

Article

Novel Integer Shmaliy Transform and New Multiparametric Piecewise Linear Chaotic Map for Joint Lossless Compression and Encryption of Medical Images in IoMTs

Achraf Daoui ¹, Haokun Mao ^{2,*}, Mohamed Yamni ³, Qiong Li ², Osama Alfarraj ⁴
and Ahmed A. Abd El-Latif ^{2,5,*}

- ¹ National School of Applied Sciences, Sidi Mohamed Ben Abdellah-Fez University, Fez 30000, Morocco; achraf.daoui@usmba.ac.ma
- ² Information Countermeasures Technique Institute, School of Cyberspace Science, Faculty of Computing, Harbin Institute of Technology, Harbin 150001, China; qiongli@hit.edu.cn
- ³ Dhar El Mahrez Faculty of Science, Sidi Mohamed Ben Abdellah-Fez University, Fez 30000, Morocco; mohamed.yamni@usmba.ac.ma
- ⁴ Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudi Arabia; oalfarraj@ksu.edu.sa
- ⁵ Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebeen El-Kom 32511, Egypt
- * Correspondence: hkmao@hit.edu.cn (H.M.); ahmedabdellatif@ieee.org (A.A.A.E.-L.)

Abstract: The discrete Shmaliy moment transform (DST) is a type of discrete orthogonal moment transform that is widely used in signal and image processing. However, DST is not suitable for lossless image applications due to its non-integer reversible nature. To overcome this limitation, we introduce the integer discrete Shmaliy transform (IDST) that performs integer-to-integer encoding, leading to a perfect and unique reconstruction of the input image. Next, a new 1D chaotic system model, the 1D multiparametric piecewise linear chaotic map (M-PWLPCM), is presented as an extension of the existing 1D PWLPCM. The M-PWLPCM includes eight control parameters defined over an unlimited interval. To demonstrate the relevance of IDST and M-PWLPCM in reversible image processing applications, they are used in a new scheme for lossless compression and encryption of medical images in the internet of medical things (IoMTs). On the one hand, the simulation results show that our scheme offers a good compression ratio and a higher level of security to resist differential attacks, brute force attacks and statistical attacks. On the other hand, the comparative analysis carried out shows the overall superiority of our scheme over similar state-of-the-art ones, both in achieving a higher compression ratio and better security when communicating medical images over unsecured IoMTs.

Keywords: discrete orthogonal moments; integer discrete Shmaliy transform; secure communication; lossless compression; encryption

MSC: 68P25



Citation: Daoui A.; Mao, H.; Yamni, M.; Li, Q.; Alfarraj, O.; Abd El-Latif, A.A. Novel Integer Shmaliy Transform and New Multiparametric Piecewise Linear Chaotic Map for Joint Lossless Compression and Encryption of Medical Images in IoMTs.

Mathematics **2023**, *11*, 3619. <https://doi.org/10.3390/math11163619>

Academic Editor: Antanas Cenys

Received: 9 July 2023

Revised: 5 August 2023

Accepted: 14 August 2023

Published: 21 August 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The internet of medical things (IoMTs) is revolutionizing healthcare by interconnecting objects, sensors and medical devices, enabling the remote monitoring of patients' health status and performing real-time diagnostics [1]. However, this connectivity is generally accompanied by two major challenges: (i) The rapid expansion in the storage capacity of medical data (images, videos, personal data, medical reports, etc.), which leads to an increased need for storage devices and limits the transmission of such massive data over limited bandwidth [2,3]. (ii) Security and privacy are key challenges for the IoMTs ecosystem. Indeed, patient data must be protected from any unauthorized access or manipulation [4]. To overcome the first limitation, compression techniques can be used, as such techniques

reduce the medical data size [5]. This reduction optimizes the use of network bandwidth, enabling fast data transmission [6]. To ensure confidential and secure transmission of medical data in IoMTs, robust encryption techniques can be successfully utilized [7]. By implementing such techniques, healthcare organizations can protect sensitive medical data from potential misuse by cyber-attackers [8]. It is clear that the compression and encryption techniques are essential in the internet of medical things (IoMT) systems, since they create a secure and efficient environment for the storage and transmission of medical data. For this purpose, researchers have recently provided some implementations of joint compression and encryption schemes for medical images [9,10]. Modern medical imaging technologies produce high-resolution image files [11], which can be costly in terms of storage space and network transmission. Compression techniques are specifically designed to reduce the size of medical image files, while preserving the clinical details of each image [12]. Medical images can be compressed by two methods: a lossy compression or a lossless one. Lossy compression techniques usually offer the possibility of achieving a high compression ratio, thus saving valuable storage space [13]. Commonly used lossy compression schemes include JPEG-2000 [14,15], JPEG [16], and so on. However, until now, lossy compression approaches are less acceptable in the field of medical imaging because they lead to the loss of critical information details in medical images [17,18]. This is why lossless compression techniques are more appropriate to the medical imaging field, as they avoid any visual information loss while reducing the size of the image file [13,19]. Lossless image compression technologies can be implemented through two main approaches: predictive coding and transform coding. Predictive coding-based compression algorithms such as JPEG-LS [20] and CALIC [21] are generally implemented in the spatial domain [22]. However, these predictor-based algorithms are independent of the image compression standard (JPEG) structure [22]. To support the JPEG standard, lossless compression schemes have been introduced in the transform coding domain [18,23,24]. Such schemes are essentially based on the use of the integer discrete cosine transform (IDCT), which was introduced to the field of image processing about 23 years ago [25]. This is why Xiao et al. are investigating a new integer discrete orthogonal transform, namely the integer discrete Tchebichef transform (IDTT), in lossless image compression [22]. In their work, IDTT has replaced IDCT in the JPEG compatible lossless compression scheme. The authors conclude that the use of IDTT improves the compression ratio over IDCT while employing the standardized JPEG scheme. Consequently, it is desirable to investigate new reversible integer transforms for improving the efficiency of transform-based lossless image compression. Once the medical images have been compressed, they can be stored or transmitted via IoMTs devices. However, the IoMT devices typically offer restricted storage capacity. To overcome this issue, cloud-based data storage can be exploited [26]. Even more, the compressed images with the confidential patient information (identity, name, diagnostic reports, etc.) can be communicated via the IoMTs. However, uploading or transmitting compressed images via the IoMTs may not be secure [27]. To guarantee a high level of security in IoMTs, cryptographic systems can be used. [28,29]. Chaotic systems have proven to be very successful in the design of cryptographic systems with high security in IoMTs [30,31]. Chaotic system models can be categorized into two main classes: unidimensional (1D) [32,33] and multidimensional (nD) [34,35]. Chaotic systems that are 1D are considered more implementation-friendly than nD systems, either at the software or hardware level, given the simple nature of 1D chaos models [36]. However, 1D chaotic systems are generally limited by certain well-known weaknesses, namely: (i) the limited number of their control parameters, which are generally used as secure keys in cryptographic systems; and (ii) the limited intervals of their control parameters, in which 1D chaotic systems behave chaotically. To overcome these limitations, it is possible to use 1D chaotic maps incorporating multiple control parameters defined over unlimited ranges [33]. In this work, we introduce a new discrete reversible transform called the integer discrete Shmaliy transform (IDST), which is able to perform integer-to-integer encoding through the factorization of Shmaliy polynomials (SPs) into single-row reversible matrices. To demonstrate the benefits of the proposed IDST in IoMTs,

it is used in a new scheme for lossless medical image compression–encryption. In this scheme, IDST is used for encoding the input image into integer coefficients, which are in turn encoded by Huffman coding to produce the compressed image. This process is compatible with the JPEG standards. In order to provide a higher security level to our scheme, we propose an extended version of the classical piecewise linear chaotic map (PWLCM). The proposed version is called the multiparametric piecewise linear chaotic map (M-PWLCM), which contains eight control parameters defined over \mathbb{R} -domain. By contrast, the classical PWLCM has only one control parameter defined over a limited interval. Next, M-PWLCM is used to encrypt the compressed medical images, and its control parameters are securely shared between authorized IoMT users as security keys. The main contribution of the current work can be summarized in the following points:

- A new reversible integer discrete Shmaliy transform (IDST) is proposed for integer-to-integer mapping in signal and image processing.
- A new 1D chaotic map called M-PWLCM incorporating eight control parameters defined over an infinite range is proposed.
- IDST and M-PWLCM are used in a proposed lossless compression–encryption scheme for IoMTs.
- The proposed lossless scheme provides an acceptable compression ratio with a high security level.
- To the best of our knowledge, the proposed framework is the first attempt to use reversible integer transforms in joint compression and encryption of medical images.
- Simulations and comparisons are provided to demonstrate the suitability of our scheme for IoMTs.

The rest of the document is structured as follows:Section 2 deals with the related work and discussion. Section 3 is devoted to presenting the preliminaries. Section 4 focuses on the derivation of the proposed IDST and its inverse. Section 5 extends PWLCM to the proposed M-PWLCM. Section 6 includes the design of the proposed lossless compression–encryption scheme. Simulation and comparison outcomes are provided in Section 7 and Section 8 concludes our work and gives its potential extensions in upcoming work.

2. Related Work with Discussion

This section briefly surveys some recent compression–encryption schemes in the field of medical imaging. Indeed, Table 1 summarizes the essential aspects of each surveyed scheme, including the used tools, as well as the advantages and disadvantages of these schemes.

Table 1. Literature survey on medical image compression–encryption schemes.

Scheme	Used Tools	Advantages	Disadvantages
[37]	<ul style="list-style-type: none"> • Entropy encoding • Deep neural learning 	<ul style="list-style-type: none"> • Image noise filtering • Compression ratio improvement • Lossless compression 	<ul style="list-style-type: none"> • Security analysis unavailable • Implemented in the spatial domain
[38]	<ul style="list-style-type: none"> • Compressive sensing • 1D chaotic Chebyshev map • 1D chaotic logistic map 	<ul style="list-style-type: none"> • Controlled compression ratio • Resistance to brute-force and statistical attacks 	<ul style="list-style-type: none"> • Lossy compression • Time consumption • Limited range of the security key’s components
[9]	<ul style="list-style-type: none"> • Multiscale transforms • Encoding techniques • RSA algorithm 	<ul style="list-style-type: none"> • Controlled compression ratio • Decompressed–decrypted image quality improvement 	<ul style="list-style-type: none"> • Lossy compression • Security analysis unavailable

Table 1. Cont.

Scheme	Used Tools	Advantages	Disadvantages
[39]	<ul style="list-style-type: none"> Modified salp swarm algorithm (SSA) Chaotic coupled map lattices (CML) Entropy coding 	<ul style="list-style-type: none"> Resistance to brute-force and statistical attacks Lossless compression 	<ul style="list-style-type: none"> Compression takes place after encryption and performed in the spatial domain The compression scheme's performance is unavailable Limited range of the security key's components
[40]	<ul style="list-style-type: none"> Compressive sensing Discrete wavelet transform (DWT) 	<ul style="list-style-type: none"> Resistance to brute-force attacks Controlled compression ratio Acceptable quality of the decompressed–decrypted image 	<ul style="list-style-type: none"> Lossy compression Time consumption Some statistical results are somewhat far from the desired levels
Proposed work	<ul style="list-style-type: none"> Integer discrete Shmaliy transform (IDST) 1D M-PWLCM Entropy encoding 	<ul style="list-style-type: none"> Acceptable compression ratio High degree of security Lossless compression compatible with JPEG standards 	<ul style="list-style-type: none"> Time-consuming for large-sized images Uncontrolled compression ratio Not robust against data loss or noise

From Table 1, we can conclude that the main objectives of joint compression–encryption schemes are as follows: (i) achieving a good compression ratio to benefit from maximum storage space, and (ii) maximizing the security level for reliable communication of medical images over IoMTs. To achieve the first objective, a compressive sensing approach can be adopted [38,40]. This approach offers a high compression ratio with easy control of this ratio. However, this approach is potentially inappropriate for medical images, as it performs lossy compression, which can lead to the loss of sensitive visual data. Furthermore, the reconstruction process in this approach is generally very time-consuming. Transform-based methods (i.e., DWT, DCT, etc.), as presented in [9], can also be used to deliver a good compression ratio. However, these methods involve visual information loss when reconstructing the medical images. To overcome this issue, lossless compression–encryption techniques can be implemented, as outlined in [37,39]. These schemes are implemented in the spatial domain and the compressed image is produced through entropy coding. However, image compression in the spatial domain using entropy coding is still limited, as it is unable to achieve a good compression ratio. To achieve objective (ii), chaotic systems are generally deployed where their initial conditions and control parameters are used as safety keys. This is why the design of new multiparametric chaotic systems for use in compression–encryption systems is of great interest for attaining higher security levels. It is clear from the above discussion that there is a real need for further development of new lossless compression–encryption schemes that can achieve higher compression ratios with superior security levels, with the aim of improving the efficiency and reliability of data storage and communication over IoMTs.

3. Preliminaries

This section provides definitions and preliminaries relevant for the present work, including SPs and its transformation.

3.1. Discrete Shmaliy Polynomials

The discrete Shmaliy polynomials (SPs) are a type of discrete orthogonal polynomial. SPs have a simpler definition than other discrete orthogonal polynomials (Tchebichef, Krawtchouk, Hahn, Dual Hahn, and Racah) due to their independence from local parameters and their linear weight function [41]. Only few works in the literature use SPs as basis

kernel for defining discrete Shmaliy transforms. Indeed, Asli et al. introduced in [42] the conventional 1D discrete Shmaliy transform (DST), which can be easily extended to 2D and 3D domains. More recently, Daoui et al. [43] have extended the conventional DST transform to the quaternion discrete Shmaliy transform (QDST) for the purpose of compact color image analysis. However, both DST and QDST convert the input signal/image function into floating-point values. Therefore, such transformations are less appropriate for input functions of integer values. To overcome this limitation, the present work develops a framework for deriving a new type of Shmaliy transform, namely IDST, which can be used to perform integer-to-integer mapping. SPs are defined by the next equation [42]:

$$S_n(x) = \frac{(-1)^n (n+1)(x-n)_n (N-x)_n}{n!(N)_{n+1}} \sum_{k=0}^{\infty} \frac{(-n)_k (x+1)_k (1-N+x)_k}{(x-n)_k (1-N-n+x)_k k!}; \quad n, x = 0, 1, \dots, N-1 \tag{1}$$

where $(p)_k$ represents the Pochhammer symbol [44], which is expressed in terms of Gamma function ($\Gamma(p)$) as

$$(p)_k = p(p+1)(p+2) \dots (p+k-1) = \frac{\Gamma(p+k)}{\Gamma(p)} \quad \text{with } k \geq 0, p > 0 \text{ and } (p)_0 = 1 \tag{2}$$

To ensure the numerical stability of SPs used for digital signal analysis, the next orthonormalized SPs are used:

$$\hat{S}_n(x) = S_n(x) \sqrt{\frac{\omega_x}{\rho_n}} \tag{3}$$

where ω_x and ρ_n represent the weight and square-norm functions of SPs, respectively. These functions are given by [42]:

$$\omega_x = \frac{2x}{N(N-1)} \text{ and } \rho_n = \frac{(n+1)(N-n-1)_n}{N(N)_{n+1}} \tag{4}$$

For efficient computation of SPs, the three-term recurrence relation below is used [43]:

$$\tilde{S}_n(x) = \lambda \tilde{S}_{n-1}(x) + v \tilde{S}_{n-2}(x) \text{ for } x = 1, 2, \dots, N \text{ and } n = 2, \dots, N-1$$

$$\lambda = \left[\frac{n^2(2N-1)}{2n-1} - x(2n+1) \right] \sqrt{\frac{4}{n(N+n)(n+1)(N-n-1)}} \tag{5}$$

$$v = -\frac{(2n+1)}{(2n-1)} \sqrt{\frac{(N-n)(n-1)(N+n-1)}{(N+n)(n+1)(N-n-1)}}$$

The initial terms of DSPs are computed via Equations (6) and (7), respectively.

$$\hat{S}_0(x) = \sqrt{\frac{x}{x-1}} \tilde{S}_0(x-1) \text{ for } x > 2 \text{ with } \hat{S}_0(1) = \sqrt{\frac{2}{N(N-1)}} \tag{6}$$

$$\hat{S}_1(x) = \frac{[-6x + 2(2N-1)]}{4} \sqrt{\frac{1}{(N+1)(N-2)}} \hat{S}_0(x) \tag{7}$$

A typical 8×8 ortho-normalized SPs matrix is given as follows:

$$\hat{S} = \begin{bmatrix} 0.1666 & 0.3944 & 0.5351 & 0.5318 & 0.4122 & 0.2508 & 0.1154 & 0.0352 \\ 0.2357 & 0.4382 & 0.3243 & -0.05373 & -0.4164 & -0.5321 & -0.3964 & -0.1745 \\ 0.2886 & 0.3903 & 0.0147 & -0.3947 & -0.3060 & 0.1931 & 0.5426 & 0.4274 \\ 0.3333 & 0.2817 & -0.2548 & -0.3418 & 0.2120 & 0.4181 & -0.1649 & -0.6170 \\ 0.3726 & 0.1259 & -0.3988 & 0 & 0.4266 & -0.1869 & -0.4056 & 0.5518 \\ 0.4082 & -0.0690 & -0.3537 & 0.3721 & 0.0288 & -0.4438 & 0.5251 & -0.3022 \\ 0.4409 & -0.2981 & -0.0674 & 0.4020 & -0.5298 & 0.4424 & -0.2555 & 0.0932 \\ 0.4714 & -0.5577 & 0.5045 & -0.3760 & 0.2332 & -0.1182 & 0.0466 & -0.0124 \end{bmatrix}$$

3.2. Discrete Shmaliiy Transform

The discrete Shmaliiy transform (DST), commonly known as discrete Shmaliiy moments (DSMs), is increasingly used in signal and image analysis, including signal and image reconstruction [42], texture classification [41], and bio-signal zero-watermarking [43]. The 2D DST of the order (n,m) is calculated by using the following formula:

$$DST_{nm} = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} I(x,y) \hat{S}_n(x) \hat{S}_m(y) \tag{8}$$

where $I(x,y)$ and $\hat{S}_n(x)$ represent, respectively, the 2D image function and SPs matrix of size $N \times M$. The next inverse DST formula is used to reconstruct the input image:

$$I_r(x,y) = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} DST_{nm} \hat{S}_n(x) \hat{S}_m(y) \tag{9}$$

where $I_r(x,y)$ is the reconstructed form of $I(x,y)$ image. The similarity between the original image and its reconstructed version can be measured by using reconstruction error criteria such as the mean square error (MSE) and the peak signal-to-noise ratio (PSNR).

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M-1} \sum_{y=1}^{N-1} [I(x,y) - I_r(x,y)]^2 \tag{10}$$

$$PSNR(dB) = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \tag{11}$$

If $MSE = 0$ and $PSNR = Inf$, the input image $\{I(x,y)\}_{x,y=1}^{x,y=N}$ and its reconstructed version $\{\hat{I}(x,y)\}_{x,y=1}^{x,y=N}$ are identical. As result, the reconstruction is considered lossless (perfect). Otherwise, the image reconstruction process is lossy. Although DST continues to attract growing interest in the field of digital signal processing, its applicability remains limited in applications requiring lossless reconstruction of the input signal. These applications include reversible data hiding, lossless compression, reversible watermarking, encryption, etc. Therefore, the extension of DST to support integer-to-integer mapping is highly required. In the next section, a new type of discrete transform, called *IDST*, is introduced.

4. Proposed Integer Shmaliiy Transform

This section details the mathematical derivation of the proposed *IDST*, which is based on the factorization of the DSPs matrix into a product of single-row elementary reversible matrices (SERMs). A DSPs kernel matrix (\hat{S}) of size $N \times N$ satisfies the following properties, which are fundamental to perform SERMs factorization:

- $\hat{S}^T \cdot \hat{S} = \hat{S} \cdot \hat{S}^T = I$. That is, \hat{S} is an $N \times N$ orthogonal matrix with $(.)^T$ is the transpose symbol and I denotes the identity matrix of size $N \times N$.

- The transpose of \hat{S} equals its inverse: $\hat{S}^T = \hat{S}^{-1}$. That is, \hat{S} is invertible.
- \hat{S} determinant is equals to 1: $\det(\hat{S}) = 1$.
- All minors of the lead sub-matrices of \hat{S} are 1 s.

The above properties allow the factorization of \hat{S} into $(N + 1)$ SERMs as follows [45]:

$$\hat{S} = PS_N \dots S_2 S_1 S_0 \tag{12}$$

where P is the permutation matrix of \hat{S} with $S_k (k = 0, 1, 2, \dots, N)$ representing the SERMs given by

$$\begin{aligned} S_0 &= I + e_N s_0^T \\ S_k &= I + e_k s_k^T, k = 1, 2, \dots, N \end{aligned} \tag{13}$$

In Equation (13), e_k denotes the k -th column of I matrix, and s_k denotes the necessary component vectors of SERMs with the k -th ($k = 0, 1, 2, \dots, N$) component equal to zero. The SERMs satisfy the following property:

$$\begin{aligned} S_0^{-1} &= S_0 = I + e_N s_0^T \\ S_k^{-1} &= I - e_k s_k^T, k = 1, 2, \dots, N \end{aligned} \tag{14}$$

The factorization of \hat{S} into SERMs leads to the achievement of the following permutation matrix:

$$P = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

with the vectors S_0, S_1, \dots, S_8 computed and then presented as follows:

$$\begin{bmatrix} s_0^T \\ s_1^T \\ s_2^T \\ s_3^T \\ s_4^T \\ s_5^T \\ s_6^T \\ s_7^T \\ s_8^T \end{bmatrix} = \begin{pmatrix} -0.92140 & 1.05128 & 1.24752 & 1.80687 & -2.26269 & 0.30536 & 1.41220 & 0 \\ 0 & -0.20606 & -0.61469 & -1.16643 & 0.74272 & -0.50777 & -0.77991 & 0.50452 \\ -0.11952 & 0 & 1.01272 & 1.15012 & -1.04730 & 0.04062 & 0.39632 & -0.49746 \\ 0.10906 & -0.41286 & 0 & 0.41043 & -0.85013 & 0.60809 & -0.03424 & -0.23866 \\ 0.52778 & -0.39710 & 0.32771 & 0 & 0.20959 & 0.09844 & -0.14779 & -0.26984 \\ 0.27546 & -0.15613 & 0.82579 & -0.63965 & 0 & -0.59176 & 0.11802 & -0.12787 \\ 0.15987 & 0.20260 & -0.67963 & 0.87676 & 0.97392 & 0 & 0.22756 & 0.34311 \\ 0.33717 & 0.21335 & 0.52981 & -0.48263 & -0.98684 & 0.19278 & 0 & -0.44249 \\ -0.60962 & 0.19162 & -0.61979 & 2.28800 & 2.01935 & -1.43218 & 1.35138 & 0 \end{pmatrix}$$

The following formula defines the proposed one-dimensional *IDST* (1D *IDST*) for a discrete signal $x = (x_0, x_1, \dots, x_7)^T$ of integer coefficients:

$$M = IDST(x) = P[S_8 \dots [S_1[S_0 x]] \dots] \tag{15}$$

where $[\cdot]$ denotes the symbol of rounding arithmetic operation. The reconstructed signal \hat{x} is computed by applying the inverse of *IDST* that is defined as follows:

$$\hat{x} = iIDST(M) = [S_0^{-1} \dots [S_7^{-1} [S_8^{-1} P^T M]] \dots] \tag{16}$$

To extend the 1D *IDST* to the two-dimensional domain, first the 1D *IDST* is applied to each column of the 2D signal function $\{I\}_{x,y=1}^{x,y=8}$. Next, the 1D *IDST* is applied to each row of the resulting matrix. Mathematically, the two-dimensional integer discrete Shmaliy transform (2D *IDST*) is calculated according to Equation (17).

$$M = IDST\left(\left(IDST(I)\right)^T\right) \tag{17}$$

The inverse of 2D-*IDST* can be used to generate the reconstructed 2D function $\{\hat{I}\}_{x,y=1}^{x,y=8}$ as follows:

$$\hat{I} = iIDST\left(\left(iIDST(M)\right)^T\right) \tag{18}$$

By performing an integer-to-integer transformation via *IDST* and its inverse, the input image can be recovered without any information loss (lossless). To confirm this statement, the similarity between the input image and its reconstructed version can be measured by using the *MSE* and *PSNR* criteria.

Figure 1 illustrates an example where the proposed *IDST* is used for the reconstruction of an integer-valued input matrix of size 8×8 (Figure 1a). On the one hand, this example shows that the forward *IDST* (Equation (17)) is able to produce an integer matrix (Figure 1b) from an integer input matrix. Thus, the proposed *IDST* is able to perform an integer-to-integer mapping. On the other hand, we can see that the inverse of the *IDST* (Equation (18)) results in a perfect reconstruction of the input matrix (Figure 1c). This is evident from Figure 1d, which plots the difference in absolute value between the input matrix and its reconstructed version using *IDST*.

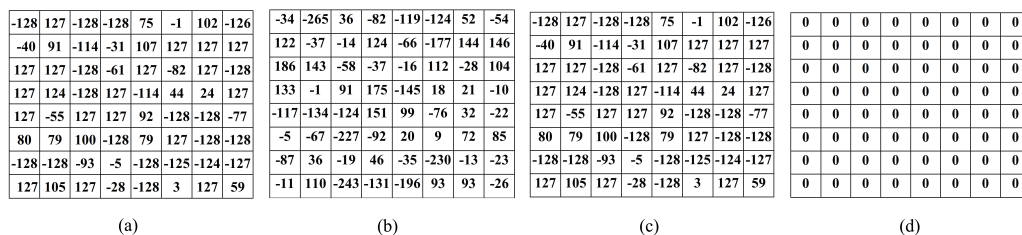


Figure 1. (a) Integer-valued input matrix of size 8×8 . (b) The forward *IDST* of (a) matrix. (c) The inverse *IDST* of (b) matrix. (d) The difference in absolute values between (a,c) matrices.

The practical utility of *IDST* in medical image analysis will be demonstrated by using *IDST* in lossless compression–encryption of medical images. This application must also offer a high level of security for resisting various cyber attacks.

5. Proposed Multiparametric Piecewise Linear Chaotic Map

The one dimensional (1D) chaotic maps are usually used in various crypto-systems for their low complexity and easy-to-implement models.

5.1. Traditional Piecewise Linear Chaotic Map

The traditional 1D piecewise linear chaotic map (1D PWLCM) is widely used in various encryption schemes. The original mathematical model of the 1D PWLCM is given by the following formula [46] :

$$x(k + 1) = F(x(k), p) = \begin{cases} x(k)/p & \text{if } x(k) \in [0, p) \\ (x(k) - n)/(0.5 - p) & \text{if } x(k) \in [p, 0.5) \\ F(1 - x(k), p) & \text{if } x(k) \in [0.5, 1) \end{cases} \tag{19}$$

where $p \in (0, 0.5)$ is the control parameter of PWLCM and its initial value is $x(0) \in (0, 1)$. Figure 2 shows the bifurcation diagram and Lyapunov exponent (LE) values of PWLCM. This figure clearly shows that PWLCM behaves chaotically if $p \in (0, 0.5)$, as all LE values

are positive and the output of this map exhibits “bifurcation” within the range [0–1]. Such behavior indicates the potential suitability of PWLCM for use in security systems. However, the PWLCM model contains only one control parameter, which is defined within a restricted interval. These issues make PWLCM highly vulnerable to cyber attacks when it is employed in security applications. To overcome these limitations, the next subsection introduces a new version of PWLCM.

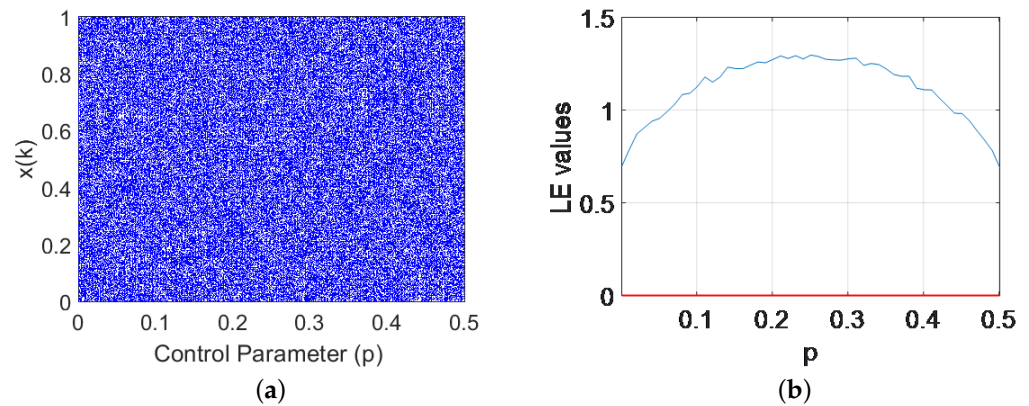


Figure 2. (a) Bifurcation diagram and (b) LE of PWLCM for $p \in (0,0.5)$ and $x(0) = 0.1$.

5.2. Proposed M-PWLCM and Its Analysis

Within this section, the proposed multiparametric piecewise linear chaotic map (M-PWLCM) is presented as an extension of the existing PWLCM. The M-PWLCM is defined by the following model:

$$x(k + 1) = \begin{cases} 2.5 \times \left(1 - \left| 10^{-2} \operatorname{atan}(\lambda_1) \right| - \left| 10^{-2} \cos(\lambda_2) \right| \right) \times x(k) & \text{if } x(k) \in [0, 0.4) \\ \left(10 - \left| 10^{-2} \operatorname{atan}(\lambda_3) \right| - \left| 10^{-2} \cos(\lambda_4) \right| \right) \times (x(i) - 0.4) & \text{if } x(k) \in [0.4, 0.5) \\ \left(10 - \left| 10^{-2} \operatorname{atan}(\lambda_5) \right| - \left| 10^{-2} \cos(\lambda_6) \right| \right) \times (0.6 - x(i)) & \text{if } x(k) \in [0.5, 0.6) \\ 2.5 \times \left(1 - \left| 10^{-3} \operatorname{atan}(\lambda_7) \right| - \left| 10^{-3} \cos(\lambda_8) \right| \right) \times (1 - x(i)) & \text{if } x(k) \in [0.6, 1) \end{cases} \quad (20)$$

where $(\lambda_1, \dots, \lambda_8)$ are the eight control parameters of the proposed M-PWLCM with its initial value $x(0)$, which should be given in $(0, 1)$. $\operatorname{atan}(\cdot)$ and $\cos(\cdot)$ are the arctangent and cosine trigonometric functions, respectively. $|\cdot|$ is the absolute value symbol.

Unlike to the original PWLCM, the proposed M-PWLCM contains eight control parameters that are defined over an unlimited interval since $\operatorname{atan}(\cdot)$ and $\cos(\cdot)$ functions are both defined over the \mathbb{R} -domain. Accordingly, we expect that the proposed model can provide a high degree of security in terms of security key space. In addition, defining control parameters on \mathbb{R} not only boosts the security level, but also provides a great facility for the user to select the authentication/security key, which is composed from the M-PWLCM control parameters.

It is worth mentioning that it is easy to adapt the M-PWLCM model given by Equation (20) to contain less than eight parameters by setting the terms $|\delta \operatorname{atan}(\lambda)|$ and/or $|\delta \cos(\lambda)|$ to zero with $10^{-3} \leq \delta \leq 10^{-2}$. Reducing the number of M-PWLCM parameters can reduce the implementation complexity, particularly in a hardware-based environment. However, by reducing the number of M-PWLCM parameters, the security key space of M-PWLCM-based systems is also reduced, which can make these systems vulnerable to cyber attacks by brute force. It is also easy to adapt the proposed M-PWLCM model to contain more than eight parameters. In fact, it is sufficient to add or subtract $|\delta \operatorname{atan}(\lambda)|$ and $|\delta \cos(\lambda)|$ terms in the proposed model’s equations. By increasing the number of the proposed model’s parameters, it is possible to reinforce the security level of M-PWLCM-based systems. However, the large number of parameters (>8) can make the behavior of M-PWLCM either non-chaotic or “poorly” chaotic (low LE values). Thus, each additional parameter in the

M-PWLCM model requires an analysis of this model’s chaotic behavior. Thus, the reason for using eight parameters in the M-PWLCM model is to preserve its excellent chaotic behavior while guaranteeing a high level of security for M-PWLCM-based security systems. The following analysis is provided to confirm this assumption.

Before exploiting M-PWLCM in security schemes, it is crucial to demonstrate its chaotic behavior and sensitivity to its control parameters. To this end, Figures 3 and 4 are presented. These figures show, respectively, the bifurcation diagrams and LE values of the proposed map when varying its control parameters over a subinterval in \mathbb{R} .

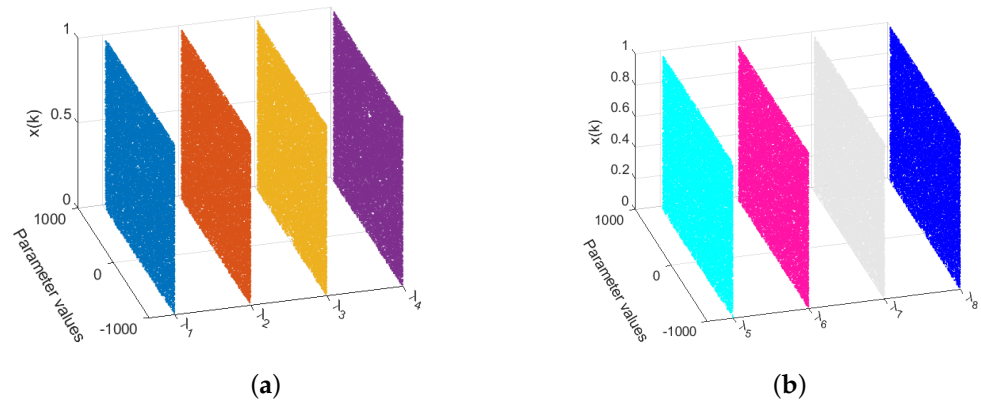


Figure 3. Bifurcation diagrams of M-PWLCM when varying its control parameters (a) $(\lambda_1, \dots, \lambda_4)$ and (b) $(\lambda_5, \dots, \lambda_8)$ in the interval $[-1000, 1000]$ with $x(0) = 0.3$.

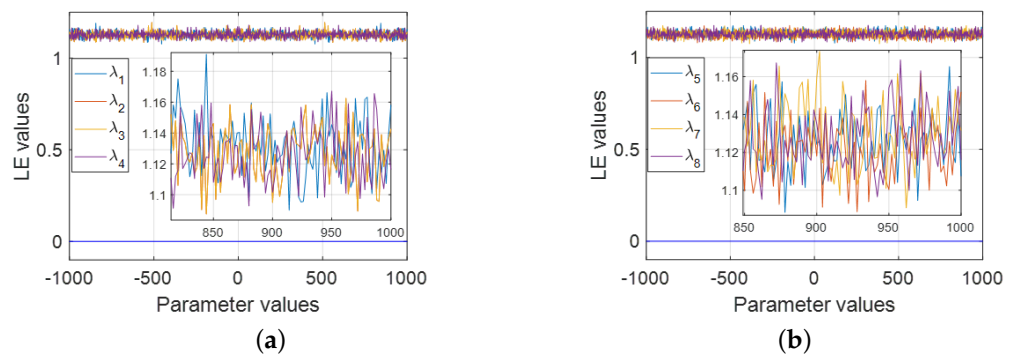


Figure 4. LE values of M-PWLCM when varying its control parameters (a) $(\lambda_1, \dots, \lambda_4)$ and (b) $(\lambda_5, \dots, \lambda_8)$ in the interval $[-1000, 1000]$ with $x(0) = 0.3$.

Figure 3 shows that the proposed map exhibits significant bifurcations when its eight parameters vary over the interval $[-1000, 1000]$. This figure graphically shows that the proposed map exhibits chaotic behavior over the range displayed in the test. Furthermore, the test results show that all the M-PWLCM parameters influence its output. These results provide a clear indication of M-PWLCM’s chaotic behavior. It should be mentioned that the interval $[-1000, 1000]$ in the current test (Figure 3) is illustrative, whereas the findings of this test are reproducible over \mathbb{R} . To better prove the chaos of M-PWLCM, LE values are computed for its control parameters over the interval $[-1000, 1000]$. The current test results are then presented in Figure 4. It is evident from this figure that $LE > 1$ for the full studied range. The same results can be obtained over \mathbb{R} . Clearly, the proposed model’s chaotic behavior is confirmed by this test.

The chaotic systems are generally of high sensitivity to their control parameters. Therefore, it is necessary to test the sensitivity level of each parameter in the proposed M-PWLCM to confirm its suitability for use in security systems. To this end, a chaotic

sequence is initially generated by the proposed model while setting the control parameters to the following values:

$$(\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8) = (7, 5, 0, 1, 8, 9, 10, 2)$$

Then, in each case, one parameter is modified by adding a small Δ -value, and a new chaotic sequence is re-generated via M-PWLCM according to the performed modification. Afterwards, the original chaotic sequence and the re-generated one are plotted with their absolute differences in the same graph shown in Figure 5. From this figure, it can be observed that any small variation by $\Delta \in [10^{-12}, 10^{-10}]$ of the control parameters results in a significant variation of the proposed map's output. This evidence validates that the M-PWLCM is very sensitive to its control parameters. Consequently, the output values produced by the proposed chaotic system can be used in security information systems and the control parameters of this system can be used as security keys.

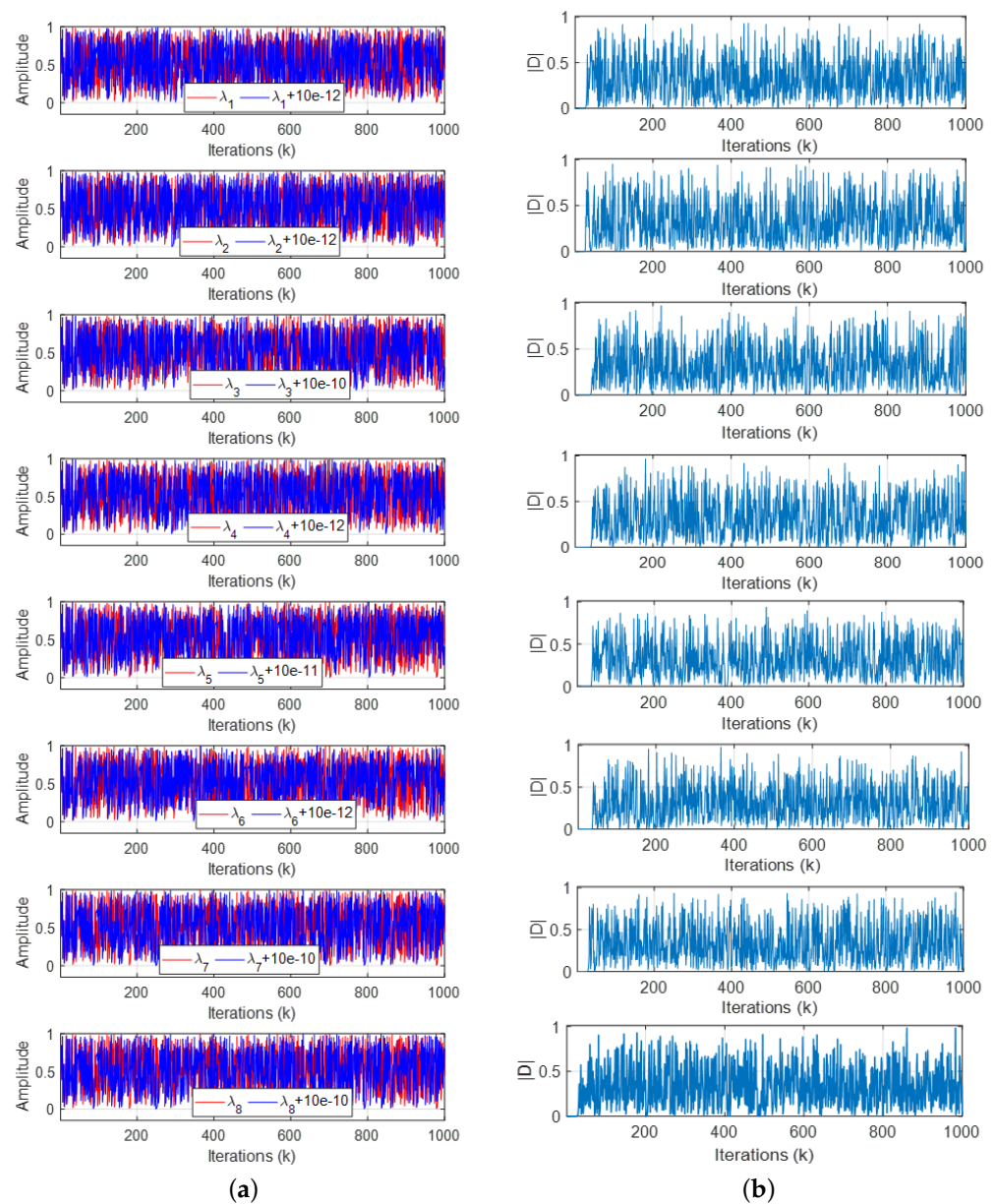


Figure 5. (a) M-PWLCM time series for 1000 iterations, and (b) the absolute difference ($|D|$) between the original series (blue color) and the ones generated following a slight variation by $\Delta \in [10^{-12}, 10^{-10}]$ (red color) of the control parameters.

The following section introduces a proposed lossless medical image compression–encryption scheme based on IDST and M-PWLCM.

6. Proposed Lossless Compression–Encryption Scheme for IoMTs

The proposed lossless compression–encryption scheme for medical images consists of two consecutive phases performed by the transmitter and the receiver, respectively. At the transmitter level, the medical image is compressed based on IDST and Huffman Coding. Then the compressed image is encrypted based on the proposed M-PWLCM. Finally, the compressed–encrypted image can be transmitted securely over a public communication channel. At the receiver level, the compressed–encrypted image is decrypted and decompressed to retrieve its original form without any information loss. It should be mentioned that the Transport Control Protocol (TCP) must be used when transmitting the compressed–encrypted image from the transmitter to the receiver because TCP supports the lossless data transmission. Figure 6 illustrates the key phases of the proposed compression–encryption scheme and its details are presented below.

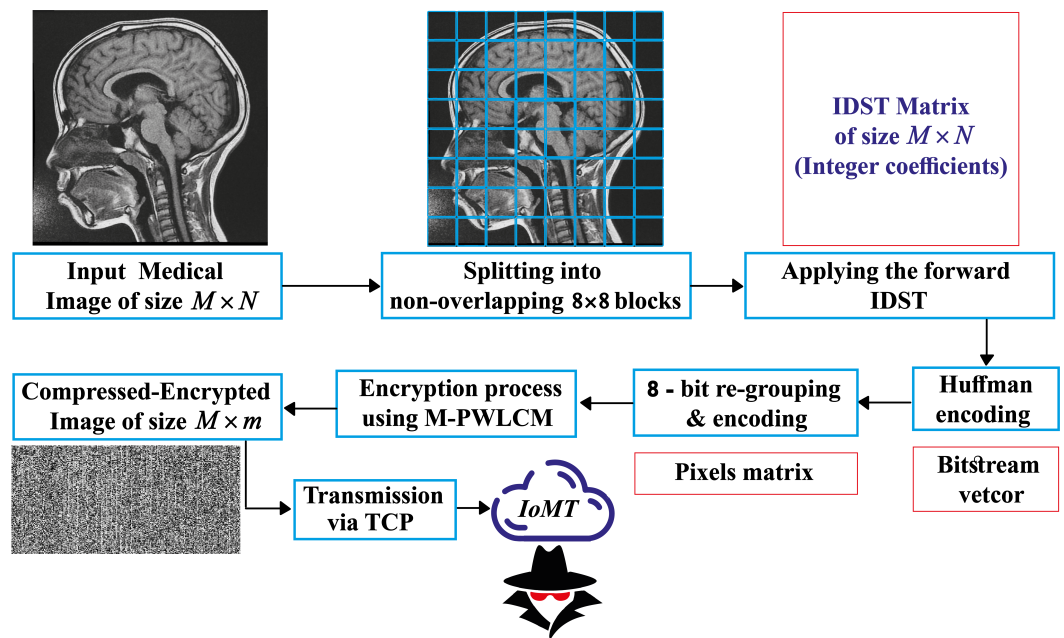


Figure 6. Proposed compression–encryption scheme.

6.1. Pre-Processing

In this step, the input I image of size $N \times M$ is divided into non-overlapping 8×8 blocks in order to apply the proposed IDST to each block. This step is a popular pre-processing step used in various image processing schemes, as it reduces the overall computational complexity of a transform-based algorithm.

6.2. Computation of the Forward IDST

The current step allows the calculation of the forward IDST of each 8×8 image block, which generates the $N \times M$ matrix, noted M , which contains integer coefficients.

6.3. Huffman Coding

Huffman coding is based on the assignment of variable-length codes to the input values. Depending on the occurrence frequency of each value, the length of the code (bit sequence) assigned to that value is determined. Indeed, the smallest bit sequence is assigned to the value of the highest frequency, and the largest bit sequence is allocated to the value of the lowest frequency [47]. The generated Huffman codes are unique for the input values. Thus, Huffman coding guarantees the absence of any kind of ambiguity

during the decoding process on the coded bit stream [48]. Huffman coding therefore aims to reduce the redundancy in the input values, resulting in a high compression ratio. Huffman coding is generally implemented in the transform domain rather than the spatial one. This is because there is less redundant information in the transform domain in comparison to the spatial domain [49].

In the present step, Huffman coding is used as an entropy coding technique for exploiting the statistical properties of *IDST* matrix data in order to assign shorter binary codes to the most probable coefficients and longer binary codes to the less probable coefficients. This process leads to an overall reduction in the size of the *IDST* matrix, producing the compressed image. The latter is represented by a sequence of binary bits stored in a 1D binary vector denoted as *VB*.

To evaluate the compression ratio using the proposed method, we can use the bits per pixel (*Bpp*) criterion, which represents the average number of bits that are required for encoding each pixel in the input image. *Bpp* can be considered as an absolute indicator of the compression ratio. This criterion is defined by Equation (21).

$$Bpp = \frac{L_B}{D_I} \tag{21}$$

where $L_B = length(VB)$ represents the length of the *VB* vector and $D_I = N \times M$ denotes the input image dimensions product. The lower *Bpp* value indicates a higher compression ratio.

6.4. Bit Stream Grouping and Coding

In this step, the *VB* vector is divided into groups of 8 bits. Then, each group is converted into its decimal representation. This process creates grayscale values, which are reshaped into a *CI*-labeled 2D matrix of size $N \times m$. This matrix represents the compressed grayscale form of the input *I* image. The compression ratio (*CR*) achieved by the proposed method is determined by using the next *CR* criterion:

$$CR(\%) = \left(1 - \frac{\text{Compressed image dimensions}}{\text{Original image dimensions}} \right) \times 100 \tag{22}$$

The higher *CR* is an indicator regarding the effectiveness of the used compression technique.

6.5. Compressed Image Encryption

The current phase is a key part of the proposed scheme for ensuring a secure communication of the compressed images over IoMTs. Indeed, medical images need to be communicated via IoMTs while guaranteeing the highest standards of security for preventing any third-party attacks. To achieve this goal, the proposed M-PWLCM is exploited according to the steps described below.

Step 1: This step consists in generating a chaotic sequence denoted *S* of length $L = N \times m$ by using the proposed M-PWLCM model (see Equation (20)). Next, the generated sequence is rounded into grayscale levels as follows:

$$PS = \lfloor S \times 255 \rfloor \tag{23}$$

Step 2: This step consists in reshaping the *PS* vector into a 2D matrix labeled as *D* of size $N \times m$.

Step 3: Use the *bitxor* operator to encrypt the compressed image as follows:

$$EI = bitxor(CI, D) \tag{24}$$

where *EI* represents the compressed–encrypted image of size $N \times m$. It is worth mentioning that at this step, the control parameters $\lambda_1, \dots, \lambda_8$, and $x(0)$ the initial value of M-PWLCM are given as security a key, noted as $KEY = (x(0), \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8)$. This key is

communicated between authorized IoMT users through a secure communication medium such as Short Message Service (SMS). Without this key, the attacker is unable to obtain any useful information from the compressed–encrypted image. It is also important to mention that the proposed system is symmetric. That is, the reverse process to that used for generating the compressed–encrypted image (EI) is performed to produce the decrypted–decompressed image, which is exactly equivalent to the input image (I).

It should be noted that the use of the proposed scheme to color medical images requires the conversion of these images from RGB to $YCbCr$ color space. This pre-processing step is adopted in lossless compression to achieve a higher compression ratio [22]. For this purpose, Equation (25) is used to convert the input image from RGB to $YCbCr$ space, and the reverse conversion is accomplished by using Equation (26) [50].

$$\begin{cases} Y = \lfloor (R + 2G + B)/4 \rfloor \\ Cr = R - G \\ Cb = B - G \end{cases} \quad (25)$$

$$\begin{cases} G = Y - \lfloor (Cr + Cb)/4 \rfloor \\ R = Cr + G \\ B = Cb + G \end{cases} \quad (26)$$

In the following section, simulations and comparisons are reported to illustrate the efficiency of the proposed medical image compression–encryption scheme in IoMTs.

7. Simulation Results

Within this section, extensive simulation and comparison results are provided to confirm the suitability of $IDST$ and M-PWLCM for lossless encryption–compression in IoMTs. First, simulation and comparison experiments are carried out to demonstrate the effectiveness of $IDST$ in lossless medical image reconstruction and compression. Next, the proposed scheme is subjected to a series of security analyses aimed at testing its ability to withstand brute-force, statistical and differential attacks, which can occur in IoMTs. It is noteworthy that all the simulations in this study are executed on a PC containing 4 GB of RAM and a processor of 2.4 GHz and Matlab R2022b (v9.13) software (The MathWorks, Inc., Natick, MA, USA) is used to perform the experiments in the present work.

7.1. Reconstruction Error Analysis

In the present test, the performance of the proposed $IDST$ is evaluated in terms of lossless reconstruction. To this end, MSE and $PSNR$ are computed following image reconstruction by using $IDST$. The image reconstruction is also performed by other discrete transforms, including the conventional Shmaliiy moments (SM) [43], Tchebichef moments (TM) [7], Charlier moments (CM) [51], Meixner moments (MM) [52], Hahn moments (HM) [53], Dual Hahn moments (DHM) [54], Racah moments (RM) [55], Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) with three wavelet basis functions (“db1”, “sym2” and “coif1”), Integer Discrete Tchebichef Transform (IDTT) [22], Integer Discrete Cosine Transform (IDCT) [23], and Integer Discrete Wavelet Transform (IDWT) [56]. To perform the current analysis, we use grayscale CT medical images of size 512×512 , which are selected from a dataset in [57]. These images are then reconstructed using the aforementioned discrete transforms and the reconstruction error is evaluated by MSE and $PSNR$ criteria. The results of the current analysis are reported in Figure 7. The results in this figure show on the one hand that $IDST$ outperforms the conventional SM in terms of reconstruction error. On the other hand, when using conventional orthogonal transforms (SM, TM, HM, DCT, DWT, etc.), the MSE obtained is minimal for all the test images but this error is different from zero, indicating that the use of these transforms does not result in a perfect reconstruction. This finding can be explained by the fact that the conventional orthogonal transforms perform integer-to-real encoding and real-to-integer decoding, respectively. These processes lead to rounding and

approximation errors when calculating conventional forward and backward transformations. On the other hand, the results in the same figure show that the integer transforms including the proposed IDST lead to perfect reconstruction ($MSE = 0$ and $PSNR = Inf$). This finding reflects the fact that the integer transforms execute an integer-to-integer mapping during the computation of the forward and backward transformations, which prevents the occurrence of any approximation errors, leading to the ideal reversibility of the grayscale values of the input image. Therefore, when designing reversible data applications such as reversible data hiding, lossless compression, encryption, etc., the use of integer-type transforms (*IDST*, *IDTT*, *IDCT*, etc.) is preferable in comparison to the conventional transforms (*SM*, *DTM*, *DCT*, etc.).

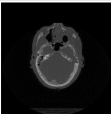
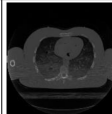
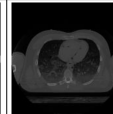
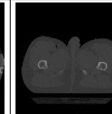
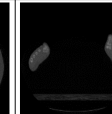
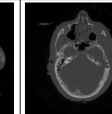
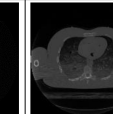
Transforms		Test images							
									
MSE	DWT	'dbl'	3.6611e-28	6.1128e-28	7.5723e-28	7.4282e-28	5.3165e-28	2.8592e-28	3.3527e-28
		'sym2'	8.9595e-23	1.2550e-22	1.5749e-22	1.1817e-22	9.7807e-23	6.7244e-23	6.4869e-23
		'coif1'	2.3934e-22	3.1931e-22	3.8002e-22	2.9490e-22	2.4986e-22	1.6463e-22	1.6802e-22
	SM	7.0022e-27	9.0693e-27	8.5460e-27	8.6624e-27	1.8238e-27	1.1273e-26	9.0693e-27	
	DHM	3.4711e-27	4.4354e-27	4.1724e-27	4.2670e-27	9.1343e-28	5.5942e-27	4.4354e-27	
	RM	1.7321e-23	2.2582e-23	2.1314e-23	2.2003e-23	4.4792e-24	2.8210e-23	2.2582e-23	
	MM	4.2814e-22	5.3314e-22	5.4360e-22	1.1280e-22	6.8699e-22	5.9219e-22	5.4838e-22	
	CM	9.6610e-29	1.1581e-28	1.1035e-28	1.1144e-28	2.4226e-29	1.4724e-28	1.1581e-28	
	HM	2.2806e-28	3.0708e-28	2.8290e-28	2.8709e-28	6.0826e-29	3.7575e-28	3.0708e-28	
	KM	1.1502e-28	1.5158e-28	1.4578e-28	1.4919e-28	2.9702e-29	1.9427e-28	1.5158e-28	
	TM	1.8919e-26	2.4505e-26	2.3183e-26	2.3503e-26	4.9295e-27	3.0619e-26	2.4505e-26	
	DCT	5.5436e-27	7.15e-27	6.7808e-27	6.9177e-27	1.4395e-27	8.9104e-27	7.1535e-27	
	IDCT	0	0	0	0	0	0	0	
	IDTT	0	0	0	0	0	0	0	
	IDST (Proposed)	0	0	0	0	0	0	0	
	PSNR	DWT	'dbl'	322.4947	320.2684	319.3385	319.4219	320.8745	323.5683
'sym2'			268.6080	267.1444	266.1582	267.4059	268.2271	269.8543	270.0104
'coif1'			264.3406	263.0887	262.3327	263.4341	264.1538	265.9656	265.8772
SM		309.6714	308.5550	308.8132	308.7544	315.5211	307.6104	308.5550	
DHM		312.7255	311.6615	311.9269	311.8296	318.5240	310.6534	311.6615	
RM		275.7402	274.5932	274.8441	274.7061	281.6188	273.6268	274.5932	
MM		261.8005	260.4062	260.8624	260.7780	267.6077	259.7613	260.4062	
CM		328.2701	327.4932	327.7031	327.6606	334.2880	326.4506	327.4932	
HM		324.5510	323.2583	323.6145	323.5506	330.2899	322.3818	323.2583	
KM		327.5116	326.3244	326.4937	326.3936	333.4029	325.2467	326.3244	
TM		305.3412	304.2383	304.4790	304.4196	311.2028	303.2709	304.2383	
DCT		310.6803	309.5810	309.8116	309.7322	316.5486	309.1256	309.5856	
IDCT		Inf	Inf	Inf	Inf	Inf	Inf	Inf	
IDTT		Inf	Inf	Inf	Inf	Inf	Inf	Inf	
IDST (Proposed)		Inf	Inf	Inf	Inf	Inf	Inf	Inf	

Figure 7. Reconstruction errors (*MSE* and *PSNR*) corresponding to grayscale medical images using conventional and integer transforms, including the proposed *IDST*.

In the next analysis experiments, the performance of existing integer transforms will be investigated in lossless image compression–encryption application that is composed of two consecutive phases. The first one is the compression phase, which is performed to significantly reduce the redundancy information in the input medical image, and the second phase involves the encryption process to provide a high degree of security during the exchange of medical images in IoMTs.

7.2. Lossless Compression Performance Analysis

Lossless compression of medical images can be performed either in the spatial domain or in the transform one. The current test compares lossless compression in the spatial domain and in the *IDST*-based transform domain. For this, the test images are compressed by Huffman coding in the spatial domain. In the transform-based domain, the lossless compression is performed by using the proposed method.

To perform the current analysis, we use grayscale medical test images of size 512×512 , which are selected from the dataset [57]. In addition, color medical images of size 2048×1024 are also used in this analysis, which are selected from the same dataset. To compare the compression performance, *Bpp* and *CR* criteria are used. The results presented in Figure 8 provide strong evidence that the use of the proposed *IDST* with Huffman coding offers significant improvement in terms of *CR* and *Bpp* for all the test images in comparison to the lossless compression in the spatial domain.

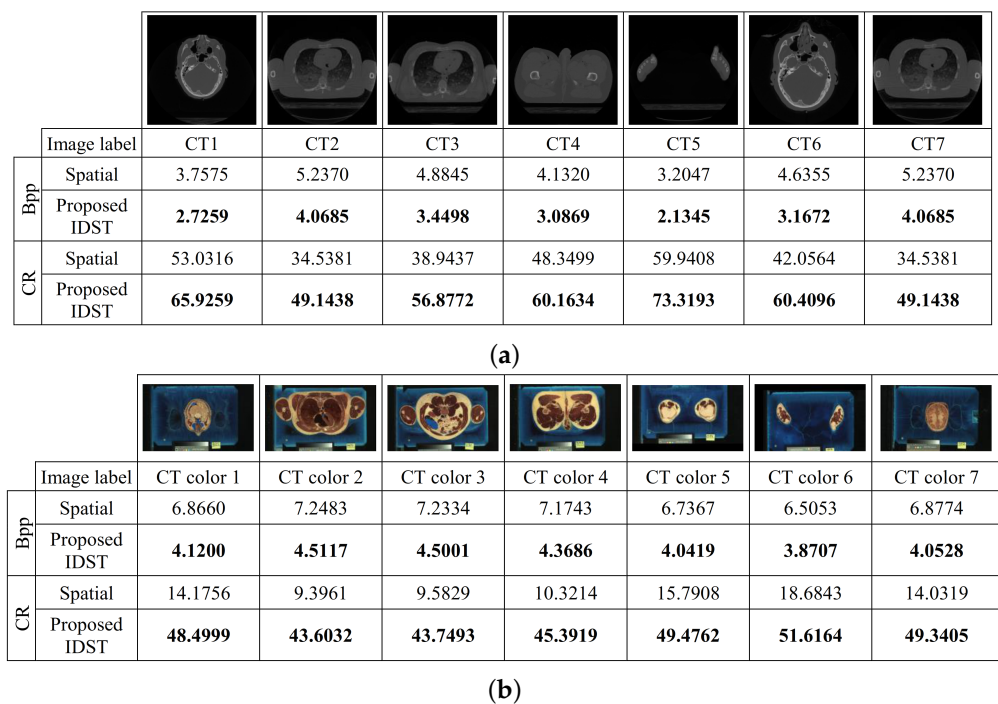


Figure 8. *Bpp* and *CR* values corresponding to (a) grayscale and (b) color medical images lossless compressed in the spatial and *IDST* domains.

The following test is intended to compare the performance of the proposed *IDST* versus existing integer transforms, namely, the integer discrete cosine transform (IDCT), the integer discrete Tchebichef transform (IDTT), and the integer discrete wavelet transform (IDWT). Our scheme illustrated in Figure 6 is used to carry out the current experiment. In fact, each integer transformation type is applied to the input test image. Next, the same steps illustrated in Figure 6 are followed to achieve the compressed image. Finally, the *Bpp* value is computed for each image by using the various transformations. The test images in the current test are the same ones seen in Figure 8. The current test outcomes are presented in Figure 9. The latter show that the lowest *Bpp* scores for all the test images (both color and grayscale) are achieved by using the proposed *IDST* and by the existing IDCT. In fact, on the one hand, we can remark that the proposed *IDST* produces competitive results to those achieved by IDCT. On the other hand, we can notice that *IDST* outperforms IDTT and IWT in terms of *Bpp*. These results provide a clear sign of the effectiveness of the proposed *IDST* for lossless image compression application.

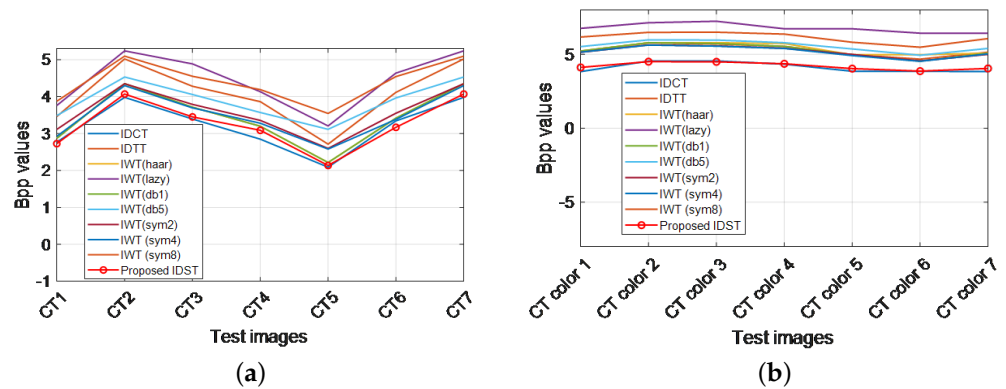


Figure 9. Comparison in terms of *Bpp* values between the proposed *IDST* and existing integer-based transformations used for lossless compression of (a) grayscale CT images and (b) color ones.

Once the effectiveness of the proposed *IDST* has been validated for lossless medical image compression, subsequent experimental analyses are carried out to validate the security level of the proposed scheme. To this end, several security analyses are performed in terms of security key space, histogram analysis, and sensitivity analysis of the security key components, etc.

7.3. Security Key Space Analysis

Key space analysis is conducted for showing the ability of our security scheme in resisting brute-force attacks. Indeed, the key space must exceed 2^{100} to withstand strong brute-force cyber attacks by using modern computers [58]. By considering the precision 2^{15} of floating values as well as the sensitivity level of each component that composes the security key of our scheme, the security key space of our scheme is about $10^{12 \times 4 + 10 \times 3 + 11} = 10^{89} \simeq 2^{295}$. This space far exceeds the recommended security key space mentioned above. Hence, the suggested compression–encryption scheme is able to provide a high degree of robustness against brute-force attacks.

7.4. Histogram Analysis

The image histogram provides statistical information regarding an input medical image. Indeed, such information can be analyzed by specific software in order to obtain useful information regarding the content of this image without the need for displaying its visual content. Therefore, the cancellation of input image statistical information is considered as an essential characteristic to be satisfied by compression–encryption schemes to prevent attacks based on statistics. In order to demonstrate the ability of our system to hide statistical information of color and grayscale medical images, the current analysis is established. For this purpose, grayscale medical images and color ones are selected from the datasets in [59,60], respectively. These images are compressed–encrypted by our scheme. Next, both the input images and their compressed–encrypted versions with the corresponding histograms are shown in Figures 10 and 11.

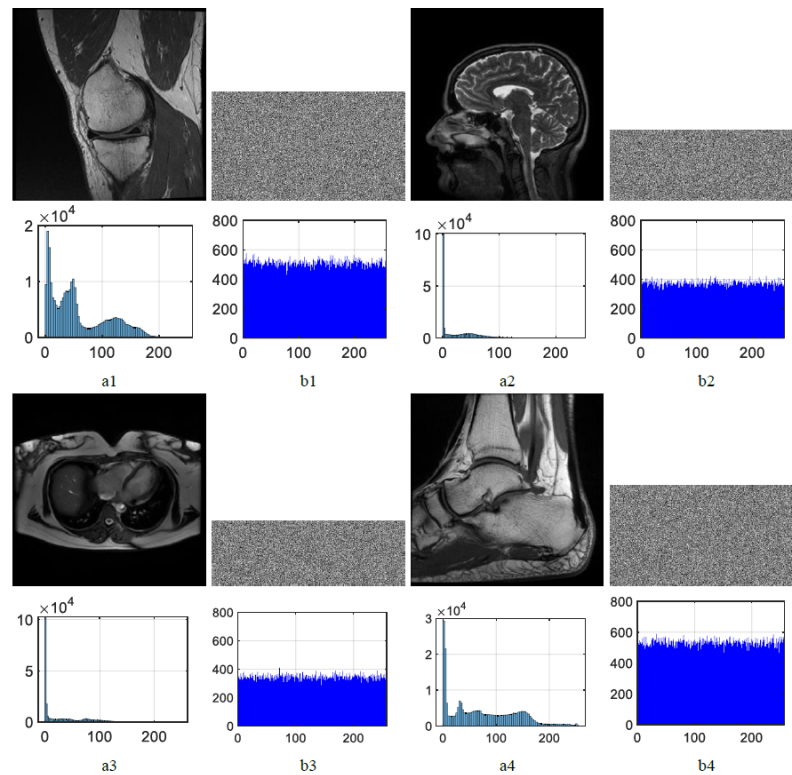


Figure 10. (a1–a4) Original grayscale medical images with size 512×512 with their corresponding histograms. (b1–b4) The compressed–encrypted versions of (a1–a4), respectively, and their histograms.

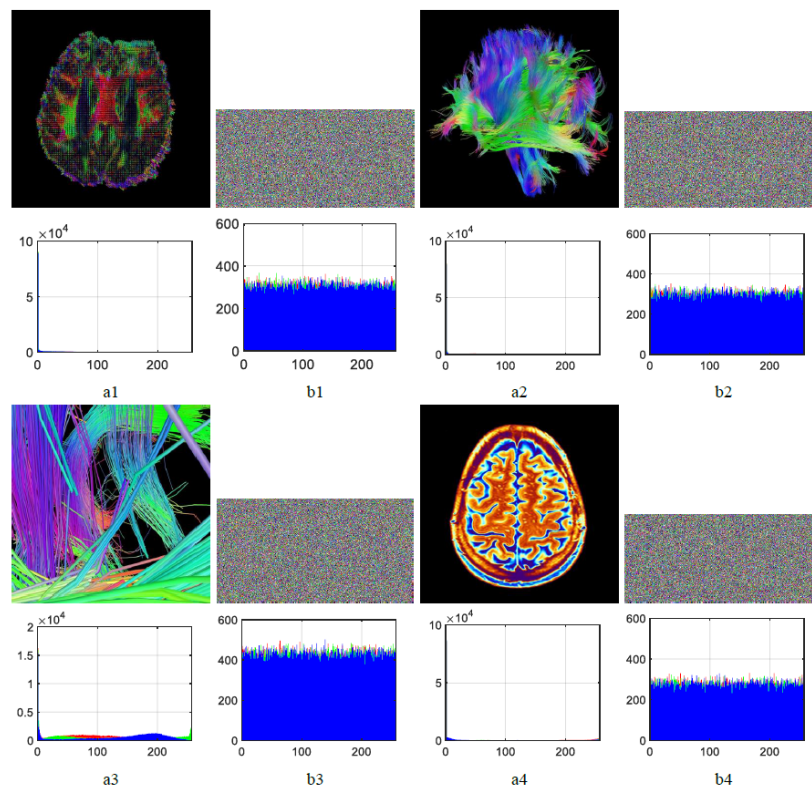


Figure 11. (a1–a4) Original color medical images of size 512×512 with their corresponding histograms. (b1–b4) The compressed–encrypted versions of (a1–a4), respectively, and their histograms.

The results shown in Figures 10 and 11 indicate that the compressed-encrypted images have flat histograms. By comparing these histograms with those of the original images, we can see the significant difference between them. Accordingly, our scheme succeeds in concealing the statistical information of the input images, indicating that no useful information can be obtained by analyzing the histograms of the compressed-encrypted images. In other words, unauthorized IoMT users are unable to extract any useful information via the analysis of the compressed-encrypted image histograms.

7.5. Correlation Analysis

Obviously, medical images include information redundancy, implying a high correlation between adjacent pixels. Since the proposed scheme includes a lossless compression phase, so it is assumed that this scheme is capable of greatly reducing the correlation between adjacent pixels. To quantify the correlation between neighboring pixels, the following correlation coefficient (CC) criterion can be used:

$$CC = \frac{C(x_1, x_2)}{\sqrt{V(x_1)}\sqrt{V(x_2)}} \tag{27}$$

where $C(x_1, x_2)$ is the covariance value of two adjacent vectors (x_1 and x_2). $V(x_1)$ and $V(x_2)$ are the variance of x_1 and x_2 .

To assess the correlation between the original images with their encrypted-compressed forms, 4000 samples are arbitrarily selected from adjacent pixels in the test images (Figure 12), which are selected from the dataset in [59]. The results presented in Figure 13 and Table 2 show that the proposed scheme is able to break the existing correlation between adjacent pixels in the original images. This indicates that our scheme not only offers lossless compression, but also guarantees the low correlation between the pixels in its output images.

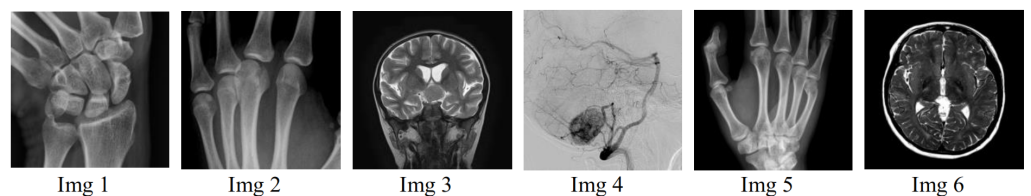


Figure 12. Grayscale medical images used in the test.

Table 2. Absolute CC values in the horizontal, vertical and diagonal direction of the input medical images and their compressed-encrypted forms.

Image	Direction	Img 1	Img 2	Img 3	Img 4	Ima 5	Img 6	Average
Input Images	Horizontal	0.9880	0.9914	0.9814	0.9705	0.9780	0.9415	0.9751
	Vertical	0.9903	0.9975	0.9850	0.9837	0.9910	0.9766	0.9874
	Diagonal	0.9953	0.9902	0.9671	0.9806	0.9865	0.9659	0.9809
Compressed-encrypted images	Horizontal	0.0031	0.0011	0.0106	0.1054	0.0161	0.0335	0.0133
	Vertical	0.0021	0.0121	0.0038	0.0320	0.0003	0.0085	0.0098
	Diagonal	0.0206	0.0303	0.0232	0.0264	0.0149	0.0165	0.0132

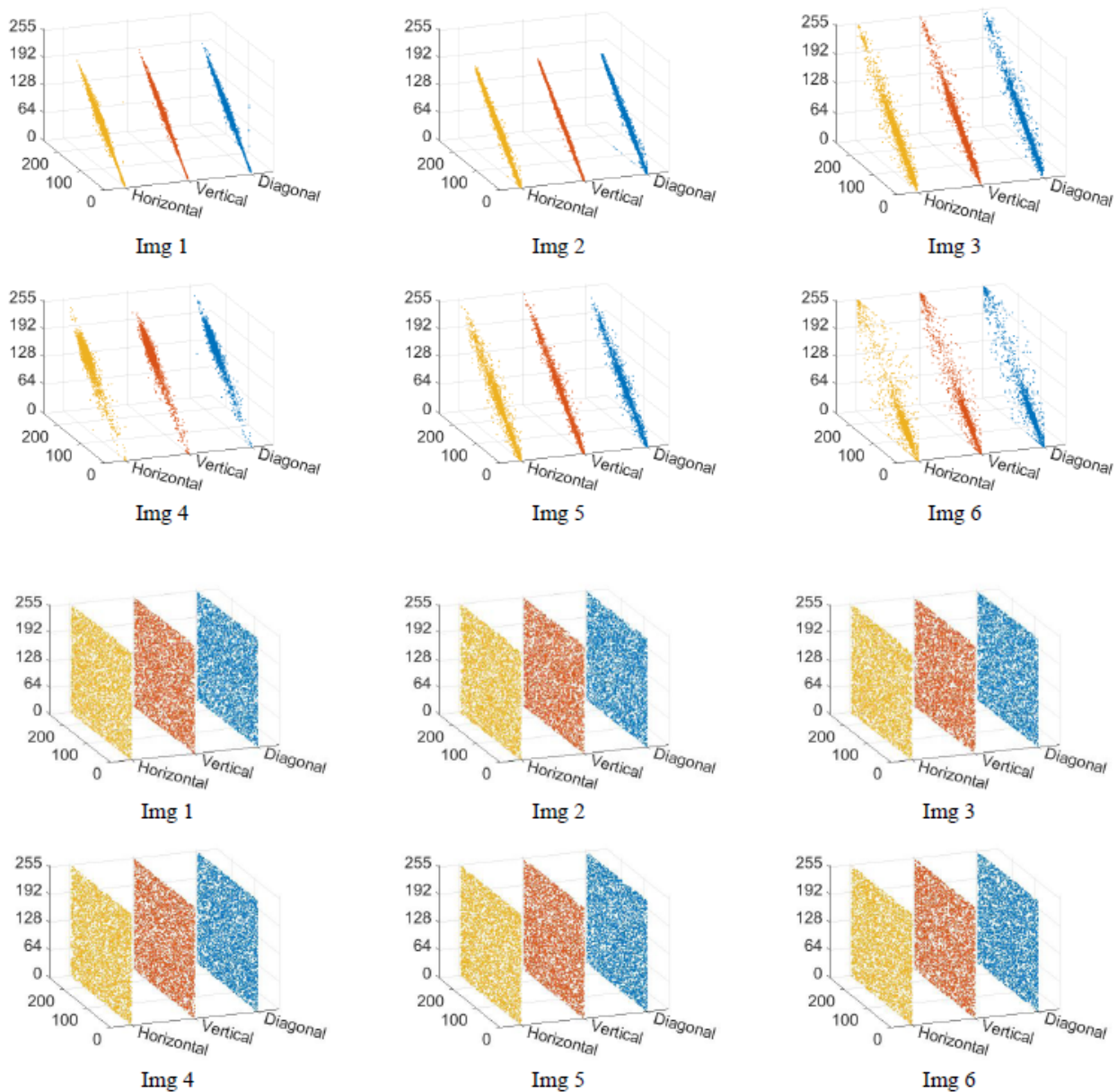


Figure 13. CC corresponding to the original Img 1–Img 6 (see Figure 12) and their compressed–encrypted versions, respectively.

7.6. Key Sensitivity Analysis

The current analysis is performed to show the effect of any slight modification of the proposed scheme’s key elements on the decompressed–decrypted image. To this end, the test images shown in Figure 11 are compressed–decrypted by our scheme using the following key $(x_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7, \lambda_8) = (0.4, 7, 5, 0, 1, 8, 9, 10, 2)$. In the decompression–decryption phase, the components of the key used are slightly varied, and the decompressed–decrypted images are then shown in Figure 14. This figure visualizes that any slight variation in the security key components by $\Delta \in [10^{-10} \dots 10^{-12}]$ results in the inability to retrieve the original images, which means that the proposed M-PWLCM can guarantee the highest security standards when communicating medical compressed images over IoMTs.

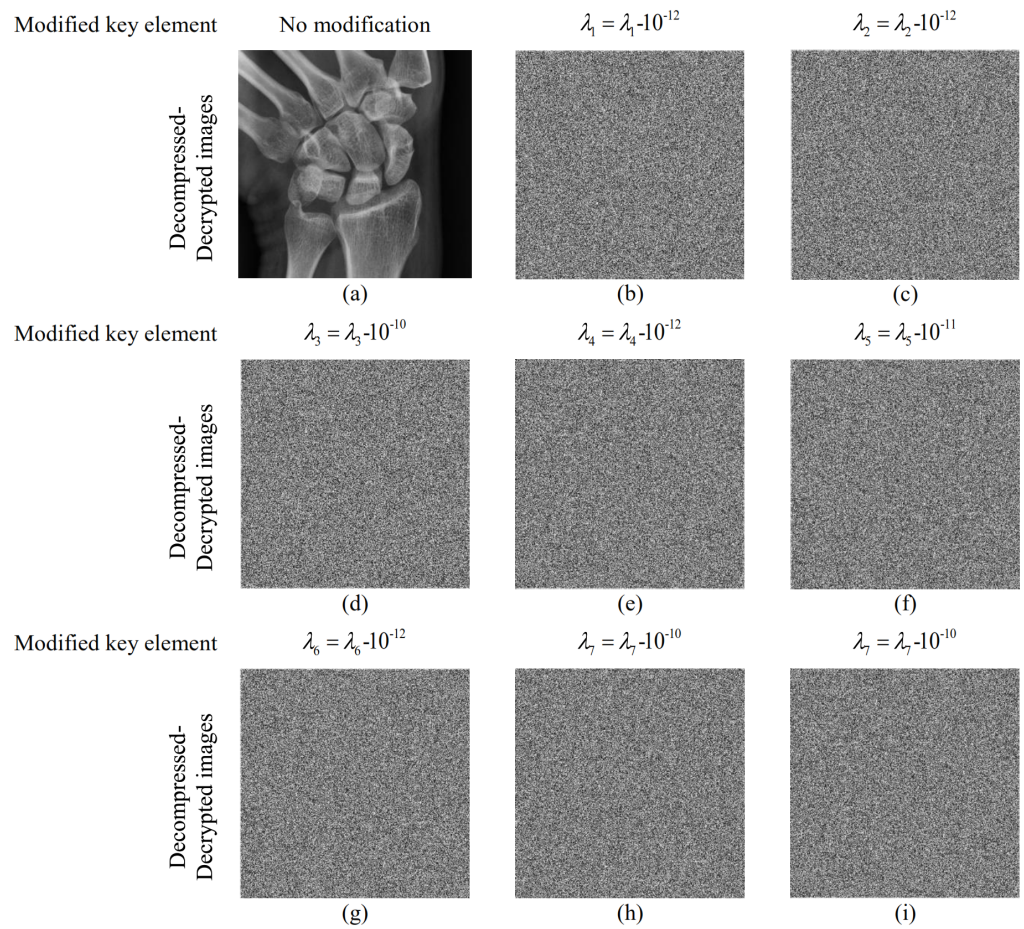


Figure 14. (a) Decompressed–decrypted Img 1 using the valid security key. (b–i) Decompressed–decrypted Img 1 using invalid security keys.

7.7. Differential Attack Analysis

Differential attacks can be used by IoMT attackers in their attempt to crack encryption schemes. To evaluate the effectiveness of our scheme in resisting such attacks, the Number of Pixels Change Rate (NPCR) and the Unified Average Modified Intensity (UACI) are used as standard evaluation criteria. NPCR and UACI are defined by Equations (28) and (29), respectively [61].

$$UACI = \frac{\sum_{i,j} |\text{Img}_{i,j} - \text{Img}'_{i,j}|}{255 \times H \times W} \times 100; i = 1, \dots, N \text{ and } j = 1, \dots, M \quad (28)$$

$$NPCR = 100 \times \frac{\sum_{i,j} Dif_{i,j}}{N \times M} \quad (29)$$

with $Dif_{i,j} = \begin{cases} 0 & \text{if } \text{Img}_{i,j} = \text{Img}'_{i,j} \\ 1 & \text{if } \text{Img}_{i,j} \neq \text{Img}'_{i,j} \end{cases}$

where $\text{Img}_{i,j}$ is the input medical image and $\text{Img}'_{i,j}$ is the compressed–encrypted version of the input image.

The analysis test carried out in the previous subsection indicates that any minor variation of the key components causes non-recuperation of the input image. This benefit is exploited to resist brute-force attacks as follows:

- Set a constant of low value: $\Delta = \mp 10^{-10}$.
- Select a key parameter (e.g., λ_3) and add Δ to this parameter ($\lambda_3^* = \lambda_3 + \Delta$).

- Use the proposed scheme for compression–encryption of the first medical image in the dataset by using the user-selected security key containing the modified parameter (λ_3^*).
- Update λ_3^* element by $\lambda_3^* = \lambda_3^* + \Delta$.
- Apply compression–encryption to the second medical image in the dataset, and so on until the proposed scheme is applied to the entire dataset.

The above steps are designed to ensure that each image in the dataset is compressed–encrypted with a unique security key. That is, the same image file produces entirely different cipher-texts after being compressed–encrypted in two distinct iterations of our algorithm.

To evaluate the validity of the above procedure to withstand differential attacks, the test images shown in Figure 15 are compressed–encrypted in two consecutive iterations of our scheme. Then, *NPCR* and *UACI* are computed for the output images. The comparison of *NPCR* and *UACI* values produced through our scheme with those reported in [61], leads to the conclusion that the proposed scheme is indeed effective in resisting differential attacks.

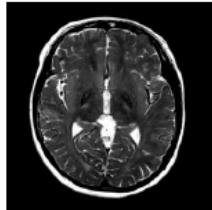
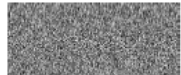


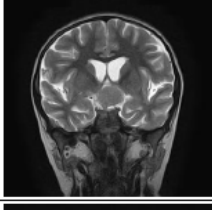



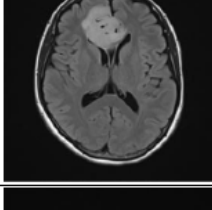
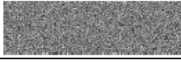
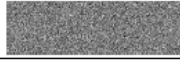
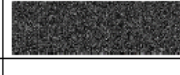
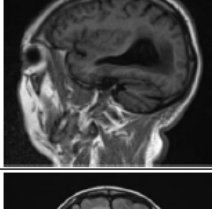



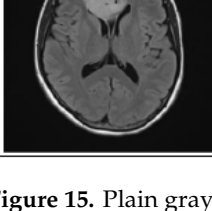



Original images	Compressed-Encrypted image		Absolute difference $ I1-I2 $	NPCR	UACI
	Iteration 1 (I1)	Iteration 2 (I2)			
				99.60	33.46
				99.61	33.47
				99.61	33.43
				99.64	33.43
				99.63	33.42

Figure 15. Plain grayscale medical images of size 512×512 and their corresponding compressed–encrypted forms and the values of *NPCR* and *UACI*.

7.8. Runtime Analysis

The aim of the current analysis is to measure the average execution time of the main phases of the proposed scheme. To this end, 100 grayscale and color medical images of different sizes (Figure 16) are selected from the [62] dataset and then used in the experiments. Each test image is compressed–encrypted by the proposed scheme. Next, the average runtime is measured for 10 executions of the next phases involved in the suggested scheme: (i) pre-processing and IDST computation, (ii) Huffman and binary-to-decimal encoding, and (iii) the encryption process. Table 3 lists details concerning the runtime of the proposed compression–encryption core steps, and Figure 17 illustrates the percentage of these steps for images of different dimensions.

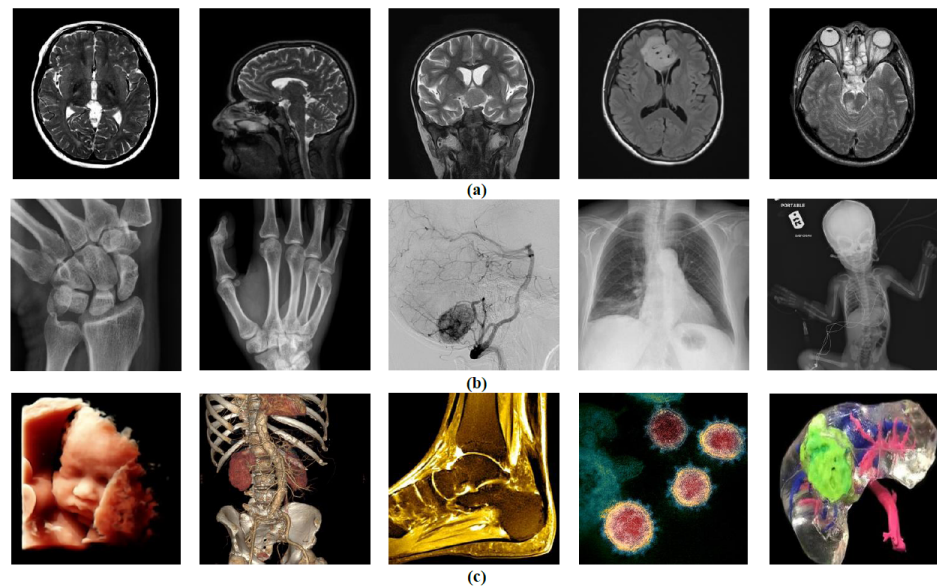


Figure 16. Set of (a–b) grayscale and (c) color medical test images of various dimensions.

Table 3. Runtime (seconds) of core steps of the proposed compression–encryption scheme.

Size of Images	Compression–Encryption Phase			Total Runtime
	Pre-Processing and IDST	Huffman and Binary-to-Integer Coding	Encryption Process	
512 × 512	0.3283	5.7249	0.0472	6.1004
1024 × 1024	1.0310	15.4158	0.1106	16.5574
1024 × 1024 × 3	3.0532	46.2225	0.3320	49.6077

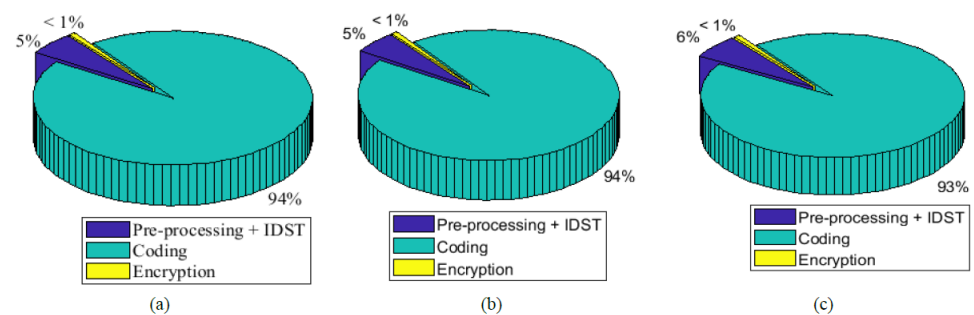


Figure 17. Detailed execution time percentage for the main compression–encryption steps for grayscale medical images of size (a) 512 × 512, (b) 1024 × 1024, and color ones of size (c) 1024 × 1024 × 3.

Table 3 shows that the execution time increases with the increase in the input image size, and from Figure 17, we can see that the most time-consuming step is the coding process (Huffman and binary-to-integer coding), which takes up around 94% of the total compression–encryption runtime. Accordingly, future work will focus on reducing the runtime of our scheme to make it more cost-effective and responsive to real-time processing.

7.9. Comparison Analysis

The first comparison is performed between the security key capacity of the proposed system and similar systems presented in [9,37–40]. The key spaces of the compared schemes, including the suggested one, are listed in Table 4. The comparison provided in the table shows that the work conducted in [9,37,40], omitted the key-space analysis. It is therefore not possible to assess the security level of the presented compression–encryption schemes against brute-force attacks. Furthermore, when comparing the proposed scheme with the ones presented in citezhang2015medical,selvi2021modified, it becomes apparent that our scheme provides a larger key space and therefore higher robustness to brute-force attacks than [38,39].

Table 4. Comparison, in terms of key space, between the proposed scheme and other similar ones.

Scheme	Proposed Scheme	[37]	[38]	[9]	[40]	[39]
Key space	2^{295}	-	2^{202}	-	-	2^{128}

The following comparison focuses on the comparison of *PSNR* values generated by different compression–encryption schemes. For this purpose, we use the proposed scheme for compression–encryption of test images, thus obtaining specific *CR* values. Next, the compared compressive sensing-based schemes reported in [9,38,40] are adopted to reach the same *CR* as that obtained by the proposed scheme. Finally, the *PSNR* values corresponding to the decompressed–decrypted images are indicated in Table 5. This table reveals that our scheme outperforms the comparative ones, achieving a *PSNR* = *Inf*. This finding is due to the fact that our scheme performs lossless image compression–encryption. On the other hand, the compared schemes lead to certain degradation of the input image after the decompression and decryption phases.

Table 5. Comparison in terms of *PSNR* between the proposed scheme and similar ones.

	Images	Img1	Img2	Img3	Img4	Img5	Img6	Average
<i>PSNR</i>	CR(%)	51.47	52.04	50.27	49.02	58.63	55.33	52.79
	Proposed scheme	Inf	Inf	Inf	Inf	Inf	Inf	Inf
	Scheme [9]	35.36	34.15	35.16	35.66	36.17	37.96	35.74
	Scheme [38]	34.12	33.69	36.15	35.78	35.02	36.98	35.29
	Scheme [40]	57.16	58.17	60.02	59.16	58.16	57.06	58.28

The current comparison is also made between the suggested scheme and existing ones implemented in the spatial domain. Indeed, the comparison between the proposed scheme and those presented in [38,39] is carried out in terms of *CR*, as these schemes perform lossless compression–encryption. The results of the current comparative test are presented in Table 6. This table proves that our method outperforms the comparable schemes in terms of *CR*. This result can be explained by the fact that the proposed system is implemented in the transformation domain using *IDST*. In contrast, the comparable [38,39] schemes are implemented in the spatial domain. The transformation-based implementation is commonly known for its superior performance compared to the spatial-based compression.

Table 6. Comparison in terms of CR between the proposed scheme and similar ones.

	Images	Img1	Img2	Img3	Img4	Img5	Img6	Average
CR	Proposed scheme	51.47	52.04	50.27	49.02	58.63	55.33	52.79
	Scheme [37]	36.12	34.25	33.96	32.10	35.02	36.72	34.69
	Scheme [39]	30.02	31.36	32.17	33.52	32.71	30.85	31.77

In the following comparison, the performance of the proposed *IDST* is compared with existing integer discrete transforms, including IDCT, IDTT, and IDWT. The comparison is carried out in terms of the *Bpp* criterion. To do this, standard 256×256 grayscale images are selected from the dataset in [63]. Figure 18 shows the test images and their corresponding *Bpp* values achieved by the compared methods. This figure shows that the lowest *Bpp* values are obtained with both IDCT and the proposed *IDST*, confirming that the suggested transform is not only useful for lossless compression of medical images, but also for other types of images.


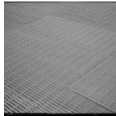


							Average
Proposed (IDST)	5.1844	4.5069	6.3552	5.2335	4.9264	5.1122	5.2198
IDCT	5.1214	4.4834	6.3360	5.2259	4.9304	5.1214	5.2031
IDTT	7.1200	6.2459	7.9828	7.0950	6.6600	6.8173	6.9868
IWT ('haar')	6.4990	6.1664	7.2578	6.6971	6.2857	6.4523	6.5597
IWT ('lazy')	6.9324	7.2798	7.7252	6.0468	7.4559	6.7621	7.0337
IWT ('db2')	6.4573	5.6956	7.1131	6.5598	6.0523	6.3091	6.3645
IWT ('sym4')	6.5065	5.6630	7.2090	6.6084	6.0572	6.3391	6.3972

Figure 18. Comparison in terms of *Bpp* values between the proposed *IDST* and existing integer-based transformations used for lossless compression of standard grayscale images.

8. Conclusions

In this work, we have introduced a new type of reversible transforms called *IDST*, which enables integer-to-integer coding for reversible image processing applications. Next, a new 1D chaotic system called M-PWLCM is developed as an extension of the existing 1D PWLCM. The introduced M-PWLCM has eight control parameters defined over an unlimited range. In contrast, its original version contains only one control parameter defined over a limited range. To demonstrate the pertinence of *IDST* and M-PWLCM, they are deployed in a new scheme for joint lossless compression and encryption of medical images in IoMTs. The proposed scheme has demonstrated an excellent performance in terms of achieving higher compression ratios and higher levels of security when communicating compressed medical images over IoMTs. Furthermore, the results of the comparative analysis highlighted the superiority of our scheme over existing ones in terms of both security level and compression ratio. Despite the good performance of our scheme, it is still limited by certain drawbacks, notably the relatively high execution time due to the use of Huffman coding. In addition, our scheme is not robust to noise and data loss. These issues are open questions that require further investigation in future work. In addition, other moment-based integer transformations should be introduced and studied in future work for reversible data applications.

Author Contributions: Conceptualization, A.D. and H.M.; methodology, A.D. and H.M.; software, M.Y. and A.A.A.E.-L.; formal analysis, M.Y., Q. Li and A.A.A.E.-L.; investigation, O.A. and A.A.A.E.-L.; resources, M.Y. and O.A.; Supervision, Q. Li and A.A.A.E.-L writing—original draft, A.D. and H.M.; writing—review & editing, Q.L. and A.A.A.E.-L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Researchers Supporting Project Number (RSP2023R102) King Saud University, Riyadh, Saudi Arabia. This research was also funded by the National Natural Science Foundation of China (grant number 62071151).

Data Availability Statement: The data are available upon request from the corresponding author.

Acknowledgments: This work was supported by the Researchers Supporting Project Number (RSP2023R102) King Saud University, Riyadh, Saudi Arabia. This research was also supported by the National Natural Science Foundation of China (grant number 62071151). Ahmed A. Abd El-Latif also acknowledges the Talented Young Scientist Program in China: TYSP for their support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dwivedi, R.; Mehrotra, D.; Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofacial Res.* **2022**, *12*, 302–318. [\[CrossRef\]](#)
2. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A survey on the edge computing for the Internet of Things. *IEEE Access* **2017**, *6*, 6900–6919. [\[CrossRef\]](#)
3. Sun, Y.; Lo, F.P.W.; Lo, B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access* **2019**, *7*, 183339–183355. [\[CrossRef\]](#)
4. Thomasian, N.M.; Adashi, E.Y. Cybersecurity in the internet of medical things. *Health Policy Technol.* **2021**, *10*, 100549. [\[CrossRef\]](#)
5. Zuo, Z.; Lan, X.; Deng, L.; Yao, S.; Wang, X. An improved medical image compression technique with lossless region of interest. *Optik* **2015**, *126*, 2825–2831. [\[CrossRef\]](#)
6. Mouradian, C.; Naboulsi, D.; Yangui, S.; Glitho, R.H.; Morrow, M.J.; Polakos, P.A. A comprehensive survey on fog computing: State-of-the-art and research challenges. *IEEE Commun. Surv. Tutorials* **2017**, *20*, 416–464. [\[CrossRef\]](#)
7. Daoui, A.; Yamni, M.; Karmouni, H.; Sayyouri, M.; Qjidaa, H. Efficient reconstruction and compression of large size ECG signal by Tchebichef moments. In Proceedings of the 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), Fez, Morocco, 9–11 June 2020; pp. 1–6.
8. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Secur. Appl.* **2023**, *1*, 100016. [\[CrossRef\]](#)
9. Raja, S. Joint medical image compression–encryption in the cloud using multiscale transform-based image compression encoding techniques. *Sādhanā* **2019**, *44*, 28. [\[CrossRef\]](#)
10. Hajjaji, M.A.; Dridi, M.; Mtibaa, A. A medical image crypto-compression algorithm based on neural network and PWLCM. *Multimed. Tools Appl.* **2019**, *78*, 14379–14396. [\[CrossRef\]](#)
11. Sutherland, J.; Belec, J.; Sheikh, A.; Chepelev, L.; Althobaity, W.; Chow, B.J.; Mitsouras, D.; Christensen, A.; Rybicki, F.J.; La Russa, D.J. Applying modern virtual and augmented reality technologies to medical images and models. *J. Digit. Imaging* **2019**, *32*, 38–53. [\[CrossRef\]](#)
12. Devaraj, S.J. Emerging paradigms in transform-based medical image compression for telemedicine environment. In *Telemedicine Technologies*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 15–29.
13. Li, Z.; Ramos, A.; Li, Z.; Osborn, M.L.; Zaid, W.; Li, X.; Li, Y.; Xu, J. Nearly-lossless-to-lossy medical image compression by the optimized JPEGXT and JPEG algorithms through the anatomical regions of interest. *Biomed. Signal Process. Control* **2023**, *83*, 104711. [\[CrossRef\]](#)
14. Ghazvinian Zanjani, F.; Zinger, S.; Piepers, B.; Mahmoudpour, S.; Schelkens, P.; de With, P.H. Impact of JPEG 2000 compression on deep convolutional neural networks for metastatic cancer detection in histopathological images. *J. Med. Imaging* **2019**, *6*, 027501. [\[CrossRef\]](#)
15. Brahimi, T.; Khelifi, F.; Kacha, A. An efficient JPEG-2000 based multimodal compression scheme. *Multimed. Tools Appl.* **2021**, *80*, 21241–21260. [\[CrossRef\]](#)
16. Liu, F.; Hernandez-Cabronero, M.; Sanchez, V.; Marcellin, M.W.; Bilgin, A. The current role of image compression standards in medical imaging. *Information* **2017**, *8*, 131. [\[CrossRef\]](#)
17. Anastassopoulos, G.K.; Skodras, A. JPEG2000 ROI coding in medical imaging applications. In Proceedings of the IASTED International Conference on Visualisation, Imaging and Image Processing (VIIP2002), Marbella, Spain, 9–12 September 2002; pp. 783–788.
18. Li, Z.; Ramos, A.; Li, Z.; Osborn, M.L.; Li, X.; Li, Y.; Yao, S.; Xu, J. An optimized JPEG-XT-based algorithm for the lossy and lossless compression of 16-bit depth medical image. *Biomed. Signal Process. Control* **2021**, *64*, 102306. [\[CrossRef\]](#)
19. Lalitha, Y.; Latte, M. Lossless and lossy compression of DICOM images with scalable ROI. *Int. J. Comput. Sci. Netw. Secur.* **2010**, *10*, 276–281.
20. Weinberger, M.J.; Seroussi, G.; Sapiro, G. The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS. *IEEE Trans. Image Process.* **2000**, *9*, 1309–1324. [\[CrossRef\]](#)

21. Wu, X.; Memon, N. CALIC-a context based adaptive lossless image codec. In Proceedings of the 1996 IEEE International Conference on Acoustics, Speech, and Signal Processing Conference Proceedings, Atlanta, GA, USA, 9 May 1996; Volume 4, pp. 1890–1893.
22. Xiao, B.; Lu, G.; Zhang, Y.; Li, W.; Wang, G. Lossless image compression based on integer Discrete Tchebichef Transform. *Neurocomputing* **2016**, *214*, 587–593. [[CrossRef](#)]
23. Suzuki, T.; Ikehara, M. Integer DCT based on direct-lifting of DCT-IDCT for lossless-to-lossy image coding. *IEEE Trans. Image Process.* **2010**, *19*, 2958–2965. [[CrossRef](#)]
24. Chen, Y.; Hao, P. Integer reversible transformation to make JPEG lossless. In Proceedings of the 7th International Conference on Signal Processing, Beijing, China, 31 August–4 September 2004; Volume 1, pp. 835–838.
25. Chen, Y.J.; Oraintara, S.; Nguyen, T. Video compression using integer DCT. In Proceedings of the 2000 International Conference on Image Processing (Cat. No. 00CH37101), Vancouver, BC, Canada, 10–13 September 2000; Volume 2, pp. 844–845.
26. Dai, H.N.; Wu, Y.; Wang, H.; Imran, M.; Haider, N. Blockchain-empowered edge intelligence for internet of medical things against COVID-19. *IEEE Internet Things Mag.* **2021**, *4*, 34–39. [[CrossRef](#)]
27. Daoui, A.; Yamni, M.; Karmouni, H.; Sayyouri, M.; Qjidaa, H.; Motahhir, S.; Jamil, O.; El-Shafai, W.; Algarni, A.D.; Soliman, N.F.; et al. Efficient Biomedical Signal Security Algorithm for Smart Internet of Medical Things (IoMTs) Applications. *Electronics* **2022**, *11*, 3867. [[CrossRef](#)]
28. Pirbhulal, S.; Samuel, O.W.; Wu, W.; Sangaiah, A.K.; Li, G. A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Gener. Comput. Syst.* **2019**, *95*, 382–391. [[CrossRef](#)]
29. Sammoud, A.; Chalouf, M.A.; Hamdi, O.; Montavont, N.; Bouallegue, A. A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis. *Comput. Secur.* **2020**, *96*, 101838. [[CrossRef](#)]
30. Ogundokun, R.O.; Awotunde, J.B.; Adeniyi, E.A.; Ayo, F.E. Crypto-Stegno based model for securing medical information on IOMT platform. *Multimed. Tools Appl.* **2021**, *80*, 31705–31727. [[CrossRef](#)]
31. Abdulbaqi, A.S.; Obaid, A.J.; Abdulameer, M.H. Smartphone-based ECG signals encryption for transmission and analyzing via IoMTs. *J. Discret. Math. Sci. Cryptogr.* **2021**, *24*, 1979–1988. [[CrossRef](#)]
32. Laiphrakpam, D.S.; Thingbaijam, R.; Singh, K.M.; Al Awida, M. Encrypting multiple images with an enhanced chaotic map. *IEEE Access* **2022**, *10*, 87844–87859. [[CrossRef](#)]
33. Daoui, A.; Yamni, M.; Chelloug, S.A.; Wani, M.A.; El-Latif, A.A.A. Efficient image encryption scheme using novel 1D multiparametric dynamical tent map and parallel computing. *Mathematics* **2023**, *11*, 1589. [[CrossRef](#)]
34. Cao, W.; Cai, H.; Hua, Z. n-Dimensional Chaotic Map with application in secure communication. *Chaos Solitons Fractals* **2022**, *163*, 112519. [[CrossRef](#)]
35. Erkan, U.; Toktas, A.; Lai, Q. 2D hyperchaotic system based on Schaffer function for image encryption. *Expert Syst. Appl.* **2023**, *213*, 119076. [[CrossRef](#)]
36. Liu, L.; Wang, J. A cluster of 1D quadratic chaotic map and its applications in image encryption. *Math. Comput. Simul.* **2023**, *204*, 89–114. [[CrossRef](#)]
37. Selvi, C.T.; Amudha, J.; Sudhakar, R. Medical image encryption and compression by adaptive sigma filtered synorr certificateless signcryptive Levenshtein entropy-coding-based deep neural learning. *Multimed. Syst.* **2021**, *27*, 1059–1074. [[CrossRef](#)]
38. Zhang, L.B.; Zhu, Z.L.; Yang, B.Q.; Liu, W.Y.; Zhu, H.F.; Zou, M.Y. Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach. *Math. Probl. Eng.* **2015**, *2015*, 940638. [[CrossRef](#)]
39. Selvi, C.T.; Amudha, J.; Sudhakar, R. A modified salp swarm algorithm (SSA) combined with a chaotic coupled map lattices (CML) approach for the secured encryption and compression of medical images during data transmission. *Biomed. Signal Process. Control* **2021**, *66*, 102465. [[CrossRef](#)]
40. Wang, L.; Li, L.; Li, J.; Li, J.; Gupta, B.B.; Liu, X. Compressive sensing of medical images with confidentially homomorphic aggregations. *IEEE Internet Things J.* **2018**, *6*, 1402–1409. [[CrossRef](#)]
41. González, G.; Nava, R.; Escalante-Ramírez, B. A comparative study on discrete Shmaliy moments and their texture-based applications. *Math. Probl. Eng.* **2018**, *2018*, 1673283. [[CrossRef](#)]
42. Asli, B.H.S.; Flusser, J. New discrete orthogonal moments for signal analysis. *Signal Process.* **2017**, *141*, 57–73. [[CrossRef](#)]
43. Daoui, A.; Karmouni, H.; Sayyouri, M.; Qjidaa, H. New method for bio-signals zero-watermarking using quaternion shmaliy moments and short-time fourier transform. *Multimed. Tools Appl.* **2022**, *81*, 17369–17399. [[CrossRef](#)]
44. Koekoek, R.; Lesky, P.A.; Swarttouw, R.F.; Koekoek, R.; Lesky, P.A.; Swarttouw, R.F. *Hypergeometric Orthogonal Polynomials*; Springer: Berlin/Heidelberg, Germany, 2010.
45. Hao, P.; Shi, Q. Matrix factorizations for reversible integer mapping. *IEEE Trans. Signal Process.* **2001**, *49*, 2314–2324.
46. Zhou, H.; Ling, X.T.; Yu, J. Secure communication via one-dimensional chaotic inverse systems. In Proceedings of the 1997 IEEE International Symposium on Circuits and Systems (ISCAS), Hong Kong, China, 12 June 1997; Volume 2, pp. 1029–1032.
47. Hermassi, H.; Rhouma, R.; Belghith, S. Joint compression and encryption using chaotically mutated Huffman trees. *Commun. Nonlinear Sci. Numer. Simul.* **2010**, *15*, 2987–2999. [[CrossRef](#)]
48. Tseng, K.K.; Jiang, J.M.; Pan, J.S.; Tang, L.L.; Hsu, C.Y.; Chen, C.C. Enhanced Huffman coding with encryption for wireless data broadcasting system. In Proceedings of the 2012 International Symposium on Computer, Consumer and Control, Taichung, Taiwan, 4–6 June 2012; pp. 622–625.

49. Yuan, S.; Hu, J. Research on image compression technology based on Huffman coding. *J. Vis. Commun. Image Represent.* **2019**, *59*, 33–38. [[CrossRef](#)]
50. Gormish, M.J.; Schwartz, E.L.; Keith, A.F.; Boliek, M.P.; Zandi, A. Lossless and nearly lossless compression for high-quality images. *Proc. Very High Resolut. Qual. Imaging II* **1997**, *3025*, 62–70.
51. Daoui, A.; Yamni, M.; Karmouni, H.; Sayyouri, M.; Qjidaa, H. Stable computation of higher order Charlier moments for signal and image reconstruction. *Inf. Sci.* **2020**, *521*, 251–276. [[CrossRef](#)]
52. Daoui, A.; Yamni, M.; Karmouni, H.; Sayyouri, M.; Qjidaa, H.; Ahmad, M.; Abd El-Latif, A.A. Biomedical Multimedia encryption by fractional-order Meixner polynomials map and quaternion fractional-order Meixner moments. *IEEE Access* **2022**, *10*, 102599–102617. [[CrossRef](#)]
53. Daoui, A.; Karmouni, H.; Sayyouri, M.; Qjidaa, H. Fast and stable computation of higher-order Hahn polynomials and Hahn moment invariants for signal and image analysis. *Multimed. Tools Appl.* **2021**, *80*, 32947–32973. [[CrossRef](#)] [[PubMed](#)]
54. Daoui, A.; Karmouni, H.; Yamni, M.; Sayyouri, M.; Qjidaa, H. On computational aspects of high-order dual Hahn moments. *Pattern Recognit.* **2022**, *127*, 108596. [[CrossRef](#)]
55. Daoui, A.; Karmouni, H.; Sayyouri, M.; Qjidaa, H. Stable analysis of large-size signals and images by Racah’s discrete orthogonal moments. *J. Comput. Appl. Math.* **2022**, *403*, 113830. [[CrossRef](#)]
56. Alotaibi, R.A.; Elrefaei, L.A. Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT). *Appl. Comput. Infor.* **2019**, *15*, 191–202. [[CrossRef](#)]
57. The Visible Human Project. Available online: https://www.nlm.nih.gov/research/visible/frozen_ct.html (accessed on 27 July 2021).
58. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [[CrossRef](#)]
59. 3.0T GE Discovery 750W MRI Scanner Images. Available online: <https://medicine.uiowa.edu/mri/30t-ge-discovery-750w-mri-scanner-images> (accessed on 11 March 2022).
60. Human Connectome Project | Gallery. Available online: <http://www.humanconnectomeproject.org/gallery/> (accessed on 20 August 2021).
61. Wu, Y.; Noonan, J.P.; Agaian, S. NPCR and UACI randomness tests for image encryption. *Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun.* **2011**, *1*, 31–38.
62. Radiopaedia. Available online: <https://radiopaedia.org/> (accessed on 25 June 2023).
63. Standard Test Images. Available online: <https://ccia.ugr.es/cvg/dbimagenes/> (accessed on 25 June 2023).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.