Check for updates

Received: 16 July 2024 | Revised: 25 November 2024 | Accepted: 1 December 2024

The Journal of Engineering

DOI: 10.1049/tje2.70038

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

A novel approach for encryption and decryption of digital imaging and communications using mathematical modelling in internet of medical things

S. Thalapathiraj[1] | J. Arunnehru[2] | V. C. Bharathi[3] | R. Dhanasekar[4] | L. Vijayaraja[4] | R. Kannadasan[5] | Muhammad Faheem[6,7] | Arfat Ahmad Khan[8]

[1]Department of Mathematics, SRM Institute of Science and Technology, Vadapalani Campus, Chennai, India

[2]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai, India

[3]School of Computer Science and Engineering, VIT-AP University, Amaravati, India

[4]Department of Electrical and Electronics Engineering, Sri Sairam Institute of Technology, Chennai, India

[5]Department of Electrical and Electronics Engineering, Sri Venkateswara College of Engineering, Sriperumbudur, India

[6]School of Technology and Innovations, University of Vaasa, Vaasa, Finland

[7]VTT- Technical Research Centre of Finland, Ltd., Espoo, Finland

[8]Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen, Thailand

Correspondence
Muhammad Faheem, School of Technology and Innovations, University of Vaasa, Vaasa, Finland.
Email: muhammad.faheem@uwasa.fi

Abstract

This research introduces an innovative algorithm for the encryption and decryption of greyscale digital imaging and communications in medicine images utilizing Laplace transforms. The proposed method presents a ground breaking approach to image encryption, effectively concealing visual information and ensuring a robust, secure, and reliable encryption process. By leveraging the inherent strengths of Laplace transform, the algorithm guarantees the complete retrieval of the original image without any loss, provided the correct decryption key is used. To thoroughly evaluate the performance of the algorithm, multiple tests were conducted, including extensive statistical analyses and assessments of encryption quality. Key performance metrics were carefully measured, including correlation coefficients and entropy values, which ranged from 7.89 to 7.99. Additionally, the algorithm's effectiveness was demonstrated through peak signal-to-noise ratio values, which spanned from 7.597 to 9.915, indicating the degree of similarity between the original and encrypted images. Furthermore, the number of pixels change rate values, ranging from 99.519241 to 99.609375, highlighted the algorithm's ability to produce significantly different encrypted images from the original. The unified average changing intensity values, falling between 35.72345678 and 35.78233456, further underscored the algorithm's proficiency in altering pixel intensities uniformly. Overall, this research offers a significant advancement in the field of image encryption, combining theoretical robustness with practical efficiency.

1 | INTRODUCTION

The protection of confidential information within digital images is achieved through image encryption, utilizing cryptographic techniques to prevent unauthorized access. Cryptography, an amalgamation of mathematics and computer science, has extensive applications in domains prioritizing information security. In the realm of digital image cryptography, meeting specific criteria is essential for ensuring data security. These criteria encompass concealing visual content by generating high entropy values, using a key space of sufficient size to resist brute force attacks, and demonstrating a significant level of security through key sensitivity analysis. Furthermore, successfully passing the differential attack test, while maintaining visual quality, is of utmost importance [1].

Image encryption schemes generally comprise two main stages: permutation and diffusion. With the increasing use and expansion of computer networks and the internet, ensuring robust network and computer data security has become imperative. Ensuring the utmost security for data against unauthorized usage and access is an essential and pressing issue. As a result, addressing security challenges becomes

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.
© 2024 The Author(s). *The Journal of Engineering* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

increasingly significant, and cryptography emerges as a widely adopted strategy to protect data. In essence, cryptography empowers secure communication between two parties across an insecure medium, ensuring that any potential intruder cannot eavesdrop on or comprehend the transmitted information. Encryption involves the concealment of essential information, rendering it unreadable and inaccessible even to individuals with specialized hacking knowledge. This vital procedure plays a pivotal role in preserving confidentiality, especially for private and personal communications. Cryptography serves as the means to secure and retain this information effectively.

The process of permutation safeguards visual information and diffusion introduces an avalanche effect by manipulating pixel values. Encryption systems that possess both robustness and security can be crafted by integrating cellular automata (CA) [1] with chaos theory [2]. CA, represented by evolving cell grids governed by specific rules, and chaotic systems, exhibiting seemingly random and unpredictable dynamics, collaborates seamlessly. This amalgamation results in intricate and unpredictable patterns, making it exceedingly arduous for adversaries to discern the original image from its encrypted counterpart. In recent times, CA and chaos theory have been employed in cryptographic image techniques. As an example, Khayyat et al. [3] introduced a blockchain-enabled approach known as shark smell optimization (SSO), applicable in Internet of Things (IoT) environments. Utilizing a combination of the Hopfield chaotic neural network (HCNN), a composite chaotic mapping, and the SSO technique, the SSO–HCNN cryptographic scheme establishes a robust encryption technique that utilizes both public and secret keys. During the diffusion phase, HCNN generates a self-diffusion chaotic matrix, and these keys are then employed in XOR operations with a scrambled image to produce the encrypted image.

The blockchain becomes the guardian of security and privacy by storing encrypted pixel values. Addressing this challenge, Li et al. [4] introduced an encryption technique that cleverly utilizes chaotic mappings and CA for image encryption. The 2D logistic-sine–coupling map and logistic-sine–cosine map are initiated with values obtained from the SHA-256 hash of the original image as the starting point of the process. Subsequently, diffusion takes place, and chaotic maps contribute to generating key matrices during the permutation phase. By arranging the elements in each row or column of these key matrices, index matrices are created, effectively scrambling the diffused image. This secure process culminates with the application of CA, yielding a cipher image that demonstrates remarkable resistance against various attack strategies. Incorporating, Dong et al. [5] achieved substantial advancements in enhancing the chaotic behaviour of the pseudo-random coupled map lattice method.

The resilience and efficiency of the proposed scheme underwent rigorous verification, including testing against differential and statistical attacks. In their work [6], Rupa et al. adopted a novel approach where they partition a large image into smaller, individual image segments. Following the permutation using CA rules, the components underwent a second-level transformation that included cross-pattern scanning and circular shift operations. The study by Lv et al. [7] employed balanced reversible Life-liked CA as a key component in their algorithm. Employing a classic confusion–diffusion structure at the block level, the proposed CA encrypted the blocks into noise-like patterns. In a separate work, Kafetzis et al. [8] utilized a customized Renyi chaotic map for designing a pseudo-random bit generator.

The continuous evolution of digital systems has emphasized the critical need for secure and efficient data handling mechanisms. Modern cryptographic approaches are being refined to combat sophisticated cyberattacks, particularly focusing on enhancing algorithmic resilience and ensuring data integrity. Recent advancements have introduced innovative encryption techniques designed to withstand potential security breaches, strengthening overall communication frameworks [9, 10]. Furthermore, the integration of optimization strategies and advanced computational models has significantly improved the performance and scalability of these algorithms in practical scenarios [11, 12]. These developments highlight the importance of adaptive and robust solutions in addressing the ever-growing challenges in cybersecurity and data processing [13, 14].

The discussed works introduce new methods for solid image encryption and authentication security of images during the transmission (Table 1). In Ref. [15], present a multi-image encryption method that integrates block compressive sensing with non-linear bifurcation diffusion, which does not only improve the efficiency of data representation through compressed sensing but also increases the security of the system against attacks through non-linear diffusion. In Ref. [16], present a multi-image encryption system based on quaternion discrete fractional Tchebyshev moment transform, using cross-coupling operations, which enhances the level of image security by multi-dimensional transforms. In Ref. [17], optical image encryption and authentication utilizes compression ghost imaging, thus creating an innovative system that provides simultaneous authentication and encryption solutions in an optical device. In the same vein, research studies featured in Refs. [18, 19] advanced watermarking and encryption techniques applied to optical images, improving the possibility of security and authentication. In Ref. [20], add to the number of multi-colour image encryption schemes by proposing a bit-level extension algorithm seeking to improve image protection against attacks.

This research was prompted by the issues of a steadily growing demand for the encryption of digital imaging and communications in medicine (DICOM) images and further medical images in the view of security dismantles. DICOM encryption today uses encryption methodologies that are not trusted and cannot be utilized in medical imaging due to the need to preserve image quality for diagnosis in the fore of varying levels of aggressiveness of the attack. Here, the challenges that have been left unaddressed in previous works are solved through the introduction of a new approach that incorporates the use of Laplace transforms (LTs) in the encryption and decryption processes of greyscale DICOM images. In this method, integrity of the image is retained as the encrypted image has been proven to be intact in the instance the clear-key

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Duodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 1 Survey of previous research works in encryption and decryption methods.

S. no.	Ref. no.	Years	Types of encryption and decryption methods	Features
1	[21]	2023	Light encryption for ROB and sophisticated encryption for ROI in multi-frame DICOM images	The method ensures shorter encryption times, offering significant time savings compared to Naïve encryption
2	[22]	2023	Double-bit unitary matrix scrambling with SVD and chaotic system diffusion	Reduces colour images to single greyscale ciphertext using asymmetric encryption, enhancing data privacy and security
3	[23]	2023	Deep learning techniques for image encryption and decryption	Leverages deep learning for encryption, resolution enhancement, detection, compression, key generation, and end-to-end protection of EHRs
4	[24]	2023	Chaos-based encryption, including symmetric, asymmetric, block ciphers, and stream ciphers	Investigates various chaos-based encryption techniques for securing images
5	[25]	2023	Annealing algorithm for image optimization based on entropy and pixel correlation	Emphasizes intricate texture feature creation through pixel randomization for enhanced security
6	[26]	2023	Chaotic maps and fuzzy numbers for encryption (decryption details unspecified)	High key sensitivity ensures security against various attacks by altering encrypted image significantly with small key changes
7	[27]	2023	2D logistic tent modular map with bit-level random permutation for stego images	Provides high embedding rates and reduced distortion, offering robust security against attacks
8	[28]	2023	Visual cryptography with HHO algorithm for determining colour levels	Ensures lower memory requirements and improved image quality while maintaining security
9	[29]	2023	Multiple layers of encryption with keys and S-boxes generated from various sources (decryption details unspecified)	Demonstrates resistance to attacks with impressive key space and encryption rate
10	[30]	2023	Fractal properties for image encryption with Henon map and CFF for diffusion	Demonstrates robustness against various attacks, including brute-force and differential attacks
11	[31]	2022	Optical image encryption with chaotic S-box and non-linear chaotic map	Uses chaotic sequences to enhance complexity and robustness in encryption
12	[32]	2021	CDG- and CBC-based encryption with EMD for ciphertext and key generation	Flexible encryption with various keys, focusing on encryption stability and effectiveness against attacks

Abbreviation: DICOM, digital imaging and communications in medicine.

is held at the correct way. The effect of the developed algorithm in this regard has been quantified through the use of various tests accompanied by performance analyses, statistical analyses, and various key parameters which include the mean correlation coefficients, the entropy, the peak signal-to-noise ratio (PSNR), the number of pixels change rate (NPCR), and unified average changing intensity (UACI), which have confirmed the success of the algorithm in enhancing the security while preserving the images. These findings significantly advanced secure methods of image encryption in the context of the healthcare sector.

2 | PROPOSED METHOD

The application of LTs extends across various domains, encompassing mathematics, computer science, physics, and electrical engineering. In image processing, LTs can be applied to enhance and analyse images in the frequency domain. Techniques like edge detection, image filtering, and image compression often involve LTs to manipulate images efficiently. In this study, a novel cryptographic scheme utilizing LT is introduced, offering numerous security transformations as needed, a crucial aspect in key alterations where the algorithm plays a vital role. This approach significantly impedes any attempts by malicious parties to trace the key through any means, making it highly challenging for adversaries. Moreover, the application of this scheme is further extended to MATLAB and artificial networks, opening up new possibilities for its utilization.

In this work, we experiment with our algorithm using DICOM images to evaluate its performance. DICOM images, also known as digital imaging and communications in medicine, are crucial elements in medical imaging. All these images conform to a particular standard that helps to link disparate medical imaging devices and systems. One of the most important elements is the additional metadata that is provided with each image file which includes patient demographics, imaging settings, type of modality, and time stamps. DICOM has many dimensions such as 2D, 3D, and even 4D for its volumetric and dynamic imaging. An equally important consideration is its integration with picture archiving and communication systems (PACS) that make it easier to store, retrieve and transfer medical information. Most of the DICOM files are encoded with lossless compression in order to retain the quality of images which is essential in accurate diagnosis. Annotations and overlays are also not woven into the original images to keep them clean.

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Duodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

ALGORITHM 1 Key generation in medical images using ASCII code

Step 1: Select the DICOM image.

Step 2: To check the DICOM image size 128 × 128 or 256 × 256 or convert the same without changing the pixel.

Step 3: DICOM image convert to pixel using MATLAB.

Step 4: Pixel value converts into ASCII code.

Step 5: Calculate the length of the message be n.

ALGORITHM 2 Encryption in medical images using Laplace transform

Step 1: Extract and convert message from DICOM image: First, retrieve a message from a DICOM (digital imaging and communications in medicine) image file. Then, using MATLAB, convert this message into its corresponding pixel representation, possibly by mapping the message text or values onto the pixel grid of the image.

Step 2: Define the plain text: Assume the plain text message is 'SUCCESS' (or any other chosen word). This message will be further encoded or processed.

Step 3: Assign numerical coefficients: Use each character of the plain text to generate numerical values (likely ASCII codes) and arrange these values as coefficients in a specific mathematical form, possibly a polynomial equation or series.

Step 4: Apply the Laplace transform: To analyse or transform the encoded information, use the Laplace transform on the polynomial or the function formed in the previous step. This can help convert the information into a different domain, often for easier manipulation or further processing.

Step 5: Retrieve ASCII values: Finally, to represent the encoded message, convert each processed part back into ASCII values. These ASCII values may then represent the final form of the message or data, prepared for further applications, storage, or analysis.

ALGORITHM 3 Decryption in medical images using inverse Laplace transform

Step 1: Consider the received encryption text and key from the sender.

Step 2: Convert the given cipher text to a corresponding finite sequence of numbers.

Step 3: To calculate key K_i.

Step 4: Use the inverse Laplace transform of the polynomial.

Step 5: Finally, we obtain the equivalent to 'SUCCESS'.

Together, these attributes make DICOM the most important technology in the present advanced medical imaging and health care systems.

This paper introduces a new cryptographic scheme utilizing the LT. The LT is employed for encrypting the plaintext, whereas its corresponding inverse transform facilitates decryption. Widely used in mathematics, physics, and electrical engineering, the LT converts a function of time into a function of complex frequency. The inverse LT, on the other hand, translates a complex frequency domain function back into the time domain. The proposed algorithm (Algorithms 1–3) offers multiple transformations to suit specific requirements, making it an advantageous feature for key changes. As a result, it becomes exceedingly challenging for any malicious attempt to trace the key through attacks. The application of this scheme extends to MATLAB and machine learning, artificial neural networks [33–36], providing further possibilities for its implementation. This approach instils a level of security that can effectively deter hackers from accessing sensitive information.

2.1 | Preliminaries

Plain text: This conveys a message that is comprehensible not only to the sender and recipient but also to anyone else who gains access to it.

Cipher text: The process of encoding a plain text message through a suitable scheme yields what is known as cipher text.

Encryption and decryption: Cipher text is obtained by transforming a plain text message through encryption, and decryption performs the reverse process, converting the cipher text message back into plain text.

LT: Given a function $f(t)$ defined for all positive values of t, the LT of $f(t)$ is defined as

$$L\left[f(t)\right] = F(s) = \int_0^\infty e^{-st} f(t)\, dt \tag{1}$$

Assuming the existence of the integral and the feasibility of computing the corresponding inverse LT is as follows:

$$L^{-1}\left[F(s)\right] = f(t) \tag{2}$$

The combination of LT encompasses both $f(t)$ and $F(s)$ as its elements.

Linearity property: According to the linearity property,

$$\text{if } L\left[f(t)\right] = F(s), \text{ then } L\left[af(t) + bg(t)\right] = aF(s) + bG(s) \tag{3}$$

Fundamental results derived via LT: Assume that the existence LT for all the functions discussed, this paper specifically includes elementary functions, covering both algebraic and transcendental functions:

$$1.\ L\left[t^n\right] = \frac{n!}{s^{n+1}} \tag{4}$$

$$2.\ L^{-1}\left\{\frac{n!}{s^{n+1}}\right\} = t^n \tag{5}$$

$$3.\ L\left[\cosh at\right] = \frac{a}{s^2 + a^2} \tag{6}$$

$$4.\ L^{-1}\left[\frac{a}{s^2 + a^2}\right] = \cosh a\, t \tag{7}$$

$$5.\ L\left[t^n f(t)\right] = \left(\frac{-d}{ds}\right)^n F(s) \tag{8}$$

$$6.\ L^{-1}\left[\left(\frac{-d}{ds}\right)^n F(s)\right] = t^n f(t) \tag{9}$$

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Daedeckin Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

2.2 | Encryption

The subsequent algorithm offers an understanding of the proposed cryptographic scheme.

The encryption method is outlined in the following:

Step 1: Extract the message from the DICOM image, convert it to pixels using MATLAB, and then transform it into ASCII code. Consider n as the length of the message.

Step 2: Consider the provided plain text as 'SUCCESS' with n equal to 7.

Based on the previous step, convert the plain text to ASCII code:

$$S-53\ U-55\ C-43\ \ C-43\ \ E-45\ S-53\ S-53 \tag{10}$$

Therefore, our plain text finite sequence is as follows:

$$T0=53, T1=55, T2=43, T3=43, T4=45, T5=53,$$
$$T6=53, TD=0 \text{ for } D>6 \tag{11}$$

Step 3: Expressing these numbers as coefficients in the form of $t\cosh(rt)$, where r is a constant.

The standard expansion is under consideration:

$$\cosh rt = 1+\frac{r^2t^2}{2!}+\frac{r^4t^4}{4!}+\frac{r^6t^6}{6!}+\frac{r^8t^8}{8!}+\frac{r^{10}t^{10}}{10!} + \cdots+\frac{r^{2k}t^{2k}}{k!}+\cdots=\sum_{k=0}^{\infty}\frac{r^{2k}t^{2k}}{2k!} \tag{12}$$

$$t\cosh rt = t+\frac{r^2t^3}{2!}+\frac{r^4t^5}{4!}+\frac{r^6t^7}{6!}+\frac{r^8t^9}{8!}+\frac{r^{10}t^{11}}{10!} + \cdots+\frac{r^{2k}t^{2k+1}}{k!}+\cdots=\sum_{k=0}^{\infty}\frac{r^{2k}t^{2k+1}}{2k!} \tag{13}$$

$$T_Dt\ \cosh 2t = T_0+T_1\frac{2^2t^3}{3!}+T_2\frac{2^4t^5}{4!}+T_3\frac{2^6t^7}{6!}+T_4\frac{2^8t^9}{8!} + T_5\frac{2^{10}t^{11}}{10!}+T_6\frac{2^{12}t^{13}}{12!}=\sum_{k=0}^{\infty}\frac{T_D2^{2k}t^{2k+1}}{2k!} \tag{14}$$

Let us consider $L(f\ (t))=T\ t\ \cosh 2t$

$$T_Dt\cosh 2t = 53t+55\frac{2^2t^3}{3!}+43\frac{2^4t^5}{4!}+43\frac{2^6t^7}{6!}+45\frac{2^8t^9}{8!} + 53\frac{2^{10}t^{11}}{10!}+53\frac{2^{12}t^{13}}{12!} \tag{15}$$

Step 4: Afterwards, compute the LT of the polynomial:

$$L[T_Dt\cosh 2t] = L\left[\frac{53}{s^2}+55\frac{2^23!}{2!s^4}+43\frac{2^45!}{4!s^6}+43\frac{2^67!}{6!s^8} + 45\frac{2^89!}{8!s^{10}}+53\frac{2^{10}11!}{10!s^{12}}+53\frac{2^{12}13!}{12!s^{14}}\right] \tag{16}$$

$$L\left[f\ (t)\right] = Tt\cosh 2t$$

$$L[T_Dt\cosh 2t] = L\left[53t+55\frac{2^2t^3}{2!}+43\frac{2^4t^5}{4!}+43\frac{2^6t^7}{6!} + 45\frac{2^8t^9}{8!}+53\frac{2^{10}t^{11}}{10!}+53\frac{2^{12}t^{13}}{12!}\right] \tag{17}$$

$$L[T_Dt\cosh 2t] = L\left[\frac{53}{s^2}+\frac{330}{s^4}+\frac{3440}{s^6}+\frac{19264}{s^8}+\frac{103680}{s^{10}} + \frac{596992}{s^{12}}+\frac{2822144}{s^{14}}\right] \tag{18}$$

Adjusting resultant values

$$53\ 330\ 3440\ \ 19,264\ \ 103680\ 596992\ 2822144$$

To *mod* 255 the given plain text string gets convert to cipher text string:

$$53\ 75\ 125\ \ 139\ \ 150\ 38\ 59$$

Encrypt the message by using the ASCII values of the given remainders:

Hence, the message 'SUCCESS' is encrypted as '5 k} ¨ *i* ˆ *u* %;'

Step 6: Next find K_i such that $K_i=\frac{(M_i-r_i)}{255}$ where $i=0,1,2,3,\ldots,n$, and any denominator can be chosen.

Thus key K_i is received as

$$0\ 1\ 13\ \ 75\ \ 406\ 2341\ 11067$$

Therefore, the cipher text is '5 k} ¨ *i* ˆ *u* %;' and the key is as follows:

$$0\ 1\ 13\ \ 75\ \ 406\ 2341\ 11067$$

2.3 | Decryption

The decryption process includes the following steps:

Step 1: The sender's encrypted text and key should be utilized as a consideration. In the provided example of the cipher text is '5 k} ¨ *i* ˆ *u* %;' and key is as follows:

$$0\ 1\ 13\ \ 75\ \ 406\ 2341\ 11067\ .$$

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Daodecin Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Step 2: Transform the provided cipher text into an associated finite sequence of numbers, that is

$$53\ 75\ 125\ 139\ 150\ 37\ 59$$

Let $T0 = 53, T1 = 75, T2 = 125, T3 = 139, T4 = 150, T5 = 37, T6 = 59$

Step 3: The given key K_i *for* $i = 0, 1, 2, \ldots n$ as

$$0\ 1\ 13\ 75\ 406\ 2341\ 11067\ .$$

Let $M_i = 255k_i + T_i$ for $i = 0, 1, 2, 3 \cdots$

$$53\ 330\ 3440\ 19264\ 103680\ 596992\ 2822144\ .$$

Now we consider

$$T t\cosh 2t = 53t + 55\frac{2^2t^3}{2!} + 43\frac{2^4t^5}{4!} + 43\frac{2^6t^7}{6!} + 45\frac{2^8t^9}{8!} + 53\frac{2^{10}t^{11}}{10!} + 53\frac{2^{12}t^{13}}{12!} \quad (19)$$

Taking inverse LT we get

$$T\left\{\frac{-ds}{ds}\right\}\ \frac{1}{(s^2 - 2^2)} = \sum_{i=0}^{\infty}\frac{q_i}{s^{2i+2}} = \frac{53}{s^2} + \frac{330}{s^4} + \frac{3440}{s^6} + \frac{19264}{s^8} + \frac{103680}{s^{10}} + \frac{596992}{s^{12}} + \frac{2822144}{s^{14}} \quad (20)$$

3 | EXPERIMENT RESULTS AND SECURITY ANALYSIS

The performance evaluation of the proposed scheme's encryption and decryption processes took place on a PC equipped with an Intel i7 processor and 8 GB of RAM, operating at 3.1 GHz. Both encryption and decryption techniques were developed using MATLAB. Experimenting with DICOM images selected from a publicly available dataset from imaging archive (TCIA) which consists of images with different classes of human body parts such as chest and breast of sizes 128×128 and 256×256, which included (a) brain, (b) skull, (c) retina, (d) teeth, (e) shoulder, (f) chest, (g) spinal cord, and (h) fingers, revealed that the encryption process required approximately 0.571781s, whereas decryption took around 0.579308s. Figure 1 visually demonstrates the results, confirming the effectiveness of our encryption method.

3.1 | Comparative study

To evaluate the efficacy of the proposed method, we undertake a statistical analysis in this section. To start with, we showcase histograms of DICOM images, contrasting the original images with their encrypted images. Next, we analyse the correlation between neighbouring pixels, the objective of comprehending the attained level of local pixel dependence in the outcomes.

TABLE 2 Correlation coefficient values.

Image	NCC
Brain	-2.03×10^{-4}
Skull	-1.84×10^{-5}
Retina	-1.69×10^{-3}
Teeth	-1.03×10^{-4}
Shoulder	-3.31×10^{-5}
Chest	-2.51×10^{-4}
Spinal cord	-1.43×10^{-3}
Fingers	-2.71×10^{-1}

Abbreviation: NCC, normalized cross-correlation.

3.1.1 | Analysing histograms

Histogram analysis is utilized to demonstrate the encryption algorithm's superior substitution and diffusion properties. We have conducted histogram analysis on various encrypted images obtained from the mentioned approaches and their respective plain images. Figure 2 illustrates one such example of histogram analysis. The relatively uniform distributions observed in encrypted image histograms indicate the method's high quality. Consequently, the encrypted images do not reveal any statistical clues, making statistical attacks challenging for the discussed approaches.

3.1.2 | Correlation analysis

Equation (1) showcases the 2D normalized cross-correlation, or correlation coefficient, utilized to gauge the similarity between two images, $A(x, y)$ and $B(x, y)$:

$$NCC = \frac{\sum_{x,y}\left(A(x,y) - \bar{A}\right)\left(B(x,y) - \bar{B}\right)}{\sqrt{\left(\sum_{x,y}\left(A(x,y) - \bar{A}\right)^2\right)\left(\sum_{x,y}\left(B(x,y) - \bar{B}\right)^2\right)}} \quad (21)$$

where symbolizing the mean intensity values of images A and B as μA and μB, respectively. Consequently, normalized within the interval of $[-1, +1]$, the 2D correlation coefficient showcases a maximum negative correlation at -1 and a maximum positive correlation at $+1$, and the original image and its encryption exhibit no association when the value is 0. The correlation coefficient obtained between the plain and ciphered image is shown in Figure 3. The obtained correlation coefficient values are shown in the Table 2.

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Duodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

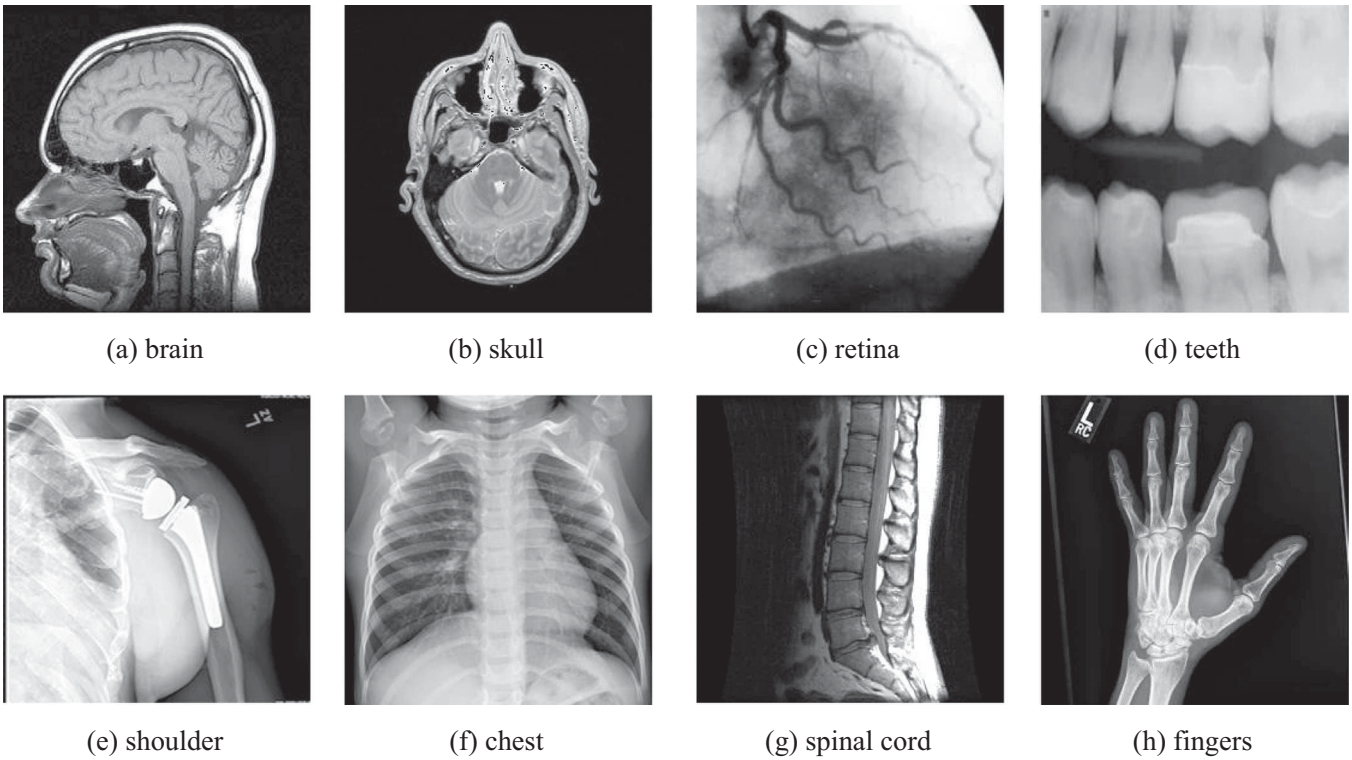


FIGURE 1 Sample images used in our work.

3.1.3 | Entropy analysis

The level of disorder in a system is commonly evaluated through the use of entropy, a commonly employed metric. In the context of cryptography, entropy is utilized to gauge the level of randomness inherent in an encrypted message. The unit of information entropy is typically expressed in bits.

The following equation allows us to define the entropy H_q of an information source q:

$$H_q = \sum_{k=0}^{R-1} p\left(q_k\right) \log_2 \frac{1}{p\left(q_k\right)} \tag{22}$$

where R represents the total number of symbols q_k in source q, whereas the probability of each symbol q_k occurring is determined by $p(q_k)$. When considering an image with 8 bits for the grey channel, there are 256 possible symbols.

Table 3 illustrates the entropy measurements of the ciphered images contained in the dataset. Among them, the image labelled shoulder as displayed the minimum value of entropy; conversely, the chest image resulted in the maximum value of entropy.

TABLE 3 The entropy values obtained from the encrypted images.

Image	H_q
Brain	7.99934567
Skull	7.99945672
Retina	7.99967821
Teeth	7.99931245
Shoulder	7.89923456
Chest	7.99984567
Spinal cord	7.89956342
Fingers	7.99967896

3.2 | Encryption quality

As visual inspection of encrypted images relies on subjective judgement, several literature sources have proposed quantitative metrics to evaluate encryption quality. These metrics quantify the pixel value deviations between the plain image and its encrypted form [37].

Therefore, accomplishing a substantial level of maximum and irregular pixel discrepancies or modifications between the plaintext and encrypted image indicates satisfactory encryption quality. In reference [37], four encryption quality metrics were defined to precisely measure and evaluate this aspect.

3.2.1 | Maximum deviation

Equation (23) from Ref. [37] is employed to calculate the maximum deviation (MD) specifically for 8-bit greyscale images.

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Duodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

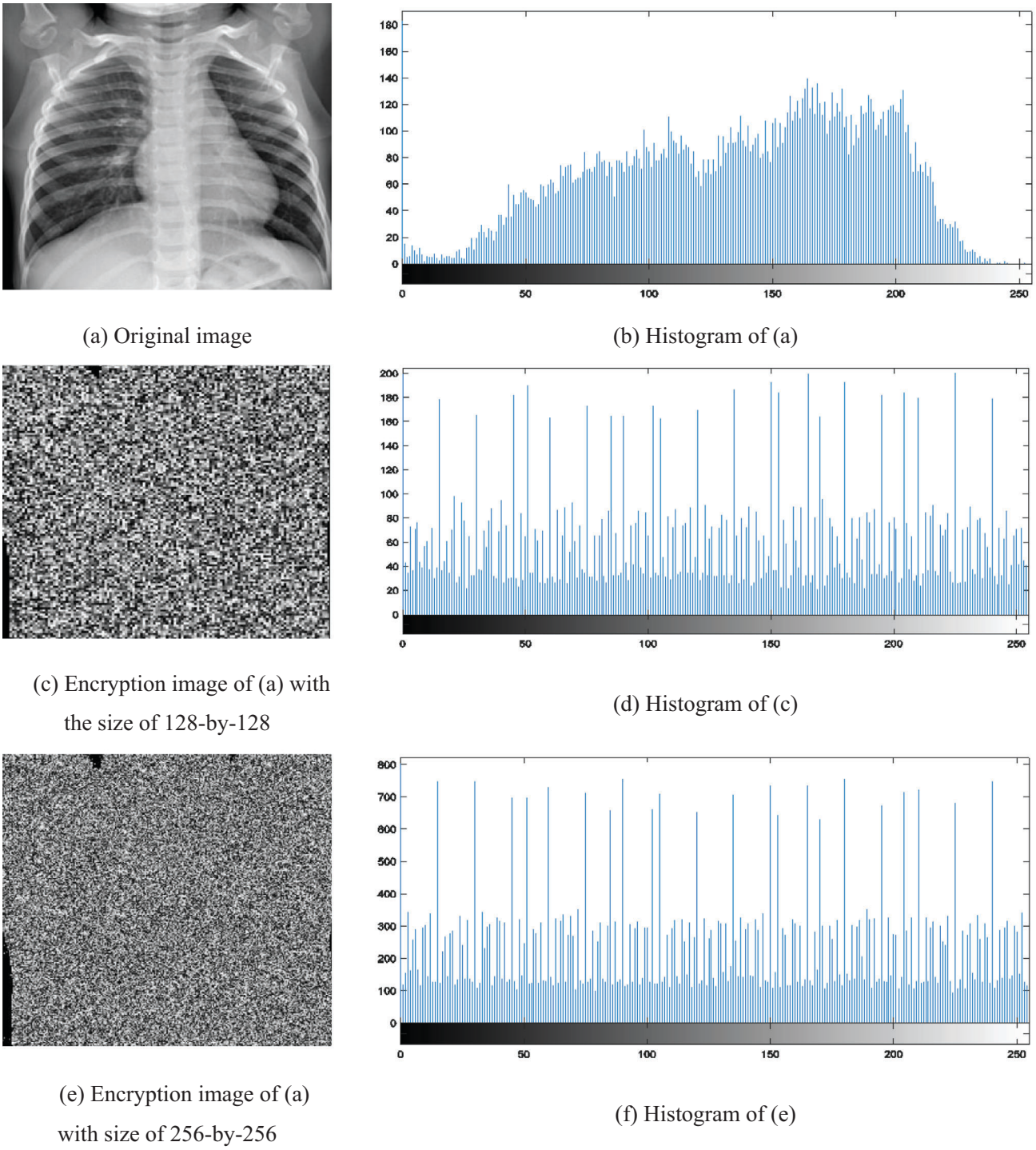


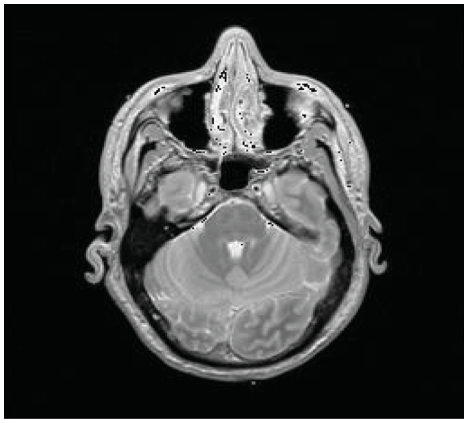
FIGURE 2 Histogram analysis of the original image (b) and encrypted images in 128-by-128 and 256-by-256 dimensions.

This equation serves as a crucial tool in determining the MD value, which is a significant metric for evaluating encryption quality:

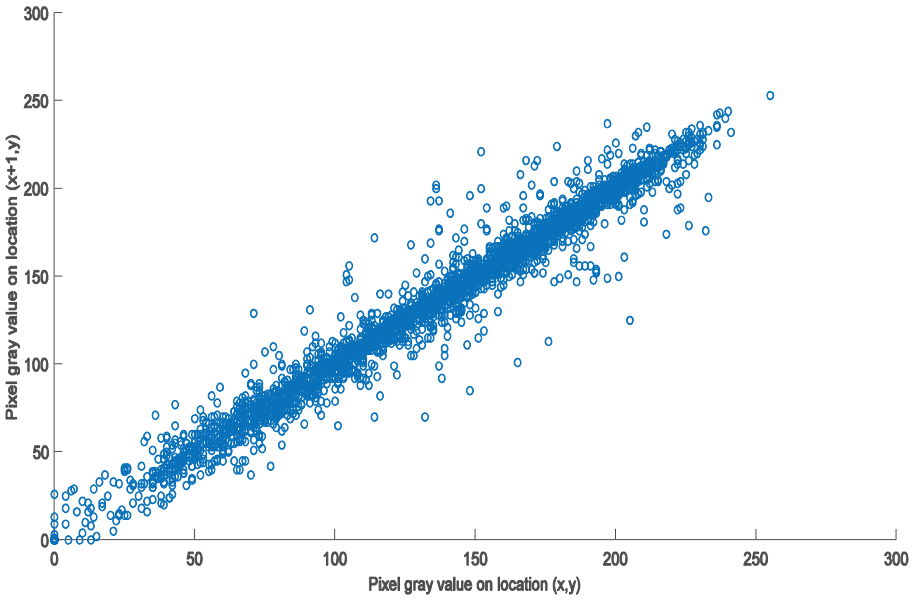
$$MD = \frac{d\,(0) + d\,(255)}{2} + \sum_{k=1}^{254} d\,(k) \tag{23}$$

The absolute contrast between the histograms of the original and encrypted images, denoted as d, is utilized in the calculation. The difference in values of these histograms at intensity level k is specifically expressed as $d(k)$. The histograms at grey levels 0 and 255 are represented by the values $d(0)$ and $d(255)$, respectively. When the MD values are higher, it indicates that

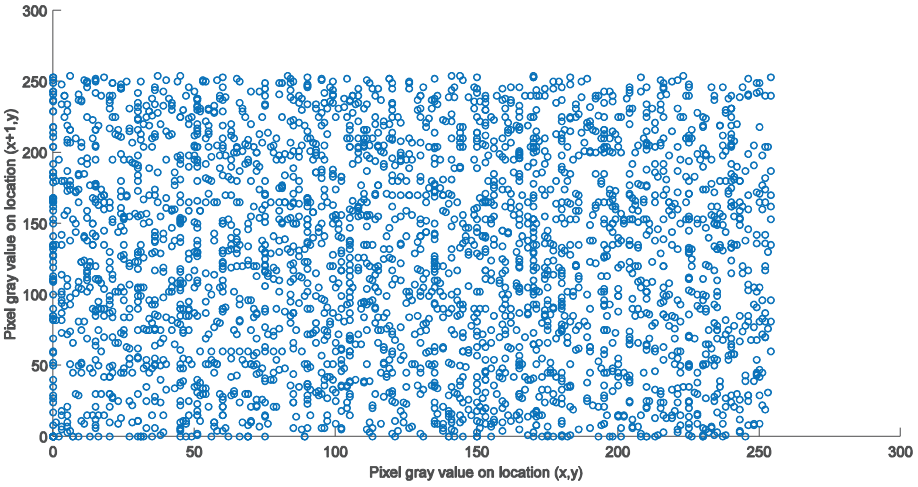
20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Duodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License



(a) brain



(b) correlation of (a)



(c) correlation of the encrypted image

FIGURE 3 Brain image and correlation of encrypted image.

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Duodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

the encrypted images have deviated more significantly from the original images.

3.2.2 | Irregular deviation

The encryption quality is measured using the irregular deviation (*ID*) metric, which assumes that the initial pixel values should be consistently randomized by an effective encryption technique. An analysis is performed on the distance between the histogram variance distribution and a uniform distribution to assess the effectiveness of the encryption algorithm.

To begin with, the absolute difference (*AD*) is determined by comparing the pixel values of the plain image (*A*) and the encrypted image (*B*):

$$AD = |A - B| \tag{24}$$

Subsequently, the histogram of the absolute difference (*AD*), denoted as h, is derived. Here, M_h is the average value of the histogram as stated by Equation (5), and $h(k)$ signifies the histogram result at index k:

$$M_h = \frac{1}{256} + \sum_{k=0}^{255} h(k) \tag{25}$$

Subsequently, the following equation, which is used to find the irregular deviance for an 8-bit image, is employed:

$$ID = \sum_{k=0}^{255} |h(k) - M_h| . \tag{26}$$

Improved encryption quality is attained when using smaller values of ID.

3.2.3 | Compared to the uniform histogram

A current encryption level factor is provided in Ref. [38], focusing on measuring the difference between the histogram of the encrypted image and both the ideal and uniform histograms.

The histogram of the encrypted image *B* is represented by h_B, with $h_B(k)$ denoting the frequency of occurrence at grey level k. The mean value of grey value k in a uniform histogram, as defined in Equation (22) for $L = 256$, is also known as $E(k)$. Using the following equation, a difference from the uniform histogram (*DU*) is obtained:

$$DU = \frac{1}{M \times N} \sum_{k=0}^{255} |h_B(k) - E(k)| \tag{27}$$

3.2.4 | Peak signal-to-noise ratio (PSNR)

The *PSNR* is a metric that provides a means to analysing the quality of the encrypted image. By measuring the pixel value variations between an original 8-bit image *A* and its encrypted representation *B*, *PSNR* can be mathematically defined using the following equation:

$$PSNR = 10\log_{10}\left(\frac{255^2}{\frac{1}{M\times N}\sum_{x,y}(A(x,y) - CB(x,y))^2}\right) \tag{28}$$

A lower *PSNR* value corresponds to a better encryption quality.

TABLE 4 The dataset's results for encryption quality.

Image	MD	ID	DU	PSNR	MSE
Brain	241,516.4	264,427.2	0.033	7.597	7574.4
Skull	126,741.6	339,738.1	0.032	8.685	7558.5
Retina	203,552.2	438,743.1	0.035	9.734	8446.2
Teeth	454,521.1	249,323.1	0.032	9.854	5747.4
Shoulder	321,632.6	225,323.2	0.033	9.915	7250.2
Chest	341,231.5	236,339.3	0.034	9.495	6337.2
Spinal cord	234,621.7	248,373.2	0.034	8.415	8451.2
Fingers	341,252.1	242,323.6	0.034	7.882	7770.3

3.2.5 | Mean square error (MSE)

Furthermore, the mean square error (MSE) serves as a prevalent statistical metric for evaluating the quality of an encryption technique [39, 40]. It determines the average squared differences between the pixels of the original image *A* and the encrypted image *B*, as indicated by the following equation:

$$MSE = \frac{1}{M \times N} \sum_{x,y} (A(x,y) - CB(x,y))^2 \tag{29}$$

Lower values of *MSE* correspond to improved encryption qualities, similar to the *PSNR*.

Outcomes of the dataset's quality metrics for encryption, averaged across each colour channel, are presented in Table 4.

3.3 | Texture analysis

The frequency of various combinations of grey levels within a certain spatial region or across the entire image is determined employing several kinds of techniques to evaluate texture [39]. In the case of greyscale images, a widely used measure called the grey-level co-occurrence matrix (*GLCM*) takes into account the spatial relationships between the pixels, considering elements like $A(x, y)$ [40]. The calculation of the grey-level *GLCM* in the following equation is based on the frequency of the correlation between a pixel of value p and another pixel with an intensity

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Daodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

value of q:

$$C_M(x,y) = C_{\Delta x,\Delta y}(p,q) = \sum_{x=1}^{N}\sum_{y=1}^{M}\begin{cases}1, & if\ A(x,y)=p \text{ and } A(x+\Delta x, y+\Delta y)=q\\ 0, & \text{otherwise}\end{cases} \tag{30}$$

where $C_{\Delta x,\Delta y}(i,j)$ denotes the frequency of occurrence for two pixels with intensities p and q, at a specific separation $(\Delta x, \Delta y)$.

3.3.1 | Homogeneity

In texture analysis, homogeneity is a metric that measures the proximity of pixel distribution and how closely the pixels are positioned to one another. The following equation outlines the mathematical expression for calculating *Homogeneity*:

$$Homogeneity = \sum_{x,y}\frac{G_M(x,y)}{1+|x-y|'} \tag{31}$$

where GM denotes the grey-level $GLCM$ in the given context. A higher level of encryption quality is associated with lower values of Homogeneity.

3.3.2 | Contrast

The *Contrast* metric, which is calculated according to the following equation [41], assesses the intensity contrast within a pixel's surrounding neighbourhood. It is desired to have the *Contrast* value as high as possible:

$$Contrast = \sum_{x,y}|x-y|^2 G_M(x,y) \tag{32}$$

3.3.3 | Energy

The following equation provides the calculation for *Energy*, a metric used to measure uniformity in the grey-level $GLCM$. A smaller *Energy* value indicates a higher degree of disorder:

$$Energy = \sum_{x,y} G_M(x,y)^2 \tag{33}$$

A higher level of encryption quality is associated with lower values of *Energy*.

Table 5 exhibits the computed results for the three GLCM metrics on the dataset (homogeneity, contrast, and energy), along with the average values obtained for each colour channel.

TABLE 5 The outcomes of texture analysis from our dataset.

Image	Homogeneity	Contrast	Energy
Brain	0.378633	11.656	0.0246591
Skull	0.378543	11.658	0.0246590
Retina	0.378563	11.669	0.0246391
Teeth	0.378404	11.373	0.0246489
Shoulder	0.378491	11.487	0.0246385
Chest	0.378502	11.693	0.0246487
Spinal cord	0.378613	11.829	0.0246497
Fingers	0.378754	11.340	0.0246390

TABLE 6 The dataset yields results for NPCR and UACI.

Image	NPCR	UACI
Brain	99.533451	35.74345674
Skull	99.519241	35.72345678
Retina	99.554766	35.75234567
Teeth	99.576081	35.76245634
Shoulder	99.597396	35.77234567
Chest	99.609375	35.78233456
Spinal cord	99.583186	35.76345467
Fingers	99.568976	35.75353678

Abbreviations: NPCR, number of pixels change rate; UACI, unified average changing intensity.

3.4 | Differential attack

Evaluating the robustness of an encryption system against differential attacks often involves utilizing two prevalent metrics: NPCR and UACI [38].

By utilizing the following equations, we can determine the $NPCR$ and $UACI$ of two single-band images $A(x,y)$ and $B(x,y)$ with dimensions $M \times N$:

$$NPCR = \frac{\sum_{x=1}^{N}\sum_{y=1}^{M} D(x,y)}{M \times N} \times 100 \tag{34}$$

where

$$D(x,y) = \begin{cases}0, & \text{if } A(x,y) - B(x,y) = 0\\ 1, & \text{in any other case}\end{cases}$$

and

$$UACI = \frac{\sum_{x=1}^{N}\sum_{y=1}^{M}|A(x,y) - B(x,y)|}{255\,(M \times N)} \times 100 \tag{35}$$

According to Ref. [32], when the encryption of two nearly identical images yields resulting images with an $NPCR$ approaching 100% and an $UACI$ exceeding 35%, it indicates a robust encryption scheme. This is attributed to the fact that even a minor alteration in the input of the technique leads to a

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipe2.70038 by Daedeecin Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

TABLE 7 Contrast of encryption time complexities in various methods.

Method	Architecture	RAM (GB)	Platform	Size image (px)	Time (s)
[5]	Intel Core i7 3.4 GHz	16	MATLAB	512 × 512	0.0134
[42]	ARMv8 1.2 GHz	1	Python	512 × 512	–
[43]	Intel Core i5 3.2 GHz	8	MATLAB	512 × 512 × 3	–
[44]	Intel Pentium-B960 2.2 GHz	2	–	512 × 512	3.007
[45]	AMD Ryzen 5 2.1 GHz	12	MATLAB	512 × 512 × 3	4.360
Proposal	Intel Core i7 3.4 GHz	8	MATLAB	512 × 512	3.257

significantly distinct output, thus substantiating the strength of the encryption scheme.

We began by selecting an *RGB* picture, denoted as A. Next, we randomly chose a pixel from one of the colour channels and modified its least significant bit, resulting in an altered image labelled B. Both A and B were subsequently encrypted using identical parameters. To assess the similarity between the encrypted images, we calculated the mean *NPCR* and *UACI* values for their respective colour channels.

To evaluate the performance of our algorithm comprehensively, we conducted 100 iterations on each picture in our dataset. The parameters mentioned in Section 3.1 were consistently applied throughout these tests. The resulting average values for each picture are presented in Table 6.

3.5 | Computational complexity

In the context of an $M \times N$ RGB image, the computational complexities of the three operations are as follows:

- Deterministic noise and cyclic permutation: $O(M \times N)$.
- Multiscale derivative dynamic (MDD) with a degree D: $O(M \times N \times D)$, where D represents the derivative's degree used in MDD.
- LT: a function $f(t)$ defined for all positive values of t.
- In conclusion, the computational complexity of our proposed method can be expressed as $O(3 \times M \times N + M \times N \times D + S)$, which simplifies to $O(M \times N \times D + S)$.

4 | COMPARISON STUDY

This work also conducted a comparative analysis between our proposed encryption algorithm and five recent works that share a foundation on chaotic systems and CA. Dong et al. [5] employed hybrid elementary CA, comprising a fusion of two global rules from a hybrid ECA, to enhance the chaotic behaviour of the Chirikov standard map-based pseudo-random coupled map lattice model. Sun et al. [41] presented the IESCA algorithm, which utilizes 2D Moore CA, specifically designed for resource-constrained IoT devices. The algorithm employs local transformations that depend on the bit states of the cellular automaton's neighbours to generate random chaotic sequences. The study explores two variants of the algorithm: one with a periodic boundary for the neighbourhood and the other with a null boundary. By investigating these versions, they aimed to understand the impact of boundary conditions on the algorithm's behaviour and performance in the context of IoT applications. The findings provide valuable insights into the suitability of the proposed approach for resource-limited devices in chaotic system-based cryptographic applications. Li et al. [22] proposed a lossless image encryption method that combines set partitioning in hierarchical trees, CA, and various chaotic systems. This innovative approach aims to enhance the security and robustness of image encryption by leveraging the unique properties of these three techniques.

Tables 7 compares the metrics of our method with other algorithms, including LT, entropy, MSE, PSNR, NPCR, UACI, key space, and encryption time. The results show that our proposed scheme is competitive with recent works in the literature, affirming its effectiveness in secure image encryption. Furthermore, our method demonstrates promising potential for various practical applications.

5 | CONCLUSION

This study introduces an innovative greyscale DICOM image encryption and decryption algorithm utilizing LT and a deterministic noise technique. The proposed method effectively enhances security while ensuring efficient concealment of visual information. The algorithm exhibits exceptional performance in key areas, including encryption quality, computational efficiency, and resilience against differential attacks. The use of LT ensures lossless recovery of the original image when the correct key is used, addressing key concerns in secure image transmission. Through comprehensive statistical analysis and testing, the effectiveness of the proposed algorithm has been rigorously validated, with strong results in various performance metrics. The algorithm demonstrates high entropy values ranging from 7.99 to 8.99, indicating excellent randomness in the encrypted images. PSNR values between 8.254 and 9.952 show minimal distortion, reflecting the algorithm's ability to maintain image quality. Additionally, the NPCR values, ranging from 99.519241% to 99.609375%, and UACI values between 35.72345678% and 35.78233456%, underscore the algorithm's ability to generate significantly altered encrypted images. The encryption time is also competitive compared to

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Daodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

existing methods, further highlighting the efficiency of the proposed technique.

This research contributes a novel greyscale DICOM image encryption and decryption algorithm that leverages LT and deterministic noise techniques. It offers a secure, efficient, and lossless encryption solution for sensitive medical imaging data, ensuring high encryption quality and robustness against attacks. The proposed method stands out for its high performance in key metrics, making it a valuable advancement in the field of secure image communication and data privacy. In future, the researchers may also focus on incorporating hybrid machine learning and blockchain-based mechanisms [46–51] for image security.

AUTHOR CONTRIBUTIONS

S. Thalapathiraj: Conceptualization; methodology. **J. Arunnehru**: Conceptualization; methodology. **V. C. Bharathi**: Data curation; software. **R. Dhanasekar**: Data curation; software. **L. Vijayaraja**: Formal analysis; writing—review and editing. **Muhammad Faheem**: Data curation; data validation; testing; writing—review and editing. **Arfat Ahmad Khan**: Investigation; writing—review and editing. **R. Kannadasan**: Writing—review and editing.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

R. Kannadasan https://orcid.org/0000-0001-7622-8261
Muhammad Faheem https://orcid.org/0000-0003-4628-4486

REFERENCES

1. Romero-Arellano, A., Moya-Albor, E., Brieva, J., Cruz-Aceves, I., Avina-Cervantes, J.G., Hernandez-Gonzalez, M.A., Lopez- Montero, L.M.: Image encryption and decryption system through a hybrid approach using the jigsaw transform and Langton's ant applied to retinal fundus images. Axioms 10, 215 (2021)
2. Kanso, A., Ghebleh, M.: An efficient and robust image encryption scheme for medical applications. Commun. Nonlinear Sci. Numer. Simul. 24, 98–116 (2015)
3. Khayyat, M., Khayyat, M., Abdel-Khalek, S., Mansour, R.: Blockchain enabled optimal Hopfield chaotic neural network based secure encryption technique for industrial internet of things environment. Alex. Eng. J. 61, 11377–11389 (2022)
4. Li, L., Luo, Y., Qiu, S., Ouyang, X., Cao, L., Tang, S.: Image encryption using chaotic map and cellular automata. Multimed. Tools Appl. 81, 40755–40773 (2022)
5. Dong, Y., Zhao, G., Ma, Y., Pan, Z., Wu, R.: A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata. Inf. Sci. 593, 121–154 (2022)
6. Rupa, I., Manideep, K., Kamale, N., Suhasini, S.: Information security using chaotic encryption and decryption of digital images. In Proceedings of the 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 15–16 July (2022)
7. Lv, W., Chen, J., Chai, X., Fu, C.: A robustness-improved image encryption scheme utilizing Life-liked cellular automaton. Nonlinear Dyn. 111, 3887–3907 (2022)
8. Kafetzis, I., Moysis, L., Volos, C., Nistazakis, H., Munoz-Pacheco, J., Stouboulos, I.: Automata-derived chaotic image encryption scheme. In: Proceedings of the 2022 11th International Conference on Modern Circuits and Systems Technologies (MOCAST), Bremen, Germany, 8–10 June (2022)
9. Alexan, W., Gabr, M., Mamdouh, E., Elias, R., Aboshousha, A.: Color image cryptosystem based on sine chaotic map, 4d Chen hyperchaotic map of fractional-order and hybrid DNA coding. IEEE Access 11, 54928–54956 (2023)
10. Gabr, M., Elias, R., Hosny, K.M., Papakostas, G.A., Alexan, W.: Image encryption via base-n PRNGs and parallel base-n S-boxes. IEEE Access 11, 85002–85030 (2023)
11. Gabr, M., Korayem, Y., Chen, Y.L., Yee, L., Ku, C.S., Alexan, W.: R 3—Rescale, rotate, and randomize: A novel image cryptosystem utilizing chaotic and hyper-chaotic systems. IEEE Access 11, 119284–119312 (2023)
12. Alexan, W., Korayem, Y., Gabr, M., El-Aasser, M., Maher, E.A., El-Damak, D., Aboshousha, A.: Anteater: When Arnold's cat meets Langton's ant to encrypt images. IEEE Access 11, 106249–106276, (2023)
13. Alexan, W., El-Damak, D., Gabr, M.: Image encryption based on fourier-DNA coding for hyperchaotic Chen system, Chen-based binary quantization S-box, and variable-base modulo operation. IEEE Access 12, 21092–21113, (2024)
14. Alexan, W., Aly, L., Korayem, Y., Gabr, M., El-Damak, D., Fathy, A., Mansour, H.A.: Secure communication of military reconnaissance images over UAV-assisted relay networks. IEEE Access 12, 78589–78610, (2024)
15. Hu, L.L., Chen, M.X., Wang, M.M., Zhou, N.R.: A multi-image encryption scheme based on block compressive sensing and nonlinear bifurcation diffusion. Chaos Solitons Fractals 188, 115521 (2024)
16. Zhou, N.R., Tong, L.J., Zou, W.P.: Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation. Signal Process. 211, 109107 (2023)
17. Hu, J.L., Chen, M.X., Zhou, S., Zhou, N.R.: Optical image authentication and encryption scheme with computational ghost imaging. J. Franklin Inst. 361(17), 107203 (2024)
18. Gong, L.H., Luo, H.X.: Dual color images watermarking scheme with geometric correction based on quaternion FrOOFMMs and LS-SVR. Opt. Laser Technol. 167, 109665 (2023)
19. Guo, Z., Chen, S.H., Zhou, L., Gong, L.H.: Optical image encryption and authentication scheme with computational ghost imaging. Appl. Math. Modell. 131, 49–66 (2024)
20. Zhou, N.R., Hu, L.L., Huang, Z.W., Wang, M.M., Luo, G.S.: Novel multiple color images encryption and decryption scheme based on a bit-level extension algorithm. Expert Syst. Appl. 238, 122052 (2024)
21. Natsheh, Q., Salagean, A., Zhou, D., Edirisinghe, E.: Automatic selective encryption of DICOM Images. Appl. Sci. 13, 4779 (2023). https://doi.org/10.3390/app13084779
22. Li, M., Fang, X., Ernest, A.: A color image encryption method based on dynamic selection chaotic system and singular value decomposition. Mathematics 11, 3274 (2023). https://doi.org/10.3390/math11153274
23. Lata, K., Cenkeramaddi, L.R.: Deep learning for medical image cryptography: A comprehensive review. Appl. Sci. 13, 8295 (2023). https://doi.org/10.3390/app13148295
24. Zhang, B., Liu, L.: Chaos-based image encryption: Review, application, and challenges. Mathematics 11, 2585 (2023). https://doi.org/10.3390/math11112585
25. Zhang, T., Zhu, B., Ma, Y., Zhou, X.: A Novel image encryption algorithm based on multiple random DNA coding and annealing. Electronics 12, 501 (2023). https://doi.org/10.3390/electronics12030501
26. Mfungo, D.E., Fu, X., Xian, Y., Wang, X.: A novel image encryption scheme using chaotic maps and fuzzy numbers for secure transmission of information. Appl. Sci. 13, 7113 (2023). https://doi.org/10.3390/app13127113

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.70038 by Duodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

27. Lan, C.-F., Wang, C.-M., Lin, W.: A novel adaptive image data hiding and encryption scheme using constructive image abstraction. Appl. Sci. 13, 6208 (2023). https://doi.org/10.3390/app13106208
28. Ibrahim, D., Sihwail, R., Arrifin, K.A.Z., Abuthawabeh, A., Mizher, M.: A novel color visual cryptography approach based on Harris Hawks optimization algorithm. Symmetry 15, 1305 (2023). https://doi.org/10.3390/sym15071305
29. Alexan, W., Alexan, N., Gabr, M.: Multiple-layer image encryption utilizing fractional-order Chen hyperchaotic map and cryptographically secure PRNGs. Fractal Fract. 7, 287 (2023). https://doi.org/10.3390/fractalfract7040287
30. Agarwal, S.: A new composite fractal function and its application in image encryption. J. Imaging 6, 70 (2020). https://doi.org/10.3390/jimaging6070070
31. Tian, P., Su, R.: A novel virtual optical image encryption scheme created by combining chaotic S-box with double random phase encoding. Sensors 22, 5325 (2022). https://doi.org/10.3390/s22145325
32. Li, W., Yan, A., Zhang, H.: Novel multiple-image encryption scheme based on coherent beam combining and equal modulus decomposition. Appl. Sci. 11, 9310 (2021). https://doi.org/10.3390/app11199310
33. Arunnehru, J., Chamundeeswari, G., Bharathi, S.P.: Human action recognition using 3D convolutional neural networks with 3D motion cuboids in surveillance videos. Procedia Comput. Sci. 133, 471–477 (2018)
34. Arunnehru, J., Kalaiselvi Geetha, M.: Difference intensity distance group pattern for recognizing actions in video using support vector machines. Pattern Recognit Image Anal. 26, 688–696 (2016)
35. Arunnehru, J., Thalapathiraj, S., Dhanasekar, R., Vijayaraja, L., Kannadasan, R., Khan, A.A., Haq, M.A., Alshehri, M., Alwanain, M.I., Keshta, I.: Machine vision-based human action recognition using spatio-temporal motion features (STMF) with difference intensity distance group pattern (DIDGP). Electronics 11(15), 2363 (2022)
36. Arunnehru, J., Nandhana Davi, A.K., Sharan, R.R., Nambiar, P.G.: Human pose estimation and activity classification using machine learning approach. In: InSoft Computing and Signal Processing: Proceedings of 2nd ICSCSP 2019 2 2020, pp. 113–123. Springer, Singapore (2020)
37. Ahmad, J., Ahmed, F.: Efficiency analysis and security evaluation of image encryption schemes. Int. J. Video Image Process. Netw. Secur. 12, 18–31 (2012)
38. Stoyanov, B., Kordov, K.: Image encryption using chebyshev map and rotation equation. Entropy 17, 2117–2139 (2015)
39. Nazir, H., Bajwa, I.S., Abdullah, S., Kazmi, R., Samiullah, M.: A color image encryption scheme combining hyperchaos and genetic codes. IEEE Access 10, 14480–14495 (2022)
40. Haralick, R.M., Dinstein, I., Shanmugam, K.: Textural features for image classification. IEEE Trans. Syst. Man Cybern. SMC-3, 610–621 (1973)
41. Sun, S., Guo, Y.: A new hyperchaotic image encryption algorithm based on stochastic signals. IEEE Access 9, 144035–144045 (2021)
42. Roy, S., Shrivastava, M., Rawat, U., Pandey, C., Nayak, S.: IESCA: An efficient image encryption scheme using 2D cellular automata. J. Inf. Secur. Appl. 61, 102919 (2021)
43. Zhang, H., Wang, X.Q., Sun, Y.J., Wang, X.Y.: A novel method for lossless image compression and encryption based on LWT, SPIHT and cellular automata. Signal Process. Image Commun. 84, 115829 (2020)
44. Mondal, B., Sing, S., Kumar, P.: A secure image encryption scheme based on cellular automata and chaotic skew tent map. J. Inf. Secur. Appl. 45, 117–130 (2019)
45. Moya-Albor, E., Romero-Arellano, A., Brieva, J., Gomez-Coronel, S.L.: Color image encryption algorithm based on a chaotic model using the modular discrete derivative and Langton's ant. Mathematics 11, 2396 (2023)
46. Faheem, M., Raza, B., Bhutta, M.S., Madni, S.H.H.: A blockchain-based resilient andsecure framework for events monitoring and control indistributed renewable energy systems. IET Blockchain 1–15 (2024). https://doi.org/10.1049/blc2.12081
47. Raza, B., et al.: Autonomic performance prediction framework for data warehouse queries using lazy learning approach. Appl. Soft Comput. 91, 106216 (2020). https://doi.org/10.1016/j.asoc.2020.106216
48. Khan, A.A., et al.: D2PAM:epileptic seizures prediction using adversarial deep dualpatch attention mechanism. CAAI Trans. Intell. Technol. 8(3), 755–769 (2023). https://doi.org/10.1049/cit2.12261
49. Faheem, M., et al.: Cyberattack patterns in blockchain-based communication networks for distributed renewable energy systems: a study on big datasets. Data in Brief 53(5), 110212 (2024). https://doi.org/10.1016/j.dib.2024.110212
50. Raza, B., et al.: Performance prediction and adaptation for database management system workload using case-based reasoning approach. Inf. Syst. 76(5), 46–58 (2018). https://doi.org/10.1016/j.is.2018.04.005
51. Faheem, M., Mahmoud Ahmad, A.-K.: Multilayer cyberattacks identification and classification using machine learning in internet of blockchain (IoBC)-based energy networks. Data in Brief 54(5), 110461 (2024). https://doi.org/10.1016/j.dib.2024.110461

How to cite this article: Thalapathiraj, S., Arunnehru, J., Bharathi, V.C., Dhanasekar, R., Vijayaraja, L., Kannadasan, R., Faheem, M., Khan, A.A.: A novel approach for encryption and decryption of digital imaging and communications using mathematical modelling in internet of medical things. J. Eng. 2024, e70038 (2024). https://doi.org/10.1049/tje2.70038

20513305, 2024, 12, Downloaded from https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/tje2.70038 by Duodecim Medical Publications Ltd, Wiley Online Library on [26/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License