

# Image Encryption Based on Chen Chaotic System, OpenSSL S-Box and the Fibonacci Q-Matrix

Rana Lotfy Mohamed Gabr 


Faculty of MET

German University in Cairo

Cairo, Egypt

rana.abdeltwab@student.guc.edu.eg

mohamed.gabr@ieee.org

Eyad Mamdouh Amr Aboshousha 



Physics Department

German University in Cairo

Cairo, Egypt

eyad.gaber@ieee.org

amr.aboshousha@guc.edu.eg

Wassim Alexan Dina El-Damak 


Faculty of IET

German University in Cairo

Cairo, Egypt

wassim.alexan@ieee.org

dina.eldamak@guc.edu.eg

Abdallah Fathy 

Department of Electronic Engineering Technology

Faculty of Engineering Technology

ElSewedy University of Technology - Polytechnic of Egypt

Cairo, Egypt

abdallah.fathy@sut.edu.eg

Marvy Badr Monir Mansour 

Department of Electrical Engineering

Faculty of Engineering

The British University in Egypt

Cairo, Egypt

marvy.badr@bue.edu.eg

**Abstract**—This paper presents a novel image encryption algorithm that leverages the chaotic properties of the Chen system, the cryptographic strength of OpenSSL, and the mathematical robustness of the Fibonacci Q-Matrix. The proposed method begins by generating an encryption key using the Chen chaotic system, known for its sensitivity to initial conditions and complex dynamic behavior. This key is then utilized in conjunction with a substitution box (S-box) generated through OpenSSL to introduce non-linearity and diffusion into the encryption process. To further enhance security, the resulting image data undergoes a series of multiplications by a large number of Fibonacci Q-Matrices, exploiting their recursive properties for added complexity and confusion. Numerical results demonstrate the proposed algorithm's superior performance in terms of security and efficiency, making it a promising solution for safeguarding digital images against unauthorized access and cryptographic attacks. **Keywords**—Chaos Theory, Cryptography, Fibonacci Q-Matrix, Image Encryption, OpenSSL, Substitution Box (S-box).

## I. INTRODUCTION

At a time where digital imagery is ubiquitous, the significance and timeliness of robust image encryption algorithms cannot be overstated. Image encryption plays a crucial role in protecting sensitive visual data across various applications, including secure communications [1], medical imaging [2], digital forensics [3], and cloud storage [4]. Traditional encryption methods like AES, DES, and RSA, while effective for text and binary data, often fall short in handling the unique characteristics of multimedia [5]. These classical algorithms can be computationally intensive and may not adequately address the large size, redundancy, and real-time processing requirements of image files. Therefore, specialized image encryption techniques that can efficiently manage these challenges are essential to ensure the confidentiality and integrity of visual information in today's digital landscape [6].

For color image encryption, the literature shows various works that conform to Shannon's ideas of confusion and diffusion [7], specifically adoptive of chaos theory. For example, the work in [8] proposes an encryption algorithm that rotates and randomizes image pixels over stages. First, a plain image is rotated and random numbers are added to each row. Next, the Lorenz chaotic map achieves confusion, while the Fibonacci Q-Matrix (FQ-matrix) diffuses the image by multiplying each  $2 \times 2$  sub-block by  $Q^{10}$ . Another work for encryption of gray images that also utilizes the FQ-matrix in combination with hyperchaos is that of [9]. In that work, an 8D hyperchaotic system is used to scramble image pixels. While FQ-matrix is applied to change gray value of pixels for diffusion capability. In addition, the authors of [10] propose a 3-stage image cryptosystem. This system utilizes the Discrete Fourier Transform (DFT), fractional-order Chen hyperchaotic system, and DNA coding for the first encryption stage; constructed S-box for the second stage; and the Mersenne Twister pseudorandom number generator (MT PRNG) for the third stage. In [11], authors proposed an image encryption algorithm that employs discrete chaotic dynamic maps that are Henon, Circle, and Duffing maps to achieve confusion and diffusion properties of a cryptographic system. Also, their algorithm exhibits minimum encryption rounds. While in [12], the authors present a technique for constructing a substitution box (S-box) for image encryption using the multiplicative group of nonzero elements of Galois field of order 256. This S-box transforms plaintext into an encrypted format using exponential and Tinkerbell chaotic maps, sensitive to initial conditions. The study in [4] introduces a multi-layer color image cryptosystem. Each layer employs an encryption key and S-box derived from a fractional-order 4D Chen system, MT PRNG, OpenSSL PRNG, Rule 30 Cellular Automata (CA), and Intel's MKL PRNG. This

system yields a totally distorted output from any input plain image which guarantees confusion and diffusion needed for secure communications. The proposed scheme for RGB image encryption in [13] is comprised of three stages to ensure confusion and diffusion. Rule 30 CA is used to get the first encryption key in the first stage. For the second stage, a robust S-box is designed based on transformation, modular inverses, and permutation. The third stage adopts the Lorenz system to produce the second key. The work in [14] introduces a color image encryption scheme using fractals, an S-box, and hyper-chaotic dynamics. Julia fractals generate keys, while a Hilbert fractal constructs the S-box for pixel replacement. The Logistic map scrambles pixels, whereas the Chen hyper-chaotic system adjusts and selects fractal images. Finally, image pixels are encrypted with an XOR operation using fractal image pixels and previous encrypted values.

This research contributes by demonstrating as well as evidencing a smart, secure, and efficient image encryption algorithm that is well-suited for color images of sensitive nature. The paper is organized as follows. Section II introduces some preliminary mathematics that is utilized in the algorithm. Section III describes the proposed algorithm. Section IV presents the computed numerical results and provides a comparative analysis with the literature. Ultimately, the conclusions of this work, as well as suggestions for future research work are discussed in Section V.

## II. PRELIMINARY MATHEMATICAL CONSTRUCTS

### A. Chen Chaotic System

The Chen chaotic system is a 3D dynamical system known for its complex and unpredictable behavior, making it ideal for cryptographic applications. Defined by nonlinear differential equations, it exhibits sensitivity to initial conditions, leading to divergent trajectories. This unpredictability is used in encryption algorithms to generate robust keys, enhancing confusion and diffusion properties crucial for secure image and data encryption. Recently, it has been mathematically given in [15] by:

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = (c - a)x - xz + cy, \\ \dot{z} = xy - bz. \end{cases} \quad (1)$$

In this system,  $x, y$ , and  $z$  are the state quantities, and  $a > 0, b > 0$ , and  $c > 0$  are the parameters of the system. At  $a = 0.25, b = 0.3, c = 1$ , the system in (1) exhibits chaotic behavior. Figure 1 displays the system dynamics, which confirm its chaotic behavior [15].

### B. OpenSSL Encryption Key

OpenSSL is a widely-used, robust library that provides comprehensive tools and implementations for cryptographic functions, making it an excellent choice for generating S-boxes in image encryption [16]. An S-box is a fundamental component in many encryption algorithms, used to perform substitution operations that enhance security by introducing non-linearity and complexity. OpenSSL's extensive cryptographic functions allow for the generation of secure, pseudo-random numbers, and complex transformations required in the creation of S-boxes. By leveraging OpenSSL, one can ensure that the

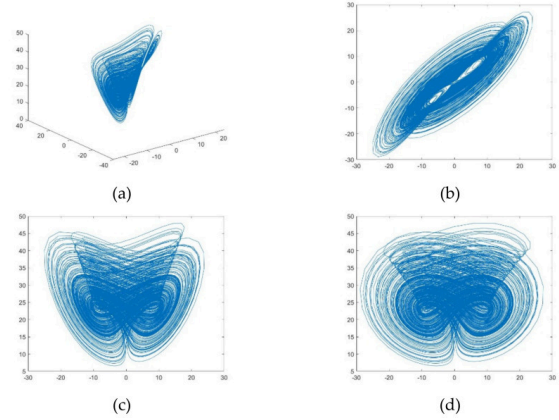


Fig. 1: Various views of the attractor for the Chen chaotic system in (1). Sub-Figure (a) gives a 3D perspective of the system. Sub-Figure (b) shows the projection of the attractor onto the  $x-y$  plane. Sub-Figure (c) displays the projection onto the  $x-z$  plane. Sub-Figure (d) depicts the projection onto the  $y-z$  plane [15].

S-boxes employed in their image encryption schemes are both secure and efficient, benefiting from the library's well-tested and optimized cryptographic algorithms. This integration helps in achieving a higher level of security in encrypted images, making them resistant to various cryptanalytic attacks.

### C. Fibonacci Q-Matrix

The Fibonacci Q-Matrix is a powerful tool in both mathematics and cryptography, particularly in the context of image encryption. The Q-Matrix, denoted as  $Q$  is defined as:

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}. \quad (2)$$

This matrix is instrumental in generating Fibonacci numbers through matrix exponentiation. For any positive integer  $n$ , the  $n$ th power of the Q-Matrix,  $Q^n$ , yields [17]:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}, \quad (3)$$

where  $F_n$  is  $n$ th Fibonacci number. This property is leveraged in image encryption algorithms to create complex, pseudo-random sequences that can be used to mask image data effectively. The recursive nature and inherent unpredictability of Fibonacci numbers when manipulated through Q-Matrix exponentiation make it a robust method for securing digital images against unauthorized access.

## III. PROPOSED ALGORITHM

### A. Steps of the Encryption Procedure

#### 1) Stage 1

- Generating a plain image then converting into 1D bit-stream  $I_{[1D]}$ .
- For a given  $Seed_{Chen}$ , a bit stream is generated from the Chen system mentioned in eq. 1 giving

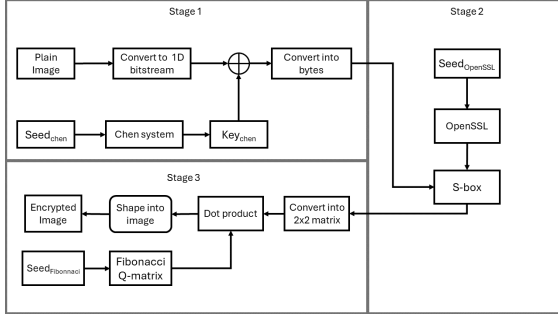


Fig. 2: The encryption procedure.

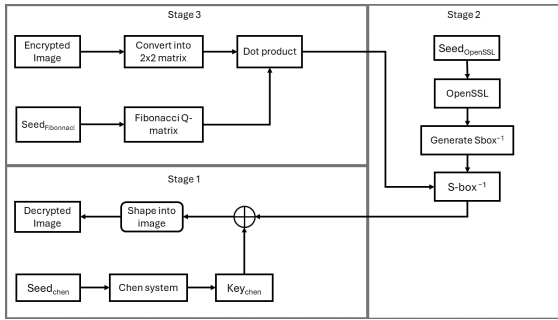


Fig. 3: The decryption procedure.

$Key_{Chen}$ , the size of the key is equivalent to the image bit-stream.

- c) After generating the key, XOR operation is performed between the image bit-stream and the key producing stage 1 encrypted image bits then converting those bits into bytes giving  $I_{[1D,Chen]}$ .

## 2) Stage 2

- a) For a given  $Seed_{OpenSSL}$ . A PRNG is generated that used for creating Sbox producing  $Sbox_{OpenSSL}$ .
- b) Then, the encrypted image bytes are subjected to  $Sbox_{OpenSSL}$  (shown in Table I) producing  $I_{[1D,Chen,SB_{OpenSSL}]}$ .

## 3) Stage 3

- a) A given  $Seed_{Fibonacci}$  is used for creating  $2 \times 2$  Fibonacci Q-matrix producing  $Key_{FibonacciQ}$ .
- b) Converting  $I_{[1D,Chen,SB_{OpenSSL}]}$  into  $2 \times 2$  matrices and dot product operation is performed with  $Key_{FibonacciQ}$  producing  $I_{[2 \times 2,Chen,SB_{OpenSSL},FibonacciQ]}$ .
- c) Finally,  $I_{[2 \times 2,Chen,SB_{OpenSSL},FibonacciQ]}$  is reshaped back into image giving encrypted image  $I'$ .

Figure 2 visually illustrates these steps.

## B. Steps of the Decryption Procedure

### 1) Stage 3

- a) The encrypted image  $I'$  is converted into  $2 \times 2$  matrices. Then, dot operation is performed with  $Key_{Fibonacci}$ . The result is then converted into 1D bytes giving  $I_{[1D,Chen,SB_{OpenSSL}]}$ .

### 2) Stage 2

- a) Inverse Sbox is generated from  $Sbox_{OpenSSL}$  giving  $Sbox'_{OpenSSL}$ .
- b) Then  $I_{[1D,Chen,SB_{OpenSSL}]}$  is subjected to  $Sbox'_{OpenSSL}$  giving  $I_{[1D,Chen]}$ .

### 3) Stage 1

- a)  $I_{[1D,Chen]}$  is converted into 1D bit-stream and XORed with  $Key_{Chen}$  giving  $I_{[1D]}$ .
- b) Finally  $I_{[1D]}$  is reshaped back giving the plain image again.

## IV. NUMERICAL RESULTS AND PERFORMANCE EVALUATION

This section showcases the computed performance evaluation metrics and how they compare to those achieved by counterpart algorithms from the literature.

Table II demonstrates the effectiveness of the proposed image encryption scheme by showcasing its application on various images. Each entry in the table displays the plain image alongside its histogram, the encrypted version of the same image with its corresponding histogram, and the decrypted image along with its histogram. The results indicate that the encryption process significantly alters the image histograms, enhancing security by obscuring the original data, while the decryption process accurately restores the original images, as evidenced by the matching histograms of the plain and decrypted images.

Table III presents a comparison of the Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) values between the proposed encryption scheme and those reported in the literature. For the Mandrill image, the proposed scheme achieves an MSE of 8283.98 and a PSNR of 8.94841 dB, slightly outperforming [4] and [10]. In the case of the Peppers image, the proposed scheme's MSE and PSNR are comparable to those in the literature, though [12] reports a higher PSNR. For the House image, the proposed scheme also demonstrates competitive performance, with MSE and PSNR values closely aligning with other studies, except for [12], which reports a higher PSNR. Overall, the proposed scheme maintains competitive image quality metrics across different images.

Table IV displays the entropy values for encrypted images using the proposed scheme and compares them with values from recent literature. The proposed scheme consistently achieves high entropy values close to the ideal value of eight, indicating strong randomness and security. For instance, the entropy for the Mandrill image is 7.99914, on par with [10] and slightly better than [4]. Similar trends are observed for the Peppers and House images, where the proposed scheme's entropy values are highly competitive, demonstrating its effectiveness in producing secure encrypted images with superior randomness compared to other methods.

Table V presents a comparison of the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) values for the proposed image encryption scheme against recent literature. The proposed scheme achieves an NPCR of 99.6302 and a UACI of 30.3828, indicating high sensitivity to pixel changes and substantial intensity variation, respectively. These values are competitive with those reported in [4], [11], [12], and [13], demon-

TABLE I: OpenSSL based S-box.

108	229	171	44	2	152	221	28	58	0	192	119	234	170	87	7
34	24	33	154	123	138	50	116	42	161	39	214	26	200	6	169
230	236	139	189	103	198	8	35	95	190	188	207	22	216	63	157
60	217	91	66	195	61	98	153	174	181	209	67	242	84	194	107
145	93	9	133	112	72	135	120	55	19	21	13	111	47	224	185
205	231	92	77	225	100	10	204	113	128	80	180	222	12	163	85
36	74	71	53	255	62	244	166	20	187	132	75	29	11	114	250
99	228	155	178	3	30	121	208	38	54	223	65	249	32	110	245
5	206	15	248	193	247	144	173	49	18	165	149	48	41	90	179
241	83	102	96	183	94	45	238	115	210	254	104	243	143	79	16
82	156	64	122	43	52	246	124	140	81	235	125	237	219	1	167
129	232	213	68	17	201	215	137	253	151	197	203	131	27	226	147
141	59	172	37	227	150	240	196	23	168	164	25	117	69	186	105
31	212	148	233	73	109	162	126	78	46	158	4	252	136	70	177
101	89	118	76	88	182	159	218	127	191	202	86	57	130	184	160
199	142	40	56	106	97	239	220	251	134	51	14	146	211	176	175

TABLE II: Implementation of the proposed image encryption scheme on different images.

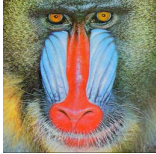
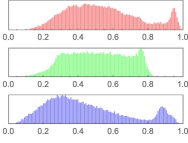
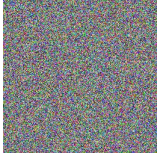
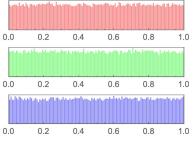
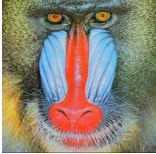
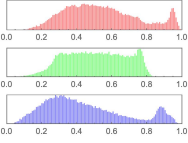

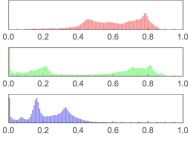

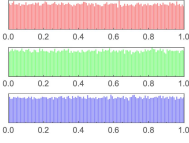

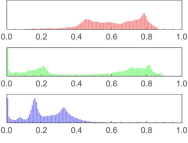
Image data	Plain image & histogram	Encrypted image & histogram	Decrypted image & histogram
Mandrill $d = 256 \times 256$	 	 	 
Peppers $d = 256 \times 256$	 	 	 

TABLE III: MSE and PSNR values comparison with the literature.

Image	Proposed Scheme		[4]		[10]		[12]	
	MSE	PSNR [dB]	MSE	PSNR [dB]	MSE	PSNR [dB]	MSE	PSNR [dB]
Mandrill	8283.98	8.94841	8320.41	8.92936	8322.19	8.92843	N/A	N/A
Peppers	10106.1	8.08496	10065.4	8.10248	10029.2	8.11813	9050	8.9455
House	8334.21	8.92216	8395.53	8.89032	8307.62	8.93604	10259	8.9931

TABLE IV: Entropy values for encrypted images comparison with recent literature.

Image	Proposed	[4]	[10]	[12]	[8]
Mandrill	7.99914	7.99866	7.99916	N/A	N/A
Peppers	7.99892	7.99834	7.99896	7.9974	7.9997
House	7.99889	7.99729	7.99897	7.9973	N/A

TABLE V: NPCR and UACI values comparison with recent literature.

Algorithm	NPCR	UACI
Proposed	99.6302	30.3828
[4]	99.5855	30.3873
[11]	99.52	26.7933
[12]	99.6692	33.5051
[13]	99.62870	30.34321

strating the effectiveness and robustness of the proposed scheme in ensuring high security through significant pixel and intensity alterations.

The co-occurrence matrices of the plain and encrypted Mandrill image, shown in Fig. 4, reveal a substantial change in texture patterns, showcasing the encryption scheme's effectiveness. The plain image's matrix displays clear and structured patterns, whereas the encrypted image's matrix appears highly randomized, indicating the successful obfuscation of spatial relationships and enhancement capability of the overall security of the encrypted image.

The DFT analysis of the plain and encrypted Peppers image, shown in Fig. 5, demonstrates a significant alteration in frequency components, indicating effective encryption. The plain image shows distinct frequency patterns, while the encrypted image exhibits a randomized frequency distribution, highlighting the scheme's success in disrupting the original image structure and ensuring data security.

A set of S-box performance evaluation metrics have been proposed in a number of research papers [18]–[21]. These are the non-linearity (NL), linear approximation probability (LAP), differential approximation probability (DAP), bit independence criterion (BIC), and strict avalanche criterion (SAC). Table VI lists their computed values for the proposed algorithm, as well as compares these values with related recent research work in the literature.

Table VII summarizes the results of a NIST analysis performed on our proposed encryption scheme, demonstrating its robust security features. The results indicate that the scheme meets the stringent randomness criteria set by NIST, with all tests successfully passed. This underscores the reliability and effectiveness of our encryption method in ensuring data security.

## V. CONCLUSIONS AND FUTURE WORKS

In this paper, a novel image encryption algorithm is developed and evaluated, leveraging the chaotic properties of the Chen system, the cryptographic capabilities of OpenSSL, and the mathematical strength of the Fibonacci Q-Matrix. Exceptional performance in security and effi-

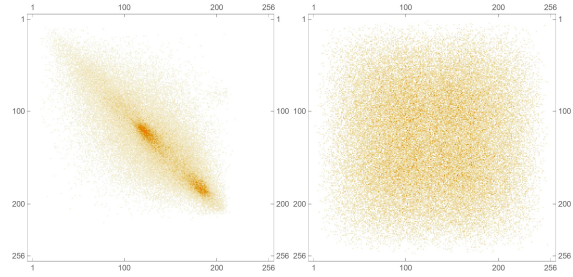


Fig. 4: Co-occurrence matrices of plain and encrypted Mandrill image.

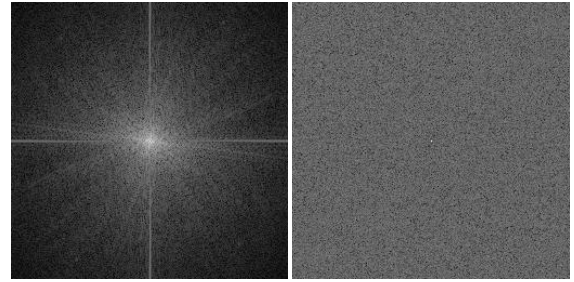


Fig. 5: DFT of the plain and encrypted Peppers image.

ciency is demonstrated. Key contributions include the use of the Chen chaotic system for key generation, enhancing security through high sensitivity to initial conditions and complex dynamic behavior. An S-box generated via OpenSSL introduces non-linearity and diffusion, while Fibonacci Q-Matrices add complexity through their recursive properties. Numerical results validate the algorithm's effectiveness, making it suitable for protecting digital images against unauthorized access and cryptographic attacks.

Future works could focus on enhancing the algorithm's scalability with larger images and higher resolutions, optimizing the overall performance to reduce computational overhead, and exploring hardware implementations on FPGAs (in a similar manner to the work in [23]) or GPUs (in a similar manner to the work in [24]) for real-time applications. Further security analyses could be conducted to evaluate resilience against advanced cryptographic attacks, including quantum attacks. Adaptation and testing on other media types, such as video and audio, would assess versatility. Additionally, user-friendly software tools and interfaces could be developed to allow the algorithm to be accessible for non-expert users and various application domains. These efforts aim to further improve the algorithm's robustness, efficiency, and applicability in safeguarding digital information.

## REFERENCES

- [1] O. Kocak, U. Erkan, A. Toktas, and S. Gao, "Pso-based image encryption scheme using modular integrated logistic exponential map," *Expert Systems with Applications*, vol. 237, p. 121452, 2024.
- [2] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37 855–37 865, 2021.
- [3] E. Akbal and S. Dogan, "Forensics image acquisition process of digital evidence," *International Journal of Computer Network and Information Security*, vol. 10, no. 5, pp. 1–8, 2018.



TABLE VI: S-box performance metrics comparison with recent literature.

S-Box	NL	SAC	BIC	LAP	DAP
Optimal	112	0.5	112	0.0625	0.015625
Proposed	108	0.504883	108	0.078125	0.015625
[4] OSSL	108	0.499023	112	0.0625	0.015625
[4] MT	108	0.503662	92	0.140625	0.015625
[4] IMKL	108	0.499268	104	0.09375	0.015625
[22]	106	0.47266	68	0.23438	0.015625

TABLE VII: NIST analysis.

Test Name	Results	Remarks
Frequency	0.867019	Success
Block Frequency	0.651474	Success
Run	0.356648	Success
Long runs of ones	0.188813	Success
Rank	0.126179	Success
Spectral FFT	0.405849	Success
Non overlapping	0.470698	Success
Overlapping	0.506129	Success
Universal	0.081046	Success
Serial	0.804702	Success
Serial	0.869155	Success
Approx. entropy	0.235608	Success
Cum. sums forward	0.346377	Success
Cum. sums reverse	0.463929	Success
Random Excursions (RE) 1	0.467290	Success
RE 2	0.721058	Success
RE 3	0.903227	Success
RE 4	0.952564	Success
RE 5	0.068856	Success
RE 6	0.532021	Success
RE 7	0.106924	Success
RE 8	0.211360	Success
Random Excursions Variant (REV) 1	0.091331	Success
REV 2	0.172244	Success
REV 3	0.303127	Success
REV 4	0.411452	Success
REV 5	0.408060	Success
REV 6	0.487663	Success
REV 7	0.935270	Success
REV 8	0.972120	Success
REV 9	0.671751	Success
REV 10	0.951729	Success
REV 11	0.852131	Success
REV 12	0.793555	Success
REV 13	0.731447	Success
REV 14	0.924978	Success
REV 15	0.522940	Success
REV 16	0.560545	Success
REV 17	0.734872	Success
REV 18	0.597118	Success

- [4] W. Alexan, N. Alexan, and M. Gabr, "Multiple-layer image encryption utilizing fractional-order chen hyperchaotic map and cryptographically secure prngs," *Fractal and Fractional*, vol. 7, no. 4, p. 287, 2023.
- [5] J. Daemen and V. Rijmen, *The design of Rijndael*. Springer, 2002, vol. 2.
- [6] K. M. Hosny, M. A. Zaki, N. A. Lashin, M. M. Fouda, and H. M. Hamza, "Multimedia security using encryption: A survey," *IEEE Access*, 2023.
- [7] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [8] H. I. Mohamed, S. M. Alhammad, D. S. Khafaga, K. M. Hosny *et al.*, "A new image encryption scheme based on the hybridization of lorenz chaotic map and fibonacci q-matrix," *IEEE Access*, 2023.
- [9] G. Biban, R. Chugh, and A. Panwar, "Image encryption based on 8d hyperchaotic system using fibonacci q-matrix," *Chaos, Solitons*

- & *Fractals*, vol. 170, p. 113396, 2023.
- [10] W. Alexan, D. El-Damak, and M. Gabr, "Image encryption based on fourier-dna coding for hyperchaotic chen system, chen-based binary quantization s-box, and variable-base modulo operation," *IEEE Access*, 2024.
- [11] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26 203–26 222, 2019.
- [12] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," *Neural Computing and Applications*, vol. 26, pp. 1137–1148, 2015.
- [13] W. Alexan, M. ElBeltagy, and A. Aboshousha, "Rgb image encryption through cellular automata, s-box and the lorenz system," *Symmetry*, vol. 14, no. 3, p. 443, 2022.
- [14] E. Hasanzadeh and M. Yaghoobi, "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys," *Multimedia Tools and Applications*, vol. 79, pp. 7279–7297, 2020.
- [15] J. Xu, B. Zhao, and Z. Wu, "Research on color image encryption algorithm based on bit-plane and chen chaotic system," *Entropy*, vol. 24, no. 2, p. 186, 2022.
- [16] W. Alexan, N. Alexan, and M. Gabr, "Multiple-layer image encryption utilizing fractional-order Chen hyperchaotic map and cryptographically secure PRNGs," *Fractal and Fractional*, vol. 7, no. 4, March 2023. [Online]. Available: <http://dx.doi.org/10.3390/fractalfract7040287>
- [17] Z. Liang, Q. Qin, and C. Zhou, "An image encryption algorithm based on fibonacci q-matrix and genetic algorithm," *Neural Computing and Applications*, vol. 34, no. 21, pp. 19 313–19 341, 2022.
- [18] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1989, pp. 549–562.
- [19] S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon, and I. Cho, "Provable security against differential and linear cryptanalysis for the spn structure," in *International Workshop on Fast Software Encryption*. Springer, 2000, pp. 273–283.
- [20] E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," *Journal of CRYPTOLOGY*, vol. 4, no. 1, pp. 3–72, 1991.
- [21] A. Webster and S. E. Tavares, "On the design of S-boxes," in *Conference on the theory and application of cryptographic techniques*. Springer, 1985, pp. 523–534.
- [22] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color image encryption through chaos and KAA map," *IEEE Access*, vol. 11, pp. 11 541–11 554, 2023.
- [23] S. M. Mohamed, W. S. Sayed, A. H. Madian, A. G. Radwan, and L. A. Said, "An encryption application and fpga realization of a fractional memristive chaotic system," *Electronics*, vol. 12, no. 5, p. 1219, 2023.
- [24] A. Saxena, V. Agrawal, R. Chakrabarty, S. Singh, and J. S. Banu, "Accelerating image encryption with aes using gpu: A quantitative analysis," in *International Conference on Intelligent Systems Design and Applications*. Springer, 2018, pp. 372–380.