ISSN: 2617-5517 (issn.org)
Al-Farabi Journal of Engineering Sciences
https://iasj.rdd.edu.iq/journals/journal/view/97
مجلة الفارابي للعلوم الهندسية تصدرها جامعة الفارابي

Fast Image Encryption Scheme with One Way S-box and Chaotic Map

Sura Mahroos Searan
Department of Computer Science, College of Computer Science and Information Technology, Anbar, Iraq
Email: surasms917@uoanbar.edu.iq

Abstract
This work presents a method for image encryption depended on the chaotic map with AES-Substitution-box that is one of a most essentials and just non-linear attribute of block cipher. Encryption algorithm consists of the encryption keys generation by using the proposed algorithm with its permutation and diffusion. This scheme is utilized to encrypt the images (color) with any size by using (substitution-permutation) table. The construction of Logistic map with one way-S-box is to use the generated key sequence, it is more robust to algebraic attacks than chaotic. One-way S-box utilized by adopting appropriate affine matrix and irreducible polynomial. The conception of confusion is applied to the texture of S-box. In the diffusion phase, the permuted bytes is swapped. The encryption step are done by encrypting an image bytes by using an S-box for substitution and applies nonlinear transformations depending on the values parsed from input fields. And then swapping it by using swap function to permute it. Every pixel is transformed independently, and the new ciphered image is created as a result of these operations. The analysis of correlation coefficient shows that the suggested algorithm effectively removes the correlation between the adjacent pixels. The ciphered image exhibits correlation coefficients near to zero in all the directions, demonstrating strong security and high randomness against the statistical attacks. The results of simulation and security analysis present that the proposed image encryption scheme has high encryption efficiency and successfully encrypts and decrypts diverse types of images. It has kindly key space and can endure statistical, brutal and diverse attacks.
Keywords: Visual Cryptography; Image encryption; block cipher; S-box; Logistic map.

1. Introduction

In the evolution of technology, security, and quick contacting have become vital appeal. These dictates require solid reckoning, and are opposite between them, as encryption side may seriously influence the compression regulation. Moreover, handheld devices have computational exchequer and finite energy, making squeeze friendly encryption a brave affair [1]. One of a settlement is to encrypt a data subset based on percept consequence. In spite of that may not be squeeze efficient, assure and format cooperative. To solve the safeness issue in these demands, the replacement box is one of the main essential and non-linear block ciphers issue. These neutralization have the features that facilely meet the block ciphers deficiency [2]. Information security is a way that corporation secures and protects the systems. Information may be guarded by encrypt it by utilizing one of encryption algorithms [3]. Traditional algorithms of cryptography are compound and get a higher set of vitality when they are utilized by exchequer strained devices to supply safe communication [4]. conservation systems are depended on the uniform key cryptology principally in the fixture that has constricted resource of hardware [5]. Various researches used a practice to developed logistic chaotic map and modified ways without disturbing its mathematical construction producing al algorithm with high level of security, surpassing many state-of-the-art algorithms [6], and encrypt the color images of any size by utilizing three variables premeditated from the values of pixel's for the three channels (RGB) of the original image. And demonstrate the algorithm security against many attacks [7]. The others used the diffusion and permuted image is overpassed in the same order and has morality key space and can withstand effectual on various attacks [8]. The cryptography objective is to supply issues that protect sensible information dispatched via networks that unprotected. These ways encrypt the data, making it occult even if

adversaries manage to gain it. The replacement box structure is the main essential nonlinear component of Advanced Encryption Standard (AES) algorithm. The replacement box donate the mixing or distraction process. The extremely non-linear-valued S-box crucially increase guard against a scope of impendence. Regrettably, the encryption is nervous by the computationally high-cost way of generating S-boxes. This affirm the essential of producing new S-box generator by the leading adversity and least computing demands to give optimal preservation [9]. Various constituent are needed to take into description such as space complexity, security, time complexity, and the property of the algorithm. The principal cryptography aim is not only utilized to give secrecy, but to supply solutions for other issues such as availability, authentication, non-repudiation, and integrity [10].

The essential article contributions are:

• Evolving an algorithm for image encryption without compromise the efficiency, protection, and fineness metrics.

• Estimating the suggested scheme with a variety set of evaluation, such as time, space complexity and Big-O-notation

• Experimentation the randomness of encrypted images that gain by the suggested scheme using the NIST Suite of Statistical Tests.

• The plain image encryption with the developed scheme yields totally divergent cipher images, that helps in beating statistical samples in encryption scheme, then the cryptanalysis is hard.

The residue of the article is ordered as follows: The section (2) considers the literature of image encryption algorithms. Section 3 considers the designed encryption scheme along with its model and pseudo code. Section 4 illustrates the evaluation criteria to assess the proposed scheme, and also encompass the evaluation and the results of suggested algorithm. Eventually, Section 5 deduce this work.

2. Related Works

Numerous techniques of image encryption schemes have been presented in the literary. Hua et al. [11] have suggested encryption way for images depended on chaotic map (2D), where the writers have utilized (sine-logistic map (2D)) to produces two arrays. The suggested way utilizes one of the produced arrays to randomly teeter the pixel of image places by connect the pixels in divergent columns and rows into rings, then shift them within ring. The designed method performance is rapid, but has a high association between cipher image pixels. Alanezi et al. [12] developed an algorithm that utilizes two maps of chaotic: (logistic-sin-map) to rearrange the main image, the other is (logistic–Chebyshev map) to exchange the gain rearranged image. The scheme then carry out an XOR operator on the replaced array with a two maps cascading to get the ciphered image. Arif et al. [13] designed a way based on (logistic maps), they utilize the main image to get a hash, and then split into 4 segments, each of them is utilized as an starting variable input for the map to gain (4) pseudorandom symbol matrix. The model then performs disposition column and row by the first and the second keys. And perform XOR way on the gain image by utilizing the third key. The ending phase is doing image replacement by using the AES-S-Box or revers AES-S-Box depending on a fourth got key. The proposed way don't conduct efficiently in the side of encryption time. Wang et al. [14] used a set of (4 chaotic maps). The developed scheme has a 3-round of scrambling utilizing logistic map and Josephus navigation, and one round of spreading using one of sin, logistic, Chebyshev, or cos maps depend on a mod way on the cells of the original image. The designed method does not done distraction on the pixel values. The suggested way has good protection attributes, as spotted through assessment metrics, but it slows in the speed. Lu et al. [15] proposed a method depend on the (Logistic-Sin-maps) and utilizes one S-Box. The method begins by getting the chaotic series and S-Box utilizing pre-shared keys as the input to it. The chaotic-series used to transpose the main image. The gain image is exchanged twice utilizing the chaotic as S-Box key. The designed system do not need the utilize of modular method, which conduct to a trivial speed-up but isn't that notable in the time of the encryption way. In the late years, various compressive-comprehend-based encryption methods have been developed. Compressive comprehend is helpful in decreases the size and time of gain images by compressing, sampling, and at the same period encrypting the main image [16]. Ye et al. [17] developed a new hyper-chaotic attitude. The portraits are first squeezed by utilizing compressive observe, and a conducting squeezed image is then encoded using elliptic curve scheme. The designed method is encrypt two main portraits at the same tour, decreasing the encryption times for multiple portraits. Despite the fact that many earlier concepts have produced image encryption, the majority of these works simply agree on the protection aspect of the proposed methods. Do not speculate on how fast encryption works.

There are numerous serious issues with picture encryption methods, protecting images from unauthorized access during storage and transmission is essential, especially for sensitive information like medical records. The proposed algorithms show robustness against various attacks, such as brute force and differential attacks, but are not efficient enough to enable fast encryption and decryption processes. Another problem is maintaining image quality, as encryption can sometimes compromise an image's visual integrity, making it less valuable. Effective key management is also required for the generation, distribution, and safe storage of encryption keys. Additionally, algorithms need to be scalable in order to process images of different sizes and formats. To avoid significant disruptions to workflow, compatibility with existing apps and image formats is crucial. The earlier studies analyze their suggested approach using a few security measures, and they test it on gray-scale photographs rather than color ones, which are the dominant image format at the time. By evaluating the suggested approach for both color and gray-scale photos and comparing it to a collection of metrics for encryption of image, this work fills the gap in earlier research. The created technique can be diffused for applications of real-time and limited resources devices, including edge devices and the Internet of Things, and is designed with encryption speed in mind.

3. Visual Cryptography

Visual cryptography is a method that makes it possible to encrypt pictures so that they may be visually decrypted [18]. Visual cryptography is an interesting blend of art and science that dispense a unique technique to image encryption. It permit for secure communication and can be adapted for many fields, including watermarking and digital security [19]. Here's a quick rundown of how it operates:

Image Division: A picture is split up into several shares, usually two. Every share resembles an arbitrary pixel pattern.

Pixel Encryption: The original image's pixels are split up into smaller pieces, and each piece is given a share. The shares are made so that the original pixel can be visually recreated when they are superimposed.

Distribution of Shares: Various parties may receive the shares. No details about the original image are revealed by a single share.

Reconstruction: The original image can be visually recreated by superimposing the shares [18].

4. Image Encryption

The image encryption depend on techniques to generate encrypted new images and to eliminate the liaison between neighbor pixels: the confusion and the diffusion. The confusion is carried out via substitution that is the changing of each pixel values in a main digital image by a map of the substitution. In the encryption of image, a controlling of confusion is done by using key to hazy the values of the original image [3]. The diffusion mean that if any pixel change in the main image, then it ought result in about half change of the pixels in the encrypted image, and the similarly, if an alteration in a single pixel in the cipher, then it ought result in a alteration in around half of the produced image pixels. A diffusion is help eliminate the liaison between nigh pixels in a main image, that is brilliant by alteration in the algorithms of encryption [8].

Security test

Attackers used numerous attacks or chosen attacks of plaintext for guessing the tie between the cipher image and its origin image to breach the scheme of encryption. For the encryption scheme to be rate secure, any changes of a pixel in the origin image should harvest a full different in the encrypted image. For evaluating the resistance of an algorithm to differential attacks, there are a set of commonly tests. These tests are: NIST Test, the number of pixels change rate (NPCR), unified averaged changing intensity (UACI), and the avalanche effect [8].

NIST Test

The NIST statistical test suite was used to analyze the logistic map's generated key stream and the altered method. Sixteen trials are included in the statistical collection for random numbers generator examination, or NIST, which measures the output series randomness. The checking was made by using NIST STS-1.6. The developed scheme in this article analyze and then compared to logistic map for time complexity, space complexity, and analyses of histogram. When a random series should be doubtful of the suggested algorithm and logistic map, the NIST statistic test is also used to measure the strong property and verify the randomness qualities [7].

Avalanche Effect

In the cryptography, the avalanche effect is where an easy change in the input leading to important changes in the output. The MSE metric used for testing the avalanche effect with easy alteration in the parameters for

calculating the average squared differ through the values of pixel of two ciphered images taken from the image with a changing of 1-bit instead through the cipher text and plain image [10].

5. The Proposed Technique for Image Encryption

After being built and evaluated for security robustness, the AES-S-box was employed in this work with the chaotic equation to encrypt image data in an eclectic manner. to increase security and produce a key-dependent permutation and replacement that is chaotic, highly diffuse, and confusing. The S-box's security was ensured by the Strict Avalanche Criterion, bit statehood, and non-linearity, among other factors. By introducing key dependent S-Box and permutation, this viewpoint also maintained the appropriate level of security. When the outputs of the logistic map and the cipher images were compared in terms of randomness and correlation, the suggested approach performed better. This system is used to encode any size of the color images by using a substitution and dynamic transposition. The pixels substitution of each channel utilizing a exchanging table of AES algorithm. The second phase is to make permutation by using three variables deliberate from the cells values of the color channels (R, G and B) of the main image. The exchanging box (S-box) operated as the non-linearity portion in a symmetric scheme of encryption. It directly regulate the work and protection ciphers level. Thus, the S-box with senior work and regulation, specifically in aspects of high effects of cryptography, is critical. The chaotic map produce pseudo-random sequences and Introduces high sensitivity to the initial conditions and Utilized for permutation of pixel or generation of the key. The S-Box provides non-linearity and confuses pixel values and prevents differential and statistical attacks, together, they provides both: confusion with S-Box and diffusion with permutation of chaotic.

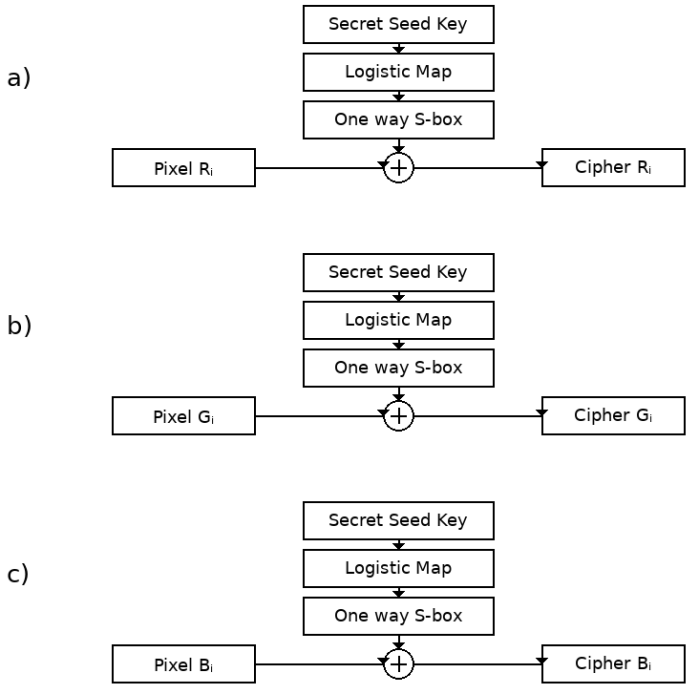

Fig 1. Suggested image encryption Scheme Model: a) for Ri. b) for Gi. c) for Bi.

The Algorithm Steps of the developed Algorithm:	
Step	Description
Input:	Pain RGB Image I, and Secret parameters of seed key (xr, xg, xb, rr, rg, rb,).
Output:	Encrypted image.
Step	Operation
1:	Initialize the parameters of secret key (0 < xr, xg. xb <1).
2:	Generate the chaotic sequences by using logistic map.
3:	Define the function of AES S-box (S:{0,…,255}).

4:	Read the main image and get pixel values: (Ri, Gi, Bi).
5:	Apply S-box substitution (MapSbox ⟵ AES).
6:	Generate key values: for R, G, and B channels: rkey = MapSbox((int)rr) * xr * 1000000 % 256 gkey = MapSbox((int)rg) * xg * 1000000 % 256 bkey = MapSbox((int)rb) * xb * 1000000 % 256
7:	Encryption: (R1, G1, B1)⟵(R, G, B)⊕the produced keys (rkey, gkey, bkey).
8:	Update the scaling factors based on the logistic model: xr = rr * xr * (1 - xr) xg = rg * xg * (1 - xg) xb = rb * xb * (1 - xb)
9:	Permute the values of xr and xb.
10:	Swap operation for (xr, xb)
11:	Repeat the steps (6 to 10) for all pixels i.
12:	Reshape the encrypted values to generate the cipher image.

The whole operation encrypts an image bytes by using an substitution and concern nonlinear transformations based on the values parsed from input, and then swapping it by using swap function to permute it. Every pixel is transformed independently, and the new ciphered image is created as a result of these operations. A small alteration to the input lead to notably different outputs. This method is appropriate for image encryption so it operates at the pixel level, providing a unique modification for each pixel based on the system.

1. Results and Discussion

The designed algorithm's implementation time coincides strongly with the requirement for chaotic implementation. Compared to a chaotic key stream, the created algorithm key is more complex and random. The NIST sts1.6 was used to evaluate randomness. The P-value indicates the likelihood of a perfect random number inventor. The test's P-value is equal to 0.01. The sequence is approved and the gain sequences are randomly dispersed if the value is more than 0.01; if not, the sequences are rejected and there is no randomness. ACHIEVEMENT indicates that the sequence is achieved and has good unpredictability, whereas an FAILURE shows that the sequence is unacceptable and not random. The histogram give statistical properties, strong encryption smooth histogram. The proposed cryptographic system attain optimal security. The figures below shows the histogram of encrypted and decrypted image for suggested algorithm.

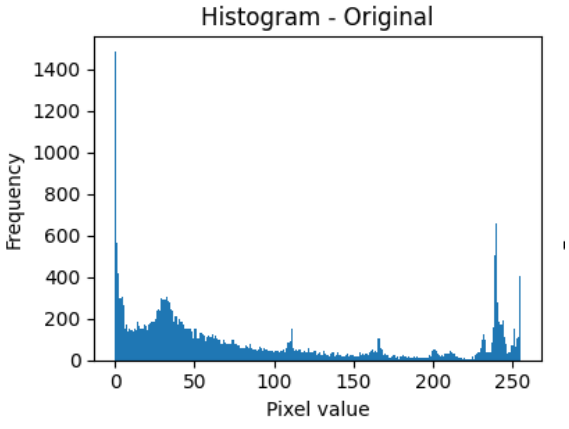

Fig 2. The encrypted image histogram for the proposed algorithm.

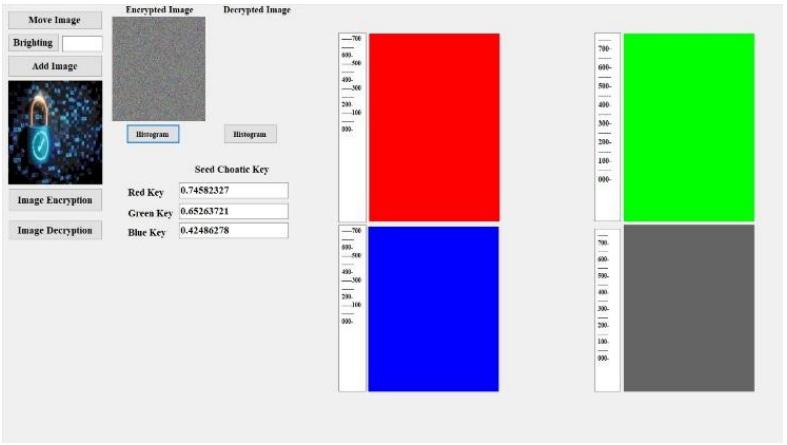

Fig 3. The distribution of the main image bytes.

The histogram of the plain image has no regular distribution, and clear valleys and peaks. The correlates with contents of image are: in dark images, the peaks are at low intensities and in bright images, the peaks are at high intensities. The histogram of the encrypted image is regular, obviate statistical attacks, hides the patterns, encrypted image give a random noise.

Figure 4 shows the byte distributions for the ciphertext values in the example. These values are easily distributed and not easy to view, as there are various possibilities for how the ciphertext character can take a readable form.

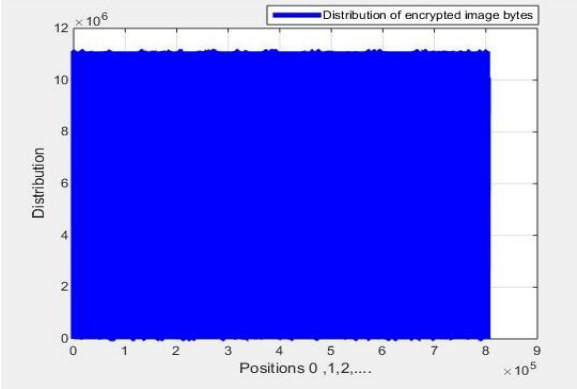

Fig 4. The distribution of encrypted image bytes.

2. The Evaluation Criteria

A) Big-O-Notation

A mathematical entry known as "Big O notation" is used to represent the worst-case or upper-case scheme of algorithm's temporal complexity of input size. It provides a consistent and concise means of expressing how the execution of algorithm grows with increasing input size.

Read the plaintext image	1
Initialize Method for S-box Mapping	1
Prepare Image Objects	1
Retrieve Scaling Factors	1
Iterate Through Image Pixels	1N
Pixel Manipulation	1N
Update Scaling Factors	1

The Big-O is 2N+5, it has linear time complexity such as logistic map.

Big O Notation plays an essential role in algorithm analysis. It discusses an algorithm's efficiency, especially how its running time or space requirements expand as the size of the input expand.

B) NIST (National Institute of Standards and Technology)

The NIST statistical test suite was used to analyze the logistic map's generated key stream and the altered method. Sixteen trials are included in the statistical collection for random numbers generator examination, or NIST, which measures the output series randomness. The checking was made by using NIST STS-1.6. The developed sheme in this paper is analyzed and then compared to logistic map for time complexity, space complexity, and analyses of histogram. When a random series should be doubtful of the suggested algorithm and logistic map, the NIST statistical test is also used to measure the strong property and verify the randomness qualities. Each of the 15 statistical tests in the test suite produces a p-value between 0 and 1. The series is considered random and passes the test if the p-value is higher than the cutoff value of $\mu = 0.01$. The NIST test results are shown in the table below.

NIST provides numerous tests aimed at analyzing the aspect of random number generators and encryption algorithms, which can help estimate whether the encryption way is secure. Key areas for assessment:

1. Randomness experimentation: Use the NIST Suite of Statistical Tests to warrant the output of the system reveal properties of randomness.
2. Security Estimation: examining how sensitive the encryption is to even the smallest input changes. This serves as a principle to guarantee the systems' dispersion attribute.

Table 1. Result of applying NIST on the key generated by the proposed algorithm and chaotic logistic map,

Test No.	Name of Statistical Test	The proposed algorithm		Chaotic logistic map	
		P-VALUE	In conclusion	P-VALUE	In conclusion
1	apen	0.31039	ACHIEVEMENT	0.051039	ACHIEVEMENT
2	The block frequency	0.955993	ACHIEVEMENT	0.055993	ACHIEVEMENT
3	The cumulative totals	0.613374	ACHIEVEMENT	0.053815	ACHIEVEMENT
4	fft	1.000000	ACHIEVEMENT	0.270812	ACHIEVEMENT
5	frequency	0.607045	ACHIEVEMENT	0.086849	ACHIEVEMENT
6	lempel-ziv	0.365834	ACHIEVEMENT	0.238573	ACHIEVEMENT
7	The linear complexity	0.930755	ACHIEVEMENT	0.201489	ACHIEVEMENT
8	longest-duration	1.000000	ACHIEVEMENT	0.459376	ACHIEVEMENT
9	Non-recurring templates	0.858166	ACHIEVEMENT	0.569039	ACHIEVEMENT
10	Overlapped templates	0.728066	ACHIEVEMENT	0.849607	ACHIEVEMENT
11	Arbitrary excursions	0.438467	ACHIEVEMENT	0.384184	ACHIEVEMENT
12	Arbitrary excursions -variant	0.418379	ACHIEVEMENT	0.359137	ACHIEVEMENT
13	Rank	0.997433	ACHIEVEMENT	0.339903	ACHIEVEMENT
14	Operates	0.179621	ACHIEVEMENT	0.569136	ACHIEVEMENT
15	Serial	0.966385	ACHIEVEMENT	0.712946	ACHIEVEMENT
16	Universal	0.354915	ACHIEVEMENT	0.216396	ACHIEVEMENT

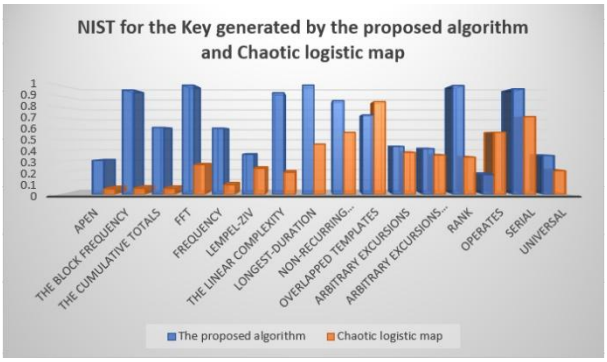

Fig 5. NIST for the key generated by the proposed algorithm and chaotic logistic map.

3. The algorithm analysis by using correlation coefficient

In the plain images, **adjacent pixels** (vertical, diagonal, and horizontal) are **correlate high**. A secure encryption algorithm must **hide the correlation**, making the ciphered image appear random.

The **correlation coefficient** measures how two adjacent pixels are highly related.

The formula of correlation coefficient

For two pixels (x and y), the correlation coefficient (c_{xy}) is defined as follows:

$$c_{\{xy\}} = \frac{Cov(x,y)}{\left\{\sqrt{\{V(x)\}} \cdot \sqrt{\{V(y)\}}\right\}} \quad (1)$$

$$Cov(x,y) = \frac{1}{N}\sum_{\{i=1\}}^{\{N\}}(x_i - M(x))(y_i - M(y)) \quad (2)$$

$$M(x) = \frac{1}{N}\sum_{\{i=1\}_i^{\{N\}x}} \quad (3)$$

$$M(y) = \frac{1}{N}\sum_{\{i=1\}_i^{\{N\}y}} \quad (4)$$

$$V(x) = \frac{1}{N}\sum_{\{i=1\}}^{\{N\}}(x_i - M(x))^2 \quad (5)$$

$$V(y) = \frac{1}{N}\sum_{\{i=1\}}^{\{N\}}(y_i - M(y))^2 \quad (6)$$

$$-1 \leq c_{\{xy\}} \leq 1$$

- x_i, y_i : mean the values of 2 adjacent pixels
- N: mean the number of pairs of the pixel
- M(x)M(y): mean
- V(x)V(y): mean the variance

The value of c_{xy} lies in **[-1, 1].**

The Procedure of Correlation Analysis

1. Select from the image a large number of adjacent pairs:
   - Diagonal
   - Vertical
   - Horizontal
2. Calculate the correlation coefficients for original image and for ciphered image.
3. Compare among the results.

The results shows that in the original image, the correlation coefficients are **near to one and** there are high similarity between the neighboring pixels. In the encrypted image, the correlation coefficients are **near to zero and** there are a good diffusion and high randomness.

Table 2. Illustrates the correlation coefficients values for the compared images,

Direction	Original Image	Ciphered Image
Diagonal	0.91	0.0004
Horizontal	0.97	0.0013
Vertical	0.93	−0.0007

The correlation in the original image shows the redundancy. The near to zero in the encrypted image shows that the chaotic map strongly randomizes the positions of pixels and the S-box masks pixel values. This proves a strong resistance against many of **statistical attacks**.

4. Conclusions

This study presents an image encryption method based on the combination of the AES S-box and chaotic map. The generated cipher image is further randomized using substitution and permutation. The image series encrypted by the suggested approach pass all statistical tests with high P-values and have no

obstructions, according to NIST randomness testing. The suggested model outperforms the logistic map in terms of encryption quality, according to the assessed encryption quality. As a result, the suggested model is highly secure. By employing XOR operations with dynamic keys that vary according to logistic variation, the code effectively encrypts an image by altering the colors of its pixels. A simple yet efficient encryption method is made possible by the independent processing of each pixel. This layout can offer a certain amount of security. We have used a number of security, quality, and efficiency parameters to examine and contrast our suggested picture encryption algorithm with the logistic map. The findings demonstrate that the suggested algorithm yields promising results in complexity, histogram, and contrast, and they also reveal that the approach has great security when compared to alternative encryption techniques. The suggested approach offers strong defense against assaults including data loss and noise. The results prove that when the cipher image is decrypted, the suggested encryption/decryption procedure may retrieve the plain image. The cipher image randomness that generated by the suggested algorithm was tested using the NIST test suite, and the findings indicate that the produced image encrypted by the suggested algorithm passed each and every NIST test. The analysis of correlation coefficient shows that the proposed algorithm effectively removes the correlation between the adjacent pixels. The ciphered image exhibits correlation coefficients near to zero in all the directions, demonstrating strong security and high randomness against the statistical attacks. We intend to generate pseudorandom numbers in future work using various chaotic maps, which may offer greater security, an even pseudo-random numbers distribution, and a bigger key space than logistic map.

References

[1] Su, Y., Tong, X., Zhang, M., & Wang, Z. (2023). Efficient image encryption algorithm based on dynamic high-performance S-box and hyperchaotic system. *Physica Scripta*, *98*(6), 065215.

[2] Khan, N. A., Altaf, M., & Khan, F. A. (2021). Selective encryption of JPEG images with chaotic based novel S-box. *Multimedia Tools and Applications*, *80*(6), 9639-9656..

[3] Sagheer, A. M., & Searan, S. M. (2017). Design of New Algorithms to Analyze RC4 Cipher Based on Its Biases. In *Shaping the Future of ICT* (pp. 347-362). CRC Press.

[4] Sagheer, A. M., Searan, S. M., & Salih, S. S. (2018). Developing RC4 Algorithm Using S-Box of Advanced Encryption Standard Cipher. *International Journal of Computing and Digital Systems*, *7*(04), 207-214.

[5] Sagheer, A. M., Salih, S. S., & Searan, S. M. (2018). Design and Implementation of Secure Stream Cipher Algorithm. *International Journal of Computing and Digital Systems*, *7*(03), 127-134.

[6] Waheed, A., & Subhan, F. (2024). S-box design based on logistic skewed chaotic map and modified Rabin-Karp algorithm: applications to multimedia security. *Physica Scripta*, *99*(5), 055236.

[7] Qobbi, Y., Jarjar, A., Essaid, M., & Benazzi, A. (2023). Image encryption algorithm using dynamic permutation and large chaotic S-box. *Multimedia Tools and Applications*, *82*(12), 18545-18564.

[8] Zheng, J., & Zeng, Q. (2022). An image encryption algorithm using a dynamic S-box and chaotic maps. *Applied Intelligence*, *52*(13), 15703-15717.

[9] Ali, R., Ali, J., Ping, P., & Jamil, M. K. (2024). A novel S-box generator using Frobenius automorphism and its applications in image encryption. *Nonlinear Dynamics*, *112*(21), 19463-19486.

[10] Kanso, A., & Ghebleh, M. (2012). A novel image encryption algorithm based on a 3D chaotic map. *Communications in Nonlinear Science and Numerical Simulation*, *17*(7), 2943-2959.

[11] Hua, Z., Zhou, Y., Pun, C. M., & Chen, C. P. (2015). 2D Sine Logistic modulation map for image encryption. *Information Sciences*, *297*, 80-94.

[12] Alanezi, A., Abd-El-Atty, B., Kolivand, H., Abd El-Latif, A. A., Abd El-Rahiem, B., Sankar, S., & S. Khalifa, H. (2021). Securing Digital Images through Simple Permutation-Substitution Mechanism in Cloud-Based Smart City Environment. *Security and Communication Networks*, *2021*(1), 6615512..

[13] Arif, J., Khan, M. A., Ghaleb, B., Ahmad, J., Munir, A., Rashid, U., & Al-Dubai, A. Y. (2022). A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution. *IEEE Access*, *10*, 12966-12982.

[14] Wang, X., Zhu, X., & Zhang, Y. (2018). An image encryption algorithm based on Josephus traversing and mixed chaotic map. *IEEE Access*, *6*, 23733-23746.

[15] Lu, Q., Zhu, C., & Deng, X. (2020). An efficient image encryption scheme based on the LSS chaotic map and single S-box. *Ieee Access*, *8*, 25664-25678.

[16] Alghamdi, Y., Munir, A., & Ahmad, J. (2022). A lightweight image encryption algorithm based on chaotic map and random substitution. *Entropy*, *24*(10), 1344.

[17] Ye, G., Liu, M., & Wu, M. (2022). Double image encryption algorithm based on compressive sensing and elliptic curve. *Alexandria engineering journal*, *61*(9), 6785-6795.

[18] Bachiphale, P. M., & Zulpe, N. S. (2025). A comprehensive review of visual cryptography for enhancing high-security applications. *Multimedia Tools and Applications*, *84*(26), 31023-31045.

[19] Karolin, M., & Meyyappan, T. (2024). Visual cryptography secret share creation techniques with multiple image encryption and decryption using elliptic curve cryptography. *IETE Journal of Research*, *70*(2), 1638-1645.