Applications of Steganography in Healthcare sector

Bini M Issac
Dept. of CSE
Amal Jyothi College of Engineering
Kottayam,India
binimissac@amaljyothi.ac.in

S N Kumar
Dept. of EEE
Amal Jyothi College of Engineering
Kottayam,India
appu123kumar@gmail.com

***Abstract*—Securing data in the healthcare industry is of utmost importance for several reasons. Healthcare data is highly sensitive, containing personal and confidential information about patients. Protecting this data is essential to ensure that patient privacy is not violated. It is crucial to ensure that the data is only accessed by authorized individuals and that it is not lost, stolen, or compromised. Healthcare organizations are subject to numerous regulations that require them to protect patient data. Also, Healthcare data is a valuable target for cybercriminals, who can use it for identity theft and other fraudulent activities. Securing patient data can help prevent such crimes and protect patients' identities. Healthcare data is essential for providing quality patient care. Securing this data ensures that healthcare providers have access to accurate and complete information about their patients, which is critical for making informed medical decisions. A data breach can be devastating for a healthcare organization's reputation, leading to loss of trust and credibility. By securing patient data, healthcare organizations can protect their reputation and maintain the trust of their patients. So,securing data in the healthcare industry is crucial for protecting patient privacy, complying with regulations, preventing identity theft, improving patient care, and protecting the reputation of healthcare organizations. We can use steganography for these applications in healthcare sector, particularly for teleradiology applications.**

***Index Terms*—Teleradiology,, Steganography, Data breach**

I. Introduction

Steganography is the practice of concealing a secret message or information within another message, image, or video in a way that the existence of the hidden information is not obvious. In the healthcare sector, steganography can be used for various purposes. Steganography can be used to protect patient data and maintain confidentiality[1] in healthcare sector particularly in telemedicine applications. Patient data can be embedded within medical images or videos, which can then be securely transmitted without the fear of being intercepted by unauthorized users. Also, Medical images can be authenticated using steganography techniques. Digital watermarking techniques can be used to embed a unique signature within the image, which can be used to verify the authenticity of the image. Steganography can be used to embed hidden information within medical images or videos, which can aid in diagnosis and treatment. For example, hidden information can be used to highlight specific regions of interest within an image or provide additional information related to the patient's condition.

Steganography can be used to authenticate drugs and prevent counterfeiting[2]. Hidden information can be embedded within the packaging of the drug, which can be used to verify its authenticity. It can be used to protect the confidentiality of medical research data. Research data can be embedded within images or videos, which can then be securely transmitted without the fear of being intercepted by unauthorized users. Overall, steganography plays a major role in protecting patient data and ensuring the confidentiality of medical information. The fundamental elements of steganography can be broken down into four parts. These parts include:

- Cover object: This is the medium in which the data will be concealed.
- Secret data: It refers to the message that will be embedded within the cover object.
- Stego object: This is the cover object after the secret data has been hidden inside.
- Stego key: It is the method used to conceal the secret data within the cover object.

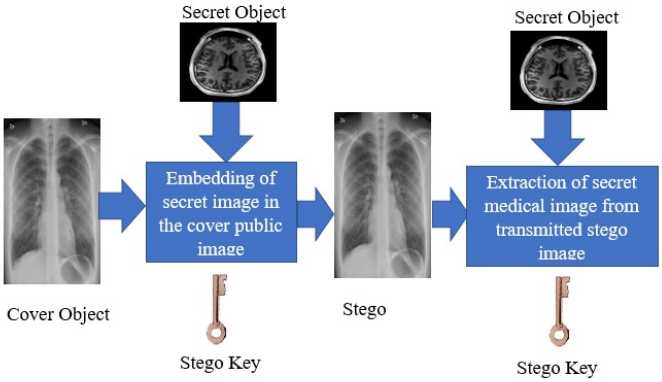

Fig. 1. Architecture of a steganographic system

Figure 1 shows the architecture of a steganographic system.Here at the sender side, a secret medical image is embedded in a cover public image called the cover object using a stego key and the resulting stego object is transmitted through the network. At the receiver side,

the secret medical image is extracted back from the stego object using the same stego key,

II. Literature Survey

There have been several papers in the literature that deal with the steganographic techniques in the healthcare sector.Some of them are discussed below. During the early stages of steganography, the process of embedding involved manipulating the Least Significant Bit (LSB) of each pixel in the original image. This was achieved by either replacing the LSB with secret image bits or adjusting it to fit additional secret image bits[3]. By doing so, the resultant stego image appeared visually similar to the original, thus concealing the presence of the secret image. However, embedding the equal number of secret binary digits in all the LSBs of the cover object make steganalysis easier. To prevent this, embedding was carried out randomly in varying locations and with varying numbers of secret image bits. The embedding capacity was determined by the dimensions of the cover image, and the selection of a suitable cover image was based on the size of the secret image. In cases where the size of the secret image exceeded that of the cover image, embedding was performed on a batch of cover images.

The literature contains various steganography schemes based on transform domains such as DCT, DFT, FFT, and wavelet[4]. The wavelet-based transform has good popularity due to its multi-resolution properties. Some embedding techniques discussed in the literature use a combination of two or more transformation techniques, and experiments have shown that this hybrid method is more effective than using a single transformation technique. When a cover image is transformed using DWT, it is divided into four sub-bands: LL, LH, HL, and HH. The LL sub-band contains a low-frequency coefficient that represents the basic information of the image, while the LH, HL, and HH sub-bands represent edge information. Embedding information in each sub-band produces a different result. Embedding in the HH sub-band provides better concealment but lower robustness, whereas embedding in the LL sub-band provides better robustness but lower concealment. Below are some of the steganographic approaches that have been studied.

In [5], a steganography technique was introduced for concealing data in medical images that utilizes an optimal pixel similarity approach. This technique employs a genetic algorithm to exploit the similarities between pixels in the images. Initially, the desired image to be hidden is selected and the doctor's comment is then added to the image. Next, the genetic algorithm applies the Least Significant Bits technique to hide the doctor's comment in the selected pixels, producing a stego image that is transmitted through the network. Finally, at the receiving end, the doctor's comments are extracted from the stego image.

Another work is proposed in which integer wavelet filter is used for hiding data in medical images. Firstly, an integer wavelet filter is used to decompose the medical cover image. Next, the confidential patient information is processed using the Arithmetic Coding (AC) and Data Encryption Standard (DES) algorithms to compress and encrypt the data before embedding it[6]. In the second step, the high-frequency subbands of the transformed medical image are analyzed to select the insignificant coefficients. Finally, the target cover bits and the secret bits are grouped together during the embedding process.

The article [7] proposes an image steganography technique that utilizes chaotic particle swarm optimization. This approach aims to identify the optimal pixel locations in the cover image for embedding secret data, while simultaneously maintaining the quality of the stego image. To increase the amount of data that can be hidden, both the host and secret images are divided into blocks that can store an appropriate number of secret bits. Particle swarm optimization is utilized to identify the best solution by iterating and adjusting a swarm of particles, with a focus on achieving an optimal outcome.

Another research work to safeguard the integrity and confidentiality of medical images using cryptography and steganography is proposed in [8]. To enhance security, steganography is utilized to add another layer of protection to the medical images in addition to cryptography. This study employs a one-time pad encryption algorithm for encrypting the medical image, which is then hidden in a cover object to produce a stego image, making it more prone to attacks. The proposed approach is implemented using MATLAB and is compared to a single layer of security approach, which involves hiding the medical image without encryption using LSB steganography . Different medical image formats, including TIFF, BMP, DICOM and JPEG, are considered, and the experimental results are analyzed.

Another research work presenting an improved image steganography method to enhance the data hiding capacity and imperceptibility of stego images, particularly in medical images of patients is proposed in [9]. The Image Region Decomposition (IRD) technique is proposed for gray scale MRI images. This technique divides the image into three distinct regions based on low, medium, and high pixel intensity values. Each region consists of k pixels, and within each pixel, the n least significant bits (LSBs) are manipulated. The embedding process is tested on four classes of MRI images with varying sizes. The imperceptibility of the embedded data is evaluated using different data volumes and verified by quality factors. Compared to other similar techniques, this steganography method achieves an average PSNR of 49.27, indicating better performance.

A research work utilizing the Bit Invert System (BIS) with three control random parameters is proposed in [10]. The selection process of bits is carried out randomly using the Henon Map Function (HMF) to enhance the level of security. To increase the payload ability and minimize the encrypted data, the scheme employs the use of the affine cipher and Huffman method for encrypting data prior to embedding. The integration of these techniques is effective for two reasons: first, it enables the determination and mapping of 0- and 1-bits during embedding, and second, it facilitates the segmentation of secret data to track and map every bit in the stego image.

An approach for image steganography based on edges is proposed is [11]. The technique involves encrypting the information using the logistic map prior to transmission, and using the Laplacian of Gaussian edge operator to detect the edges of a colored cover image. This approach provides an additional layer of security and has a high payload capacity. The proposed algorithm was tested by embedding a medical image of a patient into a 512×512 colored image in order to protect the patient's privacy. To conceal the entire secret data, it was first encrypted with the logistic map and then embedded into the edge regions of the cover image. The edge regions of the image were identified using the LoG detector. Following transmission of the encrypted data through the network, the concealed secret data was extracted by performing inverse embedding and decryption using the corresponding scheme.

A research investigating the potential use of quantum walks, which can exploit their unique quantum properties to propagate nonlinear chaotic behaviors and respond sensitively to changes in primary parameters, for efficient information security is proposed in [12]. This study presents a robust steganography protocol for E-healthcare platforms hosted in the cloud, which utilizes a classical version of the controlled alternate quantum walks (CAQWs) model. The protocol is designed to identify the areas of the image where the secret bits are overlaid and eliminates the need for pre/post encryption of the carrier and secret images. Additionally, the protocol simplifies the extraction of confidential information as it only requires the stego image and primary states to run the CAQWs. The proposed protocol is tested on a dataset of medical images and achieves excellent results, including high security, good visual quality, high resistance to data loss attacks, and high embedding capacity.

A study introducing a novel and robust image steganography method that integrates the Redundant Integer Wavelet Transform (RIWT), Singular Value Decomposition (SVD),Discrete Cosine Transforms (DCT), and the logistic chaotic map is proposed in [13]. The proposed technique utilizes the shift invariance of RIWT to achieve reversibility and robustness, while SVD and DCT enable a high level of imperceptibility by embedding the secret data in singular values. The logistic chaotic map provides extra security by encrypting the medical images, thus improving the technique's robustness. The proposed scheme's performance is compared with similar methods in the literature, and it proved to be superior in terms of robustness, imperceptibility and resistance to geometric transformation attacks. Validation was carried out using the UCID benchmarking database.

The literature also presents image steganography techniques based on deep learning[16]. In one study, V-Net and U-Net++ encoders based on convolutional neural networks (CNNs) were utilized for image steganography. Furthermore, the performance of the U-Net, V-Net, and U-Net++ architectures were comparatively evaluated.

III. Applications of steganography in healthcare

Steganography techniques have been developed to protect information from unauthorized access and hacking. These techniques provide a means of secure and covert communication, with applications spanning across various fields such as military and intelligence agencies, internet banking, online elections, medical imaging, and others.In the healthcare sector, various approaches have been employed to enhance the security of medical applications and devices. Medical information is highly sensitive and requires confidentiality protection during transmission. Within this section, we classify the applications of steganography in medical contexts based on their security features and the nature of the applications.

A. Protection of patient information

Steganography can be used to protect patient data in various ways. One approach is to hide patient information within other non-sensitive data, such as images, audio files, or video files[1]. By concealing the patient information within these files, the data can be transmitted securely without attracting unwanted attention from unauthorized parties. Additionally, the use of steganography can help prevent data leakage during transmission or storage.

Another way to use steganography to protect patient data is by embedding the data within other files that are publicly available, such as social media posts or public websites. The information can be encrypted and hidden within these files, making it difficult for unauthorized parties to access the data. Furthermore, steganography can be used to protect patient data in electronic medical records (EMRs) by hiding the data within the file itself. Steganography can also be used to protect patient data during communication between healthcare professionals. By concealing the data within other non-sensitive data, the communication can remain secure and private. In this way, steganography can help to ensure that sensitive patient data is protected and that it remains confidential and secure at all times.

B. Protection of drugs

Steganography can be used to authenticate drugs by embedding hidden and tamper-proof information within the packaging or labeling of the medication. This information can be encoded in a way that is not visible to the naked eye and can only be accessed using specialized equipment or software. This technique can help to prevent counterfeit drugs from entering the market and can provide assurance to patients that the medication they are receiving is genuine and safe.

One approach to using steganography to authenticate drugs is to embed a unique code within the packaging or labeling of the medication. This code can be accessed using a specialized reader or software, which can verify the authenticity of the medication. The code can be designed to be difficult to replicate, making it more challenging for counterfeiters to produce fake drugs.

Another approach is to use steganography to embed an image or logo within the packaging or labeling of the medication.

The image or logo can be designed to be difficult to reproduce and can provide a visible indication of the authenticity of the drug.Overall, steganography can be a valuable tool in the fight against counterfeit drugs. By embedding hidden and tamper-proof information within the packaging or labeling of medications, steganography can provide a means of authenticating drugs and ensuring that patients receive safe and genuine medication.

C. Protection of Biological signals

Steganography can be used to protect biological signals by embedding them within other non-biological data. Biological signals such as electrocardiogram (ECG), electroencephalogram (EEG), or electromyogram (EMG) are often transmitted over insecure networks or stored in vulnerable locations, which makes them susceptible to unauthorized access or modification. Steganography can help to protect these signals by hiding them within other non-sensitive data, making it difficult for unauthorized parties to access or modify them[14].

One approach to using steganography to protect biological signals is to hide them within images or audio files. The biological signal can be encoded within the image or audio file, making it difficult for unauthorized parties to detect. The signal can then be transmitted or stored alongside the image or audio file, which can help to provide an additional layer of protection.

Another approach is to use steganography to hide biological signals within other signals. For example, ECG signals can be hidden within EEG signals or vice versa. This can help to protect the signals during transmission or storage and can provide an additional layer of security.So steganography is a valuable tool in protecting biological signals. By hiding the signals within other non-sensitive data, steganography can help to prevent unauthorized access or modification of the signals, ensuring their integrity and confidentiality.

D. Protection of medical devices

Medical devices can be protected using steganography by embedding hidden and tamper-proof information within the firmware or software of the device. This information can help to ensure the integrity and authenticity of the device, protect against unauthorized access or modification, and prevent the device from being used for malicious purposes[15].

One approach to using steganography to protect medical devices is to embed a unique code within the firmware or software of the device. This code can be accessed using a specialized reader or software, which can verify the authenticity of the device. The code can be designed to be difficult to replicate, making it more challenging for counterfeiters to produce fake devices. Another approach is to use steganography to hide information within the firmware or software of the device that can be used to detect unauthorized modifications. For example, a hidden signature or checksum can be embedded within the firmware or software, which can be used to verify that the device has not been tampered with.

Steganography can also be used to protect sensitive data that is transmitted between medical devices. By embedding the data within other non-sensitive data, the communication can remain secure and private. This can help to prevent unauthorized access or modification of the data during tranmission. steganography is a valuable tool in protecting medical devices. By embedding hidden and tamper-proof information within the firmware or software of the device, steganography can help to ensure the integrity and authenticity of the device, protect against unauthorized access or modification, and prevent the device from being used for malicious purposes.

IV. CONCLUSION

This paper presents an overview of the use of diverse steganographic techniques in the healthcare sector. The study underscores the significance of enhancing information security in the healthcare industry, particularly in digital information systems like the Hospital Information System (HIS), image archiving and communication systems, and Electronic Patient Record (EPR) systems. Digitally representing medical data has many benefits, which are also discussed, but it also increases the risk of unauthorized access, interception, or manipulation of sensitive medical and confidential information. Through the analysis of relevant literature, we have demonstrated that steganography can be used effectively to ensure the confidentiality and integrity of sensitive patient information, such as medical images and electronic health records. In summary, this review paper has provided an overview of the current state of steganography in healthcare, highlighting its potential applications and benefits.

REFERENCES

[1] Sajedi H, Yaghobi SR. Information hiding methods for E-Healthcare. Smart health. 2020 Mar 1;15:100104.

[2] Huo Y, Yang Z, Wilson T, Jiang C. Recent Progress in SERS-Based Anti-counterfeit Labels. Advanced Materials Interfaces. 2022 Jun;9(17):2200201.

[3] Nolkha A, Kumar S, Dhaka VS. Image steganography using LSB substitution: A comparative analysis on different color models. InSmart Systems and IoT: Innovations in Computing: Proceeding of SSIC 2019 2020 (pp. 711-718). Springer Singapore.

[4] Kadhim IJ, Premaratne P, Vial PJ, Halloran B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing. 2019 Mar 28;335:299-326.

[5] Karakus S, Avci E. A new image steganography method with optimum pixel similarity for data hiding in medical images. Medical Hypotheses. 2020 Jun 1;139:109691.

[6] Ahmad MA, Elloumi M, Samak AH, Al-Sharafi AM, Alqazzaz A, Kaid MA, Iliopoulos C. Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images. Alexandria Engineering Journal. 2022 Dec 1;61(12):10577-92.

[7] Jaradat A, Taqieddin E, Mowafi M. A high-capacity image steganography method using chaotic particle swarm optimization. Security and Communication Networks. 2021 Jun 7;2021:1-1.

[8] Priyadharshini A, Umamaheswari R, Jayapandian N, Priyananci S. Securing medical images using encryption and LSB steganography. In2021 international conference on advances in electrical, computing, communication and sustainable technologies (ICAECT) 2021 Feb 19 (pp. 1-5). IEEE.

[9] Siddiqui GF, Iqbal MZ, Saleem K, Saeed Z, Ahmed A, Hameed IA, Khan MF. A dynamic three-bit image steganography algorithm for medical and e-healthcare systems. IEEE Access. 2020 Oct 2;8:181893-903.

[10] Hashim MM, Taha MS, Aman AH, Hashim AH, Rahim MS, Islam S. Securing medical data transmission systems based on integrating algorithm of encryption and steganography. In2019 7th International Conference on Mechatronics Engineering (ICOM) 2019 Oct 30 (pp. 1-6). IEEE.

[11] Jan A, Parah SA, Malik BA. A novel Laplacian of Gaussian (LoG) and chaotic encryption based image steganography technique. In2020 International Conference for Emerging Technology (INCET) 2020 Jun 5 (pp. 1-4). IEEE.

[12] Abd-El-Atty B, Iliyasu AM, Alaskar H, Abd El-Latif AA. A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms. Sensors. 2020 May 31;20(11):3108.

[13] Arunkumar S, Subramaniyaswamy V, Vijayakumar V, Chilamkurti N, Logesh R. SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. Measurement. 2019 Jun 1;139:426-37.

[14] Banerjee S, Singh GK. A Robust Bio-Signal Steganography With Lost-Data Recovery Architecture Using Deep Learning. IEEE Transactions on Instrumentation and Measurement. 2022 Aug 10;71:1-0.

[15] Oh SR, Seo YD, Lee E, Kim YG. A Comprehensive Survey on Security and Privacy for Electronic Health Data. Int J Environ Res Public Health. 2021 Sep 14;18(18):9668. doi: 10.3390/ijerph18189668. PMID: 34574593; PMCID: PMC8465695.

[16] Himthani, V., Dhaka, V.S., Kaur, M. et al. Comparative performance assessment of deep learning based image steganography techniques. Sci Rep 12, 16895 (2022). https://doi.org/10.1038/s41598-022-17362-1