IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 12 June 2024, accepted 9 July 2024, date of publication 18 July 2024, date of current version 29 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3430546

RESEARCH ARTICLE

CrypticCare: A Strategic Approach to Telemedicine Security Using LSB and DCT Steganography for Enhancing the Patient Data Protection

RAMYASHREE[1,2], (Member, IEEE), P. S. VENUGOPALA[3], (Senior Member, IEEE), S. RAGHAVENDRA[1], (Senior Member, IEEE), AND B. ASHWINI[4], (Member, IEEE)

[1]Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, India
[2]NMAM Institute of Technology, NITTE (Deemed to be University), Nitte, Karnataka 574110, India
[3]Department of Artificial Intelligence and Data Science, NMAM Institute of Technology, NITTE (Deemed to be University), Nitte, Karnataka 574110, India
[4]Department of Information Science and Engineering, NITTE (Deemed to be University), NMAM Institute of Technology, Nitte, Karnataka 574110, India

Corresponding authors: S. Raghavendra (raghavendra.s@manipal.edu) and B. Ashwini (ashwinib@nitte.edu.in)

ABSTRACT Digital content, such as images, texts, and audio, are now easily accessible on the Internet in a digitalized manner that enables efficient storage and transmission. As information technology evolves concurrently, there has been more cases of cybercrime including data theft and data fabrication by other parties. A wide range of strategies and methods have been used to address these issues using steganography. Steganography is a technique used to prevent unauthorized access of sensitive data by hiding secret information inside digital media containers. This paper aims to investigate the challenges of safely embedding messages into medical images using two different steganographic techniques: Discrete Cosine Transform (DCT) and Least Significant Bit (LSB). An increasingly popular method for hiding sensitive data in the LSBs of pixel values, without causing any discernible deformation is LSB-based steganography. The process of Discrete Cosine Transform alters the structure of the image and embeds the data to enhance its robustness. The DCT and LSB steganography approaches were compared in this work based on the performance parameters. The performance of LSB and DCT methods can be measured by analyzing their SSIM, PSNR, and MSE values. After evaluating different techniques of data hiding in DICOM images, it was found that LSB steganography produces an SSIM value higher than DCT and shows better performance in terms of PSNR values. By observing the results of embedding text and PDF files in DICOM images, it was concluded that LSB steganography provides superior image quality compared to DCT steganography with a data capacity of 2.03 bpp.

INDEX TERMS Discrete cosine transform, least significant bit, steganography, healthcare, mean squared error, peak signal-to-noise ratio, structural similarity index.

I. INTRODUCTION

THE development of internet and the rise of multimedia communication have greatly accelerated data transfer, giving us quick access to information at our fingertips. Nevertheless, a disadvantage of these arrangements is the inadequate guarantee of data security and copyright protection. Many strategies, including steganography, cryptography, and watermarking, are being used to allay these worries. The increasing prevalence of illegal activities, including theft and data fabrication, underscores the critical need for heightened cybersecurity measures in tandem with the rapid advancements in information technology. The increasing significance of collecting and securely managing personal health information is a critical aspect of modern healthcare, as highlighted [1]. With advancements in technology, there

The associate editor coordinating the review of this manuscript and approving it for publication was Leandros Maglaras.

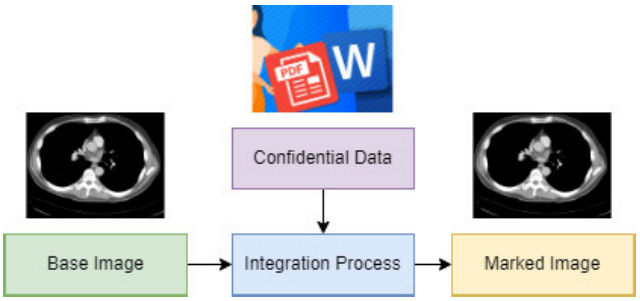

FIGURE 1. Integration process.

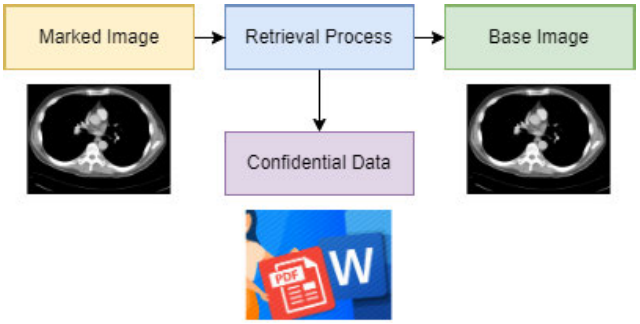

FIGURE 2. Retrieval process.

is a critical need for robust measures to ensure the security and privacy of personal health information (PHI). The significance of secure data processing techniques within the broader context of healthcare data management cannot be overstated, as they play a pivotal role in safeguarding sensitive medical data from unauthorized access, manipulation, or disclosure. As technology advances, it is crucial to acknowledge the increasing risks of unauthorized access and manipulation of sensitive information. This highlights the imperative nature of taking proactive measures to safeguard against such threats. In the comparision of flexibility among various techniques, digital watermarking emerged as the superior choice. Watermarking allows embedding an image, text, PDF, audio, or video within a multimedia entity to prevent misuse and protect copyright. Our study introduces a technique for imperceptible watermarking. Digital watermarking involves the amalgamation of a host or cover image with a secret image, constituting two distinct phases: embedding and extracting [2]. The embedding process, illustrated in Figure 1, results in the creation of a watermarked image by incorporating the secret image onto the original image through a designated algorithm [3].

In the extraction process shown in Figure 2, the secret image is retrieved from the watermarked image using the same algorithm used during the embedding phase [4].

The process of reconstruction is especially vital in domains like medical imaging, wherein the preservation of patient data confidentiality, CT scans, MRIs, X-rays, and other sensitive information is imperative. This is particularly relevant during data transmission over networks for diagnostic purposes in telemedicine [5]. The protection of patient information involves two primary methodologies.

- Medical reports are initially kept separate from patient identity to prevent unauthorized access to ensure patient confidentiality.
- Secondly, Deciphering the dataset becomes challenging due to extensive encryption, even if an attacker gains access to the reports.

This work utilizes two distinct steganographic methods, namely Discrete Cosine Transform (DCT) and Least Significant Bit (LSB), to ensure the security of medical information. The LSB technique is deemed highly effective owing to the substantial percentage extracted in experimental settings. Message retrieval is simple and error-free under ideal conditions [6]. However, it exhibits susceptibility to various types of noise, resulting in a substantial restoration of the message with a considerable number of erroneous bits. In medical imaging, the DCT is applied as a technique to represent image data in frequency components, allowing for efficient compression while preserving diagnostic information. By converting pixel values into frequency domain coefficients, DCT reduces redundant information in medical images, allowing for more efficient storage and transmission while maintaining diagnostic accuracy. In the intersection of DICOM anonymization [7] and steganography, our research underscores the imperative of safeguarding patient data within the medical imaging domain. Employing DICOM standards, we juxtapose anonymization methods—aimed at obfuscating personal identifiers to uphold privacy regulations—with steganographic techniques like LSB and DCT, which embed sensitive information into images, thus fortifying security. The technical rigor of maintaining image integrity while embedding data is scrutinized using metrics such as Structural Similarity Index(SSIM), Peak Signal-to-Noise Ratio(PSNR), and Mean Squared Error(MSE), ensuring the diagnostic value remains unaltered. This synergy of anonymization and steganography within DICOM images not only enhances the protection of patient information against unauthorized access but also preserves the data's clinical relevance, embodying a dual commitment to privacy and utility in the digital healthcare landscape. This study makes a significant contribution to the field of digital image security, specifically focusing on the safeguarding of medical information through steganographic techniques. The primary contributions of this work are outlined below:

1) This proposed work focuses on medical data in DICOM format and evaluates the effectiveness of DCT and LSB steganography techniques for securely embedding messages in medical images, ensuring that image quality remains uncompromised.
2) To evaluate the impact of steganographic techniques on image quality and robustness quantitatively,Comprehensive metrics such as SSIM, PSNR, and MSE are used.

3) Compares the effectiveness of DCT and LSB steganography for embedding messages in medical images.

The research proposes a hybrid methodology that combines LSB and DCT techniques to improve the robustness and quality of watermarking in medical images. The main focus of the proposed research is to investigate the effectiveness of steganographic techniques in maintaining image fidelity while securely embedding sensitive information. The main motivation of this work is to ensure the security of patient information by using a combined steganographic technique. Enhancing the robustness of LSB steganography against sophisticated attacks.

The contents are structured into sections, with Section II focusing on the study of Watermarking. Section III gives the overview related to the literature review. Sections IV and V comprehensively cover the proposed hybrid methodology and findings of the experiments. Section VI concludes the discussion by summarizing key insights.

II. FUNDAMENTAL ASPECTS OF WATERMARKING

Digital watermarking serves as a technique employed to embed sensitive information within data. This process is crucial for ensuring the legitimacy, authorship, and ownership of the content. Steganography is the practice of hiding information within other non-secret data, such as embedding secret messages in images without altering their appearance. Watermarking, on the other hand, involves embedding a visible or invisible marker within digital media to signify ownership or ensure authenticity. Both techniques are crucial in medical imaging for securing sensitive patient information while preserving the diagnostic quality of the images.The propoded study addresses the need for secure and high-quality data embedding in healthcare by evaluating Effectiveness of DCT and LSB steganography methods in medical images.

A. DIGITAL WATERMARKING

Digital watermarking technology protects copyright, maintains integrity, stops unauthorised copying, and tracks these digital assets by embedding particular information into digital products. The typical digital watermarking process involves three key stages: watermark generation, embedding, and detection [8]. Watermark generation is the initial stage where a unique identifier or pattern is created to be embedded in digital content, ensuring its traceability. Embedding involves the integration of the watermark into the digital content without compromising its integrity or quality. Detection is the final stage, focusing on identifying and extracting the embedded watermark to verify the authenticity or ownership of the digital asset. Considering theese three fundamentals Figure 3 illustrates the framework of digital watermarking systems.

TABLE 1. Overview of digital watermarking techniques.

Classification	Description
Visible Watermarking [14]	are often used to display copyright information or branding and act as a deterrent.
Invisible Watermarking [15]	is a Suitable method of covert tracking and authentication that is embedded within the content and imperceptible to the human eye.
Audio Watermarking [16]	Embeds information into audio signals while Preserving the perceived audio quality.
Image Watermarking [17]	Visual content can be protected from unauthorized use by applying images with proof of ownership or authenticity.
Video Watermarking [18]	Video Watermarking technology protects intellectual property in videos by embedding information directly into the video content.
Robust Watermarking [12]	This watermarking technique is specially designed to withstand intentional attacks and signal processing operations. It has been tested and proven to maintain its integrity in challenging conditions.
Fragile Watermarking [19]	It is highly effective for tamper detection and identifies any modification or even minor alterations.
Geometric Watermarking [20]	This technique alters the geometric features of an image in order to make it more resistant against cropping or resizing. Additionally, this feature may provide Protection against specific type of image manipulations.
Spread Spectrum Watermarking [21]	Spread Spectrum Watermarking spreads watermark information throughout the entire signal, which improves its robustness against various types of attacks.

B. ATTRIBUTES OF DIGITAL WATERMARKING

Digital watermarking technology encompasses four key characteristics: capacity, robustness, concealment and self-recovery [9].

1) **Capacity**: The system must articulate specific information about the embedded data to effectively address copyright concerns and ensure the protection of users' rights and interests [10].
2) **Robustness**: Indicates the system's ability to maintain the integrity and identification value of a digital watermarking, even after undergoing multiple signal processing steps [11].
3) **Concealment**: Emphasises the carrier's continued attentiveness even after the digital watermark is embedded. This guarantees that any damage to the digital result is modest and difficult to detect.
4) **Resilience**: The original image may become fragmented after processing and transformation of the watermark system [12]. However, the system can automatically recover the original image by retaining fragment data.

C. OVERVIEW OF DIGITAL WATERMARKING TECHNIQUES

The various classifications of watermarking techniques ranging from visible to invisible are explained in Table 1. It will gain insights into the strategies and benefits associated

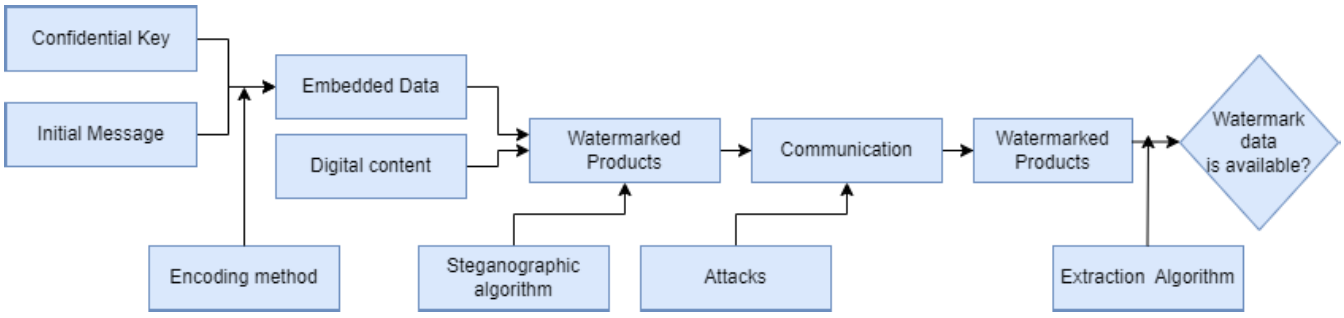

FIGURE 3. Foundational structure of digital watermarking system.

with different digital image watermarking methods.It is essential to understand these methodologies to safeguard digital products, ensure copyright compliance, and address the content protection requirement [13].

D. SECURITY ALGORITHMS FOR WATERMARKS

Algorithms for watermarking are essential tools for protecting digital content.

1) **LSB**: it is popular algorithm due to its simplicity and readability [13]. It maintains high clarity with negligible effects on loss of image quality. Its vulnerability to noise, clipping, and cropping, are its weaknesses.
2) **Texture Mapping**: Coding embeds data into the image's continuous random texture pattern.Although it performs well in texture areas, its applicability is limited, and human intervention is required [22].
3) **Patchwork approach**: It is a strong option due to its has high degree of resistance to various types of attacks, But its inability to conceal a large amount of information is a disadvantage [23].
4) **DCT**:In order to minimise the effect on the image appearance, watermarks are embedded into middle-frequency coefficients using the DCT. Unfortunately, this technique is not effective against scale attacks in block-wise DCT, because it removes invariance features and may even suppress higher frequency components.
5) **DWT**:The Discrete Wavelet Transform is a useful tool that accurately identifies both the time and space-frequency domains [24]. It performs exceptionally well against structural attacks, can tolerate cropping, and achieves a high compression ratio. Nevertheless, it has significant processing costs, takes a long time to compress, and may cause noise or blur at the margins of the image.

The choice of watermarking technique is determined by the specific requirements of digital material, including computing efficiency, robustness, and simplicity, with each algorithm offering unique benefits.

III. RELATED WORK

Least Significant Bit and Discrete Cosine Transform are destitute to the field of digital data hiding, allowing to embed and extract data into images easily and efficiently. The first technique exploits the least significant (rightmost) bit to change it and add the hidden data inside, exploiting the human eye's inability to perceive minor alterations. Courtesy of DCT, it is possible to represent an image in a specific way and hide vital data in its components. Without these methods, the use of steganography would have been limited to meaningless images, and embedding and extracted data would have suspected by functionality [25].

The LSB technique has been the subject of extensive research, with multiple studies exploring its effectiveness in concealing information within images. Mohan et al. [26] proposed a method that embeds both the message and its coded form into the carrier image using LSB embedding, achieving commendable performance results. This approach stands out for its enhanced security compared to other generic Steganography algorithms. Additionally, the method's robustness is strengthened by compressing a negative image, further improving its effectiveness across various file formats.Similarly the proposal of Salma et al. [27] highlights the need for continuous refinement and testing to ensure data safety, particularly in sensitive domains like medical image transmission using LSB.By advocating for a balanced approach that considers multiple factors, they emphasize the importance of addressing diverse requirements within different scenarios. Moreover, a novel technique has been proposed to enhance the capacity of the LSB method by embedding a large amount of data within a constrained space in the cover image [28]. This technique involves compressing the secret image and implanting it into the cover through LSB substitution, resulting in significant improvements in performance metrics such as PSNR. The findings of this study complement the efforts of [26] and [27] in advancing the capabilities of LSB-based steganography. Collectively, these studies underscore the significance of the LSB technique in data concealment and highlight the importance of continuous innovation and refinement to address evolving challenges in information security and confidentiality.

While LSB is commonly made use of for details hiding, its vulnerability to discovery motivates the expedition of options like DCT. DCT provides improved safety and security by spreading out information throughout regularity elements reducing LSB's vulnerability. This highlights the continuous search of even more durable methods in the middle of the progressing landscape of steganalysis as well as information safety and security.

In the world of digital content management as well as safety and security, Omar and Dakkak [29] and Agarwal et al. [30] both add considerable understandings right into methods essential for safeguarding digital assets. Reference [29] concentrate on watermark coding approaches using DCT, while Agarwal et al. [30] offer a relative evaluation of image security techniques, consisting of DCT-based techniques. Both studies underscore the pivotal role of DCT in ensuring data integrity and security, emphasizing its ability to withstand various forms of noise and reduce errors in message extraction. Building on this foundation, Garzia et al. [31] explore steganography in greater detail and emphasize how special it is for hiding communication in cover media. They suggest the steganographic strategy that effectively combines methods like DCT adjustments underscoring the adaptability and potential of DCT-based strategies for message security. This all-encompassing method of steganography not only highlights DCT's versatility but also emphasises how important it is for accomplishing covert communication goals while preserving data integrity.

Comprehensive investigation into the efficiancy of a combined approach utilizing the LSB and DCT techniques in steganography.The research conducted by Thejus and Namboothiri [32], Brindha and Maruthi [33], and Upreti et al. [34] explores the combination of DCT and LSB techniques for efficient information concealment and security improving. Reference [33]recommend a durable technique that integrates LSB along with DCT to install information within image coefficients accomplishing extraordinary recall precision and also credibility in steganalysis systems. To ensure data security and integrity during transmission over untrusted networks, Whereas [32] expanded this strategy by incorporating cryptographic methods and hash functions to ensuring data integrity and security during transmission over untrusted networks. Whereas [34] did the comparative analysis of DCT-based approaches in enhancing data security. Together, these studies highlight the LSB-DCT combined approach's potential to address evolving challenges in secure data transmission and privacy protection, offering insights into its effectiveness, applications, and future research directions. Table 2 presents a comparative analysis of the different watermarking approaches that have been implemented.

IV. PROPOSED METHODOLOGY

Implementing an imperceptible watermarking system is crucial for safeguarding intellectual property rights in the healthcare sector. The addition of digital watermarks to healthcare data modalities enables tracing and identifying the legal owner of copyrighted products.Just as SafeBio-Metrics [1] demonstrates the capability to maintain a secure data flow between client devices and the backend, our work focuses on embedding sensitive medical information within images while preserving their integrity. By evaluating real-world scenarios, both studies validate the effectiveness of their respective methodologies in addressing the challenges of secure data management. A comprehensive scrutiny of existing literature reveals the unequivocal predominance of MATLAB as the preferred software for executing a myriad of image and video watermarking. Considering the importance of security and the need for imperceptibility in copyright management, a robust watermarking model has been developed for the healthcare sector. The model employs a combination of LSB and DCT techniques for comprehensive fusion [43]. The model is meticulously designed to uphold a delicate equilibrium, ensuring the watermark's strength is sufficiently potent for copyright management and invisible to human observers. Crucially, the balance is maintained without compromising the integrity or usability of healthcare data. The system efficiently manages ownership and rights of watermarked healthcare data, including copyright tracking, verification, licensing mechanisms, and enforcement of copyright infringement. The foundational premise involves the cover image size should be eightfold greater than the embedded image. The model considers healthcare nuances, including privacy, data protection, regulatory compliance, and integration with existing information systems [44]. The effectiveness of the copyright management scheme in the healthcare landscape has been evaluated rigorously through performance analyses [45]. These evaluations have also helped to determine its impact on data quality and computational overhead. As a result, it has been affirmed that the scheme is capable of

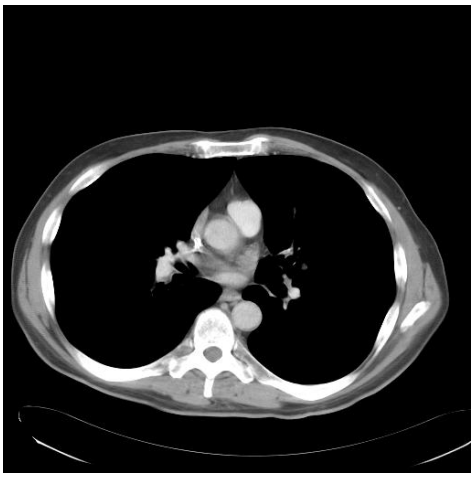

FIGURE 4. Sample DICOM Image.

TABLE 2. Comparative examination of author's approaches in watermarking.

Author	Methodology	Strength	Research Gap
M. Wang et al. [35]	Two-scale decomposition, Optimized base layer computation	Optimization for structure preservation: The Tikhonov regularization formulation for the base layer helps preserve structural information better.	Lack of very diverse images: The image datasets used are relatively small in size and diversity. Testing on larger and more heterogeneous datasets could be useful.
Sherif H. AbdEl-Haleem et al. [36]	DCT Phase Separation Scheme	Uses a fractional-order Lorenz chaotic system for watermark encryption. This increases security and key length compared to an integer order system. Comparative analysis shows improved PSNR over previous work. SSIM and robustness are competitive with minor tradeoffs.	Watermark capacity is small at bits. Using larger watermarks or multiple watermarks could be investigated.
Liang Tang et al. [37]	DCT and Laplacian Pyramid technique	The importance of DCT phase preservation is conclusively demonstrated.	Only PSNR is used as an objective measure of stego image quality.
Razika Souadek et al. [38]	DCT to transform image to frequency domain, Pixel Movement Function	Proposes a novel hybrid watermarking algorithm combining multiple transforms for improved performance. Achieves good imperceptibility with high PSNR values around 35dB.	Applications like copyright protection, authentication, tamper detection are not demonstrated.
Zhengxin Zhang et al. [39]	DCT with XOR based embedding	Novel algorithm using DC components in DCT domain. Provides improved robustness compared to spatial domain watermark. XOR-based embedding using DC relationships preserves image quality.	The watermark capacity is relatively low as only DC components are used for embedding. Methods to increase payload could be explored.
Wafaa Al-Chaab et al. [16]	Combination of compressive sensing, Moore-Penrose pseudo-inverse, and LSB steganography in a two-stage process.	The proposed hybrid system integrates encryption, compression, and steganography to enhance medical image confidentiality.	Need for comprehensive testing under diverse conditions, evaluating the system's robustness against potential attacks and variations in medical image types.
Surya Prakash et al. [40]	LSB substitution encoding, AES encryption, and secure transmission.	It offers a comprehensive solution to counter data leakage and information loss using data hiding technology.	Further refining the technique for enhanced security and accuracy, with particular emphasis on parameter specifications.
Estabraq et al. [41]	Dual-stage process encompassing steganography.	Contributes to digital security strategies aimed at safeguarding valuable data and copyright.	emerging trend in data hiding across diverse media, emphasizing payload, security, and imperceptibility
Sonam et al. [42]	LSBPM	A comprehensive exploration of the implications of modified cover images on steganographic security, with a focus on information transmission.	Significance of preprocessing methods for enhanced steganographic security, potential avenues for future research include a broader exploration of diverse preprocessing techniques and their varied impacts
Oluwakemi et al. [6]	LSB	Digital transformation of the medical field by focusing on medical data security through LSB Steganography Technique.	Integrating additional information hiding algorithms for augmented security, a potential research gap lies in the need for a comprehensive evaluation of the effectiveness and potential vulnerabilities.

providing secure and discreet copyright management within the healthcare industry. The following methodology was used for the evaluations:

A. ABOUT DATASET

Our research used a CT Medical Images dataset extracted from the Cancer Imaging Archive, consisting of a condensed

subset of DICOM type [46]. This subset comprises the middle slice of CT images, chosen based on the availability of valid age, modality, and contrast tags. The dataset includes a total of 475 series derived from 69 distinct patients, making it a valuable resource for research endeavors. It provides essential insights into medical imaging characteristics and aids in exploring pertinent clinical patterns. Figure 4 shows a visual representation of one of the images used in the research.

B. PRE-PROCESSING METHODS

The landscape of healthcare has been transformed by medical imaging, offering non-invasive modalities for diagnosing and monitoring diverse diseases and conditions. However, these images frequently contend with challenges such as noise, artifacts, inconsistencies, and diminished contrast, making it difficult to accurately interpret and analyze them. To surmount these hurdles, preprocessing techniques are employed to enhance the quality of medical images and extract relevant information for further analysis. Preprocessing methods, such as filtering, histogram equalization, and morphological operations, have traditionally been used in diagnostic imaging [47]. Although these techniques have some efficacy, they often rely on manually crafted features and may not fully utilize the complex patterns and structures inherent in medical images.

C. IDENTIFY SUITABLE WATERMARKING METHODS

The proposed method has successfully identified suitable watermarking techniques to tackle issues related to privacy and copyright.The proposed research invested on digital media within the context of the selected cover. The following presents illustrations of the LSB and DCT techniques.

1) TO INCORPORATE TEXTUAL INFORMATION AND RETRIEVE TEXTUAL DATA USING THE LSB METHOD

The LSB method is a digital image steganography technique used to conceal secret data within image files.LSB steganography involves concealing data within the least significant bits of a grayscale image and ensuring that it fits within the image capacity. During the embedding process, the data is first transformed to binary format and partitioned into individual bits. Specifically chosen bits are then embedded into the image data by manipulating the least significant bits, which represent the rightmost bits in a binary format causing minimal impact on the numerical value.The least significant bits are employed to conceal secret data since they have little effect on the overall visual look of the image, making changes unnoticeable to the human eye.

To increase data hiding using the LSB approach, it is recommended to choose a high-bit-depth carrier image, replace each pixel's LSB with hidden data bits, and use error-correction codes or encryption to ensure secure data transmission.

During the embedding process, the data is converted into binary form and inserted into the least significant bits (LSB) of each pixel using bitwise operations like 'OR' and 'AND'. The following steps need to be followed for steganographic embedding: Track the current position of both the image and secret data, and progress until all bits are embedded. Once the process is complete, save the altered image and document the method used to signify the end of secret data for future extraction. The algorithm for embedding is explained in Algorithm 1.

Algorithm 1 Embed Textual Data Using LSB

```
Initialize embeddedImage as a copy of originalImage
Initialize dataIdx to 1
for i in 1 to size(originalImage, 1) do
    for j in 1 to size(originalImage, 2) do
        Get the pixel value at embeddedImage(i, j)
        if dataIdx ≤ number of elements in data then
            Extract the LSB from pixelValue
            Store it in LSB
            Extract the data bit to embed (data(dataIdx))
            Combine lsb and the data bit
            Create the embeddedValue(EV)
            Update embeddedImage(i, j) with EV
            Increment dataIdx by 1
        else
            Break the inner loop
        end if
    end for
    if dataIdx > number of elements in data then
        Break the outer loop
    end if
end for
Return embeddedImage
```

To extract hidden data from a grayscale image altered with steganography, load the watermarked image and initialize variables to manage the extracted data. Mark the end of the hidden information and include details about the size of the embedded data. During the extraction process, the algorithm examines each pixel of the image and reads the LSB of its value. After reading the LSB, the process continues by appending it to the data buffer and moving on to the next pixel. This process continues until the desired amount of data is extracted, which is indicated by an end-of-data marker. It is crucial to keep track of the number of bits extracted and stop the process once the desired amount of data is obtained. If the extracted data is in binary, convert it to its original format. Once the desired data is successfully extracted, conclude the extraction process. The processing levels for extraction is explained in Algorithm 2.

In the extraction process, the watermarked image is loaded, and extraction variables are initialized. Each pixel of the image is examined, and the LSB of its value is read and appended to a data buffer. The extraction process continues until the end-of-data marker is found or the desired data

Algorithm 2 Retrieve Textual Data Using LSB

```
Initialize extractedData as an empty string
Initialize dataIdx to 1
for i in 1 to size(image, 1) do
    for j in 1 to size(image, 2) do
        Get the pixelValue at image(i, j)
        if dataIdx is less than or equal to numBits then
            Extract the LSB from pixelValue
            Store it in LSB
            Convert lsb to a character
            Append it to extractedData
            Increment dataIdx by 1
        else
            Break the inner loop
        end if
    end for
    if dataIdx is greater than numBits then
        Break the outer loop
    end if
end for
Return extracted data
```

amount is extracted, with the number of bits extracted being tracked. Once extraction is complete, the extracted data can be converted back to its original format if necessary, marking the conclusion of the extraction process.

The Figure 5 illustrates the process of embedding and retrieving textual data using the LSB method in steganography. It demonstrates the steps involved in concealing and extracting information within grayscale images.

2) TO INCORPORATE AND TO RETRIEVE PDF DATA THROUGH LSB

This approach explains how to insert PDF data into DICOM images using LSB replacement and extract it from the stego DICOM image. The embedding procedure is explained in Algorithm 3, begins by reading the input PDF file and DICOM image. The maximum embedding capacity of the DICOM image is then computed. If the size of the PDF data exceeds this limit, an error is generated. The PDF data is then translated to binary format, and the DICOM image is reconfigured to include the embedded data. Using LSB replacement, the PDF binary data is inserted into the DICOM image, which is then saved as a new file.Also evaluated to determine the quality of the embedded data.

The extraction method is explained in Algorithm 4. Initially reads the stego image to determine the number of bits to be extracted. The stego DICOM image is reshaped, and the least significant bits with contained PDF data are extracted. These extracted bits are then returned to their original format, and the resulting PDF data is saved in a new file.Figure 5 shows the LSB approach for embedding and retrieving PDF data in steganography.

Algorithm 3 Embedding PDF Into DICOM Using LSB Substitution

```
function embed PDF Into DICOM(pdfFileName, dicomFile Name)
    pdfData ← ReadBinaryData(pdfFileName)
    dicomImage ← ReadDICOMImage
    maxBytes ← calculateMaxCapacity(dicom)
    if size(pdfData) > maxBytes then
        raiseError("PDF file size exceeds.")
    end if
    pdfBinary ← convertToBinary(pdfData)
    numBits ← size(pdfBinary)
    dicomImage ← ReshapeDICOMImage
    embedBitsIntoDICOM(pdfBinary, dicomImage)
    stegoDicomFileName ← "stego_dicom_image.dcm"
    Save DICOMImage
    Display SuccessMessage
    calculate And DisplayPSNR_SSIM
end function
```

Algorithm 4 Extraction of PDF Into DICOM Using LSB Substitution

```
function extractPDFFromDICOM(stegoDicomFile Name)
    stegoDicomImage ← ReadDICOMImage
    numBits ← calculateNumBits
    stegoDicomImage ← reshapeDICOMImage
    extractedPDFBinary ← extractBitsFrom DICOM(stegoDicomImage, numBits)
    extractedPDFData ← convertBinaryToData
    outputFileName ← "extracted.pdf"
    DisplaySuccessMessage
end function
function calculateNumBits(image)
    return number of bits to be extracted from the image
end function
function extractBitFromDICOM(image,numBits )
    return the least significant bits from the image
end function
function convertBinaryToData(binaryData)
    return data converted from binary representation
end function
function writeDataToFile(data, fileName)
    write data to the file with fileName
end function
function displayExtractionTime
    display extraction time
end function
```

3) TO INCORPORATE AND RETRIEVE TEXTUAL INFORMATION THROUGH DCT

To perform steganography on a DICOM image, load the image from a file and read the secret message from a text file. It is not possible to directly embed a text message

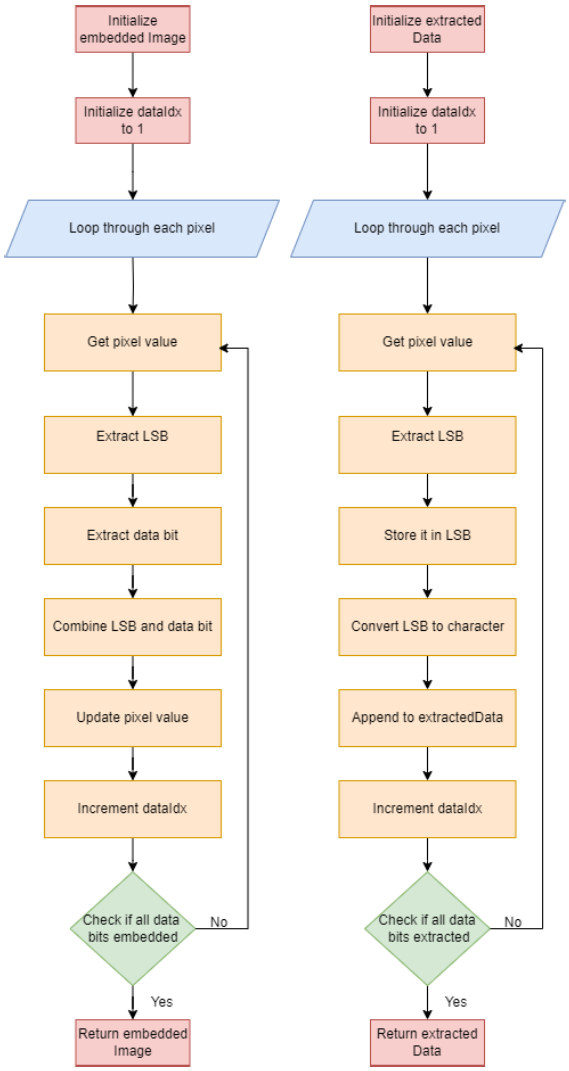

FIGURE 5. Flowchart for embedding and retrieving textual/PDF data using LSB.

Algorithm 5 Embed and Extract textual data through DCT

```
dicomImage ← ReadDICOMImage(DICOM image file path)
secretMessage ← ReadSecretMessage(Secret message text file path)
if SizeOf(secretMessage) > 10% × SizeOf(dicomImage) then
    Display "Error: File size is too large to embed in the DICOM image."
    Exit
end if
dct_coeff ← Apply2DDCT(dicomImage)
messageLength ← SizeOf(secretMessage)
for i ← 1 to SizeOf(dct_coeffs) do
    for j ← 1 to messageLength do
        pixel Value← GetPixel(dct_coeffs[i,j])

        if j ≤ messageLength then
            LSB ← ExtractLSB(pixelValue)
            LSB ← ExtractLSB(pixelValue)
            dataBit ← GetNextDataBit(secretMessage, j)
            embeddedValue ← Combine Bits(LSB, data)
            dct_coeffs[i, j] ← embeddedValue
        else
            Break                          ▷ Exit inner loop
        end if
    end for
    if j > messageLength then
        Break                              ▷ Exit outer loop
    end if
end for
embeddedImage ←ApplyInverseDCT(dct_coeffs)
Save embeddedImageas"stego.dcm"
ExtractMessage(dct_coeffs, messageLength)
extractedText ← ConvertToText(extractedMessage)
Save extractedText to a text file
```

into an image so the text message is converted into binary data. Apply a 2D DCT on the DICOM image to obtain DCT coefficients. Embed the binary message data into DCT coefficients by replacing the lowest frequency coefficients with message bits. Revert the stegonography DICOM image to its original form by applying the inverse 2D DCT.Retrieve DCT coefficients by applying 2D DCT to stego DICOM image for message extraction. Extract the binary data from the lowest frequency DCT coefficients and use it to retrieve a secret message hidden within a DICOM image.The process of embedding and extracting data is explained in Algorithm 5.

The Figure 6 visually represents these steps, with symbols and arrows illustrating the flow of the process. Each step is labeled and connected, providing a clear and concise representation of the workflow involved in incorporating and retrieving textual information through DCT for steganography in DICOM images.

4) TO INCORPORATE AND RETRIEVE PDF INFORMATION THROUGH DCT

The PDF files of different size are embedded into a DICOM image one at a time.The image name is predefined by the dataset provider as ID_0000_AGE_0060_CONTRAST_1_CT, using DCT.

The following procedure is executed by the code: It reads both a PDF file and an original DICOM image, converts the PDF data into binary format, and embeds it within the DCT coefficients of the DICOM image. The resulting stego DICOM image is saved as stego_dicom_image.dcm. Additionally, the code extracts the embedded PDF data from the stego DICOM image and saves it as extracted _pdf_from_dicom.pdf. Finally, the code performs a quantitative assessment to evaluate the fidelity of the stego DICOM image compared to the original DICOM image. This procedure is shown in Algorithm 6 and Algorithm 7.

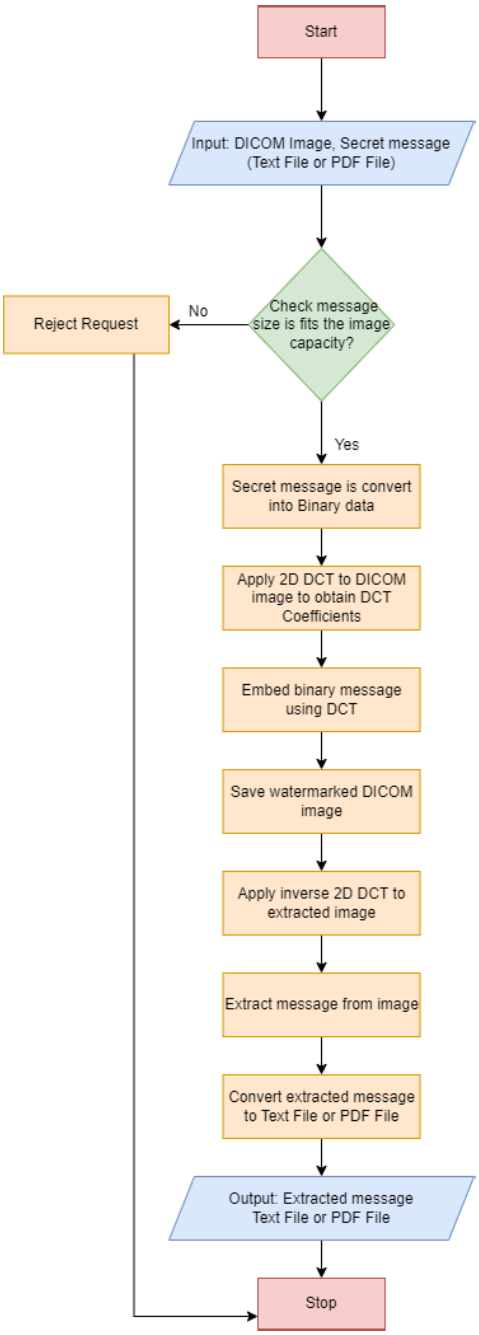

FIGURE 6. Flowchart for embedding and retrieving textual/PDF data using DCT.

Figure 6 depicts the workflow for incorporating and retrieving PDF data information in DICOM images using DCT for steganography.

D. TO ASSESS THE DATA FOR THE WATERMARK AND THE COVER IMAGE

The comprehensive evaluation of watermarking techniques using various parameters. The primary focus of this study is on Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM) metrics and Mean Squared Error (MSE), which play a crucial role in determining the effectiveness of the proposed mode in terms of quality.

Algorithm 6 Embedding PDF Into DICOM Using DCT

```
function EmbedPDFIntoDICOM(pdfFileName, dicomFileName, outputFileName)
    pdfData ← ReadPDFFile
    dicomImage ← ReadDICOMImage
    pdfBinary ← ConvertToBinarysize(pdfData)
    dicomImageDCT ← Apply2DDCT
     DCT_flat ← FlattenDCTCoefficients
     DCT_flat ← EmbedPDFData
     DCT_reshape ← ReshapeDCTCoefficients
     StegoDicomImage ← PerformInverseDCT
    Save StegoDICOMImage
    Display "PDF file embedded successfully and saved in the DICOM image"
end function
```

Algorithm 7 Extraction of PDF From DICOM Using DCT

```
function ExtractPDFFromDICOM(stegoDicom, outputFile)
    stegoDicomImage ← ReadDICOMImage
    stegoDicomImageDCT ← Apply2DDCT
     DCT_flat ← FlattenDCTCoefficients
     PDF Binary ← Extract PDF Data(DCT_flat)
    extractedPDFData ← ConvertToUint8
    Display "PDF file extracted successfully and saved"
end function
```

1) **PSNR**:The parameter metric PSNR is used to measure the peak value of the original image, indicating its quality level. A higher PSNR indicates better image quality, with images possessing greater clarity and fidelity exhibiting higher values. On the other hand, images with high PSNR may have increased levels of disturbance or noise [48]. The PSNR calculation is expressed by Equation 1, where 'L' represents the highest intensity value within the image. This mathematical representation enables the quantitative evaluation of image quality based on the peak signal-to-noise ratio.

$$PSNR = 10 * \log_{10}(L^2/MSE) \tag{1}$$

2) **SSIM**:The Structural Similarity Index (SSIM) is a metric used to measure the similarity between two images. It provides a comprehensive evaluation that goes beyond just comparing pixels. SSIM considers factors such as luminance, contrast, and structure, and produces a score between -1 and 1 [49]. A higher SSIM score indicates greater similarity between the original and stego images and takes into account a holistic assessment of structural information. The formula used

to calculate SSIM is given by Equation 2.

$$\text{SSIM}(a, b) = \frac{(2\mu_a\mu_b + P_1) \cdot (2\sigma_{ab} + P_2)}{(\mu_a^2 + \mu_b^2 + P_1) \cdot (\sigma_a^2 + \sigma_b^2 + P_2)}$$

where:

μ_a and μ_b are the means of images a and b.

σ_a^2 and σ_b^2 are the variances of images a and b.

σ_{ab} is the covariance of a and b.

P_1 and P_2 are constants with weak denominator. (2)

3) **MSE**: The Mean Squared Error (MSE) is a metric that measures the average squared difference between the predicted values and the actual values [50]. It is commonly used to evaluate the accuracy of a predictive model. The formula for calculating MSE is given as Equation 3.

$$MSE = \frac{1}{j}\sum_{k=1}^{j}(c_k - \hat{c}_k)^2 \tag{3}$$

where:

j represents the sample size,

c_k represents the actual value of k-th observation,

$\hat{c}_k$ signifies the predicted value of k-th observation.

4) **Bits Per Pixel (BPP)**:In steganographic research, the load aspect is a critical metric that quantifies the capacity of the cover image to conceal secret data. This capacity is measured in Bits Per Pixel (BPP), which directly correlates to the amount of information that can be embedded within each pixel of the image. To maintain the balance between data load and image quality, it is essential to determine the maximum BPP that ensures the cover image's alterations remain undetectable to the human eye. This threshold of imperceptibility is crucial for effective steganography, as it allows for the optimal amount of data to be embedded without alerting observers to the presence of hidden information [51].
The BPP formula employed in this study is derived from the following equation:

$$BPP = \frac{\text{Total Number of Pixels in the Cover Image}}{\text{Total Bits of Embedded Data}} \tag{4}$$

The formula 4, serves as a guideline to ascertain the upper limit of data that can be embedded within a cover image while preserving its visual fidelity. By adhering to this limit, researchers can ensure that the stego image remains indistinguishable from the original, thereby upholding the imperceptibility aspect of steganography.

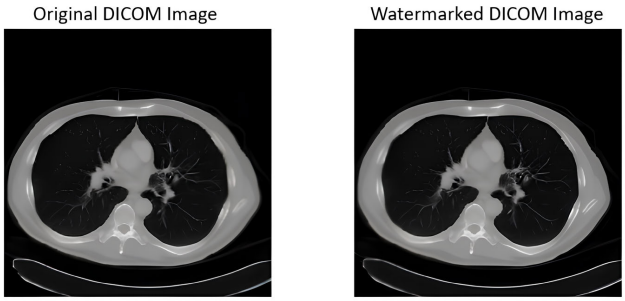

FIGURE 7. Concealing data without modifying visual appearance after adding watermarking.

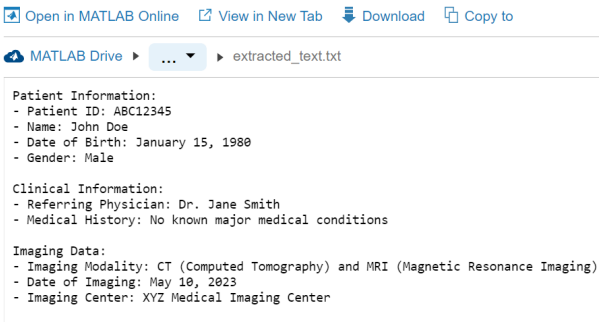

FIGURE 8. Extraction of text data from the watermarked image without any modification.

V. EXPERIMENT AND RESULTS

The experiment was carried out with the help of MATLAB R2023a and a CT medical images dataset was used as the input. The dataset comprises a total of 475 images for evaluation [46]. It was conducted on a system equipped with Windows 11 operating system, an Intel(R) Core(TM) i5 processor, and 8.00 GB RAM. The detailed procedure for embedding information extracted from a payload text and PDF file into an image. This embedding and extraction process is executed using both the LSB and DCT techniques.

A. EMBEDDING AND EXTRACTING TEXT DATA ANALYSIS USING LSB

It has been observed that the LSB approach has a high success rate in extracting messages, as shown in Figure 7. This method is error-free under ideal conditions. Figure 8 illustrates that the extracted text aligns consistently with the original text. This alignment confirms the accuracy of the text extraction process and affirms the robustness of the employed technique, preserving the integrity of concealed information.

Table 3 shows several text files embedded in an original image ID_0000_AGE_0060_CONTRAST_1_CT of size 516KB with varying file sizes ranging from 1KB to 1000 KB.The text files can be embedded in an image and extracted during retrieval. Insertion time ranges from 0.0138 to 0.9937 seconds, while extraction time ranges from 0.0043 to 0.2256 seconds.

TABLE 3. Results of embedding and retrieval of different text file through LSB.

Embedded Text File	Text File Size	Insertion Time (sec)	Extraction Time (sec)
Test1.txt	1KB	0.0138	0.0043
Test2.txt	2KB	0.062	0.0263
Test3.txt	5KB	0.1708	0.0370
Test4.txt	200KB	0.9894	0.220
Test5.txt	500KB	0.9917	0.2223
Test6.txt	1000KB	0.9937	0.2256

TABLE 4. Observations of PSNR and SSIM for the text file using LSB.

Embedded Text File	Text File Size	PSNR Value (dB)	SSIM Value
Test1.txt	1KB	87.63	1.0
Test2.txt	2KB	81.13	1.0
Test3.txt	5KB	76.88	1.0
Test4.txt	200KB	68.92	1.0
Test5.txt	500KB	67.55	1.0
Test6.txt	1000KB	65.32	1.0

PSNR values indicate the quality of an image, with higher values indicating better quality. For example, a PSNR value of 87.63 for the smallest file indicates a better image quality.SSIM values are reported, with all cases having a perfect SSIM value of 1.0. Table 4 shows that the value consistently remains at 1.0 across all cases, which suggests that the structural integrity of the image is maintained regardless of the size of the embedded text file. The proposed embedding technique maintains high image quality and consistent structural similarity during the concealment and extraction of various text files within the original image.

B. EMBEDDING AND EXTRACTING PDF FILE ANALYSIS USING LSB

Figure 9 shows the process of embedding and extracting PDF files into an initial image labeled as "ID_0000_AGE_0060_CONTRAST_1_CTT." The original size of the image is 516KB, and the embedded PDF files have varying sizes. The duration of the embedding process varies, ranging from 0.285 to 0.975 seconds. The time taken to retrieve the embedded PDF files ranges from 0.01 to 0.0312.

Elevated PSNR values indicate high image quality, such as 88.58 for the smallest file. The SSIM values show that there is no significant impact on the structural similarity of the image when embedded text is extracted In all cases, the SSIM value remains 1.0, indicating that the image structure remains unchanged even with the embedded text. Figure 10 provides a clear illustration of the different embedded PDF files and their corresponding sizes on the x-axis label, "Embedded Pdf File and Size." The y-axis and y2-axis labels show the PSNR and SSIM values associated with the embedded PDF files, respectively. This consistent outcome suggests that the experimental data can be well understood and interpreted.

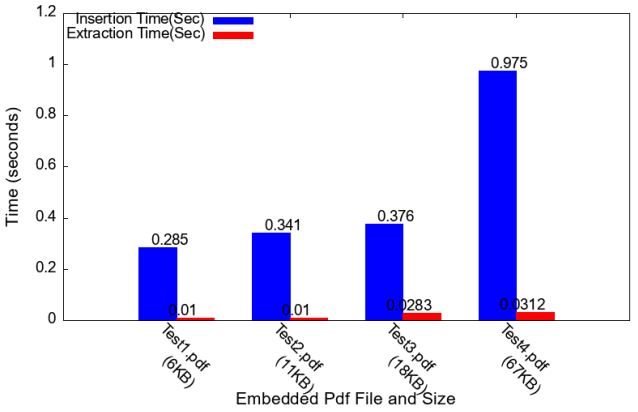

FIGURE 9. Observation for insertion and extraction of pdf using LSB.

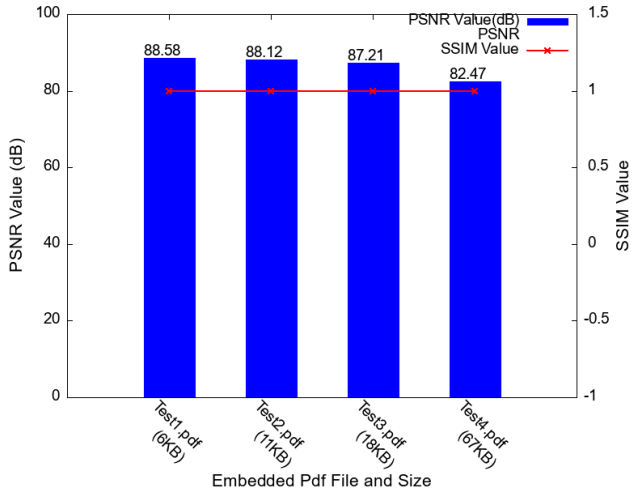

FIGURE 10. Observations of PSNR and SSIM for the PDF file using LSB.

C. EMBEDDING AND EXTRACTING TEXT DATA ANALYSIS USING DCT

The experiment was extended to incorporate the DCT as an alternative technique for embedding text data into images. The Discrete Cosine Transform is a mathematical transformation widely employed in signal processing and image compression. The DCT technique operates in the frequency domain, which makes it different from the LSB technique in terms of data embedding. In a recent experiment, text data was embedded into DICOM images using DCT, and the results were recorded. The duration for inserting and extracting data (in seconds) was recorded for various text files and presented Table 5.

Additionally, the experiment measures the quality of the images using PSNR and SSIM metrics.These metrics are reported in decibels and normalized values, respectively. The PSNR values ranged from 84.32 dB for the smallest file(1KB) to 62.37 dB for the largest value(500KB file), indicating varying levels of image fidelity. The extraction process may have difficulties in maintaining structural similarity as

TABLE 5. Results of embedding and retrieval of different text file through DCT.

Embedded Text File	Text File Size	Insertion Time (sec)	Extraction Time (sec)
Test1.txt	1KB	0.0142	0.0034
Test2.txt	2KB	0.168	0.0272
Test3.txt	5KB	0.371	0.0465
Test4.txt	200KB	0.794	0.3234
Test5.txt	500KB	0.917	0.456

TABLE 6. Observations of PSNR and SSIM for the text file using DCT.

Embedded Text File	Text File Size	PSNR Value (dB)	SSIM Value
Test1.txt	1KB	84.32	0.999
Test2.txt	2KB	79.13	0.999
Test3.txt	5KB	76.17	0.999
Test4.txt	200KB	65.28	0.989
Test5.txt	500KB	62.37	0.989

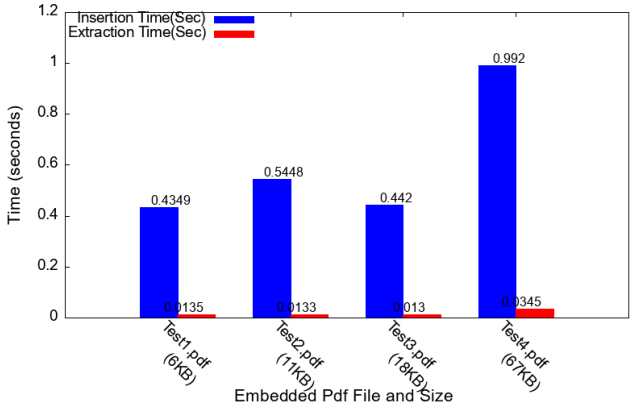

FIGURE 11. Observation of PDF Embedding and Extracting using DCT.

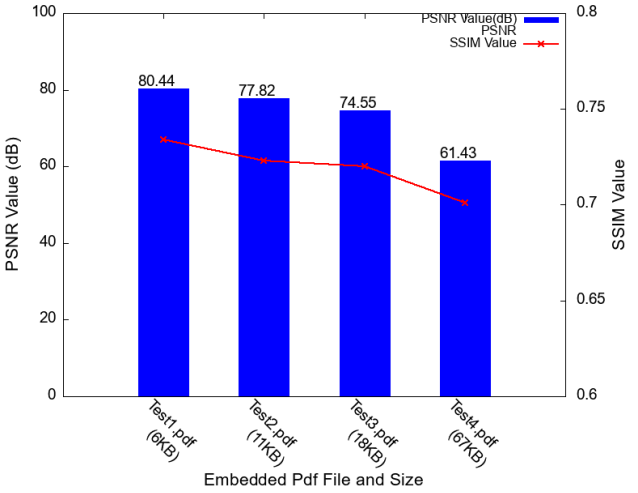

FIGURE 12. Observation of PSNR and SSIM for PDF file using DCT.

TABLE 7. Comparison of MSE-LSB and MSE-DCT for different text files.

Text File	Text File Size	MSE-LSB	MSE-DCT
Test1.txt	1KB	0.0064	0.072
Test2.txt	2KB	0.0283	0.094
Test3.txt	5KB	0.0755	0.12
Test4.txt	200KB	0.423	1.78
Test5.txt	500KB	0.544	2.99

TABLE 8. Comparison of MSE-LSB and MSE-DCT for different pdf files.

Pdf File	Pdf File Size	MSE-LSB	MSE-DCT
Test1.pdf	6KB	0.0075	0.091
Test2.pdf	11KB	0.0483	0.098
Test3.pdf	18KB	0.212	1.821
Test4.pdf	67KB	0.444	3.48

indicated by consistently low SSIM values compared to LSB. Table 6 image quality metrics for the DCT technique used for text embedding in DICOM images.

D. EMBEDDING AND EXTRACTING PDF FILE ANALYSIS USING DCT

In this experiment, several PDF files were embedded into a cover image named "ID_0000_AGE_0060_CONTRAST_1_CT" with a size of 516KB. The sizes of the embedded PDF files vary from 6KB to 67KB. The insertion time for each PDF ranges from 0.4349 to 0.992 seconds. The extraction time for each PDF is between 0.0135 and 0.0345 seconds, as shown in Figure 11.

The quality of the embedded images has been evaluated by PSNR values, which range from 61.43 to 80.44 dB. The SSIM values were measured to show similarity between original and embedded images. SSIM values ranges from 0.701 to 0.734, where higher values indicate greater similarity as shown in the Figure 12.

Table 7 compares the Mean Squared Error (MSE) for different text files, using both the LSB and DCT techniques for image steganography.

- The MSE values of LSB generally increase with the size of the text file, indicating a higher discrepancy between the original and steganographic images as the text size grows.
- MSE values of DCT increase with text file size, indicating a similar relationship
- For all text file sizes, the Mean Squared Error (MSE) values of LSB steganography are lower compared to DCT steganography. This indicates that the Discrete Cosine Transform-based method incurs a higher distortion in the steganographic images.

The above mentioned Observations of MSE are clearly represented in Figure 13

Table 8 presents a comparison of the MSE of different PDF files using LSB and DCT techniques.

- The MSE values of LSB and DCT increase as the size of the PDF file increases. This indicates a higher level of distortion in steganographic images with larger PDFs.
- The MSE values of LSB are generally smaller compared to the corresponding MSE values of DCT for all PDF file sizes, suggesting that LSB-based steganography

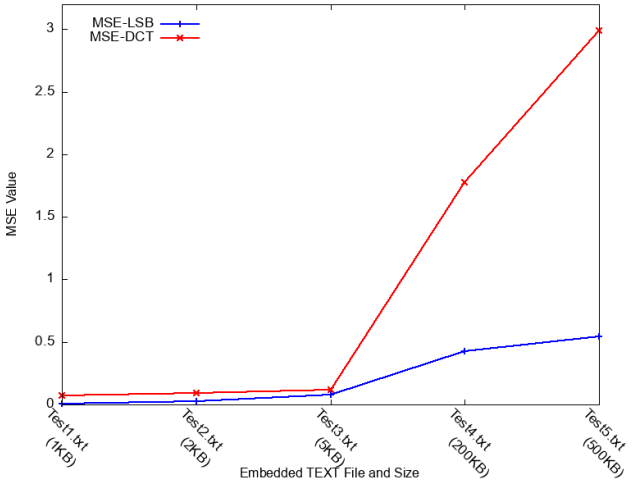

FIGURE 13. MSE Value comparison for Text File using LSB and DCT Technique.

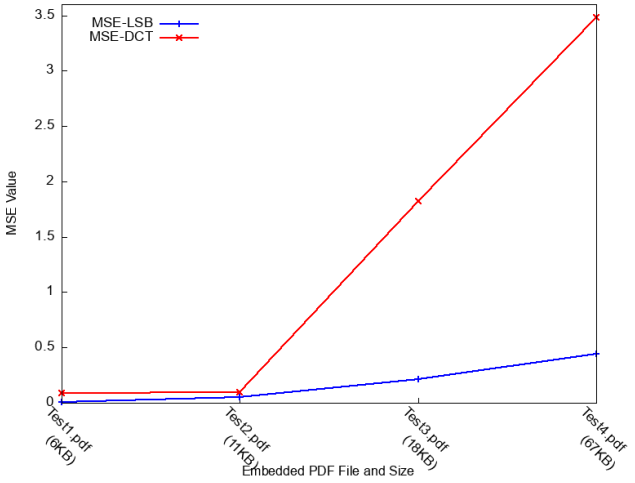

FIGURE 14. MSE Value comparision for PDF File using LSB and DCT Technique.

incurs less distortion than the DCT-based method in this context.

- The MSE values of LSB and DCT in Test4.pdf show the largest increase in distortion compared to other PDFs. This indicates a potentially more challenging scenario for steganalysis.

The observations regarding MSE mentioned earlier are visually represented in Figure 14.

The MSE analysis of pdf and text file is discussed below:The PDF file named ''Test4.pdf'' with a size of 67KB exhibits significantly higher MSE values of 3.48 using DCT technique, while it is only 0.444 in the case of LSB. Similarly, the text file named ''Test5.txt'' with a size of 500KB shows notably higher MSE values of 2.99 using DCT technique, whereas the MSE value is 0.544 in the case of LSB.

Table 9 provides a comparative overview of different watermarking methods along with their associated

TABLE 9. Comparison of PSNR, MSE,SSIM and bpp measurement results.

Authors Details	Watermarking Method	PSNR(dB)	MSE	SSIM	bpp
Proposed Work	**LSB, DCT**	**87.63**	**0.0064**	**1.0**	**2.03**
Kaur et al. [52]	LSB	75.32	0.002	0.999	4.515
Garzia et al. [31]	LSB, DCT	47.8962	1.0646	1.0	-
Amishi et al. [53]	Integer wavelet Transform	43.2753	-	0.9672	1.86
Puteri et al. [55]	LSB	43	4.027	-	2.67
Bharathkumar et al. [56]	DCT	34.16	6.45	–	4.50
Ismail et al. [57]	CNN	37	-	0.98	8
Li Li et al. [58]	LSB	45	-	-	6.3
Akash Agarwal et al. [40]	DCT, LSB and XOR	63.1844	0.0312	-	-
Bayu et al. [54]	LSB, DCT	83.728	0.059	-	-

performance metrics. Our proposed method combines LSB and DCT techniques and achieves superior results with a PSNR of 87.63 dB, low MSE of 0.0064,perfect SSIM score of 1.0 and reasonable bpp of 2.03. Kaur and Singh [52]'s method employs LSB, has a slightly lower PSNR of 75.32 dB,MSE of 0.002, SSIM of 0.999 and Little high bpp of 4.515. Garzia et al. [31]'s works on LSB and DCT methods which resulted in a lower PSNR value of 47.8962 dB and higher MSE value of 1.0646. They achieved a perfect SSIM score of 1.0. Kapadia and Nithyanandam et al. [53]'s method utilizes the Integer Wavelet Transform for watermarking. The PSNR is 43.2753 dB, which indicates relatively good,The SSIM of 0.9672 and the bpp value of 1.86 indicates that approximately 1.86 bits of information are embedded per pixel in the image. Halboos and Albakry [41]'s approach, combining DCT, LSB, and XOR resulting in a a significant decrease in PSNR to 63.1844 dB,moderate MSE 0.031235 and SSIM not used for evaluation. Finally, Wijaya et al. [54]'s method employs LSB and DCT, has a slightly lower PSNR of 83.728 dB and higher MSE of 0.0592. SSIM is not specified. This comparison highlights the effectiveness of our proposed hybrid technique that combines LSB and DCT which produces high-quality watermarking results compared to the other methods. Additionally, proposed works bpp value of 2.03 is moderate, indicating a good balance between image quality and the amount of data embedded per pixel. Therefore, it can be concluded that the proposed method outperforms the others in terms of watermarking quality.

Table 10 presents a comparison of different watermarking techniques, including the proposed approach that utilizes LSB and DCT, with four other studies. The proposed LSB-DCT watermarking method leverages the high capacity of LSB embedding with the robustness of DCT against

TABLE 10. Comparison of watermarking methods with proposed work.

Authors	Watermarking Method	Robustness Against Attacks	Practical Viability	Main Application Focus	Invisibility	Capacity	PSNR	MSE
Proposed Work	**LSB, DCT**	**High**	**Yes (Efficient and Reliable)**	**Image Steganography and Steganalysis**	**High**	**High**	**High**	**Low**
Omar et al. [29]	DCT&AEW	Resistance to noise, low errors	Yes (Effectiveness with Side Information)	Digital Watermarking for Content Identification	Medium	High	Medium	Medium
Anumol et al. [32]	Hybrid (SHA256, DCT-IDCT, LSB)	Threat-free transfer, low MSE	Yes (Efficient and Error-Free)	Secure Transfer of Medical Images	High	Medium	High	Low
Joseph et al. [4]	DWT & DCT	Imperceptibility & Robustness	Yes (Improved Quality)	Digital Watermarking for Multimedia Document Protection	High	Medium	Low	High
Bayu et al. [54]	LSB, DCT	Moderate	Moderate	Information Hiding in Images for General Applications	Low	Medium	Low	Medium

image processing attacks. This dual approach allows for a secure and resilient watermarking system that maintains the visual quality of the host image while ensuring the watermark's persistence against various forms of manipulation. The proposed method is described as efficient and reliable, suggesting that it has been tested in practical scenarios and has shown to be a feasible solution for real-world applications. Also specifically tailored for steganography and steganalysis, indicating a specialized application in the field of data hiding and detection. The selective embedding strategy optimizes the placement of the watermark, utilizing the strengths of both spatial and frequency domains to enhance the overall performance of the watermarking process and is a distinctive feature of our method.

The Table 11 presents a comparative analysis of the robustness of a watermarking method when subjected to various image attacks. Initially, the method exhibits perfect robustness, with all 1905 characters being correctly extracted, resulting in a 100% match. Zero Attack simulates a scenario where the LSBs of the pixel values might be set to zero, potentially due to a lossy transmission or compression. The method still manages to correctly extract 82.36% of the characters, suggesting that while there is some degradation in performance, the majority of the data remains intact.

Salt and Pepper Attack introduces sharp, sudden disturbances in the image, akin to black and white specks. It represents a more challenging condition for watermark extraction. The method's ability to correctly extract 82.78% of the characters indicates a slightly better resilience compared to the Zero Attack, possibly due to the method's robustness against high-frequency noise.

Gaussian Noise Attack statistical noise having a probability density function equal to that of the normal distribution, which is also known as Gaussian distribution. This attack affects the watermarking method more significantly, reducing the correct character extraction rate to 81.28%. This suggests that the method is somewhat less effective against this type of noise, which affects all pixels in a more uniform manner.

Speckle Noise Attack granular interference that inherently exists in and degrades the quality of the active radar, synthetic aperture radar (SAR), medical ultrasound, and optical coherence tomography images. Despite this, the watermarking method shows a slight improvement over the Salt and Pepper Attack, with an 82.82% match rate. This could indicate that the method has mechanisms that can handle the multiplicative noise characteristic of speckle better than additive noise.

In summary, the watermarking method exhibits commendable robustness, maintaining over 80% accuracy in character extraction across all tested noise attacks. This level of performance is significant, especially in the context of medical imaging, where the integrity of embedded patient information is crucial. The method's resilience to different types of noise attacks underscores its potential for secure and reliable data embedding in medical images, which is essential for maintaining patient confidentiality and ensuring the authenticity of medical records in digital healthcare systems.

TABLE 11. Robustness of watermarking method against additional attacks.

Attack Type	Textfile size	Number of Characters Inserted	Number of Characters Correctly Extracted	Percentage of Match
Without Attack	1KB	1905	1905	100%
Zero Attack	1KB	1905	1569	82.36%
Salt and Pepper Attack	1KB	1905	1577	82.78%
Gaussian Noise Attack	1KB	1905	1559	81.28%
Speckle Noise Attack	1KB	1905	1570	82.82%

The proposed work on comparing DCT and LSB techniques for securing medical data in telemedicine faces two major challenges. First, enhancing the robustness of LSB steganography against sophisticated attacks like statistical analysis and steganalysis is crucial for ensuring security in real-world scenarios. Second, ensuring compliance with legal and ethical regulations such as (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation) is essential to avoid legal issues and maintain patient trust. Addressing these challenges is vital for the effective use of LSB steganography in telemedicine.

VI. CONCLUSION

This research work examines various methods for protecting medical data in telemedicine by comparing two techniques - DCT and LSB. The study concludes that LSB is the more effective method for securing medical images that contain embedded text or PDFs.The effectiveness of LSB encryption can be demonstrated by its key indicators, such as a perfect SSIM score of 1.00 and high PSNR values of 87.63dB for text and 88.58dB for PDF files. Additionally, LSB encryption proves to be a practical solution due to its quick insertion and extraction times, making it suitable for real-time telemedicine applications.It has been observed that in both PDF and text files, the values of MSE values of LSB are consistently smaller as compared to MSE value of DCT values. This indicates that LSB-based steganography causes less distortion than the DCT-based method in the given context.

On the other hand, DCT has some issues with maintaining similarity during extraction. The study not only suggests that LSB steganography is superior, but also demonstrates how it meets the practical requirements of telemedicine. Choosing LSB steganography is not just about security, but also a practical step forward in merging safety with efficiency in protecting medical data. As the Healthcare industry moves forward with digitalization the proposed study points to LSB as a reliable way to secure telemedical data without making things complicated.

FUTURE SCOPE

Expanding the scope of future research to include the embedding of audio and video data within medical images can open up new opportunities for improving the security of telemedicine. It is also important to conduct a comprehensive privacy impact assessment that addresses legal and ethical considerations to ensure the responsible use of steganography techniques in safeguarding patient data within the evolving landscape of telemedicine.

REFERENCES

[1] R. Bocu and C. Costache, "A homomorphic encryption-based system for securely managing personal health metrics data," *IBM J. Res. Develop.*, vol. 62, no. 1, pp. 1–10, Jan. 2018.

[2] S. Liu, Y. Zhuang, L. Huang, and X. Zhou, "Exploiting LSB self-quantization for plaintext-related image encryption in the zero-trust cloud," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103138. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221421262200028X

[3] M. N. Sharath, T. M. Rajesh, and M. Patil, "Analysis of secure multimedia communication in cloud computing," in *Proc. 2nd Int. Conf. Intell. Comput., Instrum. Control Technol. (ICICICT)*, vol. 1, Jul. 2019, pp. 136–144.

[4] H. Joseph and B. K. Rajan, "Image security enhancement using DCT & DWT watermarking technique," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Jul. 2020, pp. 0940–0945.

[5] B. A. Shtayt, N. H. Zakaria, and N. H. Harun, "A comprehensive review on medical image steganography based on LSB technique and potential challenges," *Baghdad Sci. J.*, vol. 18, no. 2, p. 0957, Jun. 2021.

[6] O. C. Abikoye and R. O. Ogundokun, "Efficiency of LSB steganography on medical information," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 11, no. 5, p. 4157, Oct. 2021.

[7] W.-Y. Chen, M. Yu, and C. Sun, "Architecture and building the medical image anonymization service: Cloud, big data and automation," in *Proc. Int. Conf. Electron. Commun., Internet Things Big Data (ICEIB)*, Dec. 2021, pp. 149–153.

[8] R. Ramasamy and V. Arumugam, "Digital watermarking—A tutorial," *IEEE Potentials*, vol. 41, no. 4, pp. 43–48, Jul. 2022.

[9] C. Dai, "Analysis on digital watermarking technology and its applications," in *Proc. Int. Conf. Data Analytics, Comput. Artif. Intell. (ICDACAI)*, Aug. 2022, pp. 200–204.

[10] M. R. Nayak, A. K. Parida, P. Pattnayak, and A. U. Khan, "An image watermarking framework based on saliency and phase congruency using LSB matching technique," in *Proc. 19th OITS Int. Conf. Inf. Technol. (OCIT)*, Dec. 2021, pp. 369–374.

[11] D. Katz, M. Zizyte, C. Hutchison, D. Guttendorf, P. E. Lanigan, E. Sample, P. Koopman, M. Wagner, and C. Le Goues, "Robustness inside out testing," in *Proc. 50th Annu. IEEE-IFIP Int. Conf. Dependable Syst. Netw.-Supplemental*, Jun. 2020, pp. 1–4.

[12] K. Hao, G. Feng, and X. Zhang, "Robust image watermarking based on generative adversarial network," *China Commun.*, vol. 17, no. 11, pp. 131–140, Nov. 2020.

[13] S. Kashifa, S. Tangeda, U. K. Sree, and V. M. Manikandan, "Digital image watermarking and its applications: A detailed review," in *Proc. IEEE Int. Students' Conf. Electr., Electron. Comput. Sci. (SCEECS)*, Feb. 2023, pp. 1–7.

[14] A. Anand, A. K. Singh, and H. Zhou, "ViMDH: Visible-imperceptible medical data hiding for Internet of Medical Things," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 849–856, Jan. 2023.

[15] A. Kunhu, H. Al-Ahmad, and S. A. Mansoori, "A reversible watermarking scheme for ownership protection and authentication of medical images," in *Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA)*, Nov. 2017, pp. 1–4.

[16] W. Al-Chaab, Z. A. Abduljabbar, E. W. Abood, V. O. Nyangaresi, H. M. Mohammed, and J. Ma, "Secure and low-complexity medical image exchange based on compressive sensing and LSB audio steganography," *Informatica*, vol. 47, no. 6, pp. 65–74, May 2023.

[17] W. Kim and K. Lee, "Digital watermarking for protecting audio classification datasets," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2020, pp. 2842–2846.

[18] L. Rakhmawati, W. Wirawan, and S. Suwadi, "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability," *EURASIP J. Image Video Process.*, vol. 2019, no. 1, pp. 1–22, Dec. 2019.

[19] Z. F. Makhrib and A. A. Karim, "Improved fragile watermarking technique using modified LBP operator," in *Proc. Int. Conf. Comput. Sci. Softw. Eng. (CSASE)*, Mar. 2022, pp. 132–137.

[20] Z. Ma, W. Zhang, H. Fang, X. Dong, L. Geng, and N. Yu, "Local geometric distortions resilient watermarking scheme based on symmetry," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 31, no. 12, pp. 4826–4839, Dec. 2021.

[21] C. J. S. Cruz and G. J. Dolecek, "Exploring performance of a spread spectrum-based audio watermarking system using convolutional coding," in *Proc. IEEE URUCON*, Nov. 2021, pp. 104–107.

[22] J. Wang and S.-G. Jahng, "Texture filtering with filtering scale map," *IEEE Access*, vol. 9, pp. 145415–145421, 2021.

[23] N. K. Kalantari, M. A. Akhaee, S. M. Ahadi, and H. Amindavar, "Robust multiplicative patchwork method for audio watermarking," in *Proc. 16th Int. Conf. Digit. Signal Process.*, Jul. 2009, pp. 1–4.

[24] Y. Xueyi, D. Meng, W. Yunlu, and Z. Jing, "A robust DWT-SVD blind watermarking algorithm based on Zernike moments," in *Proc. Commun. Secur. Conf. (CSC)*, May 2014, pp. 1–6.

[25] Y. JinaChanu, K. Manglem Singh, and T. Tuithung, "Image steganography and steganalysis: A survey," *Int. J. Comput. Appl.*, vol. 52, no. 2, pp. 1–11, Aug. 2012.

[26] P. Mohan, P. B. Menon, P. K. Rahul, and K. S. Sidharth, "Image steganography—A new approach using block truncation coding and LSB embedding," in *Proc. 6th Int. Conf. Trends Electron. Informat. (ICOEI)*, Apr. 2022, pp. 1527–1530.

[27] S. Moufid, F. Z. Lachgar, C. El Ainzroudi, and A. A. Ben El Arbi, "Improving steganography using image compression JPEG," in *Proc. 15th Int. Conf. Adv. Technol., Syst. Services Telecommun. (TELSIKS)*, Oct. 2021, pp. 405–410.

[28] M. Khaled and A. H. Abu El-Atta, "Enhanced algorithms for steganography based on least significant bit and secret image compression," in *Proc. 10th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, Dec. 2021, pp. 266–272.

[29] A. Q. Omar and O. Dakkak, "Developing a watermarking algorithm using hide information techniques," in *Proc. Int. Symp. Multidisciplinary Stud. Innov. Technol. (ISMSIT)*, Oct. 2022, pp. 994–997.

[30] A. Agarwal, H. Arora, M. Mehra, and D. Das, "Comparative analysis of image security using DCT, LSB and XOR techniques," in *Proc. 2nd Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Aug. 2021, pp. 1131–1136.

[31] F. Garzia, R. Cusani, and A. Chiarella, "A new hybdrid steganographic technique for images," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Sep. 2022, pp. 1–6.

[32] V. B. Anumol, P. Thejus, and L. V. Namboothiri, "Enhanced security in medical image steganography—A hybrid approach using spatial and transform domain," in *Proc. 2nd Int. Conf. Interdiscipl. Cyber Phys. Syst. (ICPS)*, May 2022, pp. 197–202.

[33] K. Brindha and R. Maruthi, "A robust and secure image steganography using convolutional neural networks and transform methods," in *Proc. 7th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, May 2023, pp. 1338–1346.

[34] K. Upreti, A. Verma, J. Parashar, P. Vats, A. Verma, and J. Singh, "A comparative analysis of LSB & DCT based steganographic techniques: Confidentiality, contemporary state, and future challenges," in *Proc. 6th Int. Conf. Contemp. Comput. Informat. (ICI)*, Sep. 2023, pp. 1581–1588.

[35] M. Wang and X. Shang, "A fast image fusion with discrete cosine transform," *IEEE Signal Process. Lett.*, vol. 27, pp. 990–994, 2020.

[36] S. H. AbdElHaleem, A. G. Radwan, and S. K. Abd-El-Hafiz, "Blind watermarking using DCT and fractional-order Lorenz system," in *Proc. Int. Conf. Microelectron. (ICM)*, Dec. 2022, pp. 94–97.

[37] M. Baziyad and M. S. Obaidat, "On the importance of the DCT phase for image steganography schemes," in *Proc. IEEE 5th Int. Conf. Comput. Commun. Autom. (ICCCA)*, Oct. 2020, pp. 791–795.

[38] R. Souadek, "Robust hybrid watermarking algorithm based on DCT-PMF-DWT-SVD," in *Proc. 19th Int. Multi-Conference Syst., Signals Devices (SSD)*, May 2022, pp. 1073–1078.

[39] S. Maryam Seyed Khalilollahi and A. Mansouri, "JPEG steganalysis using the relations between DCT coefficients," in *Proc. Int. Conf. Mach. Vis. Image Process. (MVIP)*, Feb. 2022, pp. 1–4.

[40] S. P. Yalla, A. Uriti, and A. Sethy, "GUI implementation of modified and secure image steganography using least significant bit substitution," *Int. J. Saf. Secur. Eng.*, vol. 12, no. 5, pp. 639–643, 2022.

[41] E. H. Jasim Halboos and A. M. Albakry, "Improve steganography system using agents software based on statistical and classification technique," *Bull. Electr. Eng. Informat.*, vol. 12, no. 3, pp. 1595–1606, Jun. 2023.

[42] S. Chhikara and R. Kumar, "An information theoretic image steganalysis for LSB steganography," *Acta Cybernetica*, vol. 24, no. 4, pp. 593–612, Jul. 2020.

[43] E. Mathur and M. Mathuria, "Unbreakable digital watermarking using combination of LSB and DCT," in *Proc. Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, vol. 2, Apr. 2017, pp. 351–354.

[44] C.-G. Apostol and C.-I. Rincu, "Digital watermarking secured with PWLCM, chaotic-feedback and LSB data hiding," in *Proc. 8th Int. Conf. Commun.*, Jun. 2010, pp. 439–442.

[45] A. Saxena, "Digital image watermarking using least significant bit and discrete cosine transformation," in *Proc. Int. Conf. Intell. Comput., Instrum. Control Technol. (ICICICT)*, Jul. 2017, pp. 1582–1586.

[46] B. Albertina, M. Watson, C. Holback, R. Jarosz, S. Kirk, Y. Lee, and J. Lemmerman, "Radiology data from the cancer genome atlas lung adenocarcinoma [TCGA-LUAD] collection," *Cancer Imag. Arch.*, vol. 10, p. 9, Jan. 2016, doi: 10.7937/K9/TCIA.2016.JGNIHEP5.

[47] N. T. Singh, C. Kaur, A. Chaudhary, and S. Goyal, "Preprocessing of medical images using deep learning: A comprehensive review," in *Proc. 2nd Int. Conf. Augmented Intell. Sustain. Syst. (ICAISS)*, Aug. 2023, pp. 521–527.

[48] W. Dharma Walidaniy, M. Yuliana, and H. Briantoro, "Improvement of PSNR by using Shannon-fano compression technique in AES-LSB StegoCrypto," in *Proc. Int. Electron. Symp. (IES)*, Aug. 2022, pp. 285–290.

[49] I. A. Sabilla, M. Meirisdiana, D. Sunaryono, and M. Husni, "Best ratio size of image in steganography using portable document format with evaluation RMSE, PSNR, and SSIM," in *Proc. 4th Int. Conf. Comput. Informat. Eng. (ICIE)*, Sep. 2021, pp. 289–294.

[50] K. Joshi, R. Yadav, and S. Allwadhi, "PSNR and MSE based investigation of LSB," in *Proc. Int. Conf. Comput. Techn. Inf. Commun. Technol. (ICCTICT)*, Mar. 2016, pp. 280–285.

[51] P. Ping, B. Guo, O. T. Bloh, Y. Mao, and F. Xu, "Hiding multiple images into a single image using up-sampling," *IEEE Trans. Multimedia*, vol. 26, pp. 4401–4415, 2024.

[52] S. Kaur and S. Singh, "Application of hybrid encryption methodsin digital steganography technique for secure communication," in *Proc. Int. Conf. Comput. Model., Simul. Optim. (ICCMSO)*, Dec. 2022, pp. 251–256.

[53] A. M. Kapadia and P. Nithyanandam, "Secured reversible matrix embedding based on dual image using integer wavelet and Arnold transform," *Proc. Comput. Sci.*, vol. 165, pp. 766–773, Jan. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920300211

[54] B. A. Wijaya, A. J. Manalu, B. A. Tarigan, and L. S. Silitonga, "Steganography text message using LSB and DCT methods," *J. Mantik*, vol. 5, no. 3, pp. 1825–1832, 2021.

[55] P. A. Shofro, K. Widia, D. D. A. P. Astuti, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "Improved message payload and security of image steganography using 3–3–2 LSB and dual encryption," in *Proc. Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI)*, Nov. 2018, pp. 158–162.

[56] B. Bharathkumar, S. Logeswar, S. Sudharsun, and B. Karthikeyan, "An enhanced triple prime encryption approach for image encryption in LSB steganography," in *Proc. 1st Int. Conf. Adv. Electr., Electron. Comput. Intell. (ICAEECI)*, Oct. 2023, pp. 1–6.

[57] I. Kich, E. B. Ameur, Y. Taouil, and A. Benhfid, "Image steganography scheme using dilated convolutional network," in *Proc. 12th Int. Conf. Inf. Commun. Syst. (ICICS)*, May 2021, pp. 305–309.

[58] L. Li, B. Luo, Q. Li, and X. Fang, "A color images steganography method by multiple embedding strategy based on Sobel operator," in *Proc. Int. Conf. Multimedia Inf. Netw. Secur.*, vol. 2, Nov. 2009, pp. 118–121.

RAMYASHREE (Member, IEEE) received the B.E. degree in computer science and engineering from SMVITM, Bantakal, in 2015, and the M.Tech. degree in computer science and engineering from NMAMIT, Nitte, in 2019. With a background in academia, she was an Assistant Professor with the Department of Computer Science and Engineering, SMVITM, from 2015 to 2017, and again from 2019 to 2021. Additionally, she was an Assistant Lecturer with NITK, Surathkal. Currently, she holds the position of an Assistant Professor with the Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal. Her research interests include image and video processing, artificial intelligence, and machine learning. She has contributed significantly to academia, having published over 15 papers in various conferences and journals and a book chapter. With a commitment to engineering education and research in the field of computer science, she actively engages in professional service activities.

P. S. VENUGOPALA (Senior Member, IEEE) received the B.E. degree in computer science and engineering from VTU, Belagavi, in 2002, the M.Tech. degree in computer science and engineering from NITK, Surathkal, in 2007, and the Ph.D. degree from VTU, in 2018. With a background in academia, he was with the Department of Computer Science and Engineering, NMAMIT, Nitte, from 2002 to 2022, where he has been taking charge as the Head of the Artificial Intelligence Department, since 2023. His research interests include image and video processing, artificial intelligence, and machine learning. He has contributed significantly to academia, having published over 20 papers in various conferences and journals and a book chapter. He is the Organizing Chair of IEEE DISCOVER Conference, in 2021, with a commitment to engineering education and research in the field of computer science, he actively engages in professional service activities.

S. RAGHAVENDRA (Senior Member, IEEE) received the bachelor's degree in computer science and engineering from the BMS Institute of Technology, Bengaluru, the master's degree from the R. V. College of Engineering, Bengaluru, and the Ph.D. degree from the Visvesvaraya College of Engineering, Bengaluru. Currently, he is an Assistant Professor with the Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal. He has more than 11 years of experience in teaching and research across several institutions. He has authored over 40 research publications focusing on cloud computing, machine learning, and the Internet of Things. He is actively involved in various editorial roles and serves as a board member, a reviewer, and a guest editor for prestigious journals, such as IEEE, Elsevier, Springer, Wiley, Taylor Francis, and KJIP. In addition, he holds the position of the Publication Chair for Discover-21 and BHTC 2024. He has contributed as an organizing committee member of several conferences. He is a Dedicated Member of IEEE and has served as the Joint Secretary for the IEEE Mangalore Sub-Section, in 2020, and the Website Co-Chair for IEEE MSS, in 2019.

B. ASHWINI (Member, IEEE) received the B.E. degree in information science and engineering from VTU, Belagavi, in 2004, the M.Tech. degree in computer science and engineering from NMAMIT, Nitte, in 2012, and the Ph.D. degree from VTU, in 2018. With a background in academia, she has been with the Department of Information Science and Engineering, NMAMIT, Nitte, since 2004. She has been taking charge as the Head of the Information Science Department, since 2023. Her research interests include image and video processing, artificial intelligence, and computer vision. She has contributed significantly to academia, having published over 15 papers in various conferences and journals. She is the Vice Chair of IEEE Mangalore Sub Section, in 2024, with a commitment to engineering education and research in the field of information science, she actively engages in professional service activities.