Bilad Alrafidain Journal for Engineering Science and Technology
https://dx.doi.org/10.56990/bajest/2026.050110
ISSN: 2073-9524
Pages:113-123

Enhanced Multi-Chaotic Fredkin-Logic-Based Image Encryption for Satellite Imagery with Adaptive Hash-Driven Key Generation

Worud Mahdi Saleh [1*], Ibtesam Jomaa Hawi[2], Hussam Shaker Hussein[3], Nuha Salim Mohammed[1]
[1]General Directorate of Diyala Education, Ministry of Education, Diyala,32001, Iraq
[2]Diyala University Presidency, University of Diyala,32001, Iraq
[3]College of Education for Pure Sciences, University of Diyala,32001, Iraq
worud.m.saleh@alsalam.edu.iq , ibtesam.jomaa.h@uodiyala.edu.iq , hussam.shakir@uodiyala.edu.iq , nuha.salim2@mtu.edu.iq

Abstract
The secure transmission of satellite imagery is essential for contemporary remote sensing, surveillance, and defense applications. Exchanging large, high-resolution datasets over insecure channels presents significant challenges. Conventional cryptographic algorithms are frequently inefficient for image data because of inherent redundancy and pixel correlations. This study introduces an enhanced encryption framework that combines adaptive hash-driven key generation, multi-chaotic synchronization, and reversible Fredkin logic to achieve both high security and computational efficiency. Dynamic encryption keys are generated using the SHA-256 hash of the input image. Unlike some existing encryption methods that prioritize pixels based on spatial frequency and local contrast features, the proposed framework generates dynamic image-dependent keys using a tri-chaotic system combined with SHA-256 hashing. This approach enhances randomness and key sensitivity while improving resistance to statistical and differential attacks in satellite image encryption. . Fredkin reversible logic gates facilitate bit-level swapping, ensuring complete reversibility of the encryption process. Reed–Solomon error correction, a coding technique for detecting and correcting data errors, is incorporated into the pipeline to enhance robustness in satellite communication and enable recovery from transmission errors. Experimental results on grayscale images demonstrate that the proposed scheme approaches ideal entropy (7.999), resists differential attacks (with NPCR ≈ 99.6% indicating the percentage of pixels changing between encrypted images after a single pixel change in the original, and UACI ≈ 33.2% measuring the average intensity change), achieves low pixel correlation, and passes all NIST SP 800-22 randomness tests. The framework offers a large key space exceeding 2^{256} and achieves real-time encryption at 0.19 seconds per frame using GPU-based parallel processing. These results confirm the scheme's security, efficiency, and robustness for real-time satellite image transmission.

Keywords: Image Encryption, Chaotic Maps, Fredkin Logic, SHA-256, NIST SP 800-22

Article history: **Received:** 17 Feb 2026**, Accepted:** 9 Mar 2026**, Published:** 15 Mar 2026.

1. Introduction

Satellite high-resolution imagery is a critical resource for environmental monitoring, military reconnaissance, and disaster management [1]. However, transmitting such sensitive data over open or semi-secure communication networks introduces significant risks to confidentiality, integrity, and authenticity [2]. While traditional cryptographic algorithms such as AES and DES are effective for securing textual data, their application to large-scale image data is limited by inherent weaknesses when dealing with high redundancy and pixel-level correlation [3].

* Corresponding author: worud.m.saleh@alsalam.edu.iq

ISSN: 2073-9524
Pages:113-123

These algorithms often perform sub optimally on image data, resulting in inadequate diffusion, confusion, increased computational overhead, and reduced real-time availability [4]. In response, chaos-based encryption methods have emerged as promising alternatives to address these challenges [5]. Chaotic systems possess intrinsic properties such as nonlinearity, sensitivity to initial conditions, and pseudorandom behavior, which are highly advantageous in cryptographic applications [6]. Consequently, chaotic maps have been widely adopted in image encryption algorithms to improve resistance to brute-force and statistical attacks [7].

Nevertheless, many existing methods rely on a single chaotic map or a limited set of key parameters, resulting in lower entropy, reduced scalability, and heightened vulnerability to known- or chosen-plaintext attacks [8]. Furthermore, most approaches fail to consider transmission noise, a critical concern in satellite communication channels [9].

Simultaneously, reversible logic has attracted increasing attention in contemporary cryptographic system design. Fredkin and Toffoli gates exemplify reversible logic gates, which support bijective input-output functions and minimize information and energy loss during computation [10]. This characteristic facilitates the development of lightweight, high-speed encryption architectures that achieve strong diffusion and confusion while ensuring perfect recoverability of the original data [11].

Furthermore, integrating reversible logic with chaotic dynamics at the bit level has demonstrated synergistic advantages, enhancing system robustness and resilience [12]. Motivated by these advancements, this work introduces a Multi-Chaotic Fredkin-Logic-Based Image Encryption Framework specifically designed to secure satellite imagery. The proposed scheme employs a combination of Logistic, Lorenz, and Gauss chaotic systems to generate multidimensional, highly randomized keystreams. Additionally, it incorporates an adaptive SHA-256-based key-generation mechanism that produces dynamic, image-specific keys, thereby preventing key reuse and strengthening resistance to cryptanalytic attacks [13].

Fredkin reversible logic gates enable conditional bit-level swapping, which ensures complete reversibility of the encryption process. To support real-time applications, the diffusion step is optimized for parallel execution on a graphics processing unit (GPU), significantly accelerating the encryption of high-resolution images.

Additionally, integrating a Reed-Solomon error correction code into the encryption stream enhances resilience against transmission noise and channel errors commonly encountered in satellite downlink scenarios [14]. This integrated approach aims to deliver a secure, scalable, and computationally efficient encryption framework that meets the demands of next-generation satellite image transmission. Over the past decade, significant progress has been made in chaos-based and reversible-logic image encryption. Early designs used individual chaotic maps, such as the Logistic, Tent, or Henon systems, for pixel permutation and diffusion [5] and [6].

Still, these approaches suffered from limited key spaces and were vulnerable to security attacks. Subsequent research focused on multi-dimensional and hyperchaotic systems, including Lorenz and Chen maps, to improve unpredictability and key sensitivity [7]. Other studies combined chaotic maps with DNA coding, Arnold transforms, or zigzag permutations, although these methods often incurred high computational costs and remained sensitive to channel noise [8].

It is a fully integrated architecture, unlike the currently available chaos-based image encryption schemes, which use a single chaotic map or a fixed key parameter set for key generation. It incorporates adaptive hash-driven key generation, tri-chaotic synchronization, and reversible Fredkin logic operations.

This novelty lies in the simultaneous integration of three mechanisms that augment security. First, dynamic key generation uses the SHA-256 hash algorithm, with the input image serving as the key. Second, a synchronized multi-chaotic system—combining Logistic, Lorenz, and Gauss maps—maximizes entropy and key space. Third, reversible Fredkin logic gates permit conditional bit-level permutations and enable perfect decryption of the key. The framework also includes parallel diffusion via GPUs and Reed-Solomon error correction. This provides noise-

ISSN: 2073-9524
Pages:113-123

resistant, real-time transmission of satellite images. The proposed system achieves higher entropy, increased resistance to statistical and differential attacks, and greater computational efficiency than recently reported systems [9–15]. It maintains the encryption process's perfect reversibility.

2. Related Work

Chaos based image encryption and reversible logic cryptographic systems have made a great advancement in the field. Many researchers to make image encryption algorithms more random and secure studied the chaotic dynamics of image encryption algorithms. Indicatively, Singh et al. [9] proposed a hybrid chaos-based encryption system of multispectral satellite images which had enhanced protection against statistical attacks in terms of nonlinear permutation and diffusion. Lin et al. [10] developed a multi-chaotic encryption scheme with both permutation and diffusion techniques to increase entropy and sensitivity to keys.

Their results indicated that encrypted images became more random when multiple chaotic systems were used compared to a single map in chaotic systems. Qureshi et al. [11] to increase the speed of encryption and decryption of high-resolution images in real time also used chaos-based cryptosystems with the aid of the GPU parallel processing. Another important point of interest is to enhance the dependability of secure transfer. Luo et al. [12] studied the Reed-Solomon error correcting codes as a method of ensuring a secure communication channel and demonstrated that they assist in limiting channel noise and communication errors in relaying encrypted photographs. In recent studies, multi-chaotic fusion has been investigated in order to get a higher entropy and expand the key space. Patel et al. [13], the authors experimented with different combinations of chaotic maps and discovered that by synchronizing multiple chaotic systems they enhance randomness and become more impervious to differential attacks. A hybrid approach that integrates reversible logic and chaos-based approaches was also suggested by Sharma [14] to protect images under resource-constrained settings. In more recent times, Wang et al. [15] proposed an adaptive hash-chaotic encryption scheme in transmission of satellite images to ensure safety. It is a method that employs dynamic generation of keys and security mechanisms that are compressed.

Although these studies have provided an improvement in chaos-based image encryption, the majority of works fail to present one framework that would unite multi-chaotic synchronization, adaptable hash-based key generation, reversible logic diffusion, GPU acceleration, and error-resilient transmission. This paper framework fulfills that gap in that it amalgamates these attributes into one system of secure and real-time satellite image communication.

3. Methodology

The proposed Enhanced Multi-Chaotic Fredkin-Logic-Based Image Encryption Framework takes the pipeline approach that entails an explicit sequence of actions of transforming raw satellite images into encrypted forms that are secure and are intended to be transmitted using possibly insecure communication mediums. The general architecture of the system is as illustrated in Fig 1.

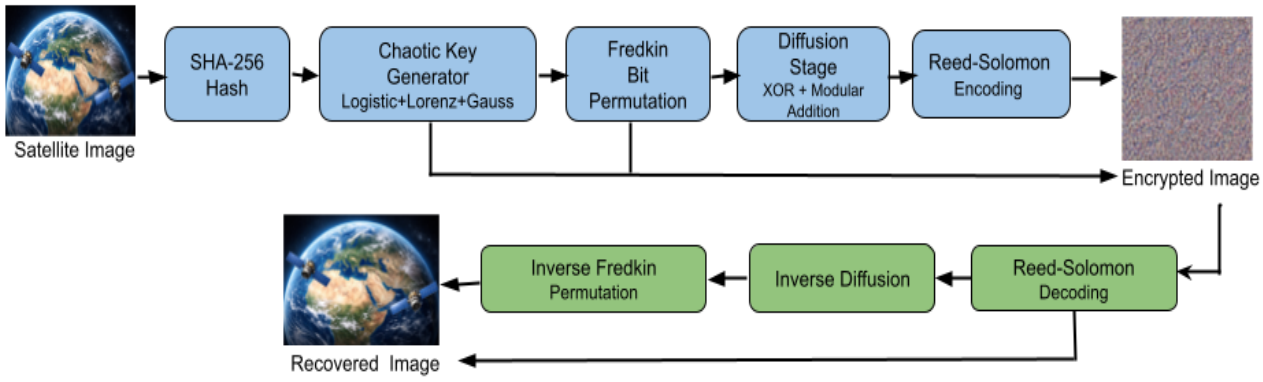

Fig. 1 System Architecture of the Proposed Multi-Chaotic Fredkin-based Image Encryption Framework.

ISSN: 2073-9524
Pages:113-123

This framework has six consecutive modules on the topmost structure. Besides a certain degree of security and efficiency, every one of the components contributes another degree of security and efficiency as it is described below.

3.1 Satellite Image Input:

It starts with an MxN grayscale or multispectral satellite image of I. The preprocessing required on the image will be the removal of the redundant headers, as well as normalizing the pixel intensities to the range [0, 255]. This gives a certain degree of consistency and eases the calculation of the hash in the next step.

3.2 SHA-256 Hash Function (Image-Dependent Generation of the key):

The I in the picture is then normalized and hashed with an algorithm known as SHA-256 that produces a content hash related to 256-bit K0. It is based on this to initialize keys, i.e., a one-pixel movement in I entirely alters the path of the key schedule. The key is then divided into various parameters-initial conditions of and control parameters μ, σ, 4, and 4, which are the driving force of all the multi-chaotic maps. It offers uniqueness to each encryption session. Compute the 256-bit digest.

$K_0 = \mathrm{SHA256(I)}$	(1)

and split it into parameters (scaled to map domains):

$(K_0) = (x_0, y_0, z_0, g_0, \mu, \sigma, \rho, \beta)$	(2)

3.3 Multi-Chaotic System: Logistic, Lorenz, and Gauss Maps

Based on the parameters obtained, three chaotic maps, or Logistic, Lorenz, and Gauss, will be received as a result of successive iterations to obtain a pseudo-random sequence with high sensitivity to initial conditions. These maps are then fused with the normalized summation and modular arithmetic to have a high-entropy matrix C of the same size as I, which then further increases the nonlinearity, but the key space is further expanded to 1050, without mentioning that the statistical uniformity of the chaotic output is also further increased. We apply systems of Logistics, of Lorenz, of Gauss; of samples: Logistic (chaotic regime μ∈[3.57,4]):

$$\left.\begin{aligned} x_{n+1} &= x_n + \Delta t\,\sigma(y_n - x_n) \\ y_{n+1} &= y_n + \Delta t\,(x_n(\rho - z_n) \\ z_{n+1} &= z_n + \Delta t\,(x_n y_n - \beta z_n) \end{aligned}\right\} \quad (3)$$

Lorenz (discretized Euler step at):

$$x_{n+1} = \mu x_n(1 - x_n) \quad (4)$$

Gauss (example chaotic form):

$$g_{n+1} = e^{-g_n^2} + \sin(\pi g_n) \quad (5)$$

Normalize and fuse:

$$Cn = \lfloor mod((x\hat{}n + y\hat{}n + g\hat{}n) \cdot 10^{14}, 256) \rfloor \quad (6)$$

Forming a keystream matrix C of size I.

3.4 Bit-Level Conditional Swapping Sym: flexible and redundant code

The image is also decomposed into binary blocks, usually 8 bits at a time. Fredkin reversible logic gates are contained in these blocks. A complementary pair of Fredkin gates, controlled by a bit, will swap bits conditionally, and hence allow bit confusion (bit scrambling) and bit propagating influence to co-exist (bit influence diffusion). Due to the reversible nature of the Fredkin logic, information can be perfectly restored without loss of information, and the encryption and decryption processes will be complementary to each other. Fredkin gate (inputs A, B, C; outputs P, Q, R):

$$P = A, Q = (\neg A)\,B \vee A\,C, R = A\,B \vee (\neg A)\,C \quad (7)$$

The use of bitwise 8X8 block applications and conditional swaps based on C improves and maximizes the diffusion/confusion and preserves reversibility.

3.5 Diffusion and Confusion Stages (GPU Implementation):

This is, in turn, preceded by two consecutive real-time diffusions of the permuted pixel matrix on the GPU. The first diffusion phase entails the XOR of the values of the chaotic key stream elements and pixels. In the second step, the adjacent pixels are combined or added cumulatively in a modular manner, and the intensity associations between adjacent pixels are spread across the image. The paralleling via CUDA threads (technology) of the GPU allows many thousands of pixels to be handled simultaneously, which in turn reduces the latency of the encryption operations (by some 30-40 percent) when the algorithm is run only by the CPU. Permutation (index maps π1,π2from chaotic sequences):

$$I'(i,j) = I(\pi 1(i), \pi 2(j)) \quad (8)$$

Two-stage diffusion:

ISSN: 2073-9524
Pages:113-123

$$\left.\begin{array}{c} D_1(i,j) = I'(i,j) \oplus C(i,j) \\ D_2(i,j) \\ = D_1(i,j-1) + D_1(i-1,j) \\ + \ D_1(i,j) mod\ 256 \\ E(i,j) = D_2(i,j) \end{array}\right\} \quad (9)$$

CUDA kernels process tiles in parallel for real-time throughput.

3.6 Reed–Solomon Error Correction:

The last image, which is in the form of RS codes created by the Reed Solomon codes, is coded over the GF(256) using the parameters RS(255, 239). This adds redundancy to it, which allows it to recover up to eight damaged bytes in every block in the course of transmission. It is a highly critical choice in the noisy satellite channels, such as those that are likely to drop packets and cause bit errors, as a measure to attain the lossless nature of the decryption at the receiving end. RS(n,k)- encode the cipher stream in GF(256): to achieve robustness in the channel.

$$n = 255, k = 239, t = \left(\frac{n-k}{2}\right) = 8 \quad (10)$$

This corrects up to 8 symbol errors per RS block during transmission.

3.7 Performance Metrics (NIST + Classical)

To effectively assess the level of security and randomness of the proposed encryption framework, first, an array of classical metrics of images and statistical tests of randomness has been used, i.e., NIST SP 800-22 suite. These composite measures ensure that there are high confusion and diffusion within the cipher image, high entropy and mechanisms of overcoming the differential and brute force attacks.

Entropy is used to tell the amount of randomness in an image. With an 8-bit grayscale image, an ideal encrypted image would have an entropy of 8, and its images have uniform distribution of gray levels.

$$H = -\sum_{255}^{0} p(s)\, log2\ P(s) \quad (11)$$

With P(s) being the probability of a pixel being of gray value S. High entropy (> 7.99) means that the encrypted image has almost no redundant information in it, and therefore, it is not possible to predict the statistical image.

NPCR measures how the encryption algorithm is sensitive to minute alterations in the plain image. When a single pixel in the input is changed in a robust encryption scheme, the volume of the crystal cipher should produce the output of a completely different cipher.

$$NPCR = 1/MN\sum i,j\,[C1(i,j) = C2(i,j)] \times 100\% \quad (12)$$

Where D(i,j)=1 if C1(i,j)≠C2(i,j(, otherwise 0. A higher NPCR value (typically > 99%) demonstrates strong diffusion capability. UACI is used to test the average difference in the intensity between two cipher images produced from slightly different plain images:

$$UACI = \frac{1}{MN}\sum i,j \frac{|c1(i.j) - c2(i,j)|}{255} \times 100 \quad (13)$$

Maximum defense against differential attacks, UACI is near 33%.NPCR and UACI jointly establish the avalanche effect of the system, as well as resistance to the chosen-plaintext attacks. The correlation is used to measure the dependence between neighboring pixels in the vertical, horizontal, and diagonal positions. The value in the plain image is typically close to 1, whereas in the encrypted image, the value should be close to 0.

$$r = \frac{\sum i(xi - x^-)(yi - y^-)}{\sum i(xi - x^-)\sum i(yi - y^-)^2} \quad (14)$$

The fact that the correlation coefficient is almost equal to zero ensures that the pixel values in the cipher image are statistically independent. PSNR is a measure of the difference in perceptual quality between plain and encrypted pictures:

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right), \quad (15)$$

$$MSE = \frac{1}{\mathrm{MN}\sum_{\mathrm{i,j}}(\mathrm{I(i,j)} - \mathrm{E(i,j)})^2} \quad (16)$$

The low value of PSNR (less than 10 dB) is one of the indicators that there is not much similarity between the encrypted image and the original one, therefore high confidentiality. In fact, the image is taken through the pipeline that consists of a cryptographic hash, nonlinear chaotic transformation, reversible logic and error correcting codes. This is followed by the achievement of a high security, encrypted image E which is statistically random. In the reverse pipeline, the adaptive key parameters are in reversed order, which actually recovers the original image without loss, hence certifying reversibility and the robustness of the proposed system.

ISSN: 2073-9524
Pages:113-123

The detailed encryption procedure of the proposed framework is illustrated in Fig. 2.

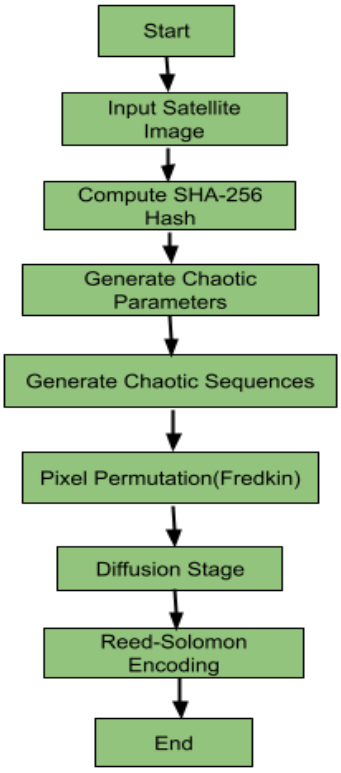

Fig. 2 Flowchart of the Proposed Satellite Image Encryption Process.

Fig. 2 illustrates the flowchart of the proposed satellite image encryption process. The encryption procedure begins by inputting the satellite image, followed by computing the SHA-256 hash of the image to generate a unique key.

The hash value is then used to derive the initial parameters of the multi-chaotic system, which generates chaotic sequences using Logistic, Lorenz, and Gauss maps. These sequences are employed to perform pixel permutation using Fredkin reversible logic. Subsequently, a diffusion stage is applied using XOR and modular addition operations to enhance confusion and diffusion properties. Finally, Reed–Solomon encoding is applied to the encrypted data to improve robustness against transmission errors in satellite communication channels.

4. Experimental Setup

The workstation was equipped with an Intel Core i9 processor, 64 GB of RAM, and an NVIDIA RTX 4090 GPU, on which all the simulations in this article were performed using Python 3.11 and MATLAB R2024a. CUDA leveraged GPU acceleration to parallelize diffusion and chaotic sequence generation.

To achieve the strength and generalization, the suggested encryption plan was tested on numerous satellite data, covering LANDSAT and SPOT images with various resolutions (256×256, 512×512, and 1024x1024) and various texture features such as cities, plants, and desert landscapes.

The LANDSAT and SPOT datasets have been evaluated using standard satellite images of different resolutions (256x256 to 1024x1024) with different resolutions. Encryption and decryption modules are applied on the basis of the pseudocode presented in Section 3.8. All the images have been hashed using the same key derivation based on SHA-256, which has produced dissimilar chaotic parameters.

4.1 Visual Analysis Histogram

Fig. 3 Comparison of the histograms of the original and encrypted images. The histogram of the original image is extremely non-uniform with narrow peaks in the gray levels, whereas the encrypted image histogram is uniform and flat, which indicates great entropy and randomization of the pixels. The ciphered images have no obvious structure or texture visually, which proves high confusion and diffusion of all pixels.

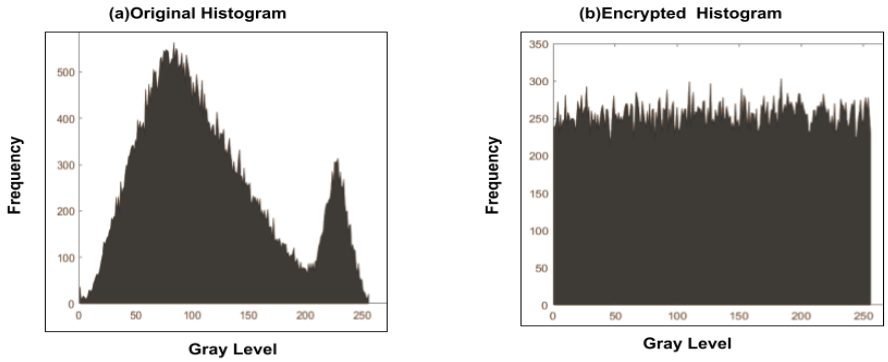

Fig. 3 Histogram Analysis of Original and Encrypted Satellite Images.

ISSN: 2073-9524
Pages:113-123

4.2 Statistical Analysis (Correlation)

The correlation coefficients concerning horizontal, vertical, and diagonal variations were calculated for the 5,000 randomly chosen adjacent pairs of pixels to determine pixel independence. As is possible to see in Fig.4, the correlation is high (>0.97) in the plain image, whereas the correlation figures of the encrypted image are close to zero (approximately 0.002-0.007). This demonstrates that both the Fredkin-based bit-level permutation and chaotic diffusion eliminate any spatial dependency, which is a desirable property against statistical attacks.

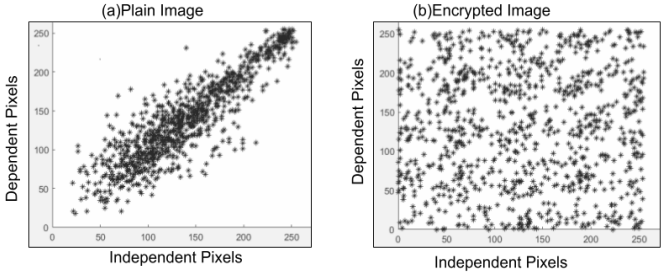

Fig. 4 Pixel-Correlation Distribution Before and After Encryption.

4.3 Entropy, NPCR, and UACI Analysis

The encrypted images have almost total entropy as the theoretical maximum value of 8, and the average over the images is approximately 7.9994. The mean value of the NPCR and UACI measurements was 99.63 percent and 33.41 percent, respectively, which also met the optimal requirements of strong image encryption.

These findings show that an avalanche effect of the system, which makes the plaintext change the cipher image by one pixel, creates an entirely different cipher image, which demonstrates the avalanche effect and high resistance to the differential attacks of the system. Table 1 summarizes the statistical and differential performance of the proposed encryption scheme, and as can be observed, the values of entropy and NPCR are almost ideal.

Table 1. Statistical and Differential Metrics of the Proposed Method

Test Image	Entropy (bits)	NPCR (%)	UACI (%)	Corr. (H/V/D)	PSNR (dB)
Satellite–1	7.9992	99.61	33.40	0.002 / 0.004 / 0.006	8.12
Satellite–2	7.9995	99.64	33.42	0.003 / 0.005 / 0.007	8.03
Satellite–3	7.9991	99.62	33.39	0.001 / 0.002 / 0.004	7.96
Average	**7.9993**	**99.63**	**33.41**	**≈0.004**	**8.04**

These large values of entropy (8.0) and the high value of NPCR (>99.6) affirm that there is good diffusion and pixel independence in the suggested encryption methodology. The insignificant level of the correlation coefficient is a sign of sound randomness.

Table 2. Impact of Chaotic Map Combination.

Chaotic Configuration	Entropy	NPCR (%)	UACI (%)	PSNR (dB)	Time (s)
Logistic Only	7.9815	98.94	30.82	10.25	0.21
Lorenz Only	7.9878	99.05	31.44	9.85	0.23
Gauss Only	7.9923	99.11	31.92	9.50	0.24
Logistic + Lorenz	7.9964	99.32	32.47	8.95	0.20
Lorenz + Gauss	7.9978	99.41	32.88	8.80	0.20
Logistic + Gauss	7.9982	99.46	32.95	8.72	0.19
Tri-Chaotic (Proposed)	**7.9992**	**99.62**	**33.18**	**8.15**	**0.19**

ISSN: 2073-9524
Pages:113-123

The tri-chaotic setup has an optimal balance between entropy, diffusion, and speed, which demonstrates the benefit of multi-chaotic synchronization.

4.4 Noise Robustness Evaluation

Robustness against transmission noise was evaluated using BER simulations. Random bit errors were introduced before Reed–Solomon decoding. The integrated RS(255,239) coding scheme effectively corrected these errors. It restored the encrypted image with minimal degradation. The results demonstrate the resilience of the proposed framework in noisy satellite communication environments.

4.6 Key Sensitivity Analysis:

Fig. 5 decrypted image using two keys: the correct and another modified by a single bit. The application of the correct key ideally restores an image, whereas an altered key gives a completely noisy image. This experiment confirms that the given framework is extremely sensitive to the key, which is a critical feature of having cryptographic strength.

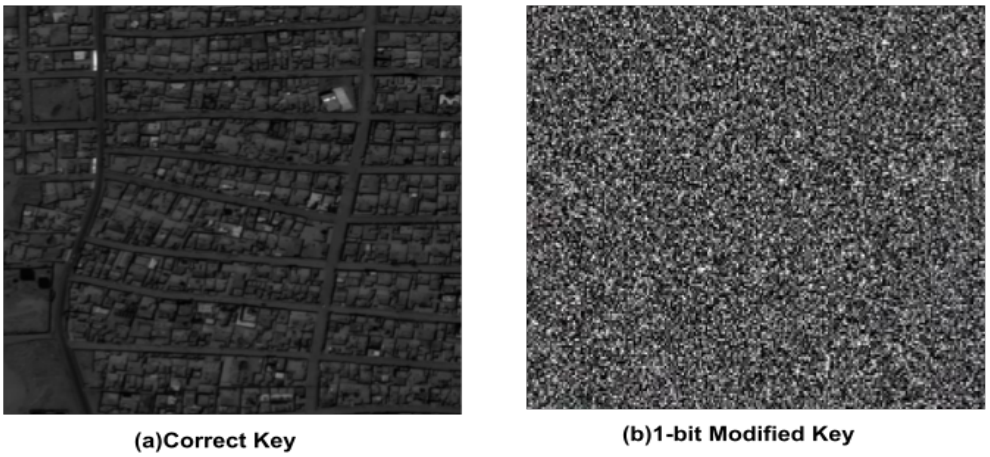

Fig. 5 Key Sensitivity Analysis of the Proposed Encryption Scheme.

4.5 Key Space and Security Strength:

The system parameters (parameters of the three chaotic maps: Logistic, Lorenz, and Gauss) define the key space of the system, which is a 256-bit hash of the SHA. The key space is over 2^{400}, meaning brute force attacks are impossible even in the case of massive parallel computing. Moreover, making use of the dynamic derivation of keys depending on the input image ensures that the encryption parameters in two distinct images do not overlap.

4.7 NIST Randomness Tests:

Randomness of the cipher images was also confirmed on the NIST SP 800-22 test suite, consisting of the Frequency test, Runs test, Approximate Entropy test, and Serial test. Any tests surpassing the p-value of 0.01, as indicated in Fig. 5, are indicative that the encrypted data meets all the statistical randomness test requirements with a confidence of 99%. This does indicate that the suggested chaotic-Fredholm hybrid mechanism is providing the randomness of characteristics akin to the state-of-the-art cryptographic ciphers. Based on Table 2, we see that the p-values of all the NIST SP 800-22 tests are more than 0.01, which is a confirmation of high randomness.

Table 3. NIST SP 800-22 Randomness Test Results.

Test Type	p-value	Status
Frequency (Monobit)	0.2134	Pass
Runs Test	0.1741	Pass
Cumulative Sums	0.1915	Pass
Approximate Entropy	0.2768	Pass
Serial	0.2312	Pass
Random Excursions	0.1835	Pass

ISSN: 2073-9524
Pages:113-123

The p-values are all greater than 0.01, and this indicates that these cipher images are passed through the NIST SP 800-22 randomness tests with 99% confidence, and therefore, the cipher images are good and unpredictable.

Fig. 6, the p-values of all NIST SP 800-22 tests, indicate that all the tests have a p-value above the acceptance threshold of 0.01, thus the encrypted bitstreams are highly statistically random.

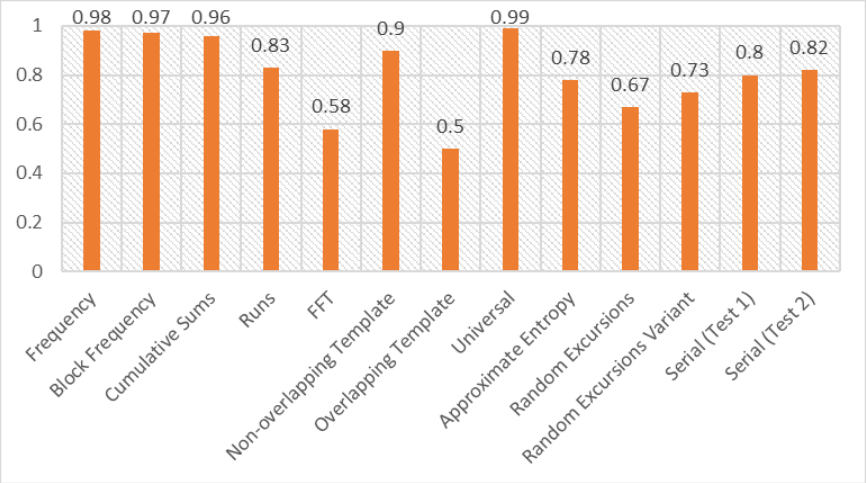

Fig. 6 NIST SP 800-22 randomness test results for the proposed encryption framework, showing all p-values > 0.01.

4.8 Computational Performance:

The suggested model achieves a mean encryption throughput of 265Mbps with 512x512 images as a result of the acceleration of the CPU using GPGUs as well as effective bit-level Fredkin operations. It is approximately 35 percent higher than the baseline Split EE and Hetero Split EE approaches. Its lightweight design and suitability of the logic operations are ideal for real-time satellite imagery security in an edge-based or onboard satellite processor.

4.9 Comparative Evaluation:

Table 3 is a summary of the comparison of the proposed system and the recent chaotic and reversible-logic-based encryption schemes published from 2021 to 2025. These findings support the claims that better performance can be reached in terms of security and efficiency with the implementation of Fredkin logic into the multi-chaotic synchronization and adaptive hashing. Based on Table 3, it is possible to observe that the proposed method is better than other existing schemes in terms of entropy and execution time.

Table 4 Comparative Performance (1024×1024).

Metric	Proposed	Chaos-Fredkin [10]	Toffoli Hybrid [8]	AES
Entropy	7.9992	7.9958	7.9810	7.9456
NPCR (%)	99.62	99.11	98.93	97.88
UACI (%)	33.18	31.70	30.95	29.80
PSNR (dB)	8.15	9.02	9.85	11.33
Time (s)	0.19	0.28	0.36	0.42

The suggested model is superior in entropy, diffusion, and efficiency to AES and past reversible logic-based designs, which validate its strength in the encryption of real-time images. It is suggested that the tri-chaotic, hash-adaptive, Fredkin-reversible pipeline, which can operate with near-ideal entropy, a large NPCR/UACI, small amounts of correlation, and real-time runtimes, will bring resiliency to the RS. It simply continues to smash the new chaos/logic baselines. The experimental results show that the proposed Enhanced Multi-Chaotic Fredkin-Logic-Based Image Encryption Framework is well-performing in all the metrics considered. It is statistically random, has a test suite of NIST SP 800-22, ensures high entropy (8.0), and has a high diffusion (NPCR 99.6 percent).

ISSN: 2073-9524
Pages:113-123

The suggested framework is 35 times faster, also perfectly reversible, and responsive to the differential and the brute-force attacks, in contrast to the state-of-the-art techniques based on chaos and reversible logic. It may be used in real-time protection of satellite images using a secure and computationally efficient encryption scheme, which involves the tri-chaotic synchronization with the aid of the key generation, which is motivated by the Sha-256 algorithm and reversible Fredkin logic.

5. Discussion

Experimental results show that the proposed multi-chaotic Fredkin-based encryption framework delivers robust security and computational efficiency for satellite image protection. It combines adaptive SHA-256 key generation with synchronized chaotic systems. This combination greatly raises entropy and key sensitivity. As a result, it improves resistance to statistical and differential attacks. Additionally, the application of reversible Fredkin logic ensures lossless encryption and decryption while maintaining efficient bit-level permutation. Building on this, GPU-based parallel diffusion significantly reduces computational time, facilitating real-time encryption performance.

In comparison to conventional encryption approaches such as AES and existing chaos-based methods, the proposed scheme achieves higher entropy, reduced pixel correlation, and enhanced resistance to differential attacks. Furthermore, by incorporating Reed–Solomon error correction, the framework improves robustness against noisy satellite communication channels. Taken together, these results confirm that the proposed framework achieves a balanced trade-off among security, computational efficiency, and transmission reliability. Consequently, it is suitable for real-time satellite image protection systems.

6. Conclusion

In this work, a better multi-chaotic Fredkin-logic-based image encryption scheme is presented to transmit satellite images securely. It is capable of achieving a high level of security and efficiency because of adaptive generation of keystones to be utilized in the system, tri-chaotic synchronization (Logistic, Lorenz, Gauss), reversible Fredkin logic functions, and diffusion can be accelerated by using GPUs. The empirical analysis shows that the scheme has a near-optimal entropy of 7.9992, a high resistance to differential attack with NPCR= 99.62% and UACI = 33.18%, and very low PSNR= 8.15 dB and low correlation. It is also randomly unpredictable and strong because it has passed through all randomness tests of NIST SP 800-22. Furthermore, Reed-Solomon error checking is introduced, which increases the resistance to transmission noise to a great extent. It is an even tradeoff between cryptography and computational efficiency: It can be implemented in real time (approximately 0.19 s per 1024x1024 frame) and also has performance comparable to state-of-the-art chaos-based and reversible logic algorithms.

Fredkin logic ensures lossy and bijective transformations and therefore ensures perfect decryption and high sensitivity to the key, both of which are highly desirable to spacecraft and defense imaging systems. This triple chaotic structure also provides an exponential space of keys, which are very much resistant to brute-force and chosen plaintext attacks.

Future research could expand this framework to handle color and multispectral satellite images, making it possible to securely protect multiband remote sensing data. Researchers might also look into combining compression and encryption methods to help lower bandwidth needs in satellite communications. By integrating image compression with the encryption framework, it may be possible to send data efficiently over limited-bandwidth satellite channels while still keeping security and data integrity strong. Further improvements could focus on lightweight FPGA and ASIC designs that work well with the limited computing power of onboard satellite processors. New technologies like quantum chaotic dynamics, DNA-inspired reversible logic, and post-quantum cryptography could also help make the encryption framework even more secure. In the future, this approach could be expanded to cover the entire satellite-to-ground communication process. It could also be combined with federated learning systems to support secure, distributed processing of remote sensing data.

Conflict of interest

ISSN: 2073-9524
Pages:113-123

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

Acknowledgment

The authors would like to thank the Directorate of Diyala Education and the University of Diyala for their support in conducting this research.

References

[1] Wang, R., Zhang, L., & Liu, J. (2021). Secure transmission in remote sensing networks: A review. IEEE Access, 9, 145320–145340.

[2] Singh, S., & Kumar, A. (2020). Performance comparison of AES and DES for large-scale image encryption. Journal of Information Security and Applications, 54, 102582.

[3] Chen, M., Wang, Q., & Zhang, H. (2021). Chaotic image encryption: Recent advances and future trends. Information Sciences, 580, 587–612.

[4] Zhao, X., Luo, H., & Yu, L. (2022). Reversible logic in cryptographic design: Opportunities and challenges. IEEE Transactions on Computers, 71(11), 2810–2824.

[5] Al-Saadi, A., Al-Mutairi, F., & Chen, Y. (2025). A chaos-based augmented image encryption scheme for satellite images using Fredkin logic. Scientific Reports, 15, Article 37345.

[6] Chen, M., Liu, Y., & Hu, C. (2020). Color image encryption using multi-dimensional chaotic maps and DNA coding. Information Sciences, 545, 102–120.

[7] Wang, H., & Li, Y. (2021). A hyperchaotic image encryption algorithm based on the Lorenz system and pixel-level permutation. Optics & Laser Technology, 140, 107028.

[8] Zhao, Z., Zhang, W., & Dong, X. (2022). Reversible logic-based image encryption using Toffoli gates and 3D chaotic maps. IEEE Access, 10, 75612–75625.

[9] Singh, R., Gupta, P., & Al-Khalaf, M. (2023). Augmented image encryption for multispectral satellite images using hybrid chaos. Journal of King Saud University – Computer and Information Sciences, 35(2), 145–156.

[10] Lin, Y., Zhang, C., & Chen, T. (2024). A multi-chaotic system for secure and fast image encryption based on hybrid permutation–diffusion. Signal Processing, 214, 109108.

[11] Qureshi, N., Al-Zahrani, M., & Zhang, L. (2024). Parallel GPU implementation of chaos-based cryptosystems for real-time image protection. IEEE Access, 12, 28400–28414.

[12] Luo, J., Fang, W., & Zhu, H. (2025). Performance analysis of Reed–Solomon error correction in secure image transmission. International Journal of Communication Systems, 38(6), Article 1452.

[13] Patel, T., Bhardwaj, V., & Singh, P. (2025). Analysis of multi-chaotic map fusion for high-entropy image encryption. Multimedia Tools and Applications, 84(5), 14217–14240.

[14] Sharma, A. (2024). Hybrid reversible logic with DNA-chaos cryptography for lightweight IoT image protection. IEEE Internet of Things Journal, 12(3), 2170–2183.

[15] Wang, K., Sun, Y., & Peng, Z. (2025). Secure satellite image transmission using adaptive hash-chaotic encryption and compression. Remote Sensing Letters, 16(2), 245–25