Residue Number System Based S-box Generation and its Applications in AES for Image Encryption

Arun Upadhyaya, C. Shantharama Rai, and Ganesh Aithal

***Abstract*- It is now more crucial than ever to provide data security, as the goals and capabilities of eavesdroppers are constantly changing. Therefore, different developers are creating cipher systems that employ various innovative techniques. Standard ciphers, such as DES and AES, use substitution boxes to ensure secure encryption and decryption of data. The substitution box (S-box) is a core module used in modern ciphers to secure data. This study introduces an efficient and straightforward method that leverages a Residue Number System (RNS) to construct an S-box. Furthermore, the AES algorithm uses the generated S-box to encrypt digital images. Parameters such as entropy, NPCR, and UACI effectively measure the security of the proposed method. The results of the performance and comparison study confirm that the proposed S-box outperforms existing methods, establishing it as a strong candidate for cryptographic use in various image security applications.**

***Index terms*-RNS, S-box, AES, Image encryption, Security analysis.**

1. Introduction

TODAY, data, and information transmission play vital roles in everyday activities and in businesses that need to communicate online. Currently, secure communication via public networks is a top priority for any organization. The need to protect data and information resources from unwanted access has significantly increased. Recently, there has been a notable increase in network security incidents [1]. When data is stored in shared networks, the necessity of safeguarding systems, data, and information increases [2]. To protect this data, it is necessary to employ cryptographic techniques that can safeguard sensitive data and information shared via networks. Since hackers attempted to breach security, several standard cryptographic methods have been developed and used to safeguard data and information [3].

Manuscript received February 04, 2024; revised August 21, 2024.

Arun Upadhyaya is an assistant professor in the department of Electronics and Communication, Shri Madhwa Vadiraja Institute of Technology and Management, Bantakal, Udupi, and a research scholar in the A J Institute of Engineering and Technology, Kottara, Mangalore affiliated to Visvesaraya Technological University, Belagavi – 590018, India (+91-968-632-3734: E-mail: arunsse2012@gmail.com).

C. Shantharama Rai is a professor and the principal in the A J Institute of Engineering and Technology, Kottara, Mangalore, affiliated to Visvesaraya Technological University, Belagavi – 590018, India (E-mail: csraicec@gmail.com).

Ganesh Aithal is a professor and vice principal in the Shri Madhwa Vadiraja Institute of Technology and Management, Bantakal, Udupi, affiliated to Visvesaraya Technological University, Belagavi – 590018, India (E-mail: ganeshaithal@gmail.com).

Users can safely share their data across an insecure network using encryption.

Block ciphers have emerged as the most efficient means of safeguarding sensitive data in contemporary cryptography. [4]. Distinct block ciphers include the Advanced Encryption Standard (AES), RC5, and Data Encryption Standard (DES). Permutation and substitution are the two important steps that these ciphers use to convert data into an unrecognizable form. The permutation operation replaces one set of bits or bytes in plaintext with another set. The substitution process, on the other hand, replaces one nonlinear data block with another. The substitution table, often referred to as the substitution box (S-box), replaces the data [5] with a new set of values, enhancing the security and confidentiality of the information. In modern block ciphers, an S-box is an essential component that helps generate a scrambled ciphertext for a given plaintext. To provide attackers with more confusion, an S-box creates a nonlinear relationship between the plaintext and ciphertext [6] - [8].

As confusion increases in the ciphertext, the strength of the cipher also increases. This means that a block cipher that uses an S-box has a cryptographic strength determined by the strength of the S-box. Researchers have conducted numerous studies on high-quality S-boxes, and the Advanced Encryption Standard (AES) is one of the most popular symmetric block ciphers that utilize the S-box. To construct AES S-box values, one must compute the multiplicative inverse of each value between 0 and 255 using the Galois Field [9]. The use of the Galois Field makes the calculation of the multiplicative inverse quite complicated and requires more time. Consequently, the S-box design is complex and computationally inefficient. Researchers in [10]–[11] enhanced the security offered by AES in several ways, while also improving the original AES S-box. The new cipher proposed by Sahmoud et al. [12] is faster and more complex than AES and uses multiple subkeys for the encryption of distinct plaintext blocks. Linear fractional transformation (LFT) is a popular algebraic concept used to build robust and dynamic S-boxes. The LFT approach was the foundation employed by the authors in [13] to create a reliable and efficient S-box. The majority of S-boxes created with LFT use Galois Field (GF) arithmetic, greatly improving the S-box production process. The authors proposed effective ways to construct S-boxes in addition to the LFT techniques. For example, the authors of [14] developed a method that employs the concept of cubic fractional transformation (CFT) to generate good S-boxes. This transformation yields robust S-boxes and is both

straightforward and highly effective. Chaotic maps have recently gained significant practicality in the creation of innovative S-boxes for secure communication [15]–[18]. Using a chaotic map-based logistic sine system (LSS)-based S-box, Qing et al. [19] presented a secure and effective image encryption technique. This chaotic map offers better features and a greater variety of chaos. S-box design techniques depend substantially on chaotic maps, yet these maps have significant drawbacks [20]. This paper describes an effective approach for building an S-box using the RNS method to address the aforementioned issues. Compared with alternative approaches, the RNS method has the following advantages: 1) low computational complexity for generating the S-box and 2) enhanced security parameters. This study provides a detailed analysis of the RNS dynamics. The results of the experiments and simulations demonstrate that the proposed method performs fairly well in terms of security.

The structure of the rest of the paper is as follows: Section 2 presents the RNS algorithm. Section 3 illustrates the construction of the proposed S-box design. Section 4 presents the implementation of the S-box in the AES algorithm. Section 5 illustrates the experimental findings, performance analysis, and specifics of the proposed AES image encryption technique using the proposed S-box and standard S-box. Section 5 presents the conclusion.

II. MATHEMATICAL BACKGROUND TO RESIDUE NUMBER SYSTEM

Unweighted number systems such as RNS offer advantages such as low power consumption, secure communications, cryptography, and parallel computations for tasks encompassing addition, subtraction, and multiplication across a spectrum of integers. High speed, power savings, reduced complexity, error detection, and corrections are some of the benefits of using RNS [21–22]. To represent a large integer more efficiently and quickly, RNS [23] uses a set of smaller integers. Sun Tsu Suan-Ching [24] introduced the mathematical concepts of the modular roots, which forms the basis for the functioning of the Chinese remainder theorem (CRT). The residue number system considers independent moduli. Each modulus residue represents an integer and, performs arithmetic operations based on the individual residue values. The residue number system enables performing arithmetic operations independently on different moduli, thus avoiding time consuming carry propagation in addition, subtraction, and multiplication.

This study addresses the implementation of building blocks for applications in cryptography based on the residue number system. A set of relatively prime moduli with N integer constants defines the residue number system

$$\{m_1, m_2, m_3, \ldots\ldots m_N\} \quad (1)$$

i.e. GCD $(m_i, m_j) = 1$ for $i \neq j$. Let M represent the least common multiple of all m_i. The stated residue number system allows the representation of every arbitrary integer X lower than M as a set of N smaller integers.

$$\{x_1, x_2, x_3, \ldots\ldots x_N\} \quad (2)$$

With each x_i

$$x_i = X \bmod m_i \quad (3)$$

represents the residue class of X in that modulus.

For unsigned numbers, the residue number system may represent any number between [0, M].

Where

$$M = \prod_{i=1}^{N} m_i \quad (4)$$

and is known as the dynamic range. All moduli must be co-primed to achieve the highest dynamic range; no modulus may have a common factor with any other modulus.

TABLE I
RESIDUE REPRESENTATION OF INTEGERS WITH TWO MODULI SETS

X	Moduli {1, 3, 5}			Moduli {1, 3, 6}		
	1	3	5	1	3	6
0	0	0	0	0	0	0
1	0	1	1	0	1	1
2	0	2	2	0	2	2
3	0	0	3	0	0	3
4	0	1	4	0	1	4
5	0	2	0	0	2	5
6	0	0	1	0	0	0
7	0	1	2	0	1	1
8	0	2	3	0	2	2
9	0	0	4	0	0	3
10	0	1	0	0	1	4
11	0	2	1	0	2	5
12	0	0	2	0	0	0
13	0	1	3	0	1	1
14	0	2	4	0	2	2

Table I illustrates the representation of integers in the residue format with two distinct residue systems. Let us consider two alternative modulus sets, {1, 3, 5} and {1, 3, 6}, as an example. Assuming that the moduli set {1, 3, 5} is relatively prime, the dynamic range of the system in the first example spans from 0 to 14. This range contains a unique representation of the integer residues. On the other hand, the moduli set {1, 3, 6} in example 2 is not relatively prime because {3} is the common divisor of 3 and 6. As a result, the range from 0 to 5 is the only range in which the integer representation of residues is unique. Thus, to obtain a higher dynamic range, the modulus values in the moduli set must be a relatively prime.

Consider a co-prime modulus set (m_1, m_2) with a dynamic range $(m_1 \times m_2 = M)$. Let $\langle x_1, x_2 \rangle$ is the RNS representation of the integers in this range where $0 \leq x_1 < m_1$ and $0 \leq x_2 <$

m_2. RNS represents numbers between 0 and *M-1* uniformly across ranges, where

$$x_1 = X \; mod \; m_1 \tag{5}$$

and

$$x_2 = X \; mod \; m_2 \tag{6}$$

For example, let us consider that M = 255. The number 255 can be represented in terms of its moduli as (15, 17), (3, 5, 17), (51, 5) and so on. Let X = 146 and the moduli be (15, 17). We can represent this number in the RNS as

$x_1 = 146 \; mod \; 15$ = 11, in addition,

$x_2 = 146 \; mod \; 17$ = 10

Hence, the residue represents 146 as 146 = {11, 10}.

III. Construction of an S-Box for AES using the RNS method

The AES algorithm requires an $16x16$ S-box with integers 0-255 arranged in random order according to the proposed method, M = 255 produces 255 numbers. The coprime moduli set for 255 are {17, 15}, {17, 3, 5}, and {51, 5}, or permutations of these moduli. The proposed method obtains the S-box by generating all residues of numbers ranging from 0 to 255 with moduli of {51, 5}. Equation 7 obtains the equivalent decimal number on the basis of residue value.

$$Y = [(x_2 \times 10^1 + x_1 \times 10^0)] mod \; 255 \tag{7}$$

Modulus {51, 5} specifically generates the numbers 0 to 255 required for the AES S-box uniquely, unlike the other moduli. The generated decimal values Y consist of only 0 to 254 unique numbers with a repetition of 0. To restrict the numbers to within 255, consider modulo 255, this will generate all the numbers except 255. This is because, for X = 0 and 255, the residues obtained are the same that is. {0, 0}. These residues yield a result of 0 when used in equation 7. Fig. 1 illustrates an example of the operation in moduli {51, 5}. The residues obtained in the RNS format are X = {32, 4}, assuming input X = 134. Equation 7 transforms the RNS digits, treating them as decimal digits, into an equivalent decimal integer. This produces an S-box value of 69.

Fig.2 illustrates the systematic procedure for actively generating the proposed S-box using coprime moduli. Table II shows the generated S-box for the prime moduli {51, 5}. The proposed method inserts 255 as the final value as shown in Table II. The sequence obtained is also random and has the required nonlinearity for the S-box.

IV. Implementation of the S-Box in AES based on the Residue number system

This study uses two distinct approaches for image encryption. The first method generates the S-box using

RNS, while the second method utilizes the rows of both the standard S-box and the ones obtained from the RNS to derive the S-box. In the first case, the AES algorithm in the SubByte round uses the generated RNS S-box, which is a 16×16 square matrix, as shown in Table II.

The experiment in the second case uses AES with the hybrid S-box, which combines the 8×16 matrix of the standard S-box and selects another 8×16 matrix from the RNS method. The obtained result is compared with the encryption performed using the standard S-box employed in the AES algorithm. The next section presents a discussion of the results obtained using these methods.

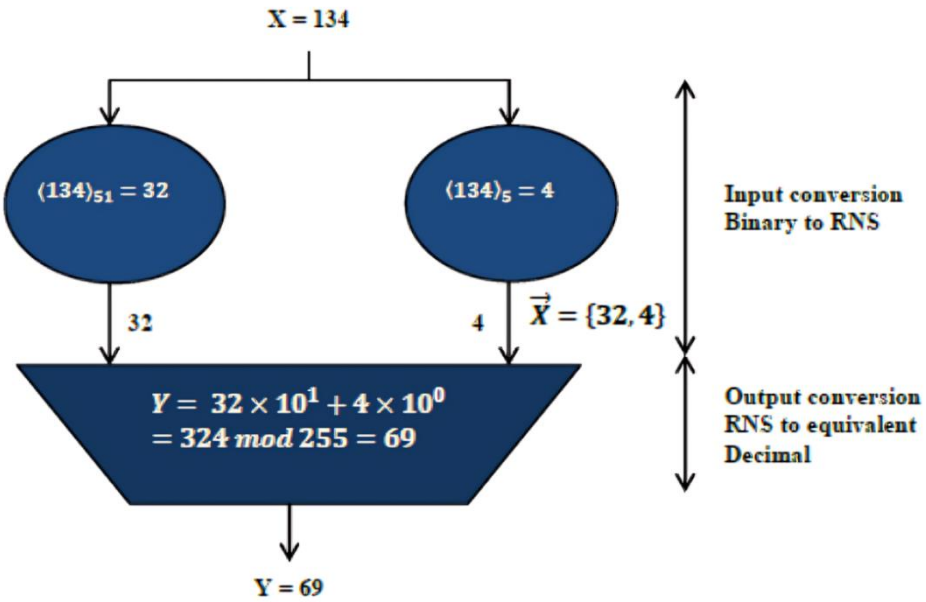


Fig. 1. RNS operations for m = {51, 5}.

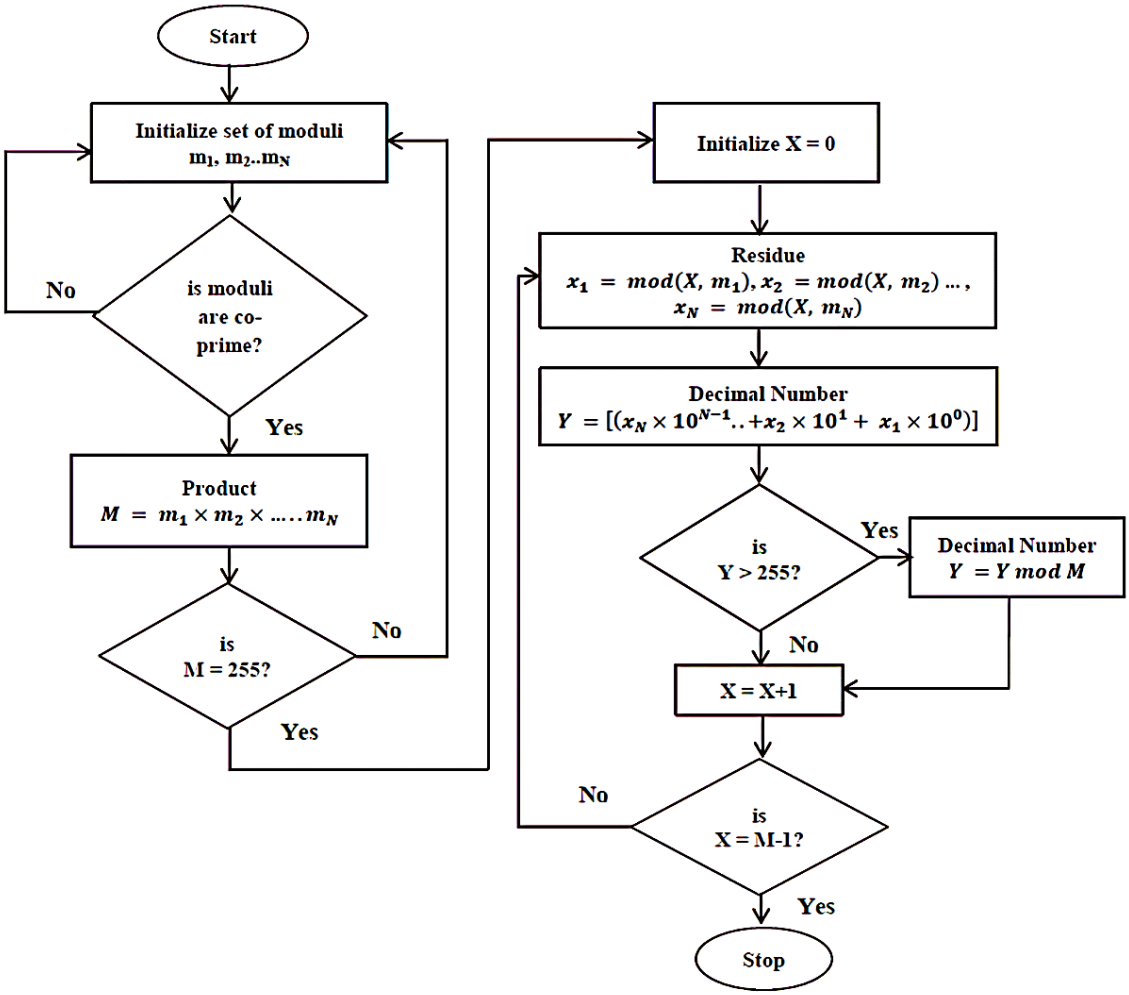


Fig. 2. Flowchart of the preliminary S-box generation.

TABLE II
GENERATED S-BOX USING RNS FOR AES ALGORITHM

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

V. Security analysis

An efficient encryption method has desirable qualities that are resistant to known attacks using cryptographic procedures. Researchers can use a wide range of security parameters to conduct thorough security assessments. This includes a histogram of the number of occurrences of a pixel, entropy, number of pixel change rate (NPCR), and unified average changing rates (UACI), mean square error (MSE), mean absolute difference (MAD), and peak signal-to-noise ratio (PSNR). The next section explains the use of 256×256 standard colour images of Barbara, Baboon and, Pepper for this analysis.

A. Visual Analysis

Fig. 3 shows the results obtained using the AES algorithm. Fig. 3(a) shows the plain images and, Fig. 3(b) shows the encrypted images generated using the standard S-box for the AES algorithm. Fig. 3 (c) and 3(d) shows the results for the RNS S-box and, the hybrid S-box, respectively. The pixels in all these images scatter randomly without leaving any traces of the plane image.

B. Histogram Analysis

The image histogram displays the frequency of the occurrence of pixel values in both the plain and encrypted images. If this distribution of the encrypted image is uniform, it is more resistant to statistical attacks [25].

Fig. 4(a) shows the number of occurrences of a pixel in the plain image of Barbara. Fig. 4(b), 4(c), and 4(d) are the histograms of occurrences of the number of pixels of the plain images encrypted using the standard, RNS and the hybrid S-box for Barbara image, respectively.

Consequently, RNS S-box encryption demonstrates equal strength against statistical attacks. The analysis indicates that the distribution of pixels in the histograms of encrypted images is uniform, thereby resisting statistical attacks.

Fig. 4(d) illustrates the histogram of encrypted images using the hybrid S-box derived from a combination of the S-box from standard AES and RNS. Here, the repetition of integers in the S-box causes the distribution to be nonuniform. Fig. 5 and Fig. 6 demonstrate similar results for the Baboon and Peppers images.

C. Entropy Analysis

Entropy, as defined in [26], evaluates the randomness or uncertainty of encrypted data by quantifying the level of unpredictability in the information. This is stated as

$$H(x) = -\sum_{0}^{255} P(x_i) log_2 P(x_i) \tag{8}$$

where X is a set of pixel values of the image; $x_i \in X$; The probability of x_i occurring in the image is expressed as $P(x_i)$. If a grayscale image has 8 bits with values ranging from 0 to 255, then the image's bit count is eight, and its maximum entropy is $H(x) = 8$ [27]. This method converts the color image to grayscale and then computes the entropy. Table III presents a comparison between the proposed method's entropy and that of the conventional approach and several recent studies. It is evident from the table that both approaches are close to achieving maximum entropy, which shows that the proposed method is robust.

D. NPCR and UACI

NPCR and UACI are two cryptanalysis techniques used to assess the resistance of encryption techniques against differential attacks. Researchers use differential analysis to assess the resilience of the proposed encryption method by actively altering one bit in the encryption key and analyzing its impact on the security of the system [28]. A comparison of the cipher image generated by changing one bit of the key with the image obtained with the original key can indicate significant differences in the pixel values. Let us denote the resulting equivalent ciphertext images as I_1 and I_2, respectively. We can compute the above parameters [29] using equations (9) and (11).

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(x,y) \times 100\% \tag{9}$$

where

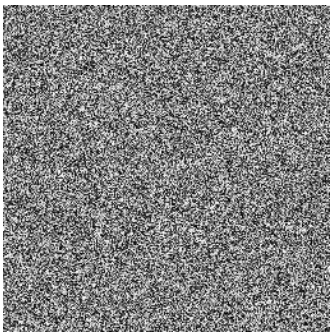
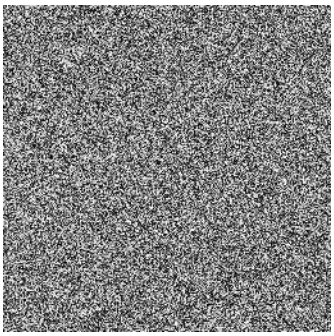
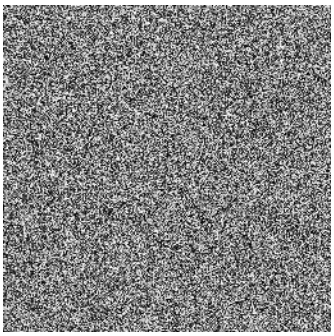
$$D(x,y) = \begin{cases} 0, if\ I_1(x,y) = I_2(x,y) \\ 1, if\ I_1(x,y) \neq I_2(x,y) \end{cases} \tag{10}$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|I_1(x,y) - I_2(x,y)|}{255} \times 100\% \tag{11}$$

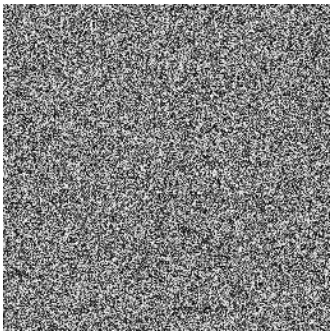
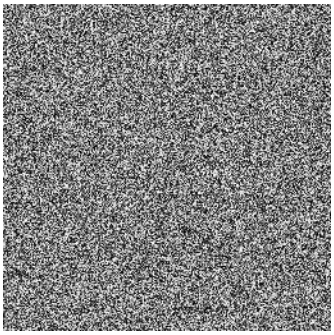
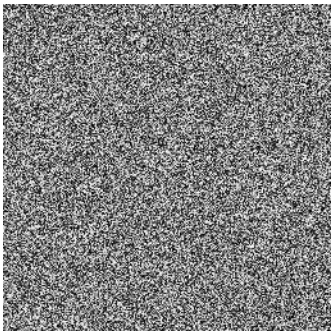
The pixel value of point (x,y) is represented in the two ciphertext images as $I_1(x,y)$ and $I_2(x,y)$ and $M \times N$ indicates the size of the image. The NPCR method identifies the relationship between the original and encrypted images. UACI defines the average density between the two images. Obtain the $D(x,y)$ matrix from (10) and use it in (9) to compute the NPCR. When comparing pixel values at the same position in the two matrices, if they are equal, the corresponding entry is 0; otherwise, it is 1. This process determines the NPCR value. The optimal value of NPCR is 99.61% and, that of UACI is 33.46% [30]. Table IV and Table V compares the parameters produced by the proposed technique with those obtained by the standard method, along with a few references. The table demonstrates that the proposed technique has strong robustness against differential attacks and is rather close to the ideal values.



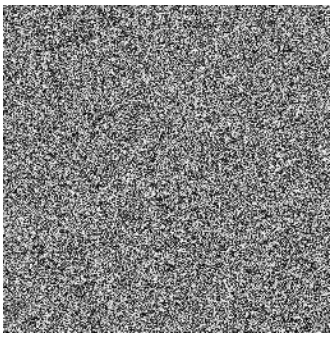
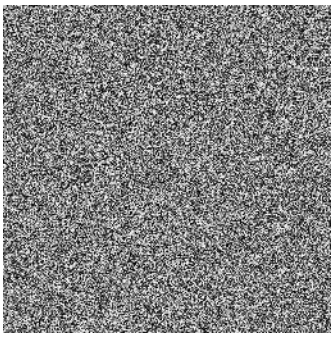
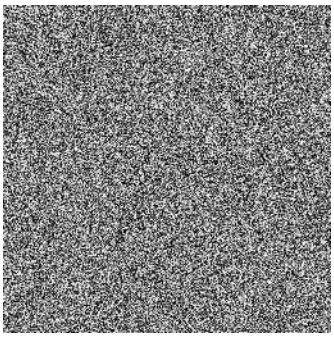
(a) Barbara, Baboon, and Pepper plain images

(b) Encrypted images using the original S-box

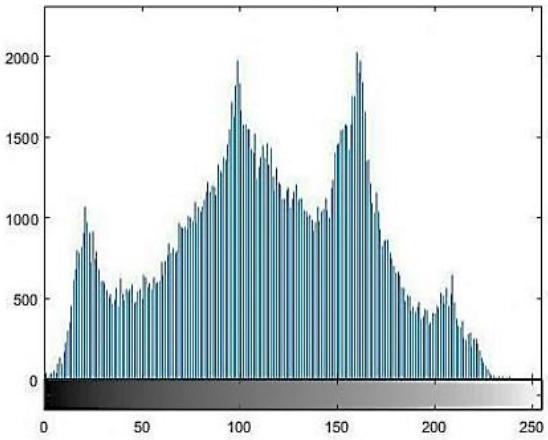




(c) Encrypted images using the RNS S-box

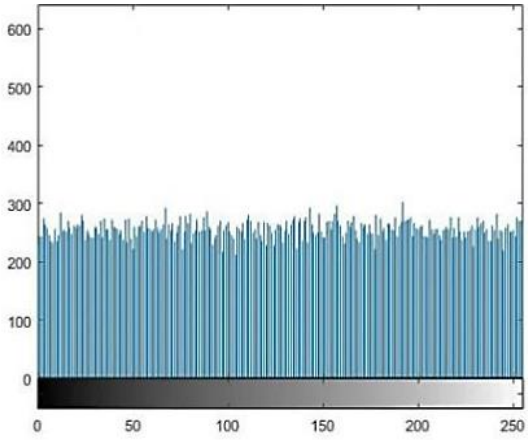




(d) Encrypted images using the hybrid S-box

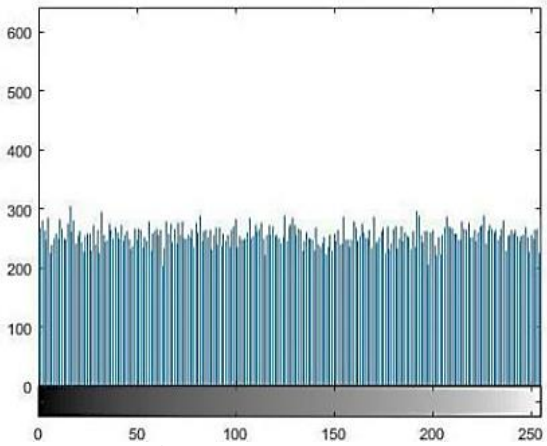
Fig. 3. Encrypted images using the AES algorithm



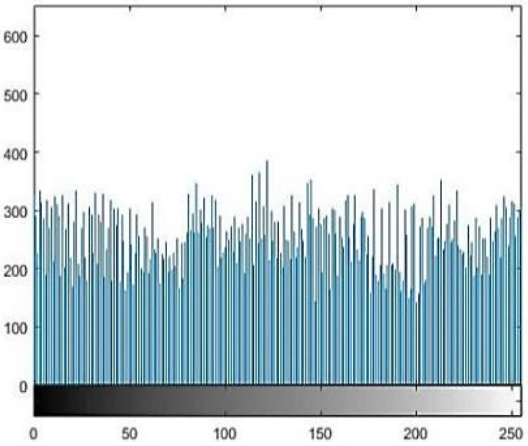
(a) Histogram of Barbara image



(b) Histogram of the encrypted image using original S-box

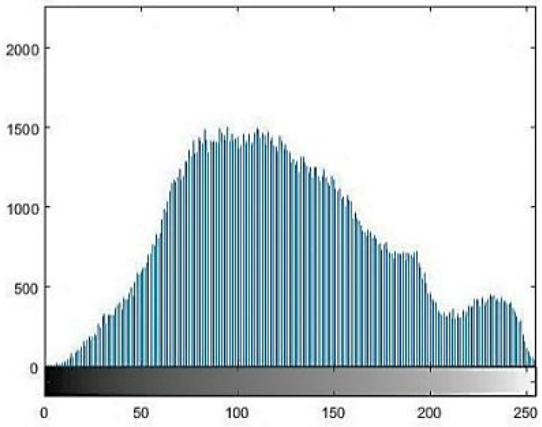


(c) Histogram of the encrypted image using RNS S-box

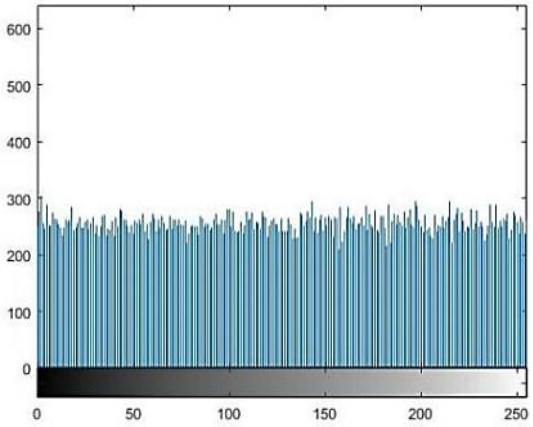


(d) Histogram of the encrypted image using hybrid S-box

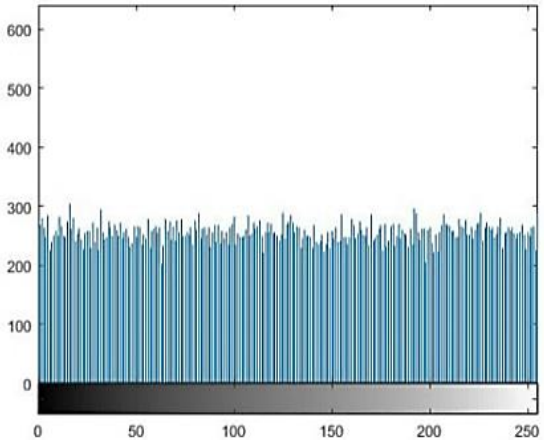
Fig. 4. Histogram of Barbara image and encrypted images



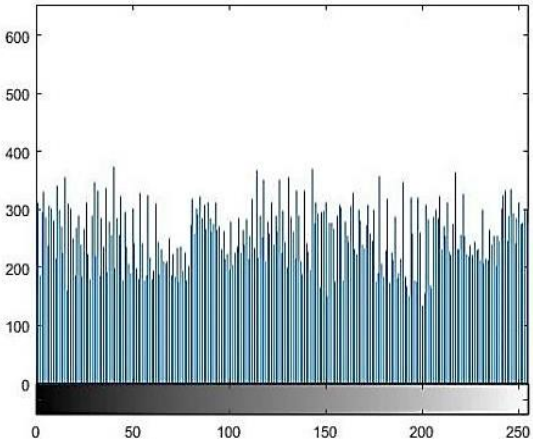
(a) Histogram of Baboon image



(b) Histogram of the encrypted image using original S-box

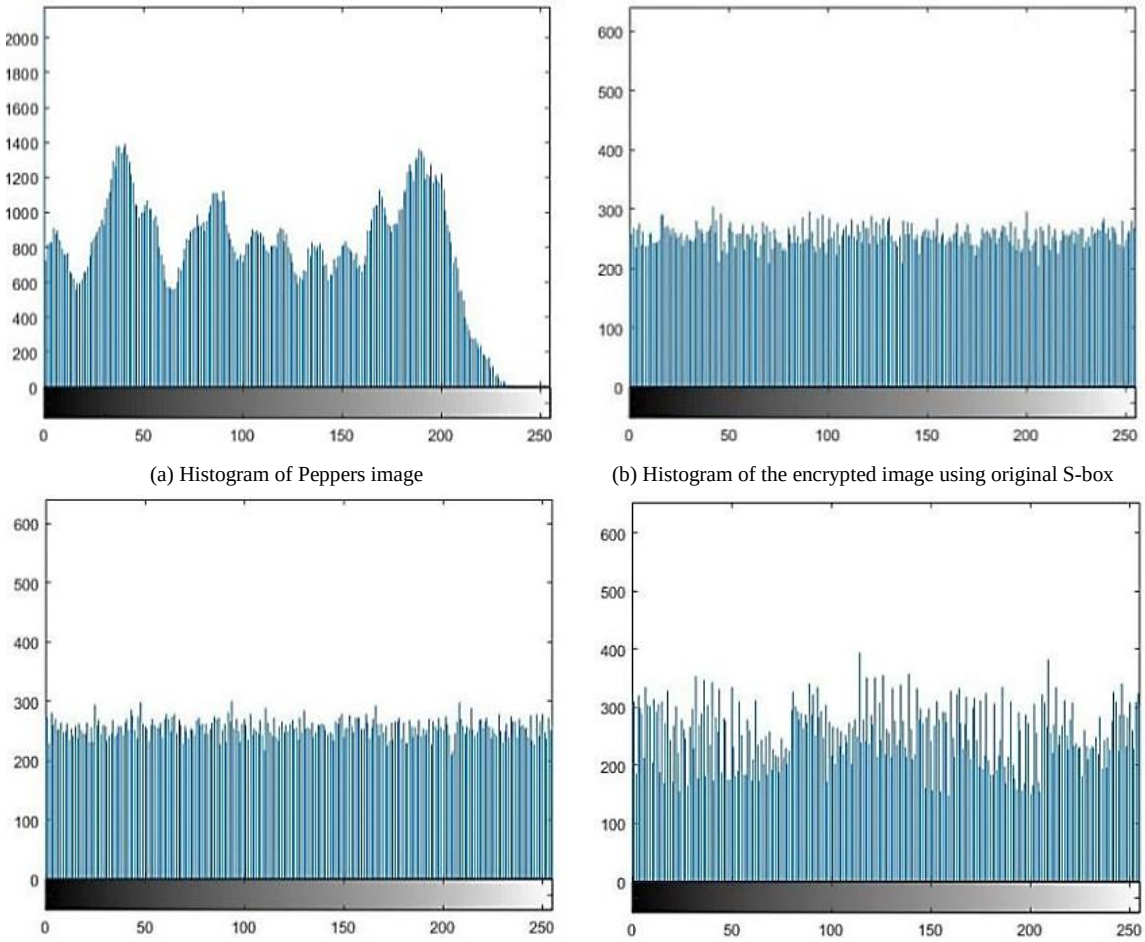


(c) Histogram of the encrypted image using RNS S-box



(d) Histogram of the encrypted image using hybrid S-box

Fig. 5. Histogram of Baboon image and encrypted images



(a) Histogram of Peppers image

(b) Histogram of the encrypted image using original S-box

(c) Histogram of the encrypted image using RNS S-box

(d) Histogram of the encrypted images using hybrid S-box

Fig. 6. Histogram of Peppers image and encrypted images

TABLE III
. COMPARISON OF INFORMATION ENTROPY BETWEEN DIFFERENT ENCRYPTION ALGORITHMS

Sr. No	Test Image	Entropy									
		Plain image	Original S-box	RNS S-box	Hybrid S-box	Ref. [7]	Ref. [18]	Ref. [38]	Ref. [41]	Ref. [42]	Ref. [43]
1	Barbara	7.4023	7.9344	7.9889	7.9662	7.9967	7.994	7.99964	-	-	7.9996
2	Baboon	7.67	7.9377	7.98892	7.9654	7.9973	7.995	7.99943	7.999238	7.9965	7.9994
3	Peppers	7.73	7.9368	7.98916	7.9649	7.9975	7.993	7.99945	7.999283	7.9966	7.9994

TABLE IV
NPCR WITH ONLY A ONE-BIT CHANGE IN THE KEY

Sr. No	Test Image	NPCR (%)						
		Original S-box	RNS S-box	Hybrid S-box	Ref. [18]	Ref. [38]	Ref. [41]	Ref. [43]
1	Barbara	99.42	99.62	99.53	99.6	99.62	-	99.622
2	Baboon	99.44	99.63	99.56	99.6	99.59	99.617	99.598
3	Peppers	99.43	99.61	99.49	99.2	99.602	99.606	99.602

TABLE V
UACI WITH ONLY A ONE-BIT CHANGE IN THE KEY

Sr. No	Test Image	UACI (%)						
		Original S-box	RNS S-box	Hybrid S-box	Ref. [18]	Ref. [38]	Ref. [41]	Ref. [43]
1	Barbara	29.4438	33.4999	33.75	33.6	33.45	-	33.45
2	Baboon	29.3745	33.3676	33.7473	33.6	33.35	33.492	33.354
3	Peppers	29.3111	33.3703	33.4793	33.3	33.453	.33452	33.453

E. Correlation analysis of the two adjacent pixels

In a plain image, adjacent pixels exhibit strong correlations in the horizontal (H), vertical (V), and diagonal (D) directions. To enhance resistance to statistical attacks, it is crucial to minimize the correlation between adjacent pixels in a ciphered image. Calculation of the correlation between plain and ciphered images involves the following steps. First, choose 3000 adjacent pairs of pixels at random from the image. Use the following equations to determine the correlation coefficient [31] – [34]:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(Y)}} \tag{12}$$

in this case, x and y re adjacent pixels

$$E(x) = \frac{1}{3000}\sum_{i=1}^{3000} x_i \tag{13}$$

$$D(x) = \frac{1}{3000}\sum_{i=1}^{3000}(x_i - E(x))^2 \tag{14}$$

$$cov(x,y) = \frac{1}{3000}\sum_{i=1}^{3000}(x_i - E(x))(y_i - E(y)) \tag{15}$$

Table VI presents the calculated correlation coefficients of the plain images Barbara, Baboon, and Pepper and their ciphered images using the proposed encryption algorithm. In all three directions, the correlation coefficients of the plain image are approximately 1, whereas those of the ciphered image are approximately 0. Thus, the proposed encryption scheme has excellent confusion and diffusion properties because the correlation between adjacent pixels is extremely low. Correlation quantifies the degree of connection between adjacent pixel values in an encrypted image, allowing us to determine the extent of the relationship between them. This provides information on how closely related the pixel values are to each other. In general, a plain image has pixel values distributed linearly. However, the encrypted image should have a nonlinear distribution.

Fig. 7(a) demonstrates that the pixel values in the original plain image of Barbara, exhibits a linear distribution in the three directions and inclines toward straight lines, providing strong evidence of their correlation.

Fig. 7(b) shows the pixel correlation of the standard AES method in all three directions. Fig. 7(c) shows the correlation for the proposed method using RNS, and Fig. 7(d) shows the correlation for the hybrid S-box for the Barbara plain image. As seen in the figure, the distribution of pixels in the three directions is uniform, which shows a weak correlation between pixels and can be effectively resistant to statistical attacks. Fig. 8 and Fig. 9 show similar results for Baboon and Pepper images, respectively.

Finally, Fig. 10(a) and 10(b) provide 3D plots for the correlation coefficient matrices of the plain Baboon image and encrypted image, respectively. While Fig. 10(a) displays values concentrated in a diagonal fashion, it is clear that Fig. 10(b) shows total random distribution of the values.

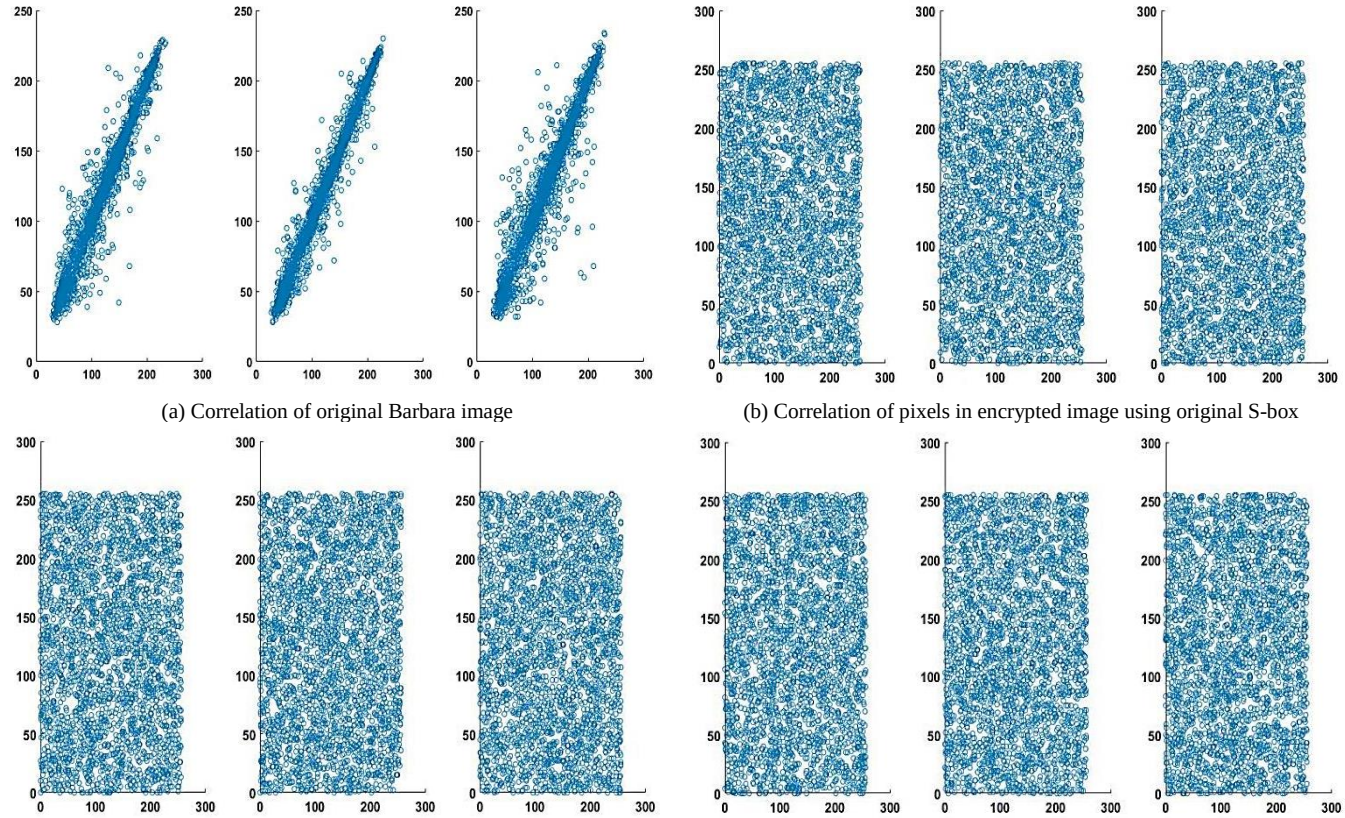
F. Frequency analysis

Another intriguing approach to assess the correlation between adjacent pixels involves examining the Fourier transform of both a plain image and its encrypted counterpart. The mathematical expression for the Fourier transform of a square image *f (i ,j)* can be written as [42]

$$F(k,l) = \sum_{-=0}^{N-1}\sum_{j=0}^{N-1} f(i,j)\, e^{-i2\pi(\frac{ki}{N} + \frac{li}{N})} \tag{16}$$

f(a,b) represents the image in the spatial domain, while the exponential term represents the basis function corresponding to each point *F(k,l)* in the Fourier space. Here, the basis functions are sine and cosine waves with increasing frequencies. This means that *F(0,0)* corresponds to the DC-component of the image, representing the average brightness, while *F(N-1,N-1)* would represent the highest frequency component. Fig. 11(b) displays the plain image with applied Fourier transform. The center of the image clearly illustrates pixels with high correlation, as indicated by the plus-sign shape at the center.

This pattern emerges because the plain image contains distinct features such as edges. Conversely, Fig. 11(c) displays the Fourier transform applied to encrypted images, presenting a relatively uniform distribution of values. This uniformity arises from the absence of any distinctive features, indicating a lack of correlation between adjacent pixels.



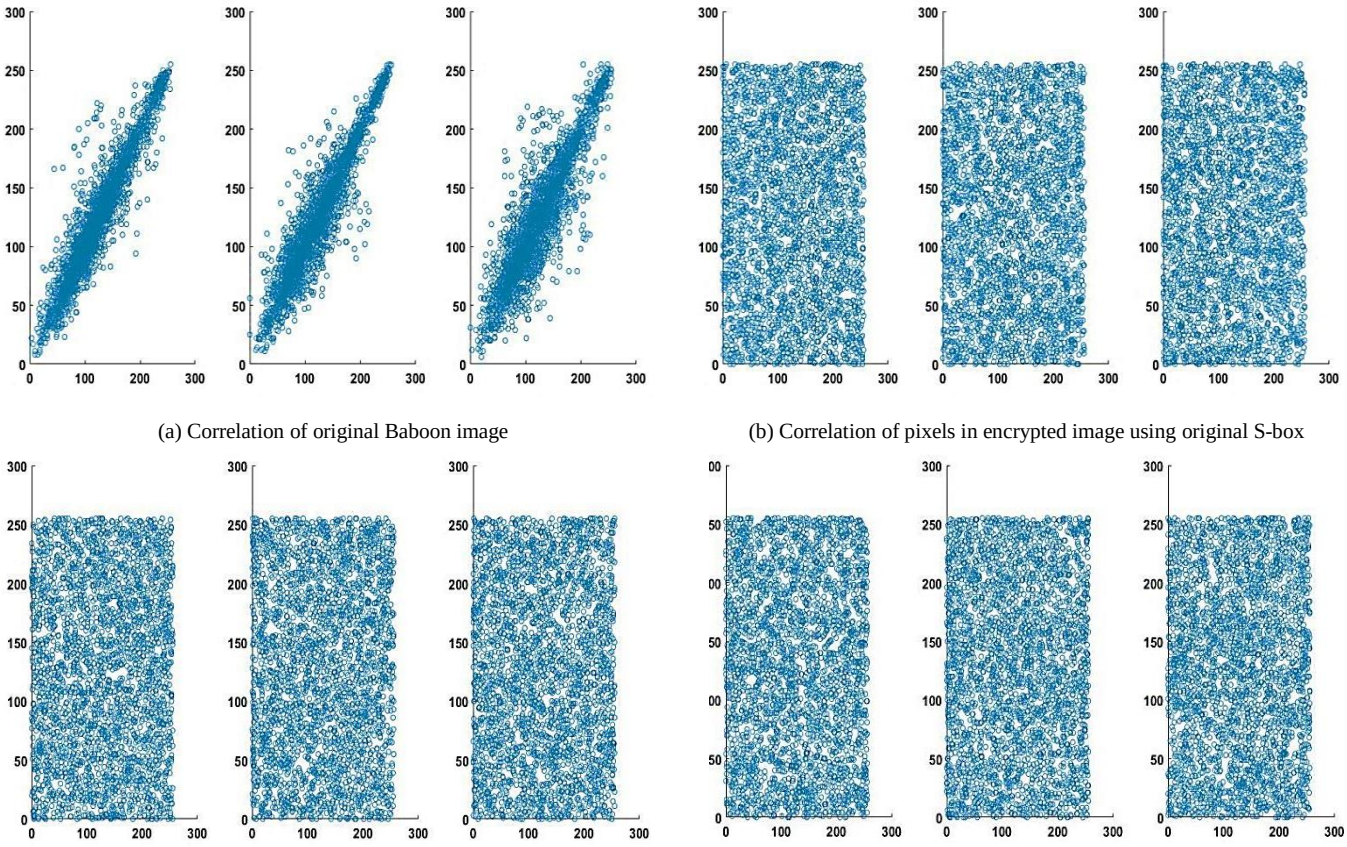
(a) Correlation of original Barbara image

(b) Correlation of pixels in encrypted image using original S-box

(c) Correlation of pixels in encrypted image using RNS S-box

(d) Correlation of pixels using the hybrid S-box

Fig. 7. Correlation analysis of Barbara and encrypted images using the AES algorithm in horizontal, vertical, and diagonal directions. x-axis – pixel gray value on location (x,y); y-axis - pixel gray value on location (x+1, y+1)



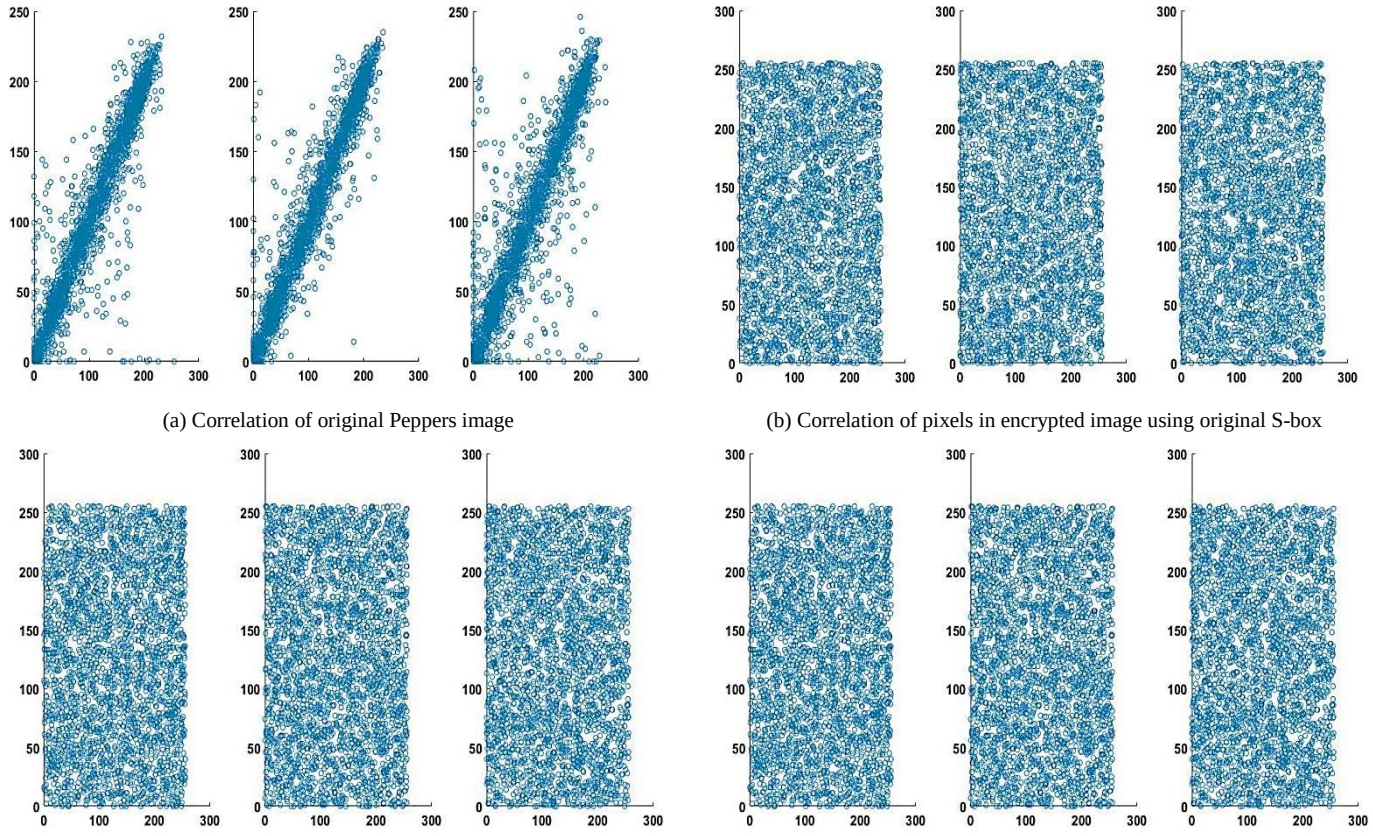
(a) Correlation of original Baboon image

(b) Correlation of pixels in encrypted image using original S-box

(c) Correlation of pixels in encrypted image using RNS S-box

(d) Correlation of pixels using the hybrid S-box

Fig. 8. Correlation analysis of Baboon and encrypted images using the AES algorithm in horizontal, vertical, and diagonal directions. x-axis – pixel gray value on location (x,y); y-axis - pixel gray value on location (x+1, y+1)



(a) Correlation of original Peppers image

(b) Correlation of pixels in encrypted image using original S-box

(c) Correlation of pixels in encrypted image using RNS S-box

(d) Correlation of pixels using the hybrid S-box

Fig. 9. Correlation analysis of Peppers and encrypted images using the AES algorithm in horizontal, vertical, and diagonal directions. x-axis – pixel gray value on location (x,y); y-axis - pixel gray value on location (x+1, y+1)

TABLE VI
CORRELATION COMPARISON OF DIFFERENT ENCRYPTION ALGORITHMS

Sr. No	Test Image	Direction	Plain image	Cipher Image					
				Original S-box	RNS S-box	Hybrid S-box	Ref. [39]	Ref. [40]	Ref. [41]
1	Barbara	(H)	0.99351	0.00647	0.02205	-0.0012	-	-	-
		(V)	0.99038	-0.00414	0.00894	0.0308	-	-	-
		(D)	0.9853	-0.03323	0.01793	0.0232	-	-	-
2	Baboon	(H)	0.93909	0.16981	-0.01826	0.0071	0.0015	0.01035	−0.01599
		(V)	0.94105	-0.05557	0.026006	-0.0333	− 0.0021	0.005657	0.000646
		(D)	0.90732	0.00053	0.007305	0.0310	− 0.0018	0.014383	0.032847
3	Peppers	(H)	0.95106	0.13096	-0.010297	-0.0191	− 0.0055	−0.01533	0.010863
		(V)	0.95559	-0.04056	0.005346	-0.0029	0.0025	−0.00081	0.005096
		(D)	0.92375	-0.02812	-0.028076	-0.0003	0.0011	0.002182	0.010197

G. PSNR, MSE, and MAD

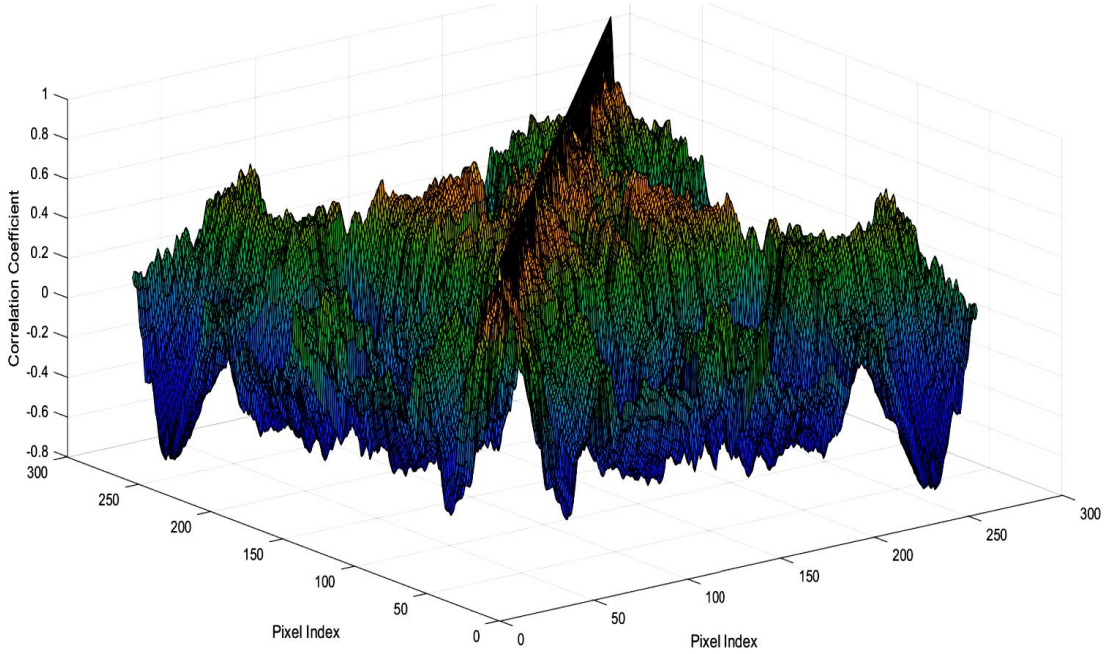
To assess the pixel value errors between two images, one can actively use MAD and MSE. It is necessary for a secure encryption scheme to have MAD and MSE values that are sufficiently large between plain and ciphered images. PSNR of an image is a measure of the peak error between a plain image and a ciphered image. The PSNR should be low because of the significant disparity. Calculate the values of MAD, MSE, and PSNR according to equations (17) to (19) [35] - [37].

$$MAD = \sum_{x=1}^{M}\sum_{y=1}^{N}\frac{|P(x,y)-I(x,y)|}{M\times N} \quad (17)$$

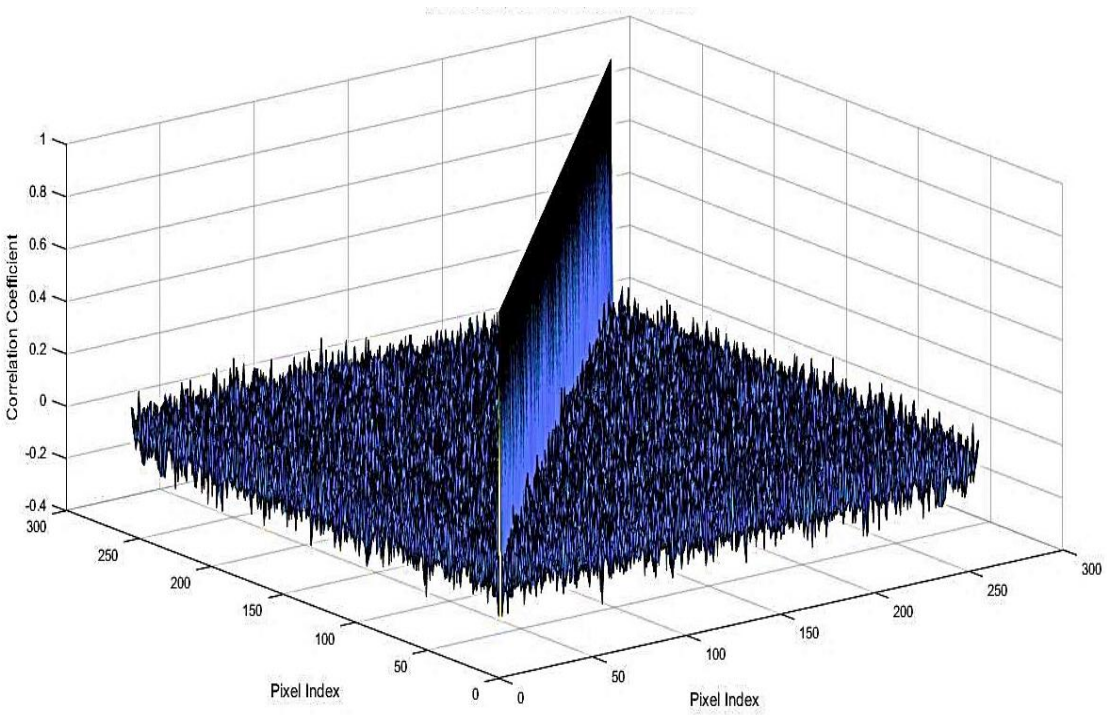
$$MSE = \sum_{x=1}^{M}\sum_{y=1}^{N}\frac{|P(x,y)-I(x,y)|^2}{M\times N} \quad (18)$$

$$PSNR = 20\, log_{10} \frac{255\times255}{\sqrt{MSE}}\, dB \quad (19)$$

where $P(x,y)$ and $I(x,y)$ represents the pixel values of the plain image and the cipher image at location (*x,y).* Table VII presents a comparison of MAD, MSE, and PSNR with standard AES. Table VI also compares the parameters with those of recent studies.



(a) for plain image



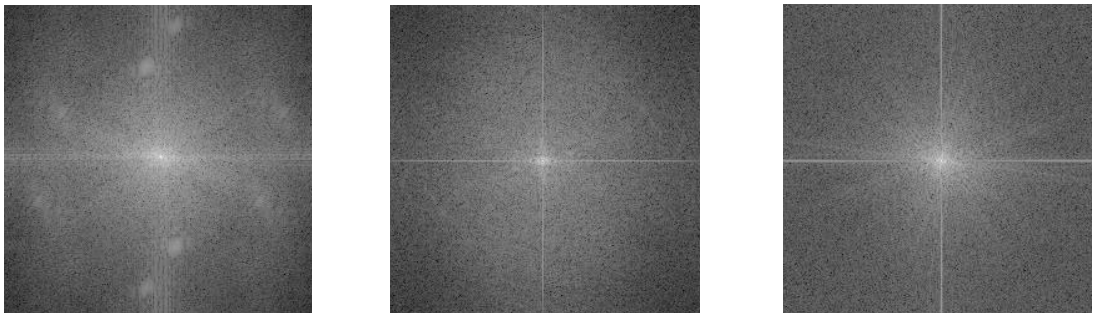
(b) for encrypted image

Fig. 10. 3D plot of the correlation coefficient matrix

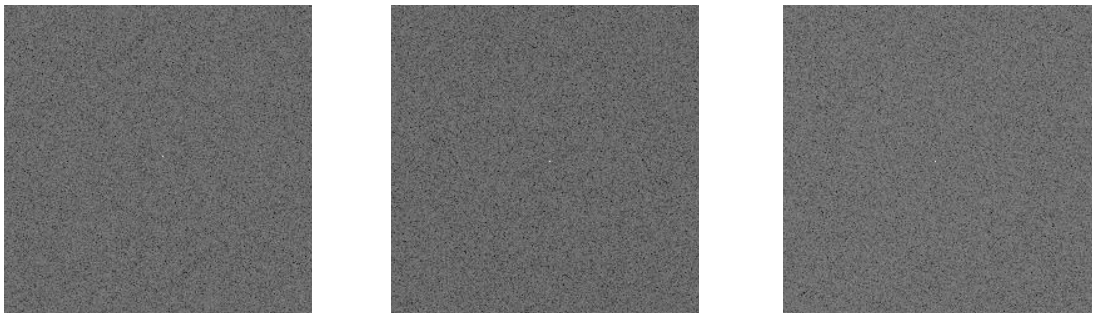
TABLE VII
RESULTS OF MAD, MSE, AND PSNR FOR PLAIN AND CIPHERED IMAGES

Sr. No	Test Image	S-box	MSE	PSNR	MAD
1	Barbara	Original S-box	2743.17	13.78	75.0939
		RNS S-box	2724.2	13.81	74.4603
		Hybrid S-box	2766.96	13.74	75.115
		Ref. [7]	8508.56	28.13	75.82
		Ref. [38]	-	-	-
		Ref. [42]	-	-	-
2	Baboon	Original S-box	6913.15	9.77	69.32
		RNS S-box	6900.99	9.78	69.6585
		Hybrid S-box	6975.32	9.73	69.841
		Ref. [7]	7038.2	27.61	70.26
		Ref. [38]	8619.66	8.9865	81.53
		Ref. [42]	10033.016	8.9283	75.46
3	Peppers	Original S-box	8092.93	9.08	74.12
		RNS S-box	8394.05	8.93	75.391
		Hybrid S-box	8442.08	8.9	75.675
		Ref. [7]	8251.72	28.51	74.78
		Ref. [38]	8992.82	8.8917	85.48
		Ref. [42]	8349.55	8.1624	81.837

(a) Barbara, Baboon, and Pepper plain images



(b) Magnitude spectrum of plain images



(c) Magnitude spectrum of encrypted images

Fig. 11. Frequency analysis using the RNS S-box

V. Conclusion

This study introduces an efficient construction scheme for an S-box based on a residue-number system. We leveraged the obtained S-box in an image-encryption scheme employing the AES algorithm. The simulations and experiments conducted provide evidence that the encryption scheme proposed in this study exhibits favourable security parameters. The proximity of the NPCR and UACI values to the ideal range indicates that the proposed method is resilient against differential attacks. However, it is worth noting that the method tends to have an entropy level closer to eight. In comparison with recent methods, the PSNR values are lower. However, security studies indicate that this approach is new and effective for ensuring cryptographic security. Hence, the proposed RNS-based S-box generation method offers significant advantages in terms of its ability to withstand common cryptanalytic attacks.

REFERENCES

[1] E. Y. Baagyere, P. A. -N. Agbedemnab, Z. Qin, M. I. Daabo and Z. Qin, "A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers," in IEEE Access, vol. 8, pp100438-100447, 2020.

[2] A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung and S. E. Venegas-Andraca, "Secure Data Encryption Based on Quantum Walks for 5G Internet of Things Scenario," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp118-131, March 2020.

[3] Tanveer, Muhammad, Ghulam Abbas, Ziaul Haq Abbas, Muhammad Waqas, Fazal Muhammad, and Sunghwan Kim. "S6AE: Securing 6LoWPAN Using Authenticated Encryption Scheme" Sensors vol. 20, no. 9, pp2707. 2020.

[4] Ahmad, Musheer, Eesa Al Solami, Xing-Yuan Wang, M. N. Doja, M. M. Sufyan Beg, and Amer Awad Alzaidi. "Cryptanalysis of an Image Encryption Algorithm Based on Combined Chaos for a BAN System, and Improved Scheme Using SHA-512 and Hyperchaos" Symmetry vol. 10, no. 7, pp266. 2018.

[5] A. K. Farhan, R. S. Ali, H. Natiq, and N. M. G. Al-Saidi, ‘‘A new Sbox generation algorithm based on multistability behavior of a plasma perturbation model,’’ IEEE Access, vol. 7, pp124914–124924, 2019.

[6] Hayat, U., Azam, N.A., Gallegos-Ruiz, H.R. et al. “A Truly Dynamic Substitution Box Generator for Block Ciphers Based on Elliptic Curves Over Finite Rings”. Arab J Sci Eng 46, pp8887–8899. 2021.

[7] Zahid, A.H., Iliyasu, A.M., Ahmad, M., Shaban, M.M.U., Arshad, M.J., Alhadawi, H.S. and Abd El-Latif, A.A. “A novel construction of dynamic S-box with high nonlinearity using heuristic evolution”. IEEE Access, 9, pp67797-67812. 2021.

[8] Z. -q. Du, Q. -j. Xu, J. Zhang and M. Li, "Design and analysis of dynamic S-box based on Feistel," IEEE Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, pp590-594, 2015.

[9] FIPS, PUB. "197. Advanced Encryption Standard (AES), National Institute of Standards and Technology, US Department of Commerce", 2001.

[10] M. S. Mahmood Malik et al., "Generation of Highly Nonlinear and Dynamic AES Substitution-Boxes (S-Boxes) Using Chaos-Based Rotational Matrices," in IEEE Access, vol. 8, pp35682-35695, 2020,

[11] Agarwal, Praveen, Amandeep Singh, and Adem Kilicman. "Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant." Advances in mechanical engineering vol. 10, no. 7, 2018.

[12] Sahmoud, Shaaban, Wisam Elmasry, and Shadi Abudalfa. "Enhancement the Security of AES Against Modern Attacks by Using Variable Key Block Cipher." Int. Arab. J. e Technol. Vol. 3. No.1, pp17-26, 2013.

[13] Altaleb, Anas, Muhammad Sarwar Saeed, Iqtadar Hussain, and Muhammad Aslam. "An algorithm for the construction of substitution box for block ciphers based on projective general linear group." AIP Advances. vol. 7, no. 3, 2017.

[14] Zahid, Amjad Hussain, Muhammad Junaid Arshad, and Musheer Ahmad. "A novel construction of efficient substitution-boxes using cubic fractional transformation." Entropy vol. 21. No. 3, 245, 2019.

[15] M. M. Dimitrov, ``On the design of chaos-based S-boxes," IEEE Access, vol. 8, pp. 117173117181, 2020.

[16] Yan, Wenhao, and Qun Ding. "A novel S-box dynamic design based on nonlinear-transform of 1D chaotic maps." Electronics vol. 10. no. 11, 1313, 2021.

[17] Manzoor, Atif, Muzammil Hussain, and Sobia Mehrban. "Performance analysis and route optimization: redistribution between EIGRP, OSPF & BGP routing protocols." Computer Standards & Interfaces vol. 68, 103391, 2020.

[18] Kadhim, Alaa. "New image encryption based on pixel mixing and generating chaos system." Al-Qadisiyah Journal of Pure Science vol. 25. No. 4, pp1-14, 2020.

[19] Lu, Qing, Congxu Zhu, and Xiaoheng Deng. "An efficient image encryption scheme based on the LSS chaotic map and single S-box." IEEE Access vol. 8, pp25664-25678, 2020.

[20] Gagnon, Iannick, Alain April, and Alain Abran. "An investigation of the effects of chaotic maps on the performance of metaheuristics." Engineering Reports vol.3. no. 8, e12369, 2021.

[21] L. Sousa, R. Paludo, P. Martins and H. Pettenghi, "Towards the Integration of Reverse Converters into the RNS Channels," in IEEE Transactions on Computers, vol. 69, no. 3, pp342-348, 1 March 2020,

[22] Ananda Mohan, P. V. "Residue number systems: Theory and applications." Basel: Birghauser, Mathematics. 2016.

[23] Omondi, Amos R., and A. Benjamin Premkumar. “Residue number systems: theory and implementation”. Vol. 2. World Scientific, 2007.

[24] Mohan, PV Ananda, P. K. Meher, and T. Stouraitis. "RNS-Based arithmetic circuits and applications." Arithmetic circuits for DSP applications, pp.186-236, 2017.

[25] K. Mandal, C. Parakash and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES," 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India, pp1-5 2012.

[26] Shannon, Claude E. "Communication theory of secrecy systems." The Bell system technical journal, vol. 28, no. 4 pp656-715, 1949.

[27] Artuğer, Fırat, and Fatih Özkaynak. "A method for generation of substitution box based on random selection." Egyptian Informatics Journal, vol. 23.no. 1, pp127-135, 2022.

[28] X. Zhang, Z. Zhou and Y. Niu, "An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding," in IEEE Photonics Journal, vol. 10, no. 4, pp1-14, Aug. 2018,

[29] Yilin Han, Ye Tao, Wenyu Zhang, Wenhua Cui, and Tianwei Shi, "Perceptron Neural Network Image Encryption Algorithm Based on Chaotic System," IAENG International Journal of Computer Science, vol. 50, no.1, pp42-50, 2023

[30] Zhu, Congxu, Guojun Wang, and Kehui Sun. "Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box." Symmetry, vol. 10, no. 9, 399, 2018.

[31] Khan, J.S., Ahmad, J. “Chaos based efficient selective image encryption”. Multidim Syst Sign Process, vol. 30, pp943–961, 2019.

[32] Waseem, H.M., Khan, M. “A new approach to digital content privacy using quantum spin and finite-state machine”. Appl. Phys. B vol. 125, no. 27 2019.

[33] Mingyue Sun, Wenhua Cui, Ye Tao, and Tianwei Shi, "Chaotic Color Image Encryption Algorithm Based on RNA Operations and Heart Shape Chunking," IAENG International Journal of Computer Science, vol. 50, no.1, pp121-134, 2023

[34] Ye Tao, Wenhua Cui, Zhao Zhang, and Tianwei Shi, "An Image Encryption Algorithm Based on Hopfield Neural Network and Lorenz Hyper Chaotic System," IAENG International Journal of Computer Science, vol. 49, no.4, pp1201-1211, 2022

[35] Zakaria, Abdul Alif, Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Norli Anida Abdullah, and Ki-Hyun Jung. "High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution." Applied Sciences 8, no. 11, 2199, 2018.

[36] Man Z, Li J, Di X, Sheng Y, Liu Z. “Double image encryption algorithm based on neural network and chaos”. Chaos, solitons & fractals. Pp152:111318, Nov 1, 2021.

[37] Younas, Irfan, and Majid Khan. "A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system." Entropy vol. 20. no. 12, pp913, 2018.

[38] R. Ali, M. K. Jamil, A. S. Alali, J. Ali and G. Afzal, "A Robust S Box Design Using Cyclic Groups and Image Encryption," in IEEE Access, vol. 11, pp.135880-135890, 2023.

[39] Waseem, Hafiz Muhammad, and Majid Khan. "A new approach to digital content privacy using quantum spin and finite-state machine." Applied Physics B vol. 125, pp1-14, 2019.

[40] Maolood, Abeer Tariq, Alaa Kadhim Farhan, Wageda I. El-Sobky, Hany Nasry Zaky, Hossam L. Zayed, Hossam E. Ahmed, and Tamer O. Diab. "Fast Novel Efficient S-Boxes with Expanded DNA Codes." Security and Communication Networks 2023, no.1, pp5767102, 2023.

[41] Song, Wei, Chong Fu, Yu Zheng, Ming Tie, Jun Liu, and Junxin Chen. "A parallel image encryption algorithm using intra bitplane scrambling." Mathematics and Computers in Simulation vol. 204, pp71-88, 2023.
[42] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab and A. Aboshousha, "Color Image Encryption Through Chaos and KAA Map," in IEEE Access, vol. 11, pp. 11541-11554, 2023,
[43] R. Ali, M. K. Jamil, A. S. Alali, J. Ali and G. Afzal, "A Robust S Box Design Using Cyclic Groups and Image Encryption," in IEEE Access, vol. 11, pp. 135880-135890, 2023.