

Medical Image Transmission Using Novel Crypto-Compression Scheme

Arwa Mashat¹, Surbhi Bhatia^{2,*}, Ankit Kumar³, Pankaj Dadheech³ and Aliaa Alabdali⁴

¹Department of Information Systems, College of Computing and Information Technology, King Abdulaziz University, Rabigh, Saudi Arabia

²Department of Information Systems, College of Computer Sciences and Information Technology, King Faisal University, Saudi Arabia

³Department of Computer Science & Engineering, Swami Keshvanand Institute of Technology, Management & Gramothan, Jaipur, Rajasthan, India

⁴Department of Information Technology, College of Computing and Information Technology, King Abdulaziz University, P.O. Box 344, Rabigh 21911, Saudi Arabia

*Corresponding Author: Surbhi Bhatia. Email: surbhibatia1988@yahoo.com

Received: 08 July 2021; Accepted: 31 August 2021

Abstract: The transmission of medical records over indiscrete and open networks has caused an increase in fraud involving stealing patients' information, owing to a lack of security over these links. An individual's medical documents represent confidential information that demands strict protocols and security, chiefly to protect the individual's identity. Medical image protection is a technology intended to transmit digital data and medical images securely over public networks. This paper presents some background on the different methods used to provide authentication and protection in medical information security. This work develops a secure cryptography-based medical image reclamation algorithm based on a combination of techniques: discrete cosine transform, steganography, and watermarking. The novel algorithm takes patients' information in the form of images and uses a discrete cosine transform method with artificial intelligence and watermarking to calculate peak signal-to-noise ratio values for the images. The proposed framework uses the underlying algorithms to perform encryption and decryption of images while retaining a high peak signal-to-noise ratio value. This value is hidden using a scrambling algorithm; therefore, a unique patient password is required to access the real image. The proposed technique is demonstrated to be robust and thus able to prevent stealing of data. The results of simulation experiments are presented, and the accuracy of the new method is demonstrated by comparisons with various previously validated algorithms.

Keywords: Cryptography; magnetic imaging resonance; steganography; watermarking; discrete cosine transform

1 Introduction

In the current world, images are easily captured by digital cameras, camcorders, and scanners and transmitted *via* social media sites. Moreover, owing to the abundance of easily accessible images online,



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

information can be shared easily. The most suitable and frequently used format for such images is JPEG, as this format can maintain high image quality during compression. However, transmission of images online can lead to various complications involving authentication, copyright infringement, privacy, and dissemination of images. For instance, images can be easily copied from the Internet without the permission of the image owner. There is thus an urgent need to protect images from fraudulent activities such as copying *via* various security channels. Embedding an invisible or transparent message in an image is a potential solution to these problems, as it is possible to extract the embedded information to verify the authenticity of the image. Digital watermarking is a technique that is used to incorporate a certain type of information called a watermark (which may be visible or invisible) in media of various types, which are referred to as the cover work [1]. In medicine, patient health monitoring data are captured in reports, which may include information in image format. However, the large amounts of data handled in hospitals may sometimes result in the wrong information being distributed to patients, with potentially life-threatening consequences. This necessitates quicker encryption–decryption processing for all images. As low-frequency coefficients are mostly zero after quantization, our suggested approach employs encryption to maintain the high compression ratio of the JPEG method, using a secure cryptosystem. The objective of this work was to provide secure protection and authentication using watermarking and steganography techniques based on DCT. A new conceptual model for medical image encryption and decryption using discrete cosine transform (DCT) is proposed. The most important potential application of this model is protection of medical image protection by steganography using a two-dimensional (2-D) matrix barcode; the suitability of the method for this application is demonstrated experimentally. The method is also validated by comparing the peak signal-to-noise ratio (PSNR) values and correlation coefficients obtained with multiple images. The main contributions of this paper are as follows.

- The various methods existing methods used for medical information security authentication and protection are reviewed.
- A secure cryptographic-based medical image reclamation algorithm is proposed based on a hybrid of DCT, steganography, and watermarking techniques.
- A framework is developed that uses the underlying algorithm to explain how image encryption and decryption are performed while retaining a high PSNR value.
- Image invisibility is prioritized over robustness in the encryption and decryption process.
- Comparison with previously validated algorithms in simulations shows that an acceptable level of accuracy is achieved by the proposed method.

This paper is organized as follows. A summary of existing work is provided in Section 2. Section 3 presents the formulation of the problem and the system design. Section 4 describes the proposed methodology. Section 5 discusses the experimental evaluations. Section 6 concludes the paper.

1.1 Importance of Steganography and Watermarking

Various methods have been designed to protect data and ensure the security of systems. Steganography is a method to guarantee the safety of data by hiding a message within another message. This method is closely related to watermarking; both techniques provide privacy *via* the transmission of hidden information. In general, a steganography system does not require the removal of hidden messages, but watermarking requires that the message is hidden securely enough to resist any attempt to eliminate it. For instance, in copyright protection, it must not be possible for the copyright information to be readily removed. In this sense, watermarking is similar to steganography. Applications of watermarks [1] mentioned in the literature include copy protection, finger prints, duplicate protection, monitoring of transmission, hidden information [2], data authentication [3], indexing, medical security [4], and tamper detection [5].

1.2 Applications of Steganography and Watermarking in Medical Image Analysis

There are several reasons for hiding data, which generally involve ensuring that unauthorized individuals are unaware of the presence of a message. Steganography can be used to conceal a chemical formula or the design of a new business innovation. It can also be used in corporate espionage to transmit trade secrets without anyone at the firm knowing. Steganography is frequently used in the non-commercial sector to conceal private information. Messages have been passed using this method since time immemorial.

Watermarking can be considered to be a subset of steganography. In steganography, there is no relation through hidden data cover, and therefore it is necessary that there is no suspicion that any intermediate has attempted to transport hidden data in watermarks. The hidden information of the medium has the ownership and no problem like a doubt that a precise medium is taking some right data. There is a discreet correspondence between the two media since the determination of steganography persists. The existence of the communication is unknown to a potential enemy, and successful violence will sense the reality of this statement. On the contrary, watermarking requires systems to be stronger than potential attacks; thus, watermarking requests are completely different from steganography ones. Digital certificates and digital signature methods are used for authentication purposes. The process of embedding copyright information or a watermark into a cover image is known as digital watermarking [6,7]. According to [8], a digital watermark can be defined as follows: “a digital cipher irremovable, strongly, and imperceptibly embedded in host data and generally contains information on the origin, status or destination of the encrypted information.” The scope of the present work is to develop a scheme that can offer full protection of digital images by concealing the owner’s personal information. By using the watermarking technique, the information provided to the embedding system can be correctly embedded and, after several image processing operations, it can be easily removed [9]. Use of the DCT technique enables the image to be made resistant against attacks. Here, an invisible watermarking method is used, which is more secure and robust than previous methods; using this approach, the user is free to upload their images and any other information on the Internet. The proposed method is applicable to various fields that use digital images, including social networking [10,11].

2 Summary of Related Work

In [12], the authors use a digital watermark method based on DCT and discrete short-wave transformation. The authors propose an algorithm for outside of the high-frequency band of the image that was converted into wavelets. Thus, these techniques help with the original image and the image of the watermark. Simulation results show that the methods are well hidden and provide good resistance against attacks during image handling operations. In [13], the authors present a proportional study of patient facts interspersed in the use of a manuscript signal of an electrocardiogram ECG in medical metaphors, using discrete Fourier transforms and DCT. For security, text information and ECG signals are encoded before being incorporated into the frequency state. Projecting coded methods, including adaptive delta variation and differential pulse code modulation, are castoff for cryptography and solidity of ECG signals. Measurable assessment of the quality of the watermark images is performed using PSNR and the standardized mean square error.

In [14], a steganography scheme is constructed to enable more secure and robust medical image transmission. The proposed system provides an effective security and archiving mechanism for protecting medical images. The steganography system uses an integer wavelet transform (IWT) to safeguard magnetic resonance images using a single image of the container. The image of the container is taken, a the turn to the left is added, and a replica container image is obtained. Then the medical study image of the patient stood in use as an undisclosed image, and the Arnold transform was smeared, yielding the

coded image. In the first situation, the encrypted undisclosed image is incorporated through the fictitious image of the container, and the reverse IWT results in a fictitious undisclosed image. In the second approach, the image of the container is taken and merged with the fictitious secret image, yielding the “stego” image. The recovered medical images showed acceptable visual quality.

In [15], the secure transmission of medical records through a community network is managed effectively. To improve protection and confirmation of medical proceedings, a watermark method is used for identification and reference. There is a great need to remove such prohibited copyrights from digital media. The authors propose the use of SHA 256 and AES (advanced encryption standard), and reckoning solidity methods. The region of interest (ROI) of a medical image has an irregular shape that encloses key evidence. The medical carbon copy and information security and the completion of SHA 256 are included in the smallest amount significant ROI tads. The compression of the recuperated SHA 256 image and the removed watermark are used for justification. The fragile filigree scheme can detect sabotage and recover images. The watermark performance is settled to endorse and shorten file authentication, and for security, copyright security, privacy protection, and digital media management.

The method presented in [16] ensures the security of transmission of medical images. The algorithms prevailing are applied to the images. This work demonstrates a different approach that chains image cryptography with the data concealment of steganography methods to achieve the transmission of delete and secure images. In this scheme, a unique copy of the original is encrypted using a set of flow encryption rules, and patient information is incorporated into the coded images by means of a data-insertion technique, without data loss, using a data concealment key for greater safety. Stenography is applied to an image embedded with a secret key. When the message reaches the retriever, counter-approaches are applied in the inverse order, yielding the patient’s unique information. To eliminate noise, the image is removed formerly decrypting the communication.

A new medical image safety system using hyper-chaos in cryptography is suggested in [17]. Combination and distribution approaches are developed in response to safety concerns related to many chaos-based image-encryption systems. The combination strategies are based on the exchange of pixels, bringing together chaotic maps that preserve the area, and the exchange process is strong-minded by the first two state-owned variables of the engaged 4-D hyper catalytic organism. During the application of a flow method, the elements of the key sequence, as quantized by the other two state variables, move rotationally, rendering the image to flat pixels. As a result, the key sequence is correlated with both the key and the simple image, which guarantees security against light text occurrences. Several tentative experiments are performed in support of this approach.

In [18], encrypted electronic patient record (EPR) codes are recycled for data encryption and content security. EPRs comprise a collection of patient information that requires data validation, data security, and secure transmission. The proposed methodology uses cryptographic and image processing processes to create an encrypted information code in image format that can be transmitted and used in a similar way to a barcode or QR code, although it is more secure. The information can be retrieved on the recipient’s side without loss of information. The use of the RSA and DES algorithms, with three keys and tracking by image processing procedures as a complement, flip makes the proposed algorithm more robust. In this work, we develop a complete graphical user interface to encode the transmitter and decoder sections.

In [19], the authors present two approaches for encryption and decryption of images using XOR processes. In the main algorithm, the encrypted image is encoded by the fundamental image using the same process and decryption, and a matching key image is used in the XOR process. In the second algorithm, one of the bit planes of the crucial images is recycled to encrypt the bit planes of the original copy, and hobbling is performed to produce an encrypted copy.

In [20], a model is presented that can protect digital multimedia content on unprotected open networks, offering security for patient information. Digital cryptography should be adapted for medical images before diffusion followed by achieving; this technique is suggested as an effective model to provide information security to patients. Watermarks are added to the patient's images to ensure they cannot be accessed by unapproved staff.

In [21], the authors present a solution to meet the growing need for safe transmission and storage of medical images on public networks. Their method concurrently encrypts and wraps a medical image using compression detection, and pixel exchange is performed; thereby, the image is compacted and encrypted using a Bernoulli matrix based on the chaos created under the existing Chebyshev map. The quantized dimensions are then encoded by chaotic cryptography of the diffusion-permutation type to provide a second level of protection. In-depth simulations are performed and the results are analyzed.

The expansion of telemedicine means that security of medical records is of key importance, particularly with respect to the protection of patient privacy [22]. Medical hubs spend a great deal of money on increasing their information security. The best means of providing security of medical information is encryption, which can be implemented through various measures. Owing to the distinct features of graphical data and evidence, the method castoffs in cryptographic images are limited and, in some cases, have certain safety flaws and limitations that affect their applications. In the document bestowing the chaotic features of automata new rules for the medical image of cryptography. The results indicate that the proposed algorithm provides greater security and greater speed. Furthermore, this method shows no errors in the decoding phase. These topographies are rarely viewed at once in an encryption algorithm.

In [23], the method of cryptography is the process of makeover information using an algorithm called cryptography so that information is made inaccessible for all but to individuals who retain special knowledge, usually in the form of a unique key. A flow code is a fast-symmetric key algorithm that is used to convert plain text into cryptographic text. Image encryption can be achieved by both "spatial domain" and transformation domain processes. There is already a fractional image encryption pattern constructed on DWT and confusing flow encryption. Here, we propose a complete image encryption pattern based on DWT and "stream ciphers." The authors of [24] present a procedure to hide nearing extinction information to produce patient electronic medical records (EMRs) and representative's EMR cryptographic text to guarantee the secrecy of concern's EMRs at what time deposited in the health folder. This approach is based on bipolar multiple-base conversion that allows masking and mixing of data within the same brand information of the image. This arrangement guarantees that only approved users will have access to the EMR. In [25], the authors suggest that the three key necessities for EPR data whacking and diffusing the repossession of the EPR should be due to the absence of the covers image, zero "Bit Error Rate" (BER) is required for EPR data and imperceptibility should not be showing for any reason. For additional privacy, encryption of the patient data can also be used for watermarking.

In [26], the authors report that steganography with an average compression ratio of 8:1 can be attained using a wavelet method. This method also provides greater security for a stag's image, which avoids the ability to insert unequally using a QR code. The system proposed in [27] retains the quality of image Stag with a normal PSNR ratio value of 50,226 DB. Trial results also confirm the suitability of the proposed method for security applications. In [28], QR and image methods are used to build a "perfect" steganography system. The image is removed and the noise is filtered to a source for a more similar image eminence. After the model, it is clear that our scheme is vigorous for JPEG outbreaks.

Compared with other new steganography schemes, our proposed method involves three advantages: (i) it uses an improved secure model that has not been established before; (ii) our schema hides secret data lacking loss and loss in a cover image at the same time; and (iii) the barcode or QR code uses secret information that could extend the applications of the method. In [29], the authors presented a digital

watermark procedure based on DCT and discrete wavelet transforms. A recognized character of human prophecy, in this set of rules, the digital watermark that is transformed with discrete cosine will be inserted in the frequency band of the image that is transformed into a wavelet. Then, the digital watermark is distilled with the help of the original image and watermark. Simulation results show that this algorithm provides good resistance and invisibility when used in image processing. The authors of [30] highlight a major problem encountered when protecting patient's privacy in relation to medical images. Following the HIPAA mandate on the safeguarding of patient's medical records, efforts have been made to ensure the concealment of data and images for the duration of storage. Program through the unreliable passage. They revise the problem of tracing illegally scattered medical data in individual communiqué surroundings to recognize a set of design necessities that must be met.

Problem Formulation and Justification

There is currently a requirement for algorithms to prevent illegal use of multimedia content, including patient information in the form of medical images. The main objective of research in this field is to develop new methods to securely store patient data. In the present work, watermarking, steganography, and DCT techniques are combined to form an optimized algorithm for encryption and decryption of images. Watermarking of images was chosen because of the potential to extend this technique to video watermarking. Steganography is used to secure and encode the patient data in images; then, DCT is used to encrypt the images. The research gaps identified from the literature survey above include the fact that most previous studies have focused on securing images by using watermarking; none used more secure and robust methods of encryption. It was also found that images have been encrypted using XOR methods, which are hackable with modern techniques.

No "standard" watermarking algorithm has been established to date. Some approaches are only applicable to gray-layer images and do not work for other image formats [31].

3 Proposed Work

Many image encryption algorithms have been developed to provide grayscale images to prevent hacking and unauthorized access. These algorithms, which include discrete wavelet transformation, DCT, and discrete Fourier transformation, have various security purposes. Here, a combined approach using DCT, steganography, and watermarking is implemented. Owing to the combination of these three techniques, the watermark is robust against different types of attacks. Although different technologies have different advantages and disadvantages, steganography is the training of smacking private or penetrating data that seems to nothing habitual. Steganography is often disorganized with cryptology techniques, because both are similar to sheltering important information. DCT has exceptional properties, enabling most of the visualization of a significant part of the image to be performed using a few DCT coefficients.

Fig. 1 shows a flow chart of the algorithms used for image watermarking, including the embedding algorithm and extraction algorithm. The steps shown on one side describe the embedding of the watermark into the real image, whereas those on the other side describe the extraction algorithm, where boxes are used to show steps included in the extraction of information from the watermarked image [32]. The image is pre-processed and then its entropy is calculated in order to discover its capacity for integrating information. The encoder uses an optical image-encoding approach and a secret key to embed an image of the watermark into the host picture's high entropy value to create the watermark. Then, the system generates a watermarked image based on the amplitude and phase-shaping information of a laser beam. The watermark embedding process is depicted in Fig. 1. Finally, in the watermark extraction phase, the watermarked image is pre-processed, and the laser beam patterns are extracted. These beam patterns are then studied to determine the overall system entropy. To achieve greater resilience and imperceptibility, the watermark is extracted with a high entropy value. The watermark is identified using

the same key. The results of this experiment show that the watermark image can be recovered using simple, resilient, and undetectable image reconstruction techniques.

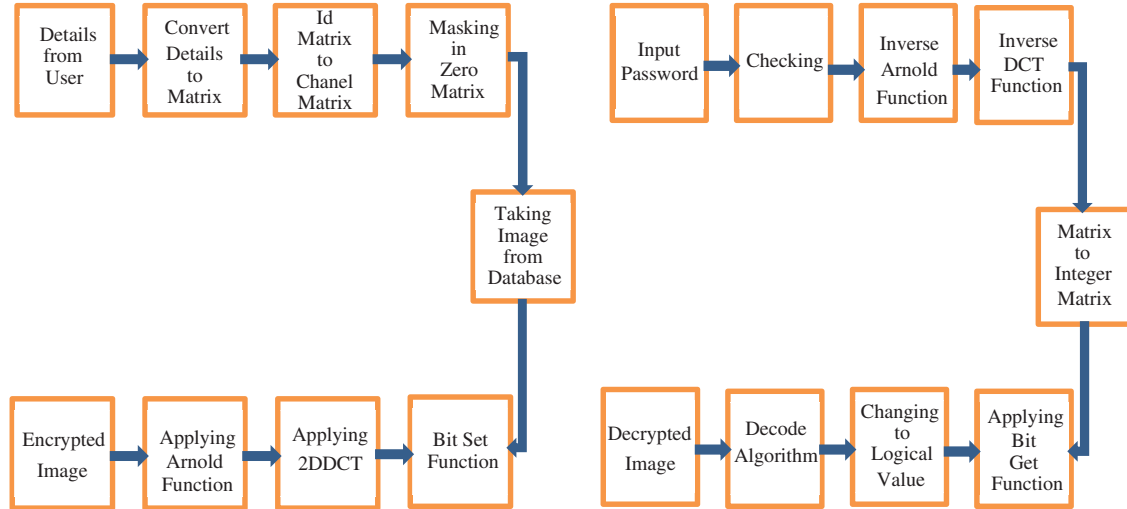


Figure 1: Encryption and decryption block diagram

To create a watermarked image, D_W , the watermark embedding method uses the following function:

$$D_W = E(I, ETP, W, K), \quad (1)$$

where E is the encryption method, I is the cover image, ETP is the information entropy, W is the watermark image, and K is the security key. The watermark extraction technique uses the following decoder function to decode the watermark image W :

$$W' = e(D_W, K, ETP, I). \quad (2)$$

An advantage of the proposed work is that it focuses on encrypting the most important information in the medical images, thereby minimizing the time spent on encryption and decryption operations. Rather than producing an unreadable image, it will help medical practitioners to preserve the information in the image.

3.1 Steganography and Watermarking: DCT Method

The original image is taken as an input; thereafter, the watermark embedding and watermark extraction processes are followed. Quality comparison is performed and PSNR values are obtained for evaluation. DCT is a method of converting an image's frequencies into equivalent cosine values, which can be represented as a sum of cosine functions. DCT is a Fourier-related transform with a finite number of data points. Only numerical values are permitted in this field. The DCT coefficients' variation determines their utility. For example, DCT is critical for image compression in the PNG image format. The 1-D DCT is expressed mathematically as follows:

$$y(k) = \alpha(k) \sum_{n=0}^{N-1} \cos\left(\frac{\pi(2n+1)k}{2N}\right), \quad k = 0, 1, \dots, N-1 \quad (3)$$

and the inverse transform is given by

$$x(n) = \sum_{k=0}^{N-1} \alpha(k)y(k)\cos\left(\frac{\pi(2n+1)k}{2N}\right), \quad n = 0, 1, \dots, N-1 \quad (4)$$

$$\alpha(0) = \sqrt{\frac{1}{N}}, k = 0 \text{ and } \alpha(k) = \sqrt{\frac{2}{N}}, \quad 1 \leq k \leq N-1, \quad (5)$$

where N is the number of given data samples: $x(0), \dots, x(N-1)$, $x(n)$ is the input data sample, $y(k)$ is the *DCT* coefficient, and $\alpha(k)$ is the scaling factor.

In the block-based *DCT* image watermarking approach, the images are first divided into several blocks. *DCT* is then applied to each image block. Finally, the process inserts the watermark into the block and a host image, which is made up of *DCT* coefficients, using an algorithm. The watermarked picture is created by applying the inverse *DCT* to the original image. Fig. 2 illustrates these processes.

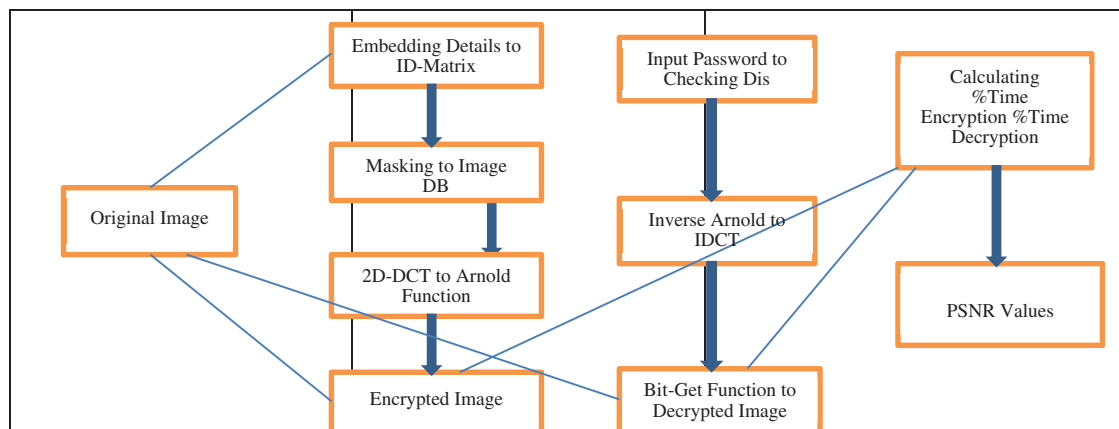


Figure 2: Processes of the method

The watermark embedding process comprises the following steps.

1. Collect detailed patient information and convert data into 2-D barcode format to improve the capacity of the watermark with image size $m \times n$.
2. Create the first scrambling method using the Arnold function from the original watermark image; then, obtain the watermark image after scrambling.
3. Apply *DCT* to the block.
4. Consider the position of embedded information, perform two-level Inverse *DCT* decomposition, and perform image encryption.

The watermark removal process can be described by the following steps.

1. Input a security password that is identified by the patient or an authorized individual.
2. Perform extraction of the watermark by reversing the embedding steps, then confirm barcode readability.

Fig. 3 shows the flowchart. The knowledge obtained from this process may be useful to eavesdroppers; however, simply encrypting the discrete cosine coefficients is insufficient. The number of encoded coefficients is increased for security, thereby making the system more robust and less complex by reducing the overall encryption and decryption time.

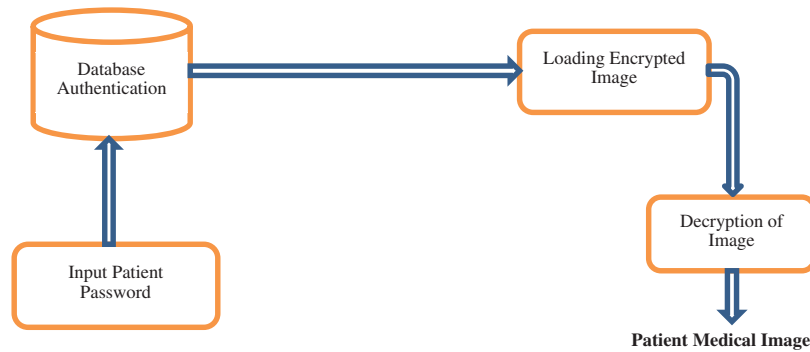


Figure 3: Digital image authentication system

3.2 Methodology Behind Implementation

In previous work, images were encrypted and decrypted using DCT-DWT transform, resulting in PSNR values of less than 50% for all images. Here, we implemented a new algorithm using DCT with barcode and watermarking methods, which achieved successful encryption and decryption of images with high PSNR values of >70% [33–35]. The pseudo code for the procedure is given in Algorithm 1.

Algorithm 1: Procedure for Encoding (Image1, Image 2, ..., image n)

Input: Name, Mobile Number Email, Domain, Age

Output: DCT base image

Name \leftarrow name

Mobile Number \leftarrow Mobile number

Email \leftarrow email

Domain \leftarrow domain

Age \leftarrow age

For image I to k: compute and assign

H \leftarrow id matrix

k1 \leftarrow image of 480×480

s \leftarrow write id matrix on pixels

e \leftarrow rows of s

d \leftarrow Columns of s

t \leftarrow rows of k

y \leftarrow column of k

End for

for size of s

l \leftarrow apply bit set function on s and k

end for

for size of s to size of k

(Continued)

Algorithm 1 (continued).

```

l ← k
For j 2 to k assign the following
J2 ← dct of l
K6 ← Arnold of J2
Kg ← Unsigned 8-bit conversion of K6
end for
Procedure for Encoding (Image1, Image 2, ... , image n)
Input : Name, Mobile Number Email , Domain, Age
Output: DCT base image
Name ← name
Mobile Number ← Mobile number
Email ← email
Domain ← domain
Age ← age
For image I to k: compute and assign
H ← id matrix
k1 ← image of 480 × 480
s ← write id matrix on pixels
e ← rows of s
d ← Columns of s
t ← rows of k
y ← column of k
End for
for size of s
l ← apply bit set function on s and k
end for
for size of s to size of k
l ← k
For j 2 to k assign the following
J2 ← dct of l
K6 ← Arnold of J2
Kg ← Unsigned 8-bit conversion of K6
end for

```

The pseudo code for decoding is given in Algorithm 2.

Algorithm 2: Procedure Decoding (image 1, image2,...image n)

Input:

Load database

Load barcode

Output:

Original Image (image 1, image 2,...image n)

Compute for image I to K :

Q1←Correct password

D1← Password

k ← Barcode

Compare d1 with correct password

End For

If q1 and d1 are same

y ← 1

else:

delete database

end if

if y: = 1

0←Apply Inverse Arnold Barcode

01← Apply Inverse dct on 0

O2←Unsigned 8-bit format 01

q ← rows in O2

a ← columns in O2

for f ← 1 to 181

for g ← 1 to 181

x ← bit get on O2

end for

end for

Zs ← Logical values of X

S ← k

j ← rows of s

k ← columns of s

(Continued)

Algorithm 2 (continued).

```

e ← y-s
O ← 1
r ← s
w ← 1
q ← 1
while 1 q is less than 5
while 1 r is less than 5
x ← 1
for u ← O to r
jk3 ← s
x = x + 1
end for
    io3 ← binary(jk3)
er ← char(io3)
w ← w + 1
r ← r + 8
end while
q ← q + 1
O ← 1
r ← s
w ← 1
end while
t ← cell 2
mul k/iop ← t
Decoded image ← k/iop.
End

```

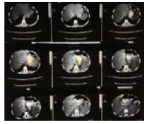
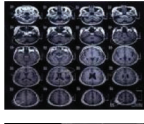
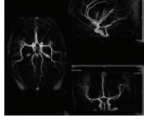


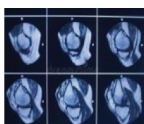
To achieve a 50% encryption compression ratio, standard techniques require that everything should be compressed before encryption. The proposed method achieves this ratio in a novel way, in which only 9% to 43% of the image's information needs to be encrypted. This enables faster encryption and decryption and therefore shorter processing times for all images. The low-frequency coefficients are mainly zero after quantization; thus, to retain the high compression ratio of the JPEG method, the suggested approach uses encryption. To this end, we have selected a cryptosystem that is safe and robust. Thus, in the eyes of the general public, medical images have been shown to be just as secure as factoring, which, according to the

general public, is an insolvable issue. Factoring methods undergo continuous improvement, as computer power is always growing [36,37]. Choosing a suitable key size for an encryption algorithm could improve the overall security of the proposed method. Encryption with a key of length 1024 or 2048 would yield an extremely powerful cryptosystem that could keep functioning for years into the future. This technology is particularly suitable for sending images, such as the results of a computed tomography scan, for medical diagnosis. This approach has clear benefits as it may be used to authenticate a document and corroborate the reliability of a source.

4 Simulation and Results

The results were obtained by visualizing different parts of images taken from reliable sources online. The analyses conducted on the dataset used NumPy (for matrix analysis), Seaborn (for advanced plotting), pandas (for data ingestion), Matplotlib (for basic plotting), and sklearn and tensorflow (for other tasks) [38]. An Inter i5 8th-generation processor was used with 16 GB RAM and a CentOS operating system. The results for a reference image subjected to encryption and decryption were shown to validate the claims. Tab. 1 shows the accuracy obtained, as well as the encryption and decryption times and PSNR values, in each case.

Table 1: PSNR values obtained for different images

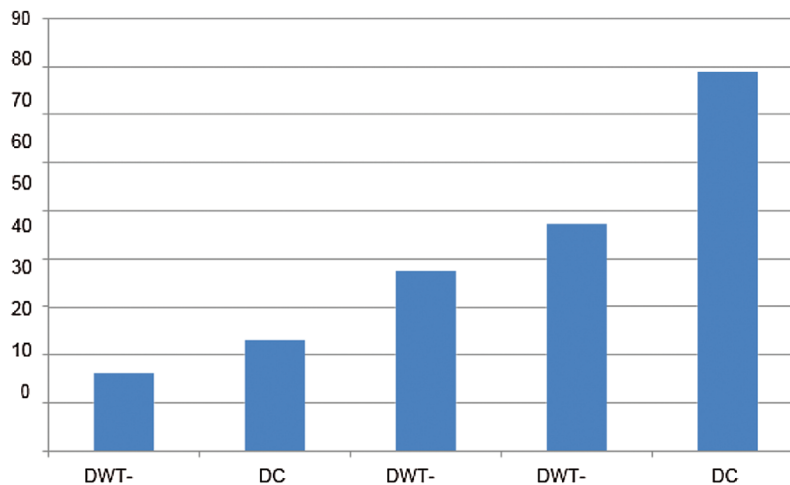
Serial No.	Name	Picture	Encryption time	% Decryption	Decryption time	PSNR
1.	Abdomen		11.67	92.64	2.02	71.66
2.	Brain		8.07	84.64	2.07	70.04
3.	Brain(ANN)		5.46	69.50	2.10	78.89
4.	Foot		9.17	78.90	206	76.94
5.	Hand		11.30	77.61	2.05	76.55
6.	Knee		7.8	97.49	2.6	70.20

Various algorithms used in previous research, as mentioned in the related work section, were compared with our method with respect to the PSNR range. As shown in Tab. 2, our proposed algorithm outperformed the others by a good margin.

Table 2: Accuracy values obtained with different algorithms

S. no.	Research papers	PSNR range	Algorithms
1.	A robust watermarking algorithm for encrypted medical images	Up to 23	DCT based
2.	An (encrypted medical, image retrieval algorithm) frequency domain	Up to 16	DWT-DCT based
3.	An efficient system for encrypted image by using hybrid compression algorithm	Up to 37.4139	DWT-DCT based
4.	New image watermarking algorithm to improve the imperceptibility and robustness	Up to 47.2724	DWT-DCT based
5.	Medical image encryption–decryption by using DCT	Up to 78.89	DCT based

A summary of the results achieved with various image-watermarking algorithms on a set of standard and medical images is presented in [Tab. 2](#) [39]. The range of PSNRs achieved is shown in each case for comparison with the present work. The accuracy of the proposed method was shown to be 78.89%; this result was validated as shown in [Fig. 4](#).

**Figure 4:** Comparison of accuracies of different methods

Medical imaging is multidisciplinary in nature, as evidenced by its use across all medical specialties. Extraordinary progress has been made in this field owing to the extensive use of telecommunications and information technology in the medical sector. However, medical professionals often oppose the use of telemedicine, because it must follow strict rules and comply with the ease provided by informatics sciences; some medical professionals are even opposed to data computerization. To address this challenge, medical imaging researchers have proposed a plethora of different compression and encryption approaches. The present work describes a novel method for encrypting medical images that selectively encrypts only a portion of the image. It makes use of an encryption technique that incorporates DCT into the compression process. The proposed design was shown to be fast, efficient, secure, and robust.

5 Conclusions

This paper presents a method for encryption and decryption of medical images using DCT. The scheme, which is based on a combination of DCT, watermarking, and steganography, protects the images from attacks and shows fake patient data in case of a breach. It achieves encryption and decryption of images with image-imperceptibility prioritized over robustness, and shows good results. The encryption and decryption pattern based on DCT involves a scrambling process to achieve high embedding capacity while maintaining a high PSNR, which is important for medical images. This paper also proposes an additional operation of image encryption after complete embedding, which requires a unique security key for the patient to decrypt the real image. As no image will be decrypted if the incorrect key is entered, this proposed system also provides patients with a high level of security. The accuracy of the proposed system is 78.89%, and comparison with existing techniques indicates that it is a more feasible solution for medical image encryption. These results provide a concept for implementation in the real-world workplace. The total and mean entropy of the plain picture never altered for all the ciphered images and the plain images. Moreover, the average number of total pixels of the images after decryption was the same as that before encryption, indicating the overall efficiency of the system. Future work will focus on various facets of medical image security, particularly optimizing PSNR values to produce a more robust solution.

Funding Statement: This work was supported by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia, under Grant No. (D-95-830-1442). The authors gratefully acknowledge technical and financial support from DSR.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] J. Zhou, L. Jinqing and D. Xiaoqiang, "A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position," *IEEE Access: Practical Innovations, Open Solutions*, vol. 8, no. 1, pp. 122210–122228, 2020.
- [2] A. El-Latif, B. Abd-El-Atty and M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, no. 1, pp. 1073–1081, 2018.
- [3] Y. Yang, X. Xiao, X. Cai and W. Zhang, "A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images," *IEEE Signal Processing Letters*, vol. 27, no. 1, pp. 256–260, 2020.
- [4] Y. Yang, X. Xiao, X. Cai and W. Zhang, "A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption," *IEEE Access: Practical Innovations, Open Solutions*, vol. 7, no. 1, pp. 96900–96911, 2019.
- [5] D. Ravichandran, P. Praveenkumar, J. B. Rayappan and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Transactions on NanoBioscience*, vol. 16, no. 8, pp. 850–858, 2017.
- [6] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou *et al.*, "Framework for efficient medical image encryption using dynamic S-Boxes and chaotic maps," *IEEE Access: Practical Innovations, Open Solutions*, vol. 8, no. 1, pp. 160433–160449, 2020.
- [7] P. Chen, J. Wu, C. Li, C. Kuo, N. Pai *et al.*, "Symmetric cryptography with shift $2n-1$, hash transformation, optimization-based controller for medical image infosecurity: Case study in mammographic image," *IEEE Photonics Journal*, vol. 12, no. 3, pp. 1–15, 2020.
- [8] S. Haddad, G. Coatrieux, A. Moreau-Gaudry and M. Cozic, "Joint watermarking-encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 1, pp. 2556–2569, 2020.

- [9] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar *et al.*, “Secure medical data transmission model for IoT-based healthcare systems,” *IEEE Access: Practical Innovations, Open Solutions*, vol. 6, no. 1, pp. 20596–20608, 2018.
- [10] A. T. Sajjad and R. Ali, “A novel medical image signcryption scheme using TLTS and henon chaotic map,” *IEEE Access: Practical Innovations, Open Solutions*, vol. 8, no. 1, pp. 71974–71992, 2020.
- [11] A. Belazi, M. Talha, S. Kharbech and W. Xiang, “Novel medical image encryption scheme based on chaos and DNA encoding,” *IEEE Access: Practical Innovations, Open Solutions*, vol. 7, no. 1, pp. 36667–36681, 2019.
- [12] P. Chen, J. Wu, C. Li, C. Kuo, N. Pai *et al.*, “Medical image infosecurity using hash transformation and optimization-based controller in a health information system: Case study in breast elastography and X-Ray image,” *IEEE Access: Practical Innovations, Open Solutions*, vol. 8, no. 1, pp. 61340–61354, 2020.
- [13] S. Rajagopalan, S. Poori, M. Narasimhan, S. Rethinam, C. V. Kuppusamy *et al.*, “Chua’s diode and strange attractor: A three-layer hardware-software co-design for medical image confidentiality,” *IET Image Processing*, vol. 14, no. 7, pp. 1354–1365, 2020.
- [14] G. R. Sinha and S. Jasjit, “Introduction to cognitive science, informatics and modelling,” *Cognitive Informatics, Computer Modelling and Cognitive Science*, vol. 1, no. 1, pp. 1–12, 2020.
- [15] N. Wang, G. Di, X. Lv, M. Hou, D. Liu *et al.*, “Galois field-based image encryption for remote transmission of tumor ultrasound images,” *IEEE Access: Practical Innovations, Open Solutions*, vol. 7, no. 1, pp. 49945–49950, 2019.
- [16] A. Khedr and G. Glenn, “Securedmed: Secure medical computation using GPU-accelerated homomorphic encryption scheme,” *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 2, pp. 597–606, 2018.
- [17] L. Jiang, L. Chen, T. Giannetsos, B. Luo, K. Liang *et al.*, “Toward practical privacy-preserving processing over encrypted data in IoT: An assistive healthcare use case,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10177–10190, 2019.
- [18] L. Wang, L. Li, J. Li and B. B. Gupta, “Compressive sensing of medical images with confidentially homomorphic aggregations,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1402–1409, 2019.
- [19] S. Basheer, S. Bhatia and S. B. Sakri, “Computational modeling of dementia prediction using deep neural network: Analysis on OASIS dataset,” *IEEE Access*, vol. 9, no. 1, pp. 42449–42462, 2021.
- [20] M. Boussif, A. Nouredine and C. Adnene, “Secured cloud computing for medical data based on watermarking and encryption,” *IET Networks*, vol. 7, no. 5, pp. 294–298, 2018.
- [21] A. Sengupta and M. Rathor, “Structural obfuscation and crypto-steganography-based secured JPEG compression hardware for medical imaging systems,” *IEEE Access: Practical Innovations, Open Solutions*, vol. 8, no. 1, pp. 6543–6565, 2020.
- [22] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh *et al.*, “Secure and robust digital image watermarking using coefficient differencing and chaotic encryption,” *IEEE Access: Practical Innovations, Open Solutions*, vol. 6, no. 1, pp. 19876–19897, 2018.
- [23] Y. Wang, C. Zhanchuan and H. Wenguang, “A new high capacity separable reversible data hiding in encrypted images based on block selection and block-level encryption,” *IEEE Access: Practical Innovations, Open Solutions*, vol. 7, no. 1, pp. 175671–175680, 2019.
- [24] J. Sun, X. Yao, S. Wang and Y. Wu, “Blockchain-based secure storage and access scheme for electronic medical records in IPFS,” *IEEE Access: Practical Innovations, Open Solutions*, vol. 8, no. 1, pp. 59389–59401, 2020.
- [25] S. Basheer, K. K. Nagwanshi, S. Bhatia, S. Dubey, G. R. Sinha *et al.*, “FESD: An approach for biometric human footprint matching using fuzzy ensemble learning,” *IEEE Access*, vol. 9, no. 1, pp. 26641–26663, 2021.
- [26] G. R. Sinha, “Fuzzy based medical image processing,” in *Advances in Medical Technologies and Clinical Practice (AMTCP) Book Series*. Pennsylvania: IGI Global, pp. 45–61, 2015.
- [27] M. Boussif, N. Aloui and A. Cherif, “Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher,” *IET Image Processing*, vol. 14, no. 6, pp. 1209–1216, 2020.
- [28] W. Guo, J. Shao, R. Lu, Y. Liu, A. A. Ghorbani *et al.*, “A privacy-preserving online medical prediagnosis scheme for cloud environment,” *IEEE Access*, vol. 6, no. 1, pp. 48946–48957, 2018.

- [29] L. Chen, B. Wutong and Y. Zhiqiang, "A secure and privacy-preserving watermark based medical image sharing method," *Chinese Journal of Electronics*, vol. 29, no. 5, pp. 819–825, 2020.
- [30] G. R. Sinha and B. C. Patel, *Medical Image Processing: Concepts and Applications*. India: Prentice Hall of India, 2014. ISBN: 978-81-203-4902-5.
- [31] B. Patel and G. R. Sinha, "Abnormality detection and classification in computer-aided diagnosis (CAD) of breast cancer images," *Journal of Medical Imaging and Health Informatics*, vol. 4, no. 6, pp. 881–885, 2014.
- [32] Q. Zhang, B. Lian, P. Cao, Y. Sang, W. Huang *et al.*, "Multi-source medical data integration and mining for healthcare services," *IEEE Access: Practical Innovations, Open Solutions*, vol. 8, no. 1, pp. 165010–165017, 2020.
- [33] K. Seol, Y. Kim, E. Lee, Y. Seo, D. Baik *et al.*, "Privacy-preserving attribute-based access control model for XML-based electronic health record system," *IEEE Access: Practical Innovations, Open Solutions*, vol. 6, no. 1, pp. 9114–9128, 2018.
- [34] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, M. M. Fouda *et al.*, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021.
- [35] J. Zhou, J. Li and X. Di, "A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden roi position," *IEEE Access*, vol. 8, pp. 122210–122228, 2020.
- [36] Y. Ding, "DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1504–1518, 2021.
- [37] S. Ibrahim, "Framework for efficient medical image encryption using dynamic s-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 160433–160449, 2020.
- [38] B. Vaseghi, S. Mobayen, S. S. Hashemi and A. Fekih, "Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption," *IEEE Access*, vol. 9, pp. 25911–25925, 2021.
- [39] S. P. Singh and G. Bhatnagar, "A novel biometric inspired robust security framework for medical images," *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, no. 3, pp. 810–823, 2021.