International Journal of Mathematical, Engineering and Management Sciences
Vol. 10, No. 5, 1397-1426, 2025
https://doi.org/10.33889/IJMEMS.2025.10.5.066

Ram Arti Publishers

Compression Sensing Satellite Image Pixel Scrambling Scheme using Unique Seed Generation for Intra-Block Confusion with LP Rotation Mechanism

Ram Chandra Barik
Department of Computer Science & Engineering,
C.V. Raman Global University, 752054, Bhubaneswar, Odisha, India.
E-mail: ram.chandra@cgu-odisha.ac.in

Devendra Kumar Yadav
School of Computer Science and Engineering,
XIM University, 752050, Bhubaneswar, Odisha, India.
E-mail: devendra@xim.edu.in

Pragyan Mishra
Department of Computer Science and Engineering,
National Institute of Technology, 769008, Rourkela, Odisha, India.
Corresponding author: 920cs5007@nitrkl.ac.in

(Received on September 16, 2024; Revised on January 4, 2025 & March 16, 2025 & April 20, 2025; Accepted on April 27, 2025)

Abstract
Without image compression, encrypted satellite image remains too large and cumbersome, making timely transmission to ground stations impractical. During transmission from space to the ground station, satellite images undergo compression to reduce bandwidth usage and encryption to safeguard data integrity and prevent unauthorized access. The unauthorized access of satellite imagery poses significant risks, including security breaches, misinformation, and compromised decision-making. To protect the integrity and confidentiality of critical geospatial data used in defense, disaster management, and environmental monitoring, robust satellite image encryption is imperative. Existing algorithms often prioritize security at the expense of processing speed or data fidelity. This paper introduces a versatile scheme for the compression and encryption of satellite images, structured in three distinct phases. In the first phase, satellite images are divided into blocks, generating unique initial conditions (seeds) for each block as security keys using the chaotic Sin map. These conditions are subsequently utilized by blockwise independent Tent Maps to produce random chaotic coefficients, enabling complex pixel scrambling through an XOR-based confusion approach. In the second phase, remote sensing images are compressed using the first-level Lifting Wavelet Transform (LWT1), maintaining image fidelity. In the third phase, blockwise rotation is achieved using Lehmer PRNG (LP) to generate random numbers for circular pixel shifts, followed by classical RSA encryption applied to the rotated blocks for secure transmission. The proposed algorithm is lightweight, offering low computational complexity that is suitable for satellite systems and other imaging applications. The SinCrypTent encryption model provides a vast key space, effectively resisting brute force and other cyberattacks. Empirical validation of the model includes differential attack analysis, correlation analysis, entropy analysis, and comparative evaluation with recent state-of-the-art algorithms, demonstrating its superior efficacy in ensuring secure and efficient satellite image encryption.

Keywords- Lifting wavelet transform (LWT), Sin map, Tent map, RSA, Lehmer pseudo random number generator (LP).

1. Introduction

Satellite image embeds crucial information for monitoring of climate change, cyclone condition, earthquake condition, agriculture, environment pollution, military operation-based tracking, and diversified application areas. After acquisition with sophisticated cameras, the Satellite images are transmitted to ground station which may be vulnerable to cyber-attack as a national threat. Hence, securing satellite images is in greater essence during transmission. Two prime concerns for securing satellite images first one is image size aspect towards bandwidth concern and second one is encryption aspect. Hence, hybrid image compression and encryption algorithms are in greater need. However, a compression sensing image encryption algorithm

must be validated against some prominent security tests such as sensitivity analysis, key space analysis, correlation analysis, and entropy measurement. Histogram analysis to check for the equal pixel distribution before encryption and after encryption. Similarly, speed analysis are also major concerns to certify the security algorithms. Safeguard against the vulnerability aspect to be testified over brute-force attacks, differential attacks, and NIST test suite also offer validation metric. Classical security algorithm has its pros and cons. In Recent days, chaos-based security algorithms offer true dynamics and randomness especially for image encryption bearing many key characteristics such as initial conditions dependency. Even stochastic with unpredictability nature of chaotic system exhibit a deterministic system under deterministic conditions. Hence hybridization of classical security and chaos-based security will offer better encryption approach.

Bensikaddour et al. (2020) introduced a novel image encryption algorithm and evaluated its efficiency in terms of minimal power consumption by implementing a hardware model on FPGA XILINX (Artix-7 XC7A100T). Huang et al. (2015) employed both compression and encryption framework for remote sensing image with Arnold map for generating initial condition-based Toeplitz matrix, which is denoted as the measurement matrix. Zhang and Wang (2018) proposed a symmetric remote-sensing image encryption algorithm that enhances both security and efficiency by grouping pixel values into big integers and encrypting them using AES combined with a chaotic system. In another study by Zhang et al. (2012) proposed an image encryption approach using both transform and spatial domains as DWT decomposition, followed by sorting of low-pass sub-band coefficients using the PWLCM system in the transform domain. The encrypted image was obtained by diffusing the reconstructed image with a 2-D Sin map and applying the XOR operation. The encryption of remote sensing images was enhanced using an anti-quantum MST3 PKE scheme to withstand quantum attacks proposed by Wang et al. (2021). Liu et al. (2021) proposed a transmission model with a dual-channel key, where they embedded a plain-text key in the cipher image using a bit-level key hiding transmission strategy. They performed cross-scrambling (Boolean) and diffusion by designing a semi-tensor product. Ahmad and Farooq (2011) employed pixel permutation with DWT and confusion through the chaotic-state modulation method. Bensikaddour et al. (2017) presented a satellite image encryption technique utilizing the AES algorithm with the GEFFE generator, demonstrating its superiority over AES-CTR. Naim and Pacha (2023) suggested a pseudo-AES algorithm with multiple rounds, where the initial key was generated by a 7D hyperchaotic system. With the increasing acquisition and online transmission of digital images, their security, and privacy have become major concerns, leading to a growing interest in encryption and compression to mitigate storage and privacy-related challenge which is being reviewed by Singh and Singh (2022). Wang and Song (2023) suggested a customized image encryption method, incorporating compression sensing approaches using DCT compression with image encryption. Zhou et al. (2023) introduced a multiple-image encryption scheme using a new chaotic confusion mechanism and an added SHA-512-based security key to resist plaintext and other well-known attacks. Mathivanan and Maran (2023) proposed a combined Logistic-Sine-Tent-Chebyshev (LSTC) map model for encrypting color images with a computational encryption time of 2.97s. Alrubaie et al. (2023) suggested a new 2DNALM image encryption algorithm using a 2D Logistic map and dual dynamic DNA sequence. Feng et al. (2022) proposed an innovative image encryption method combining plane-level filtering and discrete logarithmic transformation. Ma et al. (2023) developed a novel hyperchaotic image encryption method utilizing RSVM and scrambling-diffusion techniques for enhanced security. Liu et al. (2024) proposed a novel quantum image encryption algorithm based on four-dimensional chaos achieving high information entropy and weak pixel distribution correlation. Huang and Gao (2024) suggested a new image encryption technique using fractal geometry and a new spatiotemporal chaos system for any image employing Chebyshev Improved Coupled Sine Map Lattice and also creates index control sequences for the synchronous scrambling diffusion phase using Hilbert curve scan scrambling and fractal matrix scrambling. Ye and Huang (2016) proposed a public key elliptic curve-based compressive sensing double

image encryption technique. Zhao et al. (2024) proposed a novel satellite image encryption algorithm utilizing a seven-dimensional complex chaotic system and RNA computing. In order to ensure visual security and prevent damage and attacks, Tong et al. (2024) presents a novel visually image encryption algorithm that may embed the compressed and encrypted image into a carrier image using hyper-chaotic system with DWT based compression. Barik et al. (2024) suggested a novel medical image encryption scheme cascading Quantum Mechanics and Chaos systems employing hybrid Schrodinger Logistic Encryption method. Barik et al. (2018) introduces a novel encryption technique where information is embedded as visual objects within an image, using geometric shapes and chaotic patterns to create a grid-structured cipher host image. Decryption employs visual character recognition with artificial neural networks, ensuring a secure and effective communication methodology. Zhang et al. (2024) proposes a robust medical image encryption algorithm using Josephus scrambling and dynamic cross-diffusion techniques, enhanced by a hyperchaotic system and SHA-256 for key updating, to ensure patient privacy in smart healthcare. Barik et al. (2018) proposes a novel cryptography technique using binary image textures which are generated, reshuffled, and arranged into an image, offering a simple, low-cost, and effective approach for data security, validated through empirical case studies. Honsy et al. (2024) presents a novel three-layer multiple-image encryption (MIE) technique to securely transmit batch images over unprotected networks, addressing the limitations of single-image encryption. (Barik et al. 2017) proposes a robust cryptographic scheme that encodes message bytes as binary flat-textured geometrical objects within an image, creating a grid-structured cipher image.

Despite significant advancements in image encryption techniques, several research gaps persist in the current literature. Many studies have focused on improving encryption strength and computational efficiency, yet challenges remain in achieving an optimal balance between security, computational overhead, and energy consumption, particularly for resource-constrained devices like satellites or IoT systems. While some approaches incorporate compression and encryption for efficient storage and transmission, the integration of these methods with real-time processing and hardware implementation remains under-explored. Additionally, most algorithms emphasize robustness against traditional cryptographic attacks but fail to comprehensively address emerging threats and vulnerabilities.

The applicability of proposed encryption schemes across diverse image types and real-world scenarios, such as satellite and medical imaging requires further investigation. Moreover, existing methods often prioritize either encryption strength or compression efficiency, leaving a gap in developing holistic solutions that can simultaneously optimize both aspects without compromising performance. Hence, to bridge these gaps the proposed model in this paper introduces hybrid chaotic and signal processing techniques to enhance the usability of advanced encryption and compression methods respectively. The novel contribution of the paper is mentioned as below:

1) Block-Wise Security with Chaotic Maps: Satellite images are divided into blocks, each assigned unique security keys derived from chaotic Sin Maps. These keys are reused by Tent Maps to generate random chaotic coefficients, enabling robust pixel scrambling through XOR operations and enhancing encryption randomness.

2) Efficient Compression with Fidelity Preservation: Image compression is achieved using the first-level Lifting Wavelet Transform (LWT1), which decomposes images into approximate and detailed wavelet coefficients. This ensures efficient compression while maintaining data integrity and image fidelity.

3) Adaptive Circular Shifts Using PRNG: Sub-image blocks undergo circular pixel shifts, dynamically determined by a Lehmer Pseudo-Random Number Generator (PRNG). This introduces significant

variability and adaptability, increasing the encryption complexity.

4) Secure Asymmetric Encryption: The circularly shifted image is encrypted using the RSA algorithm, employing a public-private key pair derived from prime numbers. This provides robust asymmetric encryption, ensuring secure image transmission and resistance to cryptographic attacks.

The remaining part of this article is depicted as follows. Section 2 demonstrates the background study of signal processing-based image compression followed by the hybrid chaos and PRNG methods which are related to the proposed encryption and transmission model.

Under Section 2 *i.e*. Methods subsection 2.1 describes Lifting wavelet transform based Image compression The sub section 2.2 elaborates the mathematical and conceptual background of Tent Map and sin Map. Section 3 elucidates the compressed image encryption and transmission scheme of the proposed LWTSinocryptent model. Section 4 introduces the empirical results analysis along with a full statistical security test comparing some state-of-art existing work as subsection 4.4 is for Correlation analysis, 4.5 Entropy (Uncertainty) analysis, 4.6 Test suite of NIST, 4.7 is for time analysis, 4.8 Visual Assessment, 4.9 Plaintext and Ciphertext third party attack attribution and the subsection 4.10 focus on the resistance to noise and occlusion attack. Finally, Section 5 concludes the article.

2. Methods

Wavelet-based image compression

Grossman and Morlet proposed a new frequency domain transform as a wavelet transform localized in both the time domain and frequency domain. As per wavelet, the parent signal is broken into a series of unequal bands by dilations and compressions using a mother wavelet ((Ψ(x)) such as Haar, Daubechies, Symlet etc. The continuous wavelet transform (CWT) of any signal is mathematically specified in Equation (1) as below:

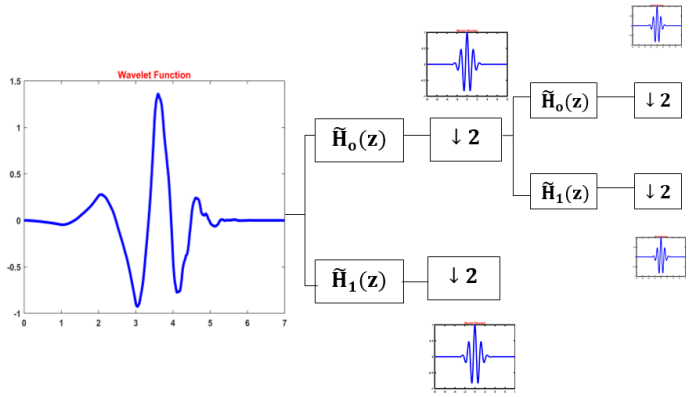


Figure 1. Wavelet function and down sampling up to level 2.

$$CWT(a,b) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} x(t)\, \psi\left(\frac{t-b}{a}\right) dt \quad (1)$$

The resolution of any signal depends on the scaling and translation parameters $a = 2^{-i}$ and $b = k2^{-i}$ respectively and the localization of the wavelet in the time domain with translation parameter as shown in **Figure 1**. CWT can be converted into discrete form through the discrete wavelet transform (DWT) with i

and k scaling parameter and translation parameter as shown in Equations (2) and (3).

$$\Psi_{i,k} = 2^{\frac{i}{2}} \Psi\left(2^{\frac{i}{2}} t - k\right) \tag{2}$$

where, $\Psi_{0,0}(t) = \Psi(t)$ is the mother wavelet hence the DWT mathematically represented as:

$$W(i,k) = \int f(t) 2^{\frac{i}{2}} \Psi\left(2^{i} t - k\right) dt \tag{3}$$

DWT extracts the local features by segregating the signal components in both time shift and scale factor. The signal resolution is calculated with a detailed coefficient and an approximate coefficient. A detailed coefficient is measured through filtering operations, whereas scale and the approximate coefficient are calculated by up-and-down sampling up to a certain level until the nature of the signal remains intact. Choosing an appropriate wavelet among the wavelet families (Daubechies, Haar, Coiflets, Biorthogonal, Mexican Hat, Symlets, Morlet, Meyer, etc.) is an important aspect concerning the problem area. Such as Haar's mother wavelet mathematically expressed as in Equation (4).

$$\Psi(t) \begin{cases} 1, & 0 \le t \le 0.5 \\ -1, & 0.5 \le t \le 1 \\ 0, & elsewhere \end{cases} \tag{4}$$

Lifting wavelet transform Wavelet signal processing is reincarnated via a lifting scheme due to a few constraints of single function, such as in both translation and scaling in higher Euclidean space, setting the unequal interval while wavelet construction and weighted inner product are needed. In general, wavelets require the concept of Fourier analysis that is minimized by using LWT which generates a series of bi-orthogonal wavelets both in the first generation and also in the second generation. It works with the convolution of the original signal with FIR filter structures and works as an odd and even pattern. **Figure 2** depicts the Lifting scheme. Mathematically define a new predict operator in the below example that takes the average of the two adjacent even samples as shown in Equation (5). Take the average out of the odd sample that came before it.

$$d(n) = x(2n+1) - \frac{1}{2}[x(2n) + x(2n+2)] \tag{5}$$

where, $x(2n)$ is predicting operator. The update is defined so that the mean of the input data vector is proportional to the sum of the approximation coefficients. We can rewrite the predict operator in the lifting in Equation (6) as

$$\begin{bmatrix} 1 & \frac{1}{4}(z^{-}1+1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -\frac{1}{2}(1+z & 1 \end{bmatrix} \begin{bmatrix} X0(z) \\ X1(z) \end{bmatrix} \tag{6}$$

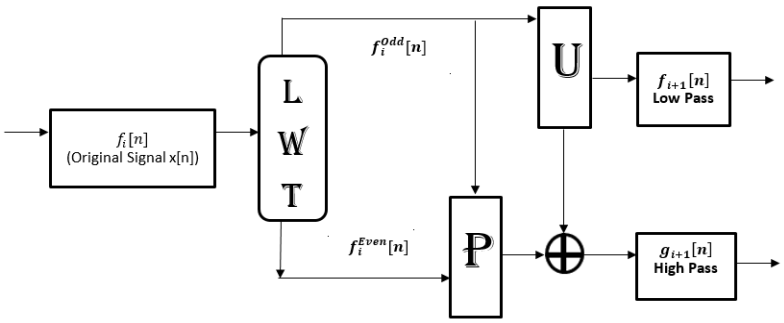


Figure 2. Lifting wavelet function even and odd.

2.1 Chaos Theory

Any minimal variation in initial conditions or seed points values of any chaos map demonstrate true dynamics and randomness which makes chaos science a popular concept that is applied in many versatile areas such as Engineering, Computer Science, Quantum Physics, Geology, Microbiology and genomics, finance, population dynamics, robotics, physiology, etc.

Tent map

It is a one-dimensional chaotic piecewise linear Map having closed interval [0, 1]. After analysing the power spectrum of tent map, it clearly depicts higher order randomness and dynamics, represented in Equations (5) and (6) and the graphical representation is shown in **Figure 18**.

$$x_{k+1} = f\ (x_k) = \ f\ (x_k, \mu) \tag{7}$$

where, k ≥ 0 even Equation (5) can be derived in Equation (6) by taking a threshold value as 0.5

$$f\ (x_k, \mu) = \begin{cases} \mu x_k, if\ 0 \le x_k \le Threshold \\ \mu(1 - x_k), if\ Threshold\ \le x_k \le 1 \end{cases} \tag{8}$$

The μ is controlling parameter and x_0 as initial condition or value. $\{x_0, x_1, \cdot\ \cdot\ \cdot\ x_k, \cdot\ \cdot\ \cdot\}$ Shows the orbit of the chaos system and $\mu \in [0, 2]$. Unstable fixed points is $\left\{0, \frac{\mu}{1+\mu}\right\}$, $1 \le \mu \le 2$ and stable fixed point $x_k^* = 0$, $0 \le \mu < 1$. At $x = 0$ one fixed point within the region $0 \le x_n < 0.5$. even $0.5 \le x_n < 1$ has another fixed point:

$$\mu(1 - x_k) = x_k$$
$$\Rightarrow 1 - x_k = \frac{x_k}{\mu}$$
$$\Rightarrow 1 = x_k\left(\frac{1}{\mu} + 1\right)$$
$$\Rightarrow x_k = \frac{\mu}{\mu+1}.$$

Lyapunov Exponent depicts the sensitivity attribute of initial conditions or values which is mathematically shown in Equations (7) and (8) as a 1-D Tent Map as below.

$$L(1) = \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} log_2 |T'(x_k)| \tag{9}$$

$$L(2) = \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} log_2 |\pm\mu| = \ log_2\mu \tag{10}$$

Both $L(1)$ and $L(2) > 0$ show strict sensitivity towards initial conditions, equivalent to 0 representing the periodic point which is a bifurcating attribute.

***Axiom* 1.** Sensitivity dependence of tent map over initial conditions x_0 [0,1] leads to chaotic characteristics.

Proof: Presume $x \epsilon$ [0, 1]. $v = \frac{j}{2^m}$ is a rational number (dyadic), $T^{[m]}(v) = 1$ hence $T^{[m+k]}(v) = 0$ in [0, 1] by taking an irrational numerals w in [0, 1], hence ∃ n such that

$$\left|T^{[n]}(v) - T^{[n]}(w)\right| > \frac{1}{2} \tag{11}$$

where, T squares each numeric value in $(0, \frac{1}{2})$, ∃ $n > m$ such that $T^{[n]}(w) > \frac{1}{2}$ based on v and w as rational and irrational numeral in [0, 1] $|x - v| < \delta$ and $|x - w| < \delta$. Equation (9) can be simplified with $\varepsilon\left|T^{[n]}(x) - T^{[n]}(v)\right| > \varepsilon\left|T^{[n]}(x) - T^{[n]}(w)\right| > \varepsilon$.

where, $\varepsilon \in \frac{1}{4}$ at the random number value x that has the sensitivity dependence over the initial conditions in [0, 1] so T is chaotic which proves this axiom.

***Axiom* 2.** Chaotic tent map is chaotic on [0, 1].

Proof: Assume S_1= (g, h) and S_2= (i, j) with open intervals in [0,1]. Take r as a least positive integer with $\frac{1}{2^r} < h - g$.

$\Rightarrow T^r(S1) = [0,1]$

$\Rightarrow (T^r)^{-1}$ ($S2$) lies with open interval of $S1$.

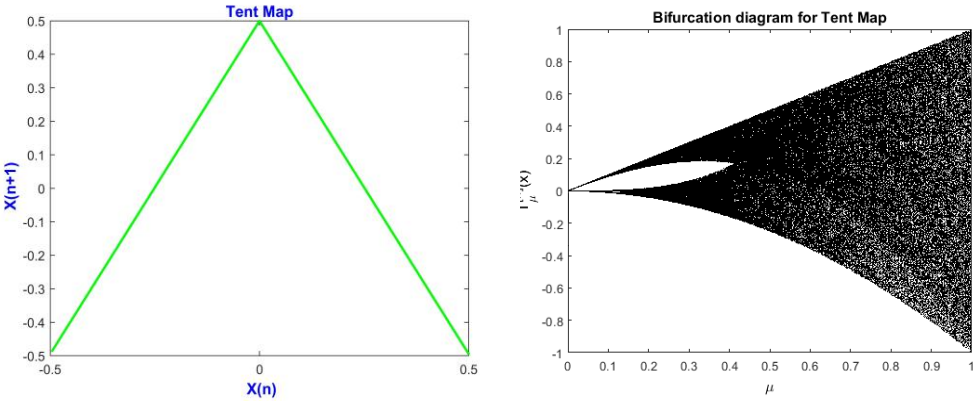


Figure 3. Generalized chaos plot (a) Graphical diagram of tent map (b) Bifurcation diagrammatic overview.

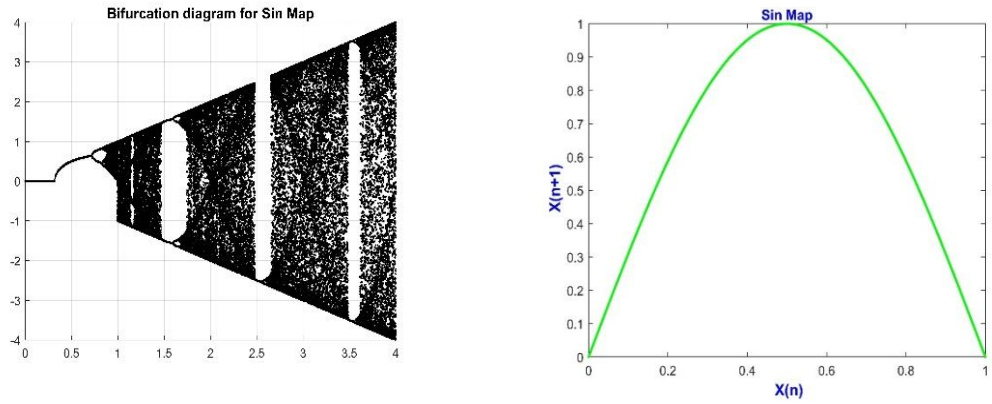


Figure 4. Generalized Chaos plot (a) Graphical plot of Sin map (b) Graphical plot of Sin map with Bifurcation attribute.

According to the periodic point density lies [0,1] there is a periodic point x in S_1 such that $Tn\ (x) \in S_2$. To depict the robust randomness property of a Tent map it uses two parameters among which one is initial conditions or initial value as x_0 and another is the controlling parameter or bias value as μ that is mentioned in Equation (5). Pictorially any Tent map is projected in **Figure 3(a)** whereas the Bifurcation attribute is shown in **Figure 3(b)**.

The sin map is shown in Equation (10) mathematically. A graphical plot(diagram) of the sin map is depicted in **Figure 4(a)**. The corresponding bifurcation attribute is shown in **Figure 4(b)**.

$$x_{n+1} = f_\lambda\ (x_n) = \ \lambda\, x \sin(\pi x) \tag{12}$$

where, $x \in [0, 1]$, $\lambda \geq 0$. To get better chaotic behavior local bifurcations, and fixed and periodic points were analyzed.

2.2 Lehmer RNG

Lehmer RNG generates Pseudo Random numbers using simple modular arithmetic expressions that are shown mathematically in Equation (11) below

$$Z_{k+1} = (\gamma.Z_k) mod\ m \tag{13}$$

where, gamma is multiplier as a controlling parameter which will be multiplied with $Z_{0,1,2...k}$ that need to be divided with modulus parameter m is a large prime integer fixed value. $Z_0 \in Z_k$, $0 \leq Z_{k+1} < m$. If $\gamma.Z_k$ is divided by m then the remainder should be any number between 0 and m-1.

Theorem 1: If the congruential sequence Z_0, Z_1, Z_2 . . .Z_k is produced by Lehmer's RNG $Z_{k+1} = (\gamma.Z_k)$ mod m with the multiplier γ and modulus m then $\exists\ h$ as an integer with $h \leq m-1$ such that (Oduwole et al., 2013): Z_0, Z_1, Z_2 . . .Z_k all are unique.
$Z_{i+h} = Z_i$, $\forall\ i = 0, 1, 2, 3, 4$ . . .

Proof: According to modular arithmetic that,
$(S_1.S_2.S_3$ . . . $S_k)$ mod $\gamma = (S_1 \text{mod}\ \gamma).\ (S_2 \text{mod}\ \gamma)$ . . .
$(S_k \text{ mod } \gamma)$
Hence $Z_i = \gamma^i.\ Z_0$ mod $m = (\gamma^i$ mod $m)\ Z_0$ mod m

Fermat's Little Theorem states that if P_r is a prime number that does not divides γ, then $a^{P_r-1} \text{mod}\ P_r = 1$.

Similarly, $Z_{m=1} = (\gamma^{m-1} \text{mod}\ m)\ Z_0$ mod $m = Z_0$ can be simplified as a generic term below
$Z_{i+Pr} = (\gamma^{i+Pr}$ mod $P_r)\ Z_i$ mod $m = Z_i$
$\Rightarrow Z_{i+Pr} = Z_i$ Hence it is proved.

Table 1. Demonstrate the fragmentation process of an image into sub-image blocks.

Input image size	Block image (Sub-image) size
256×256,512×512, 1024×1024, 2048×2048	{2×2}, {4×4}, {8×8}, {16×16}, {32×32}, {64×64}, {128×128}, {256×256}, {512×512}, {1024×1024}

3. Proposed Model: Compression Sensing Image Encryption and Transmission Scheme

The proposed encryption scheme uses a novel encryption and cyber-defense approach to protect against all kinds of cyber-attack during transmission. In the first phase, the proposed method for encryption divides the remote sensing and aerial image into sub-image blocks as shown in **Table 2**. A chaotic sin map generates randomly permuted chaos coefficient as initial seed values per block count taking (λ, x_0, π). Once for every block a seed initial value is randomly generated by sin map then those seeds are reutilized as seed or initial value for a series (block-wise) of Tent Maps (μ, $\{y_0, y_1 \cdots y_{n-1block}\}$) for encryption of each pixel within block applying XOR operation that because that will be reversible whenever decryption process will take place. After the encryption of each sub-image block, it is united to reconstruct the cipher and encrypted image. The graphical plot of hybrid Sin and Tent map is shown in **Figure 5**.

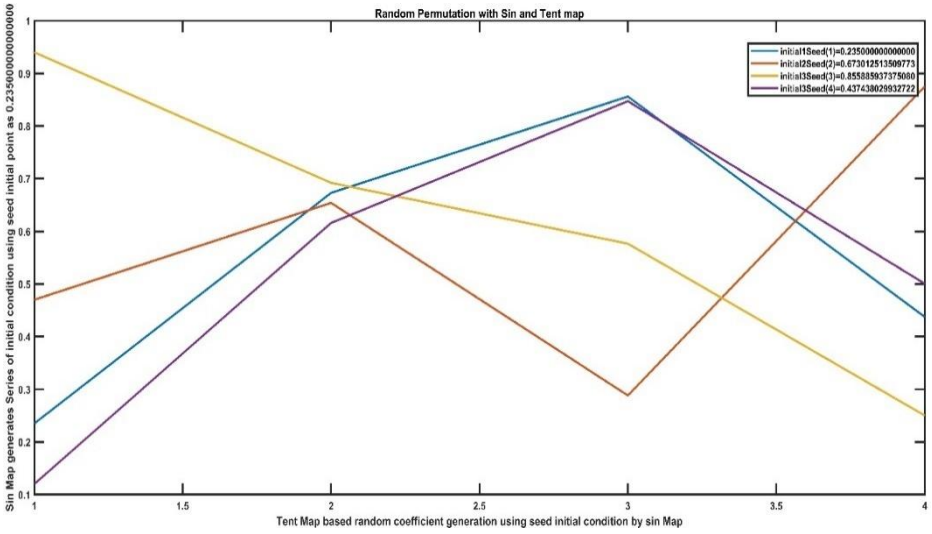


Figure 5. Graphical plot of hybrid sin and tent map dynamics based on **Table 2** chaos value.

Table 2. Shows the true dynamics with a combination of random initial conditions of Sin Map and Tent map.

Sin map:	**Tent map: control parameter μ=1.9999**	
x_0 = 0.235000000000000 **π = 3.141** **λ = 1.00000**	**Random Coefficient 1**	**Coefficient 2 ...**
x_0 = 0.235000000000000	0.469999765000000	0.939999060000235
x_1 = 0.673012513509773	0.653974645992967	0.692050361988712
x_2 = 0.855885937375080	0.288227981135778	0.576455674043575
x_3 = 0.437438029932722	0.874875622427414	0.250248630020794
x_4 = 0.980747280714147	0.038505419318987	0.077010800132556
x_5 = 0.060447329600101	0.120894598752872	0.241789076611146
x_6 = 0.188761564271262	0.377522939780960	0.755045502038980
x_7 = 0.558861241987489	0.882277074886265	0.235445732504545

At the 2nd phase, the previously obtained first phase cipher or encrypted remote sensing image is decomposed by the Discrete Wavelet Transform function choosing any one of the mother wavelets (Ψ) in this paper we took Lifting Haar wavelet as mother wavelet up to level 1. Then the outcome of the two dismantled vectors and matrix as approximated and detailed coefficient is normalized. The approximated

coefficient is an 8-bit positive coefficient (0-255) whereas the detailed coefficient is having majorly negative coefficient. To normalize the absolute lowest negative coefficient value is added to the detailed coefficient values. The concatenated approximate coefficient with normalized detail coefficient is reformed as the matrix.

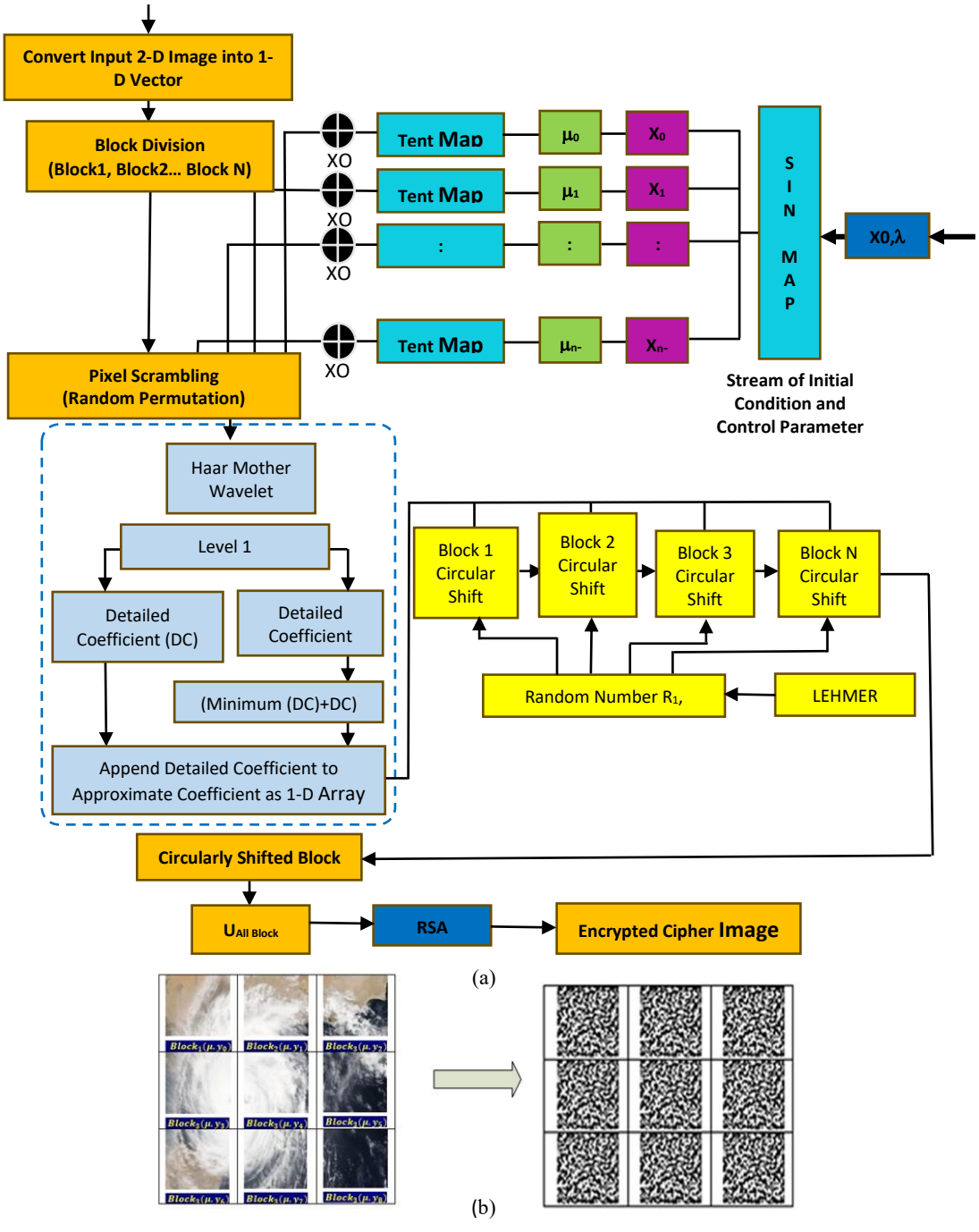


Figure 6. (a)Proposed SinCrypTent Satellite Image encryption flow diagram (b) Block division of **Figure 7(b)** for encrypted Block-wise using initial conditions and control parameters encrypted block.

In the third phase again the encrypted and compressed image is divided into blocks. Then Lehmer RNG is used to generate a unique random number to perform rotation and circular shift using (γ, z_0, m). Based on that random number the rotational count will be performed. The rows and columns of the block matrix or sub-image are shifted circularly using that random number. After the circular shift phase, each sub-image block is united to reconstruct the cipher image. Finally, the cipher image undergoes asymmetric RSA encryption with two prime numbers (P_1, P_2). The schematic and overall procedural flow of the proposed satellite and generalized image encryption is displayed in **Figure 6(a)**. In general, any image encryption algorithm security depends on pure randomness characteristics because the more random or chaotic pixel distribution the more confusion to be less chance of cyber-attack. Any chaotic map is strictly dependent on initial value and control parameters. The proposed encryption model is truly chaotic and full of confusion because initially, a Sine Chaotic map generates a fixed number of initial seed values per image block (sub-image) then the block-wise initial seed value is used by another series of Chaotic Tent maps [(λ, x_0 ・ ・ ・ x_{n-1}) $\Rightarrow$ ($\mu, y_{x_0} \ldots y_{x_{n-1}}$)]. Let us assume an image with 65536 pixels along with 256-row pixels and 256 column pixels which need to be spatially divided into 16×16 blocks with each pixel may have an 8- or 24-bit representation in memory as shown in **Table 1**. Sine map generates 256 initial seed values using equation 10 with λ is a multiplier or control parameter (λ = 1), π as another multiplier (π = 3.141592653589793) with x_0 as initial condition (λ, (x_0 ・ ・ ・ x_{n-1})) that is shown in **Table 2** having value x_0 = 0.235000000000000. The generated initial seeds are reutilized by tent maps per block using a common control parameter μ = 1.99999 as a multiplier.

Table 2 shows a clear conclusion about the random permuted chaos coefficient generated by 2 tent maps x initial (1) . . . x initial (3) by reutilizing 8 random initial conditions which are generated by the Sin map.

$$Image = Block_1 \cup Block_2 \ldots . Block_n = \bigcup_{i=1}^{n} Block_i \quad (14)$$

Equation (12) depicts the block division process of the covert image and after encryption how to reconstruct the block division matrix into an original matrix. Even the previous equation can be shown using a unique initial value per block in Equation (13).

$$B(\mu, x_0)\widehat{Block_1} \cup B(\mu, x_1) \ldots . \cup B(\mu, x_{n-1})\widehat{Block_n} \quad (15)$$

Per block, unique initial seed value (x_0, x_1 . . . x_{n-1}) generated by sin map with common control parameter λ. The block division is depicted in **Figure 6(b)**.

3.1 Encryption Procedure and Algorithm

Input: Any grayscale and color Satellite image along with other images.

Output: Cipher/ Encrypted image with Compression.

Step 1: Convert original image (OrI) into blocks (B_1, B_2, B_3 ・ ・ ・ B_k) or sub-image with the size N×N so that $OrI_i = \bigcup_{i=1}^{k} B_{NxN}$

Step 2: Iterate n block rounds: Sin map $x_{n+1} = \lambda \times \sin(\pi \times x_n)$ iteration 1 using λ, x_0 (key) to generate k random seed coefficient (x_0, x_1 ・ ・ ・ x_k).

Step 3: Uniquely generated seed coefficient (x_1, x_2 ・ ・ ・ x_k) is reused as the random initial conditions (y_0, y_1 ・ ・ ・ y_k) and mixed with the (μ_0, μ_1 ・ ・ ・ μ_k) (key) to perform the chaotic confusion within each B_k block by block using an array of Tent Maps.

Iterate k times each Tent Map with ((μ_0, μ_1 ・ ・ ・ μ_k), {y_0, y_1 ・ ・ ・ y_k}) for every block (B_k)x_{n+1} = $\mu(1-x_n)$ and intermix it to the image block by XOR ($\oplus$) operation to encrypt each block.

Step 4: Read and assemble the encrypted image block EI ($N \times N$).

Step 5: Perform level 1 decompose to EI using LWT approach by using Haar mother Wavelet shown in Equations (3) and (4) to produce an array of approximate coefficient (PC) and detail coefficient (DC).

Normalize DC = |minimum (DC)| + DC and append it behind approximate coefficient.

Step 6: All decomposed encrypted block is circularly shifted and rotated using Lehmer RNG generated random number using (γ, Z_0, m) (key).

Step 7: Assemble each encrypted block after circular rotation and feed it to RSA encryption.

Step 8: After RSA encryption the encrypted (cipher) image is transmitted. Before transmission only the security keys [λ, μ, γ, x_0, Z_0, m, minimum (DC), P_1, P_2] will be communicated to the receiving end with a separate secure channel.

3.2 Decryption Procedure and Algorithm

Decryption steps are exactly the opposite or reverse steps of the encryption process using the same set of security keys. [λ, μ, γ, x_0, Z_0, m, minimum (DC), P_1, P_2].

Step 1: First read the intensity value of cipher color or grey image $EI_i = \bigcup_{i=1}^{k} B_{NxN}$

Step 2: Perform first round decryption (DI) of the encrypted (cipher) image EI_i using RSA and its key.

Step 3: Convert decrypted image (DI) into sub-image blocks (B_1, B_2 ・ ・ ・ B_k) with size $N \times N$ so that $DI_i = \bigcup_{i=1}^{k} B_{NxN}$

Step 4: Perform reverse (-ve) circular shift or rotation of each block (B_1, B_2 ・ ・ ・ B_k). As per the same series of random number generated by Lehmer RNG using same seed Z_0, multiplier γ and prime integer m for modular division.

Step 5: Dismantle the array of approximate coefficients (PC) and detail coefficients (DC). Normalize DC= DC -minimum (DC).

Step 6: Reconstruct the image inverse DWT using the same mother wavelet decomposition approach.

Step 7: Iterate n block rounds: sin map $x_{n+1} = \lambda(1 - x_n)$ using λ, x_0 (key) to generate k random seeds (x_1, x_2 ・ ・ ・ x_k) for every block.

Step 8: Convert original image (OI) into sub-image blocks (B_1, B_2 ・ ・ ・ B_k) with size $N \times N$ so that $OrI_i = \bigcup_{i=1}^{k} B_{NxN}$.

Step 9: perform diffusion operations then Iterate k rounds: reuse xk as an array of unique initial conditions per block by using sin map with λ, x_0, (key) that is reused by tent map ((μ_0, π_1 ・ ・ ・ μ_k), {y_0, y_1 ・ ・ ・ y_k}) to conduct diffusion over every block of covert sub-image with ($\oplus$) XOR a bitwise operator.

Step 10: Unite every block to reconstruct or reframe the original image $CI_i = \bigcup_{i=1}^{k} B_{NxN}$ to access the content perceptually.

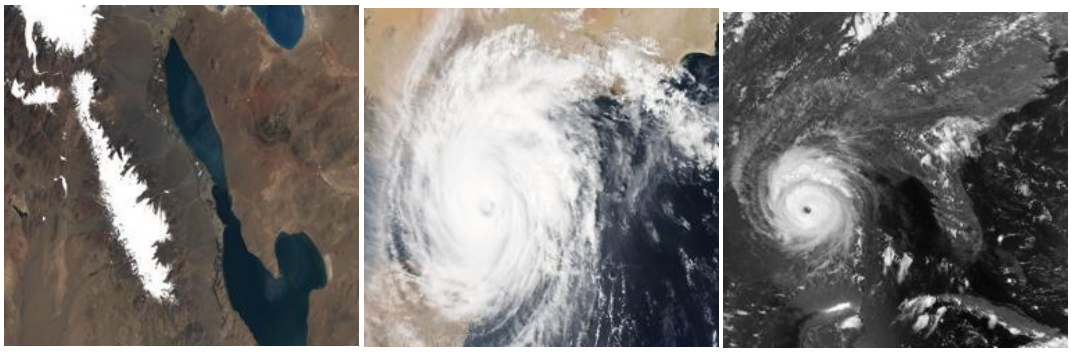


Figure 7. Remote sensing image information (a) 2016-06-24 L8mos image (b) Hurricane (c) Hurricane Andrew image.

Figure 8. Remote sensing image information (a) Rooftop image (b) Google map image (c) Washington DC Band4 image.

4. Result Analysis and Validation Metric

Practical deployment of satellite systems requires high-performance hardware, including radiation-hardened processors, robust communication modules, and advanced imaging sensors to operate in harsh space environments. The proposed technique (LWTSinocryptent) is applicable to provide content level security by conducting encryption over any kind of remote sensing image, machine vision image, biomedical image, aggrotech image including any gray image, etc. For empirical analysis in this paper is carried out using intel core (TM) i3-2350M CPU@2.3GHz 2.3GHz with 4GB RAM 64-bit processor Windows 10 Operating System with MATLAB Simulink R2018a. In this paper high resolution-based satellite, aerial images, and any plaintext image are considered for image compression and encryption for

transmission. Pixel Confusions are carryout using dual chaotic Sin and Tent map with XOR gate for complex confusion operation.

Dataset Details: For the experimental simulation over hundreds of gray scales, color remote sensing, and an aerial image along with some generalized plaintext images are collected from standard annotated datasets such as Zenodo (Gascoin, 2016), Kaggle, Google Map Image, Rafael and Richard book images (Rafael and Richard, 2013) etc. gas coin simon2016 154397, gonzalez2009digital. **Figures 7**, **8** and **9** show some satellite, and aerial images, and **Figure 10** shows some gray-scale plain images such as Airplane, Baboon and Peeper etc.

Figure 9. Remote sensing image information (a) Washed out aerial image (b) Coastal satellite image (c) Globe green image

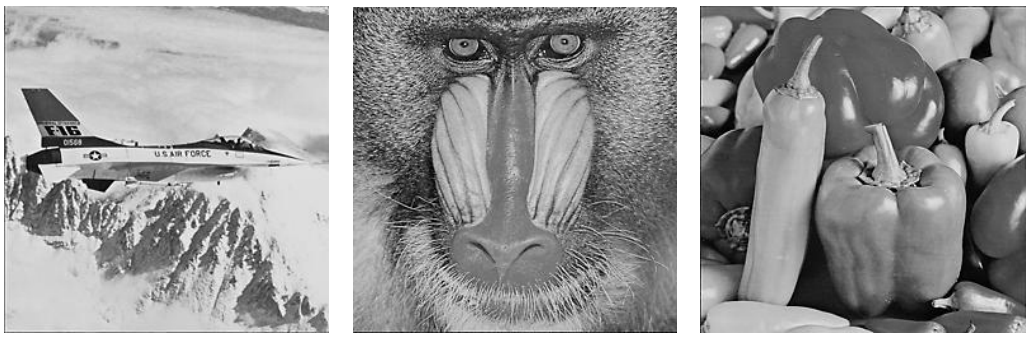


Figure 10. Plane image demonstration (a) Airplane image (b) Baboon image (c) Pepper image.

4.1 Histogram Analysis

The pixel count against the grey level of any generalized image is represented in terms of lightness/color statistically which is known as a histogram of any normal, hyperspectral image. Histogram is measured as per gray level the probability of occurrences of pixels. The transformation function is shown in Equation (16). For this **Figures 11**, **12**, **13**, **14**, **15** and **16** are taken for analysis.

$$T(r_k) = n_k) \tag{16}$$

where, k^{th}gray level is represented as r_k, n_k shows total number of pixels contributed kth gray level, where k ranges from 0 to L-1. The total image pixel count is denoted as n and represented M (Row Pixel Count) $\times$ N(Column Pixel Count) Shows the total pixel count. Equation (17) shows the normalized histogram mathematically as below.

$$p(r_k) = \frac{n_k}{n} = \frac{n_k}{M \times N} \tag{17}$$

Likewise, **Figures 11**, **12**, **13**, **14**, **15** and **16** are taken along with their image compression level. And from its **Figure 16(a)** shows original aerial image, **(b)** depicts the histogram pixel intensity distribution of the same image with maximum pixels falls towards brighter intensity (50 to 255) whereas encrypted image as demonstrated in **Figure 16(c)** and the corresponding histogram distribution as displayed in **Figure 16(d)** is approximately equal in all gray levels (0 to 255) which shows the proposed encryption algorithm is creating chaos dust properly and accurately.

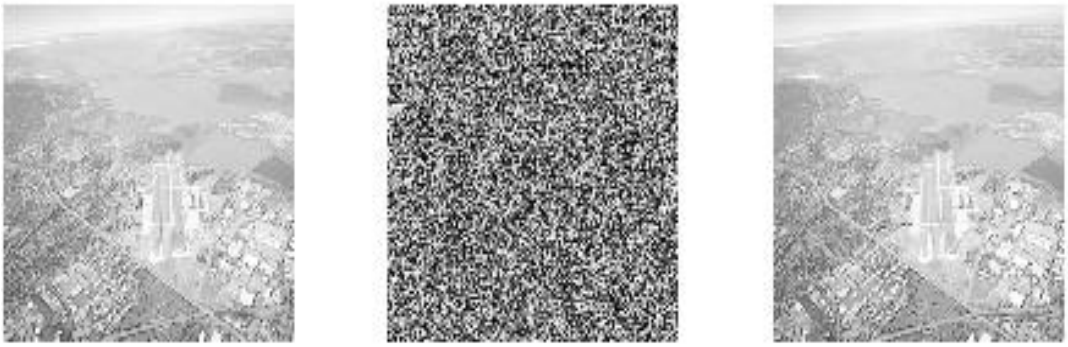


Figure 11. Image encryption (a) Remote sensing aerial image (b) Encrypted image (c) Reconstructed image after decryption.

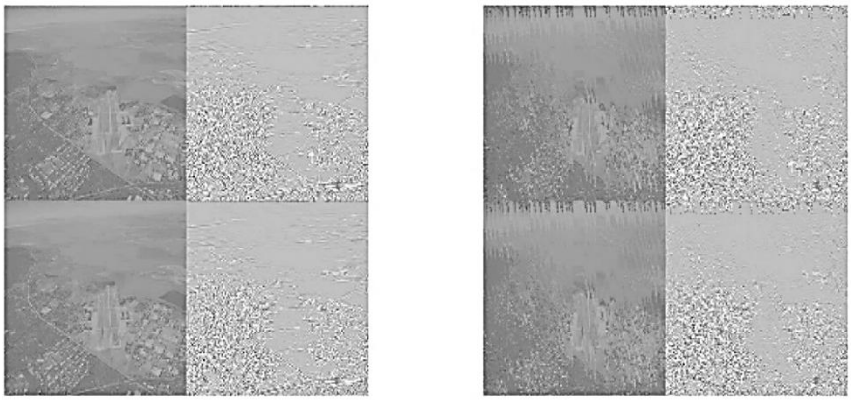


Figure 12. LWT based level 1 image compression (a) Detailed image (b) Approximate image.

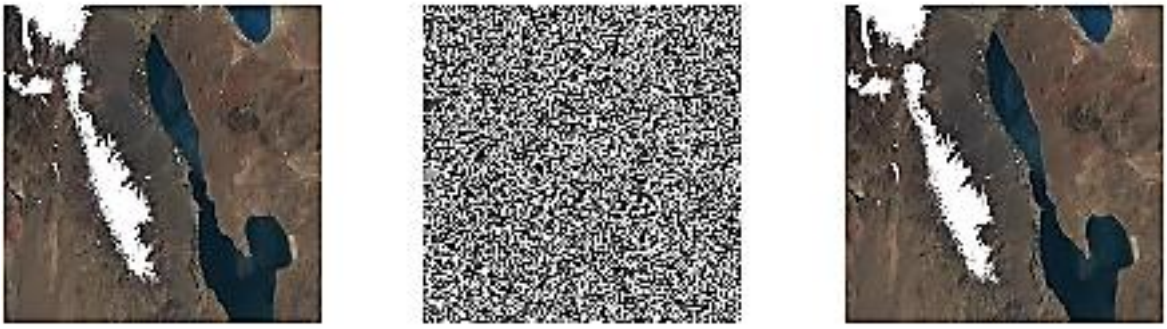


Figure 13. Image (24 bit) encryption (a) Remote sensing coastal image (b) Encrypted image (c) Recovered image.

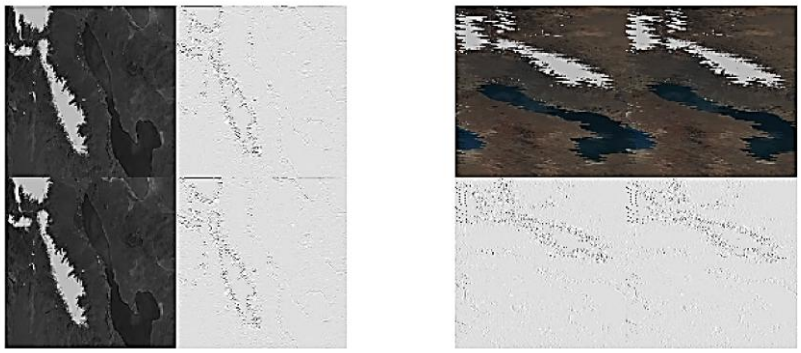


Figure 14. LWT based level 1 image compression (a) Detail image (b) Approximate image.

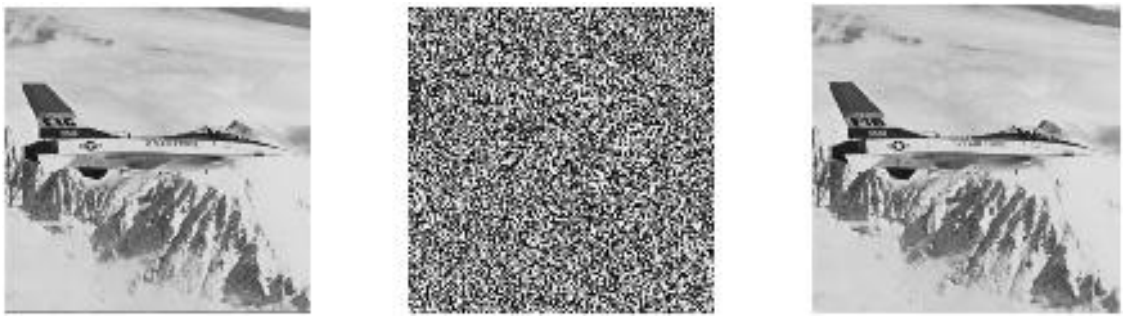


Figure 15. Image (8 bit) encryption (a) gray Airplane image (b) Encrypted image (c) Recovered image after decryption.

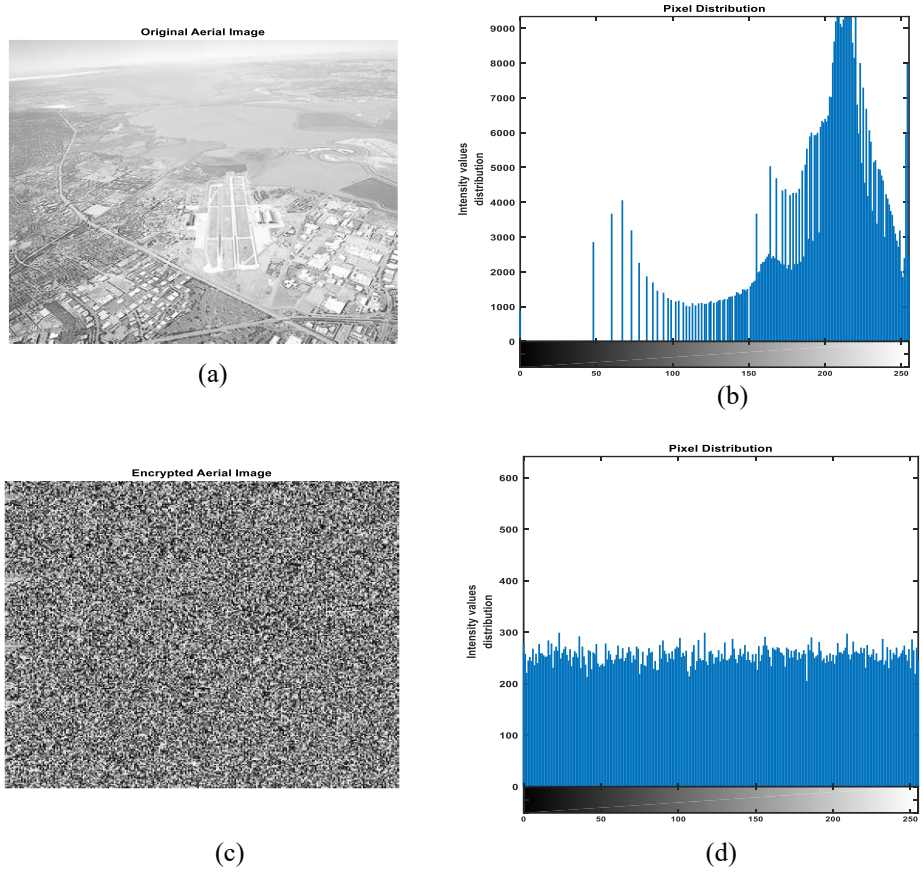


Figure 16. Pixel distribution (a) Original aerial image (b) Original image probability of pixel intensity distribution (c) Encrypted aerial image (d) probability of pixel intensity distribution.

4.2 Power Spectrum and Frequency Analysis

Randomness depicts a greater impact than any image encryption algorithm. The proposed manuscript depicts a greater stochastic behavior at every phase of encryption. This section deals with a unique analysis of the power spectrum of random sequence generator methods. Chaotic signal components frequency analysis is conducted to show the channel-wise power spectrum evaluation considering samples for time resolution (Tres). The power Spectrum (dB) plot of Sin Map, Tent map, and Lehmer RNG in **Figure 17**, **18** and **19** shows the dynamics of random distribution of 256 frequency resolution (Fres) based on samples along with their respective multiplier and initial conditions. **Figure 20** depicts the proposed chaotic encryption model overlap and combined power spectrum of the hybrid Sin and Tent map in 512 sample spaces. Frequency and Time resolution analysis is depicted with three graphical approaches Power Spectrum, Spectrogram, and Persistence plot as shown in the following Figures. In the case of **Figure 21** and **22**, the spectrogram and persistence plot of the power spectrum of the proposed model depicts dense chaotic distribution.

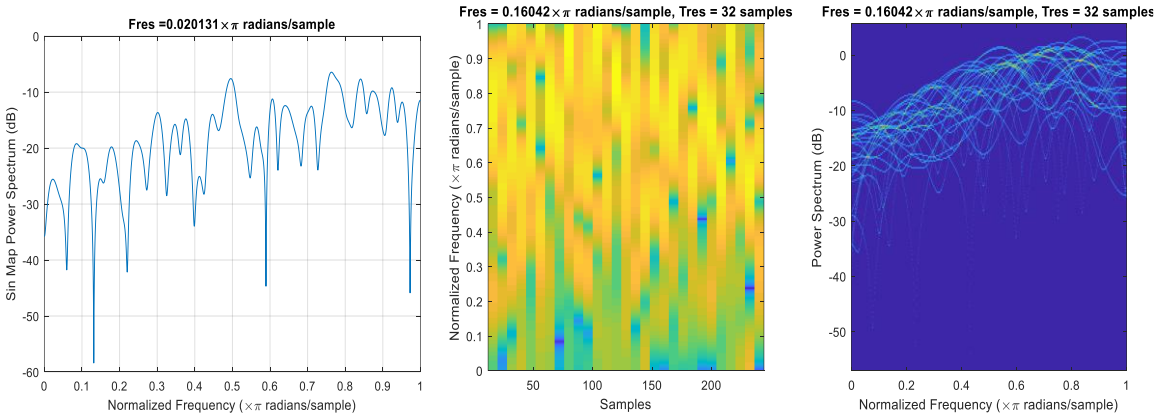


Figure 17. Graph of the discrete power spectrum for the Sin map with $\lambda = 1.05465$ initial condition as 0.235000000000000.

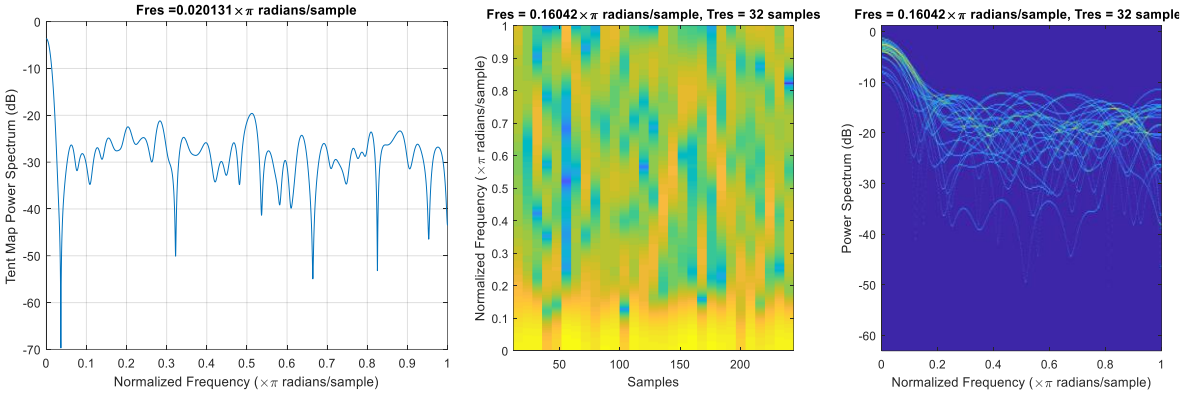


Figure 18. Graph of the discrete power spectrum for the Tent map with $\mu = 1.99999$ and initial condition as 0.004562562121178.

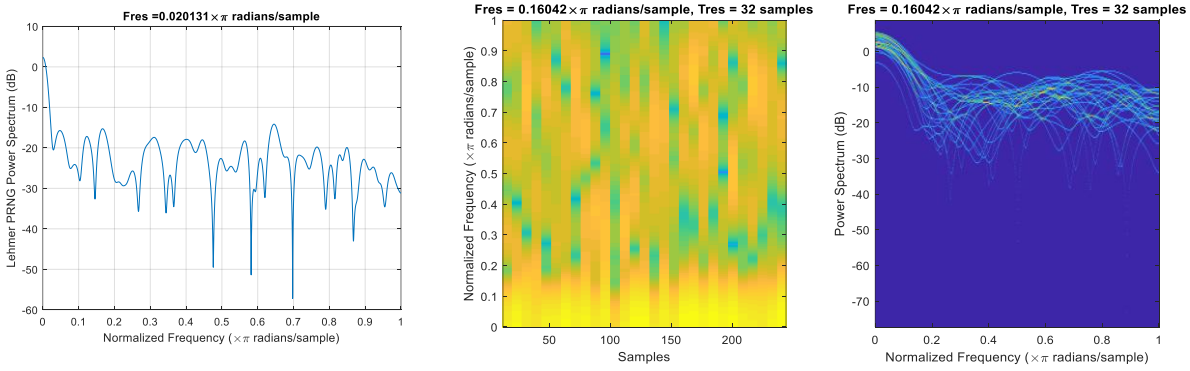


Figure 19. Graph of the discrete power spectrum for the Lehmer RNG with initial seed as $Z_0 = 0.074545671112345$ with $\gamma = 1.97896$.

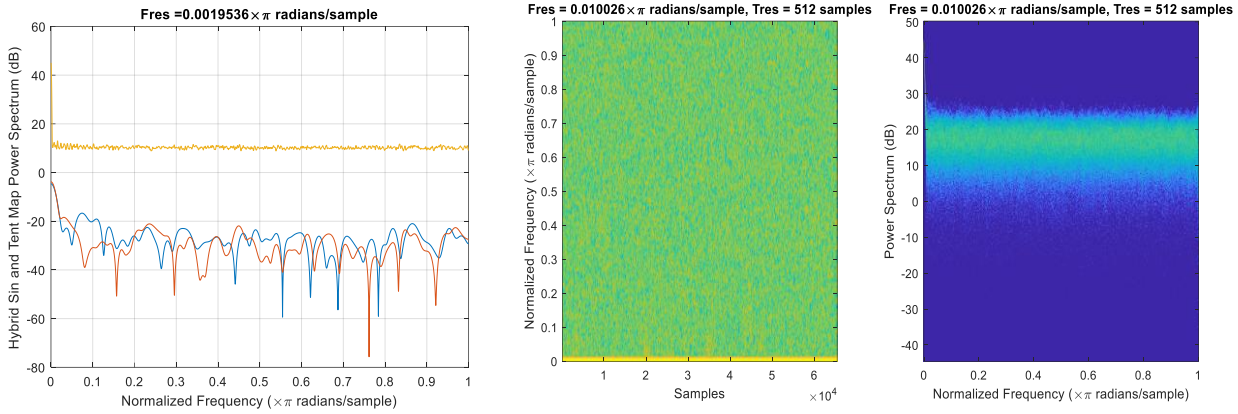


Figure 20. Graph of the discrete power spectrum of proposed hybrid (Sin and Tent Map) model with 65536 (256 × 256) frequency resolution (Fres) with 512 sample space.

4.3 Security Strength Analysis

Like the existing state-of-art image encryption algorithms the proposed SinCrypTent algorithm must also pass the prominent security testing approach to judge the efficacy. Among them NIST fixed a benchmark for any newly proposed image encryption-based security model which must pass all 15 NIST test cases. Similarly, the proposed algorithm is validated with other security measures such as histogram analysis to check the randomness for approximately equal pixel distribution in case of encrypted image. The speed analysis (measurement of efficiency based on time consumption for both encryption and decryption as well). The sensitivity analysis (Strict dependence to security key). Overall key space analysis (Total key used in the image encryption security model. The entropy calculation to measure the disorder after pixel scrambling. The more disorder leads to entropy value must be nearly 8 results to more confusion. The correlation between adjacent pixels after pixel scrambling also a major parameter fr the efficacy check of the security model.

Calculation of Key-space

Calculating all possible combination of security keys is an important aspect of key space analysis in any security algorithm which boost its cyber-defense approach. To do malicious access the eavesdropper tries to predict the security key using brute force attack. Hence it is advisable to develop strong cyber-defense approach by considering the key space very large enough to resist this attack. As a whole the proposed encryption algorithm uses four phases of encryptions and also compression using different security keys. At first sin map uses 2 security keys (λ, x_0) with controlling parameter $\lambda = 0.141592653589793$ as a multiplier and $x_0 = 0.235000000000000$ as initial seed, $\pi = 3.141592653589793$. It is used to induce a key stream of initial values or conditions per sub image block(seed) which make the proposed scheme is a novel one. Using Tent map an array of random chaos coefficient in each block that is generated by reutilizing the previously generated seed by sin map $((\lambda, \mathrm{x}_0) \Rightarrow (y_1, y_2 \cdots y_N), \mu)$. Hence, we can evaluate the key space of the proposed encryption (Sinocryptent) for any color satellite, aerial image is calculated as$10^{104} \cong 2^{354}$. Size of security keys as initial conditions or seed initial value and control parameters are considered up to 15 decimal places in case of both chaotic maps. Followed by Lehmer RNG seed as one among other security key for circular shift and rotation of block wise pixels. Finally encrypted with RSA also having 2 prime numbers as security keys.

Resistance to Brute-force attack

Key-space analysis is all possible combination of security keys in any security algorithm. The lower key space will lead to brute force attack whereas higher key space will resist strongly brute-force attack. **Table 3** depict all possible keys $[\lambda, x_0, \mu, \gamma, Z_0, m, P_1, P_2]$. used in the proposed encryption model. Mathematically the key space of the proposed encryption model can be calculated in terms of base 2 and 10. The satellite and aerial input image can be estimated with M! *N! *8! for grey image but for color image M! *N! *24! possible process. Fixed size image 256×256 divided into block of size 16×16 pixels in 2-D. Hence 256 unique initial values or conditions that is considered as security keys for 256 block using Tent Map $((y_1, y_2 \cdots y_N), \mu)$ created by sin map applying (x_0, λ) as security keys. For circular shift of each block based on the random number generated by Lehmer PRNG using initial seed and multiplier (γ, Z_0, m).

$$\text{Hence, we can calculate the key space} = 256! \times 256! \times \left|\frac{(\text{rowsize}\times\text{columnsize})}{3}\right| \times 9!$$
$$= 256! \times 256! \times \left|\frac{(\text{rowsize}\times\text{columnsize})}{3}\right| \times 9! \times 3$$
$$\cong 3.976 \times 2^{354+}.$$

Table 3. Demonstrate the total number of keys used in the proposed security model.

Stochastic and security key	Key count	Sub key	Notations
RSA	Public Key 1		P_1
	Private Key 2		P_2
Lehmer RNG	Multiplier as Key 3		γ
	Initial Value or seed as Key 4		Z_0
	Prime integer Key 5		m
DWT	Normalization parameter For Detailed Coefficient Key 6		Minimum (DC)
Sine Map	Multiplier as Key 7		λ
	Initial Value or seed as Key 8		x_0
Tent Map 1	Key 9	Subkey 8.1	$(\mu, \quad y_0)$
Tent Map 2		Subkey 8.2	$(\mu, \quad y_1)$
. . . Tent Map n		. . . Subkey 8. n	. . . $(\mu, \quad y_N)$ For each block initial seed value will vary

Differential (NPCR and UACI) attack analysis

In case of Differential attack, the attacker performs a comparison between two encrypted (cipher) images to evaluate the differences by manipulating minor modifications in the original image. Differential attack measures two popular types of comparison as unified average intensity (UACI) another type is NPCR (the number of pixels change rate) which is mathematically shown in Equations (18), (19), and (20).

$$C(i,j) = \begin{cases} 0, & T_1(i,j) = T_2(i,j) \\ 1, & T_1(i,j) \neq T_2(i,j) \end{cases} \tag{18}$$

$$NCPR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)}{M\times N} \times 100\% \tag{19}$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)\|T_1(i,j) - T_2(i,j)\|}{M\times N} \times 100\% \tag{20}$$

Here M and N are represented as image height and image width respectively. $T_1(i,j)$ and $T_2(i,j)$ are two cipher and encrypted images. The **Table 4** shows both NCPR and UACI values along with also comparative

analysis with previously published standardized methods. According to the average value obtained in the proposed method NPCR exceeds 99% and UACI exceeds 33% from which it is depicted that the proposed encryption model can resist the differential attack.

Table 4. Both Differential attack (UACI and NPCR) test analysis and comparative study.

Image encryption techniques	Images	NPCR	UACI
Zhu and Sun (2018)	Baboon (Gray Scale)	99.56	33.66
Proposed		99.54	33.35
Bensikaddour et al. (2020)	Aerial or Satellite Image (Gray Scale)	99.89	33.43
Zhang et al. (2012)		99.62	33.38
Wang et al. (2021)		99.48	33.28
Proposed		99.86	33.48
Zhao et al. (2024)	San Diego	32.14	20.57
Bentoutou et al. (2020)	Remote Sensing Oman (Alsat-1) colour Image	99.62	35.53
Liu et al. (2021)	Remote Sensing Land 1-band 1	99.60	33.50
Proposed	Remote Sensing **Figure (10)** colour Image	99.60	33.46

4.4 Correlation Analysis

Correlation is a statistical method to measure the linear relational strength and association among adjacent variables in this case these are adjacent pixels. To test the correlation among adjacent pixels in an encrypted image there are two popular parameters are utilized confusion and diffusion. Equations (21) to (26) are used to evaluate the correlation between adjacent pixels of the encrypted and original image. **Table 5** shows the correlation values obtained for the proposed encryption model and also previously existing models considering the 256×256 size of Satellite image (Barik and Changder, 2020).

Table 5. Shows correlation value comparison of the proposed technique with existing approaches for encrypted grey and color satellite or aerial image.

Image encryption techniques	Diagonal	Horizontal	Vertical	Images
Zhang et al. (2012)	0.0014	-0.0047	0.0025	Satellite, & Aerial Image
Wang et al. (2021)	0.9334	0.9527	0.9624	(Grey)
Wang et al. (2021)	0.9527	-0.0039	-0.0196	
Proposed	0.9624	0.0454	-0.0048	
Zhao et al. (2024)	-0.0014	0.0043	-0.0024	Satellite, Kiev, San Diego,
Zhao et al. (2024)	-0.0003	0.0030	0.0037	Colosseum
Zhao et al. (2024)	-0.0014	0.0011	0.0030	& Aerial Image (Color)
Liu et al. (2021)	0.8098	0.9070	0.8793	
Proposed	0.0186	-0.0232	-0.0028	

$$A_p = \frac{1}{N}\sum_{i=1}^{N} p_i \tag{21}$$

$$A_q = \frac{1}{N}\sum_{i=1}^{N} q_i \tag{22}$$

$$Mean_x = \frac{1}{N}\sum_{i=1}^{N}\left(p_i - E_p\right)^2 \tag{23}$$

$$Mean_y = \frac{1}{N}\sum_{i=1}^{N}\left(q_i - E_q\right)^2 \tag{24}$$

$$Covariance(p,q) = \frac{1}{N}\sum_{i=1}^{N}\left(p_i - E_p\right)\left(q_i - E_q\right) \tag{25}$$

$$Correlation(x,y) = \frac{Covariance(p,q)}{Mean_p Mean_q} \tag{26}$$

where, p and q are pixel amplitude (intensity) values of adjacent pixels of the images. N specifies the total pixels count within the image. $Mean_p$ representing mean of p and $Mean_q$ representing mean of q. Covariance (p, q) shows the covariance function between p and q. Correlation is evaluated with horizontal,

vertical, and diagonal coefficients that are depicted in **Table 5**. Gao and Chen (2008) show the relationship between the pain image and cipher image with horizontal as (0.9169, -0.0131), vertical as (0.9287, -0.0273), and diagonal as (0.8668, -0.0313) obtained values (Al-Shameri and Mahiub, 2013). From the obtained values as displayed in **Table 5**, it is clear that the proposed method is quite better and comparable to existing techniques from the literature. **Figure 21(a)** demonstrates the correlation distribution plot of the color satellite image and the correlation plot of the corresponding encrypted image is displayed in **Figure 21(b)**. Similarly, the grey scale aerial image correlation (scattered) plot is displayed in **Figure 22(a)** and similarly the correlation scatter plot is demonstrated for its corresponding cipher image as shown in **Figure 22(b)**. An effective encryption should significantly reduce this correlation, making encrypted images appear random and resistant to attacks. From the correlation plot it is clear that the proposed algorithm significantly reduced in correlation.

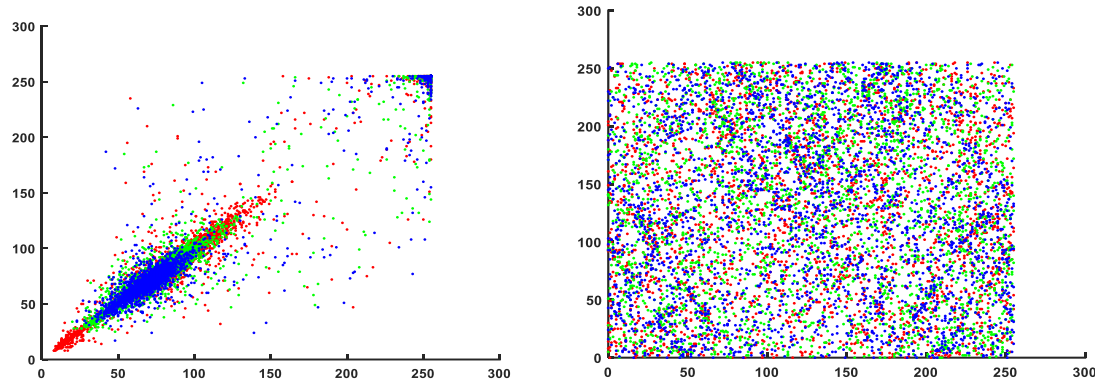


Figure 21. Correlation Analysis (a) original satellite color image **Figure 7(a)**, and **(b)** encrypted satellite color image **Figure 13(b)**.

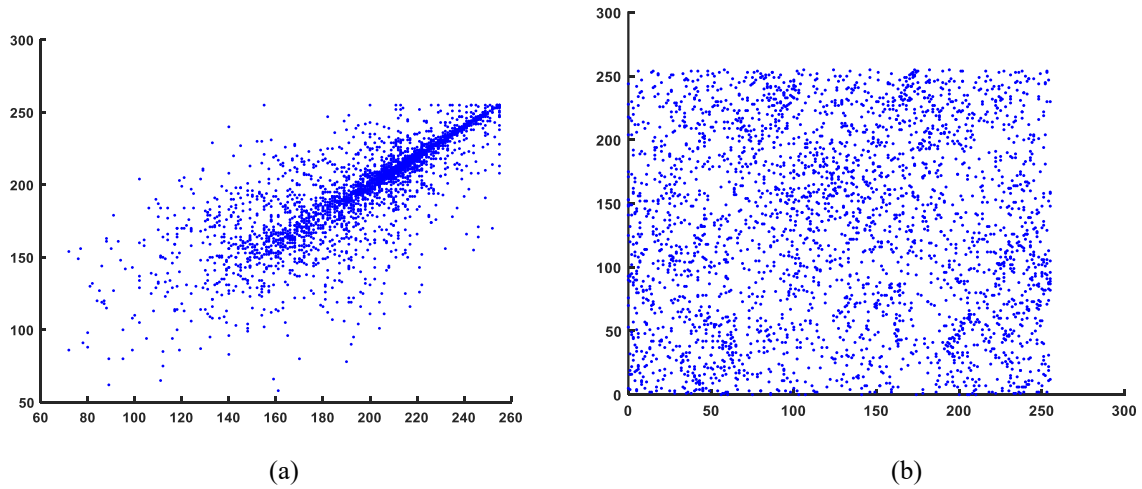


Figure 22. Correlation analysis of (a) original aerial grayscale image of **Figure 9(a)**, and **(b)** encrypted aerial grayscale image of **Figure 11(b)**.

Table 6. Shows the disorder property as entropy value of encrypted image using proposed algorithm.

Encrypted (Cipher) grey image	Baboon	Lena	Pepper	Average
Entropy Values	7.9964	7.9974	7.9973	7.9970

4.5 Entropy (Uncertainty) Analysis

Uncertainty and randomness are major factors to judge the efficacy of any image encryption-based security approach it is known as entropy which is a major evaluator in any field of science, engineering, etc.

Mathematically, entropy is shown in Equation (27). For any standardized encryption algorithm entropy value 8 is treated as the best and optimal value for evaluation.

$$H(\mathrm{s}) = \sum_{j=0}^{N-1} \mathrm{P}(\mathrm{S_i}) \log_2 \frac{1}{P(S_i)} \tag{27}$$

Where the message source entropy is represented as $H(s)$. Pre and post evaluation of entropy is carried out over Satellite and also some generalized images such as Baboon, Lena, Pepper etc. which is shown in **Table 6** along with their average value. Similarly, **Table 7** demonstrates comparative analysis of proposed encrypted model entropy value considering both satellite and generalized images with previously existing encryption model.

Table 7. Depicts comparison of entropy of proposed algorithm (LWTSinocryptent) with existing techniques.

Image encryption techniques	Aerial and satellite image	Baboon	Pepper	Average
Zhang and Wang (2018)	-	7.9910	-	-
Zhang et al. (2012)	7.9991	-	-	-
Wang et al. (2021)	7.9994	-	-	-
Liu et al. (2021)	7.9993	-	-	-
Barik and Changder (2021)	-	7.9964	-	-
Hussain et al. (2018)	-	7.9969	7.9972	7.9970
Barik and Changder (2020)	-	7.9964	7.9973	7.9975
Wang et al. (2024)	7.9993	-	-	7.9993
Proposed	7.9971	7.9969	7.9970	7.9989

4.6 Test Suite of NIST

Every standardized information security model should pass all the 15 tests as specified by NIST (National Institute of Standards and Technology) test suite. P-values are within the interval [0,1] and uniformly distributed and bit Stream sample length (N = 100). The proposed encryption model is passing all the 15 tests and validated which is shown in **Table 8**.

Table 8. Validation of proposed encryption model against NIST statistical test suite.

No.	Statistical test	P Value	Result
1.	Frequency Test	0.571020	Validated
2.	Block Frequency (M =128)	0.631124	Validated
3.	Run test	0.214002	Validated
4.	Longest Run of 1's	0.151356	Validated
5.	Binary Matrix Rank Test	0.063211	Validated
6.	DFT-Spectral Test	0.029323	Validated
7.	Non-overlapping Template Matching Test	0.123422	Validated
8.	Overlapping Template Matching Test	0.614531	Validated
9.	Maurer's Universal Statistical Test	0.717985	Validated

Table 8 continued…

10.	Linear Complexity	0.085543	Validated
11.	Serial Test 1	0.706314	Validated
	Serial Test 2	0.569108	Validated
12.	Approximate Entropy Test	0.792058	Validated
13.	Cumulative Sums Test	0.262056	Validated
14.	Random Excursions Test (x=+2)	0.356725	Validated
15.	Random Excursions Variant Test (x=-2)	0.206236	Validated

4.7 Time Analysis

Speed measurement is an important aspect to judge the efficacy of any image encryption algorithm. The simulation of the proposed encryption model is carried out using the computational hardware intel® Core™ i3-2350 CPU, 4 GB RAM, and the operating system as Windows 10 Pro with simulation is carried out using MATLAB 2018a. The image encryption speed calculation may vary depending on the high-end processor used and additional GPU. The speed comparison is shown in **Table 9** for the grayscale remote sensing image considering the image size as 256×256. Similarly, a speed comparison for the color satellite image is shown in **Table 10** which is comparatively better as comparing to Zhang et al. (2024) with 512×512 colored Baboon image which is 24.44 seconds. The proposed encryption algorithm is observed to show supremacy over many existing methods and is also quite comparable.

Table 9. Comparison of speed analysis for grey scale image encryption.

Remote sensing image encryption techniques	Time (Sec)
(Wang et al. 2021) **Figure 6(a)**	0.71
(Wang et al. 2021) **Figure 7(a)**	0.73
(Wang et al. 2021) **Figure 8(a)**	0.70
Proposed	0.52

Table 10. Comparative speed analysis of color Satellite image encryption.

Color image encryption techniques	Time (sec)	Image (256 * 256)
Liu et al. (2021)	0.23	Remote Sensing image (24-bit depth)
Proposed	0.65	

4.8 Visual Assessment

Visual assessment is also another measurement factor to validate the efficacy of different types of images (General, Hyperspectral, Super spectral, Biomedical) encryption algorithms. The pixel scrambling and confusion should be in a secure and stochastic manner so that the content of the image must not be hacked or leaked in any sense. The outcome of the proposed technique is shown in **Figures 11**, **12**, **13**, and **14** from which it could be concluded that the encrypted cipher or encrypted image cannot be replicating any visual message leak. Even after decryption the reconstructed image retail the same visual and tonal quality as a comparison to the original image.

4.9 Plaintext and Ciphertext Analysis Third Party Attack Attribution

Only cipher-text

Attacker has the access to a ROI area of cipher image. Usage of genuine secret keys can only decrypt and reconstruct the cipher image to original image (Naim and Pacha, 2023). The proposed image encryption method is best and robust because of the application of high security key space (2^{354+}) that strictly sensitive to all keys i.e., assume a security key (secret) xInitial= 0.785769766231112 for image encryption process

but a minor change in security key as xInitial $= 0.785769766231154$ leads to incorrect to get back original image. Assume in Lehmer RNG the secret key used as a seed value $Z_0 = 0.074545671112340$ instead $Z_0 = 0.074545671112345$ that leads to wrong decryption and reconstruction. Again, within stipulated time interval during transmission decrypting these keys is toughest task. According to attacker prospective it is quite harder attack to break the security model within fraction of milli second.

Known-plaintext

Attacker in this case knows a particular area or portion from both plaintext image and corresponding cipher image. Using these plaintext original image and cipher image portion pairs the attacker tries to break the security model to get the key. But the security must also be transmitted through secure channel or VPN prior to sending the ciphertext encrypted image. The proposed algorithm also uses RSA at final round of encryption to whole image using two prime numbers as secure key hence it is quite difficult to carry out Known-plaintext attack. Even for every block (sub image) by dividing the original image a unique initial condition generated by Sin Map. Again, these initial conditions are reutilized individually by number of Tent maps to create a series of unique chaos coefficient to encrypt each block level pixels to depict more stochastic behavior. Even Lehmer RNG also generates unique numbers based on this to perform rotation and block circular shift. Hybrid chaotic and classical cryptography confusion and diffusion process is introduced for each block that enables the proposed security model to resist Known-plaintext attack. Hence it is quite tougher to carry-out Known-plaintext attack successfully.

Chosen-plaintext

Here the choice to choose few sets of plaintext images by eavesdropper. As the eavesdropper knows both the encryption and decryption algorithm, they use this data to regenerate the encrypted cipher image from the selected plaintext image. The selection of plaintext images is carried out by minor deviation to evaluate correlation impact. The proposed encryption model is robust and can resist this attack.

Contrast (Clarity) Analysis

Contrast of any visual object make it distinguishable that is inherently embedded as content of an image. Moreover, it is a variation of luminance or color property. It defines the sharpness, textures, shadows, clarity, highlights the color of any object. It is measured in terms of dynamic range and contrast ratio. Mathematically contrast property of any image is defined as Equation (28).

$$Image_{Contrast} = \sum_{a,b} |a-b|^2 s(a,b) \tag{28}$$

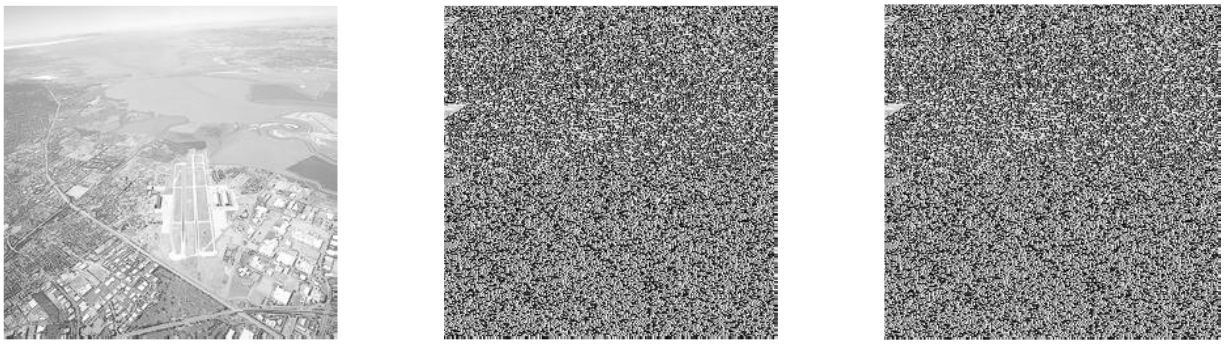
where, s (a, b) is the pixel value (grey level). Airplane grey image is evaluated with the contrast factor 8.7641 which is quite large enough after encryption with a variation obtained with empirical simulation.

4.10 Ablation Study and Analysis

Key sensitive test is an important method to validate any security algorithm that must be strictly sensitive to their keys. Because a slight manipulation in security key may lead to incorrect outcome i.e., the original image is not going to be recovered and reconstructed. Hence the key should be essentially sensitive. In the first phase of encryption sin map uses $x_0 = 0.235000000000000$ (the security key) to bring forth a series of unique initial conditions. Any small modification in initial conditions $x_0 = 0.225000000000000$ (security key) rather than $x_0 = 0.235000000000000$ leads to incorrect recovery and reconstruction of original image as shown in Fig. 23 during decryption. A series of tent map reutilizes those initial seed to generated block wise chaos coefficient. Suppose a tent map uses $\mu_0 = 1.99999999$ with $x_0 = 0.673012513509773$ similarly little modifications from $x_0 = 0.673012513509773$ to $x_0 =$

0.673012513509779 will lead to wrong recovery of the original image.

The initial seed values as initial conditions along with control parameter up to 15 place decimals in both 1-D sin map along with tent map demonstrate stochastic behavior radically. Hence above analogy clearly depict the proposed security model strictly sensitive to all the security keys.



(a) (b) (c)

Figure 23. Sensitivity dependence analysis (a) Washed out aerial grey scale image (b) corresponding encrypted image with security key as initial Condition $x_0 = 0.235000000000000$ but modification in secret key $x_0 = 0.225000000000000$ leads to incorrect decryption shown in (c).

Resistance to noise Attack and occlusion Attack

Noise is a contamination factor that obscures the original imaging signal, typically caused by issues in electronic circuitry and image sensors. When a cipher image is transmitted to its intended recipient, it may be affected by noise, such as Rayleigh noise and Salt-and-Pepper noise etc. Due to low signal-to-noise ratio conditions, the fidelity of the encrypted image may be affected. The proposed model still retains the nature of the image information as shown in **Figure 24**.

$$P(z) = \begin{cases} \frac{2}{b}(z-a)e^{-\frac{(z-a)^2}{b}} & for\ z \geq a \\ 0 & for\ z < a \end{cases} \quad (29)$$

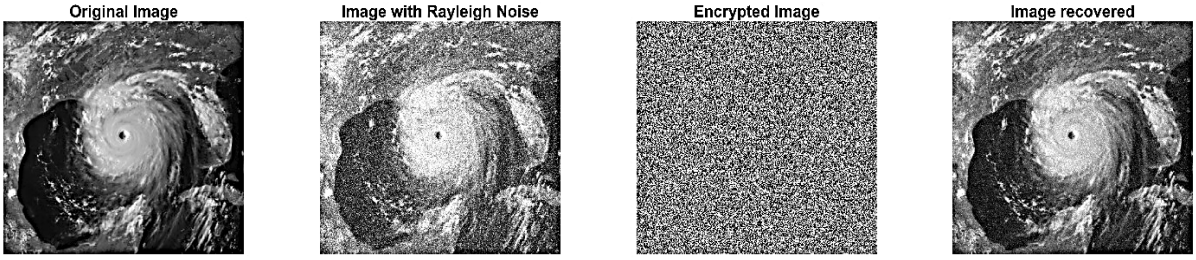
$p(z)$ represents the probability density function (PDF) of the Rayleigh noise. It indicates the likelihood of a pixel intensity or noise value z occurring. z is the random variable representing the noise intensity or pixel value being modelled. It describes the value of the noise at a specific point.

a is the location parameter (or shift parameter).
b is the scale parameter of the distribution which controls the spread or width of the Rayleigh distribution.

Larger values of b result in a broader distribution, indicating higher variability in the noise. The peak signal-to-noise Ratio (PSNR) is mathematically represented in Equation (30).

$$PSNR(in\ dB) = 10.log_{10}\left(\frac{I^2max}{MSE}\right) \quad (30)$$

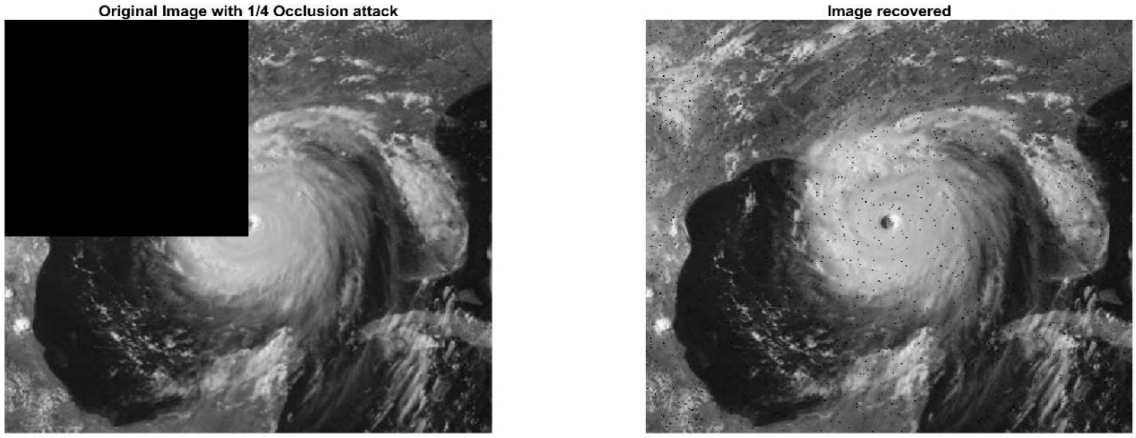
where, Imax is the maximum intensity value in the image. MSE is the Mean Squared Error. The PSNR is 54.16 as compared to Alsubaei et al. (2023) BSBE-PPODLC method whose PSNR on average 53.77.



(a) (b) (c) (d)

Figure 24. Resistance to Rayleigh noise attack with $b = 0.05$. (a) Original satellite hurricane image (b) shows Rayleigh noise affected image (c) an encrypted image (d) shows the recovered image after decryption.

An occlusion attack in image encryption involves masking or blocking parts of the encrypted image to hinder decryption or data recovery. Such attacks aim to exploit weaknesses in encryption algorithms, potentially leading to partial or complete loss of information during decryption. The proposed encryption model is able to recover the information after ¼ occlusion attack also as shown in **Figure 25**.



(a) (b)

Figure 25. (a) Resistance to 1/4 occlusion attack (b) shows the recovered image.

5. Conclusion and Future Directions

The proposed SinCrypTent satellite image encryption model introduces a sophisticated hybrid encryption framework that combines chaotic and classical (RSA) encryption with LWT compression of the cipher image. It leverages a novel hybrid security approach by integrating dual chaotic maps (sine and tent maps) for blockwise encryption, followed by a Lehmer RNG-based circular shift within each block to enhance dynamism. Additionally, classical RSA encryption and Lifting Wavelet Transform (LWT) decomposition up to the first level ensure fidelity, making the model robust for securing satellite and aerial images. To evaluate the effectiveness of the SinCrypTent algorithm, standard metrics were applied and the results demonstrate its superiority over state-of-the-art algorithms in comparative analyzes. The exceptionally large key space provides strong resistance against cyber-attacks. Thus, the SinCrypTent encryption algorithm is well-suited for encrypting satellite and general images while compressing them to retain

fidelity during transmission. However, further improvements are necessary to bolster resistance against all types of noise and occlusion attacks, particularly within the diffusion process.

Future research can extend the SinCrypTent model to 3-D satellite image encryption by incorporating volumetric chaotic maps and multi-dimensional wavelet transforms to secure spatial and spectral data. Optimizing the model for real-time processing of large 3-D datasets can enhance its applicability in advanced remote sensing and geospatial analysis.

Conflict of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Acknowledgments

Thanks to the Cyber Security Center of Excellence, C. V. Raman Global University, Bhubaneswar, National Institute of Technology, Rourkela, and XIM University, Bhubaneswar for providing unconditional support to pursue this research work. The authors thank the editor and anonymous reviewers for their valuable comments, which improved the quality of this work.

AI Disclosure

The author(s) declare that no assistance is taken from generative AI to write this article.

References

Ahmad, J., & Hwang, S.O. (2015). Chaos-based diffusion for highly autocorrelated data in encryption algorithms. *Nonlinear Dynamics*, *82*, 1839-1850.

Ahmad, M., & Farooq, O. (2011). Secure satellite images transmission scheme based on chaos and discrete wavelet transform. In *International Conference on High Performance Architecture and Grid Computing* (pp. 257-264). Springer, Berlin, Heidelberg.

Alrubaie, A.H., Khodher, M.A.A., & Abdulameer, A.T. (2023). Image encryption based on 2DNA encoding and chaotic 2D logistic map. *Journal of Engineering and Applied Science*, *70*(1), 60. https://doi.org/10.1186/s44147-023-00228-2.

Al-Shameri, W.F.H., & Mahiub, M.A. (2013). Some dynamical properties of the family of tent maps. *International Journal of Mathamatical Analysis*, *7*(29), 1433-1449.

Alsubaei, F.S., Alneil, A.A., Mohamed, A., & Hilal, A.M. (2023). Block-scrambling-based encryption with deep-learning-driven remote sensing image classification. *Remote Sensing*, *15*(4), 1022. https://doi.org/10.3390/rs15041022.

Barik, R.C., & Changder, S. (2020). Perceptual accessible image encryption scheme conjugating multiple chaotic maps. *IET Image Processing*, *14*(11), 2457-2468.

Barik, R.C., & Changder, S. (2021). A novel and efficient amino acid codon based medical image encryption scheme colligating multiple chaotic maps. *Multimedia Tools and Applications*, *80*(7), 10723-10760.

Barik, R.C., Hu, Y. C., Samal, T., & Pati, R. (2024). Dynamics of quantum mechanical schrodinger wave function and chaos for biomedical image encryption scheme. *Multimedia Tools and Applications*, *83*(11), 32813-32834.

Barik, R.C., Sahu, S.S., & Changder, S. (2018). A novel smooth texture-based visual cryptography approach for secure communication. *International Journal of Electronic Security and Digital Forensics*, *10*(2), 109-137.

Barik, R.C., Sahu, S.S., Bhoi, S.P., & Changder, S. (2017). A novel data encryption approach in the grid-structured binary image. In *Proceedings of the International Conference on Microelectronics, Computing & Communication Systems: MCCS 2015* (pp. 103-115). Springer, Singapore.

Bensikaddour, E.H., Bentoutou, Y., & Taleb, N. (2017). Satellite image encryption method based on AES-CTR algorithm and GEFFE generator. In *2017 8th International Conference on Recent Advances in Space Technologies* (pp. 247-252). IEEE. Istanbul, Turkey.

Feng, W., Zhao, X., Zhang, J., Qin, Z., Zhang, J., & He, Y. (2022). Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform. *Mathematics*, *10*(15), 2751. https://doi.org/10.3390/math10152751.

Gao, T., & Chen, Z. (2008). Image encryption based on a new total shuffling algorithm. *Chaos, Solitons & Fractals*, *38*(1), 213-220.

Gascoin, S. (2016). Satellite images of the 17 July 2016 Aru Co glacier collapse [Data set]. Zenodo.

Hosny, K.M., Elnabawy, Y.M., Salama, R.A., & Elshewey, A.M. (2024). Multiple image encryption algorithm using channel randomization and multiple chaotic maps. *Scientific Reports*, *14*(1), 30597. https://doi.org/10.1038/s41598-024-79282-6.

Huang, L., & Gao, H. (2024). Multi-image encryption algorithm based on novel spatiotemporal chaotic system and fractal geometry. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *71*(8), 3726-3739.

Huang, X., Ye, G., Chai, H., & Xie, O. (2015). Compression and encryption for remote sensing image using chaotic system. *Security and Communication Networks*, *8*(18), 3659-3666.

Hussain, I., Anees, A., Aslam, M., Ahmed, R., & Siddiqui, N. (2018). A noise resistant symmetric key cryptosystem based on S 8 S-boxes and chaotic maps. *The European Physical Journal Plus*, *133*, 167. https://doi.org/10.1140/epjp/i2018-11987-x.

Liu, X.D., Chen, Q.H., Zhao, R.S., Liu, G.Z., Guan, S., Wu, L.L., & Fan, X.K. (2024). Quantum image encryption algorithm based on four-dimensional chaos. *Frontiers in Physics*, *12*, 1230294. https://doi.org/10.3389/fphy.2024.1230294.

Liu, Z., Li, J., Di, X., Man, Z., & Sheng, Y. (2021). A novel multiband remote-sensing image encryption algorithm based on dual‐channel key transmission model. *Security and Communication Networks*, *2021*(1), 9698371. https://doi.org/10.1155/2021/9698371.

Ma, X., Wang, C., Qiu, W., & Yu, F. (2023). A fast hyperchaotic image encryption scheme. *International Journal of Bifurcation and Chaos*, *33*(05), 2350061. https://doi.org/10.1142/S021812742350061X.

Mathivanan, P., & Maran, P. (2023). A color image encryption scheme using customized map. *The Imaging Science Journal*, *71*(4), 343-361.

Naim, M., & Pacha, A.A. (2023). New chaotic satellite image encryption by using some or all the rounds of the AES algorithm. *Information Security Journal: A Global Perspective*, *32*(3), 187-211.

Oduwole, H., Shehu, S., Adegoke, G., & Onubogu, J. (2013). Fibonacci random number generator using Lehmer's algorithm. *Mathematical Theory Model*, *3*, 56-62.

Rafael, C.G., & Richard, E.W. (2013). *Digital image processing*. (3rd ed), Pearson Education, University of Tennessee, Knoxville, United States.

Ye, G., & Huang, X. (2016). A novel block chaotic encryption scheme for remote sensing image. *Multimedia Tools and Applications*, *75*, 11433-11446.

Singh, K.N., & Singh, A.K. (2022). Towards integrating image encryption with compression: a survey. *ACM Transactions on Multimedia Computing, Communications, and Applications 18*(3), 1-21.

Tong, X., Liu, X., Pan, T., Zhang, M., & Wang, Z. (2024). A visually meaningful secure image encryption algorithm based on conservative hyperchaotic system and optimized compressed sensing. *Multimedia Systems*, *30*(3), 168. https://doi.org/10.1007/s00530-024-01370-4.

Wang, C., & Song, L. (2023). An image encryption scheme based on chaotic system and compressed sensing for multiple application scenarios. *Information Sciences*, *642*, 119166. https://doi.org/10.1016/j.ins.2023.119166.

Wang, G., Ye, X., & Zhao, B. (2024). A novel remote sensing image encryption scheme based on block period Arnold scrambling. *Nonlinear Dynamics*, *112*(19), 17477-17507. https://doi.org/10.1007/s11071-024-09953-6.

Wang, X., Li, J., & Yan, H. (2021). An improved anti-quantum MST3 public key encryption scheme for remote sensing images. *Enterprise Information Systems*, *15*(4), 530-544.

Zhang, X., & Wang, X. (2018). Remote-sensing image encryption algorithm using the advanced encryption standard. *Applied Sciences*, *8*(9), 1540. https://doi.org/10.3390/app8091540.

Zhang, X., Zhu, G., & Ma, S. (2012). Remote-sensing image encryption in hybrid domains. *Optics Communications*, *285*(7), 1736-1743.

Zhang, Z., Tang, J., Zhang, F., Huang, T., & Lu, M. (2024). Medical image encryption based on Josephus scrambling and dynamic cross-diffusion for patient privacy security. *IEEE Transactions on Circuits and Systems for Video Technology*, *34*(10), 9250-9263.

Zhao, L., Zhao, L., Cui, F., & Sun, T. (2024). Satellite image encryption based on RNA and 7D complex chaotic system. *The Visual Computer*, *40*(8), 5659-5679. https://doi.org/10.1007/s00371-023-03128-x.

Zhou, Z., Xu, X., Yao, Y., Jiang, Z., & Sun, K. (2023). Novel multiple-image encryption algorithm based on a two-dimensional hyperchaotic modular model. *Chaos, Solitons & Fractals*, *173*, 113630. https://doi.org/10.1016/j.chaos.2023.113630.

Zhu, C., & Sun, K. (2018). Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps. *IEEE Access*, *6*, 18759-18770.