SRSS: A New Chaos-Based Single-Round Single S-Box Image Encryption Scheme for Highly Auto-Correlated Data

Muhammad Shahbaz Khan[1], Jawad Ahmad[1], Hisham Ali[1], Nikolaos Pitropakis[1]
Ahmed Al-Dubai[1], Baraq Ghaleb[1], William J. Buchanan[1]
[1]*School of Computing, Engineering and the Built Environment,*
Edinburgh Napier University,
Edinburgh, UK,
Emails: {muhammadshahbaz.khan, j.ahmad, h.ali, n.pitropakis, a.al-dubai, B.Ghaleb, b.buchanan}@ napier.ac.uk

***Abstract*—With the advent of digital communication, securing digital images during transmission and storage has become a critical concern. The traditional s-box substitution methods often fail to effectively conceal the information within highly auto-correlated regions of an image. This paper addresses the security issues presented by three prevalent S-box substitution methods, i.e., single S-box, multiple S-boxes, and multiple rounds with multiple S-boxes, especially when handling images with highly auto-correlated pixels. To resolve the addressed security issues, this paper proposes a new scheme SRSS—the Single Round Single S-Box encryption scheme. SRSS uses a single S-box for substitution in just one round to break the pixel correlations and encrypt the plaintext image effectively. Additionally, this paper introduces a new Chaos-based Random Operation Selection System—CROSS, which nullifies the requirement for multiple S-boxes, thus reducing the encryption scheme's complexity. By randomly selecting the operation to be performed on each pixel, driven by a chaotic sequence, the proposed scheme effectively scrambles even high auto-correlation areas. When compared to the substitution methods mentioned above, the proposed encryption scheme exhibited exceptionally well in just a single round with a single S-box. The close-to-ideal statistical security analysis results, i.e., an entropy of 7.89 and a correlation coefficient of 0.007, validate the effectiveness of the proposed scheme. This research offers an innovative path forward for securing images in applications requiring low computational complexity and fast encryption and decryption speeds.**

***Index Terms*—S-Box, chaos, image encryption, correlation, single round, single S-Box**

I. Introduction

With the rapid development of digital communication, social media, telemedicine (to transmit or store clinical image), online biometric systems (to store and transmit face portraits or fingerprints), and the Internet of Things, a large amount of digital images is transmitted over the internet and stored in cloud storage [1]. The information in these digital images may be illegally intercepted, destroyed, or tampered with during transmission or storage [2], [3]. Therefore, digital images need a high level of security. Image encryption plays an indispensable role in securing digital images. Image encryption involves two basic processes, i.e., confusion and diffusion. According to Claude Shannon [4], confusion refers to changing the values of the pixels based on a key and is usually achieved by substituting one value for another. Diffusion, on the other hand, refers to changing the position of the pixels based on a key. This is usually achieved through mechanisms like the permutation. The basic workflow of image encryption using confusion and diffusion processes is given in Fig. 1 and is mathematically expressed as follows [5]:

$$C = \delta^n \left(\gamma^m(P, K_\delta), K_\gamma\right) \tag{1}$$

where P is the plaintext image, C is the ciphertext image, δ and γ represent the confusion and diffusion processes, respectively, K_δ and K_γ are the confusion and diffusion secret keys, and n and m are the number of rounds for confusion and diffusion. A secure image encryption algorithm should be sensitive to the cipher key, with a larger key space to be effective against brute force and other attacks. The key space for a general image encryption system can be computed by Equation 2 [5].

$$KS = (KS_\delta^n \cdot KS_\gamma)^m \tag{2}$$

where KS_δ and KS_γ represent the key spaces of the confusion and diffusion processes, respectively.

Recently, chaos theory has proven to be an effective and efficient tool in image encryption, owing to its high sensitivity to initial conditions [6], randomness [7], unpredictability [8], and ergodicity [9]. When combined with the confusion and diffusion processes in image encryption, it induces non-linearity in the encrypted image and significantly enhances

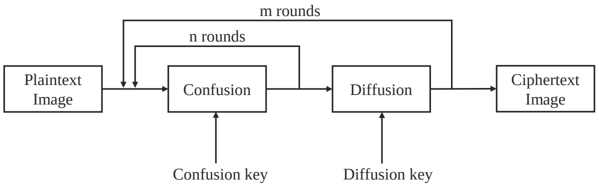


Fig. 1: Image encryption basic workflow with confusion and diffusion processes.

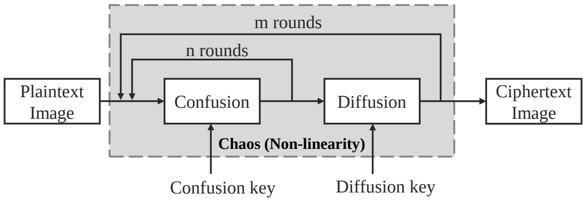


Fig. 2: Image encryption with chaos-based confusion and diffusion processes.

the security of the encryption algorithm. Fig. 2 depicts where the chaos comes in an image encryption algorithm. In most cryptographic systems, the fundamental non-linear component of the confusion process is the S-Box (substitution box) [10]–[12]. The S-box substitution method transforms inputs into altered outputs.

Usually, three common types of S-box substitution methods are utilized: single S-box using bijective mapping [13]–[15], multiple S-boxes [16]–[21], and multiple rounds of encryption with multiple S-boxes [22]–[24]. However, a common drawback of these methods is their inability to handle images with high auto-correlation, where sections of similar pixel values simply transform into different brightness levels rather than becoming adequately encrypted. This issue has also been addressed and analyzed in detail in Section 2. To address these concerns, this paper aims at proposing a new image encryption scheme that effectively scrambles the image and also mitigates the computational and latency problems in existing schemes. The proposed scheme utilizes a single S-box and only a single round of substitution and breaks the correlations in the image, even in areas of high auto-correlation.

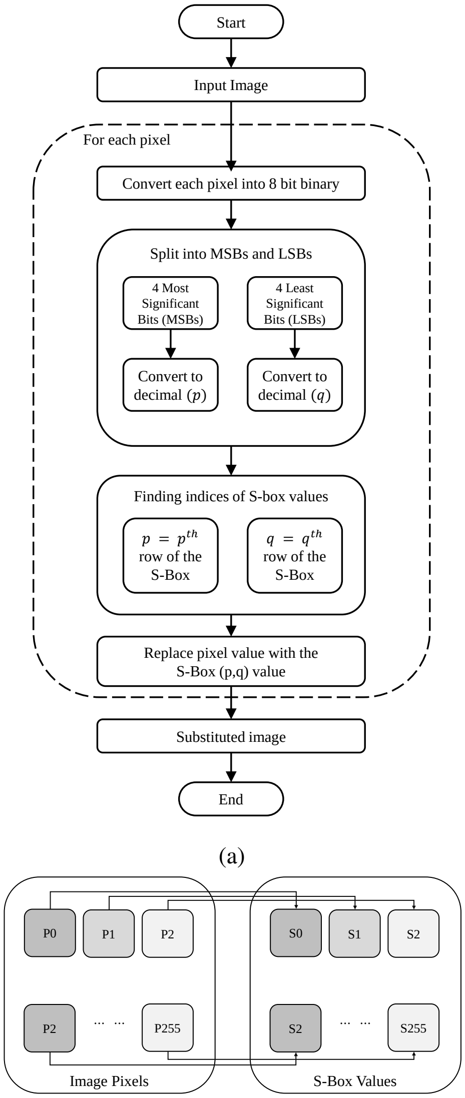
The main contributions of this paper are:

1) A new image encryption scheme 'SRSS – Single Round Single S-Box' is proposed to resolve the security, complexity, and latency issues identified in traditional s-box substitution methods. This scheme breaks the correlations in the pixels and encrypts the image by utilizing a single S-box for substitution in only a single round.
2) A new chaos-based random operation selection system – CROSS – is introduced, which eliminates the need for multiple s-boxes and hence, reduces the complexity of the encryption scheme.
3) Three types of substitution methods, i.e., single s-box, multiple s-boxes, and multiple s-boxes with multiple rounds, have been implemented and analyzed to highlight the security issues, especially for images with highly auto-correlated pixels and lower gray scales.

II. Problem Formulation

Three types of s-box substitution methods have been implemented and analyzed in detail to highlight their security issues.

A. Single S-Box Substitution Method


Start
Input Image
For each pixel
Convert each pixel into 8 bit binary
Split into MSBs and LSBs
4 Most Significant Bits (MSBs)
4 Least Significant Bits (LSBs)
Convert to decimal (p)
Convert to decimal (q)
Finding indices of S-box values
$p = p^{th}$ row of the S-Box
$q = q^{th}$ row of the S-Box
Replace pixel value with the S-Box (p,q) value
Substituted image
End
P0
P1
P2
P2
... ...
P255
S0
S1
S2
S2
... ...
S255
Image Pixels
S-Box Values

(a)

(b)

Fig. 3: (a) Single S-box substitution algorithm, (b) bijective mapping

The substitution mapping used in single s-box substitution methods is called bijective mapping. In bijective mapping, pixels are replaced with only one unique S-box value, and the S-box is considered as the bijective function $f(x)$. The substitution algorithm that utilizes bijective mapping is given in Fig. 3 (a) and the S-box bijective substitution function is given in Fig. 3 (b). This function can be realized mathematically as:

$$S : \mathrm{GF}(2^p) \rightarrow \mathrm{GF}(2^q) \tag{3}$$

if $x_1 = x_2$, then

$$f(x_1) = f(x_2) \tag{4}$$

In such s-box substitution function, the image is encrypted with only one unique element of the utilized S-Box. Pixels having identical values will be replaced with the same unique number from the S-Box and hence, will result in a change in the brightness level of the region only. The results of the

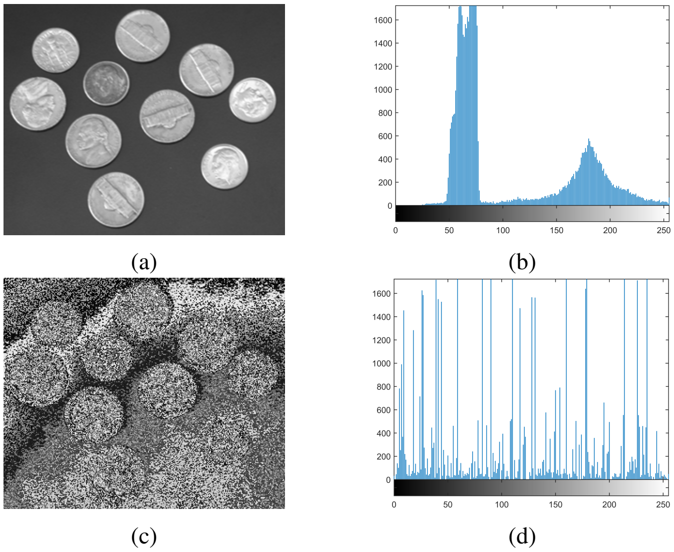


Fig. 4: Single s-box substitution results; (a-b) Coins image with its histogram, (c-d) Encrypted Coins image with its histogram.

single s-box substitution algorithm given in Fig. 4 show that the Coins image is not scrambled efficiently and all edges are visible.

B. Multiple S-Box Substitution Method

The most commonly used multiple S-Box substitution method is shown in Fig. 5. Here, chaos is used in conjunction with multiple S-boxes. Chaotic sequences are generated by using logistic map, which is given in Equation (5).

$$x_{n+1} = \mu \cdot x_n \cdot (1 - x_n) \tag{5}$$

where $\mu \in (0, 4)$ and $x_0 \in (0, 1)$.

This scheme somehow resolves the issues of single s-box substitution, but the problem of visible edges continues to exist and is evident from the results shown in Fig. 6.

C. Multiple S-Boxes and Multiple Rounds of Encryption

In addition to single s-box and multiple s-box substitution methods, multiple rounds with multiple s-boxes-based methods are also utilized. We analyzed this method for 5 rounds of substitution and used three different s-boxes for substitution. It can be seen from the results in Fig. 7 that this method also fails to scramble the pixels effectively. Furthermore, the statistical security analysis in Table 1 also shows that there's no change in the entropy of the encrypted images after every substitution round. The results of GLCM (Gray Level Co-occurrence Matrix) parameters, i.e., correlation, contrast, energy, and homogeneity are almost the same after all rounds.

D. Problem Statement

In traditional S-box substitution methods, information within highly auto-correlated regions is not adequately concealed, i.e., the areas where pixel values are identical, such as sharp edges in an image. The fact that edges remain highly visible raises significant security concerns about the effectiveness of such substitution methods.

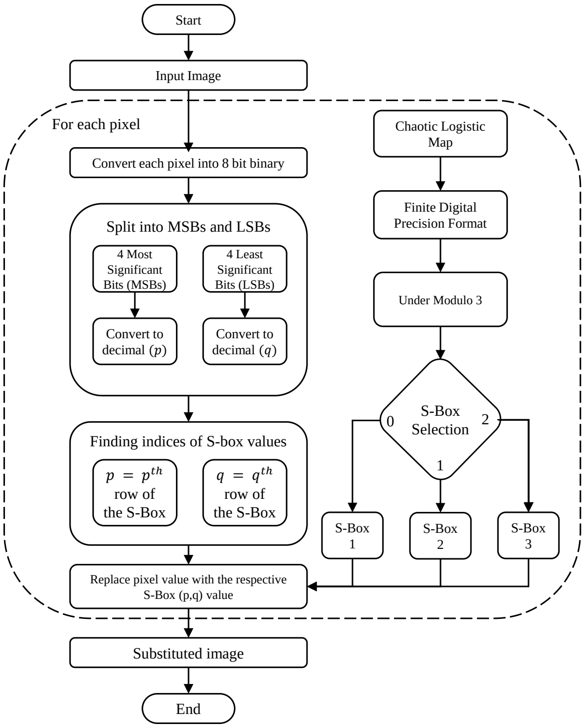

Start
Input Image
For each pixel
Convert each pixel into 8 bit binary
Split into MSBs and LSBs
4 Most Significant Bits (MSBs)
4 Least Significant Bits (LSBs)
Convert to decimal (p)
Convert to decimal (q)
Finding indices of S-box values
$p = p^{th}$ row of the S-Box
$q = q^{th}$ row of the S-Box
Chaotic Logistic Map
Finite Digital Precision Format
Under Modulo 3
S-Box Selection
0
1
2
S-Box 1
S-Box 2
S-Box 3
Replace pixel value with the respective S-Box (p,q) value
Substituted image
End

Fig. 5: Multiple S-Box Chaotic Substitution Algorithm.

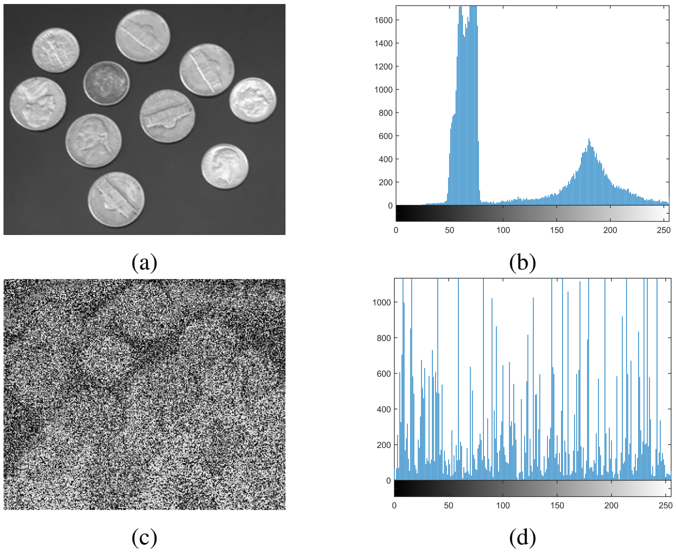
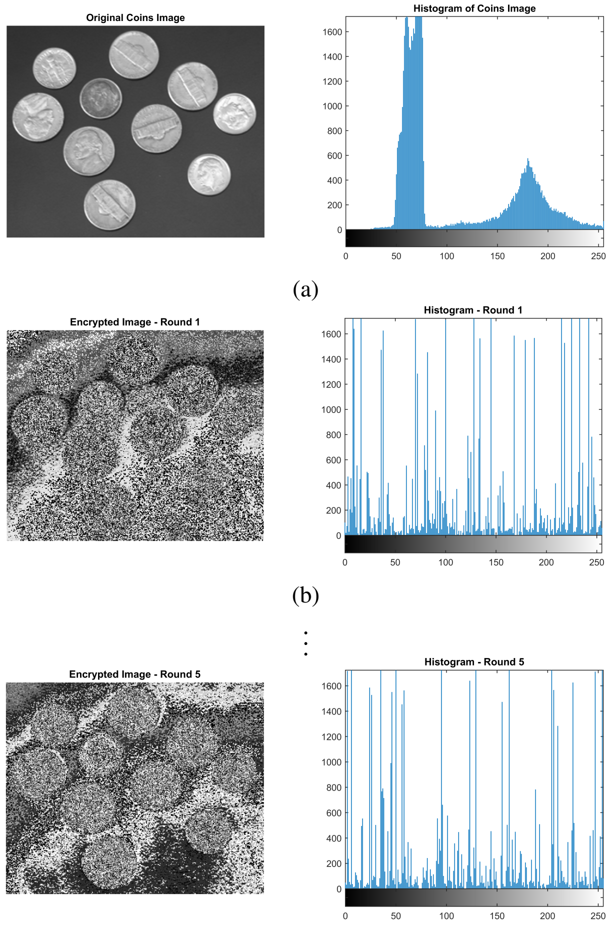


Fig. 6: Multiple s-box substitution results; (a-b) Coins image with its histogram, (c-d) Encrypted Coins image with its histogram.

This paper focuses on creating a substitution method based on a single round and single S-box that effectively scrambles the pixels of a plaintext image, eliminating the need for multiple rounds and S-boxes. Such methods are advantageous in applications demanding low computational complexity and



(a)

(b)

⋮

(c)

Fig. 7: Results of multiple rounds substitution showing no significant improvement; (a) Plaintext image, (b-c) Rounds 1 to 5.

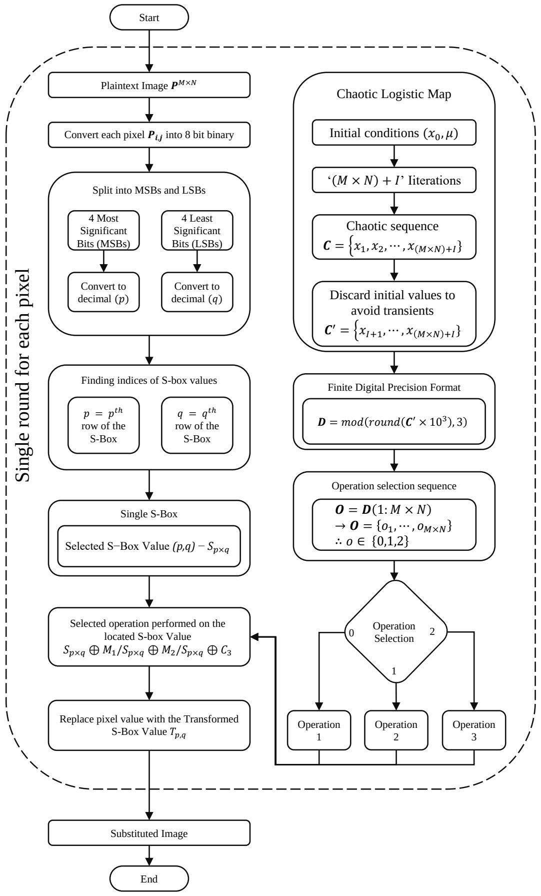

Start
Single round for each pixel
Plaintext Image $P^{M \times N}$
Convert each pixel $P_{i,j}$ into 8 bit binary
Split into MSBs and LSBs
4 Most Significant Bits (MSBs)
4 Least Significant Bits (LSBs)
Convert to decimal (p)
Convert to decimal (q)
Finding indices of S-box values
$p = p^{th}$ row of the S-Box
$q = q^{th}$ row of the S-Box
Single S-Box
Selected S−Box Value $(p,q) - S_{p \times q}$
Selected operation performed on the located S-box Value
$S_{p \times q} \oplus M_1 / S_{p \times q} \oplus M_2 / S_{p \times q} \oplus C_3$
Replace pixel value with the Transformed S-Box Value $T_{p,q}$
Chaotic Logistic Map
Initial conditions (x_0, μ)
'$(M \times N) + I$' Iterations
Chaotic sequence
$C = \{x_1, x_2, \cdots, x_{(M \times N)+I}\}$
Discard initial values to avoid transients
$C' = \{x_{I+1}, \cdots, x_{(M \times N)+I}\}$
Finite Digital Precision Format
$D = mod(round(C' \times 10^3), 3)$
Operation selection sequence
$O = D(1{:}\, M \times N)$
$\rightarrow O = \{o_1, \cdots, o_{M \times N}\}$
$\therefore o \in \{0,1,2\}$
Operation Selection
0
1
2
Operation 1
Operation 2
Operation 3
Substituted Image
End

Fig. 8: SRSS –The proposed single-round single S-box encryption scheme.

faster encryption and decryption speeds.

III. The Proposed Encryption Scheme

The proposed encryption scheme utilizes a single S-box and only a single round of substitution. Each pixel value is replaced by a value from the S-box, but before substitution, it undergoes a randomly selected operation. The proposed scheme is explained in two parts: (a) SRSS - Single Round Single S-box Encryption Scheme, and (b) CROSS – Chaos-based Random Operation Selection System. The SRSS represents the entire encryption scheme. The CROSS, on the other hand, entails the random operation selection component of the scheme.

A. SRSS – Single-Round Single S-box Encryption Scheme

The complete steps involved in the proposed SRSS encryption scheme, depicted in Fig. 8, are as follows.

- **Step 1:** Input the plaintext image $P^{(M \times N)}$ – $M \times N$ denoting the dimension of the plaintext image. Also, initiate the secret keys for the chaotic map (μ, x_0), i.e., the control parameter and the initial condition, analyzed in Section 2.2.
- **Step 2:** Iterate the chaotic map equation '$(M \times N) + I$' times to generate a chaotic sequence $C = \{x_1, x_2, \cdots, x_{(M \times N)+I}\}$. Here, I is the number of initial iterations to be discarded to avoid transients.
- **Step 3:** Discard the initial I iterations to avoid transients and keep the last $M \times N$ values, i.e., $C' = \{x_{I+1}, \cdots, x_{(M \times N)+I}\}$.
- **Step 4:** The generated chaotic sequence C' has fractional values between 0 and 1. Apply finite digital format to convert these fractional values to a sequence of integers D, i.e., $D = \text{mod}(\text{round}(C' \times 10^3), 3)$.
- **Step 5:** The modulus 3 operation in Step 3 makes sure that the chaotic sequence contains the values 0, 1, and 2. This makes our operation selection sequence of $M \times N$ dimension, i.e., $O = D(1 : M \times N) \rightarrow O = \{o_1, \cdots, o_{M \times N}\}$ such that $o \in \{0, 1, 2\}$.
- **Step 6:** Convert each pixel of the plaintext image $P_{i,j}$ into 8-bit binary and split the 8-bit binary into two equal parts, making the first 4 bits the Most Significant Bits (MSBs) and the last 4 bits the Least Significant Bits (LSBs).
- **Step 7:** To find the indices of the S-box values, which will replace the pixel of the plaintext image, convert the MSBs to decimal p and LSBs to decimal q. p corresponds

TABLE I: Statistical Security Analysis of Multiple Rounds Substitution

Security Parameter		**Round 1**	**Round 2**	**Round 3**	**Round 4**	**Round 5**
	Entropy	6.316	6.316	6.316	6.316	6.316
GLCM	Contrast	10.57	7.89	10.63	8.41	9.32
	Correlation	0.144	0.199	0.126	0.194	0.250
	Energy	0.025	0.025	0.037	0.025	0.032
	Homogeneity	0.48	0.51	0.51	0.51	0.52

to the row number of the S-box and q corresponds to the column number of the S-box, locating the S-box value $S_{p,q}$.

- **Step 8:** The operation selection sequence O containing values 0, 1, and 2, selects one of the three operations to be performed on the selected S-box value $S_{p,q}$. 0 selects Operation 1, 1 selects Operation 2, and 2 selects Operation 3. This selection is random based on the value in the operation selection sequence O.
- **Step 9:** The selected operation is performed on the selected S-box value $S_{p,q}$ and converts it into a new transformed value $T_{p,q}$. This transformed value then replaces the original pixel $P_{i,j}$ in the plaintext image.

B. CROSS – Chaos-based Random Operation Selection System

The Chaos-based Random Operation Selection System makes sure that every time for each pixel, a random operation is selected from the three operations. The operation selection sequence O is generated via a chaotic logistic map and contains random values of 0, 1, and 2. 0 corresponds to operation 1, 1 corresponds to operation 2, and 2 corresponds to operation 3. For the sake of simplicity, the operation chosen for all three operations is Bit X-OR. Three modifier constants or CROSS- secret keys, i.e., M_1, M_2 and M_3 are chosen. M_1, M_2, and $M_3 \in \{0, \ldots, 255\}$. In operation 1, the selected S-box value is first Bit XORed with M_1 before replacing the original pixel value of the plaintext image, similarly, in operations 2 and 3, the selected S-box value is bit XORed with M_2 and M_3, respectively. The designed chaos-based random operation selection system is given in Fig. 9.

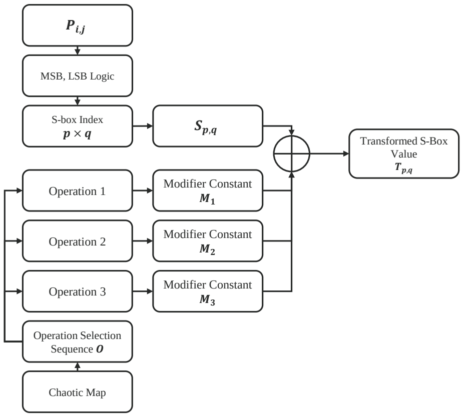


Fig. 9: CROSS – The proposed chaos-based random operation selection system.

IV. Results of the proposed SRSS scheme

A. Encryption Results of the Proposed Encryption Scheme

The proposed SRSS exhibited effective confusion of the plaintext image in just one round. The random selection of operations performed on the selected S-box values ensured that no edges are visible and all pixels have been replaced with several distinct values. The SRSS encrypted image with its histogram is given in Fig. 10. Furthermore, the results of the statistical security analysis given in Table 2 showing close to ideal values of entropy and correlation also validated the effectiveness of the proposed encryption scheme.

B. Comparison with Multiple S-boxes and Multiple Rounds Algorithm

When compared with the results of substitution methods under study, the proposed scheme exhibited considerably good security performance. It is evident from Fig. 11 that the proposed SRSS encryption scheme encrypts the plaintext image more effectively as compared to the round 5 encrypted image of the multiple s-box system.

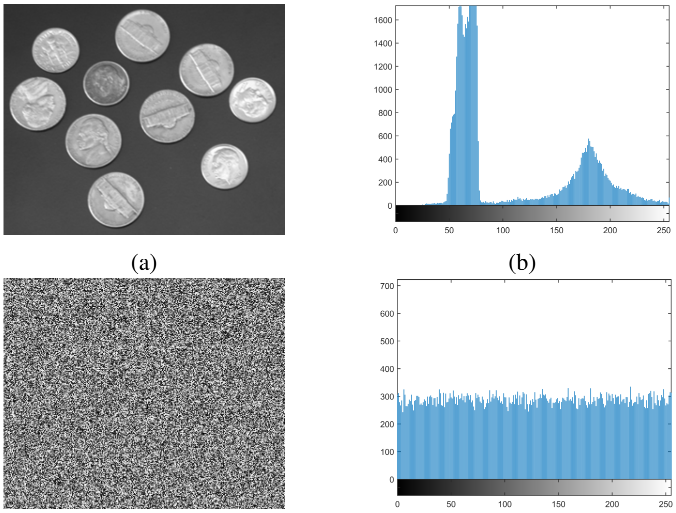
V. Conclusion

To resolve the security, latency, and computational concerns associated with traditional S-box substitution methods, this paper addressed some inherent security vulnerabilities in three types of S-box substitution methods, especially when dealing with images that have highly auto-correlated pixels and lower gray scales. Furthermore, to resolve the highlighted security concerns, this paper proposed a robust Single Round Single S-Box (SRSS) encryption scheme that simplifies the encryption process while enhancing its security efficacy. In addition to the proposed SRSS, this paper introduced a new Chaos-based Random Operation Selection System (CROSS), a mechanism designed to reduce the complexity of the encryption scheme by negating the need for multiple S-boxes. The new methods demonstrated their potency by outperforming the existing substitution methods in terms of statistical security analysis.

TABLE II: Statistical Security Analysis of the Proposed SRSS encryption scheme

Security Parameter		**Single Round**
	Entropy	7.989
GLCM	Contrast	10.45
	Correlation	0.0007
	Energy	0.015
	Homogeneity	0.389

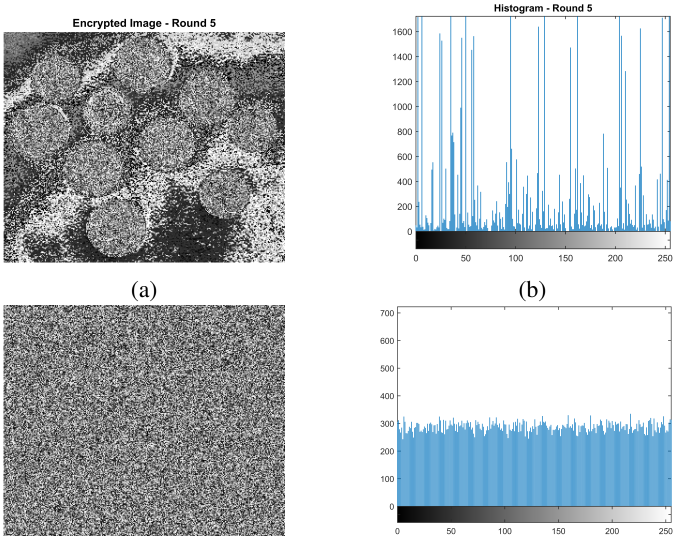
The SRSS and CROSS collectively achieved near-ideal results with an entropy of 7.989 and a correlation coefficient of 0.007, thus substantiating their effectiveness.



(a) (b)

(c) (d)

Fig. 10: Results of the proposed SRSS encryption scheme; (a-b) Coins image and its histogram, (c-d) SRSS Encrypted Coins image and its histogram.



(a) (b)

(c) (d)

Fig. 11: . Comparison of the proposed SRSS encryption scheme; (a-b) Multiple rounds encrypted image and its Histogram, (c-d) The SRSS encrypted image and its Histogram.

REFERENCES

[1] F. Ahmed, M. U. Rehman, J. Ahmad, M. S. Khan, W. Boulila, G. Srivastava, J. C.-W. Lin, and W. J. Buchanan, "A dna based colour image encryption scheme using a convolutional autoencoder," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 19, 11 2022.

[2] A. K. Sahu, K. Umachandran, V. D. Biradar, O. Comfort, V. Sri Vigna Hema, F. Odimegwu, and S. M. A, "A study on content tampering in multimedia watermarking," *SN Computer Science*, vol. 4, 02 2023.

[3] M. K. Younes and A. Jantan, "Image encryption using block-based transformation algorithm," *IAENG International Journal of Computer Science*, vol. 35, 01 2008.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 10 1949.

[5] J. Ahmad and S. J. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools and Applications*, vol. 75, pp. 13 951–13 976, 10 2015.

[6] S. Zhu and C. Zhu, "A new image compression-encryption scheme based on compressive sensing and cyclic shift," *Multimedia Tools and Applications*, vol. 78, pp. 20 855–20 875, 08 2019.

[7] X. Wang, M. Zhao, S. Feng, and X. Chen, "An image encryption scheme using bit-plane cross-diffusion and spatiotemporal chaos system with nonlinear perturbation," *Soft Computing*, vol. 27, pp. 1223–1240, 01 2023.

[8] H. Ming, H. Hu, F. Lv, and R. Yu, "A high-performance hybrid random number generator based on a nondegenerate coupled chaos and its practical implementation," *Nonlinear Dynamics*, vol. 111, pp. 847–869, 09 2022.

[9] R. Li, T. Lu, H. Wang, J. Zhou, X. Ding, and Y. Li, "The ergodicity and sensitivity of nonautonomous discrete dynamical systems," *Mathematics*, vol. 11, p. 1384, 01 2023. [Online]. Available: https://www.mdpi.com/2227-7390/11/6/1384

[10] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu, and J. Liu, "A novel block encryption algorithm based on chaotic s-box for wireless sensor network," *IEEE Access*, vol. 7, p. 53079–53090, 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8691876

[11] H. Liu, A. Kadir, X. Sun, and Y. Li, "Chaos based adaptive double-image encryption scheme using hash function and s-boxes," *Multimedia Tools and Applications*, vol. 77, pp. 1391–1407, 01 2017.

[12] J. Chen, Z. Zhu, L. Zhang, Y. Zhang, and B. Yang, "Exploiting self-adaptive permutation–diffusion and dna random encoding for secure and efficient image encryption," *Signal Processing*, vol. 142, pp. 340–353, 01 2018.

[13] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, pp. 3106–3118, 09 2014.

[14] J. Ahmad and S. J. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dynamics*, vol. 82, pp. 1839–1850, 07 2015.

[15] A. Shafique and J. Ahmed, "Dynamic substitution based encryption algorithm for highly correlated data," *Multidimensional Systems and Signal Processing*, vol. 32, p. 91–114, 05 2020.

[16] M. Khan, "A novel image encryption scheme based on multiple chaotic s-boxes," *Nonlinear Dynamics*, vol. 82, pp. 527–533, 05 2015.

[17] X. Wang and Q. Wang, "A novel image encryption algorithm based on dynamic s-boxes constructed by chaos," *Nonlinear Dynamics*, vol. 75, pp. 567–576, 10 2013.

[18] I. Hussain, A. Anees, A. H. Alkhaldi, M. Aslam, N. A. Siddiqui, and R. Ahmed, "Image encryption based on chebyshev chaotic map and s8 s-boxes," *Optica Applicata*, vol. 49, 01 2019.

[19] X. Zhang, R. Guo, H.-W. Chen, Z. Zhao, and J. Wang, "Efficient image encryption scheme with synchronous substitution and diffusion based on double s-boxes," *Chinese Physics B*, vol. 27, pp. 080 701–080 701, 08 2018.

[20] Zhu, Wang, and Zhu, "A secure and fast image encryption scheme based on double chaotic s-boxes," *Entropy*, vol. 21, p. 790, 08 2019.

[21] X. Wang, Ünal Çavuşoğlu, S. Kaçar, A. Akgul, V.-T. Pham, S. Jafari, F. E. Alsaadi, and X. V. Nguyen, "S-box based image encryption application using a chaotic system without equilibrium," *applied sciences*, vol. 9, pp. 781–781, 02 2019.

[22] Y. Zhou, L. Bao, and C. P. Chen, "A new 1d chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 04 2014.

[23] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, pp. 29–37, 01 2012.

[24] A. Ullah, S. S. Jamal, and T. Shah, "A novel scheme for image encryption using substitution box and chaotic system," *Nonlinear Dynamics*, vol. 91, pp. 359–370, 10 2017.