Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.022743
Article

Construction of Key-dependent S-box for Secure Cloud Storage

A. Indumathi* and G. Sumathi

Department of Information Technology, Sri Venkateswara College of Engineering, Sriperumbudur, 602117, India
*Corresponding Author: A. Indumathi Email: aindumathi@svce.ac.in
Received: 17 August 2021; Accepted: 28 September 2021

Abstract: As cloud storage systems have developed and been applied in complex environments, their data security has become more prevalent in recent years. The issue has been approached through many models. Data is encrypted and stored in these models. One of the most widely used encryption methods is the Advanced Encryption Standard (AES). In AES, the Substitution box(S-box) is playing a significant part in imparting the job of confusion. The security of the entire cryptosystem depends on its nonlinearity. In this work, a robust and secure S-box is constructed using a novel method, *i.e.*, fingerprint features-based permutation function. Two stages are considered to construct a strong S-box. Firstly, random numbers are generated from the fingerprint features such as bifurcation and ridge endings of the user transmitting data. Subsequently, the permutation function is adapted on the random numbers (developed in the first stage) to augment the strength of the S-box. National Institute of Standards and Technology (NIST) STS 800-22 test suite is considered to evaluate the randomness of the enhanced fingerprint-based S-box. Also, the robustness of the constructed S-box is tested using cryptographical properties, namely Strict Avalanche Criterion (SAC), Nonlinearity (NL), Differential Approximation (DA) probability and output Bits Independence Criterion (BIC). Later, the cryptographical properties of the proposed S-box are compared with several existing S-boxes. After analyzing the characteristics of the proposed scheme, it is revealed that the newly constructed S-box is powerful, robust, and safe against linear and differential assaults.

Keywords: Information Security; Cryptography; fingerprint; minutiae points; permutation function; substitution box (S-box)

1 Introduction

A new trend in the computer field is cloud computing, which is used as a method of storing data. The physical storage device makes it impossible to store huge amounts of confidential or sensitive information. Therefore, cloud computing comes into play for storing the data in accordance with their needs. As long as the data is stored in the cloud, it is easily accessible to all, and maintaining its confidentiality is not possible. To protect the data from unauthorized user, encrypted data can be stored into the cloud. Encryption is the process which converts the plain text into an unreadable form. It has two significant types of encryption techniques which are symmetric cryptosystem, asymmetric cryptosystem. Symmetric cryptosystem uses a

single key for both encryption and decryption. Stream cipher and Block cipher are the two categories of the Symmetric cryptosystem. Block cipher encrypts a block of plaintext at a time and uses confusion, diffusion process. It is hard for reverse encryption. On the other hand, stream cipher encrypts a plaintext byte-by-byte or bit-by-bit. It is dependent only on confusion, and also reversing the encrypted text is easy. Merely, a block cipher is more efficient than a stream cipher encryption algorithm. Substitution-Permutation and Feistel cipher are the two categories of block cipher encryption.

Many new cryptographic techniques are evolving recently, notably quantum computing and post-quantum cryptography. Post-quantum cryptography is a method to establish a new cryptosystem that offers better security against classical and quantum computers. NIST has recommended the AES 256 block cipher encryption algorithm as quantum-resistant, and it is one of the widely used block cipher encryption algorithms. AES converts the plaintext into ciphertext with a different number of round of operations. The number of rounds depends on the key length. Each round consists of set of operations that use a different key which includes Substitution and permutation operations. These are the essential function in AES which provides confusion and diffusion by using S-box and P-box respectively. Diffusion is the property that conceals the bond between the plaintext and ciphertext, accomplished through transposition function. P-Box (Permutation box) is responsible for diffusion operation. Confusion is the sole nonlinear component of S-box. It hides the relationship between the ciphertext and the key. S-box provides confusion by replacing one set of bits with another set of bits. Therefore, it is cumbersome for the attacker to find the key from the ciphertext. The complexity of the confusion process depends upon the robustness of an S-box. As the AES uses a static S-box in each round, it allows the attacker to cryptanalyze the ciphertext that is produced by the block cipher. In order to overcome this limitations, various methods have been suggested by the researchers for constructing S-box. Namely, Chaotic systems, affine transformation, Algebraic operations, Heuristic methods and etc. In this paper, A novel method is presented to get the robust S-box using fingerprint features. The robustness and the strength of the S-box is examined by the standard cryptographical properties needs to be examined to define the strength and robustness of an S-box. An intense literature study is carried out and described in the below section considering these needs.

1.1 Related Existing Work

Several authors have demonstrated numerous works to construct a robust S-box for effective operation. An intense literature study is carried out and portrayed below.

Jamal S.S [1] proposed the Mobius transformation method and chaotic Tent Sine system and proved that the generated S-box was strong. Wang et al. constructed dynamic S-boxes by using logistic map and Kent map [2]. Authors in [3] made use of Liu J S-boxes [4] as initial seed to construct 40320 S-boxes by utilizing S8 permutation operation on the elements of Liu J S-boxes. In [5], authors suggested Quantum Walk (QW) based S-box and used for designing a different steganography technique. Cryptographic QW S-box guaranteed high security, good visual quality, and high embedding capacity. But it requires seed values to generate the S-box.

Malik et al. [6] proposed chaos-based affine transformation generation and rotational matrices to generate dynamic AES S-boxes. It also entailed closer to optimal cryptographic properties, and therefore the proposed S-boxes are equal to AES S-box. Tian et al. [7] constructed an S-box by combining the Artificial Bee Colony Algorithm and six-dimensional hyperchaotic map (CSABC). It yielded a cryptographically strong S-box. In Reference [8], S-box was constructed based on the linear group action of a finite local ring. Authors in [9] utilized a Spatiotemporal nonlinear chaotic system and permutation function to construct the S-box. It had an improved output bit independence criterion and capacity to resist linear password attacks. Siddiqui et al. [10] constructed 8*8 robust S-box by adapting adjacency matrixes on the Galois field. Authors in [11] used the composition of transposition for constructing

bijective S-boxes. They claimed that the proposed method has better cryptographic properties. Hussain et al. Constructed nonlinear S-boxes using Symmetric group, Mobius transformation, and Chaotic logistic map [12]. It had the potential to generate a high resistant S-box. In [13], authors used Cascaded quantum-inspired quantum walks and chaos inducement for generating S-box. Özkaynak et al. [14] constructed an S-box by employing FO chaotic Chen system and predictor-corrector scheme. But it failed to satisfy the bijectivity property. Khan et al. [15] proposed Gingerbreadman chaotic map and S8 permutation to build an efficient S-box. It was efficient for secure communications. Khan et al. [16] constructed an S-box from the binary chaotic sequences. They considered algebraic degree, Balancedness, Algebraic immunity, Correlation immunity to find the strength of the S-box. They didn't evaluate some of the S-box properties like nonlinearity, differential uniformity, and SAC. Random numbers were generated from the fingerprint [17]. Dwivedi et al. [18] used the fingerprint of the sender and receiver to generate a symmetric key along with the Diffie-Hellman algorithm

1.2 Research Gap and Motivation

As discussed above, Researchers have proposed numerous methods to construct the strong S-box, notably the Pseudo-random number generator algorithm, inversion mapping, heuristic method, power polynomial, linear fractional transformation, algebraic method, and chaos-based system to generate the initial S-box due to its high randomness, nonlinearity, and simplicity. Followed by complex mathematical operations, and permutations were applied to improve the strength of the S-box. However, it adapted the initial seed values to produce the random number sequence. The attacker could easily predict these seed values that may reduce the reliability of the design. Therefore, it is essential to construct an S-box with unpredictable random sequences.

Here, we propose a method of constructing S-boxes using the fingerprint features of the sender [19] and Zigzag transformation-based permutation [20] for improving the performance of the S-box. The key reason for using fingerprint feature are as follows; fingerprint is unique for a human being, unpredictable in nature, and non-transferrable. It produces unique and random values that have better resistant to cryptanalysis attacks. The constructed S-box is utilized for at least ten rounds to encrypt the data in the AES algorithm. The S-box provides confusion by performing substitution operations among data while encrypting it. Then, the Permutation operation is employed to perform the transposition. Hence it is more difficult for the attackers to reach the original plaintext. In this way, the proposed S-box provides a higher level of security. Our proposed system is simple when compared with the existing approaches and constructs a highly secure, unpredictable S-box. We verified the numerical results of the standard cryptographical properties (SAC, NL, BIC-SAC, BIC-NL, DU), and the results show that the S-box proposed is strong.

1.3 Objectives

Based on the perceived research gaps, this work targets the following objectives:

- To construct the initial S-box using biometric features of the user like ridges and bifurcations
- To adapt Zigzag transformation-based permutation function on initial S-box for optimal S-box design.
- To investigate the randomness of the fingerprint-based S-box using NIST SP 800-22 data.
- To analyze the cryptographical properties of the proposed scheme using the online tool 'S-box analyzer' [21].
- To design a robust S-box for effective security systems compared with existing methods.

The rest of the article is structured as follows: Section 2 represents the proposed method and its design factors such as image acquisition, preprocessing, and permutation; Section 3 describes the analysis features of constructed S-box using various characteristics; Section 4 demonstrates a detailed comparative study

considering the previous works; Section 5 concludes the article based on the observed outcome from the proposed scheme.

2 Proposed Method and its Design

The elements of the S-box ought to be random, highly nonlinear. And, it needs to satisfy the basic cryptographical properties to use for encryption and decryption. Therefore, random numbers are generated from the adapted fingerprint patterns of the user transmitting the information. It has many special features, including spur, ridge endings, core points, ridge dots, bifurcations, delta points, ridge islands, ponds, and bridges. These are also known as minutiae points that can determine uniqueness, and the most frequently used features are ridges and bifurcations. In this work, we have constructed the S-box in two stages. Initially, we have built an S-box using the ridge and bifurcation features and explained in Section 2.1. And then, Zigzag transformation-based permutation is applied over the initial S-box to enhance the strength of the S-box. The user who wants to store their information in the cloud can encrypt the data using the enhanced fingerprint-based S-box. This allows the right person to decrypt the ciphertext.

2.1 Construction of Fingerprint-based S-box

Fingerprint-based S-box construction consists of four phases. It includes fingerprint image acquisition, preprocessing, feature extraction, and mathematical operations on the feature coordinates to fill the S-box. In order to prove that any fingerprint can provide a strong S-box, we have taken fingerprints of two users for our experiment.

2.1.1 Image Acquisition

In this stage, the biometric scanner scans the user's fingerprint. Notably, the fingerprint image's quality depends on the scanner's quality and the finger's position during the scanning process. It is not easy to extract accurate minutiae points from the poor-quality image. The researchers state that a good quality scanner can acquire 25 to 100 minutiae points. The observed source image of User1 and User2 from the scanner is shown in Fig. 1a.

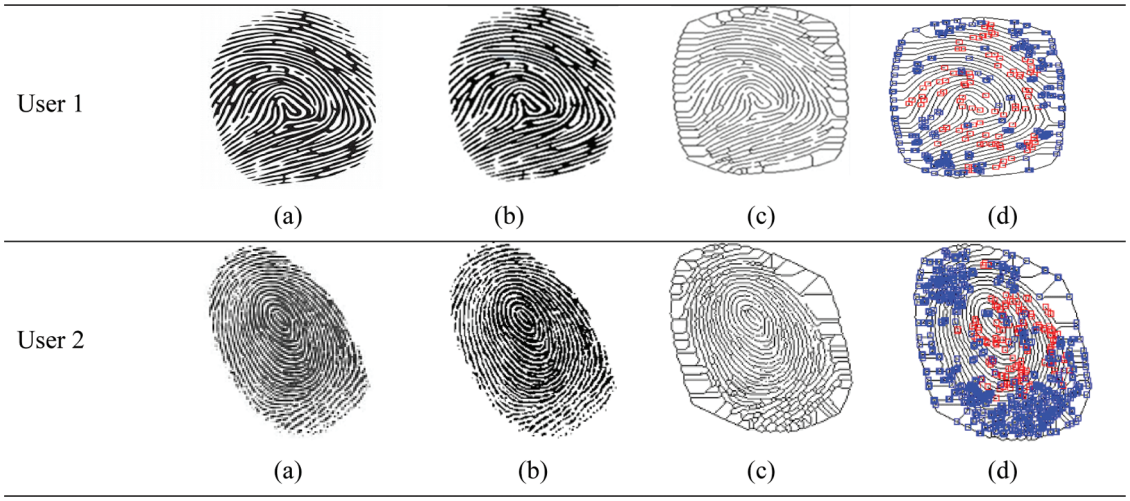

Figure 1: (a) Original Image from Scanner (b) Binarized Image (c) Thinned Image (d) Minutiae Extraction

2.1.2 Preprocessing

It plays a principal role in enhancing the quality of the acquired image. It helps to extract required features with high accuracy from the fingerprint image using the defined functions such as binarization and thinning.

i. Binarization: It is the process of transforming the acquired image into black and white (0's and 1's) through thresholding, as illustrated in Fig. 1b. The term thresholding is a technique of image segmentation that extracts the foreground image from the background image by comparing every pixel value of an image $I(\chi, \gamma)$ with the threshold value (T). If the pixel value is larger than the threshold value, it changed to white; otherwise, it maintains a black image as given in Eq. (1).

$$g(\chi, \gamma) = \begin{cases} 1, \forall I(\chi, \gamma) \geq T, \\ 0, \forall (\chi, \gamma) \leq T. \end{cases} \tag{1}$$

ii. Thinning: It is a morphological operation and is performed number of times until the image no longer changes, intending to remove imperfections from the binary image. As an outcome, the skeleton of the image with a single-pixel wide is obtained and given in Fig. 1c.

iii. Feature Extraction (FE): The last step of preprocessing is called feature extraction (FE). There are two types of FE, namely local and global features. In this work, local features are considered ridge endings and ridge bifurcations. It reduces the dimension of an image to extract precise and essential components from an image. Minutiae points (Mp) are extracted from the thinned image (Fig. 1d) as denoted in Eq. (2). Blue color specifies ridge ending, and red color indicates ridge bifurcations. This minutiae point is the most distinguishing feature among the people.

$$M_p = \left\{ M_p(\chi_i, \gamma_i) \right\}_{i=1}^{\eta} \tag{2}$$

where η denotes the extracted number of features from the fingerprint; χ, γ are the coordinates of the feature.

We constructed the initial S-box from two different fingerprints by performing an XOR operation between coordinates of the fingerprint features, and the respective consequence is illustrated in Tabs. 1 and 2. To use the S-box for encryption and decryption, it should satisfy the NIST randomness test and cryptographic properties. We use the NIST randomness assessment to evaluate the randomness of S-box values that endorse this process. The observed results show that the elements of the initial S-box are highly random. "S-box analyzer tool" [21] is used to evaluate the performance of the initial S-box. As a result, the initial S-box had 106 as maximum nonlinearity and 16 as differential uniformity. Although the range of attained nonlinearity value is optimal, differential uniformity needs to be reduced to improve the S-box strength. Therefore, the Zigzag transformation-based permutation function is applied to the initial S-box to enrich the S-box nonlinearity and decrease the differential uniformity.

2.2 Zigzag Transformation-based Permutation

It is a process of rearranging the elements of the matrix in the shape of 'Z' letter. It can improve the diffusion level and enhances the strength of the S-box further. Three types of Zigzag transformation are in use to change the position of a matrix. Namely, the Standard Zigzag Transformation process (SZT), Modified Zigzag Transformation process (MZT), and Parallel way of the Zigzag Transformation process (PZT). In SZT, the matrix elements are scanned from the top left corner, and ending with the bottom right corner (Fig. 2a). Whereas MZT (Figs. 2b–2i), scans the matrix elements from the top right corner with the direction from the right to the left or top to the bottom and ending with the bottom left corner as represented in Figs. 2b and 2d. Similarly, the top left corner matrix elements are scanned downwards and ending with the bottom right corner (Fig. 2c). The parallel– Zigzag transformation process scans the matrix elements horizontally or vertically as depicted in Figs. 2j–2l. A Blue circle and a red circle denote the

starting position and the ending position respectively. The authors of [22,23] used the MZT approach for image encryption. We use the recursive SZT permutation operation to improve the nonlinearity of the initial S-box.

Table 1: Initial S-box generated from fingerprint of User-1

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

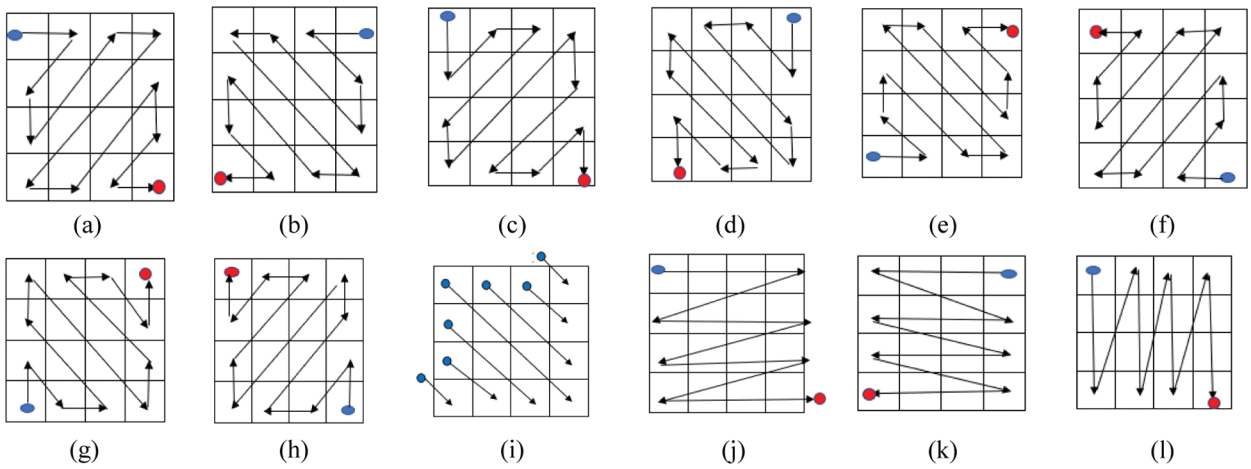

Figure 2: (a) – SZT, 2 (b) – 2 (i) – MZT, 2 (j) – 2 (l) – PZT

Table 2: Initial S-box generated from fingerprint of User-2

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

The flowchart of the complete process is given in Fig. 3 and the pseudocode is presented in Tab. 3. The enhanced fingerprint-based S-box (FSB) is illustrated in Tabs. 4 and 5.

3 Performance Analysis of Constructed S-box

3.1 Randomness Assessment

It is known that the S-box elements are random and nonlinear and it is necessary to maintain these elements as unpredictable. NIST STS, Dieharder Test are commonly used for randomness testing. Among these, NIST STS is the popular and faster random analysis method. The NIST randomness test considered fifteen statistical assessments to prove the randomness. These assessments determine the power of randomness, and the significant value (ρ) utilized for examination is 0.01, as expressed by NIST. Every assessment result is compared with the significant value (ρ). If ρ is greater than or equal to 0.01, then the sequence is random or irregular. If $\rho < 0.01$, then it is regular sequence. Moreover, if the significant value is 0, then the sequence is completely non-random. Also, if the ρ is 1, then the sequence is said to be perfectly random. The frequency test is the basic test to evaluate the randomness of the data. If the significant value (ρ) of the frequency test is less than 0.01, then there is the possibility of failing all other tests. The minimum sequence length to perform all the NIST STS test is 10,00,000 bits with minimum of 100 sequences. Each sequence should have 10,00,000 bits. Certain types of the test cannot be executed when the length of the sequences is less than the required limit. For example, the approximate entropy test and universal statistical test which requires 106 bits. In [24], the authors were used minimum of 1000 bits and maximum of 10000 bits for testing the randomness. In our case, 256 random elements are filled in the S-box proposed. To use this S-box in AES for encryption and decryption, its randomness has to be examined. We tested the randomness of the S-box elements using NIST STS-2.1.2, in two different methods.

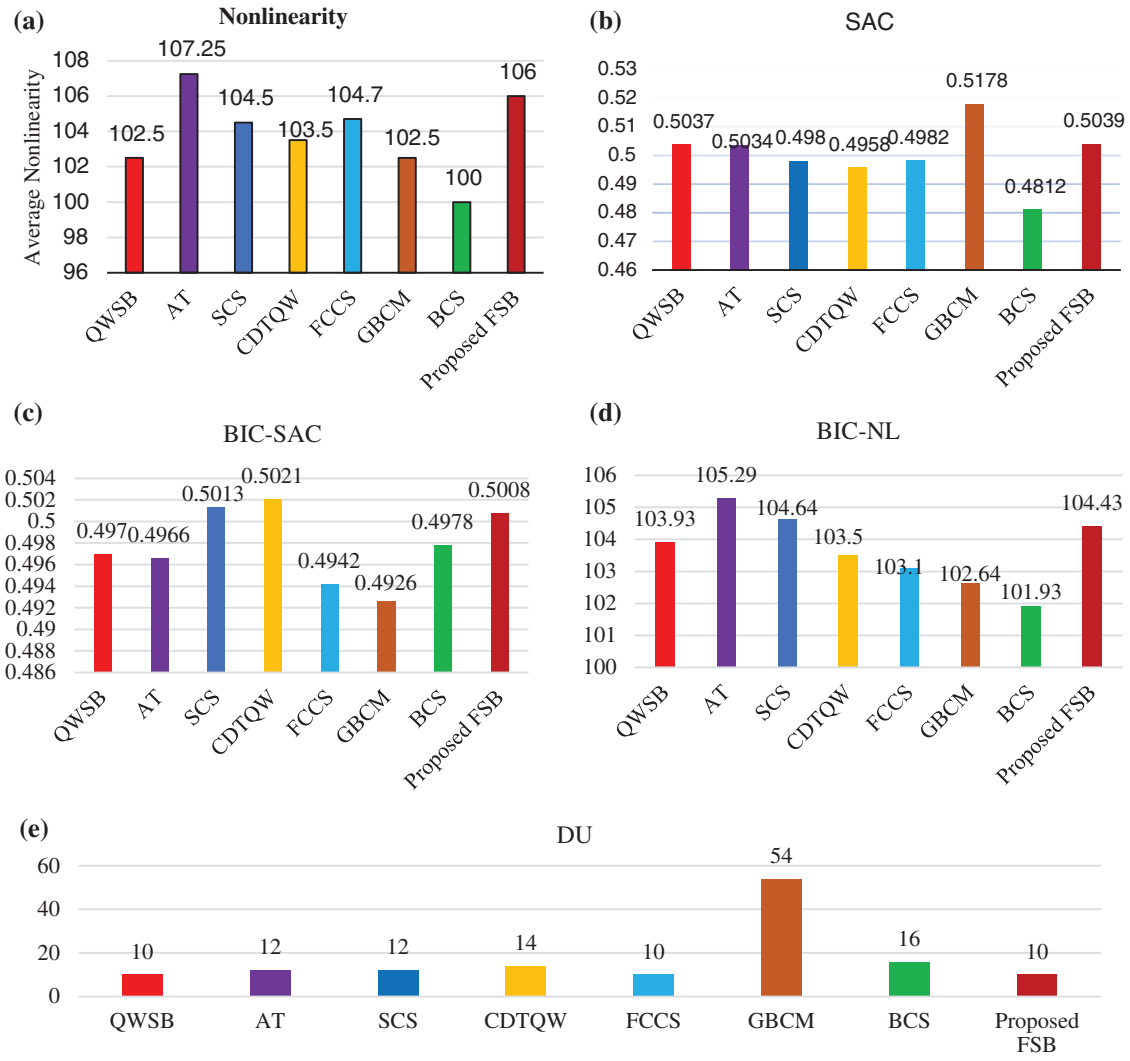

Figure 3: (a) Nonlinearity (b) SAC (c) BIC-SAC (d) BIC-NL (e) Differential Uniformity

1. The S-box elements are converted into binary sequences and concatenated together to form 2048 bits and its randomness is verified. It is perceived that the enhanced fingerprint-based S-box satisfies thirteen tests out of 15 tests. It fails to satisfy the approximate entropy test and universal statistical test because it requires a long sequence.
2. We have analyzed the randomness of Enhanced fingerprint-based S-box of User-1 from the obtained ciphertext by employing the proposed S-box in AES encryption [25]. We have generated Ciphertext of length 13028 bits and used it for randomness analysis. The numerical values of NIST tests are presented in Tab. 6 and compared with the related works. It reveals a success status for thirteen tests by considering 2048 bits as a sequence and fourteen tests for 13028 bits.

Table 3: Pseudocode of enhanced Fingerprint based S-box

Input: Raw image of the fingerprint

Output: S-box

Step 1: Initialize an S-box(16 × 16) with zeroes
Step 2: Acquire the biometric image from the biometric scanner and store it in I.
  I = Input(Image)
Step 3: Apply binarization methods on the acquired image
Step 3.1: Get the height(h) and width(w) of an image(I)
  for i = 1 to h
    for j = 1 to w
      if (I(i,j) ≥ Threshold)
        set I(i,j) = 1
      else
        set I(i,j) = 0
Step 4: Perform morphological operation on binarized image to get the thinned image
Step 5: Extract the ridge and bifurcation features (minutiae points) from the thinned image
Step 5.1: minutiae points = $\{ridge_i(\chi,\gamma), bifurcations_j(\chi,\gamma)\}$,where $1 \le i \le n_1$ and $1 \le j \le n_2$,n_1-number of ridge points and n_2-number of bifurcations
Step 5.2: Get the number of ridges and bifurcations and store it in n_1, n_2 respectively
Step 6: Initialize n, i and j with zero
  If (n<256)
    while (i<n_1 && j<n_2)
    for i = 1 to n_1
      BEGIN
        $v = ridges_i[\chi] \oplus ridges_i[\gamma]$
        $S-Box[n] = v$ //If v does not exist in S-box
        n = n+1
        i = i+1
      END BEGIN
    for j = 1 to n_2
      BEGIN
        $v1 = bifurcations_i[\chi] \oplus bifurcations_i[\gamma]$
        if (v! = $v1$)
          $S-Box[n] = v1$
          n = n+1
          j = j+1
      END BEGIN
  END IF
Step 7: print(S-box)
Step 8: new_SBox = Zigzag_transformation(S-box)
Step 9: Result = Performance_Evaluation_Test(new_SBox)
Step 10: If result = "PASS"
      Optimized_Sbox = new_Sbox
  Else
      Repeat Step 8-10
Step 11: Stop

Table 4: Enhanced fingerprint-based S-box of User-1

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

Table 5: Enhanced fingerprint-based S-box of User-2

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

Table 6: NIST test numerical values of the enhanced Fingerprint-based S-box of Uer-1

NIST statistical test/ Sequence length	Ref. [17]	Ref. [9]	Ref. [24]	Ref. [25]	Proposed	
	10,00,000 bits	2048 bits	10000 bits	100 bits	2048 bits	13028 bits
Frequency test	0.304126	1.000000	0.080519	0.580000	1.000000	0.362211
Block frequency test	0.739918	0.102530	0.494392	–	0.149349	0.459487
Run test	0.334538	0.658531	0.102526	0.500000	0.626870	0.980216
Longest run of ones in a block	0.534146	1.000000	0.678686	1.000000	0.999999	0.340905
Binary matrix rank test	0.637119	0.481248	0.69372	–	0.085200	0.858362
Discrete Fourier Transform test	0.759756	0.208675	0.121488	–	0.570187	0.407615
Non-Overlapping Template Test	0.145326	0.844144		–	0.128475	0.560620
Overlapping Template Matching Test	0.213309	0.282761		–	0.488415	0.475823
Linear Complexity test	0.202268	0.481431	0.918243	–	0.868443	0.206109
Serial Test 1	0.739918	0.645337	0.00513	–	0.600084	0.900023
Serial Test 2	0.955835			–	0.324382	0.817120
Cumulative Sums test – Forward	0.867692	0.984155	0.664283	0.580000	0.223219	0.459428
Cumulative Sums test – Backward					0.223219	0.598593
Random Excursion Test X = 1	0.110952	NA		–	0.589884	0.247998
Random Excursion Variant Test X = 1	0.468595	NA		–	0.917850	0.737315
Approximate Entropy Test	0.334538	0.024931	0.991535	–	NA	0.356464
Universal Statistical Test	–	NA		–	NA	NA

3.2 Performance Evaluation Test

Performance Evaluation Test is used to evaluate the strength of the S-box. To ensure an efficient S-box, it should satisfy the cryptographic criteria: Bijective, Nonlinearity, Bit Independence Criterion, Strict avalanche, and Linear approximation probability. In this section, the proposed S-box's cryptographical capability is analyzed with the properties mentioned above using the S-box analyzer tool.

3.2.1 Bijective

Commonly, the S-box is bijective when the observed output values of the proposed S-box fall between the defined interval. Also, a Boolean function $f : \chi \rightarrow \gamma$ denotes a bijective when there is a unique mapping between two sets. At this juncture, χ, γ are the two sets, namely input, and output sets, and mathematically modeled as follows:

$$hw\left(\sum_{i=1}^{n} a_i f_i\right) = 2^{n-1}, \tag{3}$$

The term '*hw*' represents a hamming weight; $a_i \in \{0, 1\}$; $a_i \neq 0$ $(1 \leq i \geq n)$. The proposed S-box has a distinct elements framework that satisfies the bijective property.

3.2.2 Nonlinearity

Pieprzyk and Finkelstein introduced the nonlinearity model. It is the first and foremost requirement of the S-box. To realize the higher nonlinearity, the elements of the S-box should be highly random. The optimal value of nonlinearity of the Boolean function is defined as follows:

$$NL(f) = 2^{\eta-1} - 2^{\eta-2}, \tag{4}$$

Further, Boolean function nonlinearity is described using the below equation.

$$NL(f) = 2^{\eta-1}(1 - 2^{-\eta} \max_{w \in GF(2^n)} \left|s_{(f)}(w)\right|) \tag{5}$$

Notably, the Walsh spectrum is used to compute the nonlinearity of the Boolean expression as described below.

$$s_f(w) = \sum\nolimits_{w \in GF(2^n)} (-1)^{f(\chi) \oplus \chi.w} \tag{6}$$

For symmetric Boolean functions, the nonlinearity of S-box should lie between 100 and 120. If the experimental values violate the said band, it is susceptible to cryptanalysis. However, the proposed scheme offers the best value of about 108 as maximum nonlinearity and average nonlinearity of 106 (Tab. 7), which ensures the robustness of the newly constructed S-box.

Table 7: Nonlinearity values

0	1	2	3	4	5	6	7
106	106	106	108	106	106	104	106

3.2.3 Strict Avalanche Criteria (SAC)

Tavares and Webster introduced SAC in 1986 to investigate the strength of the cryptosystem. Its scale should satisfy by changing a single input bit that reflects the change of about 50% of the output bits, *i.e.*, the SAC value should be close to 0.5. The proposed scheme produces the SAC value of about 0.5039 which satisfies the SAC (Tab. 8). A dependence matrix is evaluated to test the SAC effectiveness using the following expressions.

Table 8: Strict avalanche criterion

	1	2	3	4	5	6	7	8
1	0.5625	0.375	0.4688	0.5	0.5781	0.5156	0.5781	0.4531
2	0.4531	0.5312	0.5156	0.5156	0.5312	0.5	0.4844	0.4844
3	0.5	0.4688	0.5312	0.5938	0.4844	0.5156	0.5625	0.4375
4	0.5156	0.4688	0.4844	0.4375	0.5156	0.5312	0.5156	0.4688
5	0.5312	0.5	0.4844	0.5938	0.5156	0.5938	0.5312	0.5312
6	0.4375	0.4531	0.5625	0.4531	0.5312	0.5156	0.4844	0.4375
7	0.4688	0.5	0.4219	0.5781	0.5156	0.5625	0.5156	0.5
8	0.4531	0.5156	0.4844	0.5	0.5312	0.4531	0.4844	0.5312

$$s(f) = \frac{1}{\eta^2} \sum\nolimits_{1 \le i \le \eta} sum_{1 \le j \le \eta} - \left| \frac{1}{2} - P_{i,j}(f) \right| \tag{7}$$

3.2.4 Bit Independence Criterion (BIC)

BIC is a cryptosystem parameter introduced by Webster and Tavares. This analysis required maintaining the output bits that should not correlate with each other. Also, an adjustment in any single input bit and respective output bits should change independently for avalanche vectors. It is essential to satisfy the BIC with maximum nonlinearity and SAC, as shown in Tabs. 9 and 10.

Table 9: BIC-SAC of the proposed S-box

	1	2	3	4	5	6	7	8
1	0	0.5098	0.4785	0.5137	0.498	0.4941	0.5039	0.5137
2	0.5098	0	0.5078	0.4941	0.5078	0.5	0.4688	0.502
3	0.4785	0.5078	0	0.5234	0.5176	0.5	0.4941	0.4805
4	0.5137	0.4941	0.5234	0	0.5117	0.5195	0.5039	0.5059
5	0.498	0.5078	0.5176	0.5117	0	0.4883	0.4883	0.5176
6	0.4941	0.5	0.5	0.5195	0.4883	0	0.498	0.4863
7	0.5039	0.4688	0.4941	0.5039	0.4883	0.498	0	0.4961
8	0.5137	0.502	0.4805	0.5059	0.5176	0.4863	0.4961	0

Table 10: BIC-Nonlinearity values

	1	2	3	4	5	6	7	8
1	0	102	104	104	106	104	104	104
2	102	0	102	104	102	104	108	106
3	104	102	0	108	108	102	104	106
4	104	104	108	0	108	106	98	104
5	106	102	108	108	0	106	106	102
6	104	104	102	106	106	0	104	104
7	104	108	104	98	106	104	0	104
8	104	106	106	104	102	104	104	0

The above tables show that the value of BIC-nonlinearity and BIC-SAC are within the acceptable range. It ensures the robustness of the proposed S-box further.

3.2.5 Differential Uniformity

It evaluates the resistance power against differential attacks. The lower range of Differential Uniformity value represent a high resistance during differential cryptanalysis attack and computed using the following equation.

$$DP_f = \max_{\Delta\chi \neq 0, \Delta\gamma} \left(\frac{\#\{\chi \in Z | f(\chi) \oplus f(\chi \oplus \Delta\chi) = \Delta\gamma\}}{2^{\eta}} \right) \tag{8}$$

where Z is a collection of all possible input values; 2^{η} is the count of elements; $\Delta\chi$ and $\Delta\upsilon$ are input and output differences respectively. The analysis shows that the differential uniformity of the proposed S-box is 10, which shows the S-box's resistivity against the differential attacks.

4 Comparative Analysis with Existing Works

The observed results are compared with recently published works using different strategies to validate the effectiveness of the proposed S-box notably, QW S-box (QWSB) [5], Algebraic Technique (AT) [8], Spatiotemporal Chaotic System (SCS) [9], Cascaded Discrete-time Quantum Walk (CDTQW) [13], Fractional-order Chaotic Chen System (FCCS) [14], Gingerbreadman Chaotic Map (GBCM) [15], and Binary Chaotic Sequence (BCS). The figurative demonstration of the comparative study illustrated in Fig. 3 and the numerical reports are presented in Tab. 11.

Table 11: Numerical comparative analysis

Techniques used	Avg. NL	Min. NL	Max. NL	Avg. SAC	BIC-NL	BIC-SAC	DU
QW S-box (QWSB) [5]	102.5	96	106	0.5037	103.93	0.497	10
Algebraic Technique (AT) [8]	107.25	106	108	0.5034	105.29	0.4966	12
Spatiotemporal Chaotic System (SCS) [9]	104.5	102	108	0.498	104.64	0.5013	12
Cascaded Discrete-time Quantum Walk (CDTQW) [13]	103.5	98	106	0.4958	103.5	0.5021	14
Fractional-order chaotic Chen system (FCCS) [14]	104.7	100	108	0.4982	103.1	0.4942	10
Gingerbreadman chaotic map (GBCM) [15]	102.5	96	106	0.5178	102.64	0.4926	54
Binary Chaotic Sequence (BCS) [16]	100	84	106	0.4812	101.93	0.4978	16
Proposed - FSB of User 1	106	104	108	0.5039	104.43	0.5008	10
Proposed - FSB of User 2	104.75	102	108	0.5181	103.71	0.5023	10

It is perceived that the maximum nonlinearity of Fingerprint-based initial S-box-1 of user-1 was 106 initially, and then it is improved to 108 after permutation. Further, the average value of SAC value of the proposed scheme offered the best deal, about 0.5039. It shows that the proposed system satisfies the strict avalanche criterion. S-box quality is depending on the smaller value of differential uniformity. The differential uniformity of the enhanced FSB is 10, which is lesser than the other methodologies. The cryptographic criterions of S-box (NL, SAC, DU, BIC-SAC, BIC-NL) is compared with other S-boxes and illustrated in Tab. 11.

5 Conclusions

An effective S-box is constructed using fingerprint pattern and permutation function in this work. Initially, S-box is built from X-Y coordinates of the user's extracted fingerprint features (ridges, bifurcation). Subsequently, Recursive Zigzag transformation-based permutation function is carried out on the initial

S-box to boost the overall characteristics. Further, a randomness test and cryptographic efficiency are performed to check S-box's strength. From the observed results, the following conclusions are made:

- The maximum range of nonlinearity is obtained from the proposed S-box of about 108 and the 106 as average nonlinearity.
- SAC shows a significant scale of about 0.5039, closer to the required band (0.5).
- BIC-NL and BIC-SAC offer the best value, about 104.43 and 0.5008, respectively.
- The rate of DU also superior for the proposed scheme compared with existing methods.

The statistical results reveal that the proposed scheme satisfies all the cryptographic properties, and therefore the proposed S-box is strong enough against linear and differential attacks. An optimization model can be incorporated with this scheme for further enhancement in the future.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding this study.

References

[1] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan and I. Hussain, "Construction of cryptographic S-boxes based on Mobius transformation and Chaotic Tent-Sine System," *IEEE Access*, vol. 7, pp. 173273–173285, 2019.

[2] X. Wang and Q. Wang, "A novel image encryption algorithm based on dynamic S-boxes constructed by chaos," *Nonlinear Dynamics*, vol. 75, no. 3, pp. 567–576, 2014.

[3] I. Hussain, T. Shah, H. Mahmood and M. A. Gondal, "Construction of S8 Liu J S-boxes and their applications," *Computers & Mathematics with Applications*, vol. 64, no. 8, pp. 2450–2458, 2012.

[4] J. Liu, B. Wei, W. Cheng and X. Wang, "An AES S-box to increase complexity and cryptographic analysis," in *19th Int. Conf. on Advanced Information Networking and Applications (AINA'05)*, Taipei, Taiwan, vol. 1, pp. 724–728, 2005.

[5] A. Ahmed, A. EL-Latif, B. Abd-El-Atty and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology*, vol. 116, no. 3, pp. 92–102, 2019.

[6] M. S. M. Malik, M. A. Ali, M. A. Khan, M. Ehatisham-ul-haq, S. N. M. Shah *et al.,* "Generation of highly nonlinear and dynamic AES Substitution-Boxes (S-boxes) using Chaos-based rotational matrices," *IEEE Access*, vol. 8, pp. 35682–35695, 2020.

[7] Y. Tian and Z. Lu, "S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm," *Journal of Systems Engineering and Electronics*, vol. 27, no. 1, pp. 232–241, 2016.

[8] Attaullah, S. S. Jamal and T. Shah, "A novel algebraic technique for the construction of strong substitution box," *Wireless Personal Communications*, vol. 99, no. 1, pp. 213–226, 2018.

[9] L. Liu, Y. Zhang and X. Wang, "A novel method for constructing the S-box based on Spatiotemporal Chaotic Dynamics," *Applied Sciences*, vol. 8, no. 12, pp. 2650, 2018.

[10] N. Siddiqui, F. Yousaf, F. Murtaza, M. Ehatisham-ul-Haq, M. U. Ashraf *et al.,* "A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field," *PLOS ONE*, vol. 15, no. 11, pp. e0241890, 2020.

[11] L. Shuai, L. Wang and L. Miao, "Constructing Chaos based substitution boxes using the composition of transpositions," *Wireless Personal Communications*, vol. 115, no. 3, pp. 1881–1897, 2020.

[12] I. Hussain, A. Anees, T. A. Al-Maadeed and M. T. Mustafa, "Construction of S-box based on Chaotic map and algebraic structures," *Symmetry*, vol. 11, no. 3, pp. 351, 2019.

[13] A. A. Abd El-Latif, B. Abd-El-Atty, M. Amin and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Scientific Reports*, vol. 10, no. 1, pp. 2322, 2020.

[14] F. Özkaynak, V. Çelik and A. B. Özer, "A new S-box construction method based on the fractional-order chaotic Chen system," *Signal, Image and Video Processing*, vol. 11, no. 4, pp. 659–664, 2017.

[15] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation," *Neural Computing and Applications*, vol. 29, no. 4, pp. 993–999, 2018.

[16] M. Khan, T. Shah and S. I. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption," *Neural Computing and Applications*, vol. 27, no. 3, pp. 677–685, 2016.

[17] L. Ying, W. Shu, Y. Jing and L. Xiao, "Design of a random number generator from fingerprint," in *Int. Conf. on Computational and Information Sciences*, Chengdu, China, pp. 278–280, 2010.

[18] R. Dwivedi, S. Dey and M. A. Sharma, "A fingerprint based crypto-biometric system for secure communication," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 4, pp. 1495–1509, 2020.

[19] O. Şengel, M. A. Aydın and A. Sertbaş, "An efficient generation and security analysis of substitution box using Fingerprint patterns," *IEEE Access*, vol. 8, pp. 160158–160176, 2020.

[20] F. Artuğer and F. Özkaynak, "A novel method for performance improvement of Chaos-based substitution boxes," *Symmetry*, vol. 12, no. 4, pp. 571, 2020.

[21] A. Özkaynak, "An analysis and generation toolbox for chaotic substitution boxes: A case study based on Chaotic Labyrinth Rene Thomas System," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 44, no. 1, pp. 89–98, 2020.

[22] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius and T. Blažauskas, "An image encryption scheme based on block scrambling, modified Zigzag transformation and Key generation using enhanced Logistic—Tent Map," *Entropy*, vol. 21, no. 7, pp. 656, 2019.

[23] X. Wang and H. Sun, "A chaotic image encryption algorithm based on zigzag-like transform and DNA-like coding," *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 34981–34997, 2019.

[24] Z. Jiang and Q. Ding, "Construction of an S-box based on chaotic and bent functions," *Symmetry*, vol. 13, no. 4, pp. 671, 2021.

[25] D. G. Brosas, A. M. Sison, A. A. Hernandez and R. P. Medina, "Analysis of the randomness performance of the proposed stream cipher based cryptographic algorithm," in *11th IEEE Control and System Graduate Research Colloquium (ICSGRC)*, Shah Alam, Malaysia, pp. 76–81, 2020.