A Secure and Compound 3D Chaos-Based Image Encryption Scheme Using Hybrid Genetic Operators

Ravikumar H K[1*], Dr. M K Agarwal[2]

[1]Research Scholar, Bundelkhand University

[2]Professor, Bundelkhand University

Abstract

In today's digital era, ensuring the confidentiality of multimedia data, particularly images, has become a critical challenge due to increasing cyber threats and the inadequacy of traditional cryptographic methods. This paper proposes a Secure and Compound Image Encryption (SCIE) scheme that integrates three-dimensional Compound Sine–ICMIC (CSI) chaotic maps with hybrid genetic operators, including arithmetic crossover, multipoint crossover, and hybrid mutation strategies. The scheme enhances both confusion and diffusion, ensuring high resistance against statistical, brute-force, and differential attacks. Experimental validation was carried out on a diverse set of grayscale images, with performance evaluated using metrics such as histogram analysis, correlation coefficients, entropy, NPCR, UACI, and encryption time. Results demonstrate that the SCIE approach achieves nearly uniform histograms, significantly reduced correlation among adjacent pixels, high entropy values close to the theoretical maximum, and strong resistance against plaintext attacks, all while maintaining computational efficiency. Comparisons with existing methods confirm that the proposed system provides superior security and faster execution, making it suitable for real-time secure image transmission in applications such as healthcare, defense, and satellite communication.

Keywords: Image Encryption, Chaos Theory, Genetic Algorithms, CSI Chaotic Map, Hybrid Mutation, NPCR, UACI, Multimedia Security

1. Introduction

In the contemporary digital era, the exchange of sensitive information across open and insecure networks has become an integral part of daily activities in both professional and personal domains. Encryption, as a fundamental component of cybersecurity, plays a vital role in ensuring that this information remains protected from unauthorized access. It converts intelligible data into an unintelligible format, allowing only authorized recipients with the correct key to retrieve the original content. With the rapid advancement of computer technologies and global networking infrastructures, a substantial amount of data is now transmitted over the Internet [1]. This information is not limited to textual communication but also encompasses multimedia formats such as images, audio, and video. Among these, image data requires particular attention due to its vast applications in sectors such as healthcare, defense, satellite communication, and secure document handling.

The open nature of the Internet, however, has led to an escalation in cyber threats. Malicious actors exploit vulnerabilities to intercept and manipulate transmitted information, highlighting the necessity of robust encryption mechanisms. Traditional encryption techniques, while effective for text-based communication, often fall short when applied to images. This limitation is due to the inherent properties of images, such as their large data size, high pixel correlation, and redundancy [2]. Consequently, image encryption has emerged as a significant area of research within cryptography and information security.

In recent years, chaos-based cryptographic schemes have gained increasing attention for image encryption. Chaotic systems are highly sensitive to initial conditions and parameters, which makes them suitable for generating secure key streams [3]. By leveraging properties of confusion (permutation of pixel positions) and diffusion (modification of pixel values), chaos-based image encryption schemes can achieve high levels of unpredictability and resistance against brute-force, statistical, and differential attacks. Moreover, combining chaos with evolutionary computation techniques such as Genetic Algorithms (GA) provides further adaptability and robustness in encryption design.

This work focuses specifically on grayscale image encryption using a Secure and Compound three-dimensional Chaos-based Image Encryption (SCIE) scheme. The proposed approach integrates chaotic maps with genetic operators—such as arithmetic crossover, multipoint crossover, and mutation—to enhance both confusion and diffusion processes [4]. Performance evaluation metrics, including Unified Average Change Intensity (UACI), Number of Pixels Change Rate (NPCR), histogram uniformity, correlation coefficients, and entropy, are employed to validate the scheme's effectiveness. The ultimate objective is to ensure secure transmission of real-time image data, thereby addressing the growing demand for confidentiality in multimedia communications.

2. Related Works

The growing importance of multimedia security has motivated researchers to propose various cryptographic solutions tailored for image protection. Traditional symmetric and asymmetric encryption schemes such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), RSA, and International Data Encryption Algorithm (IDEA) have been widely employed for securing digital information (Zhang et al., [5]). However, their direct application to images often leads to inefficiency due to high computational overhead and limited adaptability to the structural properties of images. Large storage requirements, redundancy among neighboring pixels, and the demand for real-time communication necessitate specialized encryption techniques.

Classical cryptographic algorithms operate effectively for small-scale textual data but fail to achieve efficiency and security when applied to images. AES and DES, for example, employ substitution–permutation networks and key-based transformations to provide confidentiality. While secure in principle, these algorithms incur significant computational costs when encrypting large multimedia files, making them unsuitable for real-time image transmission (Civelek et al., [6]). Similarly, RSA, being an asymmetric encryption technique, ensures robust security but is computationally intensive for large data blocks.

To overcome these challenges, researchers have investigated the use of chaotic systems for cryptographic purposes. Chaotic maps exhibit ergodicity, deterministic randomness, and sensitivity to initial conditions, making them highly effective for generating pseudorandom sequences. Several low- and high-dimensional chaotic maps have been proposed for image encryption. For example, Pareek et al. [7] explored 1D and 2D chaotic maps for substitution–diffusion processes, while Zhen et al.[8] extended this concept to multi-dimensional chaotic systems. However, the limitation of conventional chaos-based methods lies in their key generation complexity and susceptibility to certain cryptanalytic attacks if not properly designed.

Evolutionary computation techniques, particularly Genetic Algorithms (GAs), have been increasingly utilized to enhance encryption processes. GAs mimic the natural selection process through operators such as crossover, mutation, and selection, allowing optimization of key generation and permutation patterns. Jalesh and Nirmala [9] emphasized the role of arithmetic crossover in Differential Evolution frameworks, demonstrating improved efficiency in cryptographic applications. Similarly, Das et al. [10] introduced a knight-move-based GA encryption model for securing document images, leveraging chessboard-inspired pixel selection to improve security.

Fister et al. [11] proposed a GA-assisted grayscale image watermarking method based on Discrete Cosine Transform (DCT), though its vulnerability to rotation and translation attacks highlighted the need for more resilient designs. Yadav et al. [12] suggested a hash-key hybrid encryption mechanism integrating chaotic systems and GA operators, achieving strong encryption with a single encryption round. Zhao et al. [13] further enhanced this approach using hyper-chaotic recombination strategies, providing efficient and scalable encryption processes.

To further improve encryption resilience, researchers have proposed hybrid approaches that combine chaos-based key streams with GA-inspired operators. Guesmi et al. [14] designed a ring crossover-based GA integrated with diffusion processes to strengthen resistance against brute-force attacks. Similarly, Wang and Zhang [15] applied DNA sequencing in conjunction with chaotic maps and GAs, achieving superior resistance to statistical and chosen-plaintext attacks. More recent works by Grulkowski et al. [16] introduced multi-objective evolutionary models that optimize both Quality of Service (QoS) and encryption security in cloud environments, extending the applicability of these techniques.

While numerous studies have explored image encryption using chaos and evolutionary algorithms, several limitations persist. Many approaches face challenges related to high computational cost, key management complexity, or insufficient resistance against differential attacks [17]. In particular, existing schemes often fail to balance high security with real-time performance, especially in applications such as medical image transmission, satellite data protection, and secure surveillance. Moreover, most prior works have focused on low-dimensional chaotic systems, which may not provide sufficient key space and randomness to resist modern cryptanalytic techniques.

To address these gaps, the present work proposes the Secure and Compound Image Encryption (SCIE) scheme. This approach integrates a three-dimensional Compound Sine–ICMIC (CSI) chaotic map with novel compound crossover and mutation operators. By combining the strengths of chaos theory and genetic algorithms, the SCIE method ensures both strong security and practical efficiency. Key advantages include enhanced randomness, large key space, improved resistance against statistical attacks, and reduced encryption time.

3. Methodology

A compound three-dimensional chaos-based image encryption scheme is developed by employing hybrid genetic operators to generate encrypted images. In the first stage, an arithmetic crossover operator is applied to produce two new offspring images. These offspring are then decomposed into multiple bit-planes. In the second stage, the resulting bit-planes are permuted using a multipoint crossover operation. A compound image is subsequently formed by combining the crossover results to generate an intermediate encrypted image.

Following this, a set of hybrid mutation operators is applied. Initially, a boundary transformation is employed, which replaces array elements from the beginning to the end. Next, a non-uniform mutation is introduced, where pixel modifications occur in a row-wise, column-wise, or diagonal manner. Finally, a uniform mutation is performed, in which pixel values are altered through a circular shift mechanism.

To further strengthen the encryption process, the key stream is generated using a three-dimensional Compound Sine–ICMIC (CSI) chaotic map, which ensures high randomness and sensitivity to initial conditions. The final encrypted image is obtained by integrating the outcomes of the hybrid crossover and mutation operations. The overall architecture of the proposed encryption framework is illustrated in Figure 1.

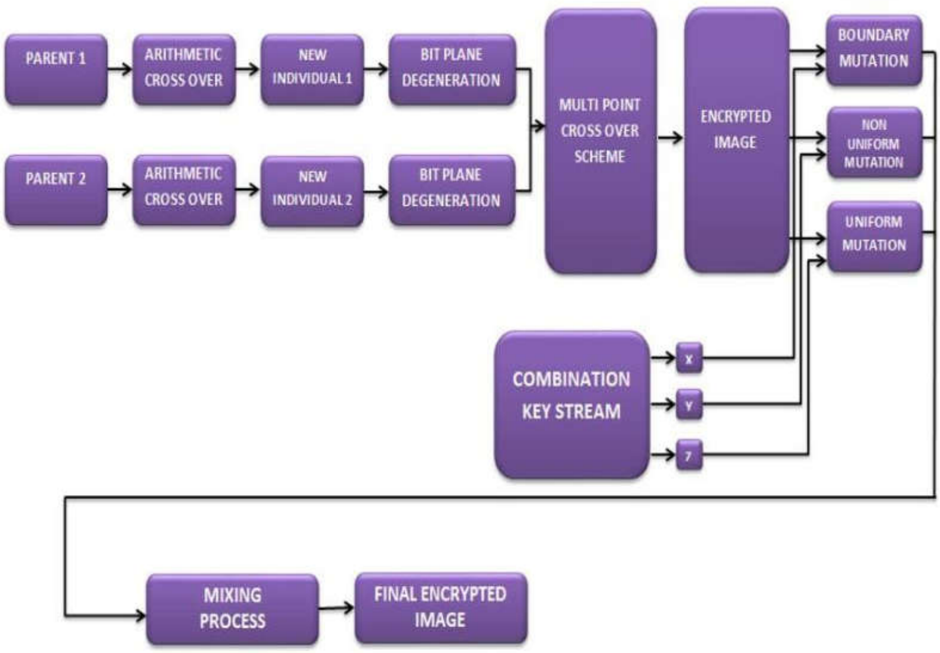

Figure 1 Instrumentality Designing of SCIE Encryption Algorithm

3.1 Arithmetic Crossover

Arithmetic crossover operation is carried out between parent 1 and parent 2

$$N1 = a1 * parent1 + (1 - a1)\, parent2 \qquad (1)$$

$$N2 = a2 * parent2 + (1 + a1)\, parent1 \qquad (2)$$

The arithmetic crossover operation is carried out using Equations (1) and (2)**.** In this process, the parameters a1 and a2 represent random variables that determine the contribution of each parent in generating the offspring. Two new individuals, denoted as N1 and N2, are produced by combining the characteristics of *Parent 1* and *Parent 2*. These offspring subsequently assume the role of parents in the next iteration, thereby facilitating the generation of successive sequences through repeated crossover operations.

3.2 Bit Plane Degeneration

This technique employs two binary bit-plane decomposition strategies for encryption. In a grayscale image, each pixel intensity value ranges from 0 to 255, which can be represented as an 8-bit binary sequence. Through bit-plane decomposition, a grayscale image can be separated into eight binary images, where the higher-order bit planes correspond to the Most Significant Bits (MSB) and the lower-order bit planes correspond to the Least Significant Bits (LSB) of the original image. In the initial stage of the proposed scheme, the plain image is decomposed into its eight constituent bit planes, forming the basis for subsequent encryption operations.

In the second stage, the bit planes are randomly divided into two groups. For instance, the higher four bit planes may be grouped together as one set, while the lower four bit planes form the second set. These two groups are then rearranged into binary sequences, where the elements of each bit plane are organized sequentially from left to right and from the higher-order planes to the lower-order planes. The resulting sequences are considered as two new parent images, denoted by N1 and N2. Subsequently, bit-plane decomposition is reapplied to these newly generated parent images, enabling further iterations of the encryption process.

3.3 **Multipoint Crossover**

The multipoint crossover is a generalization of the single-point crossover, where instead of a single cut-point, multiple crossover positions are randomly selected. In this process, the original image is first decomposed into bit planes, after which the bit positions are rearranged to generate a second bit-plane-decomposed image. The multipoint crossover operation is then applied to both parent images, N1 and N2, by interchanging their bit positions at the selected crossover points. Specifically, the bit positions of the first image are replaced with the corresponding positions from the second image, and vice versa, based on the maximum number of crossover points chosen. This operation increases randomness and enhances the diffusion property of the encryption scheme by ensuring stronger mixing between the two images.

3.4 Compound Crossover Bit Planes

Compound the bit planes after multipoint crossover operation of N1 and N2. To get the images from MSB to LSB position. Finally get an encrypted image. New encrypted image is known as child.

3.5 Mutation

The mutation operation is applied to the population after the crossover process to prevent premature convergence and to ensure that the population does not collapse into a local optimum of the optimization problem. Mutation introduces random variations in the offspring that are not directly inherited from their parents, thereby maintaining genetic diversity within the population. In genetic representation, mutation alters one or more bits in a chromosome. For instance, the binary string 000001000000010000000100 may undergo mutation at the second position, resulting in the new string 010001000100010001000100.

In the proposed encryption algorithm, a hybrid mutation technique is employed, which combines three types of mutations: boundary transformation, non-uniform mutation, and uniform mutation. This hybrid approach enhances the unpredictability of pixel modification and contributes to stronger diffusion properties in the encrypted image.

A. Boundary Mutation: This mutation replaces the array elements from top to bottom, effectively transforming the boundary positions of the image. Such replacement redistributes pixel intensity values along the image boundaries, ensuring that the edge information does not remain static during encryption.

B. Non-Uniform Mutation: In this operation, pixel values are modified in a non-uniform manner, either row-wise, column-wise, or diagonally. The degree of mutation may vary depending on the position of the pixel, which increases randomness across different image regions. This process helps in disrupting the strong correlation among neighboring pixels, a common characteristic of natural images.

C. Uniform Mutation: This mutation alters pixel positions through a circular shift mechanism. Each pixel is replaced by another pixel located at a uniformly shifted position, thereby distributing intensity values evenly throughout the image. This operation strengthens the confusion property of the encryption algorithm by ensuring that pixel values are diffused across the entire image space.

Finally, the results of these hybrid mutation operations are logically combined with a 3D Compound Sine–ICMIC (CSI) chaotic key stream, resulting in the generation of the final encrypted image. This integration guarantees both high-level security and robust resistance against statistical and differential attacks.

3.6 Concerted Key Flow

3.6.1 Sine map

The **sine map** is derived from the sine function by normalizing its inputs to the range [0,1]. In this formulation, the sine function accepts inputs within the interval [0,π], while its outputs are mapped to the range [0,1]. The sine map is mathematically defined as follows:

$$x_{n+1}=\mu \sin(\pi x_n), x_n \in [0,1],\ \mu \in [0,1] \qquad (3)$$

where x_n represents the state at iteration n_1, and μ is the control parameter that influences the chaotic behavior of the map.

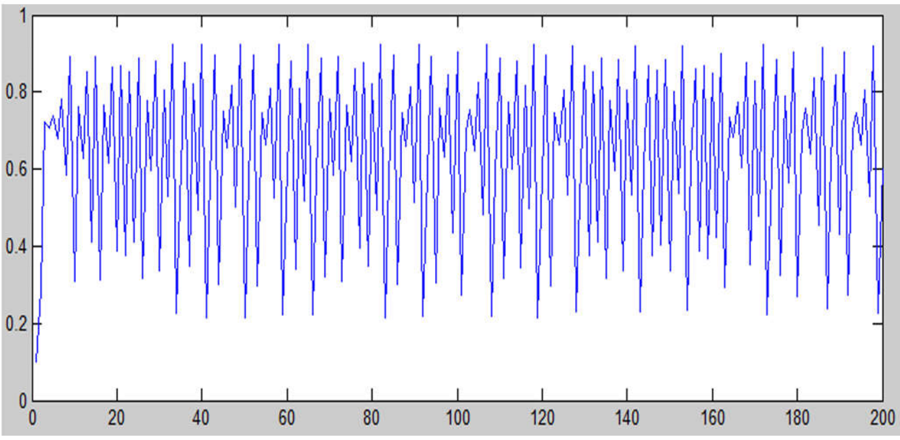

Figure 2 Sine map with 500 iterations

3.6.2 3-D Sine Map

Chaotic maps are highly sensitive to initial conditions, which is one of their fundamental characteristics that makes them unpredictable and complex to model. In such systems, even a slight variation in the initial state can result in a significantly different sequence of values generated by the iterative function. This property, often referred to as the butterfly effect, ensures that chaotic maps are well-suited for cryptographic applications, as they provide randomness and resistance against prediction-based attacks.

The one-dimensional (1D) sine map can be extended into **a three-dimensional (3D) form** to further enhance randomness, enlarge the key space, and strengthen encryption security. The 3D sine map is defined as follows:

$$x_{n+1}=\mu \sin (\pi y_n) \quad (4)$$

$$y_{n+1}=\mu \sin (\pi z_n) \quad (5)$$

$$z_{n+1}=\mu \sin (\pi x_n) \quad (6)$$

where $(x_n,y_n,z_n)\in[0,1]$ represent the states of the system at iteration n_1, and μ is the control parameter that governs the chaotic behavior.

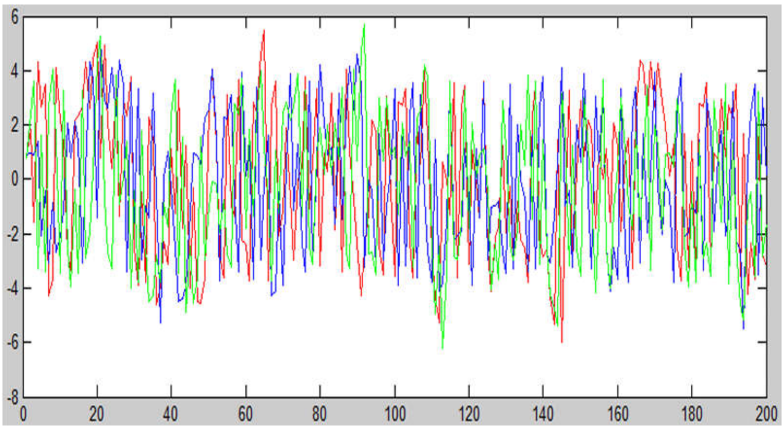

Figure 3 3D-Sine map with 500 iterations

This nonlinear system presents disorderly conduct when its parameters are esteemed in the range 3.46< A < 45.13, 0< b < 0.022, 0< a < 0.015 where x(0), y(0) and z(0) are in [0,1].

3.6.3 ICMIC Map

The Iterative Chaotic Map with Infinite Collapses (ICMIC) characterizes chaotic behavior within the interval [−1,1]. The ICMIC map is mathematically formulated as follows:

$$x_{n+1}=f(x_n),x_n\in[-1,1] \quad (7)$$

where x_n represents the state at iteration n, and the function f(·) is designed to exhibit strong sensitivity to initial conditions, high ergodicity, and complex chaotic dynamics. These properties make ICMIC particularly suitable for cryptographic applications, as it can generate highly unpredictable key streams for image encryption.

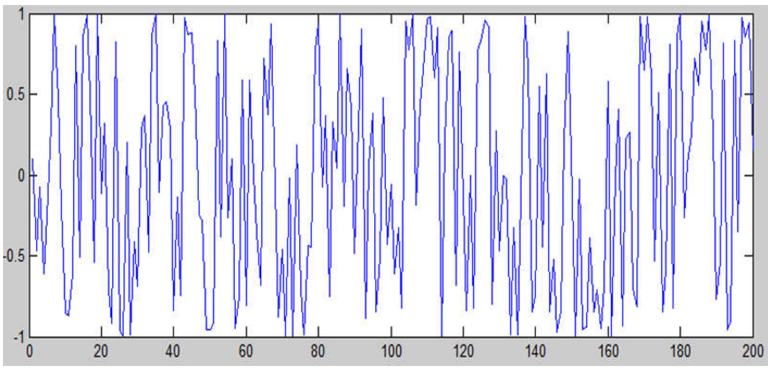

Figure.4 ICMIC map with 500 iterations

3.7 Proposed SCIE Encryption Algorithm

Step 1 - Initialize the input images

Step 2 - To apply arithmetic crossover for parent1 and parent

Step 3 - New images named 'N1' and 'N2'

Step 4 - Degenerate the bit planes of input images 'N1' and 'N2'

Step 5 - To change bit set position by using multipoint crossover to get the ciphered image

Step 6 - 3-D CSI map is used to generate secret key.

Step 7 - To apply the hybrid mutation with combined key stream

Step 8 - Mixing the mutation process to get final encrypted output

Step 9 - Calculate the NPCR, UACI, entropy, correlation coefficient.

The proposed decryption algorithm is designed as the inverse process of the Secure and Compound 3-D Chaos-based Image Encryption (SCIE) scheme. It systematically reverses each stage of the encryption process to recover the original image. The main steps of the decryption procedure include:

1. Inverse Mixing Process – Reverses the logical operations combining the key stream with the encrypted image.
2. Inverse Hybrid Mutation – Reverts the hybrid mutation operations, including boundary, non-uniform, and uniform mutations, applied during encryption.
3. Inverse Hybrid Multipoint Crossover – Restores the original pixel arrangements by reversing the multipoint crossover operation.
4. Inverse Bit-Plane Decomposition – Reassembles the bit planes into the original grayscale image.
5. Inverse Arithmetic Crossover – Recovers the original parent images from the offspring generated during the encryption stage.

The flow of the proposed decryption algorithm is illustrated in Figure 7, which provides a schematic overview of the inverse operations applied sequentially to reconstruct the plaintext image.

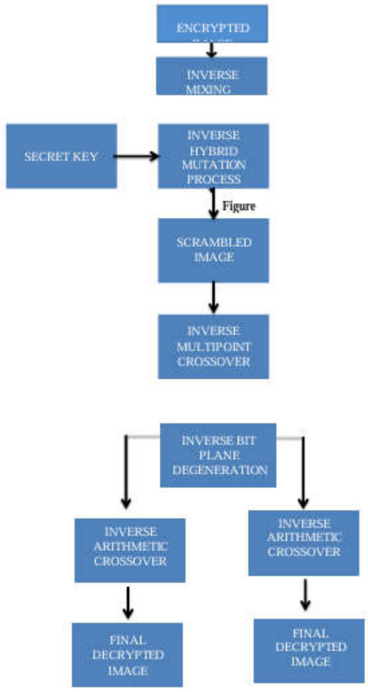

Figure 5 Square Chart of SAIE Decryption Algorithm

The decrypted image is obtained by sequentially processing the encrypted image through the inverse operations of the encryption scheme, including the inverse mixing process, inverse hybrid mutation, inverse hybrid multipoint crossover, inverse bit-plane decomposition, and inverse arithmetic crossover. This systematic reversal ensures accurate reconstruction of the original image from its encrypted form.

4. Experimental Results

The performance evaluation of the proposed encryption scheme is presented. The assessment includes histogram analysis, correlation coefficient calculation, entropy measurement, and differential analysis to examine the effectiveness and security of the algorithm. For experimental validation, approximately 200 different grayscale images of size 256×256256 \times 256256×256 pixels with 8-bit depth were tested to ensure statistical reliability and robustness of the results.

4.1 Encrypted Results

The proposed algorithm is capable of effectively combining two grayscale images into a single encrypted image. Figure 5 illustrates the results, showing the input grayscale images along with their corresponding encrypted and decrypted outputs. This demonstrates the algorithm's ability to securely encrypt multiple images while ensuring accurate reconstruction during decryption.

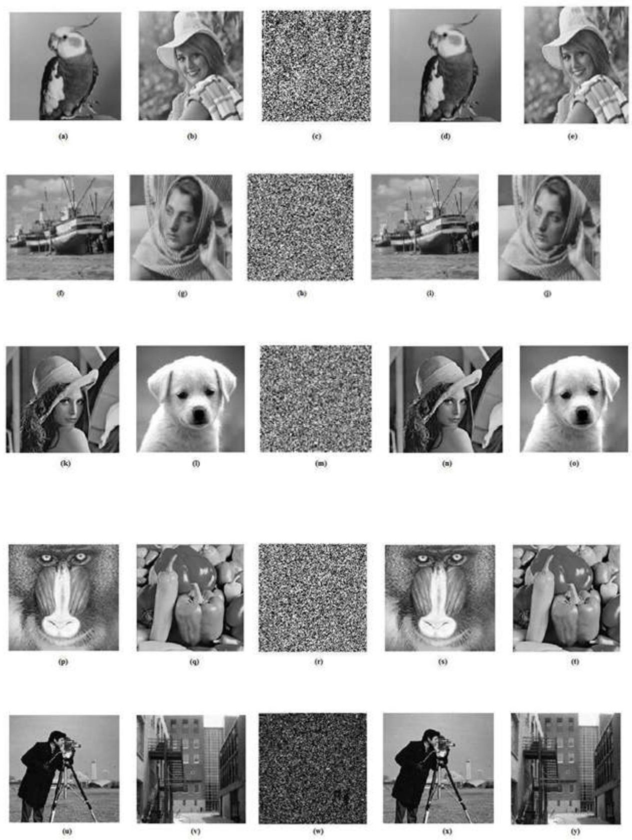

Figure 6 Input and Encrypted Images (a) Bird (b) Elaine (c) Encrypted image (d-e) Decrypted image ; Input images (f) Boat (g) Barbara (h) Encrypted image (i-j) Decrypted image; Input images (k) Lena (l)Puppy (m) Encrypted image (n-o) Decrypted image; Input images (p) Baboon (q) Peppers (r) Encrypted image (s-t) Decrypted image; Input images (u) Cameraman (v) Building (w) Encrypted Image (x-y) Decrypted Image

4.2 Statistical Analysis

4.2.1 Histogram Analysis

A histogram represents the distribution of pixel intensity values within an image. A robust encryption scheme should produce an encrypted image whose histogram is uniformly distributed, thereby resisting statistical attacks. In the proposed algorithm, the pixel intensity values of the cipher image are spread consistently across the full range [0,255], which is markedly different from the distribution of the original image.

Figure 6 presents the histogram analysis of both the original and encrypted images. It clearly illustrates that the encrypted image exhibits a uniform distribution, indicating that the original image's statistical properties are effectively concealed. Consequently, the proposed encryption system provides a higher level of security compared to conventional methods.

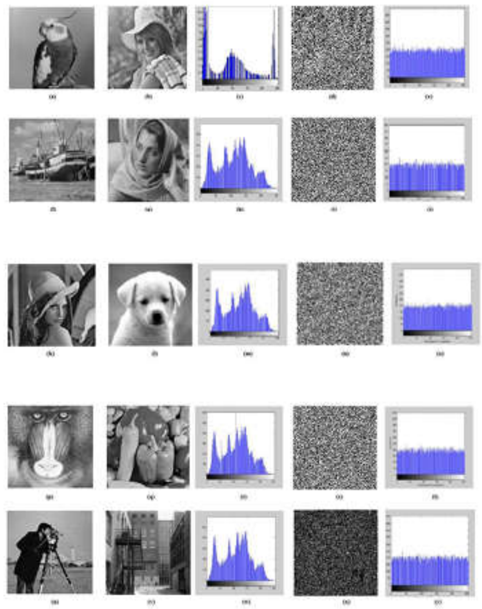

Figure 7 Histogram of Original Images and Encrypted Images (a, b and c) Input Images and its Histogram; (d and e) Encrypted Image and its histogram ; (f , g and h) Input 73 Images and its Histogram; (i and j) Encrypted Image its histogram; (k , l and m) Input Images and its Histogram; (n and o) Encrypted Image its histogram; (p ,q and r) Input Images and its Histogram; (s and t) Encrypted Image its histogram ;(u , v and w) Input Images and its Histogram; (x and y) Encrypted Image its histogram

4.2.2 Correlation Analysis

In a typical grayscale image, neighboring pixels exhibit a high correlation in the horizontal, vertical, and diagonal directions. An effective encryption algorithm must reduce these correlations so that the correlation coefficients of adjacent pixels in the encrypted image are sufficiently low, thereby resisting statistical attacks.

To analyze this property, 4000 pairs of adjacent pixels in each direction were randomly selected from both the original and encrypted images. The results indicate that while neighboring pixels in the original image are highly correlated, the corresponding pixels in the encrypted image are almost uncorrelated, demonstrating the algorithm's strong diffusion capability. The correlation coefficients are computed using the following formula:

$$r_{xy}=Cov(x,y)/D(x)\cdot D(y) \quad (8)$$

where Cov(x,y) is the covariance of adjacent pixels, and D(x), D(y) are the variances of the pixel values.

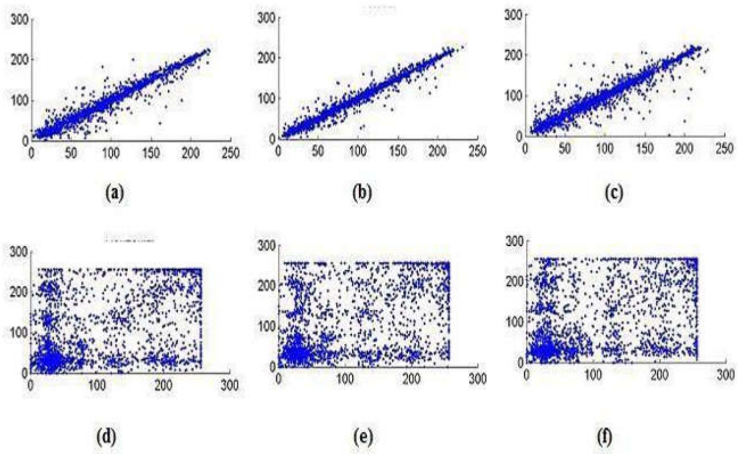

Figure 8 Horizontal, vertical and diagonal pixel Distribution of Original and Encrypted Images (a) horizontal, (b) vertical, (c) diagonal and the corresponding Encrypted Image (d) horizontal, (e) vertical, (f) diagonal

Table 1 presents the obtained results for both the plain images (PI) and cipher images (CI), highlighting the performance of the proposed encryption method in resisting statistical attacks. The results demonstrate that the correlation coefficients of adjacent pixels in the encrypted images are significantly lower than those in the original images, indicating strong decorrelation. Furthermore, a comparison with recent algorithms shows that the proposed method achieves better reduction in correlation coefficients, outperforming earlier encryption techniques in terms of resisting statistical attacks.

Table 1 Correlation analysis of various Test Images

Algorithm & Image Name		Image Size	Horizontal Correlation	Vertical Correlation	Diagonal correlation
This work	PI	256x256	0.9909	0.9846	0.9769
	CI		-0.0002	0.0001	-0.0015
Pareek & Patidar (2016)	PI	256x256	0.9719	0.9546	0.9669
	CI		-0.0013	0.0074	-0.0051
Ravichandran &	PI	256x256	0.9709	0.9843	0.9569

Padhmapriya 2016	CI		0.0214	0.0465	-0.0090
Zhen *et al.* (2016)	PI	256x256	0.9701	0.9844	0.9564
	CI		0.0011	-0.0071	-0.0005
Wang *et al.* (2015)	PI	256x256	0.9749	0.9816	0.9619
	CI		-0.0006	-0.0083	0.0056
Wu *et al.* (2015)	PI	256x256	0.9819	0.9706	0.9644
	CI		-0.0049	0.0142	-0.0155
Premkumar & Anand (2016)	PI	256x256	0.9640	0.9744	0.9485
	CI		0.0059	0.0048	0.0028

4.2.3 Information Entropy Analysis

Entropy is a measure that quantifies the degree of randomness and uncertainty in an image. It is commonly used to evaluate the uniformity of pixel intensity distribution within the image. For an 8-bit grayscale image, the maximum possible entropy is 8, indicating the highest level of unpredictability.

To calculate the entropy, the following formula is used (Pareek & Patidar, 2016):

$$H = -\sum_{i=0}^{255} P(i)\log_2 P(i) \quad (9)$$

where P(i) denotes the probability of the i-th gray level in the image. According to Equation (9), a uniform pixel distribution yields higher entropy values, reflecting better randomness and enhanced resistance against statistical attacks.

In Equation (9), mim_imi denotes the gray level, and P(mi) represents the probability of occurrence of that gray level in the image. Figure 8 illustrates the entropy analysis for a set of standard grayscale images of different sizes. The results indicate that the proposed encryption algorithm achieves high entropy values across all test images, with the bird image exhibiting the highest entropy. This demonstrates that the encrypted images possess a nearly uniform pixel distribution, confirming the effectiveness of the proposed method in maximizing randomness and resisting statistical attacks.

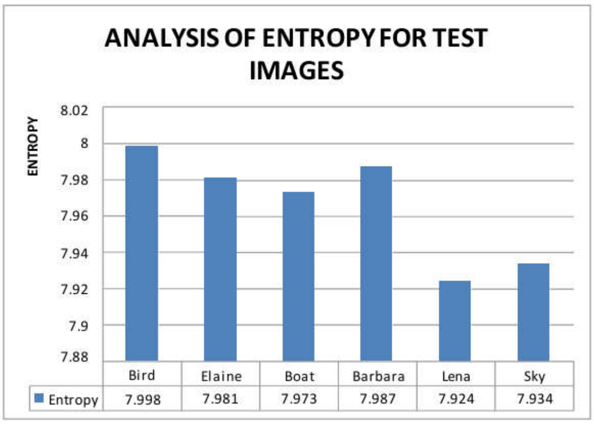

Figure 9 Analysis of Entropy for various Test Images

Table 2 NPCR analysis for various Test Images

Test Image	NPCR		
	Min	Max	Average
Bird	99.6874	99.8914	99.7894
Elaine	99.6741	99.8438	99.7590
Boat	99.6875	99.8752	99.7814
Barbara	99.6291	99.8651	99.7471
Lena	99.6341	99.7651	99.7453
Sky	99.6741	99.8738	99.7594

Table 3 UACI analysis of various Test Images

Test Image	UACI		
	Min	Max	Average
Bird	33.3674	33.5914	33.4794
Elaine	33.3741	33.4438	33.4091
Boat	33.3875	33.6752	33.5314
Barbara	33.3291	33.5651	33.4471
Lena	33.3441	33.5432	33.4021
Sky	33.3012	33.4048	33.5246

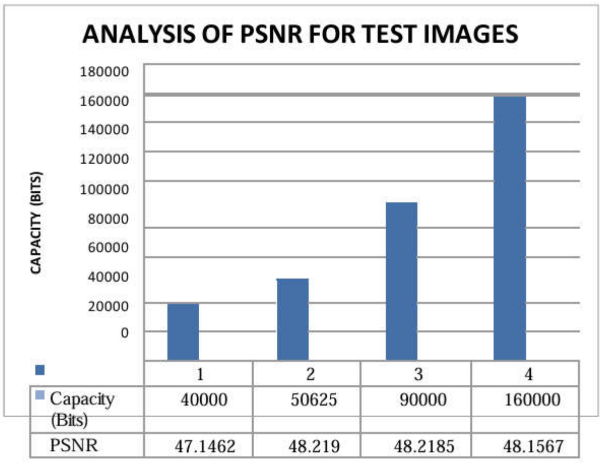

Figure 10 Analysis of PSNR for various Test Images

4.2.4 ENCRYPTION TIME

To evaluate the computational efficiency of the proposed algorithm, simulation experiments were conducted in the same MATLAB environment as reported in previous studies (Zhou et al., 2014; Wang et al., 2015; Wu et al., 2015; Pareek & Patidar, 2016; Ravichandran & Padhmapriya, 2016; Zhen et al., 2016; Premkumar & Anand, 2016) using a grayscale bird image of size 256×256256 \times 256256×256 pixels. The simulation results indicate that the average processing speed is 0.4869 MB/s for encryption and 0.6052 MB/s for decryption**.**

Figure 10 presents the execution speed comparison**,** showing that the proposed cryptosystem achieves the fastest processing rate among the tested methods while maintaining a high level of security. This demonstrates that the algorithm is not only secure but also computationally efficient for real-time image encryption applications**.**

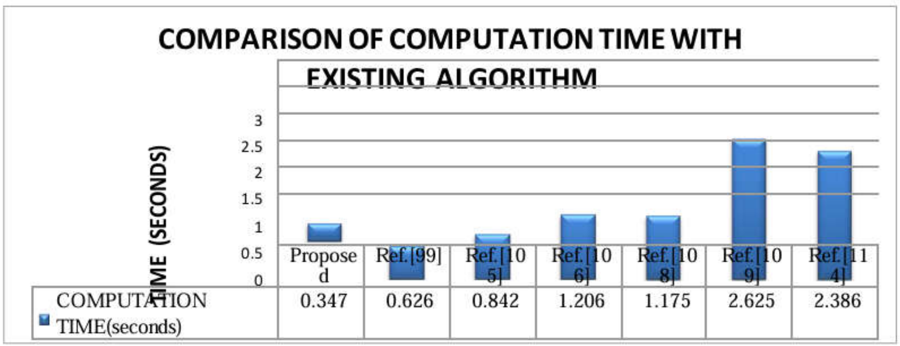

Figure 11 Analysis of Time for various Test Images

4.2.5 Comparison

The proposed cryptosystem is compared with existing image encryption schemes based on several performance metrics, as summarized in Tables 4.1–4.4. Although the key space of the proposed system is not the largest, it is sufficiently large to resist brute-force attacks effectively. The correlation coefficients for adjacent pixels in the encrypted images are closer to zero compared to other methods, indicating that the proposed cryptosystem is more resilient against statistical attacks**.**

The information entropy achieved by the proposed method is higher than that reported in previous studies, reflecting better randomness in the encrypted images. From Tables 3 and 4, the Number of Pixels Change Rate and Unified Average Changing Intensity values of the proposed cryptosystem are close to the ideal values, demonstrating strong resistance against known-plaintext and chosen-plaintext attacks**.**

Table 4 presents a detailed comparison between existing systems and the proposed scheme, validating the feasibility, security, and effectiveness of the proposed image cryptosystem.

Table 4 Parameter Comparison with the Existing Methods

Algorithm	**Robustness analysis**	**Informationentropy**	**NPCR %**	**UACI %**	**PSNR dB**	**Correlation coefficient**	**Speed Sec**
Pareek & Patidar (2016)	No	7.9975	99.5911	33.465	34.62	0.000356	2.4249
Ravichandran & Padhmapriya (2016)	No	7.9969	0.0046	33.400	40.14	-0.012652	2.4092
Zhen *et al.* (2016)	No	7.9993	99.6000	33.479	42.26	0.456253	0.1051
Wang *et al.* (2015)	No	7.9970	99.5911	33.465	41.39	0.068745	3.1733
Zhou *et al.* (2014)	Yes	7.9997	99.6033	33.355	43.12	0.007548	0.9871
Premkumar & Anand (2016)	Yes	7.9967	99.9911	36.7350	51.27	-0.00002	0.459
Proposed	Yes	7.9998	99.9914	33.54	48.16	-0.000041	0.4869

5. Conclusions

This paper introduced a Secure and Compound 3D Chaos-Based Image Encryption (SCIE) scheme that combines chaotic systems with genetic operators to address the shortcomings of traditional and chaos-only encryption approaches. By integrating arithmetic and multipoint crossover with hybrid mutation techniques, the proposed scheme achieves enhanced confusion and diffusion properties, ensuring robust protection against brute-force, statistical, and differential attacks. Experimental results confirm that the encrypted images exhibit uniform histograms, high entropy, low correlation coefficients, and optimal NPCR and UACI values, indicating strong security performance. Furthermore, the scheme demonstrates computational efficiency, achieving faster encryption and decryption speeds compared to conventional methods. These qualities make SCIE highly suitable for real-time secure image transmission in sensitive domains such as medical imaging, satellite communications, and defense applications. Future work may focus on extending the scheme to color images, video encryption, and resource-constrained environments such as IoT devices to further broaden its applicability.

References

[1].Admass, W.S., Munaye, Y.Y. and Diro, A.A. Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, p.100031.

[2] Aslan, Ömer & Aktuğ, Semih & Ozkan, Merve & Yılmaz, Abdullah & Akin, Erdal. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics. 12. 1-42. 10.3390/electronics12061333.

[3] Jolfaei, Alireza & Mirghadri, Abdolrasoul. (2010). An image encryption approach using chaos and stream cipher. Journal of Theoretical and Applied Information Technology. 19. 117-125.

[4] Roy, V., 2021. An improved image encryption consuming fusion transmutation and edge operator. *Journal of Cybersecurity and Information Management*, *8*(1), pp.42-52.

[5] Zhang, L., Liu, N., Ma, X. and Jiang, L., 2013. The transcriptional control machinery as well as the cell wall integrity and its regulation are involved in the detoxification of the organic

solvent dimethyl sulfoxide in Saccharomyces cerevisiae. *FEMS yeast research*, *13*(2), pp.200-218.

[6] Civelek, M.E., İnce, H. and Karabulut, A.T., 2016. The mediator roles of attitude toward the web site and user satisfaction on the effect of system quality on net benefit: A structural equation model on web site success.

[7] Patidar, Vinod & Pareek, Narendra & Sud, K.K.. (2009). A novel image cipher based on chaotic standard and logistic maps. Proceedings of The Fourth National Conference on Nonlinear Systems and Dynamics (NCNSD).

[8] Zheng X, Boyer L, Jin M, Mertens J, Kim Y, Ma L, Ma L, Hamm M, Gage FH, Hunter T. Metabolic reprogramming during neuronal differentiation from aerobic glycolysis to neuronal oxidative phosphorylation. Elife. 2016 Jun 10;5:e13374. doi: 10.7554/eLife.13374. PMID: 27282387; PMCID: PMC4963198.

[9] Jalesh Kumar, S. Nirmala,A novel and efficient method based on knight moves for securing the information contents of images — A parallel approach, Journal of Information Security and Applications,Volume 30,2016,Pages 105-117,ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2016.08.004.

[10] Babu, M.A., 2014. Logical development of Vogel's approximation method (LD-VAM): an approach to find basic feasible solution of transportation problem.

[11] Iztok Fister, Aleksandra Tepeh, Iztok Fister Jr., Epistatic arithmetic crossover based on Cartesian graph product in ensemble differential evolution, Applied Mathematics and Computation, Volume 283,2016,Pages 181-194, ISSN 0096-3003, https://doi.org/10.1016/j.amc.2016.02.034.

[12] Yadav, A., Dhole, K. and Sinha, H., 2016. Genetic regulation of phenotypic plasticity and canalisation in yeast growth. *PloS one*, *11*(9), p.e0162326.

[13] Zhao, H., Huang, H. and Lin, S., 2016. Chemical approaches to angiogenesis in development and regeneration. In *Methods in cell biology* (Vol. 134, pp. 369-376). Academic Press.

[14] Khaled Guesmi, Samir Saadi, Ilyes Abid, Zied Ftiti, Portfolio diversification with virtual currency: Evidence from bitcoin, International Review of Financial Analysis, Volume 63, 2019, Pages 431-437, ISSN 1057-5219, https://doi.org/10.1016/j.irfa.2018.03.004.

[15] Wang, F. and Zhang, H. (2016) An Empirical Study on the Influencing Factors of University Librarians' Psychological Capital. Shandong Library Journal, No. 4, 10-16.

[16] Grulkowski, Ireneusz. (2018). Wang et al-2018-Scientific Reports. Scientific Reports. 8. 7281.

[17] Jie Wang, Lingfeng Liu, Mengfei Xu, Xiangjun Li, A novel content-selected image encryption algorithm based on the LS chaotic model, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 10, Part A, 2022, Pages 8245-8259, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.08.007.