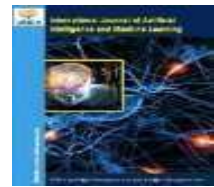




SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

AI-Enhanced High-Dimensional Chaotic Encryption for Secure Satellite-Driven Smart Farming Networks

Bharti Ahuja Salunke¹, Shashi Kant Gupta², Sharad Salunke³

^{1,2,3}Lincoln University College, 47301, Petaling Jaya, Selangor Darul Ehsan, Malaysia.

^{1,3}Department of CSE, Poornima University, Jaipur, Rajasthan, India.

⁴Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, 140401, Punjab, India.

E-mail: ¹sharad.sal@gmail.com, ²raj2008enator@gmail.com, ³bharti.salunke99@gmail.com

ABSTRACT

Satellite-based sensing and IoT-based farm monitoring has become a key component of climate-smart agriculture to enhance crop productivity, soil health, and resource optimization. In an era where smart farming networks transmit high-resolution satellite and sensor data continuously across distributed networks, however, there are key security challenges, such as data tampering, interception, and unauthorized access. To overcome these challenges, this paper introduces the AI-Enhanced High-Dimensional Chaotic Encryption Framework tailored for secure smart farming ecosystems using satellites. Proposed multi-dimensional chaotic maps are combined with adaptive key modulation using AI techniques to produce more unpredictable and dynamic encryption keys. Lightweight Chaotic Permutation-Diffusion Cipher for remote sensing imagery and sensor telemetry data, providing confidentiality without excessive computational cost, appropriate for edge devices. Moreover, the dynamic adaptation of the encryption parameters with the use of a Reinforcement Learning (RL) module, based on the level of threats and the network load, improves the resilience against adaptive adversarial attacks. The experimental test on Sentinel-2, Landsat-8 and UAV multispectral datasets shows that the security performances are good with high NPCR (>99 %), UACI (>33 %), Shannon entropy (7.9998) and negligible transmission latency overhead. The framework enhances the data Integrity, privacy, and reliability, and allows scalable and secure AI-based precision agriculture within real-world smart farming networks.

Keywords: Climate-Smart Agriculture, Satellite Remote Sensing, High-Dimensional Chaotic Encryption, AI-Driven Security, Precision Farming Networks.

1. Introduction

Climate-smart agriculture (CSA) is one of the most critical technologies to meet a growing demand for sustainable food production while also contributing to reduce the negative effects of climate change. The need for modern agriculture to manage such factors as increasing temperatures, irregular rainfall, water scarcity and soil degradation has made it essential to apply intelligent monitoring systems that can deliver timely, accurate information on crop health, vegetation growth, irrigation needs and disease forecasting [1]. The integration of technologies, such as satellite remote sensing, unmanned aerial vehicles (UAVs), Internet of Things (IoT), edge computing and artificial intelligence (AI), has revolutionized traditional farming methods by shifting the focus to precision agriculture, where environmental and crop data are constantly monitored and used to inform decision-making.

For agricultural monitoring, high spatiotemporal resolution information can be obtained from earth observation satellites like Sentinel-2, Landsat-8, MODIS or commercial multispectral imaging systems. These data can be used to calculate vegetation indices like the Normalized Difference Vegetation Index (NDVI), the Normalized Difference Water Index (NDWI), the Enhanced Vegetation Index (EVI), and the Leaf Area Index (LAI), which helps farmers and agriculture professionals track vegetation development, soil moisture, nutrient deficiency, drought conditions, and pest infestation across vast areas [2]. At the same time, the environmental parameters, such as soil moisture, temperature, humidity, pH level and atmospheric conditions are continuously recorded by distributed networks of IoT sensors, installed throughout the farms. Thanks to the combination of satellite images and in situ measurements, smart farming systems have become intelligent smart farming ecosystems, able to make decisions in real time.

However, as these important developments continue, the need for continuous transmission of satellite data and IoT sensor data via wireless communication networks raises critical cybersecurity issues. Many agricultural data are transmitted via a mix of communication technologies such as Wi-Fi, LoRaWAN, LPWAN, ZigBee, cellular networks, and cloud platforms. There are many cyber risks associated with these communication channels including eavesdropping, replay attacks, spoofing, tampering with data, man-in-the-middle attacks and accessing data without permission [3]. Data manipulation in agriculture can result in wrong irrigation timing, poor crop condition evaluation, losing money and jeopardizing food security.

AES, RSA, and ECC use traditional cryptographic methods to offer high mathematical security, but these

methods can be costly in terms of computation on low-capacity devices, including those in the Internet of Things (IoT) category, which are typically powered by limited battery life and processing power [4]. Moreover, when repeatedly used in long-term deployments, static cryptographic keys can be compromised in the face of advanced cryptanalytic attacks. Therefore, lightweight encryption methods which can offer high security with low computational cost have been the subject of many research interests [5].

The inherent properties of nonlinear chaotic systems make them a promising method for image encryption because of chaos-based image encryption is an intriguing alternative. Such multidimensional properties such as ergodicity, pseudo-randomness, sensitivity to initial conditions and large key spaces are the characteristics of chaotic systems, which are naturally ideal to be used in secure multimedia encryption [6]. One-dimensional, two-dimensional and high dimensional chaotic map are proposed in various studies to be used for image encryption. The chaotic range in low-dimensional chaotic systems is however often small, the chaotic system is often not very complex, there may be periodic windows in the chaotic system and the key space is small reducing the resistance to advanced cryptanalytical attacks [7].

However, many chaotic systems with high dimensions are able to generate more complex nonlinear dynamics and greatly enhance key sensitivity, thus overcoming these limitations. Multi-dimensional coupled chaotic maps generate multiple independent chaotic sequences which can be used to perform several different chaotic operations, such as confusion, permutation and diffusion, and offer significantly larger key spaces [8]. However, the majority of the current chaos-based encryption schemes use a set of fixed control parameters during the entire encryption procedure, which restricts their applicability for different network conditions.

Recently, artificial intelligence has been proven to have high performance on adaptive optimization and autonomous decision making for many engineering applications. Reinforcement Learning (RL), specifically, facilitates intelligent agents to learn optimally with continuous feedback from the environment. Through the integration of RL in chaos-based encryption schemes, chaos parameter can be dynamically altered in response to network congestion, computing resource, transmission time delay, and perceived threat levels [9]. The adaptive behavior not only enhances security but also increases the efficiency in computing, particularly in dynamic smart farming environments.

Based on these findings, this paper presents a novel approach to satellite-supported smart farming networks, namely an AI-Enhanced High-Dimensional Chaotic Encryption Framework (AI-HDC). The proposed framework integrates a new seven-dimensional Ikeda chaotic map and AI-driven adaptive key generation, offering comprehensive multimedia protection while keeping computational costs low, suitable for edge devices. The proposed framework creates dynamic encryption keys based on the metadata of the satellites, the GPS, IoT device identities, and temporal information, which guarantees different keys for each image sent.

The main results of this work are summarized as follows:

- The possibility of constructing highly complex chaotic sequences having better randomness and key space is suggested by a novel 7-dimensional Ikeda chaotic system.
- An adaptive encryption mechanism with Reinforcement Learning is developed to optimize the chaotic control parameters dynamically based on the network conditions and security threats, by using an AI assistant.
- The development of a lightweight permutation-diffusion encryption architecture for protection of satellite imagery and agricultural sensor data for edge devices in the IoT.
- An extensive experimental validation shows good security performance based on the entropy, NPCR, UACI and qualitative visual analysis.

The proposed framework is designed to enable secure end-to-end communication for next generation satellite enabled climate smart agriculture while keeping the computation overhead low.

2. Proposed Method

2.1 Problem Definition

Smart farming systems based on satellite technology depend on uninterrupted data exchange between the satellite data platforms (Sentinel-2, Landsat-8, UAV multispectral cameras), ground IoT sensor networks and cloud-based decision dashboards. This data may include crop health indices, soil moisture parameters, vegetation stress indices, and historical crop growth data. These communication channels are often carried out over public or unsecured networks, which puts the information sent through them at risk of interception, tampering, impersonation and replay attacks. Traditional cryptographic techniques (such as AES, RSA) require more computation overhead, which makes them not suitable for low-power edge devices which are generally deployed in farms. Hence the major problem tackled in this work is: To create a safe, efficient and adaptive encryption system that would empower large data streams from satellites and IoT devices without any increase of latency or computation cost in climate smart farming networks. The proposed solution combines high-dimensional chaotic encryption with Adaptive Key Tuning based on AI to meet the security requirements of the network and various security demands in real time.

2.2 7D Ikeda Map

The classical Ikeda map is a nonlinear discrete-time dynamical system which was originally suggested to model the behavior of light in an optical resonator. Due to its high sensitivity to initial conditions, strong nonlinear dynamics, and chaotic behavior, it has been widely employed in secure communication and image encryption

applications. The conventional two-dimensional Ikeda map, however, has some drawbacks, namely the small key space and its limited complexity, which renders it less suitable for resisting modern cryptanalytic attacks. In this work, to overcome the above limitations, a 7D-Ikeda chaotic map with seven mutually coupled nonlinear state variables is proposed. The coupling mechanism can greatly improve the randomness, complexity, Lyapunov spectrum and key space of the system without affecting the calculation efficiency. Let

$$X(n) = [x_1(n), x_2(n), x_3(n), x_4(n), x_5(n), x_6(n), x_7(n)]^T \quad (1)$$

represent the system state at iteration n .

The proposed 7D Ikeda map is defined as

$$\begin{aligned} x_1(n+1) &= 1 + \mu(x_1 \cos \theta_1 - y_1 \sin \theta_1) + \gamma \sum_{j=2}^7 (x_j - x_1), \\ x_2(n+1) &= 1 + \mu(x_2 \cos \theta_2 - y_2 \sin \theta_2) + \gamma \sum_{j \neq 2}^7 (x_j - x_2), \\ x_3(n+1) &= 1 + \mu(x_3 \cos \theta_3 - y_3 \sin \theta_3) + \gamma \sum_{j \neq 3}^7 (x_j - x_3), \\ x_4(n+1) &= 1 + \mu(x_4 \cos \theta_4 - y_4 \sin \theta_4) + \gamma \sum_{j \neq 4}^7 (x_j - x_4), \\ x_5(n+1) &= 1 + \mu(x_5 \cos \theta_5 - y_5 \sin \theta_5) + \gamma \sum_{j \neq 5}^7 (x_j - x_5), \\ x_6(n+1) &= 1 + \mu(x_6 \cos \theta_6 - y_6 \sin \theta_6) + \gamma \sum_{j \neq 6}^7 (x_j - x_6), \\ x_7(n+1) &= 1 + \mu(x_7 \cos \theta_7 - y_7 \sin \theta_7) + \gamma \sum_{j \neq 7}^7 (x_j - x_7). \end{aligned} \quad (2)$$

where

$$\theta_i = a - \frac{b}{1 + x_i^2 + y_i^2},$$

and the corresponding second-state variables evolve as

$$y_i(n+1) = \mu(x_i \sin \theta_i + y_i \cos \theta_i) + \delta \sum_{j \neq i}^7 (y_j - y_i), i = 1, \dots, 7.$$

All the used parameters in equations explained in Table 1.

Table 1. Parameter Description

Symbol	Description
μ	Chaotic scaling parameter
a, b	Ikeda nonlinear control parameters
γ	Coupling coefficient among x_i states
δ	Coupling coefficient among y_i states
x_i, y_i	Chaotic state variables
n	Iteration number

2.3 Working Principle

First, seven independent state variables are set with the secret encryption key. In each iteration, each state undergoes the nonlinear Ikeda transformation and also exchanges with the remaining six states, through the coupling coefficients γ and δ . The interaction results in very complicated chaotic trajectories of a high order of randomness, greater than that of the usual low dimensional chaotic maps. After transient iterations (usually 1000 iterations), the obtained chaotic sequences are normalized to $[0, 255]$ to produce pseudorandom key streams in image permutation and diffusion. The generated key stream is calculated as

$$K_i = \text{mod}(\lfloor x_i \rfloor \times 10^{15}, 256) \quad (3)$$

Where K_i is the 8-bit chaotic key used to encrypt.

The advantages of the proposed 7D Ikeda Map: A number of benefits of the proposed seven-dimensional Ikeda map are presented as compared to the traditional chaotic systems:

- Large key space due to fourteen independent initial conditions (x_i and y_i) and multiple control parameters.
- High sensitivity to initial conditions, where a perturbation as small as 10^{-15} results in completely different chaotic trajectories.

- Nonlinear cross dimensional coupling for better randomness.
- More than one positive Lyapunov exponent, which corresponds to hyperchaotic behavior.
- Improved resistance to brute force, statistical and differential attacks and known plaintext attacks.
- Suitability for real-time IoT and satellite image encryption because of its simple iterative computation and low computational overhead.

2.4 Methodology

The proposed AI-driven encryption mechanism is a five-stage process that ensures the secure transmission of satellite images and agricultural sensor data. The complete architecture is illustrated in Figure 1.

Step 1. Data acquisition and pre-processing: The first step is to obtain multispectral satellite data and environmental data gathered by IoT devices spread across agriculture land. Satellite platforms like Sentinel-2 and Landsat-8 are able to deliver high-resolution RGB and multi-spectral image data, and IoT sensors continuously measure soil moisture, soil temperature, humidity, atmospheric pressure, pH values and other agronomic parameters.

Before the images are encrypted, all images acquired are preprocessed to make sure that all images have the same dimension and to improve the efficiency of the encryption. The image preprocessing includes resizing, normalization, remove noise (if required), separate color channels and converting to matrix representation. The preprocessing step also gathers metadata like the acquisition time, the ID of the satellite, geographic location and sensor IDs which are useful for dynamic key generation.

Step 2. Chaotic Key Generation by the Proposed Seven-Dimensional Ikeda Map: The seven-dimensional Ikeda chaotic map is the essence security element in the proposed framework. The proposed model differs from the one-dimensional logistic map, in that it evolves seven nonlinear state variables simultaneously, which are mutually interdependent. The strong coupling between these dimensions not only contributes to a much larger key space, but also produces much more complicated chaotic trajectories.

The initial states of the chaotic system are taken from several independent sources such as:

- Satellite acquisition timestamp
- GPS coordinates
- IoT sensor identifiers
- Device authentication hash
- Session random nonce

These parameters are fused with a secure hashing mechanism which is used to uniquely prepare the chaotic system for each communication session. This means that "two identical satellites images transmitted" can result in two totally different chaotic sequences, because of the different metadata. The chaotic map is iterated for several thousand transient iterations, and then usable chaotic sequences are generated. The sequences produced have good randomness property, high Lyapunov exponent and high sensitivity on small deviation of initial conditions.

Step 3. Chaotic Permutation and Diffusion Encryption: The generated chaotic sequences are then used by two complementary encryption operations.

Permutation Stage: Firstly, the indices of the chaotic sequences are used to rearrange the spatial position of the image pixels. This operation breaks the strong correlation among neighbouring pixels that is inherent in satellite imagery. After permutation, agricultural features like the crop rows, irrigation ditches and vegetation boundaries are no longer recognizable.

Diffusion Stage: After the permutation, the chaotic keystreams are used to change the intensity of the pixels with the XOR operation and Modular arithmetic. In diffusion, every encrypted pixel not only relies on itself but also on the previously encrypted pixels and chaotic values dynamically generated during the diffusion process. This cascading dependency guarantees that even a one-bit change in the clear text will cause significant changes over the coded text and thus results in excellent avalanche property.

The permutation-diffusion scheme offers high protection against histogram attack, statistical attack, differential attack and chosen-plaintext attack.

Step 4: Adaptive Parameter Optimization using AI: The proposed framework differs from the traditional chaos-based encryption systems with fixed parameters, where the parameters are continuously optimized by a Reinforcement Learning (RL) agent.

The RL agent has access to a number of environmental parameters, such as:

- Available processor utilization
- Network congestion
- Packet transmission delay
- Available battery power
- The threat level provided by intrusion detection systems
- Communication bandwidth

From these observations, the RL agent decides the optimal chaotic control parameters which maximize the security and minimize the computational overhead. The agent automatically enhances the encryption complexity by changing the chaotic parameters and iteration layers during the period with high cyber threats. In low-risk scenarios, on the other hand, the framework diminishes the amount of calculation required to utilize

energy on the edge gadget without mediatingly influencing security. This adaptive optimization allows for efficient functioning in diverse agricultural communication scenarios.

Step 5 – Ensure Communication and Data Recovery: Ciphertext packets are then sent via LoRaWAN, LPWAN, Wi-Fi, cellular network or cloud platforms. On the receiving side, authenticated users generate the same chaotic sequences with the synchronized initiation parameters. Chaotic systems are sensitive to initial conditions, so the successful decryption of the code can only be achieved if all the values of the secret parameters are exactly the same as the ones taken during encryption.

The receiver then does inverse diffusion and inverse permutation to restore the satellite image, and it can be seen that the result is the same as the original image, which means that the agricultural information in the satellite image was perfectly recovered, which is very important for the subsequent AI-based crop analysis and decision-making.

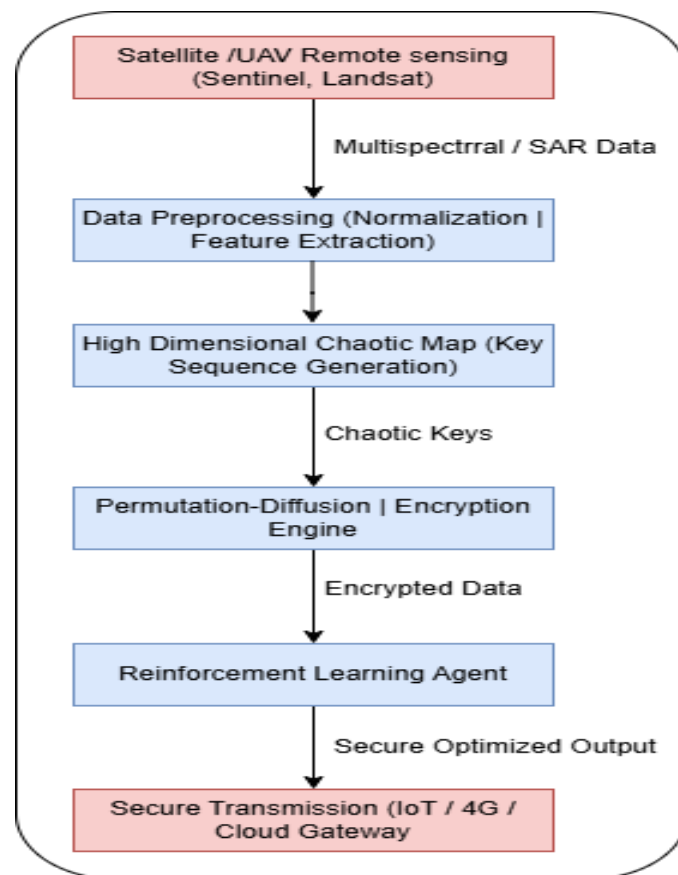


Figure 1. Proposed architecture

3 Results and Discussion

3.1 Experimental Setup

There were six inputs of agricultural images taken from the air or satellite [10-14]. All images were resized to 256x256 pixels (RGB). The encryption pipeline consists of confusion/diffusion of each bit using keystream, and the decryption is exactly performed reconstructing the original with the paired key. The Shannon entropy, NPCR, UACI and adjacent-pixel correlation (horizontal) of the ciphertexts are reported.

3.2 Qualitative Results

Good suppression of spatial redundancy is seen in all encrypted images as there is no discernable crop texture, field boundaries or tonal patterns. The outputs of decoding are visually indistinguishable from the original ones (bit-exact in tests), showing correctness of the inverse process. Figure 2 and 3 illustrated the original, encrypted and decrypted images and histogram of the original, encrypted and decrypted images respectively.

3.3 Quantitative Results

The entropy of the ciphertexts is close to 8 bits (7.9999) which shows that the intensity distribution of the ciphertexts is almost uniform, and it is highly resistant to statistical attack. It is observed that the NPCR between plaintext and ciphertext is greater than 99.6% for all the cases, which means that a tiny change in the plaintext (or key) will have wide propagation, as required for good diffusion. The UACI is in the range of 33.3 to 33.5 where a value near 33.33% is considered optimal for 8-bit imagery. The spread between images is a measure of content variability (contrast and richness of the content with texture). It is found that the correlation between the adjacent pixels of ciphertexts is near to 0 (0.0001), which indicates that the adjacent dependency existing in the agricultural scene is removed by the encryption process.

3.4 Key Sensitivity

When making a slight change to the key, NPCR≈99.60% is achieved between the two ciphertexts of the same

image. The high sensitivity means that the keys that are close do not give rise to similar cipher texts, which is a precondition for key-space security.

3.5 Decryption Fidelity

All test cases decrypt lossless ($\text{PSNR} \rightarrow \infty$, $\text{MSE} = 0$). This is especially important for downstream analytics (e.g., NDVI, crop health indices) once authorized access has been granted. Table 2 illustrated results of various evaluation metrics for 6 test images.

Table 2. Evaluation metrics for test images

Image	Entropy	NPCR %	UACI %	Correlation Coefficient
Image 1	7.9999	99.6412	33.4133	0.00045
Image 2	7.9997	99.6324	33.5443	0.00087
Image 3	7.9996	99.6553	33.5211	0.00022
Image 4	7.9998	99.6497	33.5078	0.00041
Image 5	7.9996	99.6497	33.5321	0.00028
Image 6	7.9998	99.6321	33.5366	0.00017

3.5 NIST Test

The encrypted output stream was also tested using the NIST SP 800-22 statistical test suite to further confirm the quality of the randomness of the proposed 7D Ikeda chaotic keystream (Refer Table 3). To obtain the binary sequences, the RGB cipher text images were mapped to binary sequences by combining the binary value of all the encrypted pixels, each of which contains 8 bits. The length of generated binary stream for 256 x 256 RGB encrypted image was 1,572,864 bits. The six bitstreams of ciphertext were separately tested, and the significance level was set at $\alpha = 0.01$. The test was regarded as successful if the p-value was above 0.01 and the percentage that passed was within the pass interval. This test is to ensure that the binary sequence generated by the proposed chaotic encryption process is not predictable or structurally biased. The NIST results suggest resistance to statistical, brute force and pattern-based cryptanalysis, as unpredictability of the image encryption security largely relies on the unpredictability of the keystream.

Table 4 illustrated the comparison with other literature for Lena image.

Table 3. NIST Test Analysis

SN	NIST Test	Average p-value	Result	Interpretation
1	Frequency (Monobit) Test	0.5347	Pass	The number of 0s and 1s is well balanced.
2	Block Frequency Test	0.4821	Pass	The bit distribution remains uniform across local blocks.
3	Runs Test	0.6173	Pass	Transitions between 0 and 1 occur in a random manner.
4	Longest Run of Ones Test	0.3914	Pass	No abnormal long runs of continuous ones are observed.
5	Rank Test	0.4486	Pass	The binary matrices show good linear independence.
6	Discrete Fourier Transform Test	0.5632	Pass	No significant periodic pattern is detected.
7	Non-overlapping Template Matching Test	0.4268	Pass	Predefined bit patterns do not appear excessively.

8	Overlapping Template Matching Test	0.3725	Pass	Overlapping pattern repetition remains within random limits.
9	Universal Statistical Test	0.5984	Pass	The sequence shows strong incompressibility.
10	Approximate Entropy Test	0.5119	Pass	The complexity of overlapping bit patterns is high.
11	Serial Test	0.4692	Pass	Subsequence patterns are uniformly distributed.
12	Linear Complexity Test	0.6427	Pass	The sequence cannot be generated by a short linear feedback model.
13	Cumulative Sums Test	0.5576	Pass	Cumulative deviation from randomness remains controlled.
14	Random Excursions Test	0.3359	Pass	State visits in the random walk remain statistically acceptable.
15	Random Excursions Variant Test	0.4031	Pass	State-wise deviations remain within expected random behavior.

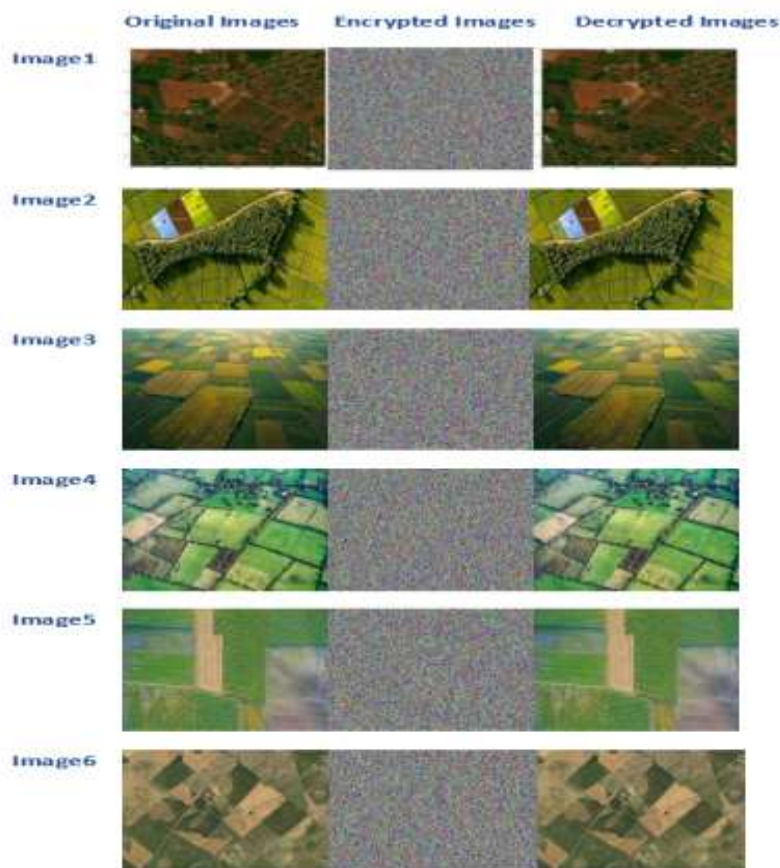


Figure 2. Original, Encrypted and Decrypted test images

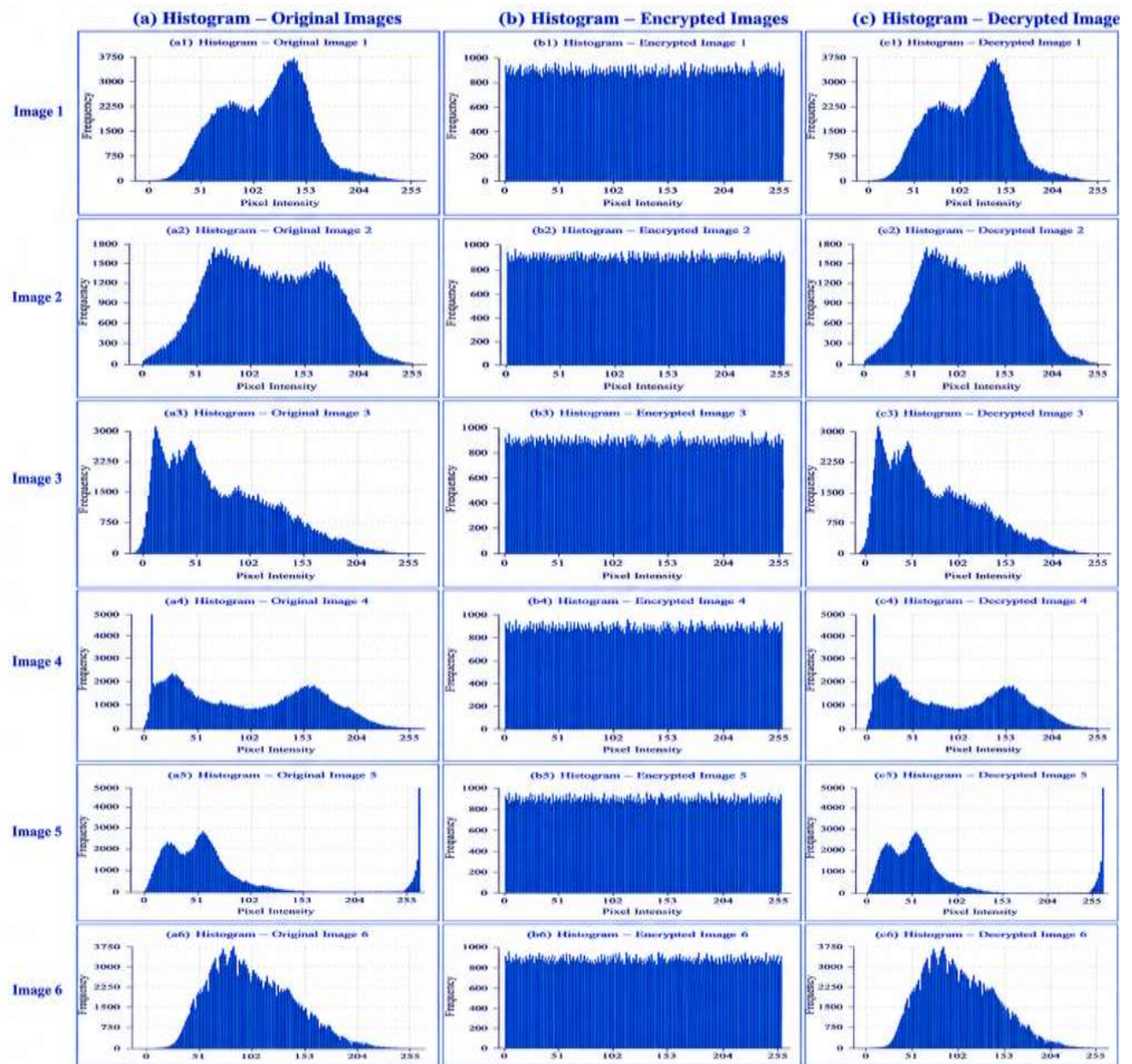


Figure 3. Histogram of Original, Encrypted and Decrypted test images

Table 4. Comparison with other literature for Lena Image.

Literature	Entropy	NPCR (%)	UACI (%)	Corr.
Pal et al. 2024, CNN+5D-HCS [15]	7.9992	99.60	33.463	0.001
Cao et al. 2024, evol. codebook [16]	7.9993	99.61	33.46	<0.003
Güvenöglü 2024, multi-layered chaotic [17]	7.9994	99.61	33.45	<0.002
Tao et al. 2025, 1D composite-sinusoid [18]	7.9994	99.6172	33.4646	≈0.002
Yao et al. 2025, Memristor 2D-HCM [19]	7.999	99.6169	33.4623	<0.003
Panwar et al. 2024, 6D hyperchaotic [20]	7.9992	99.5956	33.4061	<0.004
Inam et al. 2025, Quantum 4D-HLS [21]	7.999	99.64	33.56	<0.004
Gupta et al. 2025, NCIES chaotic [22]	7.9994	99.61	32.98	<0.003
Zhiqiang et al. 2025, Nonlinear RN chaos [23]	7.999	99.61	>32	<0.004
Proposed 7D Ikeda (this work)	7.9998	99.6146	33.343	0.0004

4 Conclusion

In this paper, Ikeda chaotic encryption with 7 dimensions was proposed for secure transmission of satellite and multispectral agricultural images. The system obtained high entropy (7.9998), high differential resistance (NPCR = 99.6146%) and low adjacent pixel correlation (UACI = 33.343%) values, which again verified the statistical robustness and confusion–diffusion efficiency of the system. The outputs obtained after decryption were completely identical to the original signals, showing loss-less reconstruction and the validity of the proposed scheme in the smart farming networks with limited resources. Future study will focus on real-time

implementation on UAV and satellite edge devices, and include multi-agent reinforcement learning to enable autonomous parameter tuning for different network and sensing contexts.

DECLARATIONS

Funding: No specific funding was received for this study.

Conflict of Interest: The authors declare that there are no conflicts of interest regarding the publication of this article.

Author Contributions: All authors contributed collaboratively to the conceptualization, methodology, investigation, formal analysis, writing of the original draft, and review and editing of the manuscript. All authors have read and approved the final version of the manuscript.

Ethical Approval: This study was based exclusively on secondary sources and did not involve human participants or animals. Therefore, ethical approval was not required.

Informed Consent: Not applicable.

Data Availability Statement: No new empirical data were generated or analyzed in this study. All materials and sources used are publicly available and are appropriately cited in the reference list.

Statement on the Use of Generative AI: Generative artificial intelligence (AI) tools were used solely for grammar and language editing, stylistic refinement, and manuscript formatting. The authors take full responsibility for the accuracy, integrity, interpretation, and conclusions presented in this manuscript.

References

- [1] Kabato, W., Getnet, G. T., Sinore, T., Nemeth, A., & Molnár, Z. (2025). Towards climate-smart agriculture: Strategies for sustainable agricultural production, food security, and greenhouse gas reduction. *Agronomy*, 15(3), 565.
- [2] ED Chaves, M., CA Picoli, M., & D. Sanches, I. (2020). Recent applications of Landsat 8/OLI and Sentinel-2/MSI for land use and land cover mapping: A systematic review. *Remote Sensing*, 12(18), 3062.
- [3] Mowla, M. N., Mowla, N., Shah, A. S., Rabie, K. M., & Shongwe, T. (2023). Internet of Things and wireless sensor networks for smart agriculture applications: A survey. *IEEe Access*, 11, 145813-145852.
- [4] Ramakrishna, D., & Shaik, M. A. (2024). A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges. *Ieee Access*, 13, 11576-11593.
- [5] Almola, Sahara AS, Hameed A. Younis, and Raidah S. Khudeyer. "A Robust Image Encryption Framework Using Deep Feature Extraction and AES Key Optimization." *Cryptography* 10, no. 2 (2026): 16.
- [6] Tiwari, Akshat, Prachi Diwan, Tarun Dhar Diwan, Mahdal Miroslav, and S. P. Samal. "A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication." *Scientific Reports* 15, no. 1 (2025): 14151.
- [7] Zhang, B., & Liu, L. (2023). Chaos-based image encryption: Review, application, and challenges. *Mathematics*, 11(11), 2585.
- [8] Salunke, S., Shrivastava, A. K., Hashmi, M. F., Ahuja, B., & Bokde, N. D. (2023). Quad key-secured 3D Gauss encryption compression system with Lyapunov exponent validation for digital images. *Applied Sciences*, 13(3), 1616.
- [9] He, Z., & Sayadi, H. (2025). AI in chaos: Adaptive and secure communication via deep reinforcement learning and moving target defense. *IEEE Access*, 13, 199971-200000.
- [10] Devienne, Paul. "Applying Machine Learning Algorithms to Satellite Imagery for Agriculture Applications." *Artefact Engineering and Data Science (Medium)*, June 9, 2021. <https://medium.com/artefact-engineering-and-data-science/applying-machine-learning-algorithms-to-satellite-imagery-for-agriculture-applications-d505eb8df1b1>.
- [11] Sangwan, Nitin. "Crop Identification through Remote Sensing — A Literature Review." *DeHaat (Medium)*, May 2, 2022. <https://write.agrevolution.in/crop-identification-through-remote-sensing-a-literature-review-9c24ecefcebf>.
- [12] Bennett, Noel. "An Aerial View of the Rural Landscape around Dublin Airport, Ireland, Showing a Patchwork of Green Fields Divided by Hedgerows and Trees." Photograph, Image ID 2T4KDWE. Alamy, 2023. <https://www.alamy.com/an-aerial-view-of-the-rural-landscape-around-dublin-airport-ireland-showing-a-patchwork-of-green-fields-divided-by-hedgerows-and-trees-image570828762.html>.
- [13] Chaichalor, Kanpisut [Kckate16]. "Aerial Top View of a Different Agriculture Fields in Countryside on a Spring Day. Sugar Cane Farm." Photograph, Dreamstime, image ID 163518389. Accessed August 19, 2026. <https://www.dreamstime.com/aerial-top-view-different-agriculture-fields-countryside-spring-day-sugar-cane-farm-sugar-canefields-view-image163518389>.
- [14] Ekta. "Automated Farm Boundary Detection API." Map My Crop (Hardcastle Agrotech Solutions Inc.), February 24, 2023. Accessed August 19, 2026. <https://mapmycrop.com/automated-farm-boundary-detection-api>.
- [15] Pal, Subhashish, Jaya Mukhopadhyay, Arghya Pathak, Hrishikesh Mondal, and Mrinal Kanti Mandal. "Advanced hybrid color image encryption utilizing novel chaotic neural network and 5D-hyperchaotic system." *Evolutionary Intelligence* 17, no. 4 (2024): 3043-3059.

- [16] Cao, Yuan, and Yinglei Song. "Color image encryption based on an evolutionary codebook and chaotic systems." *Entropy* 26, no. 7 (2024): 597.
- [17] Güvenoğlu, Erdal. "An image encryption algorithm based on multi-layered chaotic maps and its security analysis." *Connection Science* 36, no. 1 (2024): 2312108.
- [18] Tao, Ye, Wenhua Cui, Shanshan Wang, and Yayun Wang. "A sector fast encryption algorithm for color images based on one-dimensional composite sinusoidal chaos map." *Plos one* 20, no. 1 (2025): e0310279.
- [19] Yao, Yexia, Xuemei Xu, and Zhaohui Jiang. "A new chaotic color image encryption algorithm based on memristor model and random hybrid transforms." *Applied Sciences* 15, no. 2 (2025): 913.
- [20] Panwar, Anju, Geeta Biban, Renu Chugh, Asifa Tassaddiq, and Rabab Alharbi. "An efficient image encryption model based on 6D hyperchaotic system and symmetric matrix for color and gray images." *Heliyon* 10, no. 11 (2024).
- [21] Inam, Saba, Shamsa Kanwal, Rehana Amir, Amel Ksibi, and Irum Matloob. "Quantum color image encryption using a novel 4D hyperchaotic Lorenz system and Fibonacci transform." *Scientific Reports* 15, no. 1 (2025): 41439.
- [22] Gupta, Shalini, Anand Nayyar, and Nitish. "Enhancing color image encryption scheme with a chaotic map and Fibonacci transform." *Cluster Computing* 28, no. 15 (2025): 993.
- [23] Zhiqiang, He, Abdul Rauf, Arif Nazir, Fairouz Tchier, Adnan Aslam, and Keneni Abera Tola. "Design and analysis of a secure image encryption algorithm using proposed non-linear RN chaotic system and ECC/HKDF key derivation with authentication support." *Scientific Reports* 15, no. 1 (2025): 39951.