DOI: http://dx.doi.org/10.21123/bsj.2021.18.2(Suppl.).0957

# A Comprehensive Review on Medical Image Steganography Based on LSB Technique and Potential Challenges

*Bushra Abdullah Shtayt*[1*] *Nur Haryani Zakaria*[2] *Nor Hazlyna Harun*[2]

[1] Southern Technical University, Basrah, Iraq.
[2] Universiti Utara Malaysia, Malaysia.
[*]Corresponding author: bushra.abdullah@stu.edu.iq[*], haryani@uum.edu.my, hazlyna@uum.edu.my
[*]ORCID ID: https://orcid.org/0000-0003-2123-1054[*] , https://orcid.org/0000-0001-5971-1307 , https://orcid.org/0000-0002-6817-9874

Received 28/3/2021, Accepted 13/4/2021, Published 20/6/2021

## Abstract:

The rapid development of telemedicine services and the requirements for exchanging medical information between physicians, consultants, and health institutions have made the protection of patients' information an important priority for any future e-health system. The protection of medical information, including the cover (i.e. medical image), has a specificity that slightly differs from the requirements for protecting other information. It is necessary to preserve the cover greatly due to its importance on the reception side as medical staff use this information to provide a diagnosis to save a patient's life. If the cover is tampered with, this leads to failure in achieving the goal of telemedicine. Therefore, this work provides an investigation of information security techniques in medical imaging, focusing on security goals. Encrypting a message before hiding them gives an extra layer of security, and thus, will provide an excellent solution to protect the sensitive information of patients during the sharing of medical information. Medical image steganography is a special case of image steganography, while Digital Imaging and Communications in Medicine (DICOM) is the backbone of all medical imaging divisions, whereby it is most broadly used to store and transmit medical images. The main objective of this study is to provide a general idea of what Least Significant Bit-based (LSB) steganography techniques have achieved in medical images.

**Key words**: Dicom, Image Steganography, Information Security, Least Significant Bit (LSB) Medical Imaging, Telemedicine.

## Introduction:

Safe communication is one of the big challenges that has emerged with great progressions in communication technologies, especially in the field of information exchange, which requires protection (1). These progressions have imparted numerous advantages; however, at the same time, there are several risks and hazards that need to be considered as well. The advancement of information and communication technologies (ICT) and their gradual adoption by healthcare providers have enhanced the knowledge of diseases and therapies, communication between practitioners, workflow, and efficiency of processes, and generally allowed high-quality services to be provided (2).

Technologies like telemedicine are evolving daily and maintaining the safety of medical data becomes very challenging (3). Telemedicine is the utilisation of ICT to provide clinical healthcare from remote places. According to the definition by the American Hospital Association (AHA), the word 'telemedicine' starts with the Greek prefix 'tele', which means distance, as well as the meaning of the whole word 'telemedicine', which refers to is remote medicine (4-5).

Furthermore, capturing medical data by unauthorised people has lately turned out to be a serious cybercrime. If sensitive data are captured or stolen unauthorisedly, then it can lead to an infringement of basic patient rights. For example, a patient with Hepatitis does not want to spread his information to unauthorised people. Therefore, secrecy and data integrity are wanted to safeguard against use and unauthorised access. In consequence, the protection of medical information (MI) is a requirement today. Since telemedicine's early adoption, it has developed the way medical staff characterise and deal with health information, which provides more reactive manners for storing and searching a great amount of clinical data. Nevertheless, the sharing of electronic protected health information/records (ePHI/R) for consultation and diagnostic purposes involves the risk of confidentiality, identification, and originality. These medical documents are very sensitive information that describe the conditions of the patient and therefore requires unlimited safety during transportation and storage (6-7).

One of the alternatives to encryption is steganography in a cover, which is an excellent solution to protect patients' personal information while exchanging medical information. Medical image steganography is a special type of image steganography. Therefore, this work intends to investigate various information security techniques in medical imaging focusing on security goals. The basic purpose of this study is to present a comprehensive review of what Least Significant Bit-based (LSB) steganography techniques have achieved in medical images domain.

This study is subdivided into several sections: Section two discusses the medical imaging domain and the architecture of Digital Imaging and Communications in Medicine (DICOM). Section three presents the research methodology, as it reviews the general characteristics of information security and its achievements. The fourth section deals with the criteria for the protection of medical information, while the fifth section contains a brief description of steganography and the following section deals with medical image steganography in particular. In the seventh section, the most important techniques for hiding medical information is discussed. Additionally, the study deals with the most important techniques, such as LSB, for hiding medical information in the eighth section. Finally, a conclusion of this study is provided in the ninth section.

## Medical Image Domain:

Medical image is a type of medical information that is considered as the heart of telemedicine, whereby it is used for several purposes including treatment, diagnosis, training, remote learning, and medical consultations between radiologists and clinicians (8). Dealing with digital medical image, despite its great utility in modern healthcare, raises many new security problems through legal and ethical mechanisms for local archiving and remote medical services (9). As a result, even the smallest changes would impact the doctor's diagnosis; therefore, medical images require a high level of security to ensure only real changes happen.

Medical imaging points to procedures and methods utilised to produce images of different parts to the human body within digital health for treatment and diagnostic purposes. The idiom of medical imaging encompasses numerous techniques of radiological imaging including ultrasound, Computerised Tomography (CT), Magnetic Resonance (MR), X-ray, etc. These images are stored in Picture Archiving and Communication Systems (PACS) and are commonly handled within a computerised workflow based on the Digital Imaging and Communications in Medicine (DICOM) standard (10, 11).

DICOM is an international standard produced by the National Electrical Manufacturers Association (NEMA) for the communication and administration of medical imaging information (i.e. images and related data). DICOM is the backbone of all medical imaging sections, whereby it is most widely used to store and transmit medical images that allow multiple manufacturers to incorporate medical imaging devices like workstations, servers, printer, scanners, network hardware, and PACS systems (12, 13).

DICOM image files have two components: the first one is a header containing metadata such as confidential patient information, the location of the examination, the equipment that makes the header size vary from image to image and further differs depending on the imaging modality; and the other one is a greyscale matrix reflecting image intensities (14-16). The DICOM image file is composed of the following as shown in Figure 1.

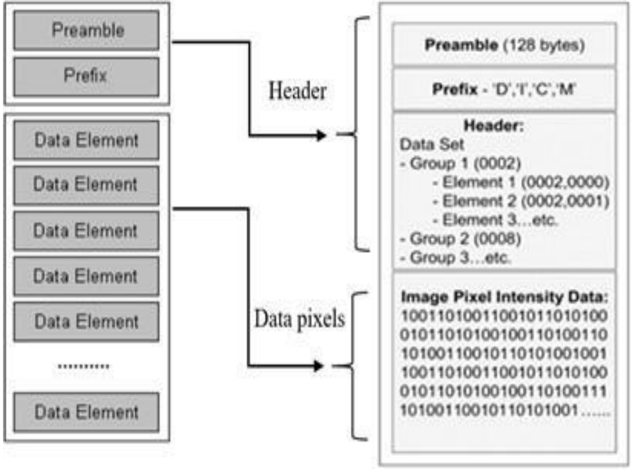


**Figure 1. DICOM Structure (17-19)**

DICOM image structure consists of four parts as follows:

- A 128-byte preface.
- The 4-byte prefix for storing 'D', 'I', 'C', and 'M' letters to define the file format.
- Metadata fields that are set to save data.

- Data pixels to form the image contained in the DICOM file.

The DICOM standard offers many advantages, such as the ability to capture medical images and share them quickly. Furthermore, clinicians can make decisions and produce patients' reports more easily. Nevertheless, there are no security mechanisms that protect the confidentiality of metadata or image authenticity as it is easy to remove, change, or otherwise disconnect the metadata (12, 20). The next section will discuss the most important challenges faced by telemedicine, especially in the field of information security for medical images.

## Methodology:

This section discusses the methods and characteristics of medical information security and investigates the important challenges facing medical image protection as well as the practical effects and requirements of medical images. Most studies on medical information security have been researched by a variety of repositories such as Google Scholar, Springer connects, and IEEE Xplore. Telemedicine is a product of 20th century ICT, which is emerging as a vital element of the solution to the healthcare crisis. Lately, vast concerns are raised about the problem of medical information security due to the rising need for telemedicine services and the known fact that applications of medical frequently handle sensitive patient information. This has become an important and crucial issue as it inevitably involves the transfer of medical information over open networks like the Internet (21-23). Nowadays, maintaining the privacy of medical information is not only an ethical requirement but also a legal one (18, 24-27). Thus, medical information must be collected and shared safely where it can only be accessed by authorised persons.

Recently, information security has become a major concern for many researchers with digital transformation and huge data, due to the urgent need to exchange information via the Internet quickly and at the same time in a secure manner. As a consequence, many technologies have emerged that aim to achieve these requirements. Nevertheless, they differ in purpose and approach, including techniques to hide and encrypt data. Figure 2 shows the information security techniques and branches.

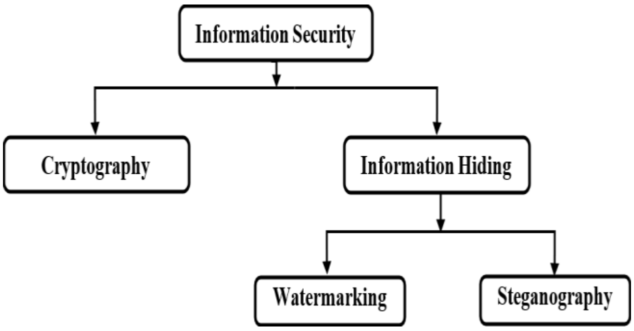


**Figure 2. Information Security Techniques and Branches (28)**

Regardless of the significant achievements of information security techniques to protect the information, the rate of adoption of these techniques is still very low in real-time applications, whereby the privacy of sensitive information is paramount, such as military reports, health records, and forensic reports, among others (29, 30). The protection system can be divided into more basic details, such as information hiding (i.e. Steganography/ Watermarking) or encryption (i.e. Cryptography) of information, or a mixture of them (31). Table 1 illustrates the objectives, general characteristics for information security techniques, and their drawbacks.

**Table 1. General Characteristics of Information Security**

| Information Security Techniques | Definition | Objectives | Characteristics or Requirements | Drawbacks |
|---|---|---|---|---|
| Cryptography | Cryptography is the art and science for protecting information from unauthorised persons by converting it into an unreadable form, meaning that it has no meaning, i.e. plain text converted to ciphertext (28, 32) | Data protection | ● Authentication<br>● Confidentiality<br>● Integrity<br>● Non-repudiation<br>● Access control and support services | The problem with cryptography lies in the existence of the original data in ci- phertext ,which appears meaningless; thus, the attacker can attract attention, interrupt the transmission, and utilise cryptanalysis to discover the meaning of the message (33). |
| Watermarking | Watermarking is a technology in which data carrier identification information is embedded with methods that can be difficult to notice and do not affect data use. Watermarking technology usually protects multimedia data copyright like the authentication of banknotes to prevent attackers from damaging watermarking (34, 35). | Protecting the carrier's copyrights and intellectual property rights to avoid removal or replacement by an invader party. | ● Capacity<br>● Robustness<br>● Security<br>● Imperceptibility | A drawback of digital watermarking is that a subscriber's inability changes some parts of the files safely without sacrificing the quality or usefulness of the host data (36, 37) |
| Steganography | Steganography is the art of hiding a file (message, image, audio, or video) inside another file (message, image, audio, or video) to avoid detection (38). | The purpose is to secure communication for hiding the presence of a message to avoid from an invader party detecting it. | ● Security<br>● Imperceptibility<br>● Capacity<br>● Robustness | The real problem in steganography is that once the existence of the secret message is revealed or even supected, the message becomes clear (39). |

From Table 1 above, it is noted that all security techniques have certain characteristics that are required to achieve the goal behind implementing this technique. For example, the characteristics of encryption techniques include authentication (the process of confirming the sender's identity and that it is issued from a trusted source, i.e. right source), confidentiality (ensuring that nobody can read the message except the meant receiver), integrity (the secret data have not been adjusted in transit by unauthorised users), non-repudiation (assures that neither the sender nor the receiver of a message must be able to deny the transmission, where the non-repudiation is closely linked to authentication), and access control (the information given can only be accessed by the authorised parties) (40, 41). Cryptography technique is very important because it helps information hiding techniques to achieve security (42), as it has been used with watermarking to provide privacy and authentication (43), as well as with steganography techniques to achieve confidentiality of hidden data (44). Steganography and cryptography techniques are considered the most common ways to ensure secure communications. Steganography is the art and science of concealing information in a carrier, whereby no one knows the existence of the hidden information except the intended receiver, while cryptography is considered the art and science for secret writing with the purpose of concealing a message's meaning (45, 46).

Many researchers have offered hybrid methods for secure secret communication based on a combination of cryptography and information hiding (i.e. watermarking and steganography) techniques to achieve all/some requirements of the techniques. In the following passages, various levels of protection methods based on watermarking algorithms with cryptography techniques will be disscussed.

Kannammal and Rani suggested a scheme to protect medical images using watermarking embedded by LSB and discrete wavelet transform (DWT) and to encrypt the watermarked image by using three algorithms (AES, RSA, and RC4) to provide two-level security (47). Additionally, Al-Haj described the use of LSB, DWT, and singular value decomposition (SVD) for multiple image watermarking method (48). DWT and SVD were utilised for embedding the robust watermarks in non-region of interest (NROI) of the cover image, while the LSB-based spatial domain method was used to embed the fragile watermarks within the region of interest (ROI) of the cover image. In Al-Haj et al. study, the authors introduced a hybrid algorithm that combined digital watermarking and encryption techniques to provide the authenticity and integrity services that are required (49). Sharma et al. suggested an approach that applied a hybrid (DWT and DCT) transformation on the cover to embed medical information of patients and watermarks simultaneously, in addition to using the Rivest–Shamir–Adleman (RSA) and MD5 algorithms for Electronic Patient Record (EPR) watermark encryption before the embedding process within the NROI and ROI portions of the medical image (50). Meanwhile, Khond and Viajayakumar introduced an efficient method for the protection of medical information by combining the encryption and watermarking techniques (51). Another group of researchers tackled two important issues, namely the authenticity and integrity of the watermark or ownership identification by embedding the biometric iris template as a watermark embedded in the fingerprint image by using dual DWT-SVD (52). On the other hand, Thakur et al. presented a joint hybrid approach based on cryptography and watermarking techniques using a combination of DWT, discrete cosine transform (DCT), and SVD for the authentication and identification of patients (53).

Besides the watermarking techniques for protecting information, there is the steganography technique that is used with cryptography to maintain the information intact from hackers. Steganography and cryptography can play a very significant role in this field by providing two-level security (54, 55). Many researchers have worked on the protection of data through combining steganography and cryptography techniques. For instance, Pandey and Shrivastava presented an algorithm to ensure the transmission of medical images through combining cryptography and steganography techniques (56). wherein their algorithm, patient information was embedded using a lossless LSB steganography technique to improve security and avoid noise, whereby the embedded image was encrypted. Trehan and Mittu proposed using a single platform of the two essential security mechanisms, i.e. cryptography and steganography, for improving patient information security (57). Patient information was encrypted using the Advanced Encryption Standard (AES) algorithm and then embedded in the cover medical image using the LSB technique. In 2016, Jain and Lenka introduced a secure architecture using crypto-stegano algorithm to secure the transmission of medical information (58). The notion of a diagonal queue was utilised, whereby the confidential cipher-blocks and sub-blocks were allocated dynamically for chosen diagonal queues to embed. Rabin public-key was used to convert medical record and identification information of patients into encrypted text, whereas various bit positions among the 8th to 5th bit LSB were sequentially used to embed the encrypted text in host medical images. Khalil introduced a method based on combined cryptography and steganography algorithms to embed a quantity of confidential data into a cover image in the transform domain (59). This method investigated the degradation of the medical image when undergoing the process of steganography in the transform domain, looking for the most suitable location to hide the encrypted message. Banjan and Dalvi presented a method based on a merge of steganography and cryptography techniques to conceal patients' information after being encrypted by using the AES algorithm (60). For the protection of the patients' information, they used two methods: (i) AES-192 encryption with LSB steganography, and (ii) AES-192 with DWT steganography. The authors employed evaluation metrics such as peak signal-to-noise ratio (PSNR) and mean squared error (MSE) to compare their results. A study by Babatunde et al. illustrated double-layer security, i.e. the combination of Triple Data Encryption (3DES) algorithm and LSB image steganography, to enhance data protection in medical or healthcare establishments (61). Table 2 summarises the important issues that are processed by information hiding and cryptography techniques, in addition to the achievements and methods used to achieve them.

**Table 2. Summary of The Achievements of Combining Information Hiding with Cryptography and The Approaches Used**

| Related References | Information Security Techniques | Achievements | | | | | | | | | Approaches |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | (9) | |
| Kannammal and Rani (47) | Watermarking and Cryptography | √ | √ | | | | | | | | ● LSB and DWT<br>● AES, RSA, and RC4 |
| Al-Haj (15) | | √ | √ | | √ | | | | | | ● LSB, DWT, and SVD |
| Al-Haj et al. (49) | | √ | √ | | | | | | | | ● RSA public-key method<br>● DWT |
| Sharma et al. (50) | | | | √ | | | | | | | ● DWT and DCT<br>● RSA algorithm |
| Khond and Viajayakumar (51) | | √ | | | | | | | | | ● Used many encryption algorithms such as RC4, AES, RSA, and DES |
| Mehta et al. (52) | | √ | √ | | | | | | | | ● FRWT with Arnold's cat map for encrypting<br>● DWT-SVD for embedding |
| Thakur et al. (53) | | √ | | √ | √ | | | | | | ● Chaotic encryption algorithm<br>● DWT, DCT, and SVD |
| Pandey and Shrivastava (56) | Steganography and Cryptography | | | | | | | | | √ | ● Lossless LSB<br>● Using two share methods to encrypt an image of another medical image, whereby the encrypted image covers the embedded image |
| Trehan and Mittu (57) | | | | | | | | | | √ | ● LSB algorithm based on zigzag<br>● AES algorithm |
| Jain and Lenka (58) | | | | | √ | | √ | | √ | | ● Rabin encryption technique.<br>● 5th-8th LSB |
| Khalil (59) | | | | | √ | | √ | | | | ● RC4 encryption technique<br>● LSB and the Discrete Fourier Transform (DFT) |
| Banjan and Dalvi (60) | | | | | | | | | | √ | ● AES-192 encryption algorithm<br>● LSB and DWT algoithms |
| Babatunde et al. (61) | | | | | | | | | | √ | ● 3DES encryption algorithm<br>● LSB algorithm |

Notes: (1) Authentication, (2) Integrity, (3) Identification, (4) Confidentiality, (5) Privacy, (6) Imperceptibility, (7) Robustness, (8) Capacity, and (9) Security

**Requirements of Medical Information Security:**

Lately, the vast and important progress in terms of information technology (IT) has resulted in a large number of alterations to the concept of medical information (MI) security because of its sensitivity and high value by nature. Modern and integrated healthcare systems like the Hospital Information System (HIS) and PACS system, among others, promotes easy access, processing, and dissemination of medical data. There are many reasons for medical knowledge sharing, such as telemedicine applications in terms of teleconsultation, telediagnosis, and telesurgery for the purposes of medical personnel e-learning (63). On the other hand, the Electronic Patient Record (EPR) replaced the obsolete patient record system in hardcopy format. Typically, EPR includes diagnosis reports, medical images, and biomedical signals, but may also include medical records like demographic data, medical examination results, medications, medical prescriptions, and others, which by nature are considered highly secret. For these causes, the security of MI today is a necessity that is derived from legislative rules to ensure authenticity, integrity, and confidentiality of MI during the exchange of dispatch and thus preserves patients' rights (8).

The context of the medical image, which is the essence of telemedicine work, contains features and requirements in addition to the ethics and legal aspects that must be worked on. This is to ensure the integrity of the medical image quality in order to avoid wrong diagnosis. Below are the mandatory characteristics of medical image security (64):

- **Confidentiality**: Assures that access to information is only open to authorised users.
- **Reliability**, depending on the results of:
  1) Integrity: The information is not altered by unauthorised persons.
  2) Authenticity: Evidence that the information relates to a certain patient and has been emitted from the correct source.
  3) The ROI Intactness: A medical image has two regions, region of interest (ROI) and region of non-interest (RONI). The steganography schemes should not negatively affect ROI. A distorted ROI leads to an incorrect diagnosis.
- **Availability:** Assurance access to the information system to be utilised under the normal listed conditions.

**Overview of Steganography:**

Steganography is the art and science of secret communication. The term steganography is a combination of two Greek words "steganos" and "graphy", whereby "steganos" means "secret or covered" and "graphy" means "drawing or writing" (65, 66). Steganography techniques can be divided into various categorised based on cover type, embedding domain, embedding and extraction approaches (67, 68). Figure 3 shows a classification of steganography techniques.

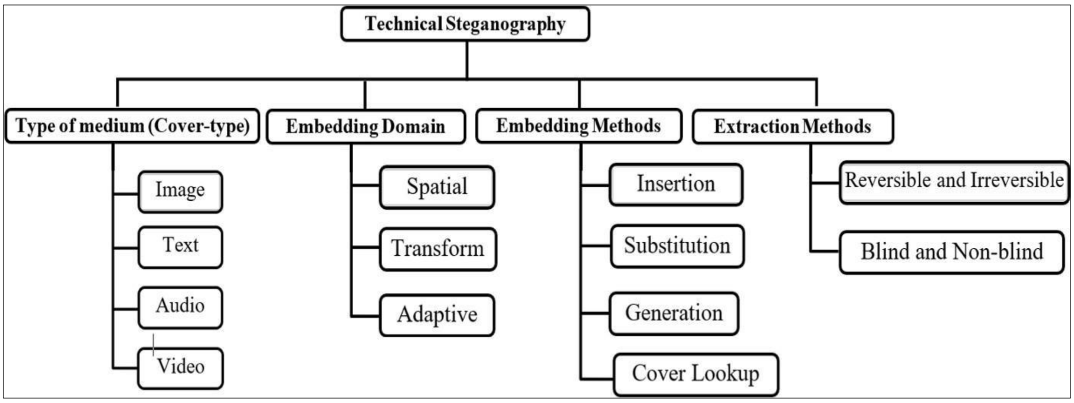


**Figure 3. Schematic Description of Steganography Techniques (69, 70)**

Steganography uses digital mediums such as text, image audio, and video as a cover to send the message; therefore, image steganography has become a significant area of research in data protection, confidentiality, and image integrity in recent years. In this work, medical image was adopted as a cover and the spatial domain as an embedding domain. The steganography of medical images requires special caution when embedding extra data inside the medical images, whereby the added information does not impact the image quality. The main benefits of telemedicine using steganography are as follows (59, 70):

- No additional storage space is needed for these methods, whereby ePHI/R is embedded within the cover's medical images so that ePHI/R does not require extra memory storage.
- In order to transmit data, ePHI/R embedded within the casing medical image is transmitted together, so that no additional bandwidth is needed for ePHI/R transmission.
- ePHI/R embedded in the medical image, therefore no one can see the presence of ePHI/R in the medical image. These techniques are safe to keep the data private.
- Protection towards manipulation as the after-effects of manipulated data will cost a life due to wrong diagnosis.

**Medical Image Steganography:**

The main purpose of using technical steganography for medical images is to increase the security, integrity, and confidentiality for both data records and medical images of patients. Medical image steganography is considered a special state of image steganography wherein medical images have special demands (62, 71). In a modern healthcare environment, a distant exchange of medical information (i.e. medical images and patient records) between hospitals/clinics has become a portion of the daily routine. Medical image steganography is employed to protect the EPR's confidentiality without affecting the quality of the medical image, whereby it conceals the EPR and diagnosis report in the medical image to solve the authentication issue and preserve patient privacy through providing a link between the patient's information and their image (15, 72). Over the recent years, more attention has been paid to improving the safety of patient information over medical databases by considering steganography schemes as a solution for covering EPR in photographs of patients, as shown in Figure 4.

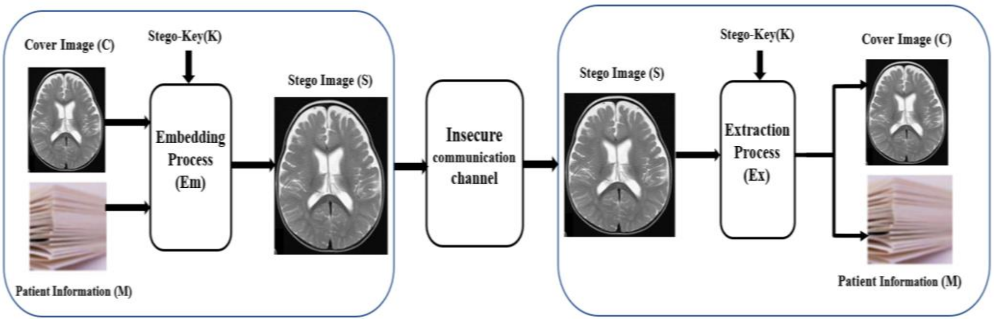


**Figure 4. Medical Image Steganography Scheme (9, 73)**

This interest has increased within several techniques of steganography that are designed to fit the requirements of medical images. Methods of steganography are employed in the healthcare system for many causes, including (74-76):

- **Privacy and confidentiality:** Since patient images and data are shared between hospitals via unsecured public networks, data privacy is an important issue as it must provide the protection and extreme careful use of patients' information (26, 77). Steganography protects communication channels to avoid drawing an eavesdropper's suspicion in order to maintain the digital medical image and sensitive patient information during data transmission.
- **Security:** The major feature of steganography is the inability of intruders to discover the message statistically. To be more precise, the security of steganography is determined by the supposition that the intruder is not capable of proving whether the cover medium contains secret data or not.
- **Memory and cost saving:** Computational and memory costs are necessary criteria for any information system evaluation. Due to the fact that medical system databases typically have a great deal of data to carry, it is fair to use methods that preserve the necessary data but require a minimum amount of memory. The required storage for patient records can be minimised in the Medical Information System (MIS), by hiding EPR inside the medical image. Compared to other methods of information security, the computational cost of information-hiding methods should be appropriate.
- **Availability:** Availability is the capability to guarantee that authorised users have access to the information system and resources related to the information system at any time.

**Basic Image Steganography Techniques:**

Image steganography techniques can be categorised into two major classes depending on the embedding domain, namely spatial and transform domain (78). The embedding domain points to the characteristics of the cover object, which are exploited in embedding messages inside it (79). In a spatial domain technique, the data are embedded directly into the pixels of the host by manipulation of image intensities with the secret data bits (80). While the coefficients of the host medium are adjusted in a transform domain technique by manipulating the image indirectly through different transforms such as integer wavelet transform (IWT), DCT, DFT, and DWT. Usually, transform domain techniques are robust against attacks and provide more security as compared to spatial techniques. Nevertheless, their drawbacks are the high computational cost and limited payload capacity (81). In contrast, spatial domain techniques are simple and easy to implement and are sufficient in an environment free of attacks and lossless compression. They also do not need longer execution time and present a high rate of payload capacity (82). Table 3 displays the variations in terms of embedding capacity, imperceptibility, and robustness between image steganography in spatial and transform domains techniques.

**Table 3. Comparison between Techniques of Image Steganography in Spatial and Transform Domains (83-85)**

| Steganography Techniques | Descriptions |
|---|---|
| Spatial domain techniques | **Benefits:**<br>● Simplicity and easy to use; the embedding process is directly carried out within LSBs of intensity values. Therefore, it is the most popular technique utilised in digital steganography and particularly in digital images.<br>● High embedding payload.<br>● Shorter computational time.<br>**Drawbacks:**<br>● Extremely weak and could be damaged by practising a slight alter for the stego image like JPEG compression.<br>● Not robust against rotating or cropping of the image. |
| Transform domain techniques | **Benefits:**<br>● More robustness against attacks such as geometric attacks and compression than spatial domain techniques.<br>**Drawbacks:**<br>● Capacity embedding is limited. Embedding information takes place in the coefficients of the transformed image; this requires added computations. |

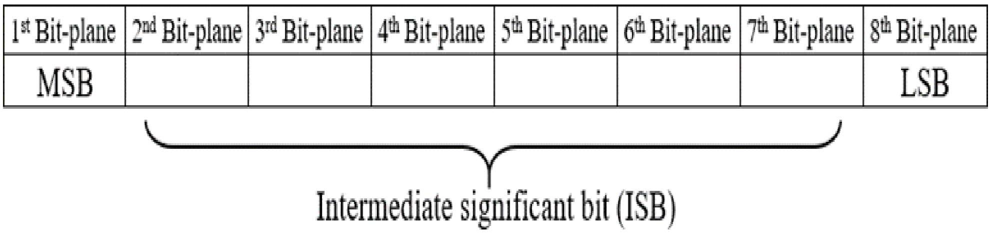
**Spatial Domain Techniques:**

Spatial domain points the actual physical position of a pixel in an image. The physical location of the host pixel must be considered when embedding data because it plays a significant role in evaluating the overall performance of the steganography algorithms (79, 86). There are numerous methods employed in the spatial domain like LSB, Grey Level Modification (GLM), and Pixel-Value Differencing (PVD).

**Least Significant Bit (LSB):**

LSB method is the most used in the spatial domain, whereby a digital image consists of a matrix of colour values and intensity. In the LSB method, the secret message bits replace the cover image pixels directly with some or all of the LSBs. The modification of the host pixels' LSB does not cause a great deal of contrast in the image and consequently, the stego image appears to be like the host image (87). 8 bits are used for each pixel in a typical greyscale image, while 24 bits/pixel in a colour image, with 8-bits for each colour component: Red, Green, and Blue (RGB) (88).

Each bit value of the 8 bit-plane can be represented by 2n-1, where n is the order of the plane beginning from 1 to 8, i.e. (20 + 21 + 22 + 23 + 24 + 25 + 26 + 27) = (1 + 2 + 4 + 8 + 16 + 32 + 64 + 128)= 255. The highest value that can fit in 8 bits is 255 and the smallest value is 0. Any alteration to the 8th bit-plane will alter the pixel value by ±1, the 7th bit-plane by ±2, the 6th bit-plane by ±4, the 5th bit-plane by ±8, the 4th bit-plane by ±16, the 3rd bit-plane by ±32, the 2nd bit-plane by ±64, and the 1st bit-plane by ±128. As an outcome, if the altered value is small (like in the 8th bit-plane), the quality of the image is kept high. While a big value (such as the 1st bit-plane) makes the quality of the image to be extremely degraded (89). The embedding process can be illustrated using the LSB method into various image formats. Assume the bit-plane is:



| 1st Bit-plane | 2nd Bit-plane | 3rd Bit-plane | 4th Bit-plane | 5th Bit-plane | 6th Bit-plane | 7th Bit-plane | 8th Bit-plane |
|---|---|---|---|---|---|---|---|
| MSB | | | | | | | LSB |

1) Let C be the original 8-bit greyscale cover image of (Mc ×Nc) pixels represented as:

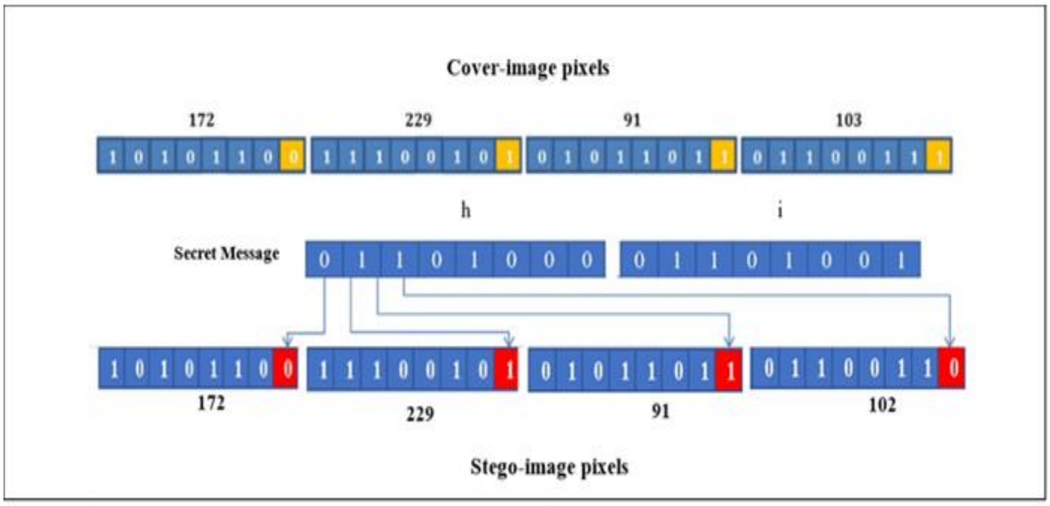
$$C = \{Xij \mid 0 \le i \le Mc , 0 \le j < Nc, Xij \in \{0, 1, \dots , 255\} \}$$ Eq. (1)

M refers to the secret message that has n-bit, represented as:

$$= \{mi \mid 0 \leq i \leq n, \quad mi \in \{0, 1\}\ \} \qquad \text{Eq. (2)}$$

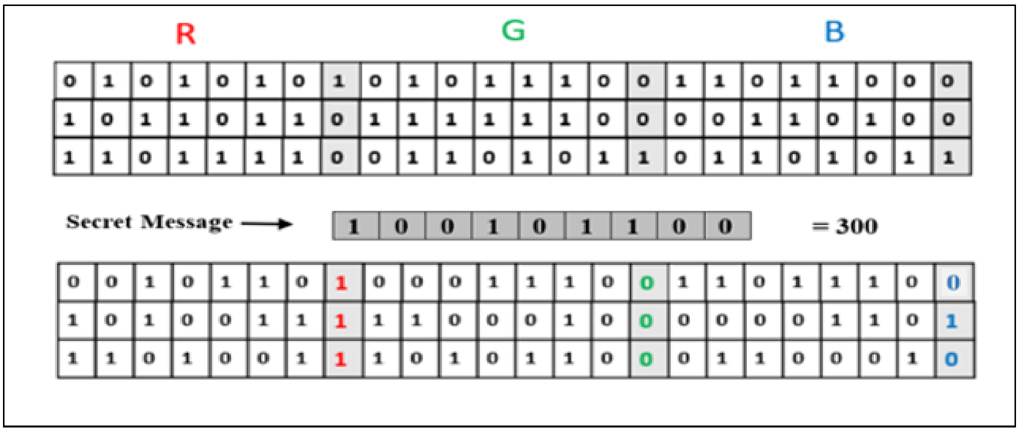
For instance, to hide the message “hi” inside a digital image, the code needs 8 pixels, i.e. 8 bytes of a cover for each letter.

Figure 5 (a) illustrates the embedded message in grey image. Red bits show the message bit value that is replaced with the cover bits in the LSB position, which are in yellow.



(a)

2) In RGB image representation. To hide a secret message (“100101100”) will need 3 pixels. Figure 5 (b) explains the embedded message in colour image.



| R | | | | | | | | G | | | | | | | | B | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 |

Secret Message ⟶ 1 0 0 1 0 1 1 0 0 = 300

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |

(b)

**Figure 5. Embedding Message in Different Images (a) Grey Image (b) Colour Image (90, 78)**

This work verifies the method of hiding patients’ confidential information in medical images by specifically using the LSB method, due to its simplicity, high embedding rate, and quality maintenance of the medical image. It can be used in helping with the diagnosis of illness as the LSB method does not cause noticeable distortion. However, the LSB technique has many shortcomings. Therefore, this section will investigate what this technique has provided in protecting medical information as many researchers have presented various LSB-based steganography schemes during the recent years to achieve different objectives and requirements. There are many existing works on steganography schemes that utilise LSB (9, 91-101).

For instance, Bremnavas et al. introduced a new steganography scheme for concealing patients’ information inside medical images by using two algorithms (91). In the first algorithm, the patients’ information was converted to the Unicode Transformation Format (UTF), and then inserted by using the LSB algorithm. Next, the chaos algorithm was used to encrypt the medical image. The key restriction of this scheme was the direct application of steganography based-LSB, which was known due to its weakness in some methods of steganalysis. Martiri et. al suggested a method for the authentication of medical images by using LSB-based steganography algorithm through injecting metadata of the image inside the image itself (92). This method focused on reducing ambiguity between patients' data and improving the level of protection by using a Rabin signature. The drawback of the suggested method was that the steganography technique was vulnerable to image processing. Nagaraju and ParthaSarathy proposed a novel method for embedding data of Electrocardiogram (ECG) signals and patient information into cover image by using LSB-based steganography algorithm (93). To enhance the method's security, he ECG signals and patient information were encrypted before the embedding process. Empirical findings pointed that the suggested method was robust and could retrieve the embedded data of patients without any distortion, even in the event of an attack such as Gaussian noise. Meanwhile, Karakis et al. described the steganography scheme based on fuzzy logic-based LSB (FL-LSB) and similarity-based LSB (SM_LSB) techniques for securing medical information by merging them inside one file format (9). The medical information included: (i) the EEG as secret data, additionally the doctor's commentaries and information of a patient, and (ii) MR as the cover image. The proposed scheme based on fuzzy logic (FL-LSB) was used to select the non-sequential LSB of the cover image pixels, while the SM-LSB algorithm was utilized to select LSB pixels for embedding the secret message by a threshold value, which was specific by test and error. The likeness values of the grey levels in the pixels were used to hide the message. Based on the experimental result, the proposed scheme guaranteed the confidentiality of the patients' data and minimised the data depot and transmission capacity of the medical data.

The suggested framework by Naidu et al. focused mainly on the confidentiality of patient data when medical images were transferred via the Internet network (94). The scheme used a combination of two algorithms: (i) the LSB algorithm, which was used for embedding the message inside the medical image to produce stego image, and (ii) the Blowfish algorithm, which was employed for the encryption and decryption of stego image. The weakness of the scheme was that it did not apply any algorithm for dividing the medical image into ROI and RONI regions and which area to exactly embed confidential data. Al-Dmour and Al-Ani presented a secure medical information method based on merged steganography and cryptography techniques (81). The scheme hid encrypted EPRs inside the medical image, specifically in RONI, to achieve confidentiality without affecting ROI, which is an important area for diagnosis. The Hamming code was used in the proposed method to reduce the number of bits that were required to be adjusted in a stego image. The Hamming code was utilised to conceal 3-bits of the secret message (sm1, sm2, and sm3) inside 4-bits of the cover (b1, b2, b3, and b4). The key limitations of this system were: (i) it did not concentrate on the integrity of the ROI region, which is a very important portion for diagnostic, and (ii) the system focused on the protection of patient information only. In 2016, Mantos and Maglogiannis suggested a method based on ROI-reversible steganography for medical image, which provided authentication as well as data integrity and imperceptibility. In this method, patient data and hashes of integrity were placed within ROI, while the information (map) necessitated for recovering the ROI was placed in RONI before being embedded. The AES-128 algorithm was employed in the encryption stage to provide security, while the LSB algorithm was used to embed the ciphertext into the RONI part of the medical image (DICOM). The key drawback of this method was that the ROI extraction and embedding processes, which could be used to hide in the ROI section, were not clarified. Furthermore, this method experienced more space exhaustion when inserting the ROI data into the RONI portion.

Jain et al. proposed a new approach to transfer patients' medical information inside the image of the medical cover by hiding the data using the concept of a decision tree with LSB replacement (96). In steganography, blocks of secret codes were allocated to the cover image to embed the data by the breadth-first search-based mapping process. Experimental results showed that the suggested approach provided privacy for patients' data through the use of the RSA encryption algorithm. Nevertheless, it was only appropriate for a small amount of data. A robust method for steganography in the edge blocks of medical cover image based on the spatial domain, like X-ray or EEG, was proposed by Santhi and Dheeptha (97). The proposed method relied on edge-based embedding for the fact that the human eyes were less susceptible to changes in the sharp areas of the image by using XOR encoding. The edge-pixel LSBs were divided into groups of four each. Using XOR, 3-bits of message were inserted into the LSB pixels of each group. Furthermore, the algorithm proposed a unique key generation randomised approach for every session to select the edge blocks required for embedding patients' information by using a sudoku puzzle template to improve the security of the message being transmitted (97).

Jain et al. added an improvement to their previous scheme of transferring confidential medical data in an improved diagonal queue by using a chaotic standard map, linear feedback shift register (LSFR), and multilevel cryptography by Rabin cryptosystem (96, 98). The confidential message blocks and sub-blocks were distributed randomly by utilising pseudo-random sequences by the sender to the cover image blocks with regard to enhanced diagonal queues. This improved protection levels and provided randomness to the algorithm being proposed. At the steganography level, the LSB replacements using chaos theory and improved diagonal queues were utilised to the protection of data. According to the analysis results, the proposed scheme provided a huge space for embedding as it only hid confidential medical data without the metadata of the cover image. Manisha and Sharmila presented a new approach combining data hiding principles with recognition of text, so that the encoded image survived the same size as the original image (99). Therefore, it was not possible to distinguish between them. The approach made use of a two-stage procedure. Adaptive LSB with the randomised encrypting method was used in the first stage to embed patients's information and to ensure the safe transmission of printed medical statements embedded within the medical image. In the second stage, the principle of extraction of text was utilised for recognising the printed text characters in the transmitted medical record by using stego-key and image processing techniques.

Recently, Hyma et al. proposed a merged technique for enhancing security by using the Blowfish algorithm to encrypt the message first (100). Then, the ciphertext obtained was embedded in an image file using the LSB algorithm to give stego1 image. For providing multilayers of security, the recently generated stego1 image would be inserted inside another same sized cover image with the aid of the LSB algorithm again to obtain stego2 image. Moreover, the SHA-256 algorithm was employed to check the integrity of data when they were outsourced. Mondal and Swain suggested a model of the reversible data hiding (RDH) with a three-layer mechanism of data embedding (101). The suggested scheme essentially covered six processes, namely encryption of image, EPR hiding, embedding of data, recovery of EPR, de-embedding, and decryption of images. The embedding procedure was performed by swapping LSB and complementing LSB. The empirical outcomes displayed big potential in security, embedding capacity, and image quality recovery. Devi et al. proposed a novel method to validate the impact of steganography on T2-weighted MR images to distinguish a normal brain from a pathological brain (102). The key goal of the proposed method was to conceal personal data during the processing of patients' medical data. The LSB replacement was used to embed some data into the MR image and to test if the stego image could yet maintain equal classification accuracy like the original cover image. The proposed method demonstrated the capability of visually masking private patient information with high imperceptibility, efficiency, and least deterioration in the use of the stego image with respect to the original image in the transmitted cover image. The proposed method illustrated the capability of the visually concealed special patient information in the transmitted cover image with high imperceptibility, least deterioration, and high capacity in the use of the stego image with regard to the original cover image. Both of the two images (stego and original) were clearly indistinguishable to the naked eye. From the literature review for steganography in medical images based on the LSB technique, the achievements of this technique are summarised in Table 4.

**Table 4. Achievements and Drawbacks of Medical Image Steganography Based on the LSB Technique**

| Related References | Achievements | | | | | | | | Drawbacks |
|---|---|---|---|---|---|---|---|---|---|
| | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) | |
| Bremnavas et al. (91) | | | | | | | | √ | ● The key restriction was the direct application of LSB-based steganography, which was known for its weakness in some methods of steganalysis |
| Martiri et al. (92) | √ | | | | | | | √ | ● The drawback of the suggested method was that the steganography technique was vulnerable to image processing. |
| Nagaraju and PathaSarth (93) | | | | | √ | √ | | | ● Did not determine which region of the medical image was used for embedding and not subjected to further measures of robustness. |
| Karakis et al. (9) | | | √ | | | | | √ | ● High noise |
| Naidu et al. (94) | √ | | √ | | √ | | √ | √ | ● The weakness of the scheme was that it did not apply any algorithm for dividing the medical image into ROI and RONI regions and which area to embed confidential data exactly. |
| Al-Dmour and Al-Ani (81) | | | | | √ | | √ | √ | ● The proposed method did not concentrate on the integrity of the ROI region, which is a very important portion for diagnostic.<br>● The system focused on the protection of patient information only. |
| Mantos and Maglogiannis (95) | √ | √ | | | √ | | | | ● In this method, more space exhaustion was apparent when inserting the ROI data into the RONI portion. |
| Jain et al. (96) | | | | √ | √ | | √ | √ | ● The method was only appropriate for a small amount of data. |
| Santhi and Dheepta (97) | | | | | √ | | | √ | ● The method suffered from a severe setback due to lower embedding capacity and higher computational cost. |
| Jain et al. (98) | | | | | √ | | √ | √ | ● High complexity |
| Manisha and Sharmila (99) | | | | | √ | | | √ | ● There was no evidence to evaluate the proposed method to demonstrate the results. |
| Hyma et al. (100) | | √ | | | | | | √ | ● The proposed framework had not been evaluated. |
| Mondal and Swain (101) | √ | | | √ | √ | | √ | √ | ● The proposed mechanism for determing ROI was unclear. |
| Devi et al. (102) | | | | √ | √ | | √ | | ● The proposed framework found a trade-off between privacy and classification. |

Notes: (1) Authentication, (2) Integrity, (3) Confidentiality, (4) Privacy, (5) Imperceptibility, (6) Robustness, (7) Capacity, and (8) Security

Although there are numerous research on medical image steganography that rely on the spatial domain and the LSB method, particularly it is noted from Table 4 that the LSB method achieved high embedding capacities with preservation of image quality. Nevertheless, it was vulnerable to any alteration by the attackers like rotation, scaling, cropping, and resizing, which might occur when an image was processed. Therefore, the researchers resorted to combining encryption and steganography together and mixing the frequency domain and spatial domain techniques to achieve secrecy in transmitting the information. This might yield better outcomes in terms of security and robustness.

## Results and Discussion:

The previous section introduced a detailed review of the spatial domain, especially image steganography techniques using LSB in the telemedicine field. The investigation of pros and cons of these techniques with respect to main steganography benchmark parameters (i.e. imperceptibility, capacity, robustness, and security) revealed that it is difficult to achieve satisfactory performance of the previous parameters simultaneously. It is evident that one or a sub-set of these parameters have been optimised by various approaches; however, they still conflicted with the other remaining parameters. Consequently, there is a necessity to develop methods of image steganography that can provide an optimal trade-off between these parameters for the application of telemedicine. Moreover, in order to achieve confidentiality and security in the sharing of patient information in telemedicine applications, medical image steganography requires an emphasis on other essential criteria, such as privacy and authentication.

## Conclusion:

This paper presented an investigation of information security techniques that was conducted due to the widespread participation in the exchange of information via the Internet, whereby many issues have emerged that require a solution. The variety of information security techniques have helped protect information; however, each has advantages and disadvantages. The study surveyed some of these techniques, especially in the field of telemedicine due to the importance of this field in helping a large segment of people by reducing the cost of treatment and time for patients and health institutions. At present, as steganography advances, the sharing of medical information, including reports and images, can become much safer. It turns out that medical image steganography has special requirements, which has made it become the focus of attention of many researchers. In this paper, the focus has been placed on the LSB technique by highlighting its important achievements, particularly related to the telemedicine domain due to its simplicity, high embedding rate, and the main goal of maintaining of medical image quality.

## Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Besides, the Figures and images, which are not ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in our organization.

## References:

1. Nosrati M, Hanani A, Karimi R. Steganography in image segments using genetic algorithm. In 2015 Fifth International Conference on Advanced Computing & Communication Technologies:IEEE. 2015;102-107.
2. Sugathan S. An improved LSB embedding technique for image steganography. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT):IEEE. 2016;609-612.
3. Usman MA, Usman MR, Shin SY. Quality assessment for wireless capsule endoscopy videos compressed via HEVC: From diagnostic quality to visual perception. Computers in biology and medicine. 2017;91,112-134.
4. Thanki R, Borra S. Medical imaging and its security in telemedicine applications:Springer. 2019.
5. Fatehi F, Wootton R. Telemedicine, telehealth or e-health? A bibliometric analysis of the trends in the use of these terms. Journal of telemedicine and telecare. 2012;18(8), 460-464.
6. Sajedi H, Yaghobi SR. Information hiding methods for E-Healthcare. Smart Health. 2019;100104.
7. Ali NA, Khalifa O, Abd Manaf A. ICT in telemedicine: Conquering privacy and security issues in health care services. Electronic Journal of Computer Science and Information Technology: eJCIST. 2013;4(1).
8. Allaf AH, Kbir MA. A review of digital watermarking applications for medical image exchange security. In The proceedings of the third international conference on smart city applications:Springer, Cham. 2018;472-480.
9. Karakış R, Güler İ, Capraz I, Bilir E. A novel fuzzy logic-based image steganography method to ensure medical data security. Computers in biology and medicine. 2015;67 172-183.
10. Rani M, Deep EG. Review Paper on Digital X-Ray Image and Steganography. IJRECE. 2017;5(3), 344–348.
11. Thomas DS, Moorthi M, Muthalagu R. Medical image compression based on automated ROI selection for telemedicine application. Int. J. Eng. Comput. Sci. 2014;3,3638-3642.
12. Qasim AF, Aspin R, Meziane F, Hogg P. ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images.

Multimedia Tools and Applications. 2019;78(12), 16433-16463.
13. Larobina M, Murino L. Medical image file formats. Journal of digital imaging. 2014;27(2), 200-206.
14. Shin HB, Sheen H, Lee HY, Kang J, Yoon DK, Suh TS. Digital imaging and communications in medicine (DICOM) information conversion procedure for SUV calculation of PET scanners with different DICOM header information. Physica Medica. 2017;44, 243-248.
15. Al-Haj A. Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. Journal of digital imaging. 2015;28(2), 179-187.
16. Raúl RC, Claudia FU, Trinidad-BIas GDJ. Data hiding scheme for medical images. In 17th International Conference on Electronics, Communications and Computers (CONIELECOMP'07). 2007.
17. Qasim AF. Reversible and imperceptible watermarking approach for ensuring the integrity and authenticity of brain MR images. [Doctoral dissertation]:University of Salford. 2019.
18. Shini SG, Thomas T, Chithraranjan K. Cloud based medical image exchange security challenges. Procedia Engineering. 2012;38, 3454-3461.
19. Varma DR. Managing DICOM images: Tips and tricks for the radiologist. The Indian journal of radiology & imaging. 2012;22(1), 4.
20. Das S, Kundu MK. Effective management of medical information through ROI-lossless fragile image watermarking technique. Computer methods and programs in biomedicine. 2013;111(3), 662-675.
21. Arumugham S, Rajagopalan S, Rayappan JBB, Amirtharajan R. Networked medical data sharing on secure medium–A web publishing mode for DICOM viewer with three layer authentication. Journal of biomedical informatics 2018;86, 90-105.
22. Arsalan M, Qureshi AS, Khan A, Rajarajan M. Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. Applied Soft Computing. 2017;51, 168-179.
23. Haas S, Wohlgemuth S, Echizen I, Sonehara N, Müller G. Aspects of privacy for electronic health records. International journal of medical informatics. 2011;80(2), e26-e31.
24. Fu C, Zhang GY, Bian O, Lei WM, Ma HF. A novel medical image protection scheme using a 3-dimensional chaotic system. PloS one. 2014;9(12).
25. Brumen B, Heričko M, Sevčnikar A, Završnik J, Hölbl M. Outsourcing medical data analyses: can technology overcome legal, privacy, and confidentiality issues?. Journal of medical Internet research 2013;15(12), e283.
26. Li M, Poovendran R, Narayanan S. Protecting patient privacy against unauthorized release of medical images in a group communication environment. Computerized Medical Imaging and Graphics. 2005;29(5), 367-383.
27. Cao F, Huang HK, Zhou XQ. Medical image security in a HIPAA mandated PACS environment. Computerized medical imaging and graphics. 2003;27(2-3), 185-196.
28. Ramakrishnan S. Cryptographic and Information Security Approaches for Images and Videos:CRC Press. 2018.
29. Idakwo MA, Muazu MB, Adedokun AE, Sadiq BO. An Extensive Survey of Digital Image Steganography: State of the Art. ATBU Journal of Science, Technology and Education. 2020;8(2), 40-54.
30. Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A. Secure medical data transmission model for IoT-based healthcare systems:IEEE Access. 2018;6, 20596-20608.
31. Yahya, A. Steganography Techniques for Digital Images:Springer. 2019.
32. Pujari MAA, Shinde MSS. Data Security using Cryptography and Steganography. IOSR Journal of Computer Engineering. 2016;18(04), 130–139. https://doi.org/10.9790/0661-180405130139.
33. Kadhim IJ, Premaratne P, Vial PJ, Halloran B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing. 2019;335(xxxx),299–326. https://doi.org/10.1016/j.neucom.2018.06.075.
34. Dhaked D, Yadav S, Mathuria M, Agrawal S. User Identification Over Digital Social Network Using Fingerprint Authentication. In Emerging Trends in Expert Applications and Security:Springer, Singapore. 2019;11-22.
35. Ou L, Qin Z, Yin H, Li K. Chapter 12 -Security and Privacy in Big Data. Big Data: Principles and Paradigms. 2016;285–308. https://doi.org/10.1016/B978-0-12-805394-2.00012-X.
36. Haddada LR, Dorizzi B, Amara NEB. A combined watermarking approach for securing biometric data. Signal Processing: Image Communication. 2017;55, 23-31.
37. Gupta V, Singh S. Secure Image Steganography & Digital Water Marking. 2012.
38. Saleh ME, Aly AA, Omara FA. Data security using cryptography and steganography techniques. IJACSA) International Journal of Advanced Computer Science and Applications. 2016;7(6), 390-397.
39. Asanbe M. Hybrid Data Security: A Review of Cryptography And Steganography Techniques. Villanova Journal of Science, Technology and Management, 2020;2(1).
40. Tripathi R, Agrawal S. Comparative study of symmetric and asymmetric cryptography techniques. International Journal of Advance Foundation and Research in Computer (IJAFRC). 2014;1(6), 68-76.
41. Paar C, Pelzl J. Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media. 2009.
42. Sheena S, Mathew S. Multimodal biometric authentication: secured encryption of iris using fingerprint ID. International Journal on Cryptography and Information Security. 2016;6(3/4), 39-46.

43. Lee HY. Adaptive reversible watermarking for authentication and privacy protection of medical records. Multimedia Tools and Applications. 2019;78(14), 19663-19680.
44. Tiwari A, Thakur YS. Multi Layer Image Steganography-Encryption mechanism employing DCT-DWT and Chaotic Network. International Journal of Applied Engineering Research. 2019;14(18), 3696-3700.
45. Mehta DM, Bhatti DG. Research Review on Digital Image Steganography Which Resists Against Compression. In Emerging Trends in Expert Applications and Security:Springer, Singapore. 2019;529-534.
46. Qadir AM, VarolN. A Review Paper on Cryptography. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS):IEEE. 2019;1-6
47. Kannammal A, Subha Rani S. Two level security for medical images using watermarking/encryption algorithms. International Journal of Imaging Systems and Technology. 2014;24(1), 111-120.
48. Al-Haj A. Secured telemedicine using region-based watermarking with tamper localization. Journal of digital imaging. 2014;27(6), 737-750.
49. Al-Haj A, Hussein N, Abandah G. Combining cryptography and digital watermarking for secured transmission of medical images. In 2016 2nd International Conference on In-formation Management (ICIM):IEEE 2016; 40-46.
50. Sharma A, Singh AK, Ghrera SP. Robust and secure multiple watermarking for medical images. Wireless Personal Communications. 2017;92(4), 1611-1624.
51. Khond S, Vijayakumar B. Selective medical image watermarking and encryption for image security. International Journal of Pure and Applied Mathematics 2018;118(14), 191-196.
52. Mehta G, Dutta MK, Kim PS. Biometric data security using joint encryption and watermarking. International Journal of Electronic Security and Digital Forensics. 2019;11(4), 379-394.
53. Thakur S, Singh AK, Ghrera SP, Elhoseny M. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. Multimedia tools and Applications. 2019;78(3), 3457-3470.
54. Singla G, Singh C. A Review on Steganography Data Hiding using Color Images. 2019.
55. Atee HA, Ahmad R, Noor NM, Ilijan AK. A combined crypto-stego system using dynamic encryption assisted intensity color steganography. International Journal of Control Theory and Applications. 2016;9(30), 175–184.
56. Pandey R, Singh AK, Kumar B, Mohan A. Iris based secure NROI multiple eye image watermarking for teleophthalmology. Multimedia Tools and Applications. 2016;75(22), 14381-14397.
57. Trehan M, Mittu S. Steganography and cryptography approaches combined using medical digital images. International Journal of Engineering Research & Technology (IJERT). 2015;4.
58. Jain M, Lenka SK. Diagonal queue medical image steganography with Rabin cryptosystem. Brain informatics. 2016;3(1), 39-51.
59. Khalil MI. Medical image steganography: study of medical image quality degradation when embedding data in the frequency domain. International Journal of Computer Network and Information Security. 2017;9(2), 22.
60. Banjan N, Dalvi P. Medical Data Security using combination of Cryptography and Steganography with AES-LSB algorithm. 2018;7(7), 31–45.
61. Babatunde AO, Taiwo AJ, Dada EG. Information Security in Health Care Centre Using Cryptography and Steganography. 2018. arXiv preprint arXiv:1803.05593.
62. Gulia S, Mukherjee S, Choudhury T. An extensive literature survey on medical image steganography. CSI transactions on ICT. 2016;4(2-4), 293-298.
63. Yüksel B, Küpçü A, Özkasap Ö. Research issues for privacy and security of electronic health services. Future Generation Computer Systems. 2017;68, 1-13.
64. Manivannan M, Suseendran G. A Review of Watermarking Requirements, Techniques, Documents, Human Perception and Applications for Medical Images.
65. Santhi G, Adithya B. A Survey on Medical Image Protection Using Various Steganography Techniques. Advances in Natural and Applied Sciences. 2017;11(12), 89-94.
66. Atawneh S, Almomani A, Sumari P. Steganography in digital images: Common approaches and tools. IETE Technical Review. 2013;30(4), 344-358.
67. Aparna P, Kishore PVV. An efficient medical image watermarking technique in E-healthcare application using hybridization of compression and cryptography algorithm. Journal of Intelligent Systems. 2018;27(1), 115-133.
68. Luo XY, Wang DS, Wang P, Liu FL. A review on blind detection for image steganography. Signal Processing. 2008;88(9), 2138-2157.
69. Khalind OS. New methods to improve the pixel domain steganography, steganalysis, and simplify the assessment of steganalysis tools. [Doctoral dissertation]:University of Ports-mouth. 2015.
70. Rashid RD. Robust Steganographic Techniques for Secure Biometric-based Remote Authentication. [Doctoral dissertation]:University of Buckingham. 2015.
71. Rashid A, Salamat N, Prasath V. An algorithm for data hiding in radiographic images and ePHI/R application. Technologies. 2018;6(1), 7.
72. Nyeem H, Boles W, Boyd C. A review of medical image watermarking requirements for teleradiology. Journal of digital imaging. 2013;26(2), 326-343.
73. Konyar MZ, Öztürk S. Reed Solomon Coding-Based Medical Image Data Hiding Method against Salt and Pepper Noise. Symmetry. 2020;12(6), 899.
74. Karmakar R, Basu A. Implementation of a Reversible Watermarking Technique for Medical Images. In Intelligent Innovations in Multimedia Data Engineering and Management:IGI Global. 2019;1-37.

75. Al-Dmour HST. Enhancing information hiding and segmentation for medical images using novel steganography and clustering fusion techniques. [Doctoral dissertation]. 2018.
76. Thiyagarajan P, Aghila G. Reversible dynamic secure steganography for medical image using graph coloring. Health Policy and Technology. 2013;2(3), 151-161.
77. Langer SG. Challenges for data storage in medical imaging research. Journal of digital imaging. 2011;24(2), 203-207.
78. Abdulwahedand MN, Mustafa ST, Rahim MSM. Image Spatial Domain Steganography: A study of Performance Evaluation Parameters. In 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET):IEEE. 2019;309-314.
79. Roy R, Changder S. Quality evaluation of image steganography techniques: a heuristics based approach. International Journal of Security and Its Applications. 2016;10(4), 179-196.
80. Kanan HR, Nazeri B. A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Systems with Applications. 2014;41(14), 6123-6130.
81. Al-Dmour H, Al-Ani A. Quality optimized medical image information hiding algorithm that employs edge detection and data coding. Computer methods and programs in biomedicine. 2016;127, 24-43.
82. Parah SA, Sheikh JA, Ahad F, Loan NA, Bhat GM. Information hiding in medical images: a robust medical image watermarking system for E-healthcare. Multimedia Tools and Applications. 2017;76(8), 10599-10633.
83. Fkirin A, Attiya G, El-Sayed A. Steganography Literature Survey, Classification and Comparative Study. Communications on Applied Electronics. 2016;5(10), 13-22.
84. Rai P, Gurung S, Ghose MK. Analysis of image steganography techniques: a survey. International Journal of Computer Applications. 2015;114(1).
85. Anandpara D, Kothari A. Working and comparative analysis of various spatial based image steganography techniques. International Journal of Computer Applications. 2015;113(12).
86. Samidha D, Agrawal D. Random image steganography in spatial domain. In 2013 International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT):IEEE. 2013;1-3.
87. Bharti J, Solanki S, Beliya A. Comparison of LSB methods and pattern. In 2017 International Conference on Recent Innovations in Signal Processing and Embedded Systems (RISE):IEEE. 2017;250-256. IEEE.
88. Kumar R, Murti PR. Data security and authentication using steganography. 2011.
89. Zeki AM, Manaf AA. A novel digital watermarking technique based on ISB (Intermediate Significant Bit). World Academy of Science, Engineering and Technology. 2009;50, 989-996.
90. Shet KS, Aswath AR, Hanumantharaju MC, Gao XZ. Design and development of new reconfigurable architectures for LSB/multi-bit image steganography system. Multimedia Tools and Applications. 2017;76(11), 13197-13219.
91. Bremnavas I, Poorna B, Kanagachidambaresan GR. Medical image security using LSB and Chaotic Logistic Map. 2011.
92. Martiri E, Baxhaku A, Barolli E. Steganographic algorithm injection in image information systems used in healthcare organizations. In 2011 Third International Conference on Intelligent Networking and Collaborative Systems:IEEE. 2011;408-411).
93. Nagaraju C, ParthaSarathy SS. Embedding ECG and patient information in medical image. In International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014):IEEE. 2014;1-6.
94. Naidu CD, Koppu S, Viswanatham VM, Aarthy SL. Cryptography Based Medical Image Security with LSB Blowfish Algorithms. ARPN Journal of Engineering and Applied Sciences. 2014;9(8).
95. Mantos PL, Maglogiannis I. Sensitive patient data hiding using a ROI reversible steganography scheme for DICOM images. Journal of medical systems. 2016;40(6), 156.
96. Jain M, Choudhary RC, Kumar A. Secure medical image steganography with RSA cryptography using decision tree. In 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I):IEEE. 2016;291-295.
97. Santhi B, Dheeptha B. A novel edge based embedding in medical images based on unique key generated using sudoku puzzle design. SpringerPlus. 2016;5(1), 1670.
98. Jain M, Kumar A, Choudhary RC. Improved diagonal queue medical image steganography using Chaos theory, LFSR, and Rabin cryptosystem. Brain informatics. 2017;4(2), 95-106.
99. Manisha S, Sharmila TS. Recognition of Characters in a Securely Transmitted Medical Image. In International conference on Computer Networks, Big data and IoT:Springer, Cham. 2018;286-292.
100. Hyma J, Sudamalla M, Vanaparthi DT, Vinnakota K, Choppavarapu VK. A New Frame-work for Secure Outsourcing of Medical Data. In Intelligent Manufacturing and Energy Sustainability:Springer, Singapore. 2020;759-767.
101. Mondal J, Swain D. A 3-layer RDH method in encrypted domain for medical information security. International Journal of Electronic Security and Digital Forensics. 2020;12(1), 1-15.
102. Devi S, Sahoo MN, Muhammad K, Ding W, Bakshi S. Hiding medical information in brain MR images without affecting accuracy of classifying pathological brain. Future Generation Computer Systems. 2019;99, 235-246.

# مراجعة شاملة لإخفاء الصور الطبية بناءً على تقنية LSB والتحديات المحتملة

بشرى عبدالله اشتيت [1]    نور حارياني زكريا [2]    نور حزلينا هارون [2]

[1] الجامعة التقنية الجنوبية، البصرة، العراق
[2] جامعة أوتارا ماليزيا، ماليزيا

**الخلاصة:**

أدى التطور السريع لخدمات التطبيب عن بعد ومتطلبات تبادل المعلومات الطبية بين الأطباء والاستشاريين والمؤسسات الصحية إلى جعل حماية معلومات المرضى أولوية مهمة لأي نظام صحي إلكتروني مستقبلي. حماية المعلومات الطبية ، بما في ذلك الغلاف (أي الصورة الطبية) ، لها خصوصية تختلف قليلاً عن متطلبات حماية المعلومات الأخرى. من الضروري الحفاظ على الغطاء بشكل كبير نظرًا لأهميته من جانب الاستقبال حيث يستخدم الطاقم الطبي هذه المعلومات لتقديم تشخيص لإنقاذ حياة المريض. إذا تم العبث بالغطاء ، فهذا يؤدي إلى الفشل في تحقيق هدف التطبيب عن بعد. لذلك ، يوفر هذا العمل تحقيقًا في تقنيات أمن المعلومات في التصوير الطبي ، مع التركيز على الأهداف الأمنية. يوفر تشفير الرسالة قبل إخفائها طبقة إضافية من الأمان ، وبالتالي ، سيوفر حلاً ممتازًا لحماية المعلومات الحساسة للمرضى أثناء مشاركة المعلومات الطبية. إخفاء الصور الطبية هو حالة خاصة من إخفاء الصور، في حين أن التصوير الرقمي والاتصالات في الطب **(DICOM)**هو العمود الفقري لجميع أقسام التصوير الطبي ، حيث يتم استخدامه على نطاق واسع لتخزين ونقل الصور الطبية. الهدف الرئيسي من هذه الدراسة هو تقديم فكرة عامة عما حققته تقنيات إخفاء المعلومات على أساس البتات الأقل أهمية **(LSB)** في الصور الطبية

**الكلمات المفتاحية**: (dicom) الأقل دلالة، إخفاء الصور، أمن المعلومات ، التصوير الطبي بالبت الأقل أهمية (LSB) ، التطبيب عن بعد.