




BTP 2024.pdf

-  My Files
-  My Files
-  Bennett University

Document Details

Submission ID

trn:oid::29034:73359822

Submission Date

Dec 8, 2024, 1:57 PM GMT+5:30

Download Date

Dec 8, 2024, 2:04 PM GMT+5:30

File Name

BTP 2024.pdf

File Size

1.2 MB

27 Pages

7,019 Words

36,469 Characters





14% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.




Filtered from the Report

- Bibliography

Match Groups

-  **95** Not Cited or Quoted 14%
Matches with neither in-text citation nor quotation marks
-  **0** Missing Quotations 0%
Matches that are still very similar to source material
-  **0** Missing Citation 0%
Matches that have quotation marks, but no in-text citation
-  **0** Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 7%  Internet sources
- 5%  Publications
- 13%  Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- 95 Not Cited or Quoted 14%**
Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%**
Matches that are still very similar to source material
- 0 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

- 7% Internet sources
- 5% Publications
- 13% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Submitted works		
	Netaji Subhas Institute of Technology on 2023-05-14		1%
2	Submitted works		
	AUT University on 2024-10-20		1%
3	Submitted works		
	AUT University on 2024-10-20		1%
4	Publication		
	Dilara Şener, Selda Güney. "Enhancing Steganography in 256×256 Colored Images...		1%
5	Submitted works		
	Netaji Subhas Institute of Technology on 2023-05-14		1%
6	Submitted works		
	University of York on 2013-12-12		0%
7	Submitted works		
	University of Carthage on 2024-02-12		0%
8	Submitted works		
	University of Durham on 2020-05-08		0%
9	Submitted works		
	Liverpool John Moores University on 2024-12-01		0%
10	Internet		
	www.mdpi.com		0%

11	Submitted works	Netaji Subhas Institute of Technology on 2021-12-20	0%
12	Submitted works	The University of Buckingham on 2015-03-18	0%
13	Submitted works	University of London External System on 2017-06-01	0%
14	Submitted works	King Fahd University for Petroleum and Minerals on 2012-04-03	0%
15	Internet	coek.info	0%
16	Internet	link.springer.com	0%
17	Internet	www.frontiersin.org	0%
18	Submitted works	University of Northumbria at Newcastle on 2011-01-10	0%
19	Submitted works	University of Wolverhampton on 2014-01-21	0%
20	Submitted works	Zarqa University on 2024-10-17	0%
21	Publication	"Advances in Intelligent Information Hiding and Multimedia Signal Processing", S...	0%
22	Internet	www.igi-global.com	0%
23	Internet	www.studymode.com	0%
24	Submitted works	University of Greenwich on 2010-05-01	0%

25	Submitted works	University of Malaya on 2012-04-17	0%
26	Internet	ir.lib.uth.gr	0%
27	Internet	vdocument.in	0%
28	Submitted works	King Fahd University for Petroleum and Minerals on 2012-04-07	0%
29	Submitted works	Middlesex University on 2007-04-12	0%
30	Submitted works	Queen Mary and Westfield College on 2011-08-26	0%
31	Submitted works	SKEMA Business School on 2024-11-01	0%
32	Internet	www.bracu.ac.bd	0%
33	Internet	academic.oup.com	0%
34	Internet	kanazawa-u.repo.nii.ac.jp	0%
35	Internet	mscr.org.my	0%
36	Internet	www.coursehero.com	0%
37	Submitted works	Kingston University on 2023-09-10	0%
38	Submitted works	Liverpool John Moores University on 2015-04-24	0%

39	Submitted works	Middlesex University on 2021-01-08	0%
40	Submitted works	Universidad Rey Juan Carlos on 2022-11-15	0%
41	Submitted works	Universiti Malaysia Pahang on 2015-08-25	0%
42	Publication	"Information Hiding", Springer Science and Business Media LLC, 2008	0%
43	Submitted works	Anna University on 2024-07-02	0%
44	Submitted works	Federal University of Technology-Nigeria on 2024-01-17	0%
45	Submitted works	Heriot-Watt University on 2023-12-07	0%
46	Publication	Tohari Ahmad, Muhammad Hanif Amrizal, Waskitho Wibisono, Royyana Muslim Ij...	0%
47	Submitted works	University of East Anglia on 2022-08-27	0%
48	Submitted works	University of New York in Tirana on 2023-07-26	0%
49	Submitted works	University of Pretoria on 2012-07-09	0%
50	Submitted works	Visvesvaraya Technological University on 2014-11-08	0%
51	Publication	Wazirali, Raniyah Abdullah. "Optimization of Perceptual Steganography Capacity ...	0%
52	Internet	dokumen.pub	0%

53	Internet	studentsrepo.um.edu.my	0%
54	Internet	www.ijcsit.com	0%
55	Internet	www.researchgate.net	0%
56	Submitted works	Higher Education Commission Pakistan on 2024-06-26	0%
57	Submitted works	International Islamic University Malaysia on 2014-10-20	0%
58	Submitted works	Kaplan College on 2024-06-23	0%
59	Submitted works	Liverpool John Moores University on 2023-03-14	0%
60	Publication	"Intelligent Techniques in Signal Processing for Multimedia Security", Springer Sc...	0%
61	Submitted works	University of Glasgow on 2011-09-05	0%
62	Submitted works	University of Greenwich on 2024-04-22	0%
63	Submitted works	University of Huddersfield on 2023-01-09	0%
64	Submitted works	University of Northumbria at Newcastle on 2009-01-23	0%

TITLE OF PROJECT-REPORT

Enhancing Telemedicine Security by Embedding Multimedia Data using Steganography

Submitted by:

Aman Muhal (2021UIT3051)

Aniket Kumar (2021UIT3069)

Under the supervision of

Dr. Mohit Sajwan



DEPARTMENT OF INFORMATION TECHNOLOGY
NETAJI SUBHAS UNIVERSITY OF TECHNOLOGY

Dec, 2024

DECLARATION



Department of Information technology

Delhi-110078, India

We, Aman Muhal (2021UIT3051) and Aniket Kumar (2021UIT3069) of B. Tech., Department of Information Technology, hereby declare that the Project I - report titled "Enhancing Telemedicine Security by Embedding Multimedia Data using Steganography" which is submitted by us to the Department of Information Technology, Netaji Subhas University of Technology, is original and not copied from source without proper citation. This work has not previously formed the basis for the award of any Degree.

Place: Delhi

(Name and signature of student(s))

Date: 08.12.2024

CERTIFICATE**Department of Information technology****Delhi-110078, India**

This is to certify that the work embodied in the Project I-Report titled “Enhancing Telemedicine Security by Embedding Multimedia Data using Steganography” has been completed by AMAN MUHAL-2021UIT3069 and ANIKET KUMAR-2021UIT3069 of B.Tech., Department of Information Technology, under my guidance. This work has not been submitted for any other diploma or degree of any University.

Place: Delhi**(Signature of Supervisor)****Date: 08.12.2024**

ABSTRACT

Telemedicine has grown rapidly in order to serve the needs of patients residing in remote areas. However, ensuring data security of the patients within this platform remains a challenge, and more so when it involves a number of multimedia components such as audio consultations. Steganography solves the problem by hiding sensitive information within digital media, which increases security through obscurity. The purpose of this paper is to provide a new way in improving the security of the telemedicine system using steganography by hiding an audio file within medical images. DICOM, or Digital Imaging and Communication in Medicine, images are used here as cover media in embedding an audio message with the Least Significant Bit method without degrading much the visual quality of an image. The proposed method for providing a balance between optimal values for data embedding capacity without damaging the high values for imperceptibility is critical towards securing patient confidentiality during transmission. Performance metrics, which in turn are assessed as regard effectiveness and efficiency in LSB-based image steganography methods for medical applications in our current proposition, include SSIM, PSNR, and MSE. The experimental results confirm the undetectable nature of the embedded data in normal analysis and underlines our approach's prospects in various secure telemedicine applications. This paper hopefully will lead to more improvements or reinforcement on the current approaches developed so far for secure telemedicine frameworks toward stronger versions.



LIST OF FIGURES

S.No	List of Figures	Page No.
1.	Figure 1.1: Embedding Process	
2.	Figure 1.2: Extraction Process	
3.	Figure 2.1: DICOM Sample	
4.	Figure 2.2: Embedding Process using LSB	
5.	Figure 2.3: Extraction Process using LSB	
6.	Figure 2.4: Embedding Process using Proposed Method	
7.	Figure 2.5: Extraction Process using Proposed Method	
8.	Figure 3.1: Comparison of Insertion and Extraction time using LSB method	
9.	Figure 3.2: Comparison of Insertion and Extraction time using Proposed method	
10.	Figure 3.3: MSE Comparison Between LSB and Proposed Methods for various audio sizes	

LIST OF TABLES

S.No	List of TABLE	Page No.
1.	Table 1.1: Spatial Domain Techniques	
2.	Table 3.1. Embedding and Extraction Times for Different Audio File Sizes using LSB	
3.	Table 3.2. PSNR and SSIM Values for Different Embedded Audio Sizes using LSB	
4.	Table 3.3. Embedding and Extraction Times using Proposed Method	
5.	Table 3.4. PSNR and SSIM Values for Different Embedded Audio Sizes using Proposed Method	
6.	Table 3.5: Comparison of MSE for LSB and Proposed Method	

CHAPTER 1 : INTRODUCTION

Rapid development within the sector of telemedicine has completely changed the course of health care, and now one can diagnose, monitor, and treat patients without their actual presence. Telemedicine opens this door to health care in far-flung and underserved areas by enabling the sharing of sensitive medical data on digital networks. It includes, but is not limited to, critical medical imaging information with CT scans, MRI, and X-rays using DICOM files. On the other side, the expansion of telemedicine faces serious challenges to data security, or otherwise known as patient privacy, especially in terms of compliance to PHI. PHI is defined as a patient's name, birth date, social security number, and any other information about the patient concerning symptoms, diagnoses, imaging, treatment plans, and many more. Such information might be subjected to unauthorized access or even manipulation; either of those situations would be disastrous with respect to the privacy of the patient and veracity of the clinical decision-making process. Consequently, security of patient information in telemedicine is among the main priorities.

The security of medical imaging data, pursued from a twofold approach, often puts the medical report and the identity apart. This way, medical imaging can keep the confidentiality of private data by preventing unauthorized accesses. In this regard, for example, such separation would help provide a situation in which accessed imaging data may still deny revealing the identity of their patient.

Second, the dataset may be very often protected through heavy encryption. This additional level of security makes it next to impossible for an attacker to interpret the data if they somehow get access to the reports. However, encryption alone may be insufficient because it can be time-consuming and may introduce latency, making it undesirable in real-time applications such as in telemedicine. Various techniques have been tried to overcome such problems and they include cryptography, watermarking, and steganography. Of these, the useful one is steganography because it provides a secret place for sensitive data within the digital media and makes such data imperceptible to unauthorized users.

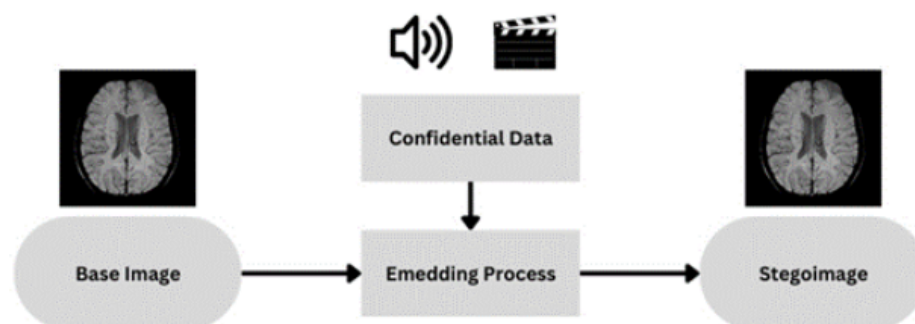


Figure 1.1: Embedding Process

Since there is embedding of relevant multimedia data like audio annotations within the DICOM files through steganography, sending it remains safe along with maintaining integrity and patient information confidential. During the embedding procedure, an image is embedded by incorporating the audio into the original image through a specified algorithm as depicted in Figure 1.1.

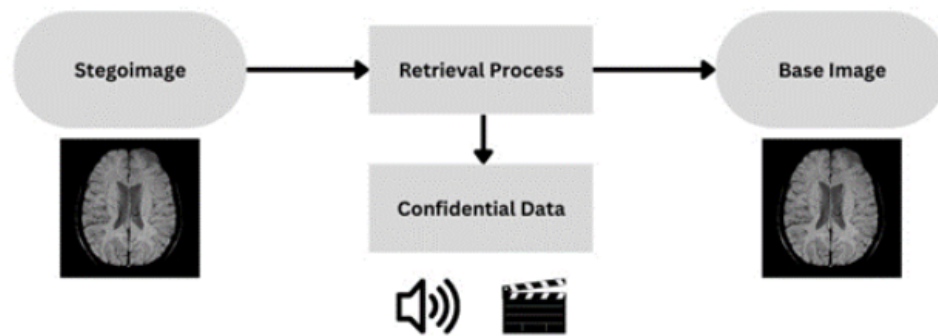


Figure 1.2: Extraction Process

The extraction process follows the audio extracted from the embedded image using the same algorithm adopted in the embedding phase and as illustrated in Figure 1.2.

The Least Significant Bit technique can be considered representative of common methods of embedding secret data within digital media without complicating the process or affecting its appearance and quality.

From this perspective, in the LSB embedding of DICOM files, the least significant bits of the image pixels are tampered with to embed the additional data, such as audio, in such a way that the visual medical information is not disturbed. While LSB is indeed efficient and easy to implement, it does suffer from limitations in robustness and security. It easily gets extracted or corrupted under the effects of noise, compression, or image manipulation, and this makes it unsuitable for high-stakes applications like telemedicine where the security of patient data is of great importance. An embedding that makes use of APVD - Adaptive Pixel Value Differencing to embed the audio into the DICOM pixel data in handling the challenges at hand is proposed for optimality. The present work developed a PVD by employing a more sophisticated methodology by which the chances of data distortion will be reduced and therefore the security of the embedded data enhanced. The encoding process, in this approach, involves the conversion of audio first into its binary form, then embedding it inside DICOM pixels. Enhanced embedding strategy that involves tracking pixel values of the difference will introduce difficulty in its detection.

Embedding is, therefore, done in complement with an embedding procedure using AES encryption to handle key information safely by which the embedded information is not to be disclosed at any stage of storage and/or transmission.

This will not only contribute to the effective strengthening of the whole steganography process but also make it easier to achieve the exact extracted data from a recipient's

perspective, appropriate for use in telemedicine applications that require safety on aspects of data confidentiality and integrity.

The proposed methods are also justified using performance metrics like SSIM, PSNR, and MSE that substantiate their efficacy. It thereby ensures that the diagnostic utilitarian value of DICOM images remains uncompromised while embedding hidden data in a secured way.

The key contributions made by this work are as follows:

1. It is proposed to upgrade the existing PVD-based solution for embedding audio data into DICOM medical images in such a way that it maintains image quality.
2. In this work, some metrics, like SSIM, PSNR, and MSE, quantitatively test the image quality and robustness.
3. A relative study of LSB and PVD is done to provide an analysis of the various strengths and weaknesses of both while performing medical data hiding without affecting the image fidelity.

The results will be important in the area of telemedicine, where confidentiality with accuracy of a patient's data is very critical. This paper presents a comparative study performed to show the robustness of both LSB and the proposed method for various conditions and hence their strengths and areas that can be further improved. It will eventually embed the security of sensitive patient information, build trust in patients, and widen its adoption in digital health solutions securely, reliably, and in a privacy-compliant manner by integrating advanced steganographic techniques within telemedicine.

1.1 FUNDAMENTAL ASPECTS OF STEGANOGRAPHY

Steganography is an embedding technique of secret data within a carrier medium, like images, audio, or video file, in such a manner that the hidden information shall not be detected by attackers. The word "steganography" itself is derived from two Greek words meaning "covered writing," where the aim has always been to mask the messages in such a way that they could not be detected by the human naked eye or ear. While encryption scrambles the data to make it unreadable without a key, steganography conceals the very existence of the data.

A typical steganographic system consists of the following crucial components:

- Medium of Cover: This is the file that will bear the secret data, which could be an image, audio, or video file.
- Payload: This is the secret message or data to be embedded within the cover medium.
- Embedding Algorithm: It is a technique which will be used to embed the payload into the cover medium. The embedding algorithm ranges from a simple LSB to more sophisticated methods.
- Extraction Algorithm: A process applied for extracting the hidden message from the carrier medium.

Steganographic techniques can be broadly classified into spatial domain techniques and frequency domain techniques. Main difference between them lies in how the data is embedded within the carrier medium.

1) **Spatial Domain Techniques:** The methods directly affect the pixel values or sample data of the cover medium to embed the secret message. These techniques are usually easier to implement and computationally less complex, but they could be more vulnerable to attacks that try to detect the embedded data. Among the spatial domain techniques, one of the most popular is the Least Significant Bit, where the least significant bits of the image or audio file are replaced by the bits of the secret message. Although easy to implement and quite effective in many cases, LSB embedding can be discovered through statistical analysis or through methods of image processing if the data is not well hidden.

2) **Frequency Domain Methods:** These work by first transforming the cover medium into a frequency space and then embedding the secret data in these transformed values. These methods are usually robust in comparison with the methods of spatial domain, since the latter affect the coefficients of frequencies, which, as a rule, are more difficult to detect. One of the most popular frequency domain techniques is discrete cosine transform, widely applied in image and video steganography. Since the data is embedded in the DCT coefficients, the hidden information is less likely to be affected by common image manipulations such as compression or noise; therefore, it is more resistant to attacks. Frequency domain methods are more complex but more secure and robust, thus providing higher security compared to spatial domain techniques.

Table 1.1: Spatial Domain Techniques

Technique	Description
LSB (Least Significant Bit)	Embeds the data by changing the least significant bit of the pixel values.
Pixel Value Differencing	It encodes data by changing the difference between adjacent pixel values.
Masking	Data implanted by changing pixel intensities with a mask that affects only the least observable bits.
Texture Synthesis	Conceals the data by generating new textures and altering the original ones in an image.
Discrete Cosine Transform (DCT)	This technique alters the DCT coefficients, embedding data in the frequency domain.
Discrete Wavelet Transform (DWT)	It changes the wavelet coefficients to disguise information within an image
Singular Value Decomposition (SVD)	Embeds information in an image by altering its matrix's singular values.

CHAPTER 2 : PROPOSED METHODOLOGY

This work proposes a methodology for embedding sensitive audio data safely into medical images without compromising the integrity of the image itself or the confidentiality of the audio information. In the health sector, sensitive medical data needs to be guarded at all costs, since unauthorized access and manipulations lead to patient breaches in privacy and security. Therefore, this procedure has looked to embed information of speech in a widely adopted form: medical images, notably the so-called DICOM images without degrading their quality. This is important for a number of applications, including telemedicine, in which patient data would need to be transmitted over a network and must be maintained secure from interception or other forms of unauthorized access.

In this technique, great emphasis will be provided to finding an optimum balance between the two entities—security on one end and the image's quality on the other end by introducing a secret key.

2.1 DATASET DESCRIPTION

The dataset used in the following work consists of medical images, taken from openly available DICOM format repositories (Figure 2.1). In general, the DICOM file format is used to store and send medical imaging data like computed tomography, MRI scans, and X-ray data along with metadata such as information about the patient and diagnosis.

There are audio files of different lengths used as the payload to be embedded within the DICOM images. These represent sensitive patient data, such as doctor's notes or diagnostic recordings, which need to be kept confidential if stored or transmitted.

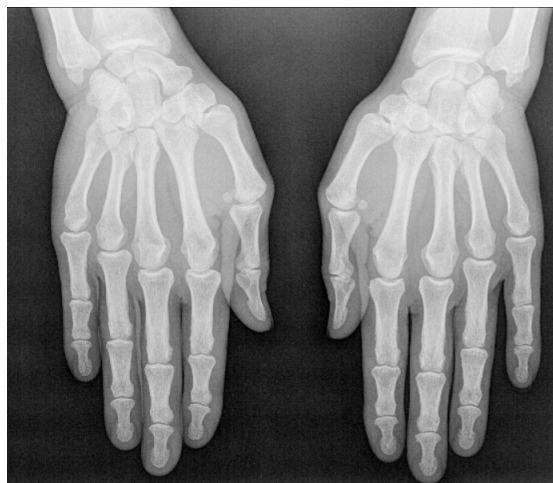


Figure 2.1: DICOM Sample

We use the selected medium—DICOM images—to embed our secret data, audio files, in order to find out the compatibility of robustness and practicality in applying this methodology for the security of sensitive medical data

2.2 PRE-PROCESSING METHODS

The pre-processing stage involves preparing both the DICOM images and the audio files for the embedding process. The following steps are undertaken:

1) DICOM Image Pre-Processing : Extract the grayscale or RGB value of a pixel from DICOM to act as the cover medium. This involves the process of normalization in order to get all values of a variable within a precise range in the dataset, which can then work along with the chosen algorithm for embedding.

2) Audio File Pre-Processing : The audio file is first changed into a binary format, in which every sample is converted into a bit stream to use as the payload. Then, the binary data is fragmented into chunks matching the embedding capacity of the DICOM image.

3) Data Validation : The size of the audio payload must be compatible with the embedding capacity of the DICOM image to avoid overloading. Anomalies in both the DICOM image and binary audio data are checked to ensure smooth embedding.

In particular, it is the pre-processing that assures the best preparation of data to perform the embedding and extraction of information without further risks, which could compromise the good quality of the cover image.

2.3 IDENTIFY SUITABLE STEGANOGRAPHY METHODS

Some possible steganographic methods embedding sensitive audio data into the medical DICOM images were dealt with in the present work, considering integrity from two sides: from the aspect of audio data itself and that of the image. The more progressive techniques of embedding and extraction of audio ensure a quite safe and effective embedding process without bringing so far much visible distortion into DICOM images. This section describes two main methods that are being used: LSB and our proposed method based on Pixel Value Differencing (PVD), which is an enhanced method for improving both the robustness and imperceptibility of the embedding process

2.3.1 TO INCORPORATE AUDIO AND RETRIEVE AUDIO USING THE LSB METHOD

Among all steganographic methods, the least significant bit is the most common for embedding secret data within a digital picture. The major advantage this offers is that the appearance of the image is minimally changed and hence the data embedded within it is almost invisible to the human eye. LSB technique is applied essentially on the fact that regarding the pixel values, the most negligible bits are contributed with little or

nothing to an image's visual value, and therefore, hiding the data as a secret at this level does not considerably degrade its integrity..

As mentioned in Figure 2.2, the audio file has to be converted into a binary format for the embedding process in the image using the LSB method. The audio data, normally kept as digital signals, for example, in WAV or MP3 format, is changed into a binary stream of bits. This process usually deals with breaking down the audio into smaller units, such as bytes or bits, which may then be used for embedding. A set of bits is generated for every audio sample.

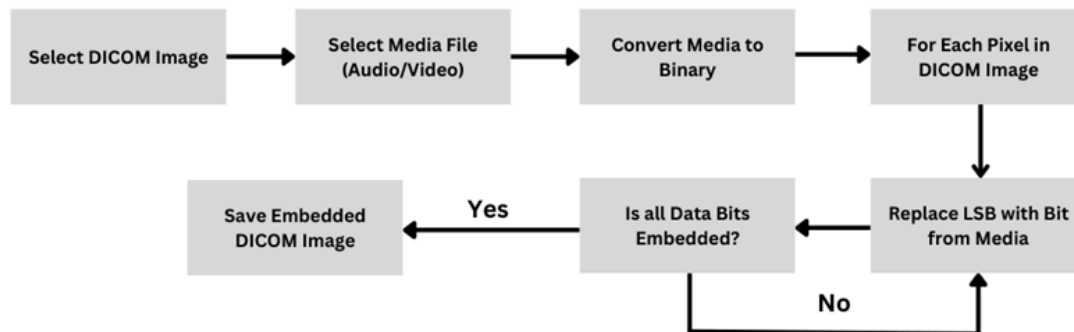


Figure 2.2: Embedding Process using LSB

To embed the audio data into the image, the binary bits of the audio file are inserted sequentially into the least significant bit of every pixel in the image. Using an example, if the image pixel value is an 8-bit integer that falls in the range of 0 to 255, only the least significant bit—the rightmost bit—would be changed to store a bit of the audio data. This means it will replace the least significant bit of the first pixel with the first bit of the audio file, the least significant bit of the second pixel with the second bit, continuing until all bits of the audio data are embedded in the image pixels.

The quality of the image is barely degraded by the LSB method, since the alteration of the least significant bit of a pixel affects the color or brightness of the pixel very little and is practically imperceptible by the human eye. However, this could be a benefit of particular value when the objective is to maintain the confidentiality of the embedded audio data while still keeping the cover image suitable for medical or other sensitive applications.

Once the audio data is embedded in the image, the next task would be to retrieve the original audio file. The attempt would begin by identifying each pixel's least significant bit as described in Figure 2.3. Each pixel of the image will carry one bit of the original audio file. The sequential extraction of these least significant bits creates a binary sequence, which, in turn, represents the audio file that has been hidden. These bits are gathered from the RGB channels of the image or from grayscale values in monochrome images. Further, the bits within this sequence are recombined into a binary stream representing the original audio file.

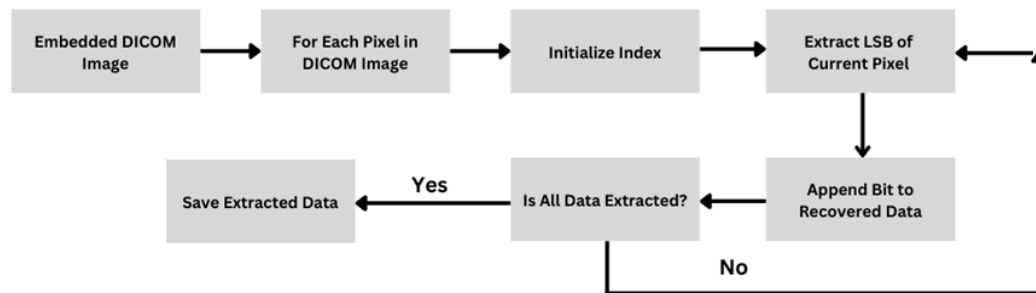


Figure 2.3: Extraction Process using LSB

This reconstructed binary sequence, when complete, is then converted back into its original audio format—for example, WAV, MP3, or whichever is preferred—using a process inversely applied to that which performed the binary-to-audio conversion. Now, the audio file is saved and can be played or further analyzed as desired.

While simple and effective, the LSB method presents a number of limitations regarding embedding and extracting audio data in images. The major disadvantages are vulnerability to image compression techniques where loss or corruption of embedded data may take place. Also, the amount of data to be hidden under the LSB depends highly on the size of the images, since only the least significant bit of each pixel could represent the data, hence minimizing its capacity to hold large quantity audio data. Larger files would need more pixels that are to store all the bits—a prerequisite not feasible in respect of the resolution of a cover image.

2.3.2 TO INCORPORATE AUDIO AND RETRIEVE AUDIO USING THE PROPOSED METHOD

The proposed method of incorporating audio information into DICOM images involves embedding, integrity checking, and extraction. Our method extends the concept of PVD by integrating advanced techniques to enhance the security of embedded audio information while maintaining the quality of the medical images.

The embedding process initiates with the loading of a DICOM image and an audio file into the system. A DICOM image is an intricate format for storing medical imaging data, such as CT scans, MRIs, and X-rays, which houses both pixel data and metadata. In embedding, first, the audio file is converted to its binary format since the image requires binary sequences for embedding.

After preparing the DICOM image and audio data, the pixel data of the DICOM image is extracted. Our approach as described in Figure 2.4 uses an APVD-based selection strategy of pixels to be used for embedding, similar to PVD but with modifications to optimize the available space for embedding while allowing minimal distortion in the

image. In the proposed method, the differences of pixel values are considered for evaluation in which the pixels that have larger differences will be chosen for embedding. This ensures that the visual quality of the image is unchanged after embedding.

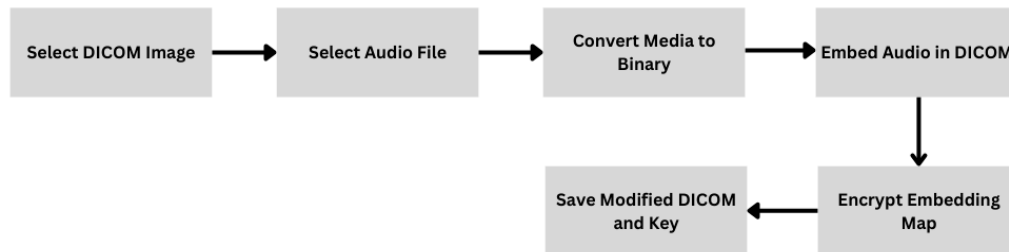


Figure 2.4: Embedding Process using Proposed Method

Herein, an embedding map of locations and bit counts of the pixels used for embedding the audio is maintained. The map provides a record of the exact pixel locations and how many bits in each pixel were changed. This embedding map is necessary in the extraction process to precisely retrieve the embedded data. First, to protect the integrity of the embedded data, the embedding map and the length of the audio will be encrypted by an AES encryption algorithm. This keeps the map secure and protects it from unauthorized access. In this way, confidentiality can be kept.

After the audio data has been embedded, the modified DICOM image is saved along with the information of the embedded audio. The final image is visually the same as the original DICOM image; hence, one would not be able to tell by just looking at the embedding process.

First, the encrypted key will be decrypted to obtain the embedding map and audio length. This AES decryption step shall be executed with the secret key to ensure that only authorized parties would have the possibility of decrypting it, hence gaining access to the embedding map.

Once the extraction algorithm has accessed the embedded map, it makes use of it for the detection of the exact pixels in which alterations have taken place throughout the embedding phase. The locations of these pixels, together with the overall count of the bits, are obtained from this map, thereby guiding it in its extraction process. Each pixel of the modified DICOM is scanned, wherein the bit value embedded in those pixels are extracted as shown in Figure 2.5.

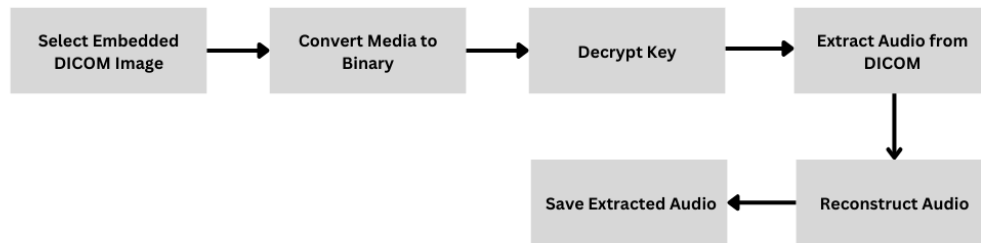


Figure 2.5: Extraction Process using Proposed Method

This extracted binary data is then reconstructed to return the audio into its original format and ensure that no information is lost during the extraction process. Then, the extracted audio is saved in a new file ready for playback or further analysis.

This technique has ensured especially delicate embedding through the AES encryption of the embedding map. An embedding map bears information on the data places in the image, and when encrypted, it allows only the owner or user authorized to make use of the embedded audio. The use of an adaptive pixel selection has given assurance that the degradation level of the image will be inconsiderable while the audio information is kept safely tucked inside.

This approach is built in such a way that it will resist blind attempts for unauthorized extraction. With this kind of implementation, even when the attacker gets access to a DICOM image, he should also have the encrypted key and embedding map to attempt the extraction of embedded audio. It's inaccessible to the attacker due to his not having an appropriate key with him for actual decryption.

2.4 EVALUATION TECHNIQUES USING VARIOUS PARAMETERS

To evaluate the performance, we consider the following standard evaluation metrics: Peak Signal-to-Noise Ratio, SSIM or Structural Similarity Index, Mean Squared Error, and Bits Per Pixel. Each metric allows a further look into one aspect with respect to quality, embedding capacity, or robustness.

2.4.1 Peak Signal-to-Noise Ratio (PSNR):

PSNR basically gives the fidelity of the embedded image with respect to the original image. Mathematically, PSNR can be given as Equation 2.1

$$PSNR = 10 * \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (2.1)$$

Where:

- *MAX*: Maximum possible pixel value (e.g., 255 for 8-bit images).
- *MSE*: Mean Squared Error between the original and embedded images

The higher PSNR means higher quality with less distortion.

2.4.2 Structural Similarity Index (SSIM) :

SSIM is a metric that estimates the perceptual quality of the embedded image by comparing luminance, contrast, and structural information defined as Equation 2.2:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (2.2)$$

where:

- μ_x, μ_y : Mean intensities of images x (original) and y (embedded).
- σ_x^2, σ_y^2 : Variances of images x and y.
- σ_{xy} : Covariance between x and y.
- C_1, C_2 : Stabilizing constants against division by zero

The values of SSIM vary between 0 and 1, with higher values indicating more structural similarity.

2.4.3 Mean Squared Error (MSE) :

MSE quantifies pixel-wise differences between the original and embedded images. It is computed as Equation 2.3:

$$MSE = \frac{1}{M*N} \sum_{i=1}^M \sum_{j=1}^N [I(i, j) - I_e(i, j)]^2 \quad (2.3)$$

Where:

- M, N : Dimensions of the image.
- $I(i, j)$: Pixel value at position (i, j) in the original image.
- $I_e(i, j)$: Pixel value at position (i, j) in the embedded image.

Lower values of MSE signify minimal distortion at the pixel level.

2.4.4 Bits Per Pixel (BPP):

BPP basically measures the embedding capacity of the steganographic technique. It is defined as Equation 2.4:

$$BPP = \frac{\text{Size of Embedded Data (bits)}}{\text{Total Number of Pixels}} \quad (2.4)$$

where:

- Size of Embedded Data (bits): Total number of bits embedded.
- Total Number of Pixels: Total number of pixels in the cover image.

Larger values of BPP provide better data embedding efficiency but are likely to increase distortion.

2.5 COMPREHENSIVE EVALUATION

In this approach, we perform the systematic evaluation of an embedding and extraction process using these metrics to assure robust evaluation. PSNR and SSIM give information about visual quality and structural integrity of the image, while MSE accounts for the pixel-level distortion quantification. BPP on the other side provides the embedding efficiency that is highly desirable in any high-capacity applications dealing with telemedicine. These evaluations build up a complete understanding of the trade-offs between imperceptibility, capacity, and robustness, highlighting an effective approach to maintaining sensitive medical data integrity.

CHAPTER 3 : EXPERIMENTS AND RESULTS

These experiments were carried out using Python language, with the help of libraries like NumPy to efficiently handle data, Wave for processing audio files , skimage for calculating image quality metrics like PSNR, SSIM, MSE and Pydicom for processing DICOM images. Also, DICOM medical images were gathered as the dataset input for the experiments. We executed our python scripts on a machine running Windows 11 having Intel(R) Core(TM) i5 processor and 16 GB of RAM. It consisted of embedding audio information obtained from a binary payload in the pixel data of the medical images. Both LSB and our proposed techniques have been applied to perform embedding and extraction in order to make comparative studies possible about each approach's efficiency and performance.

3.1 EMBEDDING AND EXTRACTING AUDIO USING LSB

It was seen from the analysis of embedding and extracting audio data using the LSB method that under ideal conditions, there was a very high success rate because the retrieval of the audio file was exactly correct. The results came out to be that the extracted audio completely matched with the original every time so that the integrity of the concealed information remains intact. This shows how robust this technique is and at the same time points out the reliability of the LSB technique in managing sensitive data.

Table 3.1. Embedding and Extraction Times for Different Audio File Sizes using LSB

Embedded Audio File	Embedded Audio Size	Embedding Time (Sec)	ExtractionTime (Sec)
Audio 1	17 kb	5.4278	3.5208
Audio 2	100 kb	5.4598	3.6821
Audio 3	200 kb	5.8675	4.3117
Audio 4	300 kb	6.5319	4.4347
Audio 5	400 kb	6.9214	4.7419
Audio 5	400 kb	6.9214	4.7419
Audio 6	500 kb	9.5708	5.1397

Table 3.1 shows embedding and extraction performance concerning the audio file size, which ranges between 17 KB and 500 KB in the DICOM image. Embedding time spans from 5.4278 seconds in the case of the smallest to 9.5708 seconds for the biggest file, whereas the extraction time is between 3.5208 and 5.1397 seconds. This indeed reflects scalability in terms of how efficiently the LSB technique could handle various payload sizes.

Table 3.2. PSNR and SSIM Values for Different Embedded Audio Sizes using LSB

Embedded Audio File	Embedded Audio Size	PSNR Value (dB)	SSIM
Audio 1	17 kb	67.08	1.0000
Audio 2	100 kb	59.24	1.0000
Audio 3	200 kb	56.23	1.0000
Audio 4	300 kb	54.47	1.0000
Audio 5	400 kb	53.21	1.0000
Audio 6	500 kb	52.23	1.0000

The PSNR and SSIM values, elaborated in the table 3.2, further ascertain that the quality of the images does not degrade during the embedding and extraction processes. PSNR values start at 67.08 dB for the smallest audio file and gradually decrease down to as low as 52.23 dB for the largest size, but the values do not fall below the acceptable range; hence, the image quality remains justifiable.

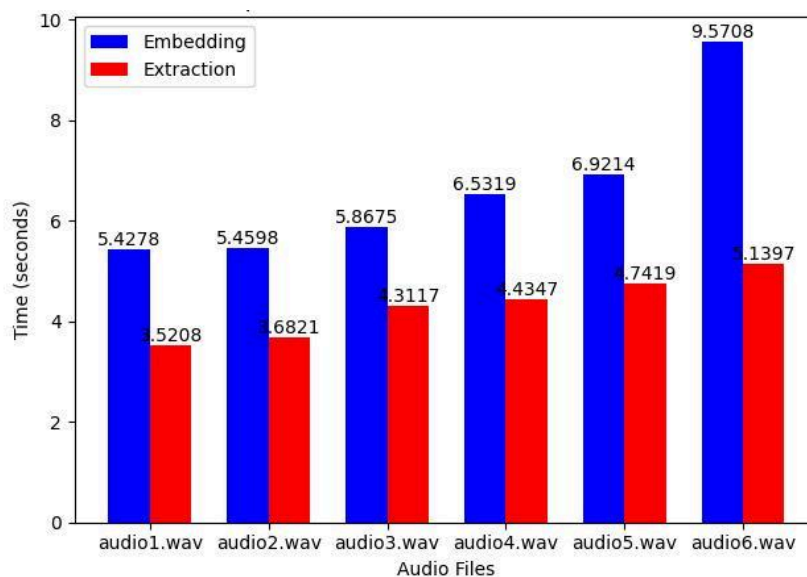


Figure 3.1: Comparison of Insertion and Extraction time using LSB method

It would also be observed that the SSIM values remain the same at 1.0 regardless of the variation in size of the audio file used; this itself demonstrates that the inherent structure within the DICOM image remains wholly intact. Both these observations clearly indicate that indeed the LSB technique can insert the audio information within the interior of medical images in a reasonably secure way without much loss into the visual presentation or without disturbing the structural cohesion of those images.

3.2 EMBEDDING AND EXTRACTING AUDIO USING PROPOSED METHOD

The efficiency and accuracy of the proposed method in handling varied sizes of the audio files can be demonstrated by analyzing the embedding and extracting of audio data using the proposed method for a number of different-sized audio files. The obtained results show that the proposed technique is strong enough to embed and retrieve audio without significant compromise in the quality of the DICOM image.

Table 3.3. Embedding and Extraction Times using Proposed Method

Embedded Audio File	Embedded Audio Size	Embedding Time (Sec)	ExtractionTime (Sec)
Audio 1	17 kb	0.2307	0.0823
Audio 2	100 kb	1.1376	0.4663
Audio 3	200 kb	1.9386	0.8722
Audio 4	300 kb	2.9064	1.3590
Audio 5	400 kb	3.8156	1.8726
Audio 6	500 kb	4.7021	2.3388

Table 3.3 depicts the embedding and extraction times for audio files from 17 KB to 500 KB. The embedding time ranges from 0.2307 seconds for the smallest file to 4.7021 seconds for the largest, while the extraction time ranges from 0.0823 to 2.3388 seconds. Again, this shows that the size of the audio is directly proportional to the time taken for embedding and extraction. The proposed technique is much faster in embedding and extracting when compared to other conventional techniques such as LSB.

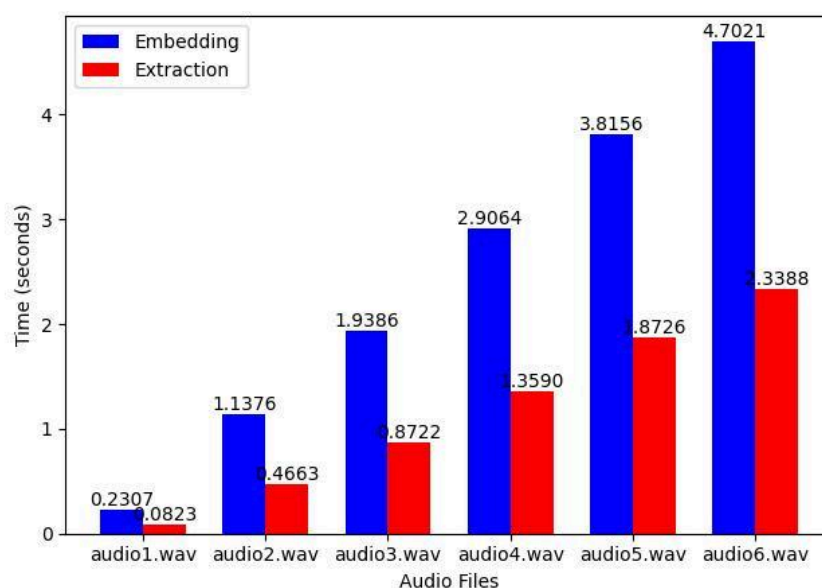


Figure 3.2: Comparison of Insertion and Extraction time using Proposed method

Table 3.4. PSNR and SSIM Values for Different Embedded Audio Sizes using Proposed Method

Embedded Audio File	Embedded Audio Size	PSNR Value (dB)	SSIM
Audio 1	17 kb	63.00	1
Audio 2	100 kb	55.07	1
Audio 3	200 kb	52.06	1
Audio 4	300 kb	50.21	1
Audio 5	400 kb	48.94	1
Audio 6	500 kb	48.11	1

It can be seen from Table 3.4 that the PSNR values range from a minimum of 63.00 dB for the smallest file to a maximum of 48.11 dB for the largest. Though there is progressive deterioration in PSNR with an increase in audio file size, the values are within permissible limits so that perceptual damage to the DICOM images is minimal.

The SSIM remains at 1.00 across all file sizes, reassuring the integrity of the structural form of the DICOM images presented in this paper. This consistency reflects that in the proposed method, very good visual and structural fidelity is there, even for larger payloads of up to 1000 KB.

The proposed scheme is highly reliable and efficient for embedding and extracting audio data within DICOM images. Ensuring a high SSIM value with acceptable ranges of PSNR, the proposed approach effectively balances security with quality and computational performance. Thus, it is very suitable for sensitive audio data in medical applications safely.

Table 3.5: Comparison of MSE for LSB and Proposed Method

Embedded Audio File	Embedded Audio Size	MSE-LSB	MSE-Proposed
Audio 1	17 kb	0.0127	0.0326
Audio 2	100 kb	0.0774	0.2023
Audio 3	200 kb	0.1550	0.4045
Audio 4	300 kb	0.2325	0.6189
Audio 5	400 kb	0.3106	0.8296
Audio 6	500 kb	0.3887	1.0058

Figure 3.3: MSE from embedding audio data using both the LSB and Proposed methods. For smaller-sized audio, such as "Audio 1" of size 17 KB, the LSB gives a low

MSE value of 0.0127, while the Proposed yields a slightly higher MSE of 0.0326. While for "Audio 2" (100 KB), the LSB method records an MSE of 0.0774, that of the Proposed method increases to 0.2023.

With the increase in size of the audio files to be embedded, a clear increasing trend in the values of MSE can be observed. For example, "Audio 3" (200 KB) gives an MSE of 0.1550 for LSB and 0.4045 for the Proposed method. The difference is heightened for big files, such as "Audio 4" at 300 KB-LSB gives an MSE of 0.2325, while in the proposed method, this is 0.6189. The MSE values are given as 0.3106 and 0.8296 for LSB and the proposed scheme, respectively, for the "Audio 5" file (400 KB).

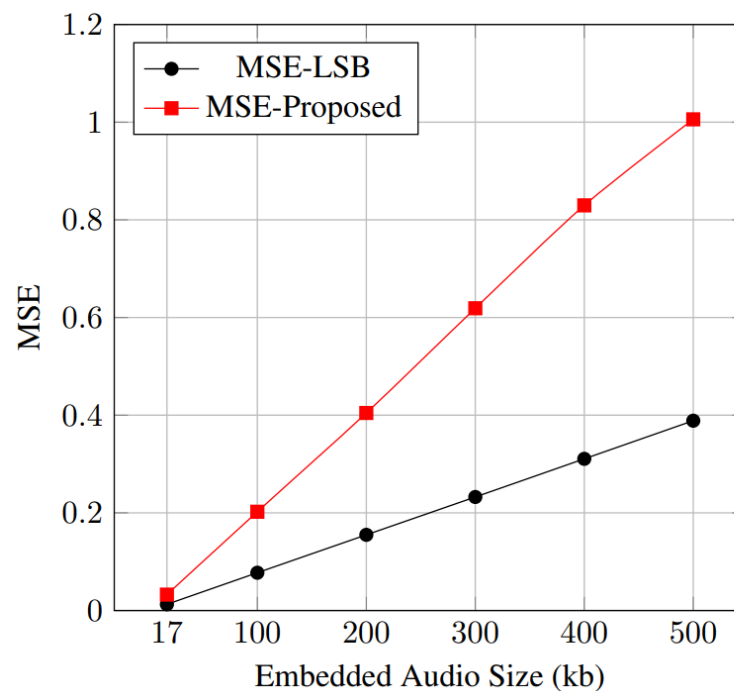


Figure 3.3: MSE Comparison Between LSB and Proposed Methods for various audio sizes

Finally, "Audio 6" of size 500 KB has a corresponding MSE of 0.3887 and 1.0058 for the LSB and Proposed methods, respectively. Results are summarized in Table 3.5, which clearly shows that the LSB technique has the least MSE value at all payload sizes, meaning minimum distortion in the host image. On the other hand, the Proposed method results in higher MSE values but allows embedding more data into an image-a desirable feature when the requirement calls for embedding a lot of data. This analysis underlines the trade-off between embedding capacity and image quality. The LSB method is more effective in applications where image fidelity is in focus, while the Proposed method provides a robust solution for embedding larger payloads, balancing capacity and security.

CHAPTER 4: CONCLUSION AND FUTURE WORK

4.1 CONCLUSION

The study will look for ways to embed and retrieve audio data in DICOM images, for the purpose of telemedicine data security. It has been found that, by making a comparison between the LSB technique and the proposed method, the latter has much better performance in terms of efficiency and data integrity. In particular, the fact that the SSIM obtained was always 1.0 and acceptable PSNR values ranging between 63.00 dB for small audio files and 48.11 dB for the bigger ones, validate the proposed approach for maintaining image quality. Moreover, the proposed methodology presents practical viability with the embedding times as low as 0.2307 seconds while starting extraction time is given as 0.0823 seconds for smaller files. Thus, all these make the method appropriate for real-world, real-time applications of telemedicine. In comparison to the embedding technique of LSB, in this proposed method, robust embedding has been done with less perceptual distortion but more structural similarity along with added security.

This work focuses on the applicability of the proposed scheme as an effective approach for embedding audio in medical images. The results emphasize the possibility of its being able to fulfill the demand for efficient and secure telemedicine systems which is continuously growing in the healthcare sector. The proposed approach forms one of the steps in securing sensitive medical data and finding a balance between efficiency and ease of implementation in this increasing digitization phase of the healthcare industry.

4.2 FUTURE SCOPE

The future of this research will be to extend the embedding techniques to include video data within DICOM images. Embedding video streams into medical images has the potential for revolutionizing telemedicine by enabling secure storage and transmission of dynamic diagnostic data, such as ultrasound recordings or procedural videos.

Also, by implementing more sophisticated steganography for embedding video, it will also avoid problems with image quality and computational efficiency, and will allow the processing of real-time data. The effect, for example, of embedding bigger payloads such as video data on the fidelity of images and extraction accuracy and performance of the system must be well investigated. Provided these issues can be addressed, embedding of video in DICOM images might enable next-generation secured integrated medical data systems.

REFERENCES

- [1] Venugopala, P. S., Raghavendra, S., Ashwini, B. (2024). CrypticCare: A Strategic Approach to Telemedicine Security using LSB and DCT Steganography for Enhancing the Patient Data Protection. *IEEE Access*.
- [2] Mosco-Garcia, J. E., Cedillo-Hernandez, M. (2024). Data Hiding Components for Solving Information Security Issues in DICOM Medical Images. In *New Trends in Intelligent Software Methodologies, Tools and Techniques* (pp. 99-109). IOS Press.
- [3] Ma, W., Wang, Y. (2024). An advanced cryptographic scheme for DICOM medical image encryption using a novel spatiotemporal chaotic lattice. *Physica Scripta*, 99(9), 095225.
- [4] Nuñez-Ramirez, D., Fragoso-Navarro, E., Mata-Mendoza, D., Cedillo-Hernandez, M. (2024). Secure management of DICOM images via reversible data hiding, contrast enhancement and visible-imperceptible watermarking. *Health and Technology*, 1-16.
- [4] Yadav, R., Singh, P. (2024). Watermarking algorithm based on phase-only CGH in fractional Hartley domain for DICOM images. *Journal of Optics*, 26(6), 065703.
- [5] Tayachi, M., Nana, L., Pascu, A., Benzarti, F. (2024). A zero-watermarking approach for DICOM images authentication based on Jacobian model. *Information Security Journal: A Global Perspective*, 1-20.
- [6] Herrmann, M. D., Clunie, D. A., Fedorov, A., Doyle, S. W., Pieper, S., Klepeis, V., ... Lennerz, J. K. (2018). Implementing the DICOM standard for digital pathology. *Journal of pathology informatics*, 9(1), 37.
- [7] Clunie, D. A. (2021). DICOM format and protocol standardization—a core requirement for digital pathology success. *Toxicologic Pathology*, 49(4), 738-749.
- [8] Paikaray, B. K., Swain, D., Chakravarty, S. (2021). Reversible selective embedding for DICOM image security and integrity using visual cryptography. *International Journal of Electronic Security and Digital Forensics*, 13(5), 498-514.
- [9] Clunie, D. A. (2000). DICOM structured reporting. PixelMed publishing.
- [10] Wu, D. C., Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern recognition letters*, 24(9-10), 1613-1626.
- [11] Hussain, M., Wahab, A. W. A., Anuar, N. B., Salleh, R., Noor, R. M. (2015, June). Pixel value differencing steganography techniques: Analysis and open challenge. In *2015 IEEE International Conference on Consumer Electronics-Taiwan* (pp. 21-22). IEEE.

- [12] Morkel, T., Eloff, J. H., Olivier, M. S. (2005, June). An overview of image steganography. In ISSA (Vol. 1, No. 2, pp. 1-11).
- [13] Kahn, D. (1996, May). The history of steganography. In International workshop on information hiding (pp. 1-5). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [14] Magdy, M., Hosny, K. M., Ghali, N. I., Ghoniemy, S. (2022). Security of medical images for telemedicine: a systematic review. *Multimedia Tools and Applications*, 81(18), 25101-25145.
- [15] Wang, Z., Byrnes, O., Wang, H., Sun, R., Ma, C., Chen, H., ... & Xue, M. (2023). Data hiding with deep learning: A survey unifying digital watermarking and steganography. *IEEE Transactions on Computational Social Systems*, 10(6), 2985-2999.
- [16] Arome, G. J. (2021). Secure Storage and Sharing of COVID-19 Data in Health Facilities using AES-Cryptography and Audio Steganography.
- [17] Abd-Eldayem, M. M. (2013). A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine. *Egyptian Informatics Journal*, 14(1), 1-13.
- [18] Alenizi, A., Mohammadi, M. S., Al-Hajji, A. A., & Ansari, A. S. (2024). A Review of Image Steganography Based on Multiple Hashing Algorithm. *Computers, Materials & Continua*, 80(2).
- [19] Meng, B., Yuan, X., Zhang, Q., Lam, C. T., & Huang, G. (2024). Encryption-then-embedding-based hybrid data hiding scheme for medical images. *Journal of King Saud University-Computer and Information Sciences*, 36(1), 101932.
- [20] Apau, R., Asante, M., Twum, F., Ben Hayfron-Acquah, J., & Peasah, K. O. (2024). Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. *Plos one*, 19(9), e0308807.