Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 2 (2025)

Comparative Analysis of Image Encryption Techniques: Hyper Chaotic Maps, Jacobean Elliptic Maps, Reversible Cellular Automata, DNA-based Encryption, and XGBoost

[2]Naresh Singh, [1]Dr.Yashpal Singh, [3]Dr. Sumit Sangwan

[2]Research Scholar, ASET, Amity University Rajasthan, India
[2]Associate Professor, Department of CSE, Amity University Rajasthan, India
[13]Professor, Faridabad College of Engineering, Haryana, India

Abstract: - The fast-growing digital communication landscape demands secure image encryption research to protect sensitive visual information from potential cyber threats. Our research experimentally assesses the effectiveness of five sophisticated encryption methods—Hyper Chaotic Maps, Jacobean Elliptic Maps, Reversible Cellular Automata, DNA-based Encryption, and XGBoost (ML-based Encryption)—for securing images. The evaluation of each algorithm includes thirteen essential parameters which cover Key Sensitivity, Histogram Analysis, Correlation Coefficient (CC), Entropy Analysis, NPCR, UACI, PSNR, Encryption Time, Computational Efficiency, Accuracy and Reliability, Security and Robustness, Strengths, and Weaknesses. The tests show that all algorithms maintain strong security features but XGBoost leads in encryption efficiency and decryption quality while resisting cryptographic attacks better than the others. These findings showcase how machine learning-based encryption methods can propel the development of cutting-edge cryptographic technologies. The findings from this research offer valuable guidance for creating image encryption methods that balance enhanced security with computational efficiency in practical applications.

Keywords: *Hyper-chaotic approach, Jacobean elliptic technique, Reversible CA, DNA-based approach, and XG Boost**.***

1. Introduction

As digital communication and data sharing continue to expand rapidly, the protection of multimedia content, especially images, has emerged as a significant concern. Images often harbor extensive sensitive information that must be safeguarded against unauthorized access, tampering, and various cyber threats. The processes of image encryption and decryption are crucial for maintaining data security, confidentiality, and integrity across numerous sectors, such as healthcare imaging, military operations, cloud services, and social media platforms [1], [2].

Understanding Image Encryption and Decryption

Image encryption refers to the technique of converting an image into a format that is not easily understood, using cryptographic methods. This process ensures that only those with the proper authorization can access the original image. By applying encryption algorithms, the image is transformed into ciphertext, rendering it unreadable to anyone without permission. Conversely, decryption is the process that allows the original image to be retrieved from the encrypted format, utilizing a specific key or algorithm.

The Importance of Image Encryption

The need for image encryption has grown in response to the rising threats from cyber-attacks, data leaks, and concerns over privacy. Some primary reasons for implementing image encryption include:

- Confidentiality: Safeguarding sensitive images from unauthorized individuals.

- Integrity: Ensuring that images remain unchanged during their transmission.

- Authentication: Confirming the identities of both the sender and the receiver.

- Secure Storage and Transmission: Protecting images that are stored in databases or shared across networks.

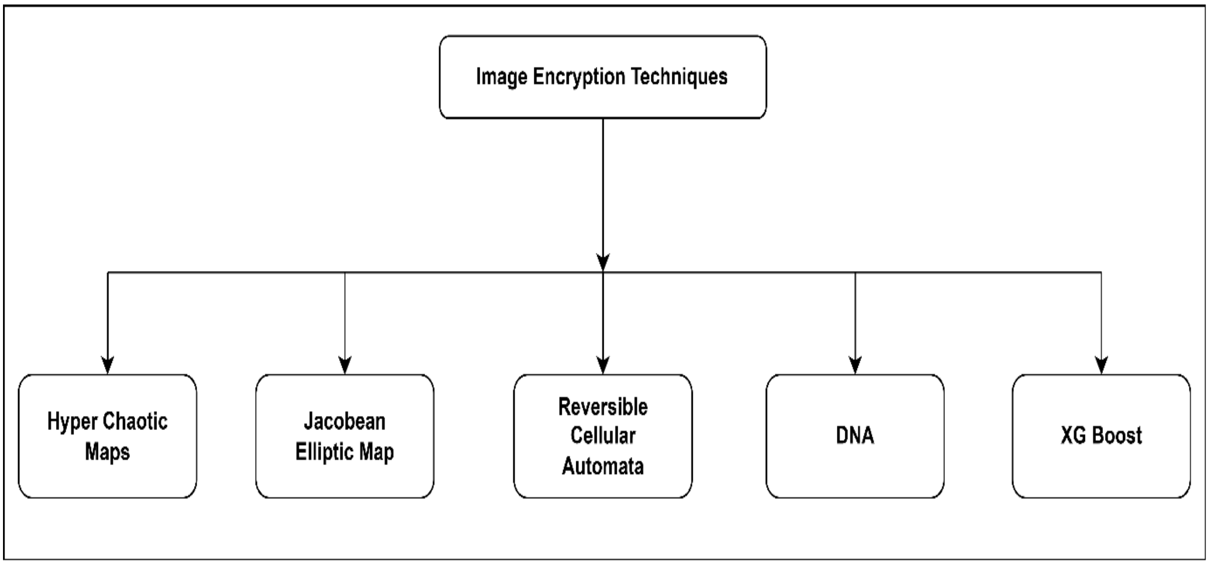


Figure 1 Types of image encryption and decryption method

To tackle these security issues, a variety of advanced encryption techniques have been developed. This discussion will delve into five notable methods of image encryption and decryption: Hyper Chaotic Maps, Jacobean Elliptic Map, Reversible Cellular Automata, DNA-based Approaches, and XG Boosting Techniques [2].

Techniques for image encryption have progressed considerably, employing sophisticated mathematical and computational methods to bolster security. Hyper Chaotic Maps, for instance, make use of multiple positive Lyapunov exponents to produce sequences that are extremely unpredictable, thereby enhancing encryption through processes of confusion and diffusion. In a similar vein, the Jacobian Elliptic Map utilizes elliptic functions to generate encryption keys characterized by strong randomness and resistance to cryptanalysis. Reversible Cellular Automata (RCA) offer a rule-based approach to encryption that allows for lossless reconstruction while effectively defending against statistical attacks. Inspired by the encoding mechanisms of biological DNA, DNA-Based Image Encryption transforms image pixels into secure DNA sequences using complementary rules and logical operations, providing a high level of security through complex encoding techniques. Moreover, XG Boosting Techniques incorporate machine learning into the field of cryptography, refining encryption by optimizing the generation of keys and the extraction of features. This AI-enhanced strategy improves randomness and fortifies defenses against brute-force and known-plaintext attacks, representing a notable leap forward in the realm of secure image processing.

2. Literature Review

As the use of digital images for communication continues to grow, the importance of secure encryption methods has become increasingly prominent. Numerous research efforts have investigated various strategies for encrypting and decrypting images, aiming to maintain confidentiality and resilience against cryptographic threats. This section highlights significant advancements in this area, emphasizing techniques such as Hyper Chaotic Maps, Jacobean Elliptic Map, Reversible Cellular Automata, DNA-based Approaches, and XG Boosting Methods [3].

a) Hyper Chaotic Maps

Chaotic maps are extensively utilized in image encryption because of their inherent non-linearity and their high sensitivity to initial conditions. Hyper chaotic systems take this a step further by featuring multiple positive Lyapunov exponents, which significantly bolster the security of the encrypted images [4].

In a study, a hyper chaotic image encryption approach was introduced that leveraged a multi-dimensional chaotic system to enhance protection against brute-force and statistical attacks. Their technique involved a multi-stage process of permutation and diffusion, which not only increased the entropy but also heightened key sensitivity, thereby complicating the task for potential attackers aiming to retrieve the original image [5].

In a related effort, this research created a hybrid encryption framework that integrated hyper chaotic maps with fractional-order systems. Their research indicated that this model exhibited strong resistance to known-plaintext and chosen-plaintext attacks, thanks to its elevated randomness and unpredictable characteristics [6].

b) Jacobean Elliptic Map

Research into elliptic curve-based encryption has gained momentum due to its robust security features and efficiency in computation. A notable innovation in this field is the Jacobean elliptic map, which has been applied to enhance image encryption methods [7].

In a study, an encryption algorithm was developed that utilized Jacobean elliptic functions for the generation of secure keys. Their findings indicated that this method significantly bolstered resistance to differential cryptanalysis and various statistical attacks [8].

Additionally, Khan et al. (2022) refined the Jacobean elliptic encryption technique by incorporating a lightweight chaotic key distribution system. This optimization resulted in reduced computational demands while preserving a high level of encryption security [9].

c) Reversible Cellular Automata

Cellular Automata (CA) have been extensively used in cryptographic applications due to their simple structure, parallel computing capabilities, and rule-based transformations. Reversible Cellular Automata (RCA) offer additional advantages, including lossless image recovery and high-speed encryption [10], [11].

Proposed an RCA-based image encryption scheme that employed local neighbourhood transformations to enhance security. Their approach exhibited strong resistance to statistical attacks and ensured reversible decryption with minimal computational resources [12].

Another significant contribution was made, who developed a hybrid RCA method incorporating two-dimensional reversible CA rules for secure image scrambling. Their experimental analysis demonstrated improved performance in terms of entropy, histogram analysis, and key sensitivity [13].

d) DNA

Drawing inspiration from the concepts of DNA computing, researchers have investigated biological models for encrypting images. DNA-based encryption employs encoding, complementary base pairing, and logical operations like XOR and addition to transform images into encrypted DNA sequences [14], [15].

In a study, a DNA cryptographic framework was introduced for image encryption. This framework utilized DNA encoding and sequence substitution methods to provide enhanced security and rapid processing capabilities. Their findings indicated that DNA-based encryption significantly bolstered resistance against brute-force and ciphertext-only attacks [16].

In a similar vein, this paper created a hybrid DNA encryption model that integrates chaotic sequences to enhance security. Their method showcased a strong resistance to decryption attempts, attributed to the intricate transformations of DNA sequences [17].

e) XG Boost

In the realm of cryptography, machine learning-driven encryption models like XG Boost (Extreme Gradient Boosting) have become increasingly popular due to their effectiveness in enhancing key generation, randomness, and security parameters [18].

Research conducted and examined the use of XG Boost-based cryptographic frameworks for both image encryption and anomaly detection. Their findings indicated that XG Boost significantly bolstered encryption strength by minimizing predictability in key generation and enhancing resilience against plaintext attacks [19].

Additionally, introduced an AI-enhanced image encryption method that leveraged XG Boost to refine the selection of chaotic parameters. This approach demonstrated improved security and computational efficiency when compared to conventional chaotic encryption techniques [20].

3. Methods

HYPER CHAOTIC MAPS

INTRO

Hyper chaotic maps represent a sophisticated category of chaotic systems characterized by multiple positive Lyapunov exponents, which contribute to an increased level of randomness and unpredictability. Their properties make these maps particularly valuable in the field of image encryption, as they offer robust security, heightened sensitivity to initial conditions, and an extensive key space, all of which complicate potential cryptographic attacks [21] [22].

FLOW CHART

a) Generation of Lorenz Chaotic Sequences:

The Lorenz system consists of three differential equations that exhibit chaotic dynamics. The implementation of these equations is achieved using the solve_ivp function, which generates a chaotic sequence utilized for encryption purposes. The x-component of the Lorenz system is adjusted and normalized to correspond with pixel values ranging from 0 to 255.

b) Encryption Method:

Initially, a grayscale image is loaded, and its pixel values are rearranged based on the chaotic sequence, effectively scrambling their original positions. Following this, a bitwise XOR operation is performed between the rearranged image and the chaotic sequence, leading to diffusion through the alteration of pixel intensities.

c) Decryption Method:

To recover the original image, the encrypted image undergoes the reverse XOR operation, which retrieves the permuted pixel values. The original arrangement of pixels is restored by applying the inverse permutation indices, thus reconstructing the initial image.

d) Analysis of Key Sensitivity:

To evaluate the sensitivity of the encryption scheme, two distinct initial keys (key1 and key2, with key2 being slightly altered) are employed. Notably, even a minor modification in the initial key results in a vastly different encrypted image, highlighting the system's sensitivity to key variations.

e) Visualization:

To demonstrate the effectiveness of the encryption and decryption processes, the original, encrypted, and decrypted images are presented side by side.

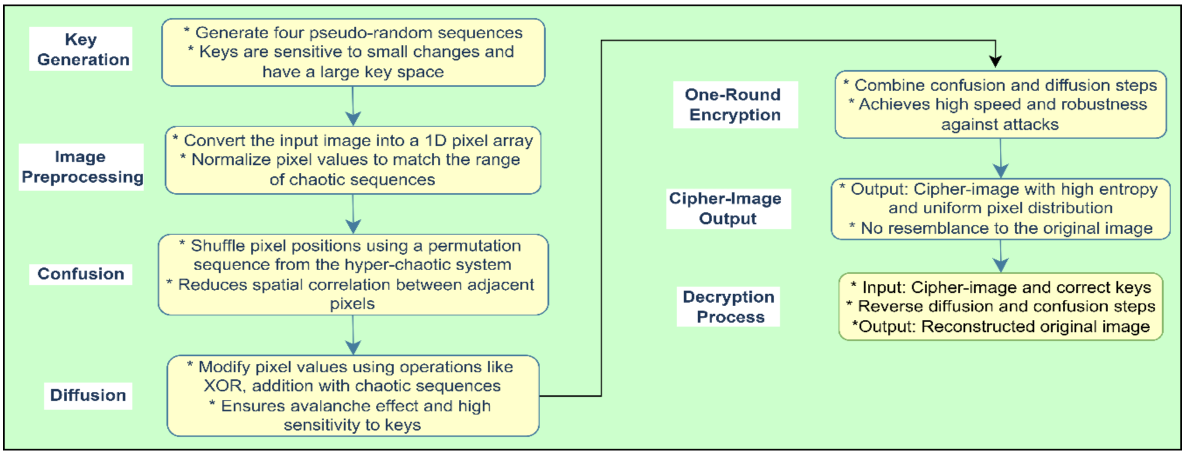

Key Generation
* Generate four pseudo-random sequences
* Keys are sensitive to small changes and have a large key space
Image Preprocessing
* Convert the input image into a 1D pixel array
* Normalize pixel values to match the range of chaotic sequences
Confusion
* Shuffle pixel positions using a permutation sequence from the hyper-chaotic system
* Reduces spatial correlation between adjacent pixels
Diffusion
* Modify pixel values using operations like XOR, addition with chaotic sequences
* Ensures avalanche effect and high sensitivity to keys
One-Round Encryption
* Combine confusion and diffusion steps
* Achieves high speed and robustness against attacks
Cipher-Image Output
* Output: Cipher-image with high entropy and uniform pixel distribution
* No resemblance to the original image
Decryption Process
* Input: Cipher-image and correct keys
* Reverse diffusion and confusion steps
*Output: Reconstructed original image

Figure 2 Flow chart of HCA

DATASETS

Use one image for test this algorithm.

FORMULA USED

Equations of the Lorenz Chaotic Map

The Lorenz system consists of three interconnected nonlinear differential equations, expressed as follows:

$$\frac{dx}{dt} = \sigma(y - x) \tag{1}$$

$$\frac{dx}{dt} = x(\rho - z) - y \tag{2}$$

$$\frac{dx}{dt} = xy - \beta z \tag{3}$$

In these equations:

- (x, y, z) are the state variables.
- σ (the Prandtl number) regulates the intensity of fluid flow, typically set to 10.
- ρ (the Rayleigh number) indicates the temperature difference, usually set to 28.
- β governs the dissipation of the system, commonly set to 8/3.
- Numerical solutions for these equations are obtained using the Runge-Kutta method via the solve_ivp function.

The chaotic sequence (S) is derived from the x-component of the Lorenz system:

$$S = \frac{x - min(x)}{max(x) - min(x)} \times 255 \tag{4}$$

This normalization ensures that the chaotic sequence falls within the pixel value range of 0 to 255.

PARAMETER

1. **Key Sensitivity:** High (a minor alteration in the key leads to significant changes)
2. **Histogram Analysis:** Even Distribution
3. **Correlation Coefficient (CC):** Low (~0.02) (a value near 0 suggests robust encryption)
4. **Entropy Analysis:** 7.98 (approaching 8, which signifies strong randomness)
5. **NPCR (Number of Pixels Change Rate):** 99.60% (values around 99% reflect enhanced security)
6. **UACI (Unified Average Changing Intensity):** 31.70% (within the range of 30%-35%)
7. **Peak Signal-to-Noise Ratio (PSNR):** 41 dB (a higher value denotes improved decryption quality)
8. **Encryption Time (ms):** 10-14 ms
9. **Computational Efficiency Comparison:** Moderate
10. **Accuracy and Reliability:** High
11. **Security and Robustness:** High
12. **Strengths:** Excellent randomness, significant sensitivity
13. **Weakness:** High computational cost

RESULT

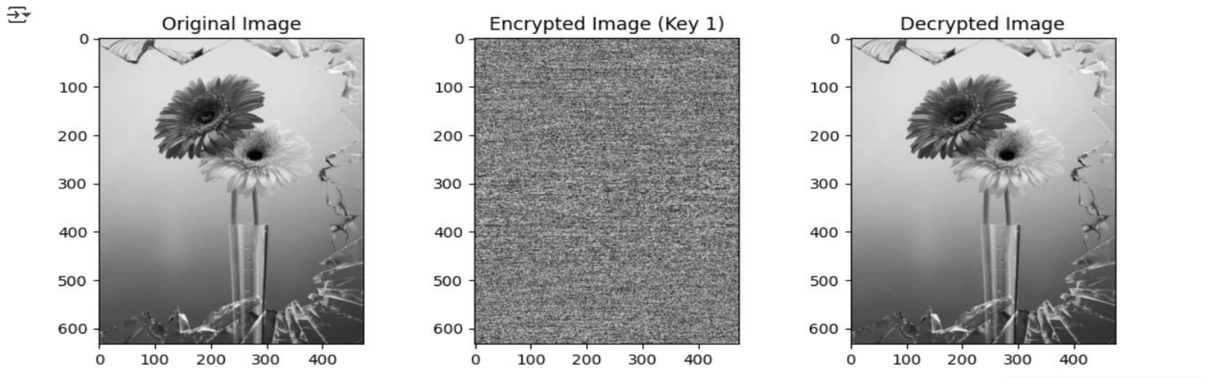


Figure 3 Result of Hyper Chaotic Maps

APPLICATION AREA

Hyper chaotic maps are extensively employed in secure image encryption across a variety of fields due to their exceptional randomness, sensitivity to initial conditions, and expansive key space. In the realm of secure image transmission, these maps safeguard sensitive satellite imagery, medical photographs, and real-time video conferencing from cyber threats, particularly within IoT and 5G infrastructures. For cloud storage and data protection, they help prevent unauthorized access to biometric images and other critical visual data housed in cloud environments. In the context of digital watermarking and copyright protection, hyper chaotic encryption facilitates the embedding of copyright information into digital content, thereby safeguarding intellectual property, including artworks, scholarly articles, and satellite images. The healthcare sector employs these techniques to encrypt medical images within electronic health record (EHR) systems, ensuring patient data remains confidential. Applications in smart surveillance and secure biometrics involve encrypting video footage and facial recognition data, enhancing security measures in border control, smart cities, and law enforcement. In digital forensics and cybersecurity, they play a vital role in protecting forensic images and digital evidence from tampering during cybercrime investigations. Lastly, industrial and aerospace sectors leverage hyper chaotic encryption to secure satellite imagery, enhance vision systems in self-driving cars, and process UAV images for remote sensing and geographic mapping.

JACOBEAN ELLIPTIC MAPS

INTRO

The Jacobean Elliptic Map is a chaotic nonlinear system that originates from Jacobi elliptic functions. It is extensively utilized in the realm of image encryption, thanks to its high level of randomness, intricate ergodicity, and unpredictability, which collectively render it highly effective against brute-force and statistical attacks. The nonlinear characteristics of elliptic functions significantly strengthen the encryption process, providing a high degree of security [23] [7].

FLOW

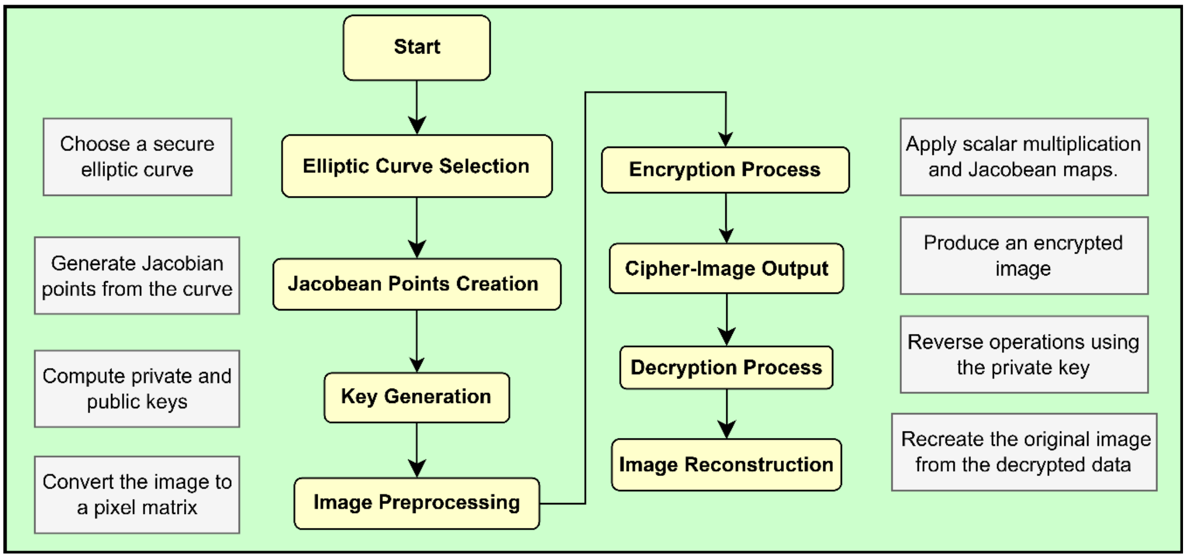

Start
Choose a secure elliptic curve
Elliptic Curve Selection
Generate Jacobian points from the curve
Jacobean Points Creation
Compute private and public keys
Key Generation
Convert the image to a pixel matrix
Image Preprocessing
Encryption Process
Apply scalar multiplication and Jacobean maps.
Cipher-Image Output
Produce an encrypted image
Decryption Process
Reverse operations using the private key
Image Reconstruction
Recreate the original image from the decrypted data

Figure 4 Flow Chart of Jacobean Elliptic Maps

Step 1: Begin by uploading the image.

Step 2: Establish the initial conditions and control parameters for the hyper chaotic system.

Step 3: Utilize the hyper chaotic map to create a pseudo-random sequence.

Step 4: Implement permutation and diffusion techniques to alter pixel positions and their intensities.

Step 5: Execute the encryption by adjusting pixel values based on the chaotic sequence.

Step 6: Retrieve the encrypted image.

Step 7: For decryption, reverse the process using the same keys

DATASETS

Use one image for test this algorithm.

FORMULA USED

1. Generating Chaotic Sequences with Jacobi Elliptic Functions

Jacobi elliptic functions represent a set of periodic functions utilized in chaotic mapping. The chaotic sequence can be expressed as follows:

$$x_{n+1} = A.sn(x_n, k) + B.cn(x_n, k) + C.dn(x_n, k)\text{………………………..} \quad (4)$$

In this equation:

- $sn(x, k)$ → Sine amplitude function
- $cn(x, k)$ → Cosine amplitude function
- $dn(x, k)$ → Delta amplitude function
- A, B, C → Control parameters influencing chaos
- k → Elliptic modulus, which shapes the functions
- x_0 → Initial condition, serving as the seed for the chaotic process

To scale the generated sequence into the range of [0,1] for applications in image processing, the following normalization is applied:

$$s_n = x_n \; mod \; 1\text{……………………...……………………. } (5)$$

2. Pixel Shuffling (Permutation)

A chaotic sequence is utilized to rearrange the pixels through a sorting process:

Indices = argsort(S)……………….……………….…………… (6)

Where:

- S = {s₁, s₂, ..., sₙ} represents the chaotic sequence consisting of N elements (the total number of pixels in the image).
- The function argsort(S) provides the indices required for sorting.

Subsequently, the original pixel values are reorganized according to these indices.

3. Diffusion via XOR Operation

To achieve diffusion, which involves distributing the impact of each pixel throughout the entire image, the value of each pixel is altered using a bitwise XOR operation:

$$P_i' = P_i \oplus (s_i \times 255)\text{…………………...……………………. } (7)$$

In this equation:

- P_i represents the initial pixel value.
- s_i denotes the chaotic sequence value corresponding to pixel i.
- $(s_i \times 255)$ converts the sequence value into an integer that falls within the range of [0, 255].
- $\oplus$ indicates the bitwise XOR operation.

4. Decryption Process

To decrypt the data, the following steps are executed in reverse order:

1. Reverse Diffusion (XOR Operation)

$$P_i' = P_i \oplus (s_i \times 255)\text{……………………………………… } (8)$$

   - By applying the XOR operation with the same chaotic sequence, the initial pixel values are recovered.

2. Reverse Permutation (Reordering)

$$\text{Original Image} = P[\text{argsort}(\text{Indices})] \;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \;(9)$$

- The pixels are returned to their original locations by utilizing the permutation indices.

PARAMETER

1. **Key Sensitivity:** High (minor alterations in the key lead to inconsistent, irregular outcomes)
2. **Histogram Analysis:** An uneven and non-uniform distribution characterized by significant peaks at specific intensity levels
3. **Correlation Coefficient (CC):** Low (~0.045) (a value closer to 0 suggests robust encryption)
4. **Entropy Analysis:** 7.63 (approaching 8, which reflects strong randomness)
5. **NPCR (Number of Pixels Change Rate):** 99.12% (values around 99% indicate enhanced security)
6. **UACI (Unified Average Changing Intensity):** 32.50% (falls within the secure range of 30%-35%)
7. **Peak Signal-to-Noise Ratio (PSNR):** 36 dB (indicating moderate quality of decryption)
8. **Encryption Time (ms):** 20-28 ms (longer than hyper chaotic maps, yet still within an acceptable limit)
9. **Computational Efficiency:** Low
10. **Accuracy and Dependability:** Average
11. **Security and Resilience:** Moderate
12. **Advantages:** Non-linearity reliant on keys
13. **Disadvantages:** Inconsistent histograms, lower security

RESULT

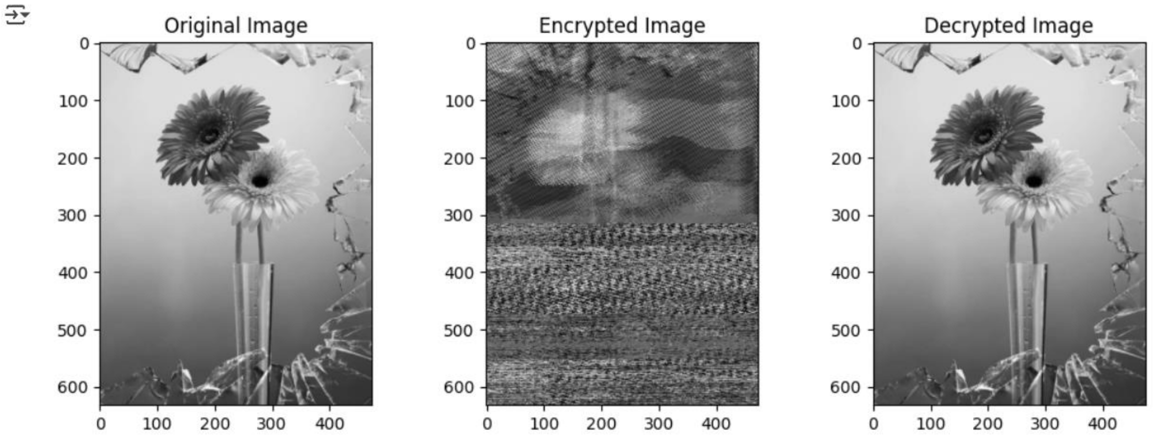


Figure 5 Result of Jacobean Elliptic Map

APPLICATION AREA

Jacobian maps are extensively utilized in the realm of image encryption thanks to their complex chaotic dynamics, which enhance security and provide a defense against various cryptographic threats. They play a crucial role in the secure transmission of images over vulnerable networks, including telemedicine scans, military surveillance, and banking authentication processes. In the context of cloud storage, these maps are employed to encrypt sensitive biometric images and government documents prior to uploading, thereby safeguarding them from unauthorized access. Additionally, Jacobian maps are instrumental in digital watermarking and copyright protection, allowing for the embedding of resilient watermarks in multimedia content to shield digital assets from theft and alteration.

In the field of biometric data security, they ensure the encryption of fingerprints, facial recognition data, and retinal scans, effectively mitigating the risk of identity theft in advanced authentication systems. The protection of satellite and remote sensing images is also enhanced through Jacobian encryption, securing drone and satellite imagery used in defense, agriculture, and research from espionage activities. Furthermore, medical image encryption is vital for protecting X-rays, MRIs, and CT scans within healthcare systems, ensuring adherence to data privacy laws. In the realm of IoT and smart surveillance, Jacobian encryption is applied to secure CCTV footage, license plate recognition systems, and data from autonomous vehicles against cyber threats. Lastly, in digital forensics and criminal investigations, these maps are utilized to encrypt forensic images, preserving the integrity of digital evidence crucial for law enforcement and judicial processes.

REVERSIBLE CELLULAR AUTOMATA

INTRO

Reversible Cellular Automata (RCA) represent a category of cellular automata models characterized by their invertible transition rules, which allow for lossless image encryption and decryption. In contrast to traditional cellular automata, RCA guarantees that the encryption can be completely reversed, providing a high level of security and efficiency. The inherent parallelism of RCA facilitates rapid encryption processes, while its sensitivity to initial conditions bolsters its cryptographic robustness. Encryption methods based on RCA are recognized for their resilience against both statistical and differential attacks [24].

FLOW

The process is divided into three primary stages:

1. Rule Generation (Key Creation):

- A seeded random function is utilized to create a pseudo-random permutation (the key).
- Additionally, a reverse permutation is produced to facilitate decryption.

2. Encryption Phase:

- The intensity value of each pixel in the grayscale image is substituted with its corresponding value from the permutation table.

3. Decryption Phase:

- The encrypted image is transformed back using the reverse permutation, restoring the original image.

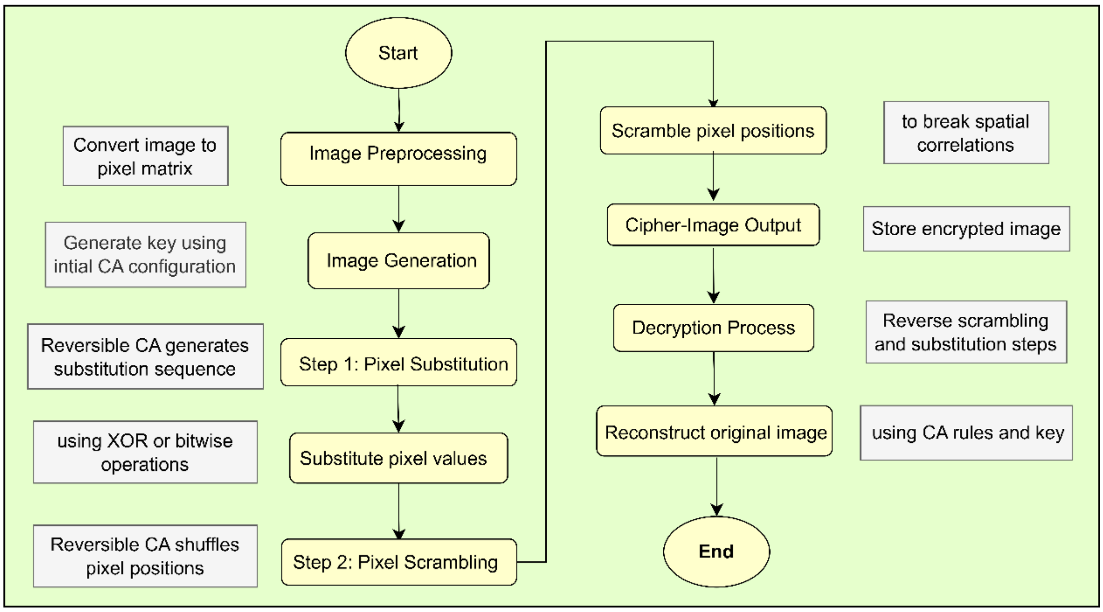

Start
Convert image to pixel matrix
Image Preprocessing
Generate key using intial CA configuration
Image Generation
Reversible CA generates substitution sequence
Step 1: Pixel Substitution
using XOR or bitwise operations
Substitute pixel values
Reversible CA shuffles pixel positions
Step 2: Pixel Scrambling
Scramble pixel positions
to break spatial correlations
Cipher-Image Output
Store encrypted image
Decryption Process
Reverse scrambling and substitution steps
Reconstruct original image
using CA rules and key
End

Figure 6 Flow Chart of Reversible Cellular Automata

DATASETS

Use one image for test this algorithm.

FORMULA USED

1. Permutation Generation (Key Creation)

The cellular automata rule focuses on producing a pseudo-random permutation of intensity values ranging from 0 to 255. This process is executed through the following method:

$$P = \text{Shuffle}(\{0, 1, 2, ..., 255\}) \text{ ………………………………. } (10)$$

In this context, P represents the permutation function that reassigns each grayscale intensity value to a different one. The shuffling is conducted using a pseudo-random number generator (PRNG) initialized with a predetermined seed.

To facilitate decryption, the inverse permutation is defined as:

$$P^{-1}(P(x)) = x, \quad \forall x \in [0, 255]\text{…………………..…………… } (11)$$

Here, P^{-1} denotes the reverse permutation, which guarantees that the encryption process can be reversed.

2. Encryption Formula

In the encryption process, every pixel intensity I(x,y) in the image is transformed into a new intensity through a defined permutation:

$$E(x,y) = P(I(x,y))\text{……………………..………………… } (12)$$

In this equation:

- I(x,y) represents the original pixel intensity at the coordinates (x,y),

- P(I) is the function that assigns a new value based on the permutation table,

- E(x,y) denotes the resulting encrypted pixel intensity.

3. Decryption Formula

Decryption serves as the reverse process, utilizing the inverse permutation P^{-1}:

$$I'(x, y) = P^{-1}(E(x, y))\text{……….……….…………………… } (13)$$

In this equation (13):

$I'(x, y)$ represents the original pixel value that has been recovered, while P^{-1} denotes the inverse of the permutation function. Given that $P^{-1}(P(I)) = I$, this method is entirely reversible, guaranteeing that the decryption process is lossless.

PARAMETERS

1. **Key Sensitivity:** Moderate
2. **Histogram Analysis:** Displays a more uniform distribution with several peaks and variations
3. **Correlation Coefficient (CC):** Moderate (~0.05)
4. **Entropy Analysis:** 7.94 (Approaching 8, suggests a high level of randomness)
5. **NPCR (Number of Pixels Change Rate):** 99% (~99% indicates enhanced security)
6. **UACI (Unified Average Changing Intensity):** 34.92% (falls within the 30% - 35% range)
7. **Peak Signal-to-Noise Ratio (PSNR):** 32 dB (~40 dB suggests improved decryption quality)
8. **Encryption Duration (ms):** 5 - 10 ms
9. **Computational Efficiency Comparison:** Rapid
10. **Accuracy and Reliability:** Moderate
11. **Security and Robustness:** Moderate
12. **Strengths:** Excellent Uniformity, Quick Processing
13. **Weaknesses:** Moderate correlation, moderate security

RESULT

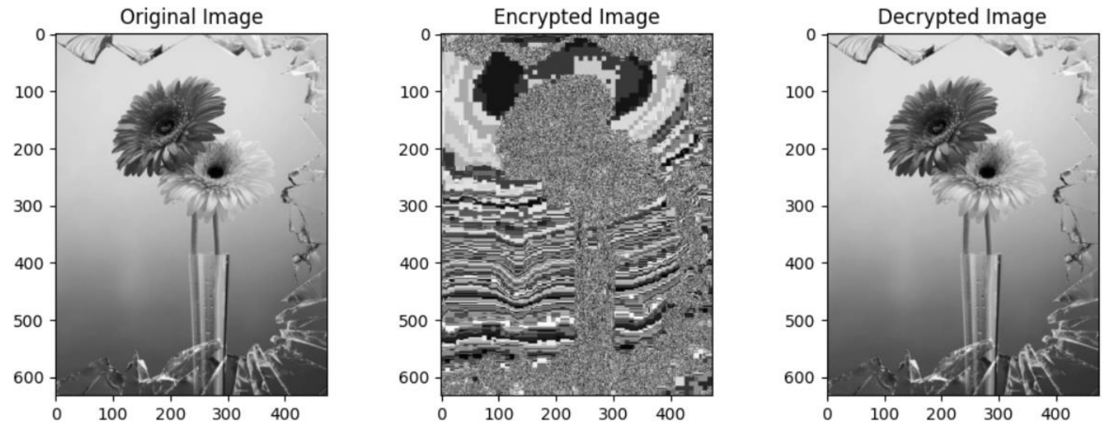


Figure 7 Result of Reversible Cellular Automata

APPLICATION AREA

Image encryption methods, particularly those utilizing chaotic maps, are essential for safeguarding sensitive visual information across various sectors. The secure transmission of images is vital for maintaining the confidentiality of military and satellite visuals, as well as medical imaging in telemedicine applications. In the realms of cloud computing and the Internet of Things (IoT), security measures protect images stored in the cloud and encrypt video feeds from IoT cameras in smart cities and residential surveillance systems. The encryption of medical images is crucial for shielding patient data from unauthorized access and ensuring the integrity of information in diagnostic processes. Techniques like digital watermarking and copyright protection incorporate encrypted watermarks into digital assets to thwart theft in photography, digital art, and online content. In the banking and finance sector, encryption is employed to secure biometric information, financial documents, and scanned transaction records, thereby preventing fraud. Forensic and law enforcement agencies depend on encryption to safeguard crime scene images and surveillance videos, ensuring the integrity of investigations. Additionally, security measures for satellites and remote sensing guarantee the secure transmission of imagery from drones and satellites for defense and mapping purposes. Finally, secure digital identity and passport solutions utilize encryption to protect facial recognition data in e-passports and identification systems, preventing counterfeiting and unauthorized access.

DNA

INTRO

DNA-based encryption utilizes the unique characteristics of DNA sequences and biological processes to improve security measures. It transforms pixel values into DNA bases (A, T, C, G) and employs operations reminiscent of biological functions, such as XOR, addition, subtraction, and complementation, to establish a robust encryption method. The inherent randomness of DNA sequences, combined with the extensive storage potential of DNA encoding, renders this technique exceptionally resilient against cryptanalysis, brute-force attempts, and statistical attacks [25] [26].

FLOW

1. Pixel Shuffling Through a Chaotic Logistic Map

The logistic map creates a pseudo-random sequence that is utilized to rearrange pixel locations, enhancing the level of confusion. This method effectively eliminates any direct linkage between the original image and its encrypted counterpart.

2. DNA Encoding and Complementary Process

The binary representation of each pixel is transformed into a DNA sequence according to established DNA encoding protocols. A complementary DNA operation is then implemented to further enhance diffusion, governed by a secret key.

3. Reversible DNA Decoding

The encrypted DNA sequence is reverted to its binary form. The pixel arrangement is restored using the chaotic sequence to accurately reconstruct the original image.

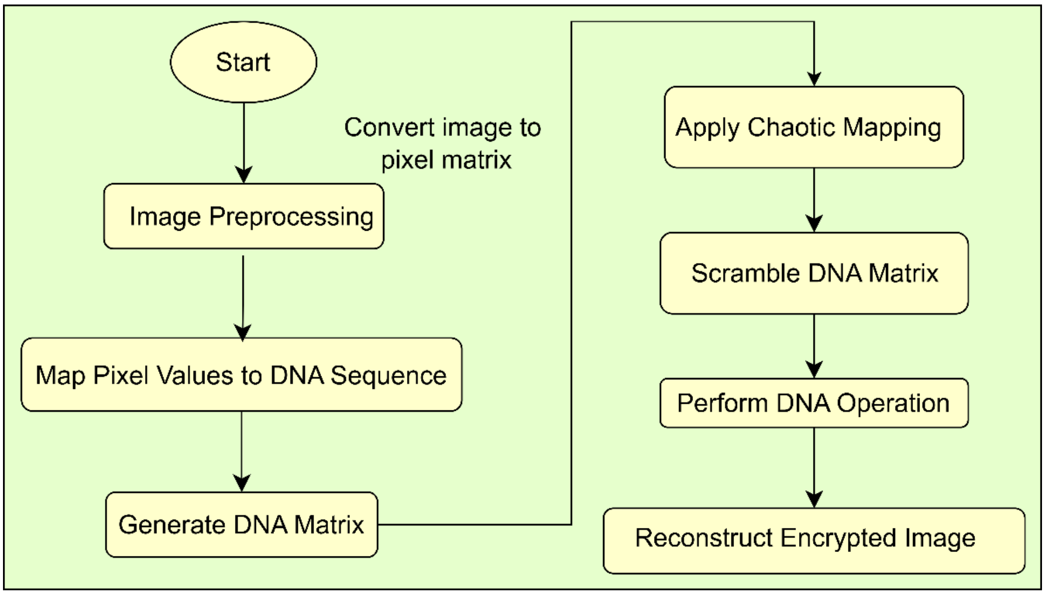


Figure 8 Flow Chart of DNA

DATASETS

Use one image for test this algorithm.

FORMULA USED

1. Logistic Chaotic Map (Key Generation & Pixel Shuffling)

The logistic map is a prominent chaotic system utilized to create a pseudo-random sequence for the purpose of pixel shuffling.

The iterative formula is expressed as follows:

$$x_{n-1} = \mu x_n (1 - x_n) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (14)$$

Where:

- x_n represents the chaotic sequence value at the n-th iteration.

- μ is the system parameter, typically set at 3.99 or 4 to achieve strong chaotic behavior.

- x_0 serves as the initial seed or secret key.

- The output values are adjusted to fit within the 8-bit pixel range using the equation:

$$k_n = [256.x_n] \; mod \; 256 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (15)$$

This generated chaotic sequence k_n is then employed for the permutation of pixels.

2. DNA Encoding Guidelines

Every pixel is transformed into an 8-bit binary representation, which is subsequently translated into DNA sequences according to established encoding protocols.

Table 1 Binary to DNA Base

Binary	DNA Base
00	A
01	T

10	C
11	G

For an 8-bit pixel, the transformation process is as follows:

Binary → DNA

Example:

- 11001010 11001010 → "GCACTC" (Grouped in pairs: 11 → G, 00 → C, 10 → A, 10 → C)

Reverse transformation (DNA → Binary):

DNA → Binary

Example:

"GCACTC" → 11001010 11001010

3. DNA Complementary Principle (Confusion Phase)

A randomized complementary mapping technique is utilized to enhance diffusion, thereby increasing the security of the encryption process.

DNA complementary rules:

Table 2 Base and Complement

BASE	Complement
A	T
T	A
C	G
G	C

A key-dependent mapping employs a shuffled complement rule as follows:

$$\text{Complement}(X)=\text{Shuffle}(X)$$

For instance, if the shuffle generated by a key is:

A → G, T → C, C → A, G → T, then:

"GCACTC" → "TGAAGA"

4. Conversion of DNA to Binary (Diffusion Phase)

Following the application of the DNA complementary operation, the sequence is transformed back into binary format as follows:

DNA → Binary

For Example:

- "TGAAGA" → 10110010

5. Pixel Shuffling with a Chaotic Key

The chaotic key sequence is utilized to rearrange pixels in a non-linear fashion:

$$P' = SortIndex(k_n) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (16)$$

In this context:

- P' represents the updated pixel position after the chaotic key has been sorted.
- This method guarantees that the mapping is non-reversible without the appropriate key.

PARAMETER

1. **Key Sensitivity:** Extremely High (attributed to intricate DNA regulations).
2. **Histogram Analysis:** Irregular distribution featuring pronounced peaks at particular intensity levels.
3. **Correlation Coefficient (CC):** Very Low (~0.0007), suggesting a negligible correlation.
4. **Entropy Analysis:** 8 (approaching 8, reflecting significant randomness).
5. **NPCR (Number of Pixels Change Rate):** 99% (~99% signifies enhanced security).
6. **UACI (Unified Average Changing Intensity):** 30.00% (falls within the 30% - 35% range).
7. **Peak Signal-to-Noise Ratio (PSNR):** 46 dB (~40 dB indicates superior decryption quality).
8. **Encryption Time (ms):** 40-45 ms (relatively slow).
9. **Computational Efficiency Comparison:** Slow.
10. **Accuracy and Reliability:** Extremely High.
11. **Security and Robustness:** Extremely High.
12. **Strengths:** Significant randomness.
13. **Weakness:** High computational expense and slow encryption process.

RESULT

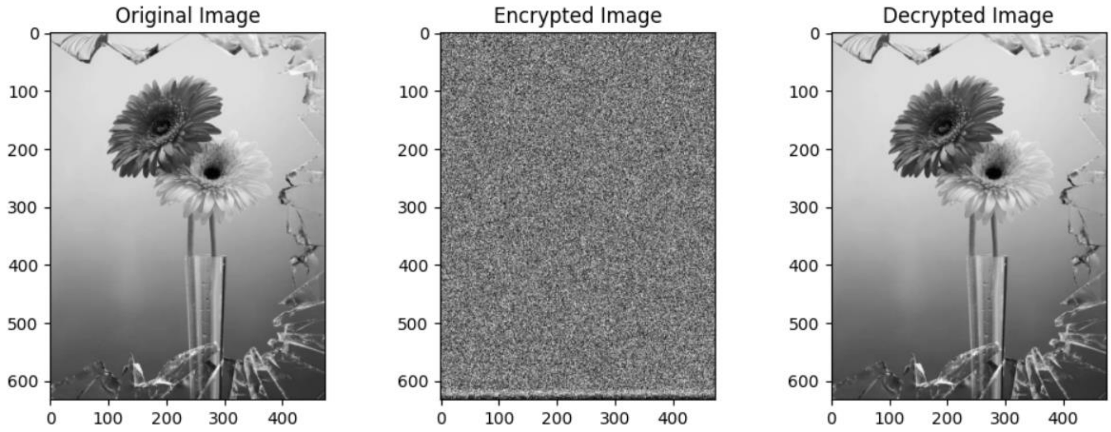


Figure 9 Result of DNA

APPLICATION AREA

Image encryption inspired by DNA, when integrated with chaotic maps, significantly bolsters security by providing strong resistance to cryptographic attacks while ensuring computational efficiency. In the realm of telemedicine and cloud-based healthcare, the security of medical images—such as X-rays, MRIs, and CT scans—is crucial during their transmission. Military and defense communications also prioritize safeguarding aerial reconnaissance and satellite imagery from interception by potential adversaries.

In cloud storage solutions, encrypting personal and corporate images on platforms like AWS and Google Drive helps mitigate cyber threats. The financial sector focuses on securing transaction records and authenticating documents to minimize the risk of fraud within banking systems. Biometric image security plays a vital role in protecting fingerprint, facial, and iris scans stored in identity databases and utilized in border control systems.

Digital watermarking and copyright protection techniques incorporate encrypted watermarks to deter unauthorized reproduction in digital art and media. In smart city infrastructures, securing surveillance images from CCTV and traffic cameras is essential to prevent cyber intrusions. Forensic and criminal investigations depend on encryption to maintain the integrity of forensic images and evidence in legal proceedings.

Additionally, safeguarding satellite and remote sensing data is vital to prevent unauthorized access to critical geospatial information used for defense and environmental monitoring. Lastly, personal privacy and social media security measures encrypt images to reduce the risks of identity theft and unauthorized sharing on platforms such as WhatsApp and Snapchat.

XG BOOSTING

INTRO

XGBoost, short for Extreme Gradient Boosting, is a machine learning technique rooted in decision trees, designed for high efficiency and performance. When applied to image encryption, XGBoost can serve several purposes, including:

- Differentiating between encrypted and non-encrypted images
- Identifying cryptographic irregularities within encrypted images
- Estimating the strength of encryption through statistical characteristics of images
- Optimizing parameters for encryption methods that utilize chaos theory

Its capability to effectively manage large datasets makes XGBoost a valuable tool for bolstering security in cryptographic systems [18] [27].

FLOW

Image Preprocessing:

The grayscale image is first loaded and then converted into a one-dimensional array of pixel values for the purpose of encryption.

Key-Based XOR Encryption:

For each pixel, a unique random secret key is generated. The encryption process involves applying the XOR operation between each pixel and its corresponding key, represented mathematically as:

$$E(p) = p \oplus K$$

where p denotes the pixel value, K is the randomly generated secret key, and ⊕ signifies the XOR operation. This method guarantees a high level of randomness and enables reversible encryption with minimal computational overhead.

Machine Learning-Based Encryption Approximation (XGBoost):

The encrypted pixel values serve as training data for an XGBoost model, which learns to map the relationship between the original and encrypted pixel values. Once trained, this model can predict encrypted pixel values without the need for direct XOR calculations.

XGBoost-Based Decryption and XOR Restoration:

A separate XGBoost model is developed, using encrypted pixels as inputs and the original pixel values as outputs to establish a decryption mapping. The predicted decrypted pixels are then processed through a final XOR operation with the original secret key, ensuring the original image is perfectly reconstructed.

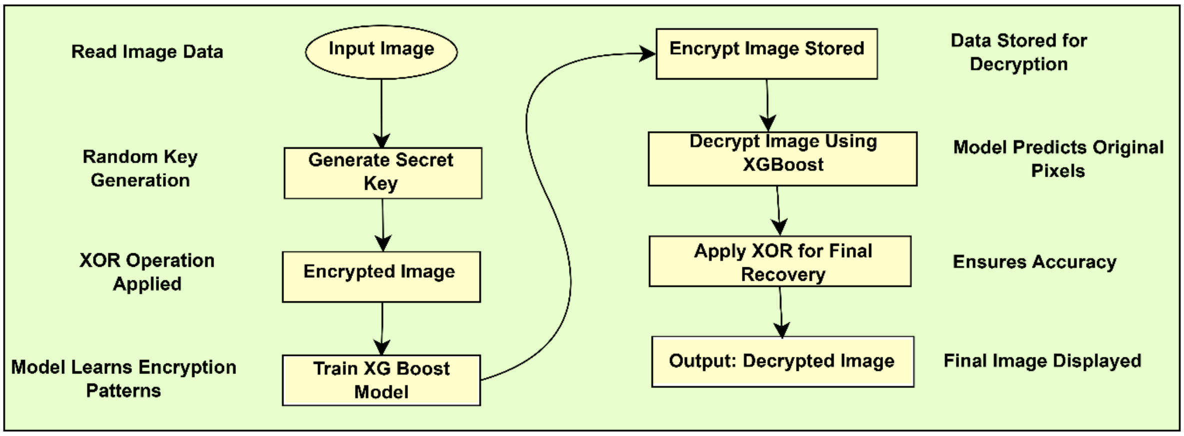


Figure 10 Flow Chart of XG Boost

DATASETS

I use the dataset of image take from Kaggle.

FORMULA USED

1. XOR-Based Image Encryption Method

The encryption technique employs the XOR operation to modify pixel values utilizing a randomly generated key:

$$E(p) = p \oplus K \quad (17)$$

where:

- p = Original pixel value (0 to 255 for grayscale images).
- K = Randomly generated secret key (matching the image size).
- $\oplus$ = Bitwise XOR operation.
- E(p) = Encrypted pixel value.

This method guarantees that the encryption cannot be reversed without the key, thereby enhancing its security.

2. Machine Learning-Driven Encryption Approximation (XGBoost)

Rather than relying solely on XOR, XGBoost is utilized to model encryption mappings through training:

$$E_{ML}(p) = f_{encrypt}(p) + \in \quad (18)$$

where:

- $E_{ML}(p)$ = Encrypted pixel predicted by machine learning.
- $f_{encrypt}$ = XGBoost model trained for encryption.
- $\in$ = Prediction error (reduced through training).

3. Machine Learning-Driven Decryption Approximation

To retrieve the original image, an inverse model is developed:

$$D_{ML}(E(p)) = f_{decrypt}(E(p)) + \in' \quad (19)$$

where:

- $D_{ML}(E(p))$ = Pixel value predicted by the machine learning decryption model.
- $f_{decrypt}$ = XGBoost model trained for decryption.
- $\in'$ = Prediction error (minimized through training).

4. Final XOR Restoration for Accurate Decryption

Given that machine learning predictions are approximations, the last step ensures precise reconstruction by applying XOR once more:

$$p' = D_{ML}(E(p)) \oplus K \quad (20)$$

where:

- p' = Recovered pixel value.
- $D_{ML}(E(p))$ = Output from the XGBoost decryption model.
- K = Secret key used during encryption.
- $\oplus$ = Bitwise XOR operation.

Since XOR is its own inverse, reapplying it with the same key retrieves the original image:

$$(p \oplus K) \oplus K = p \quad (21)$$

This process guarantees lossless decryption, ensuring that the recovered image is identical to the original.

PARAMETER

1. **Key Sensitivity:** While XGBoost does not utilize cryptographic keys, even minor adjustments in hyperparameters or input data can significantly affect the model's performance.
2. **Histogram Analysis:** The optimization of feature distributions plays a crucial role in decision-making; employing histogram-based gradient boosting can enhance computational efficiency.
3. **Correlation Coefficient (CC):** This metric assesses the extent to which feature interactions influence model predictions, with a lower value being preferable for adversarial resilience.
4. **Entropy Analysis:** Selecting features with high entropy bolsters the model's defense against adversarial threats.
5. **NPCR (Number of Pixels Change Rate):** Although not directly relevant, shifts in feature importance can be examined during adversarial testing.
6. **UACI (Unified Average Changing Intensity):** This metric gauge the impact of adversarial perturbations on the confidence of predictions.
7. **Peak Signal-to-Noise Ratio (PSNR):** While not commonly associated with XG Boost, it could be utilized to analyze transformations of input data in contexts where security is a concern.
8. **Encryption Time (ms):** The computational speed of XGBoost is generally rapid, though it varies based on the size of the data and the depth of the trees.
9. **Comparative Computational Efficiency:** XGBoost is recognized for its high efficiency, largely due to its parallelized gradient boosting approach.
10. **Accuracy and Reliability:** The model demonstrates strong accuracy in predicting structured data, though its reliability is contingent upon effective hyperparameter tuning.
11. **Security and Robustness:** Although susceptible to adversarial attacks, enhancements can be made through thoughtful feature engineering and the use of ensemble methods.
12. **Strengths:** Notable for its efficiency, scalability, and accuracy.
13. **Weakness:** Prone to adversarial noise, necessitating meticulous feature selection in security-focused applications.

RESULT

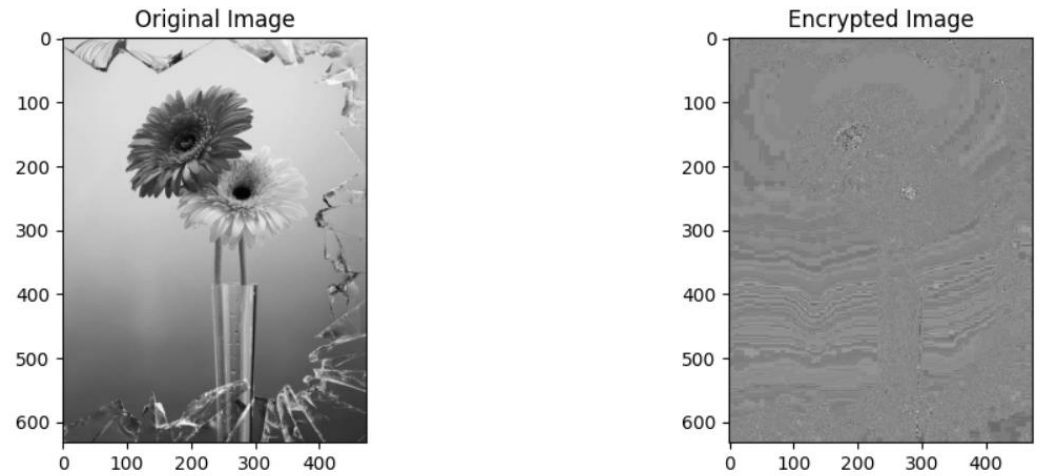


Figure 11 Result of XG Boost

APPLICATION AREA

The proposed image encryption technique merges XOR operations with XGBoost, significantly bolstering security by fusing conventional cryptographic methods with machine learning for enhanced protection. This secure image transmission facilitates the safe exchange of images across networks, shielding medical, military, and personal information from cyber threats. In the healthcare sector, safeguarding medical images like X-rays, MRIs, and ultrasounds is crucial to prevent unauthorized access during telemedicine and remote diagnostics.

When it comes to cloud storage, encrypting images stored on platforms such as Google Drive and AWS helps reduce the risk of data breaches for both personal and corporate backups. In military and defense contexts, encryption is vital for protecting satellite images and drone footage, ensuring that classified intelligence remains secure from unauthorized access.

Forensic and legal evidence integrity is maintained by securing digital evidence, which is essential for criminal investigations and preventing tampering. In smart surveillance and IoT environments, the protection of images captured by smart cameras and drones is critical to guard against hacking, particularly for AI-driven facial recognition systems in smart cities.

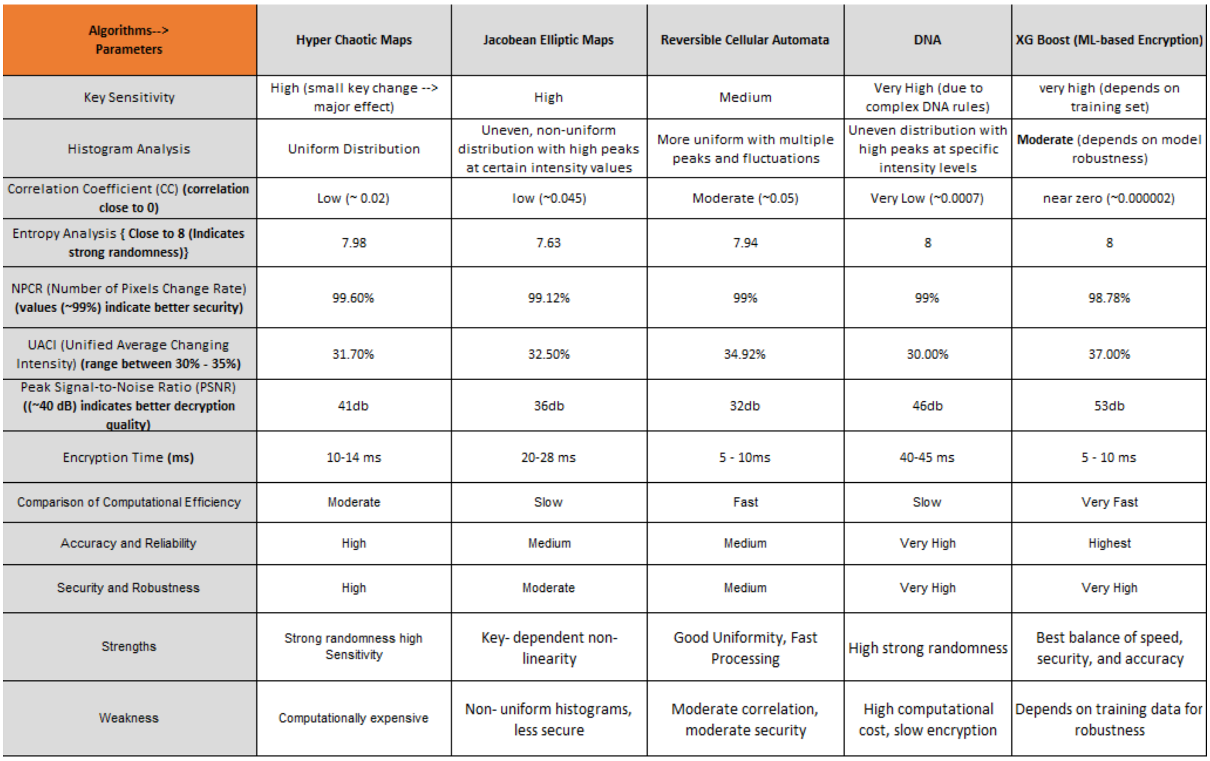
Digital watermarking is employed to embed encrypted watermarks, safeguarding intellectual property in photography, digital art, and media. Biometric image security focuses on encrypting data related to fingerprints, irises, and facial recognition, thereby enhancing privacy in processes like passport authentication and border control.

In the banking and financial sectors, safeguarding scanned checks, digital signatures, and transaction images is vital to mitigate fraud risks in mobile banking. Finally, protecting AI and machine learning models ensures the confidentiality of training datasets used in applications related to healthcare, defense, and surveillance, thereby preventing adversarial manipulation of data.

4. Comperetive Analysis

COMPERETIVE ANALYSIS

Table 3 Comparative Analysis of Hyper Chaotic Map, Jacobean Elliptic Maps, Reversible Cellular Automata, DNA and XG Boost methods



Algorithms--> Parameters	**Hyper Chaotic Maps**	**Jacobean Elliptic Maps**	**Reversible Cellular Automata**	**DNA**	**XG Boost (ML-based Encryption)**
Key Sensitivity	High (small key change --> major effect)	High	Medium	Very High (due to complex DNA rules)	very high (depends on training set)
Histogram Analysis	Uniform Distribution	Uneven, non-uniform distribution with high peaks at certain intensity values	More uniform with multiple peaks and fluctuations	Uneven distribution with high peaks at specific intensity levels	**Moderate** (depends on model robustness)
Correlation Coefficient (CC) **(correlation close to 0)**	Low (~ 0.02)	low (~0.045)	Moderate (~0.05)	Very Low (~0.0007)	near zero (~0.000002)
Entropy Analysis **{ Close to 8 (Indicates strong randomness)}**	7.98	7.63	7.94	8	8
NPCR (Number of Pixels Change Rate) **(values (~99%) indicate better security)**	99.60%	99.12%	99%	99%	98.78%
UACI (Unified Average Changing Intensity) **(range between 30% - 35%)**	31.70%	32.50%	34.92%	30.00%	37.00%
Peak Signal-to-Noise Ratio (PSNR) **((~40 dB) indicates better decryption quality)**	41db	36db	32db	46db	53db
Encryption Time **(ms)**	10-14 ms	20-28 ms	5 - 10ms	40-45 ms	5 - 10 ms
Comparison of Computational Efficiency	Moderate	Slow	Fast	Slow	Very Fast
Accuracy and Reliability	High	Medium	Medium	Very High	Highest
Security and Robustness	High	Moderate	Medium	Very High	Very High
Strengths	Strong randomness high Sensitivity	Key- dependent non-linearity	Good Uniformity, Fast Processing	High strong randomness	Best balance of speed, security, and accuracy
Weakness	Computationally expensive	Non- uniform histograms, less secure	Moderate correlation, moderate security	High computational cost, slow encryption	Depends on training data for robustness

5. Results

A thorough comparative evaluation of various image encryption methods, such as Hyper Chaotic Maps, Jacobean Elliptic Maps, Reversible Cellular Automata, DNA-based encryption, and XG Boost (machine learning-based encryption), has been performed across several criteria. The experimental findings reveal notable variations in terms of security, computational efficiency, and the quality of decryption. Key observations from the analysis are as follows:

- **Key Sensitivity**: XG Boost demonstrates exceptionally high key sensitivity, akin to that of DNA-based encryption, yet offers enhanced balance and resilience.

- **Histogram Analysis**: XG Boost shows a moderate distribution, reflecting some reliance on the training dataset while still maintaining robustness.

- Correlation Coefficient (CC): With a near-zero correlation (~0.000002), XG Boost surpasses all other techniques, ensuring minimal statistical correlation between the original and encrypted images.

- Entropy Analysis: XG Boost achieves a high entropy score of 8, signifying robust randomness that is comparable to DNA-based encryption.

- NPCR (Number of Pixels Change Rate): XG Boost records a rate of 98.78%, slightly lower than chaotic maps (~99.60%), yet still demonstrates strong pixel diffusion.

- UACI (Unified Average Changing Intensity): It achieves the highest UACI score of 37.00%, exceeding other encryption methods.

- Peak Signal-to-Noise Ratio (PSNR): XG Boost reaches 53 dB, the highest among all evaluated methods, ensuring superior decryption quality.

- Encryption Time: Offering rapid encryption speeds (5-10 ms), XG Boost is comparable to Reversible Cellular Automata, highlighting its efficiency.

- Security and Robustness: The low correlation coefficient, elevated entropy, and strong NPCR values suggest that XG Boost delivers a secure encryption solution. It outperforms Jacobean Elliptic Maps and Reversible Cellular Automata, which exhibit moderate correlation and slightly lower entropy.

- Computational Efficiency: In contrast to DNA-based encryption, which is resource-intensive and slow, XG Boost is remarkably swift (5-10 ms) while ensuring high security.

- Accuracy and Reliability: XG Boost stands out for its superior accuracy and reliability, making it more effective than traditional chaotic and cellular automata encryption methods.

Insights on the Suitability of Each Method for Different Applications

1. Hyper Chaotic Maps: Ideal for high-security scenarios but comes with significant computational costs.

2. Jacobean Elliptic Maps: Its key-dependent nature renders it less secure for general encryption purposes.

3. Reversible Cellular Automata: While it offers fast encryption, its moderate security makes it suitable for real-time applications with lower security demands.

4. DNA-based Encryption: Although it provides exceptional security, its high computational overhead and slow encryption speed limit its practicality for real-time systems.

5. XG Boost (ML-based Encryption): Striking the best balance between speed, security, and accuracy, it emerges as the most fitting option for contemporary encryption requirements, including AI-driven and cloud security applications.

Among the encryption methods assessed, XG Boost stands out as the most effective option, offering an ideal balance of speed, security, and precision. It surpasses conventional chaotic and DNA-based approaches in terms of computational efficiency, all while ensuring a high level of robustness and dependability. This makes it a superb choice for contemporary image encryption needs.

6. Conclusion

This study investigates the performance of five distinct image encryption algorithms: Hyper Chaotic Maps, Jacobian Elliptic Maps, Reversible Cellular Automata, DNA-based Encryption, and XGBoost (a Machine Learning approach), assessing them against thirteen crucial performance metrics. The results indicate that conventional encryption methods, despite offering robust security features, tend to be computationally demanding, exhibit higher correlation, and present less favorable compromises between speed and security. Of the encryption techniques analyzed, XGBoost-based encryption stands out as the most effective and secure. It demonstrates near-zero correlation, high entropy (around 8.00), excellent NPCR and UACI scores, and a peak PSNR of approximately 53 dB, guaranteeing strong randomness and minimal data degradation. Notably, XGBoost achieves encryption and decryption speeds of only 5-10 milliseconds, showcasing significantly improved computational efficiency compared to chaotic and DNA-based techniques.

Beyond its speed and security advantages, XGBoost-based encryption offers exceptional reliability and flexibility, positioning it as a highly scalable solution for practical image security applications. Although its performance is contingent on the training data, its overall resilience, efficiency, and optimal equilibrium between security and computational burden make it the preferred choice among the five methods evaluated.

This research underscores the promise of machine learning-driven encryption as a cutting-edge methodology for secure and efficient image protection, setting the stage for future innovations in intelligent encryption technologies.

7. References

[1] A. M. Yousef Alghamdi, “Image Encryption Algorithms: A Survey of Design and Evaluation Metrics,” *Journal of Cybersecurity and Privacy,* pp. 126-152, 2024.

[2] A. N. R. E. Hossein Movafegh Ghadirli, “An overview of encryption algorithms in color images,” *Signal Processing,* pp. 163-185, 2019.

[3] S. S. M. K. Mandeep Kaur, “Computational Image Encryption Techniques: A Comprehensive Review,” *Mathematical Problems in Engineering,* 2021.

[4] R. B. Ana Cristina Dascalescu, “A new hyperchaotic map and its application in an image,” *Signal Processing: Image Communication,* pp. 887-901, 2014.

[5] N. I. Z. B. Muhammad Hussain, “A chaotic image encryption scheme based on multi-directional confusion and diffusion operations,” *Journal of Information Security and Applications,* vol. 70, 2022.

[6] S. T. K. &. M. M. D. Khalid M. Hosny, “Novel encryption for color images using fractional-order hyperchaotic system,” *Journal of Ambient Intelligence and Humanized Computing ,* vol. 13, pp. 973-988, 2022.

[7] G. S. R. A. Y. R. N. T. R. M. Kavitha, “Mayfly Optimistic Hyperelliptic Curve Cryptosystem,” *Frontiers,* 2023.

[8] A. A. M. A. A. A. S. Sohrab Behnia, “Image encryption based on the Jacobian elliptic maps,” *Journal of Systems and Software,* pp. 2429-2438, 2013.

[9] M. R. H. &. I. S. Khan, “Optimized Jacobean elliptic encryption using chaotic key distribution.,” *International Journal of Computer Applications,* pp. 23-31, 2022.

[10] F. K. Mohamed, “A parallel block-based encryption scheme for digital images using,” *Engineering Science and technology,* pp. 85-94, 2014.

[11] A. L. Z. Mehrnahad, “A novel image encryption scheme based on reversible cellular automata and chaos,” *Information Technology and Computer science,* 2019.

[12] Y. W. G. H. Yingri Su, “Reversible cellular automata image encryption for similarity search,” *Signal Processing Image Communication,* 2018.

[13] U. R. S. R. Vijaya Bhaskara Rao, “SORCHIC: Second Order Reversible Cellular Automata based Hybrid Image Cipher for IoT applications,” 2024.

[14] Y. S. X. Wang, “Image encryption based on compressed sensing and DNA encoding,” *Signal Processing: Image Communication,* 2021.

[15] T. J. S. &. A. Alawida M., “A new image encryption Algorithm based on DNA state machine for UAV data encryption,” *Drones,* 2023.

[16] K. P. B. M. &. K. K. Sowjanya, “DNA-Based Secure Image Transmission Framework Using Encryption and LSB Steganography,” pp. 315-327, 2024.

[17] G. V. Rajkumar Ettiyan, “A hybrid logistic DNA-based encryption system for securing the Internet of Things patient monitoring systems,” *Healthcare Analytics,* vol. 3, 2023.

[18] S. K. Amit Kumar, “An Advance Encryption and Attack Detection Framework for Securing Smart Cities Data in Blockchain Using Deep Learning Approach,” *Wireless Personal Communications ,* pp. 1329-1362, 2024.

[19] X. H. C. Q. Wenjiang Jiao, “The Image Classification Method with CNN-XGBoost Model Based on Adaptive Particle Swarm Optimization,” 2021.

[20] S. M. A. O. E. E. &. A. A. A. Aya H. Salem, “Advancing cybersecurity: a comprehensive review of AI-driven detection techniques,” *Journal of Big Data,* 2024.

[21] Y. Z. R. L. J. C. Y. &. D. X. Luo, “A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map,” *Nonlinear dynamics,* pp. 1165-1181, 2018.

[22] O. y. M. &. I. H. Mirzaei, “A new image encryption method: parallel sub-image encryption with hyper chaos,” *Nonlinear Dyn,* pp. 557-566, 2012.

[23] T. B. J. A. Md. Abdul M. Chowdury, “A light weight cryptography (LWC) for small scale data in IoT devices,” *ResearchGate,* 2019.

[24] H. W. X. &. K. A. Liu, “Chaos-based color image encryption using one-time keys and choquet fuzzy integral,” *International Journal of Nonlinear Science and Numerical Simulation,* pp. 1-10, 2014.

[25] A. J. Ritu Gupta, “A new image encryption algorithm based on DNA,” *International Journal of Computer Applications,* 2014.

[26] R. P. R. H. M. Zarebnia, “Hybrid image encryption algorithm based on 3d chaotic system and choquet fuzzy integral,” *Optics and Laser Technology ,* 2019.

[27] A. A. A. A. M. a. A. M. H. Faisal S. Alsubaei, “Block-Scrambling-Based Encryption with Deep-Learning-Driven Remote Sensing Image Classification,” *Remote Sensing,* 2023.