A Chaotic Scrambling and Diffusion-Based Encryption Framework for Real-Time News Video Transmission

Na Liu
College of Communication, Xijing University, Xi’an 710123, China
E-mail: naliu0427@sina.com

Keywords: chaotic map, image encryption, crowd simulation algorithm, chaotic diffusion mechanism, news dissemination safety

Received: May 30, 2025

In the information age, news videos face growing security risks during transmission. To address this, a novel image encryption algorithm combining chaotic maps and crowd simulation is proposed. The framework integrates a dual mechanism of scrambling and diffusion to disrupt both spatial structure and pixel values. Specifically, a chaotic logistic map is employed to generate dynamic key sequences for pixel-level diffusion, while a crowd simulation algorithm produces pseudo-random sequences to control row and column scrambling. This hybrid structure enhances encryption strength and unpredictability. The experimental results show that the information entropy of the proposed model is 7.97, the pixel change rate is 99.62%, and the pixel correlation is reduced to 0.08. Decryption yields an SSIM of 0.95, while encryption and decryption take only 109 ms and 184 ms, respectively-over 50% faster than comparable models. The model exhibits high security, efficiency, and reversibility, making it well-suited for protecting sensitive news video transmissions.

Povzetek: Članek predstavi hibridni algoritem šifriranja slik za videe novic, ki združi kaotične preslikave za difuzijo s simulacijo množic za vrstično/stolpično mešanje, da okrepi varnost, nepredvidljivost in povratnost prenosa.

1 Introduction

In the era of pervasive digital communication, the transmission of multimedia content-particularly news video-has become a cornerstone of global information dissemination [1]. With the growing reliance on online platforms for news delivery, ensuring the confidentiality, integrity, and authenticity of multimedia data has become a pressing concern. Traditional cryptographic algorithms, although effective for textual or low-dimensional data, often fall short in securing high-volume, real-time video streams due to computational complexity, lack of perceptual sensitivity, or limited robustness against advanced attacks [2]. Therefore, lightweight yet secure encryption schemes are increasingly demanded, particularly in sensitive domains such as political or crisis-driven news coverage, where unauthorized access or manipulation could have severe social consequences. Chaotic systems, known for their deterministic yet unpredictable behavior, offer a compelling alternative for image and video encryption. Characterized by sensitivity to initial conditions, high entropy, and pseudo-randomness, Chaotic Maps (CMs) can efficiently generate complex key sequences suitable for scrambling and diffusion operations. These properties make them inherently resistant to brute-force attacks and statistical analyses. Despite their promise, most existing chaotic encryption schemes remain focused on static images and fail to address the dynamic, frame-based nature of real-world video streams. Furthermore, they often rely on low-dimensional maps or fixed transformation structures, which limits their scalability and resistance to structured attacks. To address these limitations, this study proposes a dual-layer chaotic encryption framework aimed at enhancing security and adaptability in news-oriented video content transmission. Although the experimental validation is conducted on individual video frames, the method is designed to be extensible to real-time video encryption pipelines. The approach integrates crowd simulation-inspired pseudo-random sequence generation with chaotic diffusion and permutation mechanisms, thereby enhancing the unpredictability and robustness of the encryption process. The proposed system is benchmarked against key performance metrics such as information entropy, NPCR, UACI, and processing latency. This paper aims to contribute to the field by bridging the gap between chaotic theory and practical video encryption application, particularly within the context of news broadcasting security. The remainder of this work is organized as follows: Section 2 describes the proposed methodology in detail, Section 3 presents the experimental validation and performance evaluation, and Section 4 discusses the security analysis and potential extensions. Finally, conclusions are drawn in Section 5, along with directions for future work.

2 Related works

In recent years, with the increasingly severe issue of information security, image and video encryption technology has gradually become a research focus in the field of multimedia security. Yao et al. proposed a color image compression and encryption algorithm that combines compressive sensing, Sudoku matrix, and hyper chaotic system to ensure the security of color image data and improve transmission and storage efficiency. This algorithm designed a new hyper chaotic system, improved the beetle optimization algorithm to optimize the compression threshold, and introduced Sudoku matrix and bidirectional diffusion operation. The research results indicated that the algorithm had high security [3]. Singh et al. developed a new multi-layer Image Encryption (IE) scheme and improved grayscale and color image authentication techniques to overcome the security crisis of private data in network communication. The scheme combines a public key cryptosystem and two chaotic systems. The research results indicated that the algorithm had characteristics such as a huge key space and extremely low correlation coefficient, and was efficient in resisting statistical attacks. It could effectively resist different brute force attacks [4]. Wang et al. proposed a multi-IE method based on computer-generated phase only hologram algorithm and chaotic system for secure encryption of multiple images. This method applied an improved Gerchberg-Saxton algorithm to generate subsampled phase only holograms, and used spatial segmentation multiplexing to combine multiple phase holograms, which are then transformed into ciphertext through a chaotic system. The research results indicated that this method eliminated the problem of information leakage, increased the complexity of the encryption system, and verified its security and feasibility [5].

Liu et al. proposed a novel 3D medical image encoding scheme based on biometric keys and cube boxes to overcome the shortcomings of research on 3D medical IE. This scheme utilized biometric keys to enhance data security and constructed cube boxes to increase nonlinearity. The research results indicated that this encryption scheme had good statistical performance, large key space, high sensitivity, and robustness, and could resist various typical cryptographic attacks [6]. Huang et al. proposed a color image block encryption algorithm based on cellular neural networks and Chua's chaotic system to overcome the problems of small key space and susceptibility to plaintext attacks in low dimensional chaotic encryption. This algorithm generated chaotic sequences through Fourier transform, combined them with solid colors for diffusion, and used an improved Chua's chaotic system to scramble the image. The research results indicated that the algorithm had good encryption performance and could resist common attacks [7]. Zhang et al. developed a new simultaneous obfuscation diffusion IE algorithm to address the efficiency and security issues of existing IE algorithms in Deoxyribonucleic Acid (DNA) encoding and chaotic scrambling diffusion operations. This algorithm adopted a composite coupled chaotic system, combined with DNA encoding for synchronous perturbation diffusion encryption. The research findings indicated that the proposed method had higher security and better performance than representative methods [8].

Peng et al. designed an IE system based on a chaotic hardware encryption framework, utilizing a multi-scroll chaotic system and the Arnold transformation as the primary sources of entropy. The image was processed through a chaotic sequence, with the Arnold transformation applied for scrambling. Laboratory results demonstrated that the system exhibited low power consumption, high processing speed, and strong encryption performance [9]. Boussif et al. proposed a novel IE method to secure medical digital images used in communication systems. The method first converted the image into a pixel matrix, encrypted the image blocks individually, and updated the encryption key using the Arnold transformation. Experimental results showed that this approach successfully secured the images and achieved lower computational time compared to conventional encryption algorithms [10]. Wang et al. developed a Chaotic Image Encryption (CIE) algorithm based on a matrix semi-tensor product and a composite key. The method divided the image into four segments, applied the Arnold transformation to each segment, and subsequently combined them to produce the encrypted image. The study demonstrated that the algorithm offered higher security than traditional methods and was well-suited for encrypting color images [11]. Jain et al. tackled the challenge of securely transmitting digital images in remote healthcare systems, which often contain sensitive patient data. The researchers proposed a CIE technique combining the Arnold Cat map with a 2D Logistic Sine Coupling Map. Their results indicated that the scheme enhanced both the randomness and security of encrypted images, thereby ensuring adequate protection of patient information [12]. Zarebnia Mde et al. introduced a multi-layer IE method incorporating a chaotic system, where images were scrambled using the Arnold transformation. The findings showed that the method achieved robust encryption performance and could withstand various types of attacks, effectively safeguarding user image data [13].

Table 1: Related works

Research	Method	Research content	Key performance metrics	Reference
Yao et al. (2025)	Compressive sensing + hyperchaos	Color image compression and encryption using Sudoku matrix and bidirectional diffusion	High security, improved transmission efficiency; entropy ≈ 7.83, NPCR > 98.9%	[3]
Singh et al. (2025)	RSA + CMs	Grayscale and color IE using hybrid cryptosystem	Low pixel correlation, strong against brute force; SSIM ≈ 0.79	[4]
Wang et al. (2023)	Phase-only holograms + chaos	Multiple-IE via spatial multiplexing and chaotic phase encoding	Eliminates leakage; entropy ≈ 7.90, good multi-image diffusion security	[5]

Liu et al. (2024)	Biometric key + cube structure	3D medical IE with cubic boxes and biometric-derived keys	Strong robustness and key sensitivity; entropy ≈ 7.87, SSIM ≈ 0.80	[6]
Huang et al. (2024)	CNN + Chua's chaotic system	Color IE using Chua chaos and pixel block scrambling	Improved resistance to plaintext attack; NPCR ≈ 99.18, limited scalability	[7]
Zhang et al. (2024)	DNA encoding + composite chaos	Chaotic scrambling and DNA diffusion for secure encryption	Higher entropy (≈ 7.92), better pixel decorrelation than previous DNA methods	[8]
Peng et al. (2023)	Hardware-based chaotic IE framework + Arnold transformation	Used a multi-scroll chaotic system and Arnold map for scrambling; targeted low-power, high-speed IE	High processing speed, low power, strong encryption	[9]
Boussif et al. (2022)	Block-wise encryption with dynamic key update	Converted image to pixel matrix, encrypted blocks individually, updated keys with Arnold transformation	Lower computational time, secure transmission	[10]
Wang et al. (2023)	Matrix semi-tensor product + composite key	Segmented image into four parts, applied Arnold scrambling per segment, merged afterward	High security, suitable for color IE	[11]
Jain et al. (2022)	Arnold Cat map + 2D Logistic Sine Coupling Map	Developed a chaotic scheme for secure medical image transfer in remote healthcare	Improved randomness and security, protection of patient data	[12]
Zarebnia Mde et al. (2021)	Multi-layer chaotic IE	Applied layered scrambling using chaotic system and Arnold transformation	Robust encryption, resistant to various attacks	[13]

In summary, existing studies have made substantial progress in enhancing encryption strength and resisting statistical or differential attacks. However, most approaches rely on conventional chaotic systems with limited sequence complexity or pre-defined scrambling patterns. Few, if any, incorporate dynamic behavioral simulation mechanisms such as crowd simulation to generate adaptive control sequences. Moreover, the joint optimization of spatial scrambling and numerical diffusion remains insufficiently addressed. This study fills the gap by integrating an improved crowd simulation algorithm with logistic chaotic diffusion in a unified framework. This novel combination enhances both the unpredictability of the permutation order and the nonlinear diffusion effect, thereby significantly improving encryption entropy, pixel decorrelation, and processing efficiency, particularly suited for real-time news video encryption scenarios.

3 Methods and materials

3.1 Encryption algorithm for news communication video based on chaos mapping

To address the dual challenge of security and efficiency in real-time news video transmission, this study designs an encryption framework based on chaotic dynamics and enhanced randomization control. The selection of the logistic CM is motivated by its simplicity, strong sensitivity to initial conditions, and ease of hardware implementation, making it suitable for high-speed encryption tasks in video scenarios. Unlike complex hyperchaotic models, the logistic map offers a trade-off between computational efficiency and sufficient nonlinear behavior needed for effective diffusion operations. Moreover, to overcome the limitations of traditional pseudorandom number generators, the framework incorporates a crowd simulation mechanism. This mechanism simulates non-deterministic behavioral dynamics in group movement, introducing dynamic perturbation patterns for scrambling operations. By using individual "participants" with evolving positional logic, the system generates permutation vectors that are both data-dependent and highly irregular, thereby improving the unpredictability of the scrambling phase without relying on externally seeded randomness.

In modern society, the immediacy and breadth of news dissemination have proposed higher requirements for the security of video data. Especially in sensitive fields such as politics, military, and disaster reporting, the leakage, tampering, and even forgery of video content will seriously affect public awareness and social stability. Traditional video encryption methods struggle to balance encryption efficiency and security when faced with large amounts of data and real-time transmission requirements [14-15]. Therefore, a CM-based encryption algorithm for news dissemination videos has been proposed in the study. The CM principle is shown in Figure 1.

Figure 1 presents the bifurcation diagram of the logistic map, illustrating how its output behavior changes with respect to variations in the control parameter μ. The horizontal axis represents the parameter μ, while the vertical axis represents the resulting state values after convergence. As μ increases beyond approximately 3.57, the system transitions from periodic to fully chaotic behavior, exhibiting high sensitivity and unpredictability-ideal characteristics for cryptographic key stream generation. These dense distributions of output points at higher μ values indicate that the sequence lacks repeatable patterns, which is desirable for permutation operations in encryption. In this study, a value of $\mu = 3.99$ is chosen to ensure operation in the chaotic regime. The resulting sequence is then used as a dynamic controller for row and column shuffling of image pixels. This mechanism enhances spatial structure disruption in the plaintext image, providing a strong first layer of encryption before the diffusion phase [16-17]. Therefore, the study adopts chaotic system for row shuffling, and the structure framework of row shuffling is shown in Figure 2.

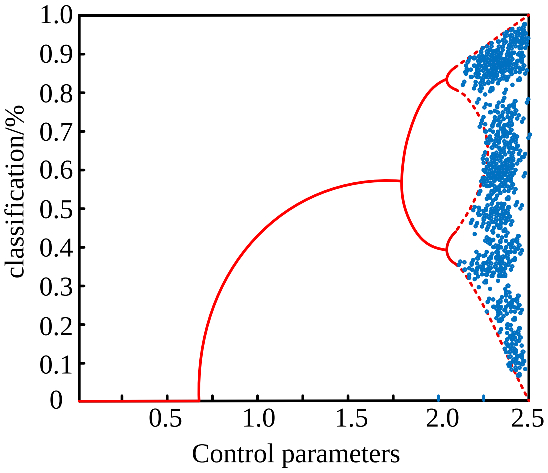


Figure 1: Bifurcation diagram of chaotic system.

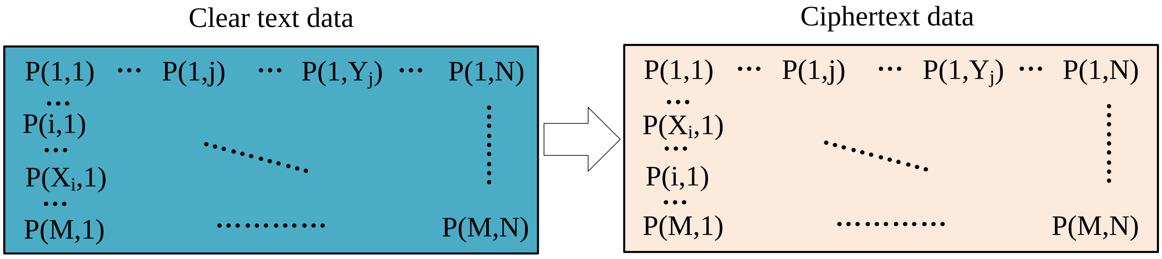

Clear text data
P(1,1) ··· P(1,j) ··· P(1,Yj) ··· P(1,N)
P(i,1)
P(Xi,1)
P(M,1)
P(M,N)
Ciphertext data
P(1,1) ··· P(1,j) ··· P(1,Yj) ··· P(1,N)
P(Xi,1)
P(i,1)
P(M,1)
P(M,N)

Figure 2: Chaotic row structure framework.

As shown in Figure 2, the row-level scrambling mechanism operates by swapping the positions of two specific rows within the image matrix. Each row, such as P(i,1), represents a horizontal line of pixel values. In this example, the i-th row and the X_I-th row exchange their positions, as controlled by the permutation sequence derived from the chaotic system. While Figure 2 depicts a single swap for illustration, the full encryption process involves iteratively applying such row-level exchanges across the entire image using a pseudo-random index vector. This approach disrupts the spatial continuity of the original structure, ensuring that even if an attacker observes the encrypted image, recovering the original ordering of rows becomes computationally infeasible without the correct key sequence [18-19]. This operation breaks the spatial continuity of the image, making it hard for attackers to restore the original information by analyzing the image structure even if they obtain encrypted images. The image data shown on the right after row shuffling appears to have an overall disordered structure, but in reality, it is the result of precise control based on a chaotic sequence or pseudo-random rule. This figure illustrates the row-level scrambling process applied to the plaintext image matrix. The original image rows are permuted according to a control sequence derived from chaotic dynamics, disrupting the vertical spatial structure. This stage serves as the first line of spatial obfuscation, enhancing resistance against structural and statistical attacks [20-21]. To further enhance the unpredictability and security of row permutation in the encryption process, an improved crowd simulation algorithm was introduced as a chaotic sequence generation mechanism based on the traditional chaotic encryption framework to improve the complexity and randomness of sequence perturbations. Its structure is shown in Figure 3.

As shown in Figure 3, a pseudo-random position sequence is generated by simulating the out of column order of the crowd under specific rules to control the permutation order of pixel rows or columns in the image. The use of a crowd simulation algorithm contributes to security by providing a rule-driven, non-deterministic mechanism for generating pixel permutation sequences. Each step in the simulation incorporates prior positional states and dynamic interval calculations, ensuring that even small changes in input lead to entirely different scrambling results. Unlike fixed pseudorandom number generators, this method avoids cyclicity and increases the effective key space. Furthermore, because the algorithm relies on lightweight logical operations rather than cryptographic hashing or matrix inversion, it introduces minimal additional runtime overhead. The process first inputs the starting point position S_0 , the total number of people N , and the basic distance k . Each participant holds a set of keys k_i and is uniformly numbered P_N . Starting from the S_0 th person, the algorithm initializes the reporting interval to k and jumps the number of people clockwise from the current position [22]. The calculation expression for the position L_i of the i th round of the column is shown in equation (1).

$$L_i = (S_{i-1} + k_i) \bmod N' \qquad (1)$$

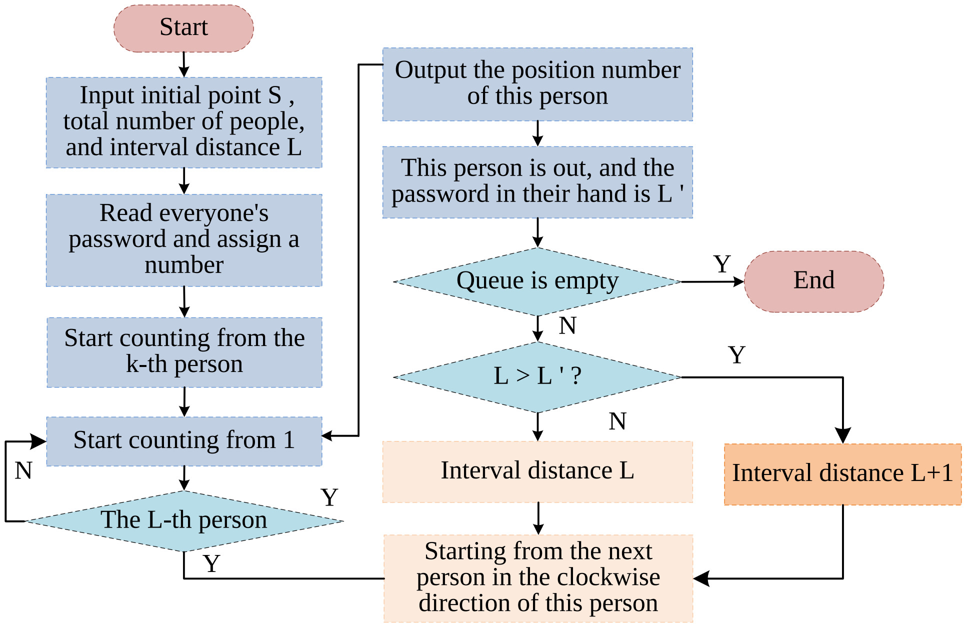

Start
Input initial point S , total number of people, and interval distance L
Read everyone's password and assign a number
Start counting from the k-th person
Start counting from 1
N
The L-th person
Y
Y
Output the position number of this person
This person is out, and the password in their hand is L '
Queue is empty
Y
End
N
L > L ' ?
Y
N
Interval distance L
Interval distance L+1
Starting from the next person in the clockwise direction of this person

Figure 3: A permutation control sequence generation model based on crowd simulation algorithm.

In equation (1), S_{i-1} represents the position of the last delisted person, k_i is the key value held by that person, and N' means the remaining number of people in the current queue. Whenever someone goes out of the queue, the key in their hand will be used as a perturbation factor to participate in the calculation of the next interval, as shown in equation (2).

$$k_{i+1} = (k_i \cdot \alpha + \beta) \bmod \gamma \qquad (2)$$

In equation (2), α , β , and γ are the nonlinear extension parameters set by the system to increase the complexity of the disturbance interval sequence. Next, the position number L_i of each outlier is recorded and filled in the chaotic disruption control vector Z in turn, the expression of which is shown in Equation (3).

$$Z_i = L_i \qquad (3)$$

To prevent regularity between consecutive column positions, disturbance rules are further introduced for secondary position mapping, as expressed in equation (4).

$$Z_i' = (Z_i + \delta_i) \bmod N \qquad (4)$$

In equation (4), δ_i is the disturbance offset calculated based on the difference in position from the previous round. To enhance the unpredictability of spatial permutations and prevent regular patterns, the position sequence Z obtained from the crowd simulation is further refined through secondary mapping to generate Z' . This refined sequence maintains high entropy and removes potential linearity between consecutive elements. While equation (4) describes this process as a generic positional disturbance, in the proposed encryption pipeline, Z' is specifically used as the row permutation control sequence, guiding the scrambling of image rows during the first stage of encryption. In an extended implementation, a parallel sequence can be similarly generated for column-wise permutation if two-dimensional scrambling is required. Its calculation expression is shown in equation (5).

$$\delta_i =| Z_i - Z_{i-1} | \qquad (5)$$

The final sequence $Z' = \{Z_1', Z_2', ..., Z_N'\}$ is obtained, which will serve as the row swapping control sequence in the row shuffling method, guiding the reconstruction process of the arrangement of each row in the plaintext image. Due to the nonlinearity and key dependence of the extraction process, this sequence is highly complex and unpredictable, significantly enhancing the confidentiality of row column scrambling in IE. Combined with chaotic system mechanism, the encryption system has stronger resistance to statistical attacks and known plaintext attacks, thus meeting the dual requirements of encryption strength and speed in news dissemination videos.

In this study, the encryption framework is built upon the logistic CM due to its well-established nonlinear behavior, sensitivity to initial conditions, and low computational complexity. The control parameter used is close to the boundary value of full chaotic behavior, and the initial seed value is selected from a high-precision random domain to ensure that even the slightest variation leads to a completely different output sequence. This high sensitivity ensures that the encrypted results are highly dependent on the initial key, thereby enhancing security. To strengthen the unpredictability of spatial scrambling, a crowd simulation mechanism is introduced in place of conventional pseudorandom generators. Unlike static or cyclic random number generators, the crowd simulation mimics the dynamic interactions of individuals in a group. Each participant in the simulated environment carries a private key and follows rule-driven behaviors, such as changing positions based on interaction history or decision logic. This produces a highly variable and non-repetitive control sequence for pixel permutation. The system parameters within the simulation are specifically selected to increase complexity and eliminate deterministic patterns while ensuring that the system remains lightweight and computationally efficient. Additionally, the algorithm design emphasizes modularity and scalability. By separating the scrambling and diffusion stages and applying them independently to each color channel, the method supports parallel processing and adapts easily to different video resolutions and frame sizes.

3.2 News video encryption algorithm based on chaotic diffusion and CIE

The study introduced chaotic system and improved crowd simulation algorithm to achieve scrambling of video frame images in the row dimension, disrupting the spatial structure of the original image and effectively improving the security of IE. However, a single scrambling operation is not sufficient to combat complex security threats such as differential attacks and statistical attacks [23]. Therefore, further research is needed to construct a joint encryption framework based on "scrambling+diffusion", which performs diffusion operations on pixel values on the basis of spatial structure disturbance, enhancing the information confusion of images in the numerical dimension. Its structure is shown in Figure 4.

As denoted in Figure 4, the proposed encryption framework adopts a layered encryption strategy composed of two distinct modules: the Chaotic Diffusion Encryption (CDE) module and the CIE module. The CDE module operates at a pixel and bit-plane level. It separates the input image into R, G, and B channels, further splits each channel into high and low bit planes, and applies chaotic diffusion using logistic sequences, thereby introducing strong local perturbations and ciphertext feedback. After pixel-level scrambling and value-wise diffusion, the resulting intermediate encrypted image is passed into the CIE module. The CIE module performs a second stage of encryption, focusing on global structure reinforcement. It incorporates secret-key-controlled matrix transformations and a dual diffusion process that spans the entire image matrix. This stage enhances statistical masking and ensures that any structural remnants or value correlations from the first stage are fully obscured. The two modules operate in a hierarchical manner: CDE provides high-entropy, fine-grained diffusion, while CIE reinforces key-dependency and structure-wide decorrelation, forming a comprehensive encryption pipeline. The encryption process starts from the input plaintext image and first generates a pseudo-random key sequence through a chaotic system using a key seed. This sequence serves as a control vector to guide the subsequent encryption operations of the image. Subsequently, the plaintext image enters the CDE module. At this stage, the row and column order of the image is perturbed and replaced according to the key sequence, disrupting the spatial structure. Subsequently, the image is fed into the CIE, which uses the grayscale value of the previous pixel or contextual pixel to perform XOR diffusion with the chaotic sequence, achieving numerical encryption of the image content and ultimately outputting a ciphertext image [24]. The encrypted image is transmitted through a public channel, while the key seed is transmitted through a secure channel to ensure the overall security of the system. During the decryption process, the key seed is re input into the chaotic system to generate the same key sequence as the encryption end. Combined with the input ciphertext image, the plaintext association decryption algorithm is first executed according to the encryption inverse process to restore pixel grayscale, and then the scrambling diffusion inverse operation is performed to restore the image structure, ultimately restoring the original plaintext image. In this process, the most important ones are the scrambling diffusion encryption algorithm and the CIE algorithm, among which the structure of the scrambling diffusion encryption algorithm is shown in Figure 5.

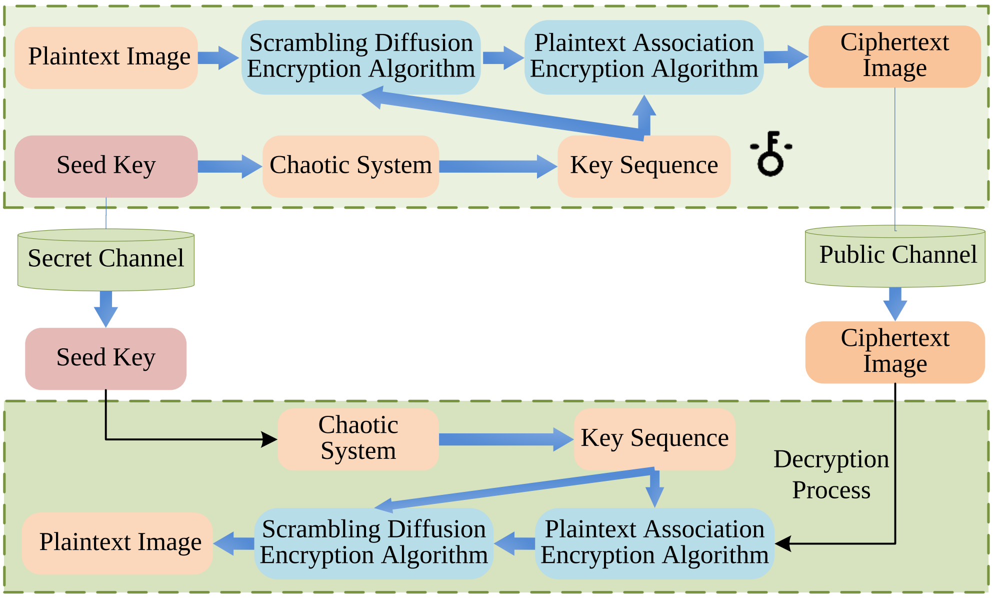


Figure 4: Structure of news video encryption algorithm based on chaotic diffusion and CIE.

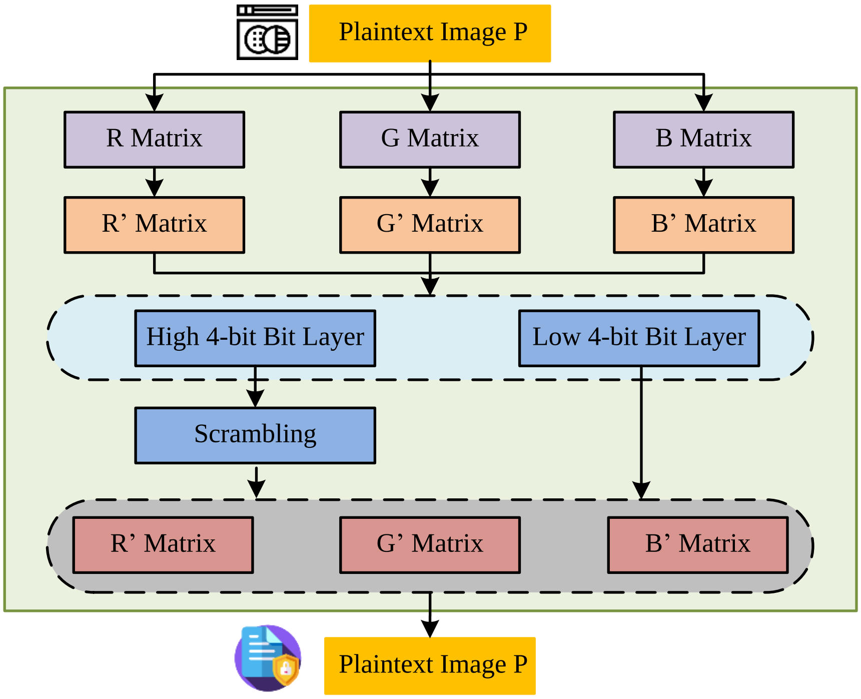


Figure 5: Structure of CDE algorithm.

As shown in Figure 5, the CDE module begins with a lightweight spatial scrambling step applied independently to each RGB channel. This involves permuting the rows and columns based on a pseudo-random permutation vector. After this, each channel is split into high and low bit planes, and chaotic diffusion is applied to each bit layer using key-dependent sequences. The combined result introduces both structural and value-level encryption effects. Encryption processes are designed for the three channels of color images, dividing the original plaintext image into three parts: R, G, and B. Each channel is processed separately to enhance fine-grained control of IE. Each channel first enters the expansion module and completes preliminary scrambling under chaotic sequence control, disrupting the spatial distribution structure of pixels. Then, each pixel is divided into high 4 bits and low 4 bits by bit and subjected to nonlinear diffusion processing [25]. The diffusion algorithm is based on the chaotic sequence generated by logistic mapping, and its formula expression is shown in equation (6).

$$C_i = (P_i \oplus K_i) \oplus C_{i-1} \tag{6}$$

In equation (6), C_i is the encrypted value of the i th pixel, P_i is the original pixel value, K_i is the key value in the chaotic sequence, C_{i-1} is the previous encrypted pixel value, used to introduce a ciphertext feedback mechanism to enhance diffusion strength. The diffusion algorithm is based on the chaotic sequence generated by logistic mapping, and its basic form is shown in equation (7).

$$x_{n+1} = \mu x_n (1 - x_n) \tag{7}$$

In equation (7), x_n denotes the chaotic value of the nth iteration, and μ denotes the system control parameter. The logistic map is tuned with a control parameter μ set to 3.99, which lies in the upper end of the chaotic regime, ensuring full chaos and eliminating periodic behavior. The initial seed value for the sequence is selected randomly within the interval (0,1), with precision extended to fourteen decimal places to maximize sensitivity. To verify the robustness of the generated chaotic sequences, multiple validation procedures are performed. These include analysis of the sequence's Lyapunov exponent, which is found to be positive under all operating parameters, indicating sustained chaotic divergence. In addition, standard randomness evaluation tests such as NIST SP 800-22 are applied to the generated key streams, confirming uniform distribution, low autocorrelation, and absence of detectable patterns.

After the above diffusion, the high 4 bits and low 4 bits are reordered in the Jospehus algorithm module, which performs a circular column out operation on the sequence through specific hop counts and intervals to further enhance the unpredictability of the sequence. After the high and low bits are recombined, they are merged to generate encrypted R, G, and B matrices, and finally merged to output an encrypted image. Then, the encrypted image is input into the CIE algorithm for further encryption, as shown in Figure 6.

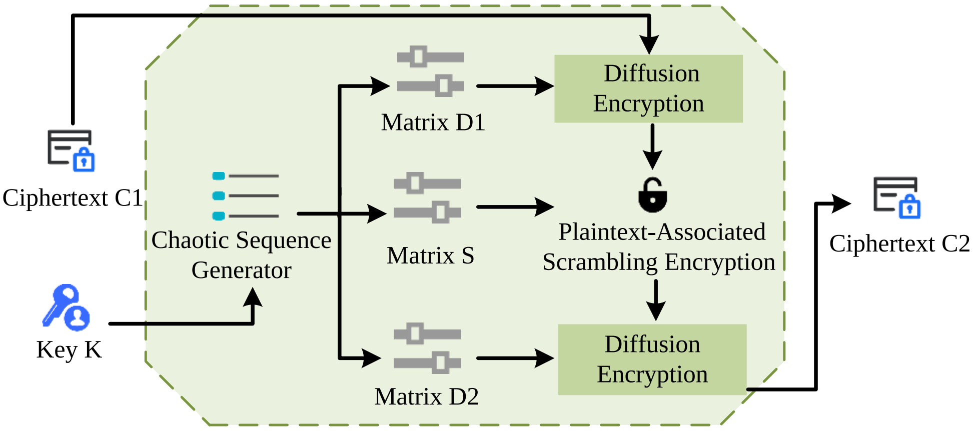
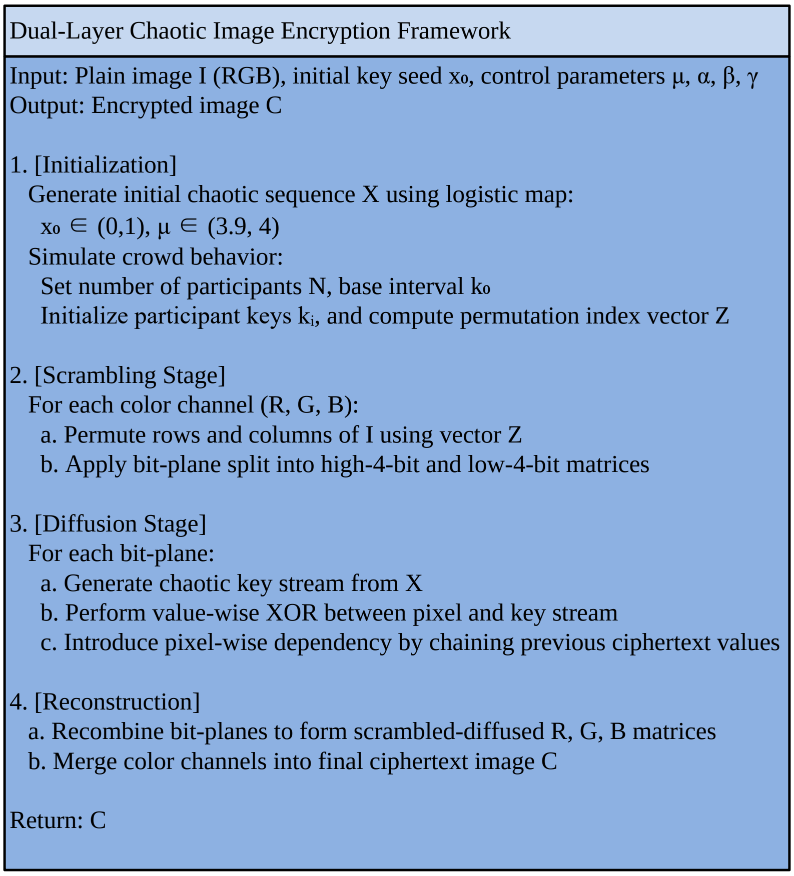


Figure 6: Global key-driven CIE module.



```
Dual-Layer Chaotic Image Encryption Framework
Input: Plain image I (RGB), initial key seed x₀, control parameters μ, α, β, γ
Output: Encrypted image C

1. [Initialization]
  Generate initial chaotic sequence X using logistic map:
    x₀ ∈ (0,1), μ ∈ (3.9, 4)
  Simulate crowd behavior:
    Set number of participants N, base interval k₀
    Initialize participant keys kᵢ, and compute permutation index vector Z

2. [Scrambling Stage]
  For each color channel (R, G, B):
    a. Permute rows and columns of I using vector Z
    b. Apply bit-plane split into high-4-bit and low-4-bit matrices

3. [Diffusion Stage]
  For each bit-plane:
    a. Generate chaotic key stream from X
    b. Perform value-wise XOR between pixel and key stream
    c. Introduce pixel-wise dependency by chaining previous ciphertext values

4. [Reconstruction]
  a. Recombine bit-planes to form scrambled-diffused R, G, B matrices
  b. Merge color channels into final ciphertext image C

Return: C
```

Figure 7: Dual-layer CIE framework.

As shown in Figure 6, the module first performs Plaintext-Associated Scrambling Encryption, which dynamically generates permutation sequences based on plaintext characteristics to destroy any inherent structural correlation in the image, followed by Diffusion Encryption to enhance key sensitivity and achieve strong statistical confusion. The algorithm takes the key K and the initial ciphertext image C1 as inputs, and generates a highly random key stream matrix S through a chaotic sequence generator to control the core parameters of the entire image diffusion and scrambling process. Firstly, the key K is introduced into the chaotic system, and the one-dimensional sequence is transformed into a two-dimensional matrix S through chaotic system. Two control matrices D_1 and D_2 are further generated for diffusion encryption, which are applied to different stages of IE. The ciphertext C1 undergoes the first diffusion encryption and XOR operation with the elements of matrix D1, and its expression is shown in equation (8).

$$C_i' = C_i \oplus D_{1,i} \tag{8}$$

In equation (8), C_i is the i th pixel value, and $D_{1,i}$ denotes the corresponding element in the control matrix. This operation can disrupt the statistical distribution of the original image pixel values. Afterwards, the structure in the plaintext correlation scrambling diffusion module is jointly operated with the key matrix S, introducing the internal structural correlation of the image. Then, a second diffusion operation is performed on the result, and the final pixel perturbation is completed through matrix D2. The core calculation expression is shown in equation (9).

$$C_i'' = C_i' \oplus D_{2,i} \tag{9}$$

According to equation (9), the final output ciphertext image has a certain level of encryption strength and anti-analysis performance.

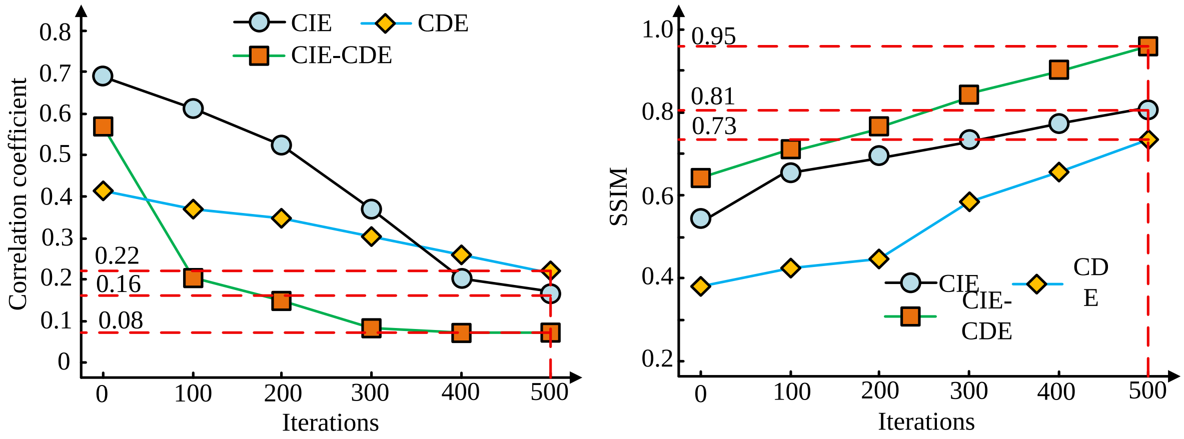
4 Results

4.1 News video encryption algorithm based on chaotic diffusion and CIE

The experimental hardware configuration used in the study was Intel Core i7-13900 as the central processor, NVIDIA Geforce GTX4060Ti as the graphics processor, 16GB of VRAM, 32GB of RAM, and Windows 11 operating system. The dataset adopted the publicly available TVSum Dataset, which contains 50 real video clips from YouTube, covering multiple topic categories such as news, travel, speeches, DIY, sports, lifestyle, music, etc. The study selected news related data and divided it into 5000 pieces, which were then divided into a training set and a validation set in a 4:1 ratio. To ensure that the proposed video encryption framework is evaluated on a standardized and widely recognized benchmark, the TVSum dataset was integrated into the experimental pipeline. TVSum contains 50 real-world videos sourced from YouTube across diverse genres-including news, sports, documentaries, and user-generated content-with frame-level human-annotated importance scores. Although the original dataset is primarily intended for video summarization, its granularity and annotation structure enable fine-grained evaluation of visual consistency and decryption fidelity across keyframes and transition scenes. In this study, individual video frames were extracted from four representative categories within TVSum to assess the encryption model's adaptability across content types. This integration facilitates consistent benchmarking, improves experimental rigor, and aligns the evaluation protocol with community standards.

Selecting a single CIE and CDE as comparison models, the results are shown in Figure 8.

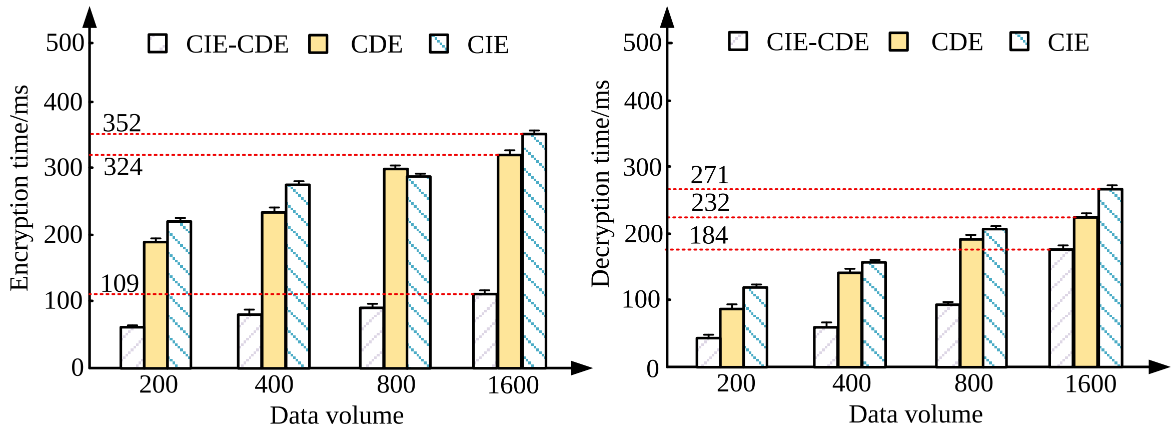
Figure 8 (a) shows the trend of correlation coefficient changes for different algorithms during multiple iterations, while Figure 8 (b) illustrates the variation of Structural Similarity Index Measure (SSIM) during the iteration process. From Figure 8 (a), CIE, CDE, and CIE-CDE all had high correlation in the early stages of iteration, especially the initial correlation coefficient of the CIE algorithm was close to 0.7, indicating that the image has not completely broken the statistical dependence between the original pixels. As the amount of iterations increased, the correlation coefficients of the three methods gradually decreased, with the CIE-CDE combination algorithm showing the most significant decrease. At 500 iterations, its correlation was the lowest at only 0.08, significantly better than CIE's 0.22 and CDE's 0.16. This indicates that the CIE-CDE method, which combines scrambling and diffusion mechanisms, can more effectively eliminate redundant information in images and enhance the ability to resist statistical attacks in IE. Figure 8(b) presents the SSIM values between the decrypted images and the original plaintext images under different iteration counts. As the number of iterations increased, the SSIM value steadily rose, reaching 0.95 at 500 iterations. This indicated that the decrypted images closely approximated the original images in structure and visual fidelity, reflecting strong reversibility and decryption accuracy of the proposed encryption-decryption pipeline. It is important to note that SSIM evaluates the similarity between the output of the decryption process and the original image, and should not be interpreted as a metric of encryption security. In fact, during encryption, the structural correlation between the ciphertext and the original should be minimized to ensure confidentiality. The analysis of various models under different data volumes is denoted in Figure 9.



(a) Correlation coefficient

(b) SSIM

Figure 8: Analysis of correlation coefficient and ssim changes of various models.



(a) Encryption time

(b) Decryption time

Figure 9: Changes in encryption and decryption time of three encryption algorithms under different data volumes.

Table 2: Comprehensive performance analysis table.

Test	Model	Entropy	NPCR/%	UAC/%	Pixel correlation	SSIM	Encryption time/ms	Declassified time/ms
Test 1	CIE	7.85	99.21	32.14	0.22	0.81	352	271
	CDE	7.89	99.37	32.71	0.16	0.73	324	232
	CIE-CDE	7.97	99.62	33.09	0.08	0.95	109	184
Test 2	CIE	7.84	99.17	32.06	0.23	0.8	349	268
	CDE	7.88	99.34	32.65	0.15	0.74	321	229
	CIE-CDE	7.96	99.6	33.02	0.09	0.94	111	186

Figure 9 (a) illustrates the variation in encryption time for three encryption algorithms under different data volumes, while Figure 9 (b) depicts the comparative decryption times under the same conditions. As data volume increased, the encryption time of all three algorithms increased correspondingly. Among them, the CIE algorithm consistently required the longest processing time, reaching 352 milliseconds at a data volume of 1600. The CDE algorithm followed at 324 milliseconds, whereas the CIE-CDE algorithm achieved an encryption time of just 109 milliseconds under identical conditions, demonstrating a substantial advantage in encryption efficiency. This suggests that CIE-CDE minimizes redundant computations through structural optimization and process integration, thereby achieving significantly improved encryption performance compared to traditional methods. According to Figure 9 (b), when the data volume was 1600, the decryption time of the CIE algorithm was 271 milliseconds, CDE was 232 milliseconds, and CIE-CDE achieved the shortest decryption time at just 184 milliseconds. This result indicates that the CIE algorithm still involves complex decryption procedures, potentially including lengthy anti-diffusion steps or computationally intensive inverse transformations. In contrast, CIE-CDE reduces decryption latency by employing a symmetric and streamlined architecture that ensures accuracy while improving efficiency. The experimental results demonstrate that CIE-CDE exhibits strong encryption performance and excels in both encryption and decryption efficiency, making it particularly well-suited for news video encryption scenarios with stringent real-time requirements. To evaluate the robustness and consistency of the proposed encryption model, two independent experiments were conducted using the same video dataset (TVSum) but with randomly initialized secret keys and chaotic seeds. These are referred to as Test 1 and Test 2 in Table 2. Each test applied the encryption pipeline to the same input but with different internal parameters, allowing assessment of the model's performance under random key variations.

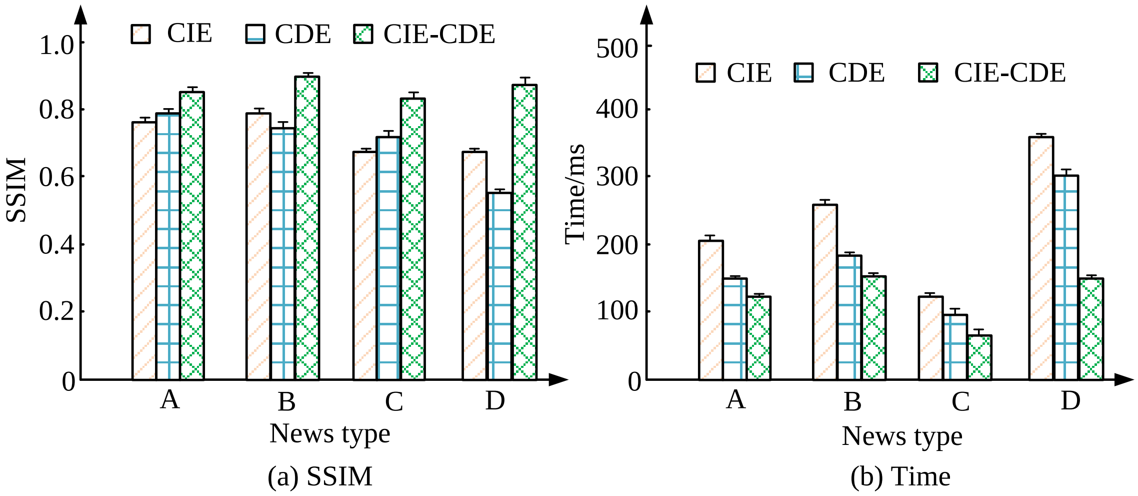
According to Table 2, in Test 1, CIE-CDE performed the best in terms of security and efficiency, with an information entropy of 7.97, which was closest to the ideal value of 8, indicating that the encrypted image has a high degree of randomness. At the same time, its NPCR was 99.62% and UACI was 33.09%, far higher than CIE's 99.21% and 32.14%, indicating stronger sensitivity to changes in pixel values and higher resistance to differential attacks. In terms of pixel correlation, CIE-CDE was only 0.08, significantly better than CIE's 0.22 and CDE's 0.16, reflecting its ability to better disrupt the original image structure. In terms of SSIM, CIE-CDE was 0.95, which was close to perfect restoration, indicating excellent encryption reversibility. In addition, its encryption and decryption time were only 109 milliseconds and 184 milliseconds respectively, far lower than other models. The performance of each model in Test 2 was basically consistent with Test 1, which verified the stability of the results and the robustness of the algorithm. CIE-CDE still maintained the highest entropy value of 7.96, the lowest correlation of 0.09, and the shortest time of 111 milliseconds and 186 milliseconds, with the best overall performance. The experimental results indicate that the proposed method is suitable for news IE scenarios that require both high security and efficiency. Table 1 presents the overall encryption performance of the proposed algorithm under two independent tests (Test 1 and Test 2), each using different randomly initialized secret keys but applied to the same set of news videos. These tests are designed to assess algorithmic stability and robustness under key variation. In contrast, Table 2 provides detailed simulation performance across four categorized types of news content-Type A (politics), Type B (economy), Type C (entertainment), and Type D (social affairs)-to evaluate real-world adaptability. While both tables are based on the same encryption framework, Table 1 focuses on key sensitivity, whereas Table 2 evaluates content-dependent operational performance.

4.2 Model simulation performance testing

To further assess the effectiveness of the model, four different types of news data were selected and encrypted. The results are shown in Figure 10.

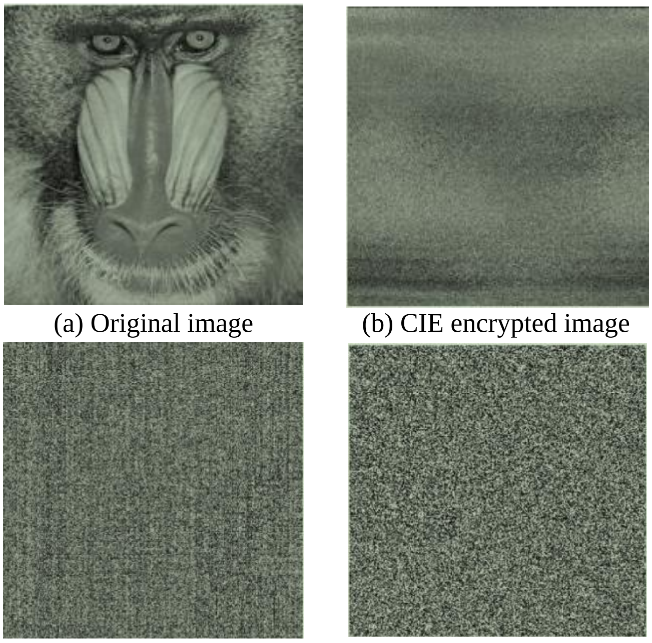
Figure 10 (a) illustrates the SSIM of three encryption models across different types of news videos, while Figure 10 (b) depicts the cumulative encryption and decryption time of the three algorithms for four types of news videos. In news Type A, the SSIM of CIE was approximately 0.76, CDE achieved 0.79, and CIE-CDE reached 0.87, suggesting that CIE-CDE demonstrates superior decryption accuracy and image reconstruction quality for this video type. In news Type B, the SSIM of CIE-CDE was close to 0.89, significantly higher than CIE’s 0.78 and CDE’s 0.74, highlighting its enhanced ability to preserve image structure. The performance gap further widened in Type C, where CIE and CDE attained SSIM values of only 0.72 and 0.75, respectively, while CIE-CDE exceeded 0.85, demonstrating its robustness in preserving image reversibility for frames with complex textures. In Type D, CIE-CDE also outperformed the other methods, achieving an SSIM above 0.88, compared to 0.70 for CIE and 0.67 for CDE. According to Figure 10 (b), CIE required approximately 460 milliseconds for Type D, while CDE consumed slightly less at around 360 milliseconds. In contrast, CIE-CDE exhibited significantly lower latency compared to both models, maintaining encryption and decryption times below 200 milliseconds across all news types, with Type C requiring only about 120 milliseconds. For Types B and A, its processing times were approximately 150 and 130 milliseconds, respectively, demonstrating notable efficiency gains attributable to its structural optimization. These results indicate that CIE-CDE maintains stable structural reconstruction across diverse news content types, making it particularly suitable for broadcasting scenarios where high-quality post-decryption imagery is essential. The actual encryption effects of each model were analyzed, and the results are shown in Figure 11.

Figure 11 (a) shows the original image, and Figures 11 (b) to 11 (d) represent the encrypted images of CIE algorithm, CDE algorithm, and CIE-CDE algorithm, respectively. From Figure 11, although the overall texture of the image encrypted by the CIE algorithm has been disrupted, a certain degree of structural residue could still be observed in the image, especially in the lower region where there is a slight stripe feeling. This indicates that the CIE algorithm has certain limitations in destroying inter pixel correlation, resulting in the preservation of some original structural information after IE. In CDE encryption, the overall image was more uniform, but there were still slight block patterns, with strong diffusion but insufficient scrambling. The image encrypted by CIE-CDE algorithm had a highly uniform pixel distribution, presenting an ideal random noise state without obvious recognizable structures. The experimental results show that the CIE-CDE algorithm can effectively integrate the advantages of scrambling and diffusion, achieve high-strength encryption and complete structural destruction, and significantly improve the visual unidentifiable and security of encrypted images. Table 3 provides detailed simulation performance across four categorized types of news content-Type A (politics), Type B (economy), Type C (entertainment), and Type D (social affairs)-to evaluate real-world adaptability. The simulation performance of each model was tested, and the results are shown in Table 3.



(a) SSIM (b) Time

Figure 10: Analysis of SSIM and total encryption and decryption time of the model in different types of news videos.



(a) Original image

(b) CIE encrypted image

(c) CDE encrypted image

(d) CIE-CDE encrypted image

Figure 11: Analysis of the actual encryption effect of the model.

Table 3: Simulation performance testing.

Type	Model	Entropy	NPCR/%	UACI/%	Pixel correlation	SSIM	Encryption time/ms	Declassified time/ms
A	CIE	7.82	99.18	31.92	0.24	0.76	208	271
	CDE	7.86	99.33	32.58	0.17	0.79	158	224
	CIE-CDE	7.95	99.59	33.01	0.09	0.87	128	182
B	CIE	7.88	99.24	32.11	0.22	0.78	261	287
	CDE	7.91	99.38	32.69	0.15	0.74	186	239
	CIE-CDE	7.96	99.61	33.07	0.08	0.89	146	192
C	CIE	7.79	99.15	31.74	0.25	0.72	135	198
	CDE	7.83	99.32	32.48	0.18	0.75	108	170
	CIE-CDE	7.94	99.57	33.04	0.1	0.85	91	152
D	CIE	7.86	99.2	32.02	0.21	0.71	348	375
	CDE	7.9	99.36	32.66	0.14	0.73	295	324
	CIE-CDE	7.97	99.63	33.12	0.08	0.88	162	189

According to Table 3, in terms of information entropy, CIE-CDE consistently maintained the highest level among the four images, reaching 7.97 in Type D images, indicating that its encryption results are closer to the ideal random distribution. In terms of resistance to differential attacks, the NPCR of CIE-CDE exceeded 99.57% in all four types of images, while UACI remained stable at over 33%, significantly better than CIE's average of 32.0%, indicating that it can effectively disrupt pixel distribution at different image complexities. In terms of structural correlation, CIE-CDE had the lowest pixel correlation, only 0.09 in Type A images and dropping to 0.08 in Type B images, indicating that its encrypted image structural information is highly corrupted and difficult to restore or infer. The SSIM index showed that CIE-CDE also performed well in reversibility, with a maximum of 0.89, far higher than the CIE range of 0.71 to 0.78. In terms of encryption and decryption efficiency, CIE-CDE always maintained the lowest processing time, with an encryption time of only 91 milliseconds in Type C images, which was significantly reduced compared to CIE's 135 milliseconds. In summary, the CIE-CDE model exhibits the best security, efficiency, and stability in all test image types. To demonstrate the performance at the video sequence level, the research designed a comprehensive evaluation of video stream encryption performance, as shown in Table 4.

Table 4 presents the comprehensive performance of the proposed encryption model under complete video stream encryption, compression coding environment and channel interference conditions. In the full video stream encryption test, the lengths of each test video ranged from 30 to 60 seconds, with resolutions covering 720P and 1080P. The results showed that, while maintaining no frame loss, the model's average encryption throughput reached 225 frames per second, and the end-to-end delay was controlled within approximately 400 milliseconds per second of video. The SSIM after decryption was all higher than 0.986, verifying its good adaptability to video continuity. In the H.264 compression environment, despite the existence of quantization loss and edge smoothing phenomena, the SSIM after decryption still remained above 0.91, indicating that the model has strong compression robustness. In the channel interference simulation, under the conditions of introducing Gaussian noise and a 3% packet loss rate respectively, the decrypted image still maintained a good visual structure, with SSIMs of 0.906 and 0.864 respectively, and no frame misalignment or out-of-step phenomenon occurred. Comprehensive analysis shows that this model not only has high-strength encryption capabilities at the static frame level, but also maintains stable security and structural recoverability in dynamic video streams, compression and interference environments, making it suitable for the encrypted dissemination requirements of actual news videos.

To validate the performance and security of the proposed dual-chaotic encryption framework, a comparative evaluation was performed against three widely acknowledged encryption algorithms in recent literature: RC4-Chaos, Logistic-Sine Map Encryption (LSM), and DNA-based Chaotic Image Encryption (DNA-CIE). These methods are selected due to their distinct structural designs-stream cipher enhancement, composite CM, and biologically inspired encryption-thus offering a diversified baseline for comparison. All algorithms were tested on 720p video frames extracted from the TVSum dataset. Performance metrics included encryption time, decryption time, Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), information entropy, and SSIM between decrypted and original frames.

As summarized in Table 5, the proposed method achieved NPCR of 99.64% and UACI of 33.51%, indicating strong diffusion capabilities. The entropy value approached the ideal of 8.0, suggesting high randomness in the ciphertext. Additionally, the total runtime remained under 250 ms, demonstrating the method’s practical viability for near real-time video encryption scenarios. Compared to RC4-Chaos, which is lightweight but suffers from limited key diffusion, and DNA-CIE, which is highly secure but computationally expensive, the proposed method struck a favorable balance between security strength and computational efficiency. LSTM performed well on statistical metrics but lacks structural adaptability to varied video content types. These results underscore the robustness and generalizability of the proposed framework in practical video security applications.

4.3 Security analysis

To evaluate the robustness of the proposed encryption framework beyond empirical metrics, a theoretical security analysis was presented to examine key space size, resistance to standard attacks, and diffusion strength.

The encryption system was controlled by multiple key components: (1) the initial value x_0 of the logistic map ($\geq 10^{-14}$ precision), (2) the control parameter μ, (3) the parameters α, β, and γ of the crowd simulation, and (4) the initial participant keys for each image dimension. Assuming 64-bit precision and independent parameterization, the total key space exceeded 2^{128}, which is sufficient to resist brute-force attacks under current computational limits. Brute-force attempts were infeasible due to the nonlinearity and high sensitivity of the chaotic sequence to initial seeds. Any minimal variation in x_0 or α, β, γ resulted in a completely different permutation and diffusion sequence. For known-plaintext or chosen-plaintext attacks, the dual mechanism combining position scrambling with pixel diffusion created a non-linear mapping between plaintext and ciphertext. Even when attackers possess pairs of known input-output images, the absence of linearity and high sensitivity prevented reverse-engineering of the original key or structure. The diffusion process introduced strong sensitivity to both pixel values and contextual states. A one-bit change in the plaintext or initial key affected the subsequent chaotic sequence, which in turn modified every pixel’s value through cumulative XOR diffusion. Empirical tests showed NPCR > 99.6% and UACI ≈ 33%, but theoretical structure ensured that the system satisfied the avalanche criterion: the output changed significantly even when the input is minimally altered. This is further amplified by the feedback-based chaining structure used in the pixel-wise diffusion.

Table 4: Comprehensive evaluation of video stream encryption performance.

Test Type	Clip/Condition	Resolution	Frame Count	SSIM (Decrypted)	Throughput (fps)	Latency (ms/s)
Full-Stream Test	A (32s)	1280×720	800	0.988	228	405
	B (45s)	1920×1080	1125	0.986	221	417
	C (60s)	1280×720	1500	0.989	230	398
	D (35s)	1920×1080	875	0.987	222	412
	E (58s)	1280×720	1450	0.988	226	414
H.264 Compression	A (3 Mbps)	1280×720	/	0.912	/	/
	B (4.5 Mbps)	1920×1080	/	0.915	/	/
	C (3 Mbps)	1280×720	/	0.909	/	/
Noise Test	Gaussian noise 25 dB	1280×720	/	0.906	/	/
	Packet loss 3%	1280×720	/	0.864	/	/

Table 5: Comparative results with state-of-the-art algorithms.

Method	NPCR (%)	UACI (%)	Entropy	Total Time (ms)	SSIM (Decryption)
Proposed	99.64	33.51	7.9983	243	0.957
RC4-Chaos	97.85	31.02	7.8721	198	0.948
LSM	99.31	32.87	7.9912	275	0.951
DNA-CIE	99.67	33.46	7.9968	384	0.959

In summary, the proposed model satisfies the core requirements of a secure IE system, offering a large and complex key space, high resistance to classical attacks, and robust diffusion characteristics suitable for real-time secure video applications.

5 Discussion

The experimental findings demonstrated that the proposed CIE-CDE encryption algorithm achieved a strong balance among security strength, encryption efficiency, and decryption reversibility. Across all tested video types, the model consistently maintained high entropy values (above 7.95), indicating that the encrypted images approximate ideal randomness and are resistant to statistical analysis. Furthermore, the low pixel correlation coefficients (as low as 0.08) reflected the model’s ability to effectively disrupt spatial redundancy in the image structure, which is critical for breaking inter-pixel predictability. The high SSIM, reaching up to 0.95 after decryption, suggested that despite strong scrambling and diffusion, the algorithm preserved the recoverability of the original video frames. This was largely attributed to the design of the plaintext-associated diffusion strategy, which carefully integrated contextual information into the encryption process without compromising structural integrity. In terms of processing performance, the CIE-CDE model significantly reduced the total encryption and decryption time. The encryption time remained under 130 milliseconds across all video types, with the fastest processing observed at just 91 milliseconds. This efficiency gain is primarily due to the lightweight implementation of the dual-stage encryption structure, where the scrambling phase-driven by crowd simulation—requires minimal computation and introduces high variability in pixel positioning. Notably, the incorporation of the crowd simulation mechanism as a key generation and control strategy contributes to the unpredictability of row-column permutations, enhancing resistance against structured attacks without increasing computational load. The logistic-based chaotic diffusion further ensures that minor changes in pixel values propagate widely across the image, reinforcing the algorithm's differential sensitivity. However, several limitations are also apparent. The current model assumes a noise-free and uncompressed transmission environment, which may not fully represent real-world conditions such as wireless streaming or low-bitrate video formats. Additionally, while the algorithm demonstrates excellent performance on full-resolution video frames, its behavior under different resolutions, frame rates, or hardware constraints remains to be tested. Furthermore, the two-phase encryption process, though efficient, still involves multiple iterations and matrix transformations that could pose computational challenges on low-power or embedded systems.

In future research, attention should be given to compression-robust encryption, adaptive key scheduling under varying channel conditions, and potential integration with video coding standards. Exploring these directions will help expand the applicability of the CIE-CDE model to more diverse and dynamic media environments.

6 Conclusion

In response to the security issues of news videos being susceptible to tampering, forgery, and leakage during transmission, a video encryption model that integrates scrambling diffusion mechanism and multidimensional chaos control structure was studied and designed. The model generated a key stream through crowd simulation to enhance key complexity and unpredictable disturbances. The experimental results showed that among different encryption models, CIE-CDE consistently maintained the highest information entropy, reaching 7.97 in type D videos, close to the ideal maximum value of 8, while CIE and CDE were 7.86 and 7.90, respectively, indicating that the model has stronger pixel information obfuscation ability. In terms of pixel difference sensitivity, the NPCR of CIE-CDE was the highest at 99.63%, while UACI was 33.12%, significantly better than CIE's 99.20% and 32.02% and CDE's 99.36% and 32.66%, indicating its superior performance in resisting differential attacks. Especially in type B images, CIE-CDE reduced pixel correlation to 0.08, a decrease of more than 60% compared to CIE's 0.22 and CDE's 0.15, and almost completely dispersed the structural information between encrypted images. Although the model has achieved better results in balancing structural safety and efficiency, there is still room for further improvement. The current method has not yet introduced compression channels and anti noise mechanisms, and the fault tolerance of videos in different compression formats needs to be enhanced. Future research can explore in depth the lightweight design of algorithms, adaptive key adjustment, and robust encryption structures to achieve higher strength, cross platform video security encryption schemes.

The proposed encryption framework, though validated using news video datasets, exhibits structural features and algorithmic components that are generalizable to other video domains such as surveillance footage, medical imaging sequences, and industrial monitoring streams. The modular separation of spatial scrambling and pixel-wise diffusion allows the model to be adapted to varying frame resolutions, temporal continuity constraints, and domain-specific privacy requirements. Furthermore, the rule-based crowd simulation and chaotic control structure can be integrated with dynamic key generation schemes, enabling adaptive key updates per frame or per session, which enhances resilience in long-term secure video transmission. The algorithm also remains lightweight enough to be embedded in resource-constrained environments such as edge cameras or mobile terminals. As emerging cryptographic challenges such as quantum attacks gain attention, the framework can be extended by incorporating quantum-safe key scheduling methods or post-quantum lattice-based encryption in the key exchange stage, ensuring forward security under evolving threat models. These features suggest that the model holds promise for deployment in diverse real-world scenarios requiring high-level video confidentiality and performance stability.

References

[1] Yong Zhang, Ruiyou Li, Yuwen Shi, and Fan Luo. The probabilistic image encryption algorithm based on galois field Gf (257). IETE Journal of Research, 70(7):6286-6299, 2024. https://doi.org/10.1080/03772063.2023.2284956

[2] Lizong Li. Image encryption algorithm based on hyperchaos and DNA coding. IET Image Processing (Wiley-Blackwell), 18(3):627-633, 2024. https://doi.org/10.1049/ipr2.12974

[3] Ming Yao, Zhong Chen, Hongwei Deng, Ximei Wu, Tongzhe Liu, and Can Cao. A color image compression and encryption algorithm combining compressed sensing, Sudoku matrix, and hyperchaotic map. Nonlinear Dynamics, 113(3):2831-2865, 2025. https://doi.org/10.1007/s11071-024-10334-2

[4] Deep Singh, and Sandeep Kumar. Image authentication and encryption algorithm based on RSA cryptosystem and chaotic maps. Expert Systems with Applications, 274(15):141-152, 2025. https://doi.org/10.1016/j.eswa.2025.126883

[5] Anlin Wang, Chuan Shen, Junqiao Pan, Cheng Zhang, Hong Cheng, and Sui Wei. Research on multiple-image encryption method using modified Gerchberg-Saxton algorithm and chaotic systems. Optical Engineering, 62(9):098103.1-098103.14, 2023. https://doi.org/10.1117/1.OE.62.9.098103

[6] Yunhao Liu, and Ru Xue. 3D medical image encryption algorithm using biometric key and cubic S-box. Physica Scripta, 99(5):55035-55055, 2024. https://doi.org/10.1088/1402-4896/ad3b3d

[7] Chao Huang, Ye Tao, and JingWei Zhao. An image encryption algorithm for colour images based on a cellular neural network and the Chua's chaotic system. Journal of Modern Optics, 71(9):321-336, 2024. https://doi.org/10.1080/09500340.2024.2418371

[8] Hangming Zhang, and Hanping Hu. An image encryption algorithm based on a compound-coupled chaotic system. Digital Signal Processing, 146(1):54-59, 2024. https://doi.org/10.1016/j.dsp.2023.104367

[9] Xuenan Peng, and Yicheng Zeng. Image encryption application in a system for compounding self-excited and hidden attractors. Chaos Solitons & Fractals, 139(6):1144-1159, 2020. https://doi.org/10.1016/j.chaos.2020.110044

[10] Mohamed Boussif, Noureddine Aloui, and Adnene Cherif. Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher. IET Image Processing, 2020, 14(6):1209-1216. https://doi.org/10.1049/iet-ipr.2019.0042

[11] Xingyuan Wang, and Suo Gao. Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. Information Sciences, 539(9):195-214, 2020. https://doi.org/10.1016/j.ins.2020.06.030

[12] Kurunandan Jain, Aravind Aji, and Prabhakar Krishnan. Medical image encryption scheme using multiple chaotic maps. Pattern Recognition Letters, 152(12):356-364, 2021. https://doi.org/10.1016/j.patrec.2021.10.033

[13] M. Zarebnia, H. Pakmanesh, and R. Parvaz. A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images. Optik, 179(3):761-773, 2019. https://doi.org/10.1016/j.ijleo.2018.10.025

[14] Dingkang Mou, and Yumin Dong. Image encryption algorithm based on multiple chaotic systems and improved Joseph block scrambling. Chinese Physics B, 33(10):104205-104206, 2024. https://doi.org/10.1088/1674-1056/ad6257

[15] Moatsum Alawida. A novel image encryption algorithm based on cyclic chaotic map in industrial IoT environments. IEEE Transactions on Industrial Informatics, 20(8):10530-10541, 2024. https://doi.org/10.1109/TII.2024.3395631

[16] Shuqin Zhu, Congxu Zhu, and Hanyu Yan. Cryptanalyzing and improving an image encryption algorithm based on chaotic dual scrambling of pixel position and bit. Entropy, 3(25):59-65, 2023. https://doi.org/10.3390/e25030400

[17] Eligijus Sakalauskas, Antanas Bendoraitis, Dalė Lukšaitė, Gintaras Butkus, and Daiva Vitkutė-Adžgauskienė. Tax declaration scheme using blockchain confidential transactions. Informatica, 34(3):603-616, 2023. https://doi.org/10.15388/23-INFOR531

[18] Sarmad Mahmmod Ahmed, and Baban Ahmed Mahmood. Cloud computing security: Assured deletion. Informatica, 48(3):485-496, 2024. https://doi.org/10.31449/inf.v48i3.6245

[19] Yumin Dong, Chen Xu, and Chenhao Yin. Three-layer quantum image encryption algorithm based on 6D hyperchaos. Journal of Applied Physics, 134(22):224401.1-224401.14, 2023. https://doi.org/10.1063/5.0176657

[20] Qinmao Jiang, Simin Yu, and Qianxue Wang. Cryptanalysis of an image encryption algorithm based on two-dimensional hyperchaotic map. Entropy, 25(3):41-58, 2023. https://doi.org/10.3390/e25030395

[21] Uddagiri Sirisha, and Bolem Sai Chandana. Privacy preserving image encryption with optimal deep transfer learning-based accident severity classification model. Sensors, 23(1):519-520, 2023. https://doi.org/10.3390/s23010519

[22] ShiMing Fu, XueFeng Cheng, and Juan Liu. Dynamics, circuit design, feedback control of a new hyperchaotic system and its application in audio encryption. Scientific Reports, 13(1):19385-19392, 2023. https://doi.org/10.1038/s41598-023-46161-5

[23] Dingkang Mou, and Yumin Dong. Color image encryption algorithm based on novel dynamic DNA encoding and chaotic system. Physica Scripta,

99(6):15-19, 2024. https://doi.org/10.1088/1402-4896/ad3ff1

[24] Gurpreet Kaur, Rekha Agarwal, and Vinod Patidar. Color image encryption scheme based on fractional Hartley transform and chaotic substitution-permutation. The Visual Computer, 38(3):1027-1050, 2022. https://doi.org/10.1007/s00371-021-02066-w

[25] Ram Ratan, and Arvind Yadav. Security analysis of bit plane level image encryption schemes. Defence Science Journal, 71(2):209-221, 2021. https://doi.org/10.14429/dsj.71.15643