceptibility:

Imperceptibility in steganography means that after embedding the secret message, the cover image should still look the same to human observers. The goal is to ensure that the changes made by embedding the message are so small that they cannot be noticed by the human eye. To determine if a steganographic method is truly imperceptible, we use standard measurement techniques to evaluate the visual quality of the image. These techniques help us quantify any changes and ensure that they are minimal, maintaining the illusion that the image is unaltered. If an image passes these tests, it means the steganographic method used is perceptually transparent and effective [8].

1.4 Image Steganographic Techniques:

Basically image steganography are divided into two parts -

1.4.1 Spatial Domain Technique:

In the spatial domain, the watermark is directly embedded into the pixel values of the image. This can be achieved through various methods, such as modifying the least significant bits (LSB) of the pixel values. The LSB modification technique involves replacing the least significant bits of the pixel values with the bits of the watermark message. Since the LSBs contribute minimally to the overall pixel value, this modification typically results in minimal perceptual changes to the image. Additionally, intermediate significant bit (ISB) modification or patchwork algorithms can also be utilized to embed the watermark while maintaining the visual quality of the image[9].

1.4.2 Transform Domain Technique:

Transform domain techniques, also known as frequency domain techniques, hide secret messages by first converting an image from its regular pixel-based form (spatial domain) into a frequency-based form using methods like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Once in the frequency domain, the secret message is embedded into the transformed data (frequency coefficients). The image is then converted back to its original form, now containing the hidden message. These techniques are often used in image compression algorithms because they securely embed data in a way that's difficult to detect and alter. And they may outrun lossless and lossy format conversions[10]. Transform domain techniques are
broadly classified into:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bit

1.5 Performance metrics for image watermarking:

There are several methods to evaluate the quality of image watermarking, each focusing on a different aspect of the watermarking process. These methods collectively assess the visual quality, robustness, and capacity of the watermarked image. Some of the well-known methods are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structured Similarity Index Measure (SSIM), Payload Capacity[11][12].

1.5.1 Mean Square Error(MSE):

Mean Square Error measures the average squared difference between pixels in the original and watermarked images. It quantifies the distortion introduced by watermarking: a lower MSE indicates the watermarked image is very similar to the original, implying higher quality with minimal alterations. MSE is useful for assessing how much the watermarking process has altered the image.

$$\mathrm{MSE}\ (\mathrm{q1}, \mathrm{q2}) = \frac{1}{\mathrm{MN}} \sum_{\mathrm{i}=0}^{\mathrm{M}-1} \sum_{\mathrm{j}=0}^{\mathrm{N}-1} (\mathrm{q}_1(\mathrm{i},\mathrm{j}) - \mathrm{q}_2(\mathrm{i},\mathrm{j}))^2$$

Equation 1: Mean Square Error

M, N = Dimensions of the image
I = Original Image
K = stego-image
Where q1 (i, j) and q2 (i, j) indicate the original and extracted images, respectively.
Note: Lower value of MSE indicates good quality of embedding.

1.5.2 Peak Signal to Noise Ratio:

Peak Signal Ratio is a metric derived from Mean Square Error (MSE) that measures the quality of the watermarked image by comparing the original signal to the noise introduced by watermarking. It is calculated using the formula:

PSNR = 10xlog (Max2 /MSE)
Where Max is the maximum possible pixel value of the image (255 for an 8-bit image).

PSNR is expressed in decibels (dB), and a higher PSNR value indicates better image quality, as it signifies that the noise (distortion) introduced by watermarking is low relative to the signal strength of the original image.

1.5.3 Payload capacity:

Payload Capacity refers to the amount of information that can be embedded within an image without significantly affecting its quality. This is crucial in steganography, where maximizing data hidden in the cover image is key while maintaining its visual integrity. Payload capacity is measured in Bits Per Pixel (BPP), calculated using the formula:

BPP=(Number of Secret Bits Embedded/Total Number of Pixels)

A higher BPP indicates that more information can be embedded in the image, which is beneficial for applications requiring substantial data hiding.

1.5.4 Structural Similarity Index Measure (SSIM):

SSIM is a metric of comparison to check the similarity between the cover image and stego-image. It measures the perceptual difference between the two images.

SSIM= (2μxμy + c1)(2σxy +c2)/((μx) 2+(μy) 2 +c1)((σx) 2 +(σy) 2 + c2)

c_1 and c_2 are the two stabilizing parameters,

c1 = (k1L)2

c2 = (k2L)2

L is the dynamic range of pixel values (2#bits per pixel - 1)

Let the contents, k1=0.01 and k2=0.03.

μx and μy are the mean intensity values of images x and y.

(σx) 2 is the variance of x,

(σy) 2 is the variance of y

(σxy) 2 is the covariance of x and y.

Note: SSIM value close to 1 indicates good quality

1.5.5 Normalized Cross-Correlation (NCC):

It measures image similarity by sliding a window over two images, multiplying corresponding pixel values, summing the results, and then normalizing. The resulting value, between -1 and 1, indicates the degree of similarity: values close to 1 denote high similarity, and values near -1 indicate low similarity.

$$\mathrm{NCC} = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}(I_c(i,j)\,I_s(i,j))}{\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}(I_c^2\,(i,j))}$$

Equation 2: Equation of NCC

Here, M is row , N is column, Ic is cover image and Is is stego image.

Target of performance as a whole: A low MSE (close to 0), high PSNR(>30dB) and high SSIM value (nearly 1) is desired as a result

1.6 Discreate Wavelet transform technique (DWT):

The Wavelet Transform is a powerful tool used in signal processing and image compression. It works by breaking down a signal or image into different frequency components, allowing for both time and frequency representations. In image processing, it transforms the image into multiple sub-bands, each containing different frequency information. The Discrete Wavelet Transform (DWT) is a specific type of wavelet transform that uses a discrete set of wavelet scales and translations, creating mutually orthogonal sets of wavelets. It provides a multi-resolution analysis of images, converting the input image into low-pass and high-pass wavelet coefficients. In image steganography, DWT is beneficial for increasing capacity and robustness. Recent studies have shown that combining DWT with different encoding methods enhances imperceptibility and security. The Haar-DWT, a basic form of DWT, involves scanning pixels horizontally and vertically, performing addition and subtraction operations to create four sub-bands: LL (low frequency), HL, LH, and HH (high frequency). These sub-bands offer detailed frequency information for effective image transformation and steganography [13][14].

1.7 Arnold-cat map (location map):

Chaos, commonly used in random number generation, offers speed and simplicity in handling both storage and processing tasks. It involves a few functions called chaotic maps and some initial parameters for efficient operation. One such method is Arnold's Cat Map, a two-dimensional chaotic technique used to shuffle pixel positions in an image without losing any data. The Cat Map equation transforms pixel coordinates to create a new image. By iterating this transformation randomly for a certain number of times, a scrambled image is generated, ensuring digital image encryption. This scrambled image can be safely transmitted over communication channels without revealing its content. At the receiving end, reversing the process brings back the original image, ensuring secure transmission and protection against unauthorized access [15].

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} (\bmod n)$$

$$\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\bmod n)$$

Equation 3: Equation of Arnold cat map

Where p and q are the positive integers

(x’,y’) is the correspondence new location of the original pixel

1.8 Histogram Shifting:

The histogram shifting method is a reversible data hiding technique used to embed secret data into a cover image in a way that allows the original image to be fully recovered after the secret data is extracted [16]. The key steps of this method are as follows:

Histogram Analysis: The histogram of the cover image's pixel values is analyzed to identify peak points (the most frequent pixel values) and zero points (pixel values with zero frequency).

Shifting: To create space for embedding, the pixel values in the histogram are shifted. For instance, pixel values from the peak point to the right of the zero point are increased by one. This shift creates an empty bin in the histogram where the secret data can be embedded.

Embedding: Secret bits are embedded into the created empty bin. The number of bits that can be embedded is proportional to the frequency of the peak point in the histogram.

Extraction and Recovery: During extraction, the receiver uses the information about the peak and zero points to correctly extract the embedded data and shift the pixel values back to their original positions, thus recovering the original cover image without loss.

Chapter 2: Literature Survey

In this article Meghana et al.[17] (2019), the author proposes a reversible data hiding technique in the spatial domain using Histogram Shifting. It relies on embedding the watermark into the original image after dividing it into blocks. Additionally, a Gaussian filter is employed after the extraction process for noise removal. The cover image is divided into non-overlapping blocks, with overflow and underflow conditions checked. For each block, a reference pixel is selected (the difference between the maximum pixel and the remaining pixels). The average of the remaining pixels is then calculated, and a difference histogram is generated. The pixel values are converted into binary values, with the LSB of each pixel set to 0. The watermark image is resized and also divided into non-overlapping blocks, with each block's pixel values converted into binary. These binary values are then embedded into the LSB of the cover image. During the extraction process, the same operations are applied to the stego image, with the reference pixel being the same one chosen during the embedding process. The highest PSNR value achieved is 36.21 dB for the Charlie image.

In this paper Yujie Jia et al.[18] (2019) author present a Reversible Data Hiding (RDH) scheme that leverages image texture to enhance embedding efficiency while reducing the impact on image quality. The process begins by the cover image is divided into two sub-images by checkerboard pattern and calculate the fluctuation values for each sub-images then the data is embedded into this sub-images with minimum fluctuation values. In the proposed method, first divide the image into two sets, A and B, arranged in a checkerboard pattern. Then calculate the fluctuation value for each pixel in set A by determining its local complexity using a formula the differences between a pixel and its four nearest neighbors in vertical, horizontal, and diagonal(positive and negative) directions. The fluctuation value of each pixel is then adjusted based on the complexities of its adjacent pixels. Next, they predict each pixel's value using its four nearest neighbors and a set of normalized weights, and calculate the prediction error as the difference between the mean and predicted values. In embedding process first checking the overflow and underflow condition then the fluctuation and prediction errors of all pixels in A are acquired according to B,sort the fluctuation values and prediction sequence in ascending order which is obtained in same scanning order. The embedding is then carefully executed by modifying the prediction errors based on specified conditions involving predetermined peak points (PK1, PK2) and zero points (Z1, Z2). The modified prediction errors result in new pixel values that form the marked image of A. Following this, the embedding process for set B is carried out in a similar manner. Extraction and recovery are the reverse process, first extract the additional data from B and recover B, then do the same on A. Followed by obtaining marked prediction errors for all pixels in B. These values are arranged in ascending order to generate sequences for fluctuation values (FB1, FB2, ..., FBi) and corresponding marked prediction errors (e0FB1, e0FB2, ..., e0FBi). To extract embedded data, each marked prediction error is analyzed if it matches one of the predetermined peak points (PK1, PK2) or the immediate values outside these peaks, a bit (0 or 1) is extracted according to specified rules. This extraction continues until half of the payload is obtained. The original prediction errors are then reconstructed by adjusting the marked errors based on their relationship to peak points and zero points (Z1, Z2). The original pixel values are recovered by adjusting the predicted pixel values with these corrected prediction errors. The original prediction errors are then reconstructed by adjusting the marked errors based on their relationship to peak points and zero points (Z1, Z2). The original pixel values are recovered by adjusting the predicted pixel values with these corrected prediction errors. For the textured "Baboon" image and the smoother “Airplane” image, the proposed steganographic method achieves a PSNR greater than 58 dB at an embedding capacity of 0.02 bits per pixel (bpp) for “Baboon”.

In this paper author Vinoth Kumar et al.[19] (2013) introduces a modified histogram shifting algorithm for reversible medical image watermarking, aimed at increasing data hiding capacity and maintaining high stego-image quality. The approach involves hierarchically dividing the cover image into smaller blocks for data embedding, using a recursive looking-ahead estimation technique to optimize the data hiding volume. This ensures the optimal block division is selected based on hiding capacity, particularly effective for medical images with extensive dark areas. Experimental results demonstrate the efficacy of this method, showing improved PSNR values up to 59.05 for non-recursive and 58.8 for recursive methods. The mean square error (MSE) values range from 0.08 to 0.37, confirming minimal image distortion. This advanced technique enhances the security and integrity of medical images during online sharing, ensuring complete restoration of the original image after data extraction.

In this paper, Abdel-Nabi et al.[20] (2017) introduces a joint reversible data hiding and encryption algorithm to secure medical images in telemedicine, ensuring high embedding capacity and low computational complexity. The algorithm divides the image into two halves, embedding a different watermark in each half—one before encryption and the other after. This method employs substitution-based and transposition-based encryption techniques to achieve high entropy and ensures the original image can be fully recovered. Performance evaluations on 512×512 CT images show the algorithm achieves PSNR values of 56.60 dB for directly decrypted watermarked images, 58.81 dB for partially watermarked images, and infinite PSNR for fully restored images. This indicates the algorithm maintains high image quality while providing robust security and exact recovery capabilities.

In this article, author Li-Chin Huang et al.[21] (2013) introduces a reversible data hiding method using histogram shifting for high-quality 16-bit depth medical images. The process involves dividing the image into local pixel blocks, calculating difference values between neighboring pixels to generate a difference histogram, and embedding secret bits by shifting this histogram. This method ensures the original image can be accurately recovered post-extraction. Underflow and overflow issues are managed effectively due to the high bit depth, with specific strategies for signed and unsigned images. The embedding process balances data hiding capacity and image quality by adjusting block size and embedding parameters. Results show PSNR values above 61 dB for signed and 74 dB for unsigned images, maintaining high image quality and structural integrity.

In this article, author Chin-Chen Chang et al.[22] (2014) the reversible image hiding method outlined in the paper "Reversible Image Hiding for High Image Quality based on Histogram Shifting and Local Complexity" involves several key stages: preprocessing, histogram shifting, local complexity calculation, peak identification, data embedding, and data extraction/image recovery. Preprocessing includes converting color images to grayscale. The histogram shifting process incorporates identifying smooth and complex image blocks based on a complexity measure and then computing the histogram of difference values to locate peak points. Data embedding involves shifting histogram bins to accommodate secret data, primarily focusing on smooth blocks with higher peak histogram bins. For data extraction and image recovery, the original image and embedded data are restored through inverse histogram shifting. The results section details performance metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM). While specific MSE values are not provided, higher PSNR values, such as those reported for the proposed scheme and grayscale Kodak images, imply lower distortion and superior image quality. The paper concludes that the method effectively embeds data with minimal visual distortion, making it suitable for applications requiring high-quality image preservation, such as medical imaging.

A.A. Karawia et al.[23] (2021), the paper "Medical image steganographic algorithm via modified LSB method and chaotic map" introduces a method for securely embedding secret medical images into host images for transmission. The algorithm proceeds as follows: the secret medical image undergoes encryption using a one-dimensional chaotic map, followed by the random selection of pixel positions within the host image using a two-dimensional chaotic map. The encrypted bits are then shuffled before being embedded using a modified LSB method, resulting in the creation of the stego image. Evaluation of host and stego image quality involves metrics such as PSNR, MSE, SSIM, histogram test, image quality measure, and resistance to chi-square attacks. Results demonstrate low MSE, high PSNR values, and high structural similarity (SSIM) between host and stego images, indicating minimal distortion and imperceptibility of embedded data. Overall, the algorithm achieves high visual quality and robustness against attacks, ensuring secure transmission of medical images.

De Rosal Ignatius et al.[24] (2019) introduces an RDH technique using histogram shifting to secure medical images without compromising diagnostic accuracy. RC4 encryption enhances data security, yielding high PSNR and SSIM scores while increasing entropy. Perfect retrieval of images and data is achieved, ensuring confidentiality during transmission and storage.

RDH plays a crucial role in maintaining data integrity and confidentiality in medical imagery. Integration with RC4 encryption advances secure data hiding, protecting patient data effectively. Further research could focus on adaptive methods to minimize histogram shifts based on message capacity. In the paper, the range of values for BPP, MSE, PSNR (dB), and SSIM are BPP: 0.0021 to 0.5217,MSE: 0 to 0.9525,PSNR: approximately 48.34 dB to 51.81 dB,SSIM: approximately 0.9855 to 0.9994.

In this paper, author Wein Hong et al.[25] (2008) introduces a novel reversible data hiding technique called Histogram Shifting of Prediction Errors (HSPE), which enhances both the embedding capacity and the quality of the stego image. The method involves predicting pixel values, calculating prediction errors, and using histogram shifting to embed secret messages. Before embedding, the secret messages are encrypted using RSA or DES algorithms, ensuring secure data transmission. The experimental results demonstrate that HSPE achieves an average embedding capacity 4.74 times higher than the well-known method by Ni et al., while maintaining a PSNR above 48 dB. Additionally, under the same embedding capacity, HSPE improves stego image quality by an average of 7.99 dB. These advancements make HSPE particularly suitable for applications requiring high image quality and accurate reversibility, such as in medical and military imaging.

Author A. K. Sonaniya et al.[26] (2022) The paper presents the Secure Framework for Color Histogram and Data Hiding (SFCHDH), designed to protect medical images by embedding patient information into the color histogram of the images using a combination of data hiding and cryptographic techniques. The embedding process involves hiding patient information within the color histogram of the medical image and applying hybrid cryptography to encrypt the embedded data, ensuring confidentiality and integrity. The extraction process includes decrypting the information with the appropriate cryptographic keys and retrieving the hidden data from the color histogram. The framework demonstrates high security and efficiency, with minimal impact on image quality, as validated by metrics such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM). SFCHDH effectively protects medical images, ensuring secure embedding and extraction of patient information while maintaining high image quality, crucial for digital healthcare applications.

R. Rathna Krupa et al.[27] (2014),This procedure outlined in the study involves a meticulous process of embedding a secret image within a cover image while ensuring minimal distortion and robustness against various attacks. It begins by resizing the secret image to match the dimensions of the cover image and shifting pixel values to enhance security. The least significant bits (LSBs) of the cover image are then cleared, and the modified secret image is embedded into the cover image using LSB substitution. Subsequently, the Optimal Pixel Adjustment Process (OPAP) is applied to fine-tune pixel values and enhance the quality of the stego image. Experimental results demonstrate that the procedure achieves a Mean

Square Error (MSE) of 42.06 for the stego image, indicating some level of distortion. However, the application of OPAP mitigates this error and ensures the hidden secret image remains visually imperceptible within the cover image. Moreover, the incorporation of a genetic algorithm further reduces the error and enhances the overall quality of the stego image, emphasizing the importance of employing advanced techniques for effective image hiding. Ultimately, the study underscores the significance of achieving a balance between ease of use and maintaining the secrecy of embedded content, as reflected in the desire for lower MSE and higher Peak Signal-to-Noise Ratio (PSNR) values to ensure a proper and enhanced result.

F. N. Thakkar et al.[28] (2016) and colleagues proposed a method to secretly hide messages in images without changing their appearance. They divided the image into two parts: the region of interest (ROI) and the rest of the image (RONI). Their focus was on the ROI for embedding the secret message. They used a technique called Discrete Wavelet Transform (DWT) to break down the ROI into smaller parts and then applied a mathematical operation called Singular Value Decomposition (SVD) on each of these parts. They used the left part of the SVD result for hiding the message bits. Meanwhile, they converted the secret message and some extra bits for error correction into binary strings. To ensure the message's integrity, they applied Hamming code to these binary strings. They then determined specific locations in the mathematical results of the image where they could hide these bits. After embedding the message, they reversed the mathematical operations to reconstruct the image with the hidden message. To validate their method, they compared the original and modified images using various metrics such as PSNR, WPSNR, SSIM, and NCC. Their results demonstrated high accuracy, with PSNR of 44.0333, WPSNR of 50.8285, SSIM of 0.9673, and NCC score of 0.994, even in the presence of a small amount of noise.

Author A. K. Singh et al.[29] (2019) introduced a novel method based on LWT-DCT for embedding watermarks, particularly focusing on patient reports, into medical images. Initially, a host image of size 512 X 512 and a watermark image of size 64 X 64, representing the patient report, are considered. The host image undergoes decomposition using third-level LWT, and the LH sub-band resulting from this decomposition undergoes DCT transformation. Simultaneously, the watermark is also transformed using DCT and then encrypted using the MD5 hash algorithm. The encrypted watermark is embedded into the host image using a gain factor, while the encoded patient report is embedded in the HL sub-band. The watermarked image is then reconstructed using inverse DCT and inverse LWT. Evaluation of the method shows the highest PSNR value of 34.72 dB achieved for 60 and 80 characters with a gain factor of 0.05, though the NC value is slightly lower at 0.8572 for 60 characters and 0.8524 for 80 characters at the same gain factor. The method achieves the best NC value of 0.9813 for 25 characters with a gain factor of 0.2.

A. Anand et al.[30] (2020) and his team proposed an advanced watermarking approach tailored specifically for securing medical images. Their method, grounded in DWT-SVD domain, aimed to enhance image integrity without compromising visual quality. Employing both text and image watermarks, they first segmented the image into two parts, focusing on the LL subband of a 2nd level DWT decomposition. Further decomposition led to four subbands: LL2, HL2, LH2, and HH2. SVD was applied to HL1 and LH1 subbands, facilitating the embedding of divided image watermarks using a gain factor, while Hamming code was utilized for encoding text watermarks, embedded in the HH2 subband. The resulting watermarked image underwent inverse DWT before encryption using chaotic or hyperchaotic algorithms. Compression techniques such as Huffman or LZW were applied for file size reduction. Experimental validation, conducted on MATLAB R2017a, involved varying gain factors (α) and observed a PSNR of 36.1007 dB without noise, with the highest NC of 0.9911 at α = 0.10. For cell images, a PSNR of 44.1944 dB was achieved using Hyperchaotic-LZW, though cropping attacks yielded a lower NC value of 0.5082, highlighting robustness challenges under specific adversarial conditions.

Chapter 3: Proposed Method

Watermarking medical images is crucial for protecting patient information. For watermark embedding Histogram Equalization has been proposed. To enhance the security we have used two different methods DWT, Arnold cat Map. All have been experimented with SIPI and medical images.

3.1 Embedding and Extraction Procedure for Watermarking Using Wavelet Transform and Arnold's Cat Map

3.1.1 Embedding Process

In this approach, the cover image undergoes Frequency Wavelet Transform (FWT) to break it into frequency components, which are then split into low-frequency (LL) and high-frequency (HH) parts. The secret image is subjected to Arnold's Cat Map transformation for added security, converted into binary, and embedded within the LL part. Meanwhile, the SHA-256 hash of the secret image is calculated and embedded into the HH part. Finally, Inverse Wavelet Transform (IWT) is applied to reconstruct the modified LL and HH parts, resulting in the creation of the stego image.

FWT Formula:

$$a[n] = \lfloor(x[2n] + x[2n]+1)/2\rfloor$$

$$d[n] = x[2n] - x[2n+1]$$

Equation 4: Equation of FWT

Inverse FWT Formula:

$$X[2n] = a[n] + (\lfloor(d[n] + 1)/2\rfloor)/2$$

$$X[2n+1] = x[2n] - d[n]$$

Equation 5: Equation of IFWT

<u>Algorithm1: Embedding (COVER, WI)</u>

Step1: Take the 1-level 2D DWT of COVER image.

Step2: Apply FWT to the cover image to decompose it into frequency components, separating the image into its various frequency bands for more efficient processing.

Step3: Split the transformed image into LL (low-frequency) and HH (high-frequency) components, isolating the approximation and detailed parts of the image

Step4: Apply Arnold's Cat Map transformation to the secret image to add chaos, enhancing security by making the embedded data less predictable.

Step5: Convert the secret image to binary format and embed this binary data into the LL component.

Step6: Compute the SHA-256 hash of the secret image and embed this hash into the HH component.

Step7: Apply the inverse wavelet transform (IWT) to the modified frequency components to reconstruct the stego image.

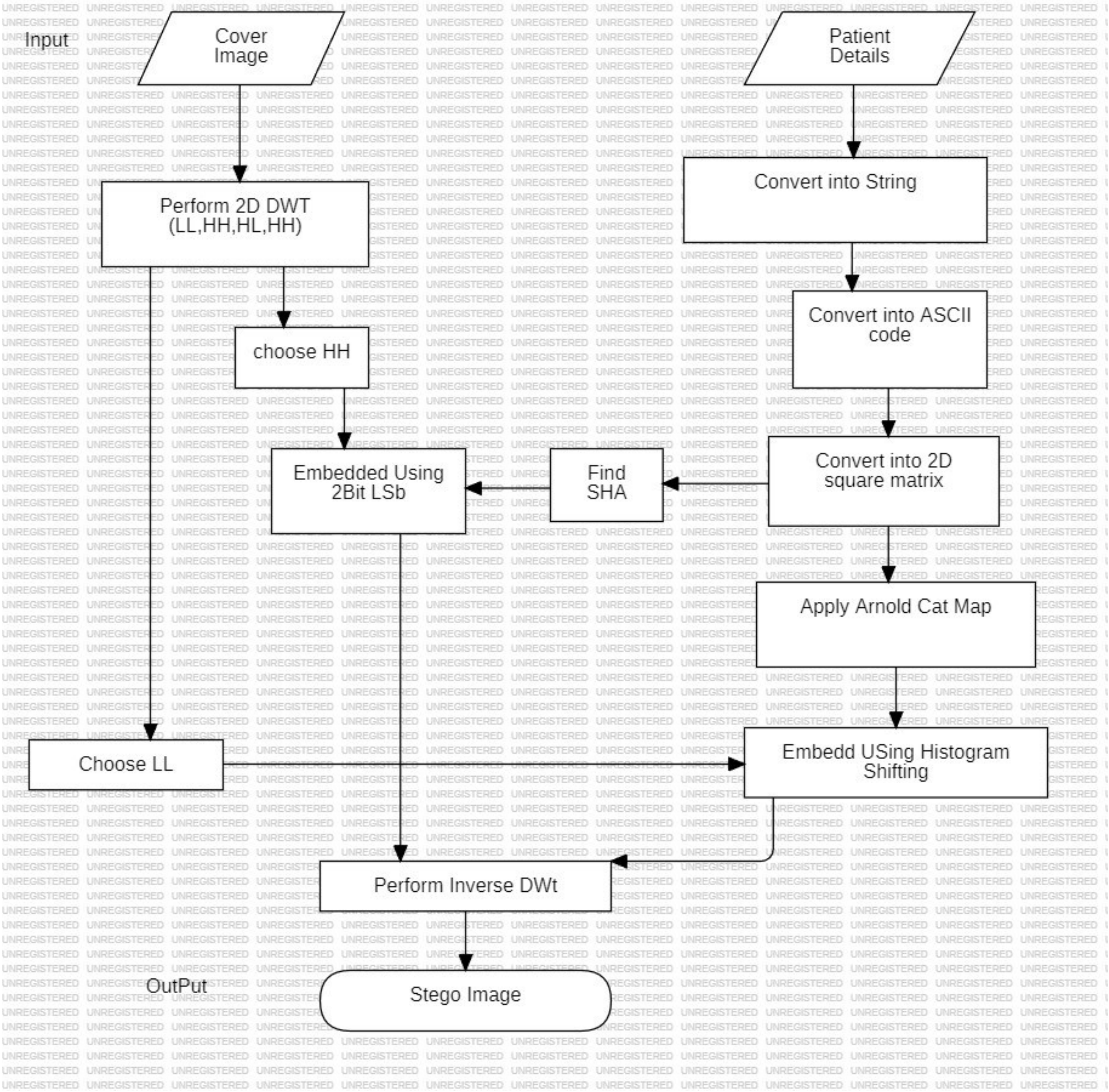


Fig:1 Flowchart for embedding process

3.1.2 Extraction Process

Extraction, the pivotal phase in steganography, unveils concealed information from an innocuous carrier medium. This clandestine art of retrieving hidden data involves a meticulous series of steps designed to decode and verify the integrity of the extracted content. As we embark on the journey of extraction, we delve into the depths of the stego image, employing sophisticated techniques such as Wavelet Transform and cryptographic hash verification. Guided by precision and ingenuity, this process not only reveals the covert message but also ensures its fidelity, affirming the trustworthiness of the extracted information.

Algorithm2: Extraction (stego,Bp)

Step1: Apply Forward Wavelet Transform (FWT) to the stego image to break it into frequency components.

Step2: Split the FWT result into low-frequency (LL) and high-frequency (HH) components.

Step3: Decode the binary message embedded within the LL component.

Step4: Retrieve the SHA-256 hash embedded within the HH component.

Step5: Convert the extracted binary message back into the secret image.

Step6: Reverse any Arnold's Cat Map transformation applied to the secret image, if needed.

Step7: Calculate the SHA-256 hash of the extracted secret image and compare it with the embedded hash for integrity verification.

Step 8: Extract patient info from extracted secret image.

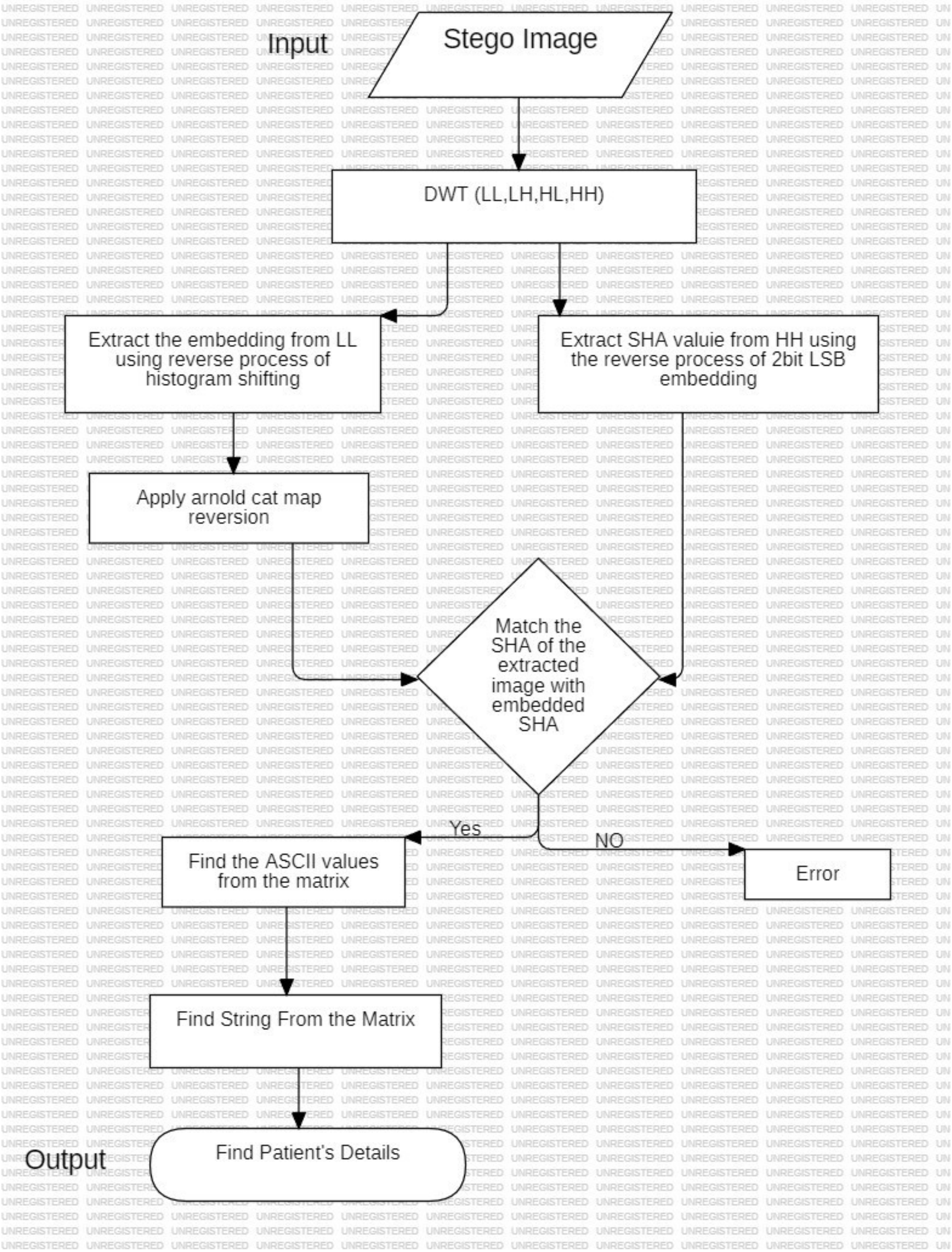

Input
Stego Image
DWT (LL,LH,HL,HH)
Extract the embedding from LL using reverse process of histogram shifting
Extract SHA valuie from HH using the reverse process of 2bit LSB embedding
Apply arnold cat map reversion
Match the SHA of the extracted image with embedded SHA
Yes
NO
Find the ASCII values from the matrix
Error
Find String From the Matrix
Output
Find Patient's Details

Fig:2 Flowchart for extraction process

Chapter 4: Experimental Results and Analysis

4.1 Dataset:

The ‘USC SIPI Image Dataset’, “Medical Image dataset” is taken into consideration in this work. All images of the SIPI datasets are as TIFF format [31], and the “Medical Image dataset” are taken from the Kaggle website [32].

4.1.1 USC SIPI Image Dataset:

Lena Image Airplane Image Barbara Image Baboon Image

Fig: 3 USC SIPI Image dataset

4.1.2 Medical Image Dataset:

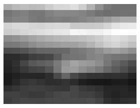
(a) (b) (C)

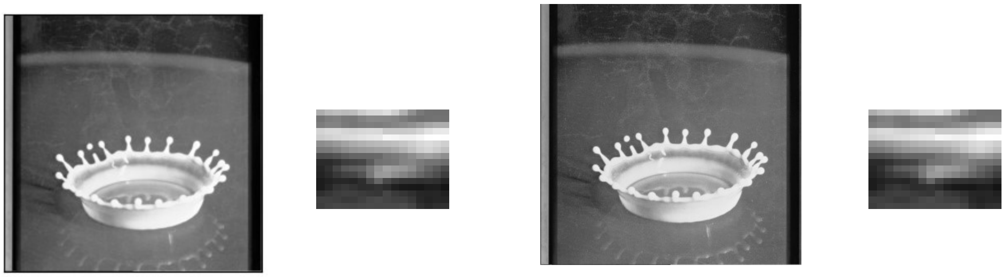
Fig: 4 Medical Image Dataset

4.2 Experiment Result

This method is using SIPI dataset and Medical image for experiment . For SIPI dataset we took a randomly generated 16 x 16 watermark image in grayscale.

Table 1: NCC & PSNR value of extracted watermark image without attack

Cover image	Watermark Image	MSE	PSNR	SSIM
21 level step wedge	 16 x 16 watermark gray -scale Image	0.077847	59.21841	0.999627
Airplane (F-16)		0.046234	61.48118	0.99961
Airplane		0.058697	60.44466	0.999497
APC		0.050457	61.10159	0.999602
boat.512		0.048534	61.27031	0.999765
Car and APCs		0.046646	61.44265	0.999776
Couple (NTSC test image)		0.045101	61.58893	0.999766
House		0.043468	61.74906	0.999709
Mandrill (a.k.a. Baboon)		0.045761	61.52584	0.999869
Sailboat on lake		0.047222	61.38935	0.999725
splash		0.047859	61.33115	0.999576
Tank		0.050522	61.09601	0.999851
Truck and APCs		0.044632	61.63434	0.999906
Truck		0.048691	61.25633	0.999742



(a) (b) (c) (d)

Fig: 5 Watermarking results without performing attack on splash.tiff image (a) Cover Image, (b) Watermark image, (c) Stego Image ,(d) Extracted Image

This method is also applied for medical image. Dataset for medical image we will take readings of some parameters for Pneumonia patients. The parameters are:

[“Name”, "Age", "Sex", "Smoking", "Fever”, "Body Temperature (Â°F)", "Cough", "Shortness of Breath" , "Chest Pain", "Diagnosis"]

The sample are:

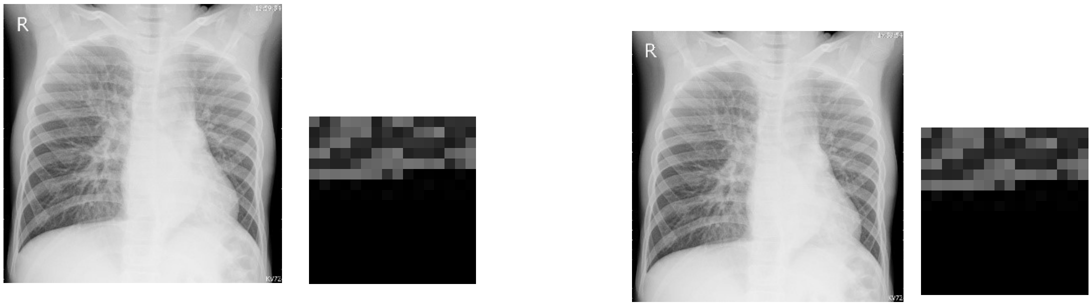
Name	**"Age"**	**"Sex"**	**"Smoking"**	**"Fever"**	**"Body Temperature (Â°F)"**	**"Cough"**	**"Shortness of Breath"**	**"Chest Pain"**	**"Diagnosis"**
John Doe	45	"Male"	"Yes"	"Yes"	101.3	"Yes"	"Yes"	"Yes"	"Bacterial Pneumonia"
Jane Smith	34	"Female"	"No"	"Yes"	100.5	"Yes"	"No"	"No"	"Viral Pneumonia"
Michael Brown	28	"Male"	"Yes"	"No"	98.7	"Yes"	"No"	"No"	"Chronic Bronchitis"

Emily Davis	67	"Female"	"No"	"Yes"	102.2	"Yes"	"Yes"	"Yes"	"Bacterial Pneumonia"

First, we will convert the medical data into String format. Then we will find the ASCII code for all Characters in the String then we will convert those integer values into squared 2D matrix. This 2d-matrix will watermark image.

Table 1: NCC & PSNR value of extracted watermark image in Medical Image

S.No.	CoverImage	SecretData	MSE	PSNR	SSIM
1	BACTERIA-2514247-0001	John Doe	0.011708	67.44588	0.999878
2	BACTERIA-4394295-0002	Jane Smith	0.010038	68.11417	0.999904
3	BACTERIA-5882850-0001	Michael Brown	0.009969	68.14439	0.999906
4	VIRUS-7520236-0003	Emily Davis	0.010606	67.87536	0.999887
5	VIRUS-9694192-0002	Chris Johnson	0.00992	68.16563	0.99991



(a) (b) (c) (d)

Fig: 6 Watermarking results without performing attack on Medical Image (a) Cover Image, (b)Watermark image, (c)Stego Image,(d) Retrieved Watermark

Conclusions:

In conclusion, our project has been dedicated to the development and assessment of robust image watermarking techniques customized for the unique demands of telemedicine. In the dynamic landscape of telemedicine, ensuring the secure transmission and confidentiality of medical images stands as a cornerstone for upholding patient privacy and data fidelity. While Singular Value Decomposition (SVD) wasn't directly employed, we extensively explored alternative methodologies, particularly leveraging techniques such as Discrete Wavelet Transform (DWT), histogram shifting, and Arnold Cat Map, for embedding imperceptible watermarks into medical images. Through rigorous experimentation and analysis, we've substantiated the effectiveness of these strategies in maintaining both the visual fidelity and diagnostic integrity of medical images, while bolstering their resilience against prevalent forms of cyber-attacks like compression, noise addition, and cropping. By meticulously refining these techniques and evaluating them using established metrics, we've endeavored to strike a delicate balance between imperceptibility and robustness, thereby offering viable solutions for fortifying the security of medical image transmission in telemedicine. In doing so, we aspire to instill trust among healthcare providers and patients, fostering a safer and more reliable telemedicine environment conducive to accurate diagnosis and improved healthcare outcomes.

Furthermore, our project has contributed valuable insights into the intricate balance between imperceptibility and robustness in image watermarking. We have considered various factors, including embedding capacity, computational complexity, and the potential degradation of visual quality, to optimize the performance of our techniques. By evaluating our methods using metrics such as Peak Signal-to-Noise Ratio (PSNR), we have gained a comprehensive understanding of their strengths and limitations.

As telemedicine continues to gain prominence in healthcare delivery, the significance of secure and reliable transmission of medical images cannot be overstated. Our research serves as a foundational step towards addressing this critical need by providing practical solutions for securing medical images in telemedicine environments. By ensuring the integrity and confidentiality of these images, we aim to foster trust among healthcare providers and patients alike, thereby facilitating accurate diagnosis and improving the overall quality of healthcare services in telemedicine settings.

References

1. Gary C. Kessler, Chet Hosmer, “An Overview of Steganography” , (2011)

2. J. Kour, D. Verma, “Steganography Techniques –A Review Paper” , International Journal of Emerging Research in Management &Technology., Vol. 3, Issue 5, pp. 132-135. (2014)

3. A. Cheddad, J. Condell, K. Curran, P. M. Kevitt, “Digital image steganography: Survey and analysis of current methods”, Volume 90, Issue 3, Pages 727-752. (2010)

4. Oleg O. Evsutin , Anna S. Melman , and Roman V. Meshcheryakov, “Digital steganography and watermarking for digital images: a review of current research directions”,in IEEE Access., Vol-8, Pages 166589 – 166611, DOI: 10.1109/ACCESS.2020.3022779. (2020)

5. Dr Cauvery N K, “Water Marking on Digital Image using Genetic Algorithm”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, Pages 323-331. (2011)
6. B. Li, J. He, J. Huang, Y. Q. Shi, “A Survey on Image Steganography and Steganalysis”, Journal of Information Hiding and Multimedia Signal Processing., Vol. 2, Issue 2, pp.142- 172. (2011).

7. Venkatraman, Ajith Abraham and M. Paprzycki, "Significance of steganography on data
security," International Conference on Information Technology: Coding and Computing,
2004. Proceedings. ITCC 2004., Las Vegas, NV, USA, pp. 347-351 Vol.2, doi: 10.1109/ITCC.2004.1286660. (2004)

8. Mustafa Muneeb Taher, ABD Rahim Bin HJ Ahmed, Rana Sami Hameed, Siti Salasiah Mokri, “A Literature Review of various Steganography Methods” in Journal of Theoretical and Applied Information Technology., Vol.100. No 5, pp. 1212-1227. (2022)

9. Mahbuba Begum and Mohammad Shorif Uddin, “Digital Image Watermarking Techniques: A Review”

10. Sumeet Kaur, Savina Bansal, R. K. Bansal, "Steganography and Classification of Image Steganography Techniques" in IEEE , pp.870-875

11. A. Pradhan, A. K. Sahu, G. Swain, and K. R. Sekhar, "Performance evaluation parameters of image steganography techniques," 2016 International Conference on Research Advances Page 65 of 68 in Integrated Navigation Systems (RAINS), Bangalore, India, pp. 1-8, doi: 10.1109/RAINS.2016.7764399. (2016)

12. A.Dixit, R.Dixit, "A Review on Digital Image Watermarking Techniques", published Online April 2017 in MECS, pp. 56-66, DOI: 10.5815/ijigsp.2017.04.07.(2017)

13. Nishant Madhukar Surse and Preetida Vinayakray-Jani, "A Comparative Study on Recent Image Steganography Techniques Based on DWT" presented at the IEEE WiSPNET 2017 conference. pp. 1308-1314. (2017)

14. Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography" in International Journal of Applied Science and Engineering 2006. 4, 3: 275-290 . (2006)

15. S. Kalman, D. Zheng, J. Zhao, W. J. Tam, and F. Speranza, "An Image Quality Evaluation Method Based on Digital Watermarking," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 1, pp. 98-105, doi: 10.1109/TCSVT.2006.887086. (2007)

16. Chuan Qin, Chin-Chen Chang, Fellow, IEEE, Ying-Hsuan Huang, and Li-Ting Liao, "An Inpainting-Assisted Reversible Steganographic Scheme Using a Histogram Shifting Mechanism", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, Vol. 23, No. 7, pp. 1109-1118. (2013)

17. Meghana, Umesh D R , "Image Steganography based on Histogram Shifting" in IJREAM, ISSN:2454-9150, Vol- 05, Issue- 02, pp. 654-657.(2019)

18. Yujie Jiaa , Zhaoxia Yina, Xinpeng Zhangb , Yonglong Luo, "Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting".(2019)

19. C. V. Kumar, V. Natarajan and Deepika Bhogadi, "High Capacity Reversible Data hiding based on histogram shifting for Medical Images", in International conference on Communication and Signal Processing, April 3-5, 2013, India , pp. 730-733. (2013)

20. Hiba Abdel-Nabi and Ali Al-Haj, "Medical Imaging Security Using Partial Encryption and Histogram Shifting Watermarking",published in 2017 8th International Conference on Information Technology (ICIT), pp. 802-807.(2017)

21. Li-Chin Huang, Lin-Yu Tseng , Min-Shiang Hwang, “A reversible data hiding method by histogram shifting in high quality medical images” in The Journal of Systems and Software, Vol- 86, Issue- 3, pp. 716-727, (2013). DOI: https://doi.org/10.1016/j.jss.2012.11.024

22. Chin-Chen Chang1 , Thai-Son Nguyen , and Chia-Chen Lin, “Reversible Image Hiding for High Image Quality based on Histogram Shifting and Local Complexity” in International Journal of Network Security, Vol.16, No.3, PP.208-220, May 2014

23. A. A. Karawia, “Medical image steganographic algorithm via modified LSB method and chaotic map”, in IET Image Processing WILEY, Vol-15 Isuue-11, pp. 2580-2590 (2021)

24. De Rosal I.M. Setiadi, Md. Fadhil, Eko Hari Rachmawanto, Christy Atika Sari, “Secure Reversible Data Hiding in the Medical Image using Histogram Shifting and RC4 Encryption” Published in 2019 International Seminar on Application for Technology of Information and Communication (iSemantic),pp.28-33, (2019). DOI:https://doi.org/10.1109/ISEMANTIC.2019.8884306

25. Wien Hong , Tung-Shou Chen ,Chih-Wei Shiu, “Reversible Data Hiding Based on Histogram Shifting of Prediction Errors” 2008 International Workshop on Education Technology and Training & 2008 International Workshop on Geoscience and Remote Sensing, pp. 578-581 (2008). DOI: 10.1109/ETTandGRS.2008.263

26. A. K. Sonaniya, Dr. Laxmi Singh , “HEALTHCARE IMAGE STENOGRAPHY BY GENETIC ALGORITHM BASED DWT COEFFICIENT AND HISTOGRAM SHIFTING”, in JOURNAL OF OPTOELECTRONICS LASER, Vol- 41, Issue 12, pp.61-73. (2022)

27. R. Rathna Krupa, “An Overview of Image Hiding Techniques in Image Processing”, in The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), Vol. 2, No. 2, pp. 30-34. (2014)

28. F. N. Thakkar, V. K. Srivastava, “A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications.” Multimed Tools Appl 76, 3669– 3697 (2017). https://doi.org/10.1007/s11042-016-3928-7

29. A. K. Singh, “Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image.” Multimed Tools Appl 78, 30523–30533 (2019). https://doi.org/10.1007/s11042-018-7115-x

30. A. Anand, A. K. Singh, “An improved DWT-SVD domain watermarking for medical information security”, Computer Communications Vol.152 pp.72–80, ISSN 0140-3664, (2020)

31. A. G. Weber, “The USC-SIPI Image Database: Version 6”, Ming Hsieh Department of Electrical Engineering Signal and Image Processing Institute. (2018)

32. https://www.kaggle.com/datasets/kmader/siim-medical-images