ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 15, Issue, 05, pp.4721-4725, May, 2024

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

CHAOITIC DYNAMIC S-BOX GENERATION FOR IMAGE ENCRYPTION

Anusha[1]*., Manasa Bhat[2]., Medini Naik[3]., N G Sowjanya[4]., and Arun Upadhyaya[5]

Department of Electronics and Communication Engineering Shri Madhwa Vadiraja Institute of Technology and Management bantakal-574115

DOI: http://dx.doi.org/10.24327/ijrsr.20241505.0882

ARTICLE INFO

Article History:

Received 10th April, 2024
Received in revised form 25th April, 2024
Accepted 19th May, 2024
Published online 28th May, 2024

Keywords:

Chaotic Map, Latin Square, affine-power-affine, Substitution Box, Image Encryption

ABSTRACT

The Dynamic Substitution boxes are generated initially using the Logistic map and piece-wise linear chaotic map method. The chaotic behavior is introduced through the Logistic map, which is utilized to select one of a thousand S-boxes and determine the row and column of the selected S-box. The algorithm combines the advantages of keyed Latin square and affine-power-affine transformation to encrypt digital images that are highly correlated. This process results in an encrypted image that maintains a high level of performance and security. Experimental results are conducted to assess the algorithm. The analysis shows that the algorithm is effective in providing high security for digital media.

INTRODUCTION

Today, as the internet continues to be an integral part of our daily lives, the need for secure transfer of multimedia data over this open network has become more crucial than ever before. The increasing need for secure multimedia data transfer over the Internet has led to the development of cryptographic systems for secret storage, writing, and transmission. The openness of public networks calls for mechanisms that can ensure end-to-end secrecy of digital media. This is crucial as the Internet provides a medium of exchange and communication for people worldwide.

Cryptographic systems are designed to ensure the secrecy of stored, written, and transmitted information by addressing aspects of information security like confidentiality, integrity, non-repudiation, and authentication. Substitution boxes (S-boxes) play a crucial role in modern cryptographic systems by obfuscating the relationship between cipher text and secret keys. One approach to generating S-boxes involves using chaotic image-encryption methods. S-box plays vital role in creating confusion between cipher text and secret key, making them resistant to linear and differential cryptanalysis. This is called Shannon's property of confusion. Its effectiveness is dependent on the type of data and the region of use, while its strength is determined by the degree of confusion the S-box introduces.

An efficient image encryption scheme using Henon map, skew tent map, and S-box, proving its security and resistance to statistical attack (Khan, Jansher, Jawad Ahmad, and Seong Oun Hwang., 2015) is presented. The paper presents a 3D chaotic system and dynamic AES key dependent S-box for encrypting and decrypting color images, demonstrating high security and resistance against attacks (Alabaichi, Ashwak Mahmood., 2016). The proposed key-dependent dynamic approach for generating Pure Dynamic S-box using Logistic map enhances security by satisfying cryptographic properties, simplifying high entropy properties, and reducing encryption time overhead (Katiyar, Shishir, and N. Jeyanthi.,2016).This study introduces a new secure image encryption algorithm using a chaotic-based S-box structure, incorporating the crucial S-Box component of block encryption, revealing its complex dynamic features (Çavuşoğlu, Ünal, et al, 2017).

The paper discusses the cryptographic properties and generation of 4-bit and 8-bit S-boxes, highlighting their superiority over 32 4-bit DES S-boxes and their logical and easy generation (Dey, Sankhanil, and Ranjan Ghosh.,2018). The study introduces a five-step color image encryption method in 3D space, utilizing substitution and permutation operations for enhanced performance and key space (Broumandnia, Ali., 2019). A new image encryption method is proposed using a chaotic map and symmetric key generation system, ensuring secure, efficient, and practical file encryption/decryption (Ramasamy, Priya, et al., 2019). The cubic

Corresponding author:* **Anusha
Department of electronics and communication engineering Shri Madhwa Vadiraja Institute of Technology and Management bantakal-574115.

polynomial mapping method efficiently generates strong 8x8 S-boxes, meeting bijective function requirements and maintaining simplicity, consistency, and cryptographic strength compared to other techniques (Zahid, Amjad Hussain, and Muhammad Junaid Arshad., 2019).

The Sine-Tent map enhances 1D discrete chaotic maps performance, while a double S-box-based image encryption algorithm improves S-box production efficiency and resistance to attacks, making it promising for cryptosystems (Zhu, Shenli, Guojun Wang, and Congxu Zhu., 2019). The study explores chaotic systems, designs an S-box generation algorithm, compares performance with literature, and develops a new image encryption algorithm based on these generated S-boxes (Wang, Xiong, et al., 2019). This study presents randomized block ciphers using chaotic maps as an entropy source, achieving good security and robustness with fewer rounds compared to the Rijndael algorithm (Artiles, José AP, Daniel PB Chaves, and Cecilio Pimentel., 2019).

The study introduces a new image encryption scheme using chaotic S-Boxes and a discrete compound chaotic system, enhancing cryptography performance and demonstrating potential for real-time encryption (Lu, Qing, Congxu Zhu, and Xiaoheng Deng., 2020). The study explores the construction of a strong S-box for block ciphers using linear fractional transformation and permutation function, highlighting the importance of effective construction techniques (Nizam Chew, Liyana Chew, and Eddie Shahril Ismail., 2020). The paper introduces a new S-Box Generation Method and Advanced Design using a combined chaotic system, addressing traditional genetic algorithms' shortcomings like low calculation efficiency and non-convergence (Zhu, Ding, et al., 2020). The study introduces a novel method for creating dynamic S-boxes with high nonlinearity, demonstrating its efficiency and simplicity, and its high cryptographic strength against standard security criteria (Zahid, Amjad Hussain, et al., 2021).

The study presents a Mandelbrot set S-box cryptosystem for image encryption, utilizing complex numbers and Chen chaotic maps, which resists cryptanalytic attacks through diffusion and robustness properties (Aslam, Mazzamal, et al., 2022). The paper presents a secure image encryption scheme using a piece-wise quadratic polynomial chaotic map, demonstrating its robust behavior and higher dynamic complexity compared to traditional chaotic qmaps (Zhu, Shenli, et al., 2023).

The study assesses image encryption's suitability for real-time applications, finding a decryption time of less than a second for , based on visual inspection, histogram analysis, cross-correlation analysis, and entropy values (ElBeltagy, Mohamed, et al.,2022).

METHODOLOGY

The proposed methodology for the design of dynamic S-boxes is initializing a 256-value linear array S, iterating a piece-wise linear chaotic map, and sampling the chaotic state-variable *x*. A random number m is extracted from x, and the elements of S are exchanged at positions m and k. The Fisher-Yates shuffle is applied, and the resultant shuffled linear array is translated to a table. The key drives the dynamic generation of S-boxes, which can be generated by making minor changes. The method can construct 1000 different S-boxes by updating the initial value of $x(0)$ with an increment of 0.000223 for each S-box every time. The proposed scheme is simple, low algorithmic complexity, and computational cost, and generates efficient S-boxes with better cryptographic features.

Chaotic Logistic map

The logistic map is a system model that describes the behavior of a population over time, based on a parameter r (1)

Chaotic logistic maps are a popular method for generating pseudorandom sequences for encryption algorithms. They are used to generate a sequence of chaotic values, which are then used as a key for encryption. The research reveals that when $r \in [0, 3]$, x's value reaches a fixed value after iterations without chaotic dynamics. When $r \in (3,3.57)$, the map oscillates between two fixed values without chaotic dynamics. Chaotic dynamics occur when $r < 4$. In an encryption system, the initial value r and $x(0)$ act as a secret key, requiring exact values at the receiver end for successful decryption. This key-dependent algorithm makes information extraction from the encrypted image difficult for attackers.

Piece-wise Linear Chaotic Map

The piecewise linear chaotic map (PWLCM) is a well-studied chaotic system with good dynamical properties. Its state equation is given by (2)

The piecewise definition of a system trajectory in PWLCM involves a system visiting the entire interval (0,1) for every parameter value in the range (0,1). The initial values assigned to $y(0)$ and p control the map's behavior. PWLCM is known for its statistical features and lack of periodic windows, making it suitable for generating dynamic S-boxes, components used in cryptographic algorithms for confusion and diffusion. To use PWLCM for dynamic S-boxes, initialize it with appropriate initial values and iterate the map equation for a sufficient number of iterations to generate the desired chaotic sequence.

This algorithm encrypts images using chaos, substitution boxes, affine-power-affine transformation, and keyed Latin square. The S-Box and element of S-Box are randomly selected using the digits of the chaotic map variable. The pixels of the image are confused by performing XOR operations on the pixel value, the output of affine-power-affine transformation, the previous cipher pixel value, and the value of the Latin square. The resultant image is rotated and flipped about its left diagonal. The process is repeated for a number of rounds to obtain.

The encrypted image. The steps of the proposed image encryption algorithm through chaotic substitution include generating 1000 dynamic S-boxes, inputting plain-image P with secret key components β, $x(0)$, $C(0)$, and Latin square key K, updating key components, reshaping the image into a 1D array, and generating Latin square using key K. The cipher image pixel is calculated using the APA-transformation of the value obtained from the kth S-Box at the index (l, m). The cipher image is then reshaped into a 2D matrix and performed two 90º anti-clockwise rotations and then flipped about its left diagonal. If $r < \beta$, the original image is obtained.

Affine-Power-Affine Transformation

An Affine-Power-Affine (APA) transformation is a cryptographic technique used in symmetric encryption algorithms, combining affine transformations and power functions. It is commonly used in substitution-permutation network (SPN) ciphers. The general form of an APA transformation is (3)

The Affine-Power-Affine (APA) transformation and Advanced Encryption Standard (AES) are two widely used symmetric encryption algorithms. AES is widely accepted due to its

security, efficiency, and widespread adoption. APA transformations, on the other hand, rely heavily on constants, power value, and modular arithmetic properties.

AES is highly optimized and efficient, while APA transformations may not be as efficient due to factors like input space size and power function complexity. AES supports key lengths of 128, 192, and 256 bits, but APA transformations may be vulnerable to different cryptanalytic techniques. AES is standardized by organizations like NIST and ISO, while APA transformations may find niche applications or be used in combination with other cryptographic primitives. It is evident that the affine-power-affine S-box has 253 non-zero coefficients, whereas the algebraic formulation of the AES S-box has just 9 terms. This indicates that the affine-power-affine S-box is more resilient to algebraic attack. Other cryptographic features of the AES S-box are also carried over to the affine-power-affine S-box.

Table 1. The coefficients involved in the algebraic expression of APA S-box are listed in the following table

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	141	79	209	184	139	151	199	15	58	187	27	222	47	104	83	219
1	55	167	249	241	246	114	255	111	171	36	121	160	168	44	142	61
2	93	210	65	163	153	166	201	38	56	63	149	150	216	179	78	230
3	39	30	194	156	138	66	169	227	183	32	195	24	67	161	4	130
4	102	181	43	3	19	52	48	126	178	171	91	42	76	14	62	148
5	162	211	54	206	26	132	41	251	8	92	117	69	228	129	232	174
6	84	156	198	9	234	248	213	109	50	29	170	220	224	37	45	31
7	34	72	244	185	203	97	81	122	106	159	118	82	46	215	131	189
8	67	191	192	157	73	254	86	152	229	212	223	94	155	15	40	239
9	245	136	90	140	173	137	71	88	144	235	39	127	17	10	64	7
10	23	193	231	247	12	21	17	6	190	115	119	5	74	105	256	217
11	103	242	60	28	145	197	240	75	51	1	49	225	218	11	60	147
12	112	208	100	125	236	176	143	130	109	214	53	233	22	23	134	101
13	172	65	30	253	13	165	236	68	180	73	186	103	2	205	135	95
14	16	96	110	221	123	33	164	57	135	196	99	89	120	182	124	146
15	113	237	98	128	20	252	207	238	241	204	154	202	200	116	133	250

Keyed Latin Square

The Latin square of order n is a grid with n distinct symbols, designed by Leonhard Euler. It is commonly used in games like Sudoku, where there are constraints on the block. For a given order n, there can be a large number of possible Latin squares, such as 10 power 37 for order 10. This is why Latin squares are used in image encryption algorithms.

Wu et al. in 2013 proposed an algorithm for developing a keyed Latin square, based on a 256-bit external key. This algorithm combines the strengths of both chaotic systems and the Latin square to create an effective image encryption algorithm.

Fisher-Yates Shuffle

The Fisher-Yates shuffling algorithm, first proposed in 1938 by Ronald Fisher and Frank Yates, is a method for shuffled arrays to ensure equal probability of permutations. Richard Furstenfeld later modified the algorithm to have a time complexity of *O(n)*, making it widely used due to its efficiency and unbiasedness. The algorithm starts with an array of n elements, iterates from 1 to 1, generates a random integer between 1 and *i*, swaps elements, and repeats until all elements are shuffled. The random generation of indices ensures unbiasedness. In this application, the algorithm is used to shuffle an initial array of 256 elements, representing an S-box. A piecewise linear chaotic map is incorporated for random generation, potentially improving security properties, especially in cryptographic applications.

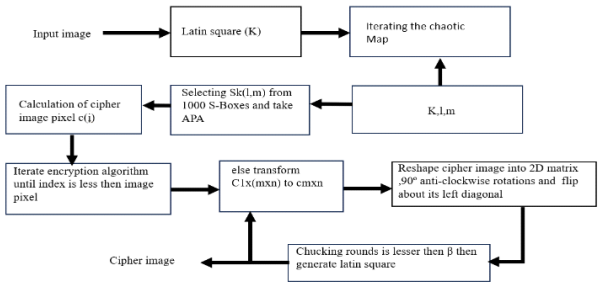


Fig. 1 Block diagram depicting the proposed image encryption algorithm

RESULTS

The suggested encryption technique Uses MATLAB 2011a, two 256×256 plain images are encrypted. The resultant encrypted photos show various properties. While the suggested algorithm produces virtually identical images with significant distortion, the other technique fails to meet expectations. The histogram analysis emphasizes the suggested scheme's advantages. Its encrypted images have a more uniform and flat distribution similar to noise, indicating strong encryption. The initial encryption settings are *K*='12A34F56E78D90C31B72AF4835DC0981237654CD185 A3FEB01CAE7259018FD14' , , *x(0)*=0.23456 and λ = 3.99, The encrypted images are shown in Fig. 2 and Fig. 3.

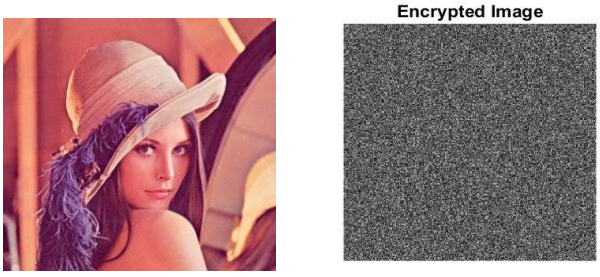


Fig. 2 Plain-images: (a) Lena (b) Encrypted images with proposed algorithm

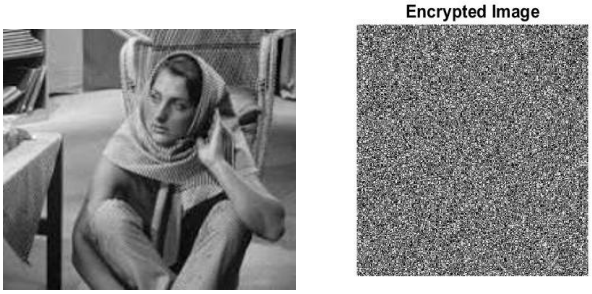
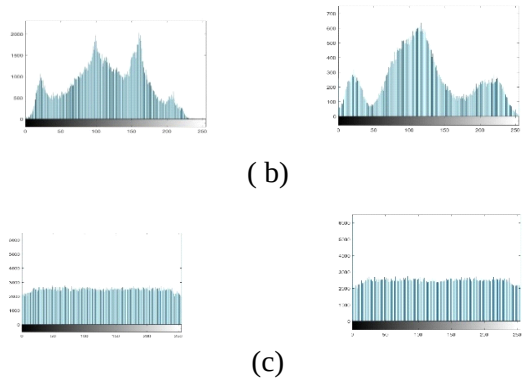


Fig. 3 Plain-images:(a) Barbara (b) Encrypted images with proposed algorithm

Histogram analysis

The distribution of pixel intensity levels in a image can be visually represented as a histogram. This is important for analyzing how various shade levels are dispersed throughout the image. A histogram may disclose a lot of vital information about an image, such as the existence of a specific pattern, the brightness, and so on. In theory, an encrypted image's histogram should be flat. Each pixel value should appear about equally frequently. This characteristic is critical for preventing statistical and frequency-based assaults. Encrypted images with flat histograms always contain relatively little information about the original image. Histogram analysis is shown in figure.



(b)

(c)

Fig. 5 histogram of (a) Lena (b) Barbara
(c) encrypted image

Correlation Coefficient

The correlation coefficient is a statistical metric that determines the degree and direction of a link between two variables. In the context of images, it may be used to calculate the similarity or dissimilarity of two photographs. To calculate the correlation coefficient between two photographs, each image is commonly represented as a matrix of pixel values. The correlation coefficient is then computed by comparing the similarity of comparable pixel values in the two photographs. A correlation coefficient of one shows a complete positive correlation, which means that the images are identical. A value of -1 denotes complete negative correlation, implying that the images are absolute opposites. A value of zero indicates no association, meaning that the images are wholly distinct. In image processing, correlation coefficients are used which is shown in figure.

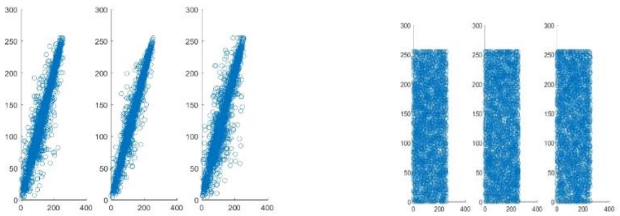


Fig. 6 Correlation Coefficient of (a) Lena (b) encrypted image

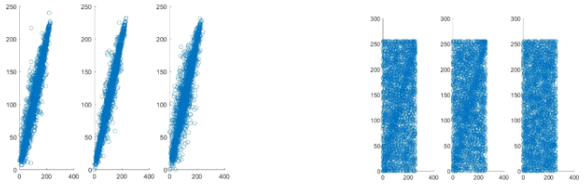


Fig. 7 Correlation Coefficient of (a) Barbara (b) encrypted image.

Pixel auto-correlation

Pixel auto-correlation, as used in image encryption, is the statistical link between the values of individual pixels in a image and their spatial locations. It calculates the degree to which the intensity values of pixels at various points in the image are correlated or similar. While low auto-correlation indicates randomness or lack of correlation, high auto-correlation indicates that nearby pixels are similar or show some pattern. In order to evaluate the security and efficacy of encryption algorithms, it is essential to analyze the pixel auto-correlation in encrypted images since it offers information about the level of distortion or randomness that is introduced during encryption. Robust encryption techniques strive to reduce auto-correlation in order to hinder adversaries from using spatial patterns or redundancies to crack the image.(4)

Image Entropy

The degree of uncertainty or unpredictability in an image's pixel values is measured by its entropy. It measures the degree of disarray or information included in the image. Entropy is an important parameter for evaluating the complexity and unpredictability added during the encryption process when it comes to image encryption. Greater complexity and unpredictability are indicated by higher entropy levels, which strengthen the encrypted image's defense against cryptographic assaults meant to extract the original content. To improve security, encryption methods aim to boost image entropy. This means that encrypted images are difficult to decipher without the right key and have a high degree of unpredictability. Cryptographers can determine the strength of encryption schemes and how resistant they are to different cryptanalytic approaches by studying image entropy. (5)

This indicates the optimal entropy value for message source S and corresponds to a real random source. An encrypted image would have an anomaly if its entropy was far lower than the optimal value of 8. potential for predictability, endangering the security of the image. Table 2 displays the information entropy for the original and encrypted photos. The proposed encryption system exhibits little information loss and is safe against the entropy attack, as demonstrated by the entropy measurements obtained for encrypted images.

Table 2. Entropy measures of images

Image name	Plain image	Reference	proposed
Lena	7.7598	7.956	7.9658
Barbara	7.6099	7.95	7.9644

Number of Pixels Change Rate

A statistic called Number of Pixels Change Rate (NPCR) is used to assess how well image encryption methods work, especially with regard to how well they can spread changes throughout the encrypted image. It calculates the fraction of pixel value changes that occur from minor changes in the plaintext between two encrypted images. More uniform dispersion of changes throughout the image is a sign of a more robust encryption algorithm against differential attacks, in which adversaries use the differences between plaintext and ciphertext to deduce encryption keys or obtain insight into the encryption process. This is indicated by a higher NPCR. Cryptographers are able to analyze the security strength and diffusion qualities of image encryption techniques by evaluating NPCR in conjunction with other metrics such as Unified Average Changing Intensity (UACI). (6)

Table 3. NPCR measures of images

Image name	Reference	proposed
Lena	99.589	99.59
Barbara	99.60	99.73

Unified averaged changed intensity

Unified Averaged Changed Intensity (UACI) is a statistic extensively used in image processing and computer vision. It is used to quantify the average intensity change throughout a series of photos or frames, which is important in activities like motion detection, image stabilization, and video processing. UACI assesses mobility or variations within a sequence of photographs by assessing changes in pixel intensity over time,

hence facilitating in the analysis and management of visual data. Its application extends to various domains, including surveillance, medical imaging, and entertainment, where accurate perception and interpretation of dynamic visual content are paramount.

Table 4. UACI measures of images

Image name	Reference	proposed
Lena	33.443	33.81
Barbara	33.51	33.816

CONCLUSION

In this research, we introduced a novel image encryption technique that generates 1000 dynamic S-boxes using Fisher-Yates shuffle and chaos, and then generates an encrypted image using Latin square, chaos, and an affine-power-affine structure. Our approach offers great security since it generates an S-box at random using a chaotic logistic map to replace an image pixel with a Latin square that is created from an external key, resulting in an encrypted image pixel. To guarantee that the cipher image has no association with the original image and to boost the technique's resilience, more than two encryption algorithm rounds are advised. The technique's key space is incredibly high, indicating that brute-force attacks are unlikely to succeed with our algorithm. Additionally, the results of the experiments and several security evaluations indicate that the suggested method is resistant to selected plaintext, known-plaintext assaults, and statistical attacks assault. The suggested approach performs better when compared to current image encryption techniques, demonstrating its exceptional applicability and practicability

References

1. Alabaichi, Ashwak Mahmood. 2016."Color image encryption using 3D chaotic map with AES key dependent S-Box." International Journal of Computer Science and Network Security (IJCSNS) 16.10 105-115.
2. Artiles, José AP, Daniel PB Chaves, and Cecilio Pimentel. 2019. "Image encryption using block cipher and chaotic sequences." Signal processing: image communication: 79 24-31.
3. Aslam, Mazzamal, et al.2022."A strong construction of S-box using Mandelbrot set an image encryption scheme." PeerJ Computer Science 8: e892.
4. Broumandnia, Ali.2019."The 3D modular chaotic map to digital color image encryption." Future Generation Computer Systems 99:489-499.
5. BUCHANAN, W. J.2017. “DNA and Plaintext Dependent Chaotic Visual Selective Image Encryption”.
6. Cassal-Quiroga, Bahia Betzavet, and Eric Campos-Cantón.(2020)."Generation of dynamical S-boxes for block ciphers via extended logistic map." Mathematical Problems in Engineering 2020:1-12.
7. Çavuşoğlu, Ünal, et al. 2017."Secure image encryption algorithm design using a novel chaos-based S-Box." Chaos, Solitons & Fractals 95:92-101.
8. Dey, Sankhanil, and Ranjan Ghosh.2018. "A review of cryptographic properties of S-boxes with Generation and Analysis of crypto secure S-boxes." Cryptology ePrint Archive.
9. ElBeltagy, Mohamed, et al. 2022."Image encryption through rössler system, prng s-box and recamán's sequence." 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). IEEE.
10. Jun, Wang Ji, and Tan Soo Fun. 9. 2021:"A new image encryption algorithm based on single S-box and dynamic encryption step." IEEE Access: 120596-120612.
11. Katiyar, Shishir, and N. Jeyanthi.2016."Pure dynamic S-box construction." International Journal of Computers 1.
12. Khan, Jansher, Jawad Ahmad, and Seong Oun Hwang. 2015."An efficient image encryption scheme based on: Henon map, skew tent map and S-Box." 2015 6th International conference on modeling, simulation, and applied optimization (ICMSAO). IEEE.
13. Lidong, Liu, et al. 2020). "A dynamic triple-image encryption scheme based on chaos, S-box and image compressing." IEEE Access 8:210382-210399.
14. Lu, Qing, Congxu Zhu, and Xiaoheng Deng. 2020. "An efficient image encryption scheme based on the LSS chaotic map and single S-box." IEEE Access 8:25664-25678.
15. Muhammad, Zahir Muhammad Ziad, and Fatih Özkaynak.2020."An image encryption algorithm based on chaotic selection of robust cryptographic primitives." IEEE Access 8:56581-56589.
16. Nizam Chew, Liyana Chew, and Eddie Shahril Ismail.2020."S-box construction based on linear fractional transformation and permutation function." Symmetry 12.5:826.
17. Ramasamy, Priya, et al.2019."An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map." *Entropy* 21.7:656.
18. Ramzan, Muhammad, et al.2021."Construction of s-boxes using different maps over elliptic curves for image encryption." IEEE Access 9:157106-157123.
19. Wang, Xiong, et al.2019."S-box based image encryption application using a chaotic system without equilibrium." Applied Sciences 9.4:781.
20. Zahid, Amjad Hussain, et al.2021."A novel construction of dynamic S-box with high nonlinearity using heuristic evolution." IEEE Access 9:67797-67812.
21. Zahid, Amjad Hussain, and Muhammad Junaid Arshad.2019."An innovative design of substitution-boxes using cubic polynomial mapping." Symmetry 11.3:437.
22. Zamli, Kamal Z.2021."Optimizing S-box generation based on the adaptive agent heroes and coward’s algorithm." Expert Systems with Applications 182:115305.
23. Zhu, Ding, et al. 2020."A new S-box generation method and advanced design based on combined chaotic system." Symmetry 12.12:2087.
24. Zhu, Shenli, et al.2023."Secure image encryption scheme based on a new robust chaotic map and strong S-box." Mathematics and Computers in Simulation 207:322-346.
25. Zhu, Shenli, Guojun Wang, and Congxu Zhu.2019."A secure and fast image encryption scheme based on double chaotic S-boxes." Entropy 21.8:790.

How to cite this article:
Anusha., Manasa Bhat., Medini Naik., N G Sowjanya., and Arun Upadhyaya. (2024). Chaoitic Dynamic S-Box Generation For Image Encryption. *Int J Recent Sci Res.* 15(05), pp.4721-4725.

****