DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

A Comprehensive Review on Security of Medical Image in Telemedicine

Arwa Sabah Ridha[1], Ashwaq T. Hashim[2]
[1]Department of Computer Sciences, University of Technology, Baghdad, Iraq
[2]Control and System Engineering Department, University of Technology, Baghdad, Iraq
[1]arwa.s2004@gmail.com, [2]60102@uotechnology.edu.iq

Abstract— *Medical imaging is a sensitive and important type of data that requires robust encryption to protect it during transmission over networks. Confidentiality is a critical aspect to consider when securing information systems, and encryption techniques. These images have unique characteristics, including large data size, redundancies, and similarities between neighboring pixels, making them different from text. To confirm the security of medical images and prevent unauthorized access or manipulation, highly secure algorithms are necessary due to the rapid advancement of network technologies. This survey aims to explain the different methods currently used to protect medical data, such as encryption, steganography, steganography, and methods of hiding, as well as the difference between full encryption of the medical image and partial encryption only of the important sections of the images. In order to arrive at the most effective approach, a number of prior experiences and studies were used. This article discusses recent advancements in this field, highlighting the need for secure encryption schemes to withstand adversarial attacks and ensure the confidentiality of medical images.*

Index Terms— *Medical Image, Encryption, Decryption, Steganography, Hiding Data.*

I. INTRODUCTION

Nowadays, information is transmitted through the internet rapid which includes everything from simple texts, images, to video materials. Conversely, the internet is vulnerable to different forms of attack hence the need for encryption so as to protect confidential data against eavesdroppers. The principle of Confidentiality, Integrity and Availability is used for medical images that can be employed in medical sciences, military communication or biometric applications [1].

In some cases, like image medical, data embedding is necessary in order to encompass other useful information like the patient's particulars and notes from the doctor into the bigger database set up for ease of retrieval by an authorized user. In order for medical images to be effective, data hiding must possess several essential properties; namely high-quality data is required to ensure that it is undetectable but still possible to recover in case of necessity. The medical files must be secure, accessible and complete enough [2]. Some of the widely used imaging systems in medicine include computed tomography (CT), magnetic resonance imaging (MRI), PET, and X-ray analysis. These are some of the essential imaging techniques that support medical diagnosis and scientific research as they reveal images with anatomic details which help identify illnesses or conditions in the bodies [3].

In the context of medical images, the impact of digital image technology in medical systems, particularly in the diagnosis of diseases. It focuses on the development of health

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

security through a merger of digital photos with the net. This includes noise detection, feature extraction, image segmentation, watermarking, and image compression for various techniques used with digital images in medical diagnostic procedures highlighting the need for high privacy standards for patient's digital images in healthcare systems [1] [4].

It is now typical for medical institutions to share medical information, containing medical images and patients' records, at a distance. Their relationship also involves an exchange where they share patients' information relevant to care provision between them on a daily basis which has become routine in their joint operation [5]. Image information is transferred in an encrypted fashion so that it appears as secret information. A network-based exchange of images must be protected by using image encryption so that hackers cannot reverse engineer the image. The differences between image encryption and text encryption follow from specific features of images like big size, high redundancy, and spatial correlation which make them different from texts.

In the context of information security techniques, the terms "security," "imperceptibility," "capacity," and "robustness" refer to important characteristics or requirements. Security pertains to protecting information from unauthorized access, imperceptibility relates to hiding the presence of a message, capacity refers to the amount of data that can be concealed, and robustness indicates the ability to withstand attacks or modifications without compromising the hidden information. These characteristics are crucial for ensuring the effectiveness and reliability of security techniques such as cryptography, watermarking, and steganography [6]. Different data hiding techniques have been recommended by researchers over the last two decades on the medical image. These methods are intended to address specifications of high-quality, reversibility and high capacity. Nevertheless, different means not necessarily all meet the three requirements at once. Therefore, classification is made in terms of a particular element that addresses.

II. LITERATURES ANALYSIS

Digital medical images are used more and more often for diagnosis and treatment which leads it to be paid more attention to [7]. However, all that should not be forgotten when there is great amount of privacy involved, and some of them, though not many, may have a high the potential for disastrous accidents arises when such private photos are stolen accessed or used by non-authorized accesses. The unlawful utilization of medical imaging by a hacker or an evil database administrator can result in dire consequences like medical marketing and fraudulent insurance claims that often lead to death. Thus, it is very crucial to protect medical images [8] [9].The fundamental steps for medical image encryption are illustrated in *Fig. 1*.

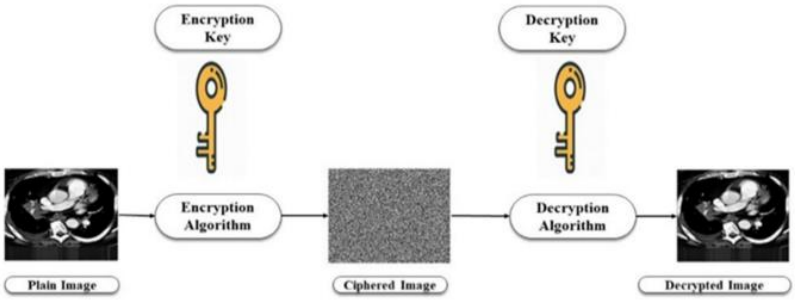

FIG. 1. MIDICAL IMAGE ENCRYPTION[10].

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

A. Review Based on Medical Image Encryption

Securing digital images can be accomplished through several methods, involving image steganography, image watermarking, and image encryption [11]. Between these methods, encryption is considered the most effective approach for ensuring the security of medical images. Encryption involves converting the original image into an unreadable form utilizing a secret key, making it impossible to restore the image without the key [12] [13]. It is a technique for converting image into a distorted form. There are three types of image encryption.

- Fully image Encryption
- Partial Image Encryption
- Selective Image Encryption

i. Full image encryption

This section discusses the concept of fully layered image encryption, which involves encrypting the entire image. This encryption scheme is suitable when there are no restrictions on content transmission but has drawbacks such as slow execution time and limitations in terms of scalability and bandwidth. These limitations can lead to disabled functionalities and high transmission rates as shown in *Fig. 2.*

.

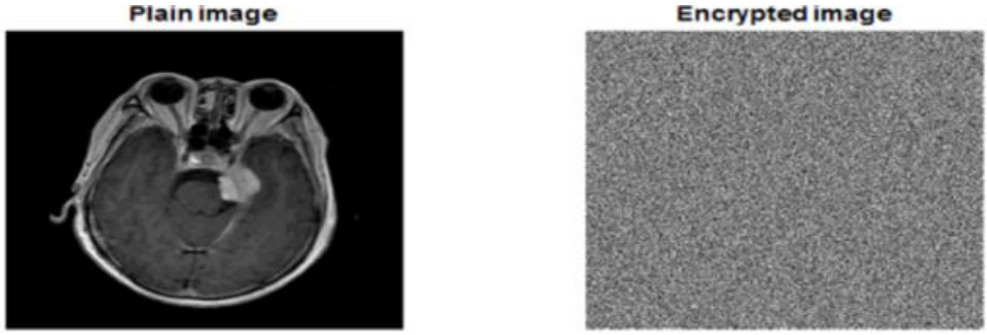

FIG. 2. FULL ENCRYPTION [14].

Boussif, M., et al (2017) [15] introduced new approach for m-Health secure mobile medical imagery retrieval. A novel semi-reversible watermarking technique, robust against JPEG compression, is combined here with proposed new fragile watermarking and encryption algorithm. This will ensure total security for the medical images, their information and reports with regard to confidentiality, authenticity and integrity respectively. The experimental demonstrates that their suggested algorithm makes a great deal of protection and performance while implemented on the Android platform.

Kumar, S.,et al (2019) [16] suggested Protecting medical data by a hybrid technique; chaotic map combined with the FrDCT medical image coefficients. FrDCT is flexible encryption for medical images with proposed algorithm; apply FrDCT to image and then use chaotic map on FrDCT coefficients. The algorithm is better than FRFT on the parameter α, and experimental studies show its efficiency exceeding other methods.

Manjula G. & Mohan H. S. (2020) [17] proposed enhanced AES encryption of patient data coupled with cover-up of medical imaging for secure communication channel. In addition, they include an updated S-box that is based on a Hash function, in order to improve their Rijndael AES encryption. This method seeks to provide strong safety precautions in safeguarding patients' data as medical image transmission.

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

Priya, S., & Santhi, B. (2021) [18] proposed an approach for rendering watermarked medical information invisible through visual encryption. Furthermore, an authentication of the source through biomic-based authentication approach is proposed. This method consists of image encryption via visual meaning and finger print image encryption which produced favorable experimental outcomes while avoiding attacker difficulties.

Hashim A., et al. (2021) [19] presented an image encryption system with the goal of increasing security and efficiency. The system employs both block-based encryption and chaotic map features. The method overcomes problems in the Blowfish algorithm and delivers increased security and performance, providing good encryption performance for pictures.

Hashim A., et al. (2021) [20] called the class of techniques with quadratic maps, researchers put forward to minimize pixel correlations and entropy in medical images. Finally, the encryption has been done by using advanced encryption standard picture cypher for confusion and diffusion, the approach ensured secrecy when pictures containing confidential information are transferred over networks.

Jirjees S., et al. (2022) [21] proposed several new guidelines to improve the design of traditional block ciphers, and in addition especially emphasized improving their image encryption ability. They propose the use of a hyperchaotic system and Chebyshev maps to attain low pixel correlation; and introduce an RC6-like block cipher with 3-D permutation modes. The encryption technique employs a Feistel network of type three in cascaded architecture, with the like-chaining process where decoding ciphertext block depends on previous blocks and has great prospects for secure image transmission.

Li, X., & Peng, H. (2023) [22] proposed a mechanism called ResNet showed that encryption and decryption of medical images relied on a deep learning architecture. The jump connections and residual subnetworks in the ResNet, ResNet used to extract meaning from images, but also speed up model convergence. With a logistic chaotic system used to encrypt the ResNet model output, unpredictability, and complexity are brought into play within encryption itself. Besides, an attention strategy is employed to make the model more sensitive towards ROI in medical images and further enhance encrypted network security.

Wang, X., & Wang, Y. (2023) [23] provided an encryption technique for numerous medical images to fulfill the security needs in electronic medical systems. Researchers used a ROI method, the system encrypted grayscale and color medical images at the same time. The approach increased overall security by the coordinates and hash value of the plaintext images as the secret key. The Logistic-Tent chaotic system generated chaotic sequences for scrambling and diffusion throughout the encryption process, resulted in excellent encryption effectiveness, resistance to numerous assaults, and quicker encryption speed.

ii. Partial Image Encryption

Partial encryption protects only a portion of communications that are particularly important, requiring less light projection but providing sufficient data security. So the best way is to encrypt certain parts in combination with taking standard samples. This approach tries to find a middle ground between security and efficiency, particularly in real-time multimedia communications. Lots of encrypted data is expensive, not just monetarily but in terms of keeping the connection stable as well [24].

This means dividing data into two halves, one encrypted using a standard or new cipher and the other not. The encrypted and unencrypted parts are reassembled to recapture the original material, with decryption steps following those of encryption. As a strategy to reduce computational complexity in safe image encryption, partial-encryption is

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

increasingly used. The image is divided into two parts, one encrypted and the other unchanged. Decryption is the reverse process of encryption [25].

For this reason, the partial image encryption approach is often used to maintain a balance between privacy and security on one hand; visual quality and usefulness of images on the other. Also by reducing amounts of encrypted data it provides cheaper methods with adequate levels personal confidentiality as shown in *Fig. 3*.

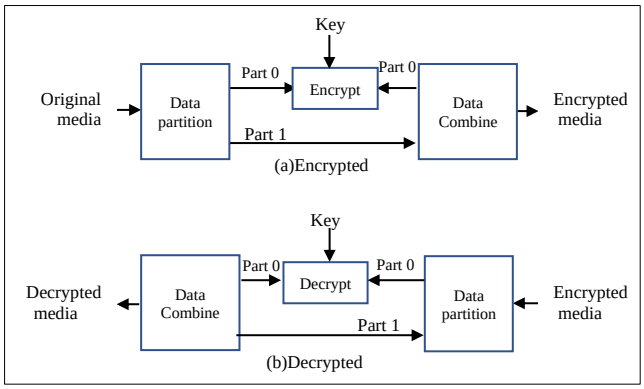

FIG.3. BLOCK DIAGRAM OF PARTIAL ENCRYPTION/DECRYPTION [25].

Parameshachari et al (2017) [26] suggested using dual DNA addition and combining chaotic map to partially encrypt medical images. The approach included encoding the grayscale image using multiple patterns, doing DNA addition with a chaotic sequence derived from a random number table (a chaotic map), and modifying these to get different Partial Encrypted Images.

Abdmouleh, M. et al (2019) [27] described a method for encrypting medical images by selectively encrypting certain coefficients obtained through a mathematical transformation called discrete cosine transform (DCT). By encrypting specific DCT coefficients at both low and high frequencies, the system achieved a significant decrease in processing time through encryption and decryption, while maintaining the high compression rate of the compression algorithm used for the images.

Heidari, S., et al (2019) [28] proposed a new method of quantum selective encryption approach toward encrypting medical images. In a nutshell. The method they have proposed for protecting the ROI is based on modifying the bit depth planes of the given image with a specific key and results show that pixels are less correlated with histogram analysis showing good performance as compared to the entropy rate.

Kiran & Parameshachari (2021) [29] presented a scheme for partial image encryption in which, LSM is employed to selectively choose and encrypt image blocks according to a percentage value. The level of encryption can also be adjusted based on the adjustment of the control threshold value. The method improved security while also cutting down computing requirements and ensuring real–time applications of encryption with reduced complexity.

Li, J. et al (2020) [30] developed an algorithm for the protection of vital sections in medical images. The regions with high values of coefficient of variation were located using this measure, while other regions were analyzed based on texture complexity. A reversible data-hiding algorithm designed for identified regions embedded in high-texture zones. For security purposes, arnold transformation was used. Lastly, they created a qr code based on the encryption parameters, and image basic information used for substituting the original key regions.

Received 10/December/2023; Accepted 19/January/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

P. Rashmi et al (2023) [31] introduced the Improved Chaos Encryption (ICE) approach and made use of the Lorenz 96 model to increase unpredictability and improve security. Based on experimental data, the peak signal-to-noise ratio (PSNR) of 104.7 dB is achieved by the ICE model, which is a better outcome than the LSB-ROI technique.

iii. Selective Image Encryption

The selective image encryption is proved to be of great value in many fields because it can help cut the computing expenses, time and cost. The advantage of selective encryption is enhanced efficiency compared to traditional encryption procedures that encipher the whole image instead of certain regions of the photos. Unlike full image encryption algorithms that have proven to be computing extensive, this approach attempts to address this by utilizing less sophisticated processing.

Cao, W., et al (2017) [32]described a way to encrypt medical images, with edge maps taken from the source image used for encryption. The algorithm divided into three parts: Bit-plane decomposition, random sequence generation, and permutation. They can choose from a variety of advantages that include any type of image as the source, cascading multiple permutation techniques in order, and selecting alternative bit-plane decomposition methods. The fourth advantage is the freedom to build different edge maps with alternate combinations of feature detectors or choice thresholds. The proposed algorithm has a large key space, strong sensitivity to changes in the key, and good robustness to security attacks against it.

Parameshachari, et al. (2020) [33] proposed The ROI selective image encryption methodology based on techniques of permutation and diffusion, which involved development with a Hilbert curve and Skew Tent map-based active contour image segmentation strategy for the groundwork after decomposition utilizing an adaptive cascade filtering technique. The suggested method has the potential to improve image security through histogram tools, diffusion characteristic testing, entropy or correlation analysis, and key sensitivity.

Kiran & B. Parameshachari (2020) [34] suggested a method that encrypts only particular regions of the image using both threshold entropy and ACM. The approach proposed achieved lossless encryption with low computational complexity and fast execution time by detecting significant blocks in the source image and determining insignificant.

Khashan, O. & AlShaikh, M. (2020) [35] proposed encryption method aimed at protecting medical image edge maps. The suggested encryption method used a one-time pad algorithm to encrypt important image blocks, which allowed acceptable throughput (adequate for real-time applications) with fast and simple procedures of both the process of running it in conjunction with easy privacy key management. The method resulted robust resistance against cryptography security violation attacks.

Shen, Y.,et al (2021) [36] proposed a selective encryption scheme for medical images using the Fuzzy C-Means Clustering algorithm and face biometric. Researchers introduced a method to extract the ROI based on the algorithm and generate a random phase mask using face biometrics for encryption.

Selective encryption encrypts only some portions or objects of an image, leaving the remainder of the image unencrypted. Only the targeted areas are protected due to selective encrypting it while the remainder of the image was unchanged.

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

TABLE I. SUMMARY OF MEDICAL IMAGE ENCRYPTION TECHNIQUE AND RESULTS COMPARISON

C	Image Dataset	Image Type & Size	Encryption Type	Method	Evaluation Metrics Result	Limitations	Execution Time (secs)
Parameshachari et al (2017) [26]	medical images	Gray	Partial Encryption	PIE using DNA coding and dual DNA	NPCR 100.000 UACI 55.19088 MSSIM - 0.1995 UQI 0.36326 MSE 38.2238	susceptible to error Rates and Reliability	It reduces the computational time
Boussif, M., et al (2017) [15]	MR imaging CT imaging DX imaging SC imaging	Gray 560×560 512x512 2022x1736 224x176	Full Encryption	m-Health semi-reversible watermarking	NPCR 99.8964 UACI 33.4545 Entropy 7.9417	Applicability specially with diversity of medical images and the specific requirements of m-Health scenarios	good performance implemented on the Android platform.
Cao, W., et al (2017) [32]	Medical image (MRI, X-ray, CT and US)	256 × 256	Selective Encryption	fuzzy edge maps EMMIE	NPCR 99.60% UACI 33.48%	concerns about the computational efficiency, especially when dealing with large medical image datasets	less time cost
Kumar, S.,et al (2019) [16]	Medical images	Gray 512 × 512	Full Encryption	FrDCT	NPCR 99.609375% UACI 33.463541% Correlations Horizontal 0.01723 Vertical 0.014486 Diagonal 0.01984	Limited Evaluation Metrics	0.1594
Heidari, S.,et al (2019) [28]	medical images	Gray	Full Encryption	BRQI		Time Complexity	time complexities
Abdmouleh, M. et al (2019) [27]	medical images	Gray	Partial Encryption	DCT	-	potential challenges such as noise	achieves a significant reduction in processing time during encryption and decryption
Manjula G. & Mohan H. S. (2020) [17]	medical images	-	Full Encryption	enhanced AES algorithm with new S-box generated	-	Keys management	Encryption 0.204 Decryption 0.15
Li, J. et al (2020) [30]	cancer imaging (TCIA)	Gray 512×512	Partial Encryption	generate a QR code and replace	PSNR 15.8565	key to decode in the QR	-

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

	(Brain, Lung , Neck)		original key regions.		code must be known by authorized users.	
Parameshachari, et al. (2020) [33]	medical images	Gray 256 x 256	Selective Encryption	ROI and ROB	MSE 36.2388 PSNR 32.5391 NPCR 47.5328 UACI 15.5345	used only in real time medical image encryption with limited resource utilization	0.43 sec
Kiran & Parameshachari B. D(2020) [34]	medical images	Gray 256 × 256, 512x512 1024x1024	Selective Encryption	ACM LSB	Entropy 7.982	Complexity in calculation	0.065 sec
Khashan, O. & AlShaikh, M. (2020) [35]	medical images	Gray 225 × 225	Selective Encryption	chaotic map	NPCR 99.017 UACI 32.630	Complexity in operations	0.0669 sec
Priya, S., & Santhi, B. (2021) [18]	DICOM medical	Gray	Full Encryption	biometric-based authentication	NPCR 59.7861 UACI 0.000033	Noise Ratio (PSNR)	-
Hashim A., et al. (2021) [19]	Images	256 × 256	Full Encryption	Modified Blowfish Algorithm	NPCR 99.62 UACI 33.35	Time excution	decrease execution time
Hashim A., et al. (2021) [20]	medical images	-	Full Encryption	Hybrid AES with Chaotic Map	Keyspace 2^{349} NPCR 99.61 UACI 43.55	Key management	-
Kiran & Parameshachari (2021) [29]	Brain Fetus Images	Gray 256 x 256	Partial Encryption	LSM	MSE 35.355 PSNR (dB) 32.646 NPCR 100% UACI 40.876%	Many counting operations with multiple keys used	0.095 **sec**
Shen, Y.,et al (2021) [36]	medical images	Gray	Selective Encryption	FRFCM	The Standard map 0.0105,0.0099 and 0.0166	Involves a lot of processes	Encryption 0.2037 Decryption 0.0402
Jirjees S., et al. (2022) [21]	Images	Color 256 x 256	Full Encryption	RC6-like block cipher with the 3D permutation model	Entropy 7.9981 Correlation - 0.0025	Multiple operations take more time	-
Li, X., & Peng, H. (2023) [22]	MRI and COVID-19 Chest X-ray datasets.	Gray 512 × 512	Full Encryption	ResNet	Entropy 7.9887 Correlation 0.0021	Time excution	-
Wang, X., & Wang, Y. (2023) [23]	medical images	Color and Gray 512 × 512	Full Encryption	LTS	-	Computational Efficiency	faster encryption speed
P. Rashmi et al (2023) [31]	Medical Images	512×512	Partial Encryption	ICE	PSNR 97.61 dB	Excution and time durations	-

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

Table I summarizes numerous image encryption algorithms utilized in many sectors, including medical imaging and cancer imaging. Each technique's image dataset, encryption type, evaluation metrics, and execution time are all listed in the table. Partial encryption, complete encryption, and approaches such as DNA coding, watermarking, and biometric-based authentication are among the strategies listed.

There are two sorts of image encryption techniques, as previously stated: complete image encryption and partial image encryption. Full image encryption encrypts the entire image; however, it has downsides such as lengthy execution time and scalability and bandwidth restrictions. Partial image encryption, on the other hand, focuses on encrypting only specified areas of an image, enabling a balance between security and efficiency, especially in real-time multimedia interactions. Several approaches and algorithms are discussed, emphasizing their benefits and experimental findings in terms of encryption performance and image quality.

B. Review Based on Medical Image Steganography

Steganography is the practice of creating and sending invisible, secret communications [37]. Medical image steganography is a technology used to protect the secrecy of Electronic Patient Records (EPR) while retaining image quality. It entails concealing the EPR and diagnosis report within the medical image, so establishing a link between the patient's information and their image. Therefore, this method skirts over authentication problems and protects patient privacy by hiding sensitive data inside the image [5]. If sensitive data is integrated into medical photographs, then the healthcare worker can send information securely while reducing illegal access or interception risks [37].

How to classify what kind of cover is used, into which field the information pertains and how to employ a hiding method or an extraction method are all described. Classification of many steganography techniques is given in *Fig. 4.* Such classification and categorization can be found throughout this field of research [38]. In image steganography, the cover image is used as a template and information buried inside it using an embedding method. This procedure produces a stego-image, and the encryption yields a key. This reverse embedding function is used during decryption. If the key matches, the secret message can be obtained.

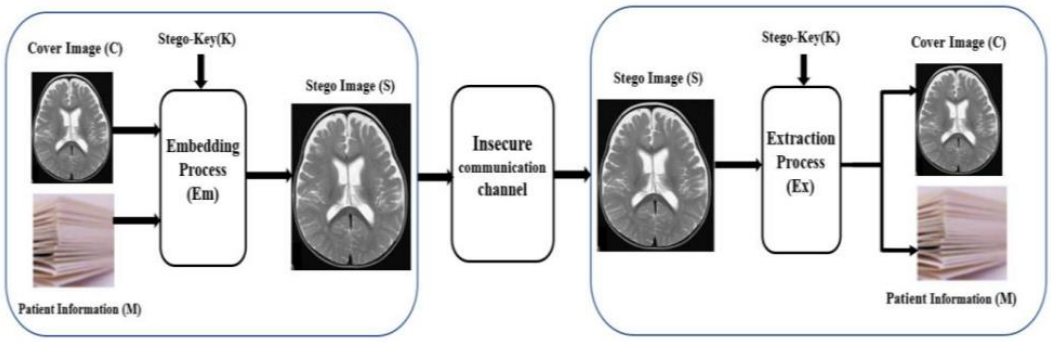

FIG. 4.SCHEME FOR MEDICAL IMAGE STEGANOGRAPHY [38].

The problem with steganography is that, once the existence of a hidden message is discovered or even suspected by an unintended party, the coded information immediately loses its secrecy. That is to say, the effectiveness of steganography depends upon secrecy regarding what has been hidden; once this secret gets out then no longer can messages be said to exist in a veiled form [39].

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

In the realm of information security, there are two primary kinds of image steganography techniques: transform domain and spatial domain. Spatial domain approaches rely on changes in pixel intensities to place hidden data directly into the host image. On the other hand, transform domain techniques change host image coefficients by means of various types of transformation, such as Fourier or wavelet transformations. Transform domain techniques afford greater security, but at a much higher computational cost and with less processing space available; by contrast spatial-domain solutions are simple to implement band cheap [40] [41].

TABLE II. COMPARING IMAGE STEGANOGRAPHY TECHNIQUES IN THE TRANSFORM AND SPATIAL DOMAINS

Division	Spatial domain	Transform domain
Advantages	▪ Because of their simplicity and ease of application, spatial domain approaches in image steganography are popular and frequently employed. ▪ A steganography technique's capacity to conceal a vast quantity of hidden information within an image. ▪ Spatial domain approaches have a shorter computing time than transform domain techniques.	For image steganography, transform domain techniques are more resistant to attacks like geometrical distortions and compression than spatial-based ones. This means that when the transform domain technique is used, hidden information will be less influenced by or altered as a result of such attacks. The steganographic process therefore has greater robustness and security.
Disadvantages	• Being exceedingly fragile and vulnerable to harm from minor changes such as JPEG compression. This implies that when the stego image is transformed or compressed, the concealed message inserted utilizing spatial domain techniques may be readily compromised or lost. • It is not robust with respect to image rotation or cropping. This means that if the stego image generated by these methods is rotated or cropped, hidden information will be un-accessible/lost.	More resistant to attack are transformed domain approaches, such as those based on modifying an image's coefficients. Their ability to embed information is limited though. But compared to spatial domain approaches, in which embedding is done right inside the LSBs of intensity values; doing so requires some extra calculations.
Limitations	• Low Capacity • Vulnerability to Attacks • Reduced Image Quality • Inefficiency in Color Spaces	• Detectability by Advanced Tools • Limited Robustness • Complexity and Computational Overhead • Sensitivity to Key Parameters
Example	LSB	DCT

Embedding capability, imperceptibility and resilience are compared for different spatial domain or transform domain image steganography approaches in Table II. Spatial methods which directly alter pixel intensities are low-cost to develop and spacious, but may be vulnerable to attacks. Transform domain approaches, which change the coefficients themselves by means of transforms and thereby achieve greater security but at a higher cost

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

in terms of computational resources used as well having lower limits on their capacities to hold data traffic.

Kannammal and Rani (2014) [42] recommended the use of LSB and DWT methods to watermark medical images. Researchers improved security even further by encrypting the watermarked image using three algorithms: AES, RSA, and RC4. This method was designed to give medical photos even more protection by making use of watermarking and encryption techniques.

Sharma et al. (2017) [43] Proposed a system that combines DWT and DCT for integrating medical information and watermarks in the cover image. researchers also applied the Rivest-Shamir-Adleman (RSA) and MD5 algorithms to encrypt EPR watermarks before embedding them in nonregion of interest (NROI) regions, which include white spots not related with Edema - and ROI--regions that are associated with edemas. Also, steganography and cryptographic techniques have also been studied to protect the data. Two layers of protection against unauthorized access provides integrity for transmission of data.

Mansour, R. F., & Abdelrahim, E. M. (2019) [44] designed a highly effective reversible print picture steganography model which used the Discrete Ripplet Transformation method to secretly insert messages into medical cover images For example A dual cryptosystem model that combines the proposed steganography method another way of ensuring safe communication called RSA. This adaptive evolutionary algorithm made the model much more capable of hiding data and escaping attention. The steganography model Based on wavelet transform, it has high PSNR, embedding ability, and imperceptibility, the steganography model is considered better than previous algorithms.

Khashan, O. A., & AlShaikh, M. (2020) [45] offered a steganographic scheme that uses nuclear spin generator technology to conceal information in medical images. They review the proposed method in detail--histogram analysis, PSNR calculation, key space estimation and statistical package. These results show how effective this unusual hiding of information in medical images truly is.

Karakus, S., & Avci, E. (2020) [46] proposed a new optimization-based technique for increasing the amount of hidden data while still maintaining very good image quality based on pixel similarities. Better performance in visual quality analysis metrics such as MSE, RMSE, PSNR, and so on demonstrates the effectiveness of this method.

C. Review Based on Data Hiding in Medical Images

Data hiding is a security method in which the secret data are buried inside cover images. In reversible data hiding, both the original image and recovered secrets can be reconstructed without loss of quality. This section provides a variety of methods for hiding and recovering embedded data, which are divided into three domains: spatial domain, encryption-domain and compressed-domain. Modifying pixel pairings, difference expansion of quads, multiple-layer data hiding, histogram shifting, and other approaches to improve data hiding capacity while retaining image quality [47]. are examples of these techniques. The section summarizes the relevant work in each domain as shown in *Fig. 5*.

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

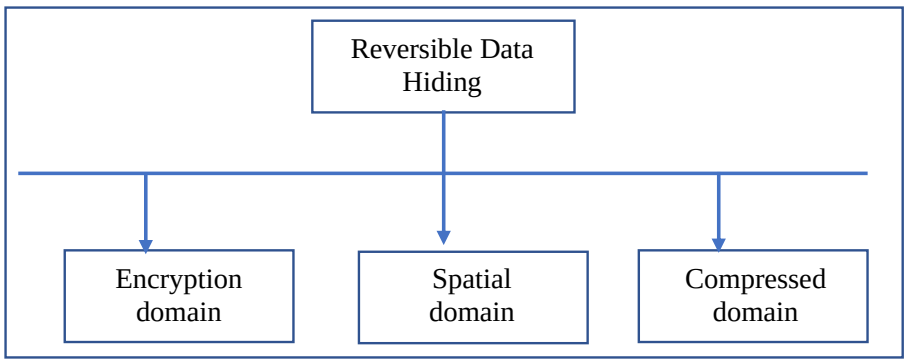

FIG. 5. DATA HIDING [47].

- ***Spatial Domain***

In this section we will provide a discusses the use of different techniques for data hiding and extraction, specifically in the spatial domain. These techniques aim to increase the embedding capacity while addressing issues like underflow and overflow during the embedding process.

Dmour and Ani (2016) [48], suggested a method for protecting secret data that combined steganography with cryptography, researchers employed Hamming code and syndrome trellis code as message coding techniques. Edge detection was also applied to recognize and embed data in edge pixels, resulting in increased stego picture quality. The sensitive data was integrated in the NROI, while the ROI was kept for future changes.

Parah et al. (2017) [49] proposed a scheme that combined the pixel repetition (PRM) method with modular arithmetic. The authors compared the effectiveness of MOD 4 and MOD 8 techniques. The proposed method tested on common medical images.

Parah et al. (2017) [50] proposed a method of concealing patient information in medical photographs. Researchers separated the image into blocks and classified the pixels as seed or non-seed. Intermediate significant bit replacement implanted the patient's info in those non-seed pixels, and checksum bits were also incorporated to prevent least significant bit removal during data transfer.

Parah, S. A et al (2020) [51] One such method for concealing the EHR behind medical photographs in an IoT-driven healthcare system was proposed by researchers, In other words Periodically transmitting digital signatures to check if any identity thefts have occurred Numerous problems were brought out with staff preference shortage It was especially necessary The method put the EHR into scaled-up images using PRM and module arithmetic, a solution that is both powerful computationally yet economical. The results achieved showed that the proposed method is reversible, secure and not visible to the naked eye. So, it can be used in IoT-based healthcare systems for application in the context of smart cities.

- ***Encrypted Domain***

Liu, Y., Qu, X., & Xin, G. (2016) [52] extending prediction error expansion (PEE), proposed a sorting method to integrate patient information into further use of the ROI. Through the use of PEE and sorting, user can integrate patient information in ROI. Furthermore, to facilitate recovery researchers put another piece of information into the NROI by the histogram shift method.

Aydogan & Bayilmis (2017) [53] recommended that patient diagnostic information be incorporated into photos by means of a block-matching technique. researchers showed eight

Received 10/December/2023; Accepted 19/January/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

types of scanning orders, six of which are new and can enhance image quality and ease embedding.

Parah, S. A., et al. (2017) [54] proposed pixel to block conversion, a data security technique that uses chaotic encryption. The researchers developed a technique to strengthen image data by adding checksum bits to detect and locate tampering and using intermediate significant bit substitution (ISBS) to insert EPR.

- ***Compressed Domain***

Rani, M., & Lakshmanan, S. (2016) [55] came up with run length encoding, a method for compressing medical photographs The technique divided into three steps. The first step involved the hiding of text data in a medical image.

Rani, M., & Lakshmanan, S. (2016) [56] proposed an encoding scheme called run-length coding, the technique divided into three phases: The first phase involved data hiding. In the second, images have been compressed; in the third images have been decompressed.

TABLE III. COMPARISONS OF DIFFERENT METHODS BASED ON PSNR

Ref	Image dataset	Image Type & Size	Domain	Method	Evaluation Metrics Result	Limitations
Al-Dmour & Al-Ani (2016) [48]	Medical images	gray (255 × 255)	Spatial Domain	Hamming code and Syndrome Trellis code	PSNR (db): 68.28	Image security improvements take time to implement
Liu, Y., et al (2016) [52]	Medical images	Gray	Encrypted Domain	LSB substitution	PSNR (db): 102.25	Security issue
Rani, M., & Lakshmanan, S. (2016) [55]	Medical images	Gray	Encrypted Domain	Run-length encoding	PSNR (db): 44.22	The need for an abundant storage environment suitable for processing medical images.
Rani, M. M., & Lakshmanan, S. (2016) [56]	Medical images	Gray	Encrypted Domain	Run-length encoding	PSNR (db): 48.32 Embedding rate (bpp): 0.5	Applies only to grayscale images.
Parah, S. A., et al. (2017) [54]	Medical images	-	Encrypted Domain	Pixel to block	PSNR (db): 46.36	Multiple, complex operations affected the system's speed.
Parah, S. A., et al. (2017) [50]	Medical images	gray (512 × 512)	Spatial Domain	ISBN	PSNR (db): 46.84	Although the system provided high security, it took more implementation time

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

Parah, S. A.,et al (2017) [49]	Medical images	gray (64 × 64)	Spatial Domain	Watermark Data (EPR)	BER 49.25 NCC 0.5053 BER 0.5016 NCC 49.94	The system contained many complex processes
AYDOĞAN, T., & BAYILMIŞ, C. (2017) [53]	Medical images	(512 × 512)	Encrypted Domain	Scanning order selection	PSNR (db): 56.6 Embedding rate (bpp): 0.5	The system is vulnerable, if modern threat methods are used
Parah, S. A et al (2020) [51]	Medical images (Med1, Med2, Med3 Med4)	gray (512 × 512)	Spatial Domain	PRM and EHR	PSNR (db): 37.59, 37.61, 38.80 and 39.02	Complex calculations and repetitions took a lot of time during implementation

Table III presents a comparison of different methods used in reversible data hiding based on their PSNR. The methods are categorized into compressed, spatial, and encrypted domains, and their respective authors, techniques, PSNR values. This comparison provides insights into the performance and characteristics of these methods for hiding data while considering factors like image quality and data capacity.

The uses of data hiding in an image have some common objectives as shown:

A. safeguarding patient's data with medical images being examples of such data. It is therefore feasible to send or preserve the patient's identity and incorporate this data in image itself.

B. Verifying images through techniques such as watermarking. The reason for this is that it confirms if the images have not been interfered with through transfer or storage [57].

C. With regard to image ownership and copyright, data hiding techniques have been proposed for indicating ownership or copyright on an image so as to dissuade unauthorized use or distribution.

D. Metadata, which involves additional metadata or other pertinent information that can be added into the image's body cavity, promotes proper categorization of images for easier location in information management [58].

III. CONCLUSIONS

In medical image encryption, it is crucial to protect against network-based image attacks to ensure security. The preservation of accuracy and quality in medical images is crucial, and the challenge lies in finding a balance between competing characteristics like security and complexity in cryptographic algorithms. The main contribution of this work is a detailed classification of contemporary image encryption, steganography, and data hiding schemes, as well as their limitations, which should be addressed by future research. A tables-based summary of prominent encryption techniques has been provided, which can assist researchers in selecting suitable encryption methods for e-health applications. The purpose of this table is to shed light on how to encrypt the data for the purposes of providing security for patients using telemedicine technology. This paper also highlights a viable system to incorporate embedding ability and recover all information, even in cases of

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

noise-induced. The paper also emphasizes the requirement for additional studies to safeguard confidentiality used in healthcare applications.

ACKNOWLEDGMENT

I express my sincere thanks to the members of the Computer Department at the University of Technology who provided me with constant support and encouragement during my PhD study.

REFERENCES

[1] K. P. Kavitha and P. VidhyaSaraswathi, "A survey on medical image encryption," 2017.

[2] M. Fallahpour, D. Megias, and M. Ghanbari, "Reversible and high-capacity data hiding in medical images," IET Image Processing, vol. 5, no. 2, pp. 190-197, 2011.

[3] N. M. Ghadi and N. H. Salman, "Deep learning-based segmentation and classification techniques for brain tumor MRI: A review," Journal of Engineering, vol. 28, no. 12, pp. 93-112, 2022.

[4] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," Optics and Lasers in Engineering, vol. 110, pp. 24-32, 2018.

[5] B. A. Shtayt, N. H. Zakaria, and N. H. Harun, "A comprehensive review on medical image steganography based on LSB technique and potential challenges," Baghdad Science Journal, vol. 18, no. 2 (Suppl.), pp. 957-957, 2021.

[6] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data security using cryptography and steganography techniques," International Journal of Advanced Computer Science and Applications, vol. 7, no. 6, pp. 201-206, 2016.

[7] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," Optics and Lasers in Engineering, vol. 88, pp. 197-213, 2017.

[8] P. Ping, F. Xu, and Z. J. Wang, "Image encryption based on non-affine and balanced cellular automata," Signal Processing, vol. 105, pp. 419-429, 2014.

[9] H. Liu and X. Wang, "Image encryption using DNA complementary rule and chaotic maps," Applied Soft Computing, vol. 12, no. 5, pp. 1457-1466, 2012.

[10] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical Image Encryption: A Comprehensive Review," Computers, vol. 12, no. 8, pp. 160, 2023.

[11] K. M. Hosny, M. M. Darwish, K. Li, and A. Salah, "Parallel multi-core CPU and GPU for fast and robust medical image watermarking," IEEE Access, vol. 6, pp. 77212-77225, 2018.

[12] J. Liu, S. Tang, J. Lian, Y. Ma, and X. Zhang, "A novel fourth order chaotic system and its algorithm for medical image encryption," Multidimensional Systems and Signal Processing, vol. 30, pp. 1637-1657, 2019.

[13] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," IEEE Access, vol. 9, pp. 37855-37865, 2021.

[14] D. Kumar, V. K. Sudha, and R. Ranjithkumar, "A one-round medical image encryption algorithm based on a combined chaotic key generator," Medical & Biological Engineering & Computing, vol. 61, no. 1, pp. 205-227, 2023.

[15] M. Boussif, N. Aloui, and A. Cherif, "New Watermarking/Encryption Method for Medical Images Full Protection in m-Health," International Journal of Electrical & Computer Engineering, vol. 7, no. 6, pp. 2088-8708, 2017.

[16] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," Medical & Biological Engineering & Computing, vol. 57, pp. 2517-2533, 2019.

[17] G. Manjula and H. S. Mohan, "A secure framework for medical image encryption using enhanced AES algorithm," International Journal of Scientific & Technology Research, vol. 9, no. 2, pp. 3837-3841, 2020.

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

[18] S. . Priya and B. Santhi, "A novel visual medical image encryption for secure transmission of authenticated watermarked medical images.," *Mobile networks and applications*, pp. 1-8, 2021.

[19] A. T. Hashim, A. H. Jassem, and S. A. Ali, " A novel design of Blowfish algorithm for image security.," *In Journal of Physics: Conference Series. IOP Publishing.*, vol. 1818, nº 1, p. 012085, (2021, March).

[20] A. T. Hashim, A. K. Jabbar, and Q. F. Hassan, " Medical image encryption based on hybrid AES with chaotic map.," *In Journal of Physics: Conference Series. IOP Publishing.*, vol. 1973, nº 1, p. 012037, (2021, August).

[21] S. W. Jirjees, N. A. Yousif, and A. T. Hashim, " Colour image privacy based on cascaded design of symmetric block cipher.," *J. Eng. Sci. Technol*, vol. 17, pp. 2135-2156, 2022.

[22] X. Li and H. Peng, " Chaotic medical image encryption method using attention mechanism fusion ResNet model," *Frontiers in Neuroscience*, vol. 17, p. 1226154, 2023.

[23] X. Wang and Y. Wang, " Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points," *Expert Systems with Applications*, vol. 213, p. 118924, 2023.

[24] Y. Mao and M. Wu, " A joint signal processing and cryptographic approach to multimedia encryption," *IEEE Transactions on Image processing*, vol. 15, nº 7, pp. 2061-2075, 2006.

[25] B. D. Parameshachari, Investigation on partial image encryption methods., Thesis Submitted in partial fulfillment of the Requirements for the award of the degree of DOCTOR OF PHILOSOPHY, 2014.

[26] B. D. Parameshachari, H. T. Panduranga, and S. K. Naveenkumar, " Partial encryption of medical images by dual DNA addition using DNA encoding.," *In 2017 international conference on recent innovations in signal processing and embedded systems (RISE) IEEE.*, pp. 310-314, 2017.

[27] M. K. Abdmouleh, H. Amri, A. Khalfallah, and M. S. Bouhlel, " An efficient crypto-compression scheme for medical images by selective encryption using DCT.," *International Journal of Advanced Intelligence Paradigms*, vol. 13, nº 1-2, pp. 32-42, 2019.

[28] S. Heidari, M. Naseri, and K. Nagata, " Quantum selective encryption for medical images.," *International Journal of Theoretical Physics*, vol. 58, pp. 3908-3926, 2019.

[29] P. Kiran and B. D. Parameshachari , " Logistic sine map (LSM) based partial image encryption.," *In 2021 National Computing Colleges Conference (NCCC) IEEE.*, pp. 1-6, (2021, March).

[30] J. Li, Z. Zhang, S. Li, R. Benton, Y. Huang, M. V. Kasukurthi, et al. , " A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology.," *BMC Medical Informatics and Decision Making,*, vol. 20, pp. 1-16, 2020.

[31] P. Rashmi, M. C. Supriya, and Q. Hua, "Retracted:: Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare.," 2023.

[32] W. Cao, Y. Zhou, C. P. Chen, and L. Xia , "Medical image encryption using edge maps.," *Signal Processing*, vol. 132, pp. 96-109., 2017.

[33] B. D. Parameshachari, H. T. Panduranga, and S. liberata Ullo, "Analysis and computation of encryption technique to enhance security of medical images.," *In IOP conference series: materials science and engineering,IOP Publishing.*, vol. 925, nº 1, p. 012028, (2020, September).

[34] Kiran and B. D. Parameshachari, "Selective Image Encryption of Medical Images Based on Threshold Entropy and Arnold Cat Map," *Biosc.Biotech.Res.Comm*, vol. 13, nº 13, pp. 94-202, 2020.

[35] O. A. Khashan and M. AlShaikh, "Edge-based lightweight selective encryption scheme for digital medical images.," *Multimedia Tools and Applications*, vol. 79, nº 35-36, pp. 26369-26388, 2020.

[36] Y. Shen, C. Tang, M. Xu, and Z. Lei, "Optical selective encryption based on the FRFCM algorithm and face biometric for the medical image," *Optics & Laser Technology*, vol. 138, p. 106911, 2021.

[37] D. Vaishnav and A. S. Thoke, " Medical image steganography: A survey.," *2018 International Conference on Communication information and Computing Technology (ICCICT)IEEE.*, pp. 1-5, 2018.

[38] M. Z. Konyar and S. Öztürk, " Reed Solomon coding-based medical image data hiding method against salt and pepper noise," *Symmetry*, vol. 12, nº 6, p. 899, 2020.

[39] M. O. Asanbe,, "Hybrid data security: a review of cryptography and steganography techniques.," *Villanova Journal of Science, Technology and Management.*, vol. 2, nº 1, 2020.

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.24.2.7

[40] M. N. Abdulwahedand, S. T. Mustafa, and M. S. M. Rahim, " Image spatial domain steganography: A study of performance evaluation parameters.," *In 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*, pp. 309-314, (2019, October).

[41] A. Fkirin, G. Attiya, and A. El-Sayed , "Steganography literature survey, classification and comparative study.," *Communications on Applied Electronics*, vol. 5, nº 10, pp. 13-22, 2016.

[42] A. Kannammal and S. Subha Rani, "Two level security for medical images using watermarking/encryption algorithms.," *International Journal of Imaging Systems and Technology 24*, vol. 1, nº 2014, pp. 111-120, 2014.

[43] A. Sharma, A. K. Singh, and S. P. Ghrera, "Robust and secure multiple watermarking for medical images.," *Wireless Personal Communications*, vol. 92, pp. 1611-1624, 2017.

[44] R. F. Mansour and E. M. Abdelrahim, "An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications.," *Multidimensional Systems and Signal Processing*, vol. 30, pp. 791-814, 2019.

[45] O. A. Khashan and M. AlShaikh, "Edge-based lightweight selective encryption scheme for digital medical images.," *Multimedia Tools and Applications*, vol. 79, nº 35-36, pp. 26369-26388, 2020.

[46] S. Karakus and E. Avci , " A new image steganography method with optimum pixel similarity for data hiding in medical images," *Medical Hypotheses*, vol. 139, p. 109691, 2020.

[47] D. Bhagat and R. Bhardwaj, "A survey on medical images for reversible data hiding techniques.," *In 2019 Amity International Conference on Artificial Intelligence (AICAI), IEEE.*, pp. 811-817, (2019, February).

[48] H. Al-Dmour and A. Al-Ani, ". Quality optimized medical image information hiding algorithm that employs edge detection and data coding.," *Computer methods and programs in biomedicine*, vol. 127, pp. 24-43., 2016.

[49] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, " Hiding clinical information in medical images: a new high capacity and reversible data hiding technique.," *Journal of biomedical informatics*, vol. 66, pp. 214-230, 2017.

[50] S. A. Parah, F. Ahad, J. A. Sheikh, N. A. Loan, and G. M. Bhat, " A new reversible and high capacity data hiding technique for E-healthcare applications.," *Multimedia Tools and Applications*, vol. 76, pp. 3943-3975, 2017.

[51] S. A. Parah, J. A. Sheikh, J. A. Akhoon, and N. A. Loan, "Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication.," *Future Generation Computer Systems*, vol. 108, pp. 935-949, 2020.

[52] Y. Liu, X. Qu, and G. Xin " A ROI-based reversible data hiding scheme in encrypted medical images.," *Journal of Visual Communication and Image Representation*, vol. 39, pp. 51-57., 2016.

[53] T. Aydogan and C. Bayilmis, "A new efficient block matching data hiding method based on scanning order selection in medical images.," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 25, nº 1, pp. 461-473, 2017.

[54] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat , "Hiding clinical information in medical images: a new high capacity and reversible data hiding technique.," *Journal of biomedical informatics*, vol. 66, pp. 214-230, 2017.

[55] M. Rani and S. Lakshmanan, " A Novel Method of Data Hiding and Image Compression for Medical Images.," *International Journal of Advanced Information Technology (IJAIT)*, vol. 6, nº 1, 2016.

[56] M. M. Rani and S. Lakshmanan, " An integrated method of data hiding and compression of medical images.," *arXiv preprint arXiv:1604.02797.*, 2016.

[57] N. M. Makbol and B. E. Khoo, " A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition.," *Digital Signal Processing*, vol. 33, pp. 134-147, 2014.

[58] T. Denemark, "Image Information Hiding Based on LSB Matching Revisited," *IEEE Transactions on Information Forensics and Security*,, 2017.

Received 10/December/2023; Accepted 19/January/2024
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*