International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Robust Digital Watermarking using Pixel Color Correlation and Chaotic Encryption for Medical Image Protection

Namita D. Pulgam[1] , Subhash K. Shinde[2]

Submitted: 10/09/2022 **Accepted:** 20/12/2022

Abstract: Due to the ease with which image manipulation is accomplished, digital image authentication plays a major challenge in the digital revolution. With the rapid advancement of healthcare technology, electronic medical records can now be easily stored in the telemedicine field, which raises the concern for the security of the patient's medical data. Watermarking plays a major role in the healthcare domain as patient records are shared securely over the network if records are encoded with an encryption technique and inserted as a watermark. This must preserve the image's quality and correctly extract patient data from the encoded image even if any geometrical attack is performed to steal the information. Several watermarking approaches have been developed still need to develop a robust and secure watermarking scheme. This paper reviews watermarking scheme along with chaos-based encryption techniques and the benefits of using them over traditional encryption techniques. A watermarking approach based on pixel color correlation (WPCC) is proposed and chaos-based encryption and the Arnold transformation is used, to establish two levels of protection for patient medical records. To ensure secure transmission of information, the proposed approach encrypts the patient record before embedding it as a watermark in a medical image. The performance of the proposed method is evaluated and the system's robustness is checked against different attacks with Bit Error Rate (BER) and Normalized Correlation parameter (NCC). Proposed method generates images with high Peak Signal Noise Ratio (PSNR) ranging from 24.74dB to 36.07dB and Structural Similarity Index (SSIM) ranging from values 0.84 to 0.97. Assessment of evaluation parameters shows that the designed system is able to hide and extract a patient's medical record securely and the system is resilient to different attacks.

Keywords: *Digital Image Watermarking, Encryption Technique, Medical Images, Patient Data Security, Telemedicine*

1. Introduction

Without an in-person visit, telemedicine allows experts in the field to analyse, diagnose, and treat patients from a distance utilizing telecommunications technology and software. Follow-up visits, specialist consultations, medication monitoring, chronic condition management, and other diagnostic facilities that can be provided remotely via secure video and audio links are all common applications for telemedicine innovation. As a result, telemedicine is becoming a more vital aspect of the healthcare industry. These techniques make use of advanced information and communication technology within healthcare environments for image or patient data sharing or transmission. Telemedicine also demands integration of medical images and the corresponding Electronic Patient Record (EPR) data for better diagnosis and understanding of the disease. This is a good initiative in the digital era and beneficial to many but this has some security issues, which need to be handled efficiently. Issues can be anything corresponding; insecure service can cause a problem to the patient in terms of manipulated data analysis, which can lead to the wrong prescription. Intruders can use critical metadata against patients in malicious ways: to shame people, to blackmail people and insurance fraud also. Hence, medical image storage and transmission plays an important role as cyber security measures. Many techniques has been designed like encryption, cryptography and watermarking to manage a wide range of privacy and security risks that may affect privacy.

[1] *Ramrao Adik Institute of Technology, D Y Patil deemed to be University, Mumbai, India.*
[2] *Lokmanya Tilak College of Engineering, Mumbai, India.*
* *Corresponding Author Email: namita.pulgam@rait.ac.in*

1.1. Digital Watermarking

In digital watermarking technique, an image of proprietor legitimacy as a watermark is inserted in the host image, and the data from the watermark can be retrieved afterwards. A digital watermark added to an image, is visible information either as a text or as any other picture used to protect the host image, or it makes it more difficult to replicate the material for illegal activities. Watermarking can be done in two ways viz. visible watermarking and invisible watermarking as shown in figure 1. A visible watermark is a semi-transparent text or image inserted in the original image whereas in an invisible watermarking process a transparent watermark is placed to a photo by modifying the image at the pixel level. In the watermarked image, secretly hidden data can only be extracted with specialized software to identify the copyright proprietor and also provides security to the hidden data [1]. Medical images can be easily manipulated and reproduced without being distorted. Watermarking, on the other hand, will benefit forensics because any image or evidence that has been tampered with is not accepted as a legal proof, but watermarked photographs are accepted. Watermarked images can include tracking components that helps to know how many copies of any particular image have been placed or created for the commercial purposes to make profit.

In watermarking (Figure 1), a standard logo image is added as a watermark into an image using two different methods to create a watermarked image. In the first case, the watermark image is clearly visible, making it very easy to identify the owner or designer of the image. As a result, unless and until that image is edited to remove the watermark, it becomes difficult to use it for illicit purposes. In the second method, the watermark is applied invisibly, making the hidden text or image invisible to all. As a result, it is possible that someone who is unaware of the hidden image, or that it is used on purpose to damage someone by altering the image utilizes an image inadvertently.

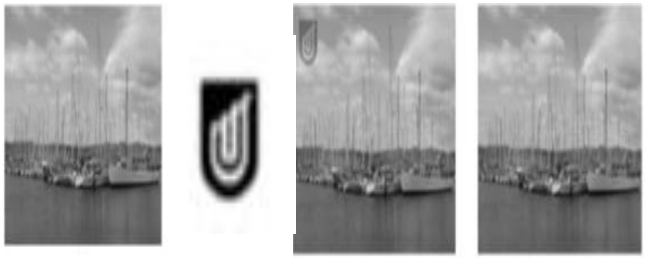

Fig. 1. An illustration of watermarking techniques namely visible and invisible (a) original image (b) watermark (c) generated watermarked image with visible watermark inserted at top-left corner (d) watermarked image with invisible watermarking technique [1].

Understanding the idea of telemedicine and telehealth fields alongside the significance of utilizing watermarking in the advanced medical services for integrity verification, authentication and data hiding is important and explained well in [2],[3]. Survey on various watermarking techniques in the medical domain, alongside the overview, general ideas of watermarking, significant characteristics, ongoing applications, ideas of embedding and recovery process of watermark, classification of watermarking techniques based on various parameters and the summary of different strategies is explained in [4-6]. Recent trends of watermarking techniques with their limitations and conventional attacks which should be considered while designing digital watermarking technique is explained in [5], [6]. Secure system for transferring medical image , face image , patient information and electronic health record (EHR) from one health center to another can be designed with the combination of cryptography and watermarking method tested to ensure the authorship and integrity of medical image data [4] , [7], [8]. The analysis can be carried out by calculating metrics like Mean Square Error (MSE), PSNR and SSIM on the watermarked images and confirms imperceptibility of the embedded watermark data [8].

1.2. Limitations of Digital Watermarking

Watermarking can not prevent image copying, but it can be used to track down and identify who owns photos that have been duplicated [1-3]. Watermarking systems must achieve a balance between robustness and imperceptibility. Watermarking techniques are exposed to skilled attacks. The requirements for robustness may differ from one system to the next. Watermark attacks are made not just to remove the watermark, but also to make it unreadable. Resizing and compressing images to convert them from one file format to another can cause the watermark to fade and become unreadable.

1.3. Conventional Attacks

Any processing in a watermarking system that could result in harmful detection of the watermark or interruption of the communication conveyed by the watermark is referred to as an assault. The watermarked image is distorted due to these attacks. Attacks are carried out through geometric alterations such as rotation, translation, sheering, or scaling of an image, as well as image enhancements such as sharpening, colour calibration, and contrast change. These seek to alter the watermark by exploiting the injected information rather than removing the watermark image itself. Compression attack performed results in the destruction of an image's watermark. The insertion of text or the addition of a second watermark to an image is performed with image composition and multiple watermarking attacks, which causes a problem authenticating the owner information. Image filtering and noise introduction can be used to reduce image quality, making watermark detection and extraction more difficult. [5, 6]

The following are the significant contributions made by the study: a) Proposing a robust watermarking algorithm for medical images' copyright and validity b) Improve the security of medical image transactions by integrating encryption techniques with the proposed watermarking scheme, c) Examine and evaluate the proposed technique for the selected medical image modalities.

The paper is organized as follows: The second section offers a comprehensive review of the literature. The proposed digital watermarking approach is discussed in Section 3. The simulation results for the proposed method are presented in Section 4. Section 5 is where the paper ends.

2. Literature Survey

Various works have presented a variety of watermarking approaches for content authentication, Intellectual Property Rights (IPR) protection, also for security of secret data, which have been applied in the spatial or frequency domain. Watermarking method to insert patient record into the Magnetic Resonance Imaging (MRI) images and effect of watermark embedding in frequency domain using Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) techniques in spatial domain with Least Significant Bit (LSB) technique is explained in [9]. Experimental results reveal that embedding processes in frequency domains are resistant to one type of attack, while embedding processes in spatial domains are resistant to a different type of attack. In [10] author explained a secret image-sharing scheme for protecting the unauthorized copying and modification of a sensitive digital image. In addition, this study includes a comparison of methods like Steganography, visual cryptography, watermarking, DWT etc. For medical computerized tomography images, an image watermarking technique is proposed in [11] using the combination of Singular Value Decomposition (SVD) and DWT. In comparison with traditional SVD and DWT based systems, this proposed system has better performance when it comes to robustness, imperceptibility and security. To overcome the security challenge a zero watermarking based approach with 3-dimensional hyper chaos and 3-dimensional dual tree complex wavelet transformation is suggested in [12]. The suggested approach scrambles the watermark with 3D hyper chaos before applying the 3D DTCWT-DCT transformation on medical volume data.

According to the study, watermarking aids in the security of digital intellectual property, such as ensuring patient privacy during medical image and telemedicine data exchange. Watermarking techniques can also be used for a variety of purposes; however, an invisible watermark is less confrontational than a visible one because it can be located. Watermarks interrupt the image, making it difficult for viewers to focus on the real subject being displayed, and this distraction directs the viewer's attention to the watermark rather than the image's substance. It is also relatively straightforward to remove the watermark using today's digital image tools, and photographs can be freely exchanged. As a result, when working with digital watermarking, it is critical to maintain the system's secrecy, security, and integrity. Papers with different cryptographic algorithms are studied and used for designing system to improve security and the ability to check that the image has not been tampered with without permission.

The conventional watermarking procedures help in identification of source as well as maintaining patient metadata for biomedical images [14]. Comparative analysis of both symmetric algorithms like DES, AES, Blowfish and asymmetric cryptographic algorithm RSA has been done for privacy of patients by considering various inputs like text or image files [13-16]. Comparative study between all these encryption algorithms and watermarking techniques is carried out using evaluation aspects like throughput, decryption and encryption time. In [16] author explained encryption as well as lossless compression techniques with additional security for secure data transmission in their study. The advantages and disadvantages of various compression and encryption technologies were examined in this research. For data security, the results of the analysis showed that encryption as well as compression approaches should be used.

Based on the design, flexibility, reliability, security, and constraints, a comparison of existing symmetric cryptography algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) have been conducted, concluding that AES is the efficient algorithm in terms of efficiency, security and architecture [17], [18]. AES takes less time to encrypt and decrypt data than DES, and DES has a higher encryption and decryption throughput than AES, implying that AES outperforms DES [18]. An algorithm based on cryptography to provide integrity, authentication and confidentiality for the pixel information and header is proposed in [19]. AES-GCM is used for achieving confidentiality and the Whirlpool hash function ensures integrity. With the calculated values of histogram analysis, correlation and entropy, it proves that the system is able to achieve confidentiality, authentication, and integrity. Experiments have shown that the method is capable of being used in telemedicine services.

Watermarking system designed with basic encryption algorithms is not efficient enough as it is difficult to extract exact watermark if any attack is performed on the system. Hence, to improve imperceptibility and robustness of the system a strong encryption algorithm has to be used. This can be achieved through chaos based encryption algorithms and review of this is presented further.
A strategy for reversible watermarking based on prediction error expansion is described in [20] The authors propose a system employing chaos maps to encrypt watermark and location map prior to embedding. An experimental result shows that the extracted watermarked image quality is good in comparison with the covered image. In [21] author presents a watermarking technique based on chaotic encryption to hide electronic medical records in medical images which can be utilized in e-healthcare and telemedicine. Watermark is inserted in the host image by modifying the difference between DCT coefficients of adjacent blocks. To ensure a double layer of protection along with chaotic encryption, the Arnold transform is applied. The proposed technique is put to the test against various attacks like compression, cropping, sharpening and median filtering and the proposed scheme is resilient, according to the findings.

A system using the chaotic sequence and a modified AES algorithm as encryption algorithm is presented in [22]. Arnold chaos sequence is used to produce the encryption key in this method. The original image is then encrypted with the chaotic system's round keys and a modified AES method. In [23] authors proposed multimedia encryption based on chaos with models of 2D alteration for high-security data transmission. The proposed system provides good encryption quality reproduced by chaos and it is resistant to attacks. This proposed encryption system for speech cryptosystem provides high-security characteristics and a low correlation between actual and encrypted voice signals.

A color image digital watermarking system that is resistant to geometric attacks is elaborated in [24]. The suggested watermarking algorithm's robustness and quality are assessed and experimental results show that the system is robust against conventional and geometrical attacks. To protect medical images, a technique with a dynamic secret key is presented in [25]. Secret keys are retrieved from the information of the pixels in the system, and the positions of the pixels are then permuted using a periodic confusion method and pseudo-random sequences. Finally, depending on logistic system sequences and the XOR operator, permuted image pixels are coded. Evaluation of the system is done and results assure the efficiency of the suggested schema by resisting cryptographic attacks.

Image data has unique qualities like bulk capacity, high redundancy, and strong pixel correlation, all of which place significant demands on any encryption technique. Algorithms used in classical encryption such as RSA, DES, AES, and others have a low level of security and are extremely vulnerable to assaults. Chaotic image encryption algorithms can solve this problem since they generate keys with a high level of unpredictability and reduce the encryption process' computational cost [26] [27]. The benefits of a chaotic-based image encryption technique are ease of use, higher encryption speed, and resistance to attacks.

3. Proposed Watermarking using Pixel Color Correlation (WPCC)

Digital watermarking is a process in which information is embedded into an image in such a way that the additional payload is undetectable to the naked eye. Image watermarking has been suggested as a useful method for identifying an image's source, owner or authorized consumer. Data authentication, broadcast monitoring, and Copyright protection are some of the uses for watermarking combined with encryption. Hence, to address issues related to telemedicine the facility system has been designed for medical image security as depicted in figure 2. Here digital watermarking along with encryption techniques is implemented to

provide copyright protection to the medical image being shared among medical centers. Patient record is encrypted with Chaos and Arnold encryption technique is used to add one more level of security so that the patient's personal information will not be disclosed with any person unless they have access to it. This encrypted image is embedded into the cover image to get the watermarked image. After decryption, the watermark image can be recovered from the encrypted watermarked medical image. The extracted watermark represents patient's medical record as inserted in the embedding process. In addition, robustness of the system is checked with various attacks. Proposed system is explained in detail with further sections.

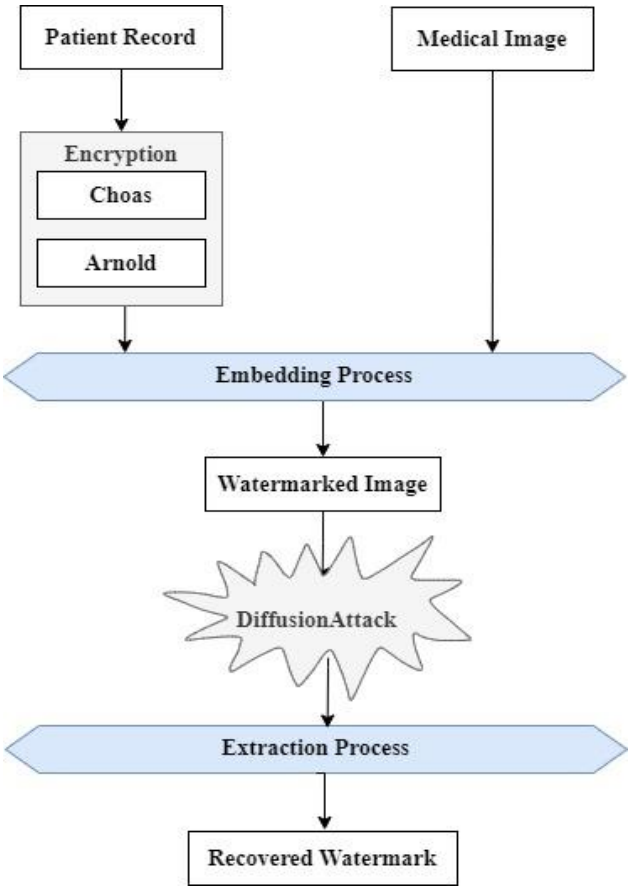

Fig. 2. Proposed System's Block Diagram.

3.1. Chaos based Encryption Technique

Chaos-based cryptographic algorithms are efficient and have distinctive traits like sensitive dependence on initial circumstances, non-periodicity, non-convergence, and mixing, all of which make chaotic systems unpredictable. Chaotic systems are a better choice for developing cryptosystems because their vulnerability to the initial condition parameter and mixing characteristics are similar to the confusion and diffusion features of a good cryptosystem. Cryptography using chaos makes the encryption process easier to execute, faster, and resistant to most attackers [26].

As shown in Figure 3, the first phase of chaos-based image encryption is confusion, and the second phase is diffusion. The pixel locations are modified over the entire image in the confusion phase, making the image unrecognizable. Pixel scrambling is the name given to the process of changing the chaotic map's beginning conditions and control parameters. This is the key, and it is iterated for a long period to widen the scrambling, resulting in an unrecognizable image. Confusion, or just scrambling, will not provide security because they are vulnerable to the majority of attacks. As a result, the scrambled image is sent through a diffusion phase, which seeks to change the value of pixels throughout the image. Initial circumstances and control parameters are included in a chaotic map as the key is used to change the pixel value, and this process is fed back to phase one. To achieve security, this is iterated for a long time.

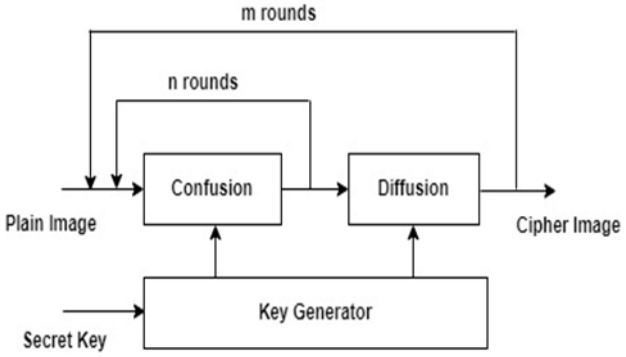

Fig. 3. Architecture of a Chaos-Based Image Cryptosystem [26].

3.2. Arnold Transformation

The security of information can be improved by employing a variety of encryption techniques, one of which is the Arnold transform. Because the Arnold scrambling algorithm is simple and periodic, it is commonly used in digital watermarking technologies. Scrambling can be used to improve the robustness of digital watermarking by changing the distribution of the error bit in the image. After numerous cycles, the original image can be retrieved due to Arnold scrambling periodicity [29] [30].
This two-dimensional encryption algorithm works effectively in applications that encode images of type NXN. As indicated in equation (1), the Arnold transformation can be stated numerically.

$$\begin{bmatrix} \mathbf{x_n} \\ \mathbf{y_n} \end{bmatrix} = \begin{bmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{2} \end{bmatrix} \begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix} \textbf{(mod N)} \qquad \text{---------- (1)}$$

where (x_n, y_n) are the coordinates of the input image and (x, y) are encrypted image pixel coordinates. The transform causes pixel locations to alter, resulting in an image that is chaotic and different from the original. The Arnold transform produces an encrypted image that corresponds to the original image one-to-one. The Arnold encryption's pseudo-random nature results in a jumbled image that cannot be cracked without knowing the sequence adopted. The number of iterations, which can be set at the start of the operation, determines the encryption strength. The equation is used to decrypt the encrypted message using the inverse Arnold transform (2).

$$\begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix} = \begin{bmatrix} \mathbf{2} & \mathbf{-1} \\ \mathbf{-1} & \mathbf{1} \end{bmatrix} \begin{bmatrix} \boldsymbol{x_n} \\ \boldsymbol{y_n} \end{bmatrix} \textbf{(mod N)} \qquad \text{---------- (2)}$$

3.3. Watermarking using Pixel Color Correlation (Proposed Watermarking Technique)

Watermarks in the frequency domain are dispersed randomly

across the entire image, making it impossible for an attacker to change them. As a result, frequency domain techniques are used to design the majority of systems. DCT Transform Digital watermarking is a frequency domain technique that involves changing frequency coefficients to implant a watermark. Images are broken down into blocks of size 8x8, 16x16, or larger in the DCT method. If the image is lowered to greater compression ratios during processing, these blocks become visible and the blocking effect occurs. Another drawback with DCT-based methods is that the original image is altered in an irreversible manner, making accurate recovery impossible. To circumvent these problems, the paper presents a watermarking approach in which the patient's medical record is included in the cover image, which is a medical image. To create a watermarked image, the secret image i.e. a patient's record is encrypted first and then inserted into the cover image. The hidden image will be decoded after the watermark has been extracted.

Algorithm:

Input : Cover Image CI, Secret Image SI

Output : Extracted Watermark

Step 1: Start.

Step 2: Location of pixels of each color intensity 0 to 255 in Cover image is stored in list say δ.

Step 3: Check the image and get count of zero value pixels i.e.

$i=i+1\ \forall\ i$ such that $\delta(i+1)=0$ and $i \leq 256$

$\delta(1 \text{ to } i) = \delta(i+1)$

Step 4: $\delta(i) = \begin{cases} \delta(i-1) & \text{if } \delta(i) = 0 \\ \delta(i) & \text{otherwise} \end{cases}$ where i = 2 to 256

Step 5 : Generate Key $\alpha = \delta(SI)$

Step 6 : Embed secret image into cover image with key to get Watermarked Image i.e. $\gamma = (CI, key)$

Step 7 : Perform attacks

Step 8 : Extract watermark from watermarked image with the key

Step 9 : Stop.

Proposed watermarking approach makes the list of the locations of pixel color value (step 2 of algorithm). Step 3 checks for the count of zero value pixel. It is possible that some of the pixel colors are not matching with any pixel. Then, that pixel color is set to nearest color location and stored in the list. For e.g. If pixel with maroon color is not available then color of that pixel is set to red color pixel. This step 4 helps while extracting image even after any attack has been performed. In step 5 key is generated which contains the locations of the colors of pixels of encrypted secret image. Embedding and extraction is performed with this key.

Working directly with pixel values makes it simple to choose pixel data from the watermarked image, even if an attack is carried out, and aids in the precise reconstruction of the secret image later on. This algorithm performs better than a DCT-based approach because the proposed method maintains pixel information in the file, but DCT does not preserve pixel information and DCT works on a block of image that is influenced by noise.

4. Experimental Details and Results

The suggested approach is tested and analysed using a variety of cover medical images, including US, CT, X-ray, MRI, mammography, and normal images like lena, baboon, and Pepper. These images were taken from public medical databases [32, 33] and the images size is 512 × 512 pixels as shown in Figure 4. The patient's medical report is used as watermark image for the experiment as illustrated in Figure 4. The watermark image has a size of 256 × 256 pixels.

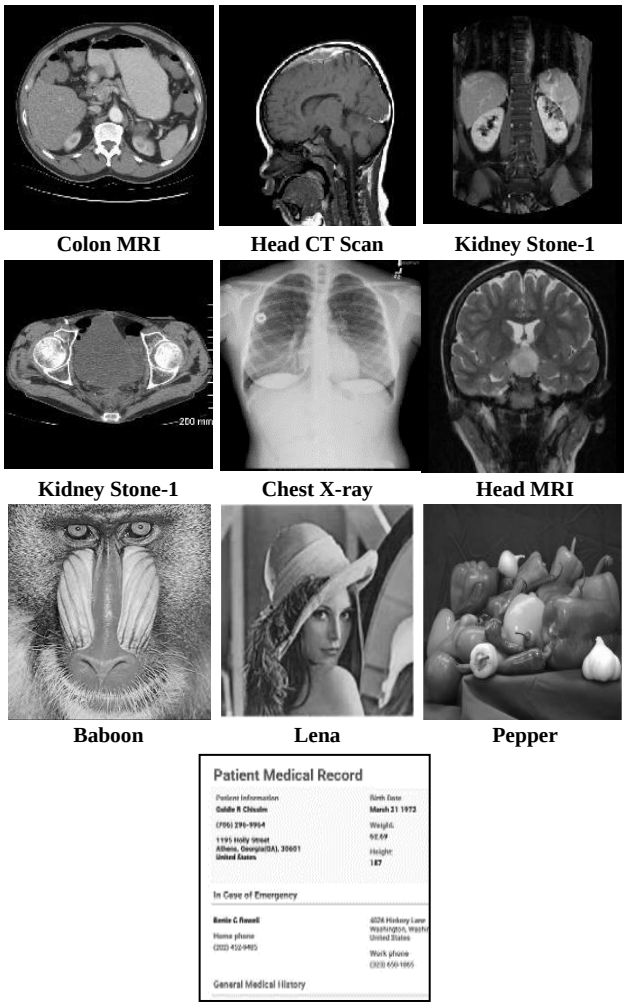

Fig. 4. Input Images and Watermark Image.

In this experiment, all methods are carried out on the same platform on a laptop with an Intel(R) Core (TM) i3-4005u CPU @ 1.70 GHz and 4 GB RAM with the Windows 8.1 operating system and MATLAB 2018. The experimental results are organized into two sections: the first focuses on determining imperceptibility, while the second examines robustness against various attacks.

4.1. Evaluation Parameters

In medical image watermarking , it is necessary to protect the image's quality as well as the patient's information. As a result, two types of benchmarking are required when assessing a watermarked image: the first is to assess the image's quality, and the second is to assess the extracted watermark's correctness. By comparing the extracted and original watermarks, the accuracy of extracted watermarks will be determined. As a result, the watermarking community frequently uses the Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index Measure (SSIM) to evaluate the fidelity of embedding algorithms. To measure the reliability of an extracted watermark several image quality indicators such as Bit Error Rate (BER), and Normalized Cross-Correlation (NCC) have been used. PSNR, MSE and SSIM is calculated using the equations 3, 4 and 5 respectively.

$$\text{PSNR} = 10\log\frac{(2^v-1)^2}{\text{MSE}} \quad \text{---------- (3)}$$

$$\text{MSE} = \frac{1}{\text{MN}}\sum_{l=1}^{M}\sum_{k=1}^{N}\left(H_{l,k} - E_{l,k}\right)^2 \quad \text{---------- (4)}$$

$$\text{SSIM}(x,y) = \frac{(2\,\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2+\mu_y^2 + c_1)(\,\sigma_x^2+\sigma_y^2 + c_2)} \quad \text{---------- (5)}$$

The system's BER and NCC values determine how resistant it is to image processing procedures. If errors are introduced into the data, the system's integrity may be affected, making it important to evaluate the system's performance. The greater the NCC and smaller the BER, the better the system's resistance against attacks. BER is calculated using equation 6 and NCC is calculated using equation 7 as shown below.

$$\text{BER} = \frac{1}{\text{MN}}\left[\sum_{i=1}^{m}\sum_{j=1}^{n} w_0(i,j) \oplus w_x(i,j)\right] \quad \text{---------- (6)}$$

$$\text{NCC} = \frac{\sum_{i=1}^{m}\sum_{j}^{n} w_0(i,j)\, w_x(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}[\,w_o(i,j)]^2} \quad \text{---------- (7)}$$

Here, the smallest number of bits is represented by 'v' that may indicate a particular image's maximum intensity, E and H are the marked and host images respectively. Number of columns and rows of the host image are represented with N and M respectively. PSNR is used to evaluate the watermarked image's quality. The structural similarity index SSIM and peak signal to noise ratio PSNR were also used to assess the quality of the watermarked images. A greater PSNR value implies that the system is efficient, i.e. there is no noticeable difference between perfect and distorted image.

Proposed system is compared with existing system [21, 31] for the execution time required. Existing system [21] takes on an average 0.402s and [31] takes 0.553s whereas proposed system requires 0.0349s. Hence, time complexity wise proposed technique is better.

4.2. Imperceptibility Analysis

SSIM and PSNR have been chosen as quantitative measures for evaluating the quality of watermarked images. For several medical image modalities and general images, the proposed method generates images of excellent quality with a high PSNR ranging from 24.74dB to 36.07dB. Watermarked image received after embedding process and watermark extracted from the same is shown in figure 5. This is divided into two rows where first row represents watermarked image and second row represents extracted watermark.

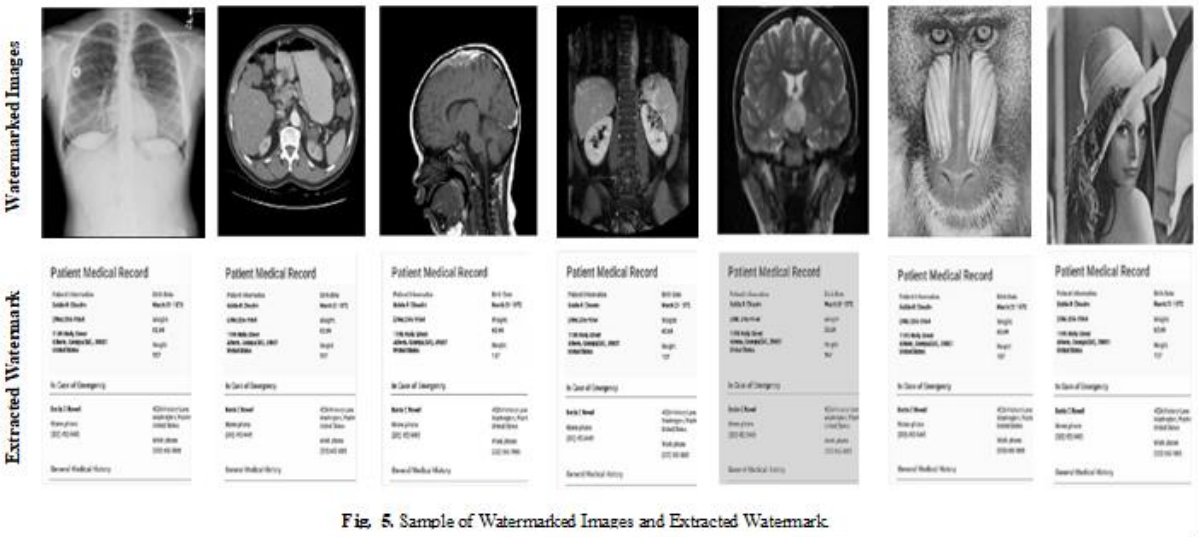

Fig. 5. Sample of Watermarked Images and Extracted Watermark

Performance of the proposed system is compared [21] and [31]. In existing system [21] watermarking technique based on chaotic encryption and Arnold transform is defined to hide electronic medical records in medical images The watermark is embedded in the host image using the suggested approach by altering the difference among DCT coefficients of adjacent blocks. Paper [31] provides a non-blind and robust watermarking system based on a combination of singular value decomposition (SVD), finite ridgelet transform (FRT), and Arnold scrambling based encryption for secure medical images. In proposed system, watermarked medical image is encrypted before sending it at the receiver end to provide security. The comparison results are reported in Table 1. The objective performance measures for input images when no attack is done to the watermarked content is shown in table 1. Figure 5 and table 1 show that the watermarked images' objective and subjective quality both are excellent.

Table 1. Objective Performance Analysis of proposed System

Input Image File	Proposed System		Existing System [21]		Existing System [31]	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Chest X-Ray	30.24	0.92	26.41	0.92	30.41	0.91
Colon MRI	27.71	0.92	26.61	0.92	30.85	0.91
Head CT Scan	28.58	0.95	26.67	0.91	32.67	0.94
Kidney Stone	36.07	0.97	26.41	0.95	29.67	0.91
Breast Mammography	29.8	0.96	26.41	0.95	31.8	0.94
MRI	33.67	0.97	26.4	0.95	31.85	0.92
Babbon	24.74	0.81	26.41	0.99	25.42	0.98
Peppers	32.41	0.95	26.51	0.98	30.67	0.96
Lena	29.52	0.84	26.4	0.99	28.56	0.97

As depicted in figure 6 , a comparison of PSNR with existing techniques has been conducted. The comparison findings reveal that the presented approach provides high-quality grayscale images.

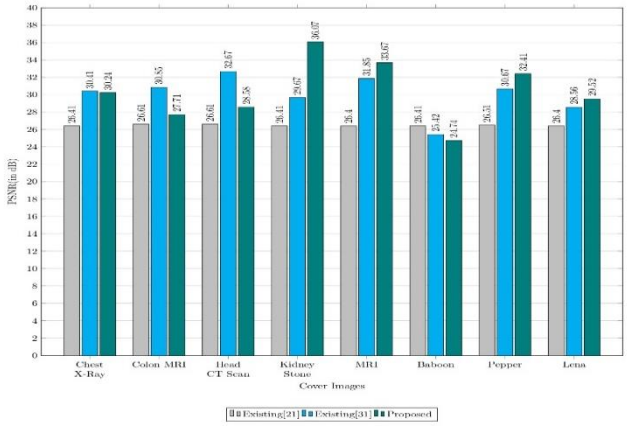

Fig. 6. Evaluation of PSNR for Different Images in Comparison with Existing Technique.

The proposed system's SSIM values are calculated and compared as shown in figure 7. Table 1 shows the SSIM comparison findings, results demonstrate that the suggested technique produces better watermarked images than existing systems.

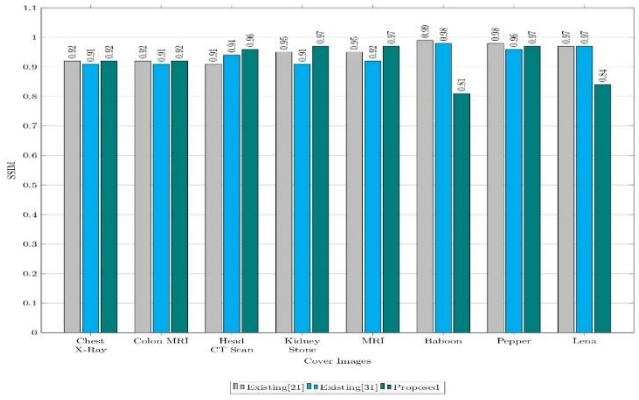

Fig. 7. Evaluation of SSIM for Different Images in Comparison with Existing Technique.

4.3. Robustness Analysis

When an identifiable watermark is extracted from a watermarked image following an attack, the watermarking system is considered to be cohesive. On the watermarked images, several assaults were employed to assess the reliability of the proposed approach, including rotation, resizing, filtering, noise addition, compression, and so on. To assess the system's robustness, objective measures such as NCC and BER were used.

4.3.1. Analysis for Rotation Attack

The most typical uses of rotation are to enhance the aesthetic value of an image and to produce new ones. With rotation attack intruder tries to identify the watermark embedded in the image by creating new image. Figure 8 shows the watermarked images before and after attack as well as the retrieved watermarks after a 10-degree rotation. Figure 8 shows that the rotated images yield recognized watermark, and the BER in Table 2 indicates that the designed scheme is rotation-resistant.

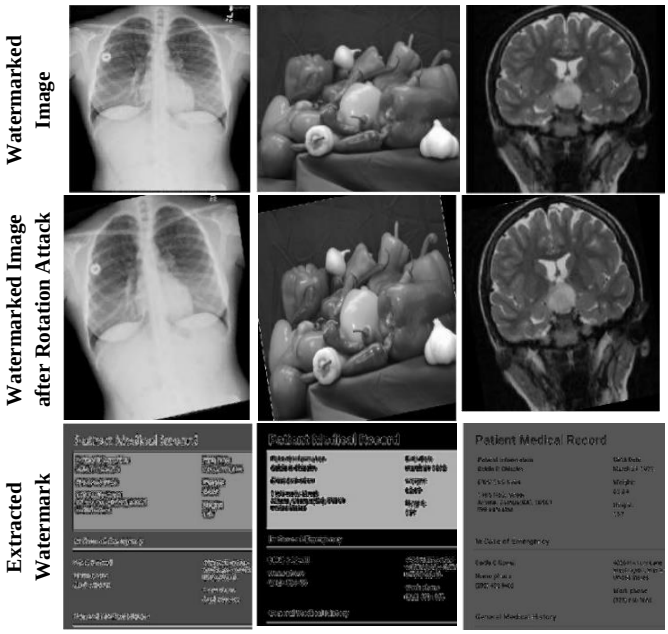

Fig. 8. Watermarked Image, Distorted Image & Retrieved Watermark after Rotation Attack.

4.3.2. Resizing Attack Analysis

The system's robustness was also evaluated in a resizing attack. Resizing or Scaling is used to affect the visual appearance of an image as well as the amount of data included in the image representation. For the experiment purpose, the watermarked Lena image and watermarked chest X-ray image was resized to 0.8 and 1.6 times its original dimensions. Figure 9 shows the resized images as well as the watermarks extracted from them. The figure clearly shows that resized images yield recognized logos, implying that the suggested scheme is resistant to resizing. Table 2 compares the NCC and BER results achieved for the resizing assault with the previous approach. Table 2 shows that the proposed strategy outperforms the techniques under consideration.

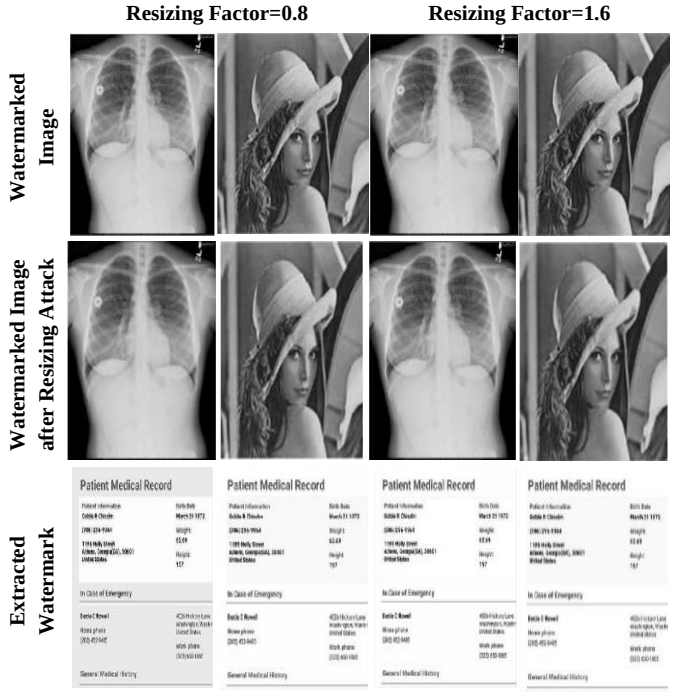

Fig. 9. Watermarked Image, Distorted Image & Extracted Watermark after Resizing Attack.

4.3.3. Analysis of Robustness against Noise and Filtering Assaults

Some of the attack adds a noise signal to an image in order to deliberately corrupt the image, hence reducing its visual quality. Filtering is applied to the watermarked image, resulting in a difference map made up of noise. The goal of these assaults is to erase the watermark data from the watermarked object. The fact that the watermark is usually an additive noise signal included in the host signal is exploited in such attacks.

For experiment, with a noise, density of 0.01 Salt and pepper noise was introduced to the watermarked images, as well as Gaussian noise with a mean of zero and variance of 0.001. Figure 11 depicts the results, which demonstrate that the proposed approach is resilient to distortions because detectable watermarks were retrieved from degraded Lena and chest x-ray images. Image filtering techniques, such as 3X3 median filtering and low-pass filtering attacks, were also used to assess the system's robustness. The findings given in Figure 11 demonstrate that the suggested approach is also resistant to filtering attacks. It was also demonstrated that the suggested approach is resistant to attacks such as histogram equalization and sharpening. Figure 10 shows the results. The proposed schemes' results were compared to those found in [21]. Figure 10 shows that the designed system outperforms the schemes used for comparison. This is because the suggested method calculates and saves the correlation between pixel colour for subsequent use during watermark insertion and extraction from the attacked images.

4.3.4. JPEG Compression Attack Analysis

The most widely used image compression technology for compressing images in order to save storage and transmission time is JPEG compression. Adversaries may attempt to compress watermarked images, making it impossible for the copyright holder to authenticate his ownership. Since JPEG compression truncates high-frequency components, reducing watermarked watermark being retrieved. As a result, the reliability of any watermarking system should be verified for JPEG compression attacks as well. The performance of the proposed approaches was evaluated using JPEG compression. For images like Lena, Chest X-ray etc., the comparison findings are presented in Table 2, which illustrates that the suggested technique is more resistant to compression attacks than the alternatives.

5. Conclusion

Currently in the telemedicine field, patient's medical records are shared with specialists for the expert opinion and to provide proper treatment to the patient. This has been possible due to fast development of healthcare technology which also, improves the issues related to the security of the patient's medical information and has become a prime concern nowadays. Hence secured proposed system is designed with digital watermarking and encryption technique. Traditional encryption systems are not that efficient to provide security to medical images hence we used the chaotic cryptography technique because of its lower mathematical complexity and better security. Chaotic maps are more effective for image encryption because of their randomness property. To increase the security level Arnold transformation is also used along with chaotic encryption techniques. Most of the systems are implemented with DCT or DWT to embed watermarks into the cover image. In DCT-based methods, the original image is damaged in a non-reversible manner and becomes difficult to recover precisely. To avoid this issue watermarking technique based on the image intensity values is proposed in this paper and key will be generated within that. The encryption strategy under consideration is adequate against a differential attack, despite minor changes in the original images resulting in a substantial difference in encrypted pixels. Henceforth, proposed system can be used in telemedicine and e-healthcare fields to transmit a patient's record securely over the network for consultancy purposes.

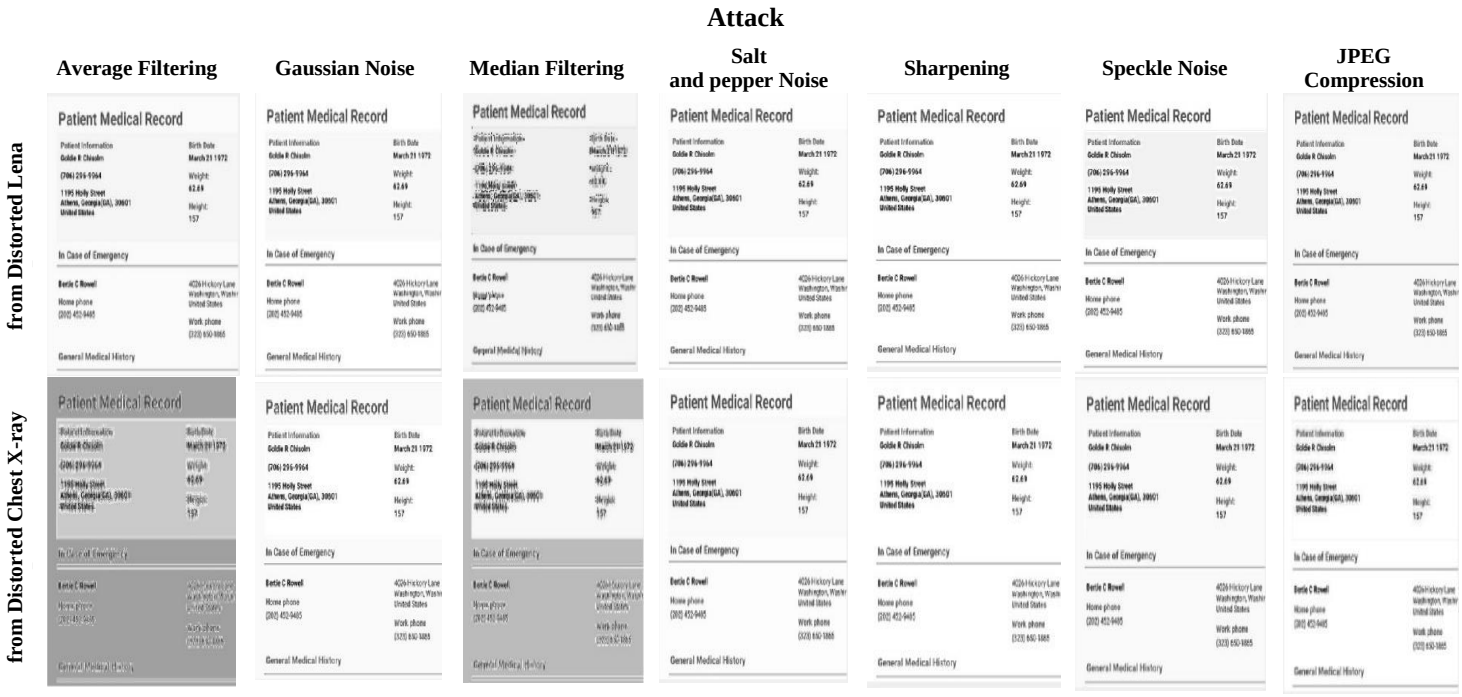

Fig. 10. Extracted Watermark Images after Performing Different Attacks on Lena and Chest X-ray Images.

Table 2. Analysis of the watermark recovered from attacked Chest X-ray image and Lena image

Attack	Lena						Chest X-Ray					
	Proposed		Existing [21]		Existing [31]		Proposed		Existing [21]		Existing [31]	
	NCC	BER(%)	NCC	BER(%)	NCC	BER(%)	NCC	BER(%)	NCC	BER(%)	NCC	BER(%)
Average Filter	0.9999	19.88	0.9938	32.46	0.9856	41.25	0.9862	51.86	0.9948	28.35	0.9852	42.35
Gaussian low-pass filter	0.9999	19.93	0.9940	32.40	0.9646	45.86	0.9870	48.78	0.9949	28.33	0.9501	50.86
Gaussian Noise	0.9999	10.09	0.9961	23.00	0.9763	17.23	0.9995	16.45	0.9962	20.25	0.9663	18.23
Histogram Equalization	0.9990	14.44	0.9372	24.62	0.9831	18.65	0.9991	14.62	0.1984	82.81	0.9821	16.46
JPEG2000 Compression	0.9999	17.11	0.9995	23.63	0.9759	16.53	0.9999	11.83	0.9995	19.21	0.9859	15.31
JPEG Compression	0.9999	25.52	0.9997	23.94	0.9865	21.41	0.9998	13.16	0.9998	18.21	0.9765	20.41
Median Filter	0.9952	24.37	0.9984	31.37	0.9861	27.58	0.9880	22.44	0.9980	24.98	0.9618	25.88
Motion blur	0.9998	21.79	0.9806	36.80	0.9485	23.42	0.9737	66.56	0.9879	31.28	0.9285	24.34
Rescaling Factor= 0.6	0.9999	16.67	0.9995	18.40	0.9542	30.84	0.9987	34.82	0.9993	26.42	0.9452	35.84
Rescaling Factor= 1.2	0.9999	3.49	0.9997	15.93	0.9823	29.76	0.9999	16.37	0.9997	25.66	0.9542	28.66
Rotation by 10	0.8940	85.0	0.6791	58.75	0.9474	32.34	0.8846	55.91	0.8895	36.69	0.8974	22.34
Salt and pepper noise	0.9999	5.98	0.9992	22.01	0.9840	22.13	0.9999	8.05	0.9989	19.44	0.9940	20.13
Sharpening	0.9999	9.82	0.9963	16.20	0.9999	11.52	0.9999	12.29	0.9976	14.72	1.0000	10.24
Speckle Noise	0.9998	33.33	0.9992	23.11	0.9833	28.72	0.9997	35.58	0.9983	19.71	0.9933	25.27

References

[1] Wang FH., Pan JS., Jain L.C. (2009), “Digital Watermarking Techniques. In: Innovations in Digital Watermarking Techniques. Studies in Computational Intelligence”, vol 232. Springer, Berlin, Heidelberg, doi: 10.1007/978-3-642-03187-8_2.

[2] S. Kumar and B. K. Singh, (2018), "A Review of Digital Watermarking in HealthCare Domain," 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), pp. 156-159, doi: 10.1109/CSITSS.2018.8768733.

[3] Allaf A.H., Kbir M.A. (2019) “A Review of Digital Watermarking Applications for Medical Image Exchange Security” Innovations in Smart Cities Applications Edition 2. SCA 2018. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham, doi: 10.1007/978-3-030-11196-0_40.

[4] Aparna, Puvvadi and Kishore, Polurie Venkata Vijay, (2020) "A Blind Medical Image Watermarking for Secure E-Healthcare Application Using Crypto-Watermarking System", Journal of Intelligent Systems, vol. 29, no. 1, pp. 1558-1575. doi: 10.1515/jisys-2018-0370.

[5] Begum, Mahbuba, and Mohammad S. Uddin, (2020), "Digital Image Watermarking Techniques: A Review", Information Journal, vol. 11, doi: 10.3390/info11020110.

[6] Anand, Ashima. (2021), “Watermarking techniques for medical data authentication: a survey:, Multimedia Tools and Applications, Springer, Vol 80. doi:10.1007/s11042-020-08801-0.

[7] Roček, Aleš , Javornik, Michal , Slavicek, Karel and Dostal, Otto. (2021), “Zero Watermarking: Critical Analysis of Its Role in Current Medical Imaging”, Journal of Digital Imaging, Springer, Vol. 34. doi: 10.1007/s10278-020-00396-0.

[8] V. Raj, A. B. S, S. Janakiraman, S. Rajagopalan and R. Amirtharajan, (2020), "Scattering Watermark on DICOM Images," International Conference on Computer Communication and Informatics (ICCCI), IEEE, Coimbatore, India , pp. 1-4, doi:10.1109/ICCCI48352.2020.9104174.

[9] E. Elbasi and V. Kaya, (2018), "Robust Medical Image Watermarking Using Frequency Domain and Least Significant Bits Algorithms", International Conference on Computing Sciences and Engineering (ICCSE), IEEE Kuwait, pp. 1-5, doi: 10.1109/ICCSE1.2018.8374221.

[10] Chanu, O.B., Neelima, A., (2019), “A survey paper on secret image sharing schemes”, International Journal of Multimedia Information Retrieval, Springer, Vol. 8, pp. 195–215, doi:10.1007/s13735-018-0161-3.

[11] R. A. Movahed, M. R. Rezaeian and S. Ghasemi, (2019), "An Image Watermarking Algorithm for Medical Computerized Tomography Images," 5th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), IEEE, Shahrood, Iran, pp. 1-5, doi: 10.1109/ICSPIS48872.2019.9066018.

[12] Liu, Jing Ma, Jixin , Li, Jingbing , Huang, Mengxing , Sadiq, Naveed and Ai, Yang, (2020), “Robust Watermarking Algorithm for Medical Volume Data in Internet of Medical Things”, IEEE Access. pp. 1-1, doi:10.1109/ACCESS.2020.2995015.

[13] M. Panda, (2016), "Performance analysis of encryption algorithms for security", International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), IEEE, Paralakhemundi, India, pp. 278-284, doi: 10.1109/SCOPES.2016.7955835.

[14] S. Bansal and G. Mehta, (2017), "Comparative analysis of joint encryption and watermarking algorithms for security of biomedical images", 7th International Conference on Cloud Computing, Data Science and Engineering, IEEE, Noida India, doi: 10.1109/CONFLUENCE.2017.7943224.

[15] S. Singh and R. Devgon, (2019), "Analysis of Encryption and Lossless Compression Techniques for Secure Data Transmission," 4th International Conference on Computer and Communication Systems (ICCCS), Singapore, pp. 1-5, doi: 10.1109/CCOMS.2019.8821637.

[16] Pk, Kavitha and Saraswathi, Vidhya, (2019), "A Survey on Medical Image Encryption", 1st International Conference on Applied Soft Computing Techniques, Kalasalingam University, Krishnankoil, vol. 3, doi:10.32628/ICASCT2501.

[17] Philip, A. M., and D. S. . Hemalatha. "Identifying Arrhythmias Based on ECG Classification Using Enhanced-PCA and Enhanced-SVM Methods". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, May 2022, pp. 01-12, doi:10.17762/ijritcc.v10i5.5542.

[18] S. S. Ghosh, H. Parmar, P. Shah and K. Samdani, (2018), "A Comprehensive Analysis Between Popular Symmetric Encryption Algorithms", IEEE, Punecon, doi:10.1109/PUNECON.2018.8745324

[19] S. Srilaya and S. Velampalli, (2018), "Performance Evaluation for DES and AES Algorithms-An Comprehensive Overview," 3rd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology (RTEICT), Bangalore, India, pp. 1264-1270, doi: 10.1109/RTEICT42901.2018.9012536.

[20] Kabisha, M. S., Rahim, K. A., Khaliluzzaman, M., & Khan, S. I. (2022). Face and Hand Gesture Recognition Based Person Identification System using Convolutional Neural Network. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 105–115. https://doi.org/10.18201/ijisae.2022.273

[21] M. Brindha, (2018), "Confidentiality, Integrity and authentication of DICOM medical images", 2nd International Conference on Inventive Systems and Control, IEEE, Coimbatore, India, doi: 10.1109 / ICISC.2018.8398924

[22] Vishakha Kelkar, Dr. Kushal Tuckley, (2018), "Reversible watermarking for medical images with added security using chaos theory", 3rd International Conference on Communication and Electronics Systems (ICCES), IEEE, Coimbatore, India, doi: 10.1109 / CESYS.2018.8724039.

[23] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh and G. M. Bhat, (2018), "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," in IEEE Access, vol. 6, pp. 19876-19897, doi: 10.1109/ACCESS.2018.2808172.

[24] Arab, A., Rostami, M.J. and Ghavami, B., (2019), "An image encryption method based on chaos system and AES algorithm", Journal of Supercomputing, vol. 75, pp. 6663–6682, doi: 10.1007/s11227-019-02878-7.

[25] Garg, D. K. . (2022). Understanding the Purpose of Object Detection, Models to Detect Objects, Application Use and Benefits. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 01–04. https://doi.org/10.17762/ijfrcsce.v8i2.2066

[26] Yasser, I.; Mohamed, M.A.; Samra, A.S.; Khalifa, F., (2020), "A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications", Information Entropy Algorithms for Image, Video, and Signal Processing, Entropy 2020, vol. 22, pp. 1253. doi: 10.3390/e22111253.

[27] Bhatti, Uzair , Yuan, Linwang , Yu, Zhaoyuan , Li, Jingbing , Nawaz, Saqib Ali , Mehmood, Anum and Zhang, Kun., (2020), "Hybrid Watermarking Algorithm Using Clifford Algebra With Arnold Scrambling and Chaotic Encryption", IEEE Access, pp. 1-1, doi:10.1109/ACCESS.2020.2988298.

[28] Sareh Mortajez, Marziyeh Tahmasbi, Javad Zarei, Amir Jamshidnezhad, (2020), "A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images", Informatics in Medicine Unlocked, vol. 20, doi:10.1016/j.imu.2020.100396.

[29] P. R. Sankpal and P. A. Vijaya, (2014), "Image Encryption Using Chaotic Maps: A Survey," Fifth International Conference on Signal and Image Processing, IEEE, Bangalore, India, pp. 102-107, doi: 10.1109/ICSIP.2014.80.

[30] L. Kocarev, (2001), "Chaos-based cryptography: a brief overview," IEEE Circuits and Systems Magazine, IEEE, vol. 1, no. 3, pp. 6-21, doi: 10.1109/7384.963463.

[31] Amir Daneshgar, Behrooz Khadem, (2015), "A self-synchronized chaotic image encryption scheme", Signal Processing: Image Communication, Elsevier, Vol. 36, pp. 106-114, doi:10.1016/j.image.2015.06.005.

[32] V. I. Arnold and A. Avez,(1968), " Ergodic Problems of Classical Mechanics. (Advanced Book Classics). New York, NY, USA: Benjamin.

[33] N. A. Libre. (2021). A Discussion Platform for Enhancing Students Interaction in the Online Education. Journal of Online Engineering Education, 12(2), 07–12. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/49

[34] Min, Li, Ting, Liang and Yu-jie, He. (2013). "Arnold Transform Based Image Scrambling Method", Proceedings of 3rd International Conference on Multimedia Technology, Atlantis Press, doi: 10.2991/icmt-13.2013.160.

[35] Thanki, R., Kothari, A. Multi-level security of medical images based on encryption and watermarking for telemedicine applications. Multimed Tools Appl 80, 4307–4325 (2021). https://doi.org/10.1007/s11042-020-09941-z.

[36] Suckling, J., Parker, J., Dance, D., Astley, S., Hutt, I., Boggis, C., Ricketts, I., et al. (2015). Mammographic Image Analysis Society (MIAS) database v1.21 [Dataset]. https://www.repository.cam.ac.uk/handle/1810/250394

[37] Medical Image Database. Available: https://medpix.nlm.nih.gov/.