Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Image Steganography-Based Preservation of Patient Data Confidentiality in Healthcare Systems: A Survey

*Noor Alhuda Abbas Jasim [1], Suhad Ahmed Ali[2], Majid Jabbar Jawad[3]

Department of Computer Science, College of Science for Women, University of Babylon, Iraq

Email: [1] scw227.nour.alhda@student.uobabylon.edu.iq , [2] wsci.suhad.ahmed@uobabylon.edu.iq , [3] wsci.majid.jabbar@uobabylon.edu.iq

ARTICLE INFO

Received: 21 Dec 2024

Revised: 20 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

In the modern time marked by extensive digital advancement, there has been a marked increase in patient information exchanges across multiple channels in the healthcare industry. However, increased information exchanges have created extensive fears about patient information security and secrecy. The current research presents a thorough review of steganography as a technique for enhancing information secrecy in healthcare surveillance systems. Steganography is a technique in which information is embedded in pictures,

Functions serve as a novel method to ensure patient information is available only to entitled parties. The goal in this research is to consider various algorithms according to their computational complexity, solidity, and efficiency. In addition, we discuss the related ethical implications for steganography application in healthcare information, specifically in patient anonymity and information integrity preservation. From examining different research works and cases in instances, this research endeavors to provide insights for steganography application for secure information handling in healthcare surveillance systems while ensuring secrecy.

Keywords: Data Confidentiality, Healthcare Monitoring Systems, Image Steganography, Patient Information Sharing, Data Security, , Traditional Image Steganography , Coverless Image Steganography.

1. INTRODUCTION

The shift towards healthcare information technologies has greatly changed patient information management and dissemination, making healthcare providers able to retrieve this information in real time. The advancement came at a time when there were increased concerns about patient information security. The increased cases of data breaches and cyberattacks targeting healthcare organizations have raised patient information security as a major agenda in healthcare systems worldwide [1,2]. Illegal use of EHR can have serious consequences, including cases of identification deception, deception, and loss of patient trust [3]. Within this paradigm, steganography applied to pictures—a method for concealing information in digital photos—proved to be effective as a method for ensuring confidentiality in healthcare surveillance systems. For making preventing the unauthorized person from accessing to medical information, steganographic methods are used. In this method, the patient information is embedded in medical image [4]. With steganography, the security risks are ensured are minimized and while at the same time the information integrity is satisfied.

There are some works related to using steganography for preserving medical information are proposed, but have raised questions about stego-attack resilience, computational complexity, and ethical concerns, thus suggesting a need for research [5,6]. In this article, the current works of steganographic methods in medical monitoring systems will be analyzed. This article examines the

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

current methods, assessing their effectiveness, and raising meaningful questions, this research aims to establish steganography as a key element in ensuring the safe and optimal distribution of patient information. The key contributions of this survey include the following aspects:

a. **An Extensive Review of Confidentiality Matters in Data**: It appears that the questionnaire offers a comprehensive analysis of matters related to patient information handling and confidentiality in healthcare surveillance systems.

b. **Methods for Image Steganography:** The article can have a comprehensive review of the various steganography methods for hiding patient information in images in order to ensuring information transmission while the confidentiality is maintained.

c. **Evaluation of Current Methodologies**: The evaluation includes the security, effectiveness, and efficiency of contemporary steganographic techniques in preserving the confidentiality of information in healthcare systems and determine the benefits and drawbacks of each.

d. **Integration in Healthcare Environments:** explaining how to improve data security while preserving usability and delivering high-quality patient care by integrating it into current healthcare surveillance systems.

e. **Influence in Patient Information Communication:** The contributions may include information on how steganography might be used to improve the exchange of patient data between healthcare providers while simultaneously ensuring adherence to rules like HIPAA.

f. **Future Research Directions:** The survey probably recommends future lines of inquiry for improving steganography-based data confidentiality protections in the healthcare industry, taking into account new risks and technological developments.

g. **Case Studies or Applications**: It contains case studies or illustrations showing how steganographic techniques are used in real-world healthcare situations.

These contributions would provide researchers, practitioners, and policymakers with information about how to integrate cutting-edge methods to promote data confidentiality and develop effective patient care through better information exchange

2. PATIENT DATA CONFIDENTIALITY CHALLENGES IN HEALTHCARE SYSTEM

Data confidentiality is critical in healthcare due to the sensitivity of patient information. Research shows that healthcare data breaches damage medical institutions' reputations in addition to jeopardizing patient privacy [3]. Regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) emphasize how critical it is to follow safe data handling practices [1,2] highlight the weaknesses associated with electronic health records (EHRs) and the need for strong data security measures. PHI (personal health information) needs to be safeguarded against not authorized access and violations. Figure (1) shows overview of some common challenges affecting data confidentiality.

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

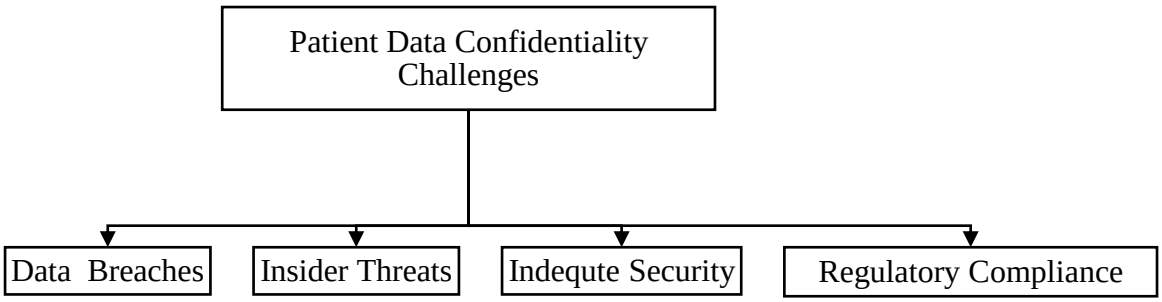

Figure (1): Some common challenges affecting data confidentiality

Below is an overview of some common challenges affecting data confidentiality:

a. **Data Breaches**: Data breaches may arise from a number of weaknesses, including as unpatched software, insecure passwords, and third-party service provider weaknesses.

b**. Insiders Threats**: Insiders or staff members who have access to private information could purposefully or inadvertently

compromise confidentiality.

c. **Inadequate Security Policies:** Organizations may lack clear and comprehensive data protection policies, leading to inconsistent practices and vulnerabilities.

d. **Regulatory Compliance Issues Description:** Challenges in complying with Regulations like the HIPAA (Health Insurance Portability and Accountability Act) .

A complete solution typically involves multiple aspects, including policies, technological safeguards, and procedures to ensure that patient data remains confidential.

3. IMAGE STEGANOGRAPHY

Image steganography is a technique for communicating that involves hiding information in an image [7]. Data could be hidden using secret message insertion by either encoding it for every bit in the image or mainly inserting it as a message in the noisy areas that represent areas that are less observed, like those with a lot of natural color variation. Additionally, because covert data may disperse randomly throughout an entire cover, Images are now the most common cover objects for steganography.

Therefore, the following sections of this study will focus on information concealment in images [8]. Image steganography is Split into two branches: Traditional Image Steganography (TIS) and Coverless Image Steganography (CIS).

3.1 Traditional Steganography for Images (TIS)

The Fig. 2 displays the general Block diagram of the (TIS). The approach frequently used in this procedure entails embedding the phrase "secret data" describes information. in which the messages sent by the individual are kept confidential. the term ‘cover image ‘refers into the image that be utilized to convey the confidential message. The term "stego image" refers to the image with hidden data. Additionally, Messages can be generated from the images themselves or put Both stego-images and cover images with the aid of a key. The receiver often employs a key if used for extracting the Stego image's secret data [9].

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

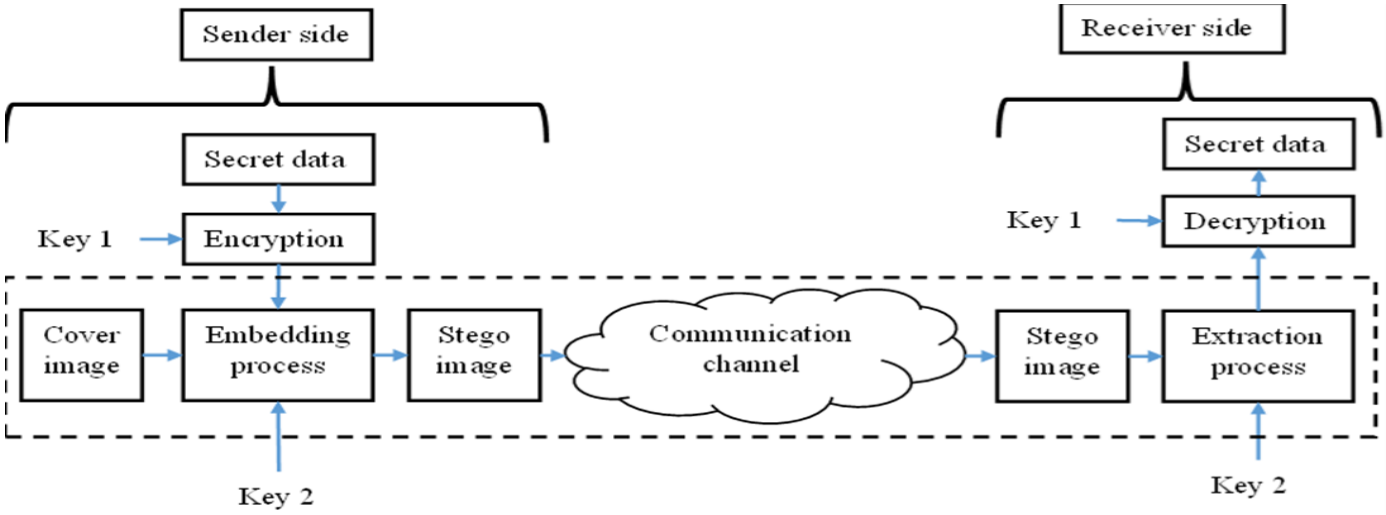

Figure (2): General form of TIS

TIS can be classified into several categories:

1. The Least Important Bit (LSB)Insertion: Its common method changes an image's least important pixel values to embed a secret

data. The alterations are often impossible for the human eye to detect.

2. Transformational Domain Methods: These methods such as the DWT (Discrete Wavelet Transform) or DCT (Discrete Cosine Transform), include manipulating the coefficients of transformed images to embed hidden information. They offer better resilience against attacks compared to LSB methods.

3. Masking and Filtering: 24 bit and grayscale images are the primary targets of masking and filtering techniques. The process of masking an image involves altering the masked area's brightness. The likelihood of detecting a change in brightness decreases with its magnitude., where the information is hidden by altering the color depths through masking and filtering processes.

In TIS, the embedding process alters the statistical characteristics, which can be detected by steganalysis methods [9]. **Traditional image steganography, however, suffers from a serious weakness in that the cover image retains the modification traces made by embedding, which renders successful steganalysis impossible [10].**

3.2 Coverless Image Steganography (CIS)

CIS, also can be called image steganography without embedding. Coverless doesn't mean there is no cover during embedding, but during embedding operation the statistical characteristics of the cover image is unaltered. This facility overcome the tampering of cover during embedding operation. An image steganography framework called coverless steganography is used to concealing the secret data by looking for appropriate images which include these data. These images are regarded as stego-images. While the carrier is still used in coverless image steganography, it is not altered. The concealed information is represented by its own features, including pixel brightness value, color, texture, edge, contour, and high-level semantics. The carrier is passed without going through the standard steganography technique's construction of the camouflage carrier (the secret information), In terms of resistance to well-known attacks including brightness change, rescaling, JPEG compression, and contrast enhancement, improving the confidentiality of information's security of the CIS framework outperforms earlier steganography techniques. Due to the fact that it is imperceptible and it cannot be read. The CIS has a lot of development potential. The fundamental concept of coverless image steganography is to examine the carrier's qualities and map them to the secret information in

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

accordance with predetermined rules based on the features' properties. The secret information can be directly represented by the carrier in this way. The stego cover is directly produced or acquired using the secret information. Despite the fact that an image is made up of only pixels and that the information they contain is completely different, but not always hold all the features in the text, according to earlier studies on the topic. Features included in the image have been proposed in the past, including SIFT, SURF, HOG, etc. Figure (3) describes the block diagram of the technique.

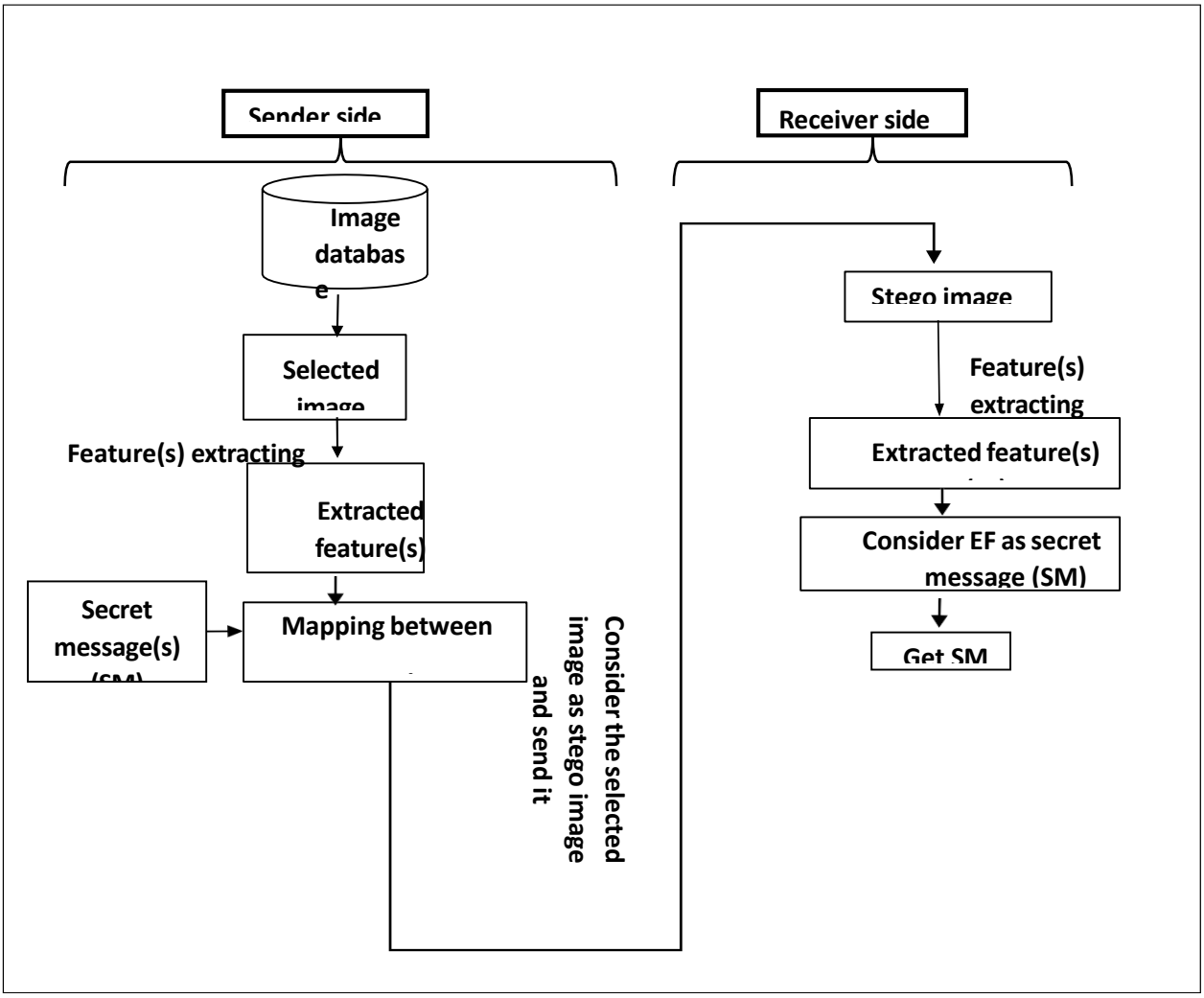

Figure (3): General form of CIS [11]

The major concern of steganography for coverless images is how to locate the cover images which already contain the secret data.

The following are coverless image steganography's main contributions:

1) The secret communication is possible without modifying the image of Stego.

2) Since the stego-image remains unaltered, the existing steganalysis tools are unable to identify confidential information.

4. SOME IMAGE STEGANOGRAPHY METHODS

Image steganography can be classified into two methods namely traditional steganography and coverless steganography.

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4.1 Traditional Image Steganography Methods

This section briefly discusses some of the Traditional image steganography methods.

In 2015, Arroba proposed a method for hiding the results of medical test in medical digital Image using digital image steganography. This method tries to improve medical data security, confidentiality and integrity. In embedding process, the cover image (the bmp-file) is processed by splitting it into blocks to facilitate data embedding. Then, text data is concealed in the least significant bits (LSBs) of the image's pixel values. The embedding image from the stego image is extracted using a key that is part of the system. In this method, ensures that the embedded data does not impact the quality of the image. The experiments were done using a cover image that was either 640 x 480-pixel grayscale or 256-color. The quality of the images was determined using the PSNR, or peak signal-to-noise ratio measure. The resultant PSNR measure of 28.722 dB was acceptable. The approach is adapted for particular resolutions and formats of the image, i.e., 8-bit, 256-color images, with the likelihood of it being limited for use with different images. The implementation of the method suffers from the need for the system for several phases such as the segmentation of the image, positional detection, and character substitution [12].

In 2020, The researchers proposed a method for hiding medical information in images using a nuclear spin generator to generate pseudorandom byte. In this method, embedding process include multiple steps: first pseudorandom bytes are generated multiple times. patient information is then encrypted using an XOR operation with the pseudorandom byte sequence. then, define the non-black pixel's input gray level [a, b] intervals, and the encrypted data is converted into a binary sequence using ASCII tables for embedding into the final pixel bits from the [a, b] interval. Finally, pixel values are adjusted if necessary to ensure they remain within the designated range. The results of high image quality are measure by using PSNR. The method is low performance with increased some cropping attack [13].

In 2020, two techniques are combined, Elliptic Curve Cryptography (ECC) and image-based steganography. The combination is used to offer a superior degree of security for protecting sensitive data. In the proposed method the dated is encrypted using ECC for ensuring strong protection through the creation of small, efficient encryption keys. Then, the encrypted data is embedded in an image using steganography method. Image with size 654x512 as cover is used in the experimental and message with length 600 characters and 101 words as secret message. Experiment results shows that this proposed method provides high security with ECC, better PSNR and requires minimal processing power, less memory, a modest amount of network connectivity, and poor communication skills. [14].

In the 2020, a robust image steganography is proposed. The proposed is based on a classical transcription of controlled alternate quantum walks (CAQWs) for secure medical image transmission in cloud-based electronic health care systems. To extract hidden images, the new steganography architecture removes the requirement for pre- or post-encryption and extraction processes, just the stego image and the CAQWs' primary states are needed. A set of simulation-based analyses on a set of grayscale and color medical images for evaluating the proposed method. A 256 × 256 and 128 × 128 cover images, and on 2-bit and 8-bit secret messages are used in the experiments. This method provides acceptable visual quality, robust security, a high embedding capacity, and resistance to data loss attacks [15].

In 2021, a Queen Traversal pattern to hide biological data using a Sudoku-based scrambling algorithm to find the pels over the DICOM image is proposed. The cover image is encrypted using A scrambling machine based on Sudoku. The Queen Traversal pattern is used to find the pels over the image channels, and for the embedding, the secret code is separated into distinct data vectors. The secret message is then embedded into the color channels of the encoded image. The image is descrambled in order to produce the stego image. The secret message is extracted using LSB methods. cover image with size 1200×1200 and secret message with length 109,200-bits are used in the

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

experiments. Experimental results show that the proposed method gives a high level of protection for the secret content without being complicated. Also, high-quality Stego images with multiple security levels is produced. [16].

In 2022, The researchers proposed a method for hiding information Confidentiality in medical images using a genetic algorithm that enables the host pixels that will embed the bits of the secret image. The method employs a private key made up of two values. In the genetic algorithm, the first is used as a seed to produce random values, while the second is made up of the host pixel positions that match the bits' values in the secret image. In this method, at the very least, the seed needs to be distributed via a secure channel. The main feature of this method is that the cover image is not modified during the image concealing process. In this method, the stenographic method based on a genetic algorithm to enhance the PSNR level reduction. The results are outstanding because the SSIM and PSNR were 1 and ∞, respectively. Since the stego image is not distorted, the mean square error is zero. [17].

In 2022, Hussah proposed a method for preserving patient Data Confidentiality using steganography. In this method, patient's personal information encoded as secret image. To satisfy security matter, the secret image of patient's personal data will be compressed and encrypted before embedding process. In the embedding process, IWT is utilized to transform the cover medical image. Then, the encrypted data will be embedded using least significant bits of cover image's coefficients, and finally the inverse IWT is used to build the stego-image. In this method, the resulted stego image suffer from insufficient quality therefore a Hybrid Fuzzy Neural Network method is applied to reduce the distortion between original and stego cover image. The experiments are done on cover image with size 512×512 and secret message with length 8 to 192 digits. The results of imperceptibility are measure by using PSNR while NCC is used for measuring secret data conditionality. The PSNR value is about 53 dB and NCC value is near 1. The method is not tested the robustness against any attacks [18].

In 2022, the researchers proposed a new approach for steganography of images utilizing a hybrid compression method integrating Discrete Wavelet Transform (DWT) with Artificial Neural Networks (ANN), and a hyperchaotic DNA sequence model. This method maintains image quality of medical image steganography with low MSE values, High PSNR value compared to existing methods and enhanced security in medical images. The cover image using this method has a PSNR of 57.21, DWT has a PSNR of 45.26, and a neural network has a PSNR of 44.26. [19].

In 2023, Partha, Pabitra and Tapas proposed a method for robust steganography employing SVM and IWT to preserve data integrity and authenticity while enhancing security and resilience. wherein the Region of Interest (ROI) and Non-Region of Interest (NROI) in the medical picture are first distinguished utilizing SVM. In order to integrate confidential information in the NROI portion of the medical image (Cover Image), IWT is then used. To make the suggested approach more robust, we have used a circular array and a secret key that is shared. In this method, the resulted stego image the high imperceptibility. The experiments are done on the cover image with 256 x 256 in size and secret message with length 512. The results of imperceptibility are measure by using (PSNR) and to evaluate the resilience utilizing the (SSIM). The PSNR value is about 64 decibels and improved robustness with a 0.96 SSIM. When the dataset is sufficiently big, the SVM classifier model may perform poorly using this method. [20].

In 2023, the researchers suggested data-hiding technique based on the Hilbert Random Secure Distribution for inserting patient secret information in a cover image MRI sample. This method integrates the most important bit (MSB) and the least important bit (LSB) steganography together with a Hilbert Random Secure Distribution model to ensure high randomness and security. By embedding sensitive patient data into MRI cover images. The key image is designed to be surprising and to allow for the safe and random distribution of secret bits to prevent the intruder's access. The experiments are done on cover image with size 125*125 and 512 *512 and 250 *250 and secret message with 1870, 7500,

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

32000 characters. This method provides high security and resistance to attacks with minimal distortion and high PSNR up to 61. This method focusses on specific image sizes and types (e.g., MRI images). So, it possible never work with other images type and sizes [21].

In 2024, the researchers proposed a method for data-hiding for DICOM medical image utilizing the HOG-LSB technique to include EPRs, or electronic patient records into medical images from DICOM, or Digital Imaging and Communications in Medicine. In this method using SHA-256 and Adversarial Neural Cryptography (ANC-SHA-256) to encrypt and hide the RGB patient image inside the Region of Non-Interest (RONI) of the medical imaging. Prior to embedding, we encrypt the RGB patient image using ANC-SHA-256. In order to confirm the authenticity and integrity of medical images, we use a safe hash technique with 256 bits (SHA-256) to create a digital signature from the data associated with the DICOM file. The experiments are done on cover image with size 56 × 56 × 3 and secret message with length 6000 bit. The Experiments were carried out to evaluate visual quality assessment using a variety of medical datasets that use ultrasound, MRI, CT, and X-rays as cover images. This method performs well in visual quality metrices, such as the PSNR average of 67.55, the NCC average of 0.9959, the SSIM average of 0.9887, the UQI average of 0.9859, and the APE average of 3.83. The suggested method is effective in telemedicine applications and provides great security with a ratio of 99% while transmitting Electronic Patient Records (EPR) remotely over the Internet. It is also robust against a variety of geometric attacks and histogram analysis [22].

In 2024, Hadjer, Okba and Ahmed proposed a method for hiding sensitive patient data within medical images with less effect on the quality of their diagnosis based on the Mask-RCNN model. The Mask-RCNN used for locating and segmenting regions within medical images that are medically less significant. The method embeds information using DCT - based steganography. The focus is on embedding within insignificant regions determined by Mask-RCNN model. The method consists of three primary steps: training neural networks to identify areas, embedding data to conceal it, and extracting embedded information. The experiments are done on cover image with size 512×512 from CT and MRI medical images. The results of imperceptibility are measure by using PSNR while NCC is used for measuring the robustness of the model and calculate how the cover and the Stego images differ from one another. The best PSNR value is about 115 db. In this method, the resulted stego image the high imperceptibility. The method has embedding capacity lower than some other techniques [23].

In 2024, the researchers proposed a method for protecting medical health records with cutting-edge steganography techniques in imaging. Using this method, medical records are first encrypted., and depending on how many multimodal medical images a patient has, the ciphertext is then divided into many pieces. In order to conceal the encrypted patient health record segment using a modified least important bit embedding procedure, a key generator chooses medical pictures at random from the multimodal image information. This method adds an added layer of protection since, even if a file ends up in the incorrect hands, and a portion of it is decoded, it won't show any information that can be understood until all the pieces of other medical photos have been recovered and put together in the right order. These experiments are done on cover image with size 240×240 and employed 21 patients' multimodal 3255 MRI images. PSNR, MSE, and SSIM were among the measures used to assess the method's robustness. The outcome display that the method is strong, and the image quality is preserved as well. high security by integrate encryption and steganography. In this method, when number of characters increases PRNR value is decrease [24].

4.2 Coverless Image Steganography

In 2024 The researchers proposed a new method for hiding information in images using Generative Adversarial Networks (GAN) with attention vectors. This method maintains important information in sensitive regions of images. The method was tested on three types of datasets: brain tumors, glaucoma, and ovarian cancer. The Results achieves high accuracy compared to other methods,

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

such as SteganoGAN, HCISNet, and CSIS, with this new method e achieving an accuracy of up to 96% in brain tumor classification. This method is ability for maintains the quality of secret images while allowing for a minimal reduction in embedding capacity (less than 2%) [25].

While traditional image steganography offers promising advantages for securing patient data in healthcare, several limitations hinder its effectiveness. Understanding these limitations is crucial for healthcare providers considering the implementation of steganographic techniques to safeguard sensitive information. The limitations can be listed as follows:

a. **Vulnerability to Detection:** Steganographic methods, particularly those that alter the least important bits of an image, can be susceptible to detection and analysis by specialized algorithms created to find hidden information. This vulnerability diminishes the efficiency of steganography as a covert method of information hiding [26].
b. **Limited Data Capacity:** Traditional image steganography methods typically have restricted data-carrying capability. The volume of data that may be integrated without substantially altering the visual appearance of the image is often minimal, which poses a challenge for healthcare applications that may require embedding substantial amounts of data [27].
c. **Quality Degradation:** Embedding data into images can lead to noticeable degradation in image quality. While techniques like DCT and DWT can mitigate this effect, there are still instances where the visual fidelity may be compromised, which can be critical in a clinical context where image interpretation is essential [28].
d. **Compatibility with Image Formats:** Some steganography techniques are format-specific, meaning that they work effectively only with certain image file types (e.g., BMP, PNG, or JPEG). This restricts their applicability in healthcare settings that utilize various imaging modalities and file formats [29,30].

Table (1.1) lists the summary of Reference #, Year, Steganography type, Size of cover, Methodology, Strength, Weakness, Dataset, Metrics, Secret Message Length.

Table 1.1: Synopsis of related works

Reference #	the year	Steganography type	Size of cover	Methodology	Strength	Weakness	Dataset	Metrics	Secret Message Length
[12]	2015	TIS	A grayscale or 256 color image (640 x 480 pixels)	LSB	- Transfer the high-security medical image along with the test results. -Simple to use,	- Complexity in Implementation because the system involves multiple steps, including image	-	- PSNR - MSE	110

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

					effective in terms of security, and capable of concealing all patient information. -Connect computer technology and medicine in a practical method to facilitate the exchange of medical data between physicians in various nations.	splitting, position finding, and character substitution -The method is designed to specific image formats and resolutions (e.g., 8-bit, 256-color images), which may limit its use with another image -Low PSNR			

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[13]	2020	TIS	336 *336 720 * 720 480 * 480	Using nuclear spin to generate pseudorandom bytes	- Minimal Distortion: Produces high PSNR values (above 113 dB), indicating minimal distortion in stego images compared to original images. - Resistance to cropping attacks, maintaining the integrity of the embedded information.	- Hardware Dependency: It relies on a nuclear spin generator, which may not be readily accessible or feasible for most users. - Resistant to some attacks, its reliance on specific techniques may introduce new vulnerabilities if exposed to advanced cryptographic attacks. -Not measures the robustness of the extracted secret message	NEMA Medical Image Database	- PSNR -MSE - BER -NCC -SSIM	83,883 260,969 116,373 (bits)

Research Article

[14]	2020	TIS	654x512	ECC encryption combined with image-based steganography.	-Security with ECC, better PSNR requires minimal processing power, less memory, a modest amount of network connectivity, and poor communication skills.	Complex Implementation	15 images: CT, MRI, X-ray	-PSNR -MSE	600 characters and 101 words
[15]	2020	TIS	128*128 256*256	(CAQWs)	- Good visual quality and resilience to attacks that cause data loss Such as (noise (add salt and pepper) and clipping) - High embedding capacity. - Robust security. - Resistan	-No need for encryption before or after embedding	Medical image dataset (color and grayscale)	NAE-IF -AD -SC, PSNR, SSIM, UIQ, NCC, and	2-bit/8-bit

					ce to som.				
[16]	2021	TIS	1200*1200	Sudoku-Queen Traversal	- Enhanced Security: The QTBCE technique combines encryption and steganography, providing multi-layered security for sensitive medical data. -Content Confidentiality: The use of Queen Traversal for pixel access allows for effective hiding of medical history, enhancing confidentiality.	-Data Capacity Constraints: The capacity for data embedding may be limited due to the partitioning of secret content and the channel limitations, potentially restricting the amount of content that can be hidden. - Potential for Image Quality Degradation: Despite efforts to maintain quality, there might still be some degradation in	Biomedical DICOM image	- PSNR -MSE - Content Embedding and Extraction Time	109,200-bits

Research Article

						stego-image perceived by users.			
[17]	2022	TIS	-	Genetic Algorithm for Pixel Selection	-No alteration of cover image -high PSNR -MSE = 0 -SSIM = 1	- The seed needs to be distributed via a secure method.	30 medical images	-PSNR -SSIM -MSE	-
[18]	2022	TIS	512*512	IWT-LSB	-Quality Preservation: Techniques such as Using IWT, or the Integer Wavelet Transform to maintain the quality of medical images, which is critical in healthcare settings where image	-Not test towards robustness. -Need Quality enhancement of stego-image (High-quality images are often required for embedding without distorting the original content, which may	-	-PSNR -MSE -NCC	8 and 192 digits

Research Article

					integrity is paramount. -The method is adaptable to various kinds of data. (e.g., grayscale and color images) and can accommodate various embedding techniques, enhancing its applicability to diverse healthcare scenarios. -The result shows that the suggested method can conceal secret data with	restrict the use of lower-quality images common in some healthcare settings). - Potential for Data Loss			

Research Article

					large length.				
[19]	2022	TIS	-	Hybrid compression using DWT, Neural Network, and DNA sequence of hyper chaos	- Maintain image quality. - Low MSE values. - High PSNR value compared to existing methods. - Enhanced security in medical images	- it possible effect on sensitive components of a medical image	Medical images	-PSNR -MSE -NCC -AD -SC -NAE	-
[20]	2023	TIS	256×256	SVM – IWT	- Enhanced Security: Utilizing a shared secret key and a	- Weakness in robustness toward some attacks such as	medical Images: Breast MRI from TCGA	- PSNR - SSIM - BER - NCC	512

Research Article

					circular array for embedding increases the security of the embedded information, making it less susceptible to unauthorized extraction. The suggested method achieves a high peak signal to noise ratio (PSNR) of 64 db. -, indicating that the confidential data may be incorporated with minimal visible distortion to the cover image.	JPEG compression (40%), Histogram equalization, and Rotate (90). - When the dataset is sufficiently big, the SVM classifier model may perform poorly using this method. - Computational complexity, dependence on image characteristics, and potential misclassification issues	- BRCA, 500 images. of 50 women patients		

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[21]	2023	TIS	125x125250x250 512x512	Hilbert Convex Similarity with random distribution With LSBHRSD, MSBHRSD	-High security, resistance to attacks, minimal distortion - High PSNR up to 61	-Focus on specific image sizes and types (e.g., MRI images). So it possible never work with other images type and sizes	MRI samples, 10 images	-PSNR -MSE -PRD -SSIM	1870, 7500, 32000 characters
[22]	2024	TIS	56×56× 3	HOG-LSB	- Reduced Visual Distortion: Changes made in RONIs are less likely for HVS, or the Human Visual System) to perceive, maintaining visual quality. -Strong against geometric and histogram	- Limited Embed Capacity: Only certain regions are used for data hiding, potentially limiting the total available space for embedding. - Dependence on Accurate segmentation of RONIs: Incorrect identification of RONIs	- MRI, CT, X-ray, and ultrasound medical image	- PSNR -MSE -NCC -UQI - APE	6000 bits

					analysis and physical adjustments. - Efficient Storage of EPR: By utilizing RONIs, electronic patient records (EPRs) can be stored within the images without degrading the efficiency of medical image processing.	can lead to unusable data or impact visual quality.			
[23]	2024	TIS	512*512	Mask RCNN – DCT	- DCT embedding in mid-frequency components ensures minimal perceptible changes, preserving image quality.	-Reliance on the accuracy of Mask-RCNN; if it misidentifies regions, it could lead to data loss or image degradation.	- Images of CT - Images of MRI	- PSNR - NCC - IoU	-

Research Article

					- Improves the selection process using texture and complexity evaluation, further reducing detection risks.	- Alterations in the chosen areas might still affect minor image quality, potentially risking diagnostic utility.			
[24]	2024	TIS	240 * 240	LSB	-High security by integrate encryption and steganography -Using a updated methods for Least Significant Bits (LSBs)	-When number of characters increases PRNR value is decrease. - Relies on the availability of multiple.	BraTS	- PSNR -SSIM -MSE	-
[25]	2024	CIS	240*240	AVG-GAN	Maintains important informtion in picture sensitive areas .	Reduction in embedding capacity (less than 2%).	-Brain tumors. - Glaucoma. -An ultrasound ovarian cancer medical	-RS -BPP - WPSNR - SSIM - PSNR	-

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

							image .		

4.3 Challenge against applying CIS in medical field

The similarity and correlation between the medical images are high. It is highly likely that the same hash sequence will be produced by various images. The features of medical pictures differ from those of natural pictures. Typically, Grayscale medical pictures have a black backdrop. and various elements within these images can have comparable gray-scale values. Additionally, the medical imaging process can introduce noise, artifacts, and geometric distortions. As a result, current algorithms for coverless steganography designed for natural pictures cannot be directly applied to medical pictures.

5. APPLICATIONS STEGANOGRAPHY'S USE IN HEALTHCARE MONITORING SYSTEM

The integration of Steganography's Use in Healthcare monitoring systems presents several benefits:

a. **Secure Patient Data Transmission:** Studies indicate that steganography can significantly improve the security of patient data during transmission over insecure channels [31]. By embedding data within images, the risk of interception is minimized.
b. **Patient Confidentiality Preservation:** Image steganography can ensure that sensitive information is only accessible to authorized personnel. reference [5] highlight case studies where steganography has been successfully employed to protect patient confidentiality in telemedicine.
c. **Data Integrity and Authentication:** Some studies suggest that steganographic techniques can also serve as a means of data integrity verification. The embedded information can be checked for authenticity, ensuring that the transmitted data has not been altered [32].

6. IMPACT ON PATIENT INFORMATION SHARING

In the modern healthcare landscape, the sharing of patient data between medical professionals is vital for delivering high-quality care. However, this sharing often includes sensitive data that need to be safeguarded in order to abide by regulations such as HIPAA, the Health Insurance Portability and Accountability Act). Steganography offers excellent ways for improving patient information exchange while preserving data privacy.

a. **Facilitation of Secure Communications:** Steganography can improve the healthcare professional communications security by hiding secret patient information inside items, such photos or audio recordings. Steganography makes it more difficult for unauthorized people to obtain data by transparently hiding it. For example, according to a study by AlEisa HN [33], which examines the applicability of steganography in the security of medical records used in telemedicine, the capacity to transmit encrypted data hidden in innocuous images can significantly decrease the risk of data breaches during transmission.

b. **Ensuring HIPAA implementing:** The HIPAA places strict requirements on the handling and sharing of patient data, requiring healthcare providers to institute proper measures to maintain confidentiality and security. By applying steganography to embed patient information, Healthcare

institutions can improve information exchange efficacy while guaranteeing compliance with HIPAA. Dholakia et al. [34] argued that the use of steganographic methods can offer an additional layer of security, as information that is not perceptible reduces the likelihood of unauthorized disclosure, which aligns with HIPAA's emphasis on protection personal health information (PHI).

c. **Improved Collaboration Among Healthcare Professionals:** Using steganography technique can improve the health professionals, where the exchanging sensitive can be implemented securely among professional. A study proposed by reference [35] showed that the steganography which is used in health systems to transmit patient condition updates at the time of occurrence, facilitates the integration of these updates into regular communication channels. So, the procedure helps health teams make the best decisions possible by giving them fast and accurate information while avoiding the needless disclosure of private information.

d. **Challenges and Considerations:** Implementing steganography in healthcare information systems presents difficulties despite its benefits. Because steganographic methods are complicated, some healthcare organizations may be discouraged from adopting them, particularly if they lack technical expertise. Additionally, Kumar et al. [36] raised issues with detection, pointing out that although steganography might protect data from unauthorized users, it may still be susceptible to sophisticated forensic techniques used to reveal hidden data. This challenge necessitates continuing valuation and refinement of steganographic methods to keep pace with developing cybersecurity threats.

e. **Ethical Implications and Trust Factors:** The ethical consequences of the application of steganography in patient information sharing must be examined thoroughly. Though steganographic techniques offer improved confidentiality, medical practitioners must be careful to ensure that their utilization does not undermine patients' trust. According to Rana et al. [37], informing patients on how their information is managed, even with the use of such sophisticated techniques as steganography, is vital to sustaining patients' trust in medical practitioners.

7. FUTURE RESEARCH DIRECTIONS FOR HEALTHCARE DATA CONFIDENTIALITY WITH STEGANOGRAPHY

With increased reliance of the healthcare sector on online platforms for patient data management and communication, data integrity and confidentiality have become absolutely essential. Steganography offers a potentially useful approach for enhancing these security measures; nevertheless, with advancements in technology on the rise and new threats evolving, an evolving research model for future research is imperative. Below are key areas of focus for future research efforts on the use of steganography in the field of healthcare based on recent advances in technology and evolving cybersecurity threats.

a. **Hybrid Security Models:** Subsequent research can explore the development of hybrid models that integrate steganography with cryptographic techniques with other safety mechanisms. Researchers should evaluate the viability of such integrated technologies for providing complete safety frameworks for patient details. A study by Gaur et al. [38] showed that combining steganographic techniques with encrypting mechanisms could significantly increase safety by adding several levels of safety, making unauthorized access virtually impossible.

b. **Adaptive Steganography Techniques**: With the development of machine learning and data analytics, the exploration of adaptive steganography techniques tailored to specific data types (e.g., images, text, electronic health records) offers a rich avenue for research. The work of Rezaei, S., Javadpour [39] emphasizes the ability of intelligent algorithms to adjust steganographic methods in real-time according to the context and level of data sensitivity being shared.

c. **Embedded System Security:** As healthcare increasingly incorporates IoT, or the Internet of Things devices, the requirement for safe information transmission among these devices turn into urgent.

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Future studies could concentrate on creating steganographic systems specifically designed for Internet of Medical Things (IoMT) devices, as suggested by Bhaduri et al. [40]. Such research could address how to embed sensitive health information within operational data or diagnostic outputs from medical devices, ensuring that even if these devices are hacked, critical patient data remains concealed.

d. **Detection and Robustness Against Attacks:** The identification of new threats highlights the need for detection techniques that increase the resilience of steganographic mechanisms toward detection and attack of different types. Work by Anwar et al. [41] highlights the need for the development of techniques that are robust toward revealing content that threatens patient confidentiality by using highly sophisticated forensic tools.

e. **Ethical and Regulatory Considerations:** As the health industry increasingly incorporates steganographic tools, it is critical that scholarship simultaneously explores the ethical and regulatory implications of these tools. Examining topics like patient consent, data ownership, and compliance with rules such as HIPAA is essential to ensuring that intricate data-protection systems are in line with moral standards in the medical field. According to Xiang et al. [42], in order to ensure data security, ethical frameworks and compliance should stay up to date with developments in computer science tools.

f. **Educational Frameworks for Healthcare Professionals:** It is necessary to create educational frameworks that educate healthcare personnel on the value of data confidentiality and steganography. Nadhan and I. Jeena [43] contend that training programs focused on novel technologies, including steganography, will allow healthcare workers to adhere to confidentiality standards and embrace innovative solutions efficiently.

APPLICATIONS OF STEGANOGRAPHY IN HEALTHCARE: CASE STUDIES AND EXAMPLES

The implementation of steganographic techniques in actual healthcare scenarios is a promising frontier for enhancing data security and confidentiality. Applications and case studies demonstrating the efficient use of steganography are essential for comprehending its usefulness in protecting sensitive information as healthcare professionals progressively digitize patient records and communications. Here are several case studies and instances that show the successful implementation of steganography in various healthcare contexts.

a. **Telemedicine Security**: In a case study carried out by Duy and others. [44], steganography had been employed to secure telemedicine communications. Patients often share sensitive healthcare information with workers through video calls and messaging applications. The study showed how medical information, such as diagnostic reports, could be included in video files, offering a secure way to share information without sacrificing communication quality. The researchers highlighted an important reduction in unauthorized data access during trials of this steganographic method, emphasizing its efficacy in real-world telehealth applications.

b. **Secure Patient Record Sharing**: A practical application was reported by Tahir et al. [45], where steganographic methods were utilized within an electronic health record (EHR) system to enhance patient data confidentiality. In this study, patient medical histories and treatment plans were embedded within standard patient pictures (e.g., MRIs or x-rays) used for tele-radiology. This method not only protected sensitive data through transmission but also guaranteed that medical personnel could retrieve necessary information efficiently during a specially designed application.

c. **Data Integrity Validation** :In another study by Hashim et al. [46], steganography was used for both data protection and integrity validation of patient information in hospital management systems. The researchers implemented a system where critical patient data (e.g., medication schedules) was embedded in images transmitted from pharmacies to hospitals. Besides securing the data exchange, the embedding process enabled checksum verification, ensuring that the data had not been altered in transit, thereby enhancing trust in health information systems.

d. **Embedding Health Alerts in Medical Imagery** :An innovative application discussed by Bhatt et al. [47] involved embedding critical health alerts into medical images using steganography. In this case, automatic systems were set up to analyze images obtained from diagnostic devices (e.g., MRIs, CT

scans) and embed emergency alerts for healthcare professionals within these images. For instance, if an analysis detected abnormal results requiring urgent attention, a message could be embedded within the accompanying image, ensuring that crucial information remained secure, yet accessible within the context of medical practice.

e. **Enhancing Confidentiality in Patient Surveys :**A case study carried out by Baig et al. [47] explored the application of steganography in enhancing the confidentiality of patient surveys conducted online. The researchers embedded survey responses within non-sensitive images, ensuring that even if the survey data was intercepted, the actual responses would remain hidden. This technique was particularly effective in locations where patient confidentiality is critical, such as mental health assessments.

CHALLENGES AND ETHICAL CONSIDERATIONS

Steganography technique may offer benefits to healthcare system, but there are a number of problems must be resolved:

a. **Detection and Countermeasures:** According to reference [48], steganographic content can be disclosed via strong detection techniques, which could risk data secrecy. In order to overcome this challenge, more reliable steganography methods must be periodically improved.

b. **Regulatory Compliance:** Implementing steganography in the healthcare industry needs adherence to regulatory standards, which can differ depending on the country. The significance of conforming steganographic procedures to HIPAA and GDPR regulations in order to guarantee legal compliance is highlighted by Kwon et al. [49].

c. **Ethical Concerns:** It is critical to consider the ethical implications of patient autonomy and informed consent. Steganography shouldn't ever interfere with a patient's right to know how their information is used and shared [50].

DISCUSSION

In the healthcare industry, data confidentiality is crucial, especially as the sector continues to adopt digital solutions for sharing patient data. As telemedicine, electronic medical records (EHRs), and Internet of Medical Things (IoMT) applications grow in popularity, maintaining the privacy of sensitive patient data becomes a pressing challenge. By embedding the sensitive data into medical photographs, image steganography presents a promising method for protecting patient data, guaranteeing safe communication and adherence to regulations such as HIPAA. Applying steganography in healthcare monitoring systems is still evolving, several key research questions can guide further exploration in this field:

Research Questions	Answers
Q1: What are the current methodologies of image steganography used to enhance confidentiality of data in healthcare monitoring systems?	Current methodologies include insertion of transform domain methods (such the DWT and DCT), LSB, masking, and adaptive steganography. Every method has its own advantages and disadvantages, although transform domain techniques typically offer more manipulation resistance. According to studies, these approaches can be tailored especially for use in healthcare applications, improving the security of EHR sharing and telemedicine [51].
Q2: How effective is image steganography in preserving the quality of medical images while ensuring data confidentiality?	Image steganography aims to preserve image quality while making hidden data undetectable. Research show that techniques like DCT and DWT can successfully conceal data with few visual changes. According to studies, well-designed steganographic systems can

Journal of Information Systems Engineering and Management
2025, 10(50s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	make trade-off between high embedding capabilities and high quality of medical images, which makes them suitable for uses like remote diagnostics [52].
Q3: What are the main obstacles to the adoption of steganography in medical care monitoring systems?	The primary challenges to applying steganography in healthcare include awareness and understanding of the technology among healthcare providers, concerns about detection and potential data hacking, and the need for compliance with various regulations. Also, worries about installation complexity and potential effects on healthcare monitoring systems' performance may prevent broader adoption. Overcoming these challenges needs healthcare professional-focused training and education programs [53].
Q4: How can combining image steganography with other technologies (e.g., blockchain, AI) to enhance the data confidentiality in healthcare?	Combining steganography with blockchain technology can greatly improve data confidentiality by ensuring tamper-proof records and safe data embedding. Blockchain can monitor hidden data integrity, while AI can maximize steganographic techniques' efficacy and flexibility. This integrated approach may lead to perfect solutions for safe patient data exchange, strengthening the system's resistance to different security risks [40].
Q5: What extent does user perception influence the implementation of steganography in healthcare monitoring systems?	The way users perceive new technologies is a major factor in their readiness to accept them. Studies suggests that positive perceptions about the benefits of steganography, like enhanced patient confidence and improved patient trust, may promote adoption. However, applying steganography technique may be hampered by false beliefs about its efficacy and complexity. Programs for healthcare personnel to learn could increase acceptance rates, which would make it easier to integrate steganography into healthcare systems more generally [34].

CONCLUSIONS

Steganography can preserve the patient confidentiality and data security in the healthcare industry. By embedding sensitive information in secure files, it facilitates safe and simple data sharing while adhering to confidentiality rules like HIPAA. However, issues with detection risks need to be resolved. Therefore, ongoing research and development is necessary to ensure that this technology may be applied in healthcare in the future in a safe and efficient manner.

a. Steganography has a great deal of promise to improve security and HIPAA compliance when used in patient information sharing. Healthcare organizations can improve information flow while maintaining patient confidentiality by embedding sensitive information with ordinary data. To optimize the advantages of this cutting-edge technology, stakeholders must continue to be alert about implementation difficulties, detection risks, and ethical issues. To guarantee that the incorporation of steganography into healthcare systems improves patient care while respecting the values of secrecy and trust, more study and development will be necessary.

b. Robust data confidentiality procedures are more significant than ever as technological developments continue to influence the healthcare industry. Steganography technique offers excellent chance to preserved patient information. However, tackling the changing threats in the healthcare environment will require more studying in the healthcare field like hybrid security models, adaptive techniques, IoMT security, attack resilience, ethical considerations, and professional training. In a rapidly evolving digital world, practitioners and researchers can collaborate to improve the confidentiality and integrity of sensitive patient data by concentrating on these research directions.

c. Steganography's real-world uses in healthcare demonstrate how it can greatly improve patient confidentiality and data security. EHR systems, telemedicine, integrity verification, medical imaging, and patient evaluations are just a few of the case studies that show how embedding private data in harmless files can improve healthcare compliance with data protection laws like HIPAA and promote efficient communication between medical professionals. In order to address new cybersecurity risks and preserve patient confidence in digital healthcare solutions, it is imperative that these methods be continuously investigated in a variety of healthcare sceneries. Future studies should keep looking at cutting-edge uses and the long-term effects of implementing steganographic techniques in healthcare systems.

d. The discussion and research questions highlight the importance of image steganography in preserving data confidentiality in healthcare monitoring systems. Integrating steganography and comprehending user perceptions are essential for improving patient information exchange securely as the healthcare landscape changes. In order to further progress data confidentiality in healthcare, future works should focus on addressing current challenges and investigating new technological combinations.

REFERENCES

[1] Stoumpos AI, Kitsios F, Talias MA. Digital Transformation in Healthcare: Technology Acceptance and Its Applications. Int J Environ Res Public Health. 2023 Feb 15;20(4):3407. doi: 10.3390/ijerph20043407. PMID: 36834105; PMCID: PMC9963556.

[2] Metty Paul, Leandros Maglaras, Mohamed Amine Ferrag, Iman Almomani, Digitization of healthcare sector: A study on confidentiality and security concerns, ICT Express, Volume 9, Issue 4, 2023.

[3] Basil NN, Ambe S, Ekhator C, Fonkem E. Health Records Database and Inherent Security Concerns: A Review of the Literature. Cureus. 2022 Oct 11;14(10):e30168. doi: 10.7759/cureus.30168. PMID: 36397924; PMCID: PMC9647912.

[4] Usman, Muhammad Arslan & Usman, Muhammad Rehan. (2018). Using image steganography for providing enhanced medical data security. 1-4. 10.1109/CCNC.2018.8319263.

[5] Yanuar, M.R.; MT, S.; Apriono, C.; Syawaludin, M.F. Image-to-Image Steganography with Josephus Permutation and Least Significant Bit (LSB) 3-3-2 Embedding. Appl. Sci. 2024, 14, 7119. https://doi.org/10.3390/app14167119

[6] Aleisa, Hussah. (2022). Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things. Journal of Healthcare Engineering. 2022. 1-11. 10.1155/2022/7528583.

[7] M. Y. Valandar, P. Ayubi, and M. J. Barani, “A new transform domain steganography based on modified logistic chaotic map for color images,” Journal of Information Security and Applications, vol. 34, pp. 142–151, Jun. 2017, doi: 10.1016/j.jisa.2017.04.004.

[8] Boryczka, Mariusz, and Grzegorz Kazana. 2023. "Hiding Information in Digital Images Using Ant Algorithms" Entropy 25, no. 7: 963. https://doi.org/10.3390/e25070963

[9] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, “Coverless Image Steganography: A Survey,” IEEE Access, vol. 7, pp. 171372–171394, 2019, doi: 10.1109/ACCESS.2019.2955452.

[10] W. Wen, H. Huang, S. Qi, Y. Zhang, and Y. Fang, “Joint Coverless Steganography and Image Transformation for Covert Communication of Secret Messages,” IEEE Trans Netw Sci Eng, pp. 1–12, 2024, doi: 10.1109/TNSE.2024.3354941.

[11] Mangi, Hadeel & Ali, Suhad & Jawad, Majid. (2023). Enhancing of coverless image steganography capacity based on image block features. TELKOMNIKA (Telecommunication Computing Electronics and Control). 21. 1364. 10.12928/telkomnika.v21i6.24816.

[12] O. I. AlFarraji, " Hiding The Results of Medical Test in Medical Digital Image", Journal of Engineering Research and General Science, vol.3, no.5 , pp. 2091-2730 , 2015.

[13] B. Stoyanov and B. Stoyanov, "BOOST: Medical image steganography using nuclear spin generator" , *Entropy*, vol. 22 , pp. 501, 26 2020.

[14] Eshraq S. Bin Hureib1† and Prof. Adnan A. Gutub "Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography." IJCSNS International Journal of Computer Science and Network Security, Vol. 20, No. 8, August 2020.

[15] B.A.El-Atty , A. M. Iliyasu , H.Alaskar and A. A. A. El-Latif " A Robust Quasi-QuantumWalks-based Steganography Protocol for Secure Transmission of Images on Cloud-based E-healthcare Platforms", Sensors ,

vol. 20, no. 11, p. 3108, May 2020 , 31 2020 .

[16] R. B. Krishnan , N. R. Kumar , N. R. Raajan,G. Manikandan , A. Srinivasan ,D. Narasimhan , " An Approach for Attaining Content Confidentiality on Medical Images Through Image Encryption with Steganography" , Wireless Personal Communications, 22 2021 .

[17] E. Vazquez , S. Torres , G. Sanchez , J-G. Avalos , M. Abarca , T. Frias, E. Juarez , C.Trejo , &D. Hernandez , "Confidentiality in medical images through a genetic-based steganography algorithm in artificial intelligence" , *Frontiers in Robotics and AI*, pp. 1031299, 06 2022.

[18] H. N. AlEisa, "Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things", Journal of Healthcare Engineering, pp. 7528583, 06 2022.

[19] V. Seenappa1, N. C. Krishnappa , P. K. Mallesh2, " Hybrid Compression and DNA Sequence of Hyper Chaos System for Medical Image Steganography ", International Journal of Intelligent Engineering and Systems,

Vol.15, No.3, 6 2022 .

[20] P. Chowdhuri, P. Pal, and T. Si, "A novel steganographic technique for medical image using SVM and IWT" ,*Multimedia Tools and Applications*, pp. 20497-20516 , 06 2023.

[21] Hussein K. Alzubaidy , D. Al-Shammary , M. H. Abed, Ayman Ibaida , And K. Ahmed " Hilbert Convex Similarity for Highly Secure Random Distribution of Patient Privacy Steganography " . Digital Object Identifier, vol. 11, pp. 115816–115827, 18 2023 .

[22] M .A. Hameed , M. Hassaballah , R. Abdelazim , A.K. Sahu , " A novel medical steganography technique based on adversarial neural cryptography and digital signature using least significant bit replacement", *International Journal of Cognitive Computing in Engineering ,pp.* 127, PII: S2666-3074(24)00030-5 , 13 2024 .

[23] H. Saidi, O. Tibermacine, and A. Elhadad, "High-capacity data hiding for medical images based on the Mask-RCNN model" , *Scientific Reports*, pp. 14- 7166, 26 2024.

[24] G. Latif , J. Alghazo, N. Mohammad,S.E. Abdelhamid , G.B. Brahim , K. Amjad , " A Novel Fragmented Approach for Securing Medical Health Records in Multimodal Medical Image" Applied Sciences , pp. 14(16), 6293 . 19 2024.

[25] A. Virupakshappa, & D.S. Uplaonkar , " Deep learning-based coverless image steganography on medical images shared via cloud" , *Engineering Proceedings*, pp.59,176 , 18 2024 .

[26] Chang, C. C., Wu, P. H., & Chang, C. Y. (2001). An improved LSB image hiding method. Proceedings of the International Conference on Signal Processing Applications and Technology.

[27] Saidi H, Tibermacine O, Elhadad A. High-capacity data hiding for medical images based on the mask-RCNN model. Sci Rep. 2024 Mar 26;14(1):7166. doi: 10.1038/s41598-024-55639-9. PMID: 38531893; PMCID: PMC10966061..

[28] Lin, Shinfeng & Shie, Shih-Chieh & Guo, J.Y.. (2010). Improving the robustness of DCT-based image watermarking against JPEG compression. Computer Standards & Interfaces. 32. 54-60. 10.1016/j.csi.2009.06.004..

[29] Sinha, Bimal Kumar. "Comparison of PNG & JPEG Format for LSB Steganography." (2015).

[30] Elgabar, Eltyeb E. A bed. "Comparison of LSB Steganography in BMP and JPEG Images." (2013)

[31] Atiyah, Rana & Shadeed, Intisar. (2022). Security and Confidentiality in IoT Healthcare System: A systematic review. Journal of Al-Qadisiyah for Computer Science and Mathematics. 14. 10.29304/jqcm.2022.14.1.882.

[32] M. Ahmad Bamanga, A. Kamalu Babando, and M. Ahmed Shehu, 'Recent Advances in Steganography', Steganography - The Art of Hiding Information. IntechOpen, Mar. 14, 2024. doi: 10.5772/intechopen.1004521.

[33] AlEisa HN. "Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things". J Healthc Eng. 2022 May 6;2022:7528583. doi: 10.1155/2022/7528583. PMID: 35571336; PMCID: PMC9106500..

[34] Kumar P. P, Raj E. B. An Enhanced Cryptography for ECG Steganography to Satisfy HIPAA Confidentiality and Security Regulation for Bio-Medical Datas. Biomed Pharmacol J 2016;9(3).

[35] Nagamany Abirami, M. S. Anbarasi, "An Efficient Multilayer approach for Securing E-Healthcare Data in Cloud using Crypto – Stego Technique," Engineering World, vol. 6, pp. 128-135, 2024, DOI:10.37394/232025.2024.6.13

[36important] Mohamed Abdel Hameed, M. Hassaballah, Riem Abdelazim, Aditya Kumar Sahu,

A novel medical steganography technique based on Adversarial Neural Cryptography and digital signature using least significant bit replacement, International Journal of Cognitive Computing in Engineering, Volume 5, 2024, Pages 379-397, ISSN 2666-3074, https://doi.org/10.1016/j.ijcce.2024.08.002.

[37] Komalasari, Rita. "Machine Learning in Health Information Security: Unraveling Patterns, Concealing Secrets, and Mitigation." Enhancing Steganography Through Deep Learning Approaches, edited by Vijay Kumar, et al., IGI Global, 2025, pp. 139-164. https://doi.org/10.4018/979-8-3693-2223-9.ch006

[38] Sambyal, Sidhant & Arora, Bhavna. (2023). Hybrid Security Model for Securing Healthcare Data on Cloud. 10.21203/rs.3.rs-2908979/v1.

[39] Rezaei, S., Javadpour, A. Bio-Inspired algorithms for secure image steganography: enhancing data security and quality in data transmission. *Multimed Tools Appl* **83**, 82247–82280 (2024). https://doi.org/10.1007/s11042-024-18776-x

[40] Joseph B. Awotunde, Idowu D. Oladipo, Muyideen AbdulRaheem, Ghaniyyat B. Balogun, and Adekola R. Tomori , "An IoMT-based steganography model for securing medical information "International Journal of Healthcare Technology and Management 2022 19:3-4, 218-236

[41] Hashim, M. M., Rhaif, S. H., Abdulrazzaq, A. A., Ali, A. H., & Taha, M. S. (2020, July). Based on iot healthcare application for medical data authentication: Towards a new secure framework using steganography. In IOP Conference Series: Materials Science and Engineering (Vol. 881, No. 1, p. 012120). IOP Publishing.

[42] Bamanga, Mahmud Ahmad, and Aliyu Kamalu Babando. "Recent Advances in Steganography." Steganography-The Art of Hiding Information: The Art of Hiding Information (2024): 23.

[43] Nadhan, Archana S., and I. Jeena Jacob. "Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications." Biomedical Signal Processing and Control 88 (2024): 105511.

[44] Duy, Liem & Minh, Thy & Huynh Thanh, Tu. (2017). Adaptive steganography technique to secure patient confidential information using ECG signal. 336-340. 10.1109/NAFOSTED.2017.8108088.

[45] Tahir, Mohammed Y., Maurice Mars, and Richard E. Scott. "A review of teleradiology in Africa–Towards mobile teleradiology in Nigeria." SA Journal of Radiology 26.1 (2022): 2257.

[46] Hashim, M. M., et al. "Securing medical data transmission systems based on integrating algorithm of encryption and steganography." 2019 7th International Conference on Mechatronics Engineering (ICOM). IEEE, 2019.

[47] Baig, Mirza Mansoor, and Hamid Gholamhosseini. "Smart health monitoring systems: an overview of design and modeling." Journal of medical systems 37 (2013): 1-14.

[48] Provos, Niels & Honeyman, Peter. (2001). Detecting Steganographic Content on the Internet.

[49] Kwon J, Johnson ME. Security practices and regulatory compliance in the healthcare industry. J Am Med Inform Assoc. 2013 Jan 1;20(1):44-51. doi: 10.1136/amiajnl-2012-000906. Epub 2012 Sep 6. PMID: 22955497; PMCID: PMC3555315.

[50] Olejarczyk JP, Young M. Patient Rights and Ethics. [Updated 2024 May 6]. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2025 Jan-. Available from: https://www.ncbi.nlm.nih.gov/books/NBK538279/.

[51] Mansour, Romany F., and Moheb R. Girgis. "Steganography-Based Transmission of Medical Images Over Unsecure Network for Telemedicine Applications." Computers, Materials & Continua 68.3 (2021).

[52] Hussien, Amar. (2022). Image Steganography Based Spatial and Transform Domain Techniques: A Review. Fusion: Practice and Applications. 8. 08-15. 10.54216/FPA.080101.

[53] AMUSAN, Elizabeth Adedoyin, Oluwaseun Modupe ALADE, and Justice Ono. "Model For Secure Transmission Of Medical Telemonitoring Data Using Crypto-Stegano Techniques." University of Pitesti Scientific Bulletin Series: Electronics and Computer Science 24.1 (2024): 1-10.