Scientific Journal of Informatics
Vol. 10, No. 2, May 2023

p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

S-box Construction on AES Algorithm using Affine Matrix Modification to Improve Image Encryption Security

Alamsyah[1*], Budi Prasetiyo[2], Yusuf Muhammad[3]
[1,2,3]Department of Computer Science, Faculty of Mathematics and Natural Sciences, Universitas Negeri Semarang, Indonesia

Abstract.
Purpose: In this study, the AES algorithm was improved by constructing the S-box using a modified affine matrix and implementing it so that there was an increase in security in image encryption.
Methods: The method used in this study starts from selecting the best irreducible polynomial based on previous studies. The irreducible polynomial chosen is $x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$. With this irreducible polynomial, an inverse multiplicative matrix is formed. The formed inverse multiplicative matrix is implemented in the affine transformation process using the best three affine matrices based on previous research and 8-bit additional constants using AES S-box. This formulation produces three different S-boxes, i.e., S-box$_1$, S-box$_2$, and S-box$_3$. Finally, the resulting S-boxes are implemented to carry out the image encryption process and are tested for their security level.
Results: The test results show an increase in image encryption security compared to previous studies. The rise in security occurred at the entropy value of 7.9994 and the NPCR value of 99.6288%.
Novelty: The novelty of this paper is the improvement of the S-box construction implemented in image encryption resulting in increased security in image encryption.

Keywords: AES, S-box, Affine matrix, Affine transformation, Image encryption
Received January 2023 / **Revised** February 2023 / **Accepted** February 2023

INTRODUCTION

Information is precious and must be guarded so that it does not fall into the hands of irresponsible people. The development and progress of information technology every year are increasingly sophisticated and modern. New technologies have sprung up along with the times, which has made it easy to access information. Therefore data security is very important to develop. Security in data can be increased through algorithms that make it difficult for someone to solve it.

To determine whether an algorithm can secure data correctly, it can be seen in terms of the time the break-in process takes to solve the paired data. One of the algorithms that can handle and develop data security systems is the Advanced Encryption Standard (AES) algorithm [1], [2] where the original message or data is converted into a form of code that cannot be recognized or reread. The AES algorithm cannot run optimally without S-box [3], [4]. The S-box is a fundamental component in cryptography that exchanges values in a symmetric key that randomises input bits into output bits.

S-Box construction greatly affects a data's security level [5]–[7], especially in the process of encryption and decryption. In previous studies, the S-Box has been discussed. There is an S-box study based on images that use a chaotic system [8], [9], equilibrium point [10], and dynamic S-box [11]–[17].

Unfortunately, previous studies have not obtained optimal S-box construction results [18]–[20] on implementing the encryption process for image security [21]–[23]. In this study, the method used is the affine matrix which has been modified to increase the security of an image. An Affine matrix is an 8 X 8 matrix in which all elements consist of the numbers 0 or 1. An Affine matrix acts as a matrix transformation in forming an S-box.

[*]Corresponding author.
Email addresses: alamsyah@mail.unnes.ac.id
DOI: 10.15294/sji.v10i2.42305

METHODS

The proposed AES algorithm design flow is depicted as shown in Figure 1. Each of the steps in Figure 1 is explained in detail in the next section.

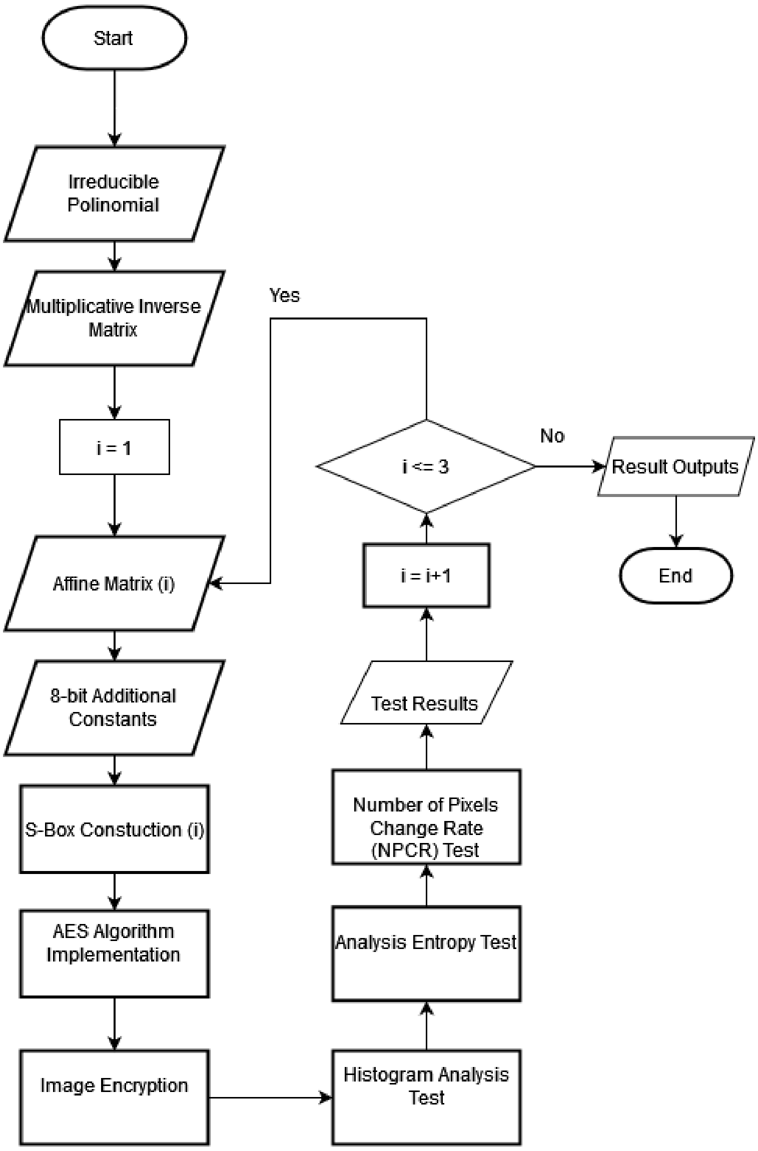


Figure 1. Flowchart of the proposed method

Irreducible Polynomial

An irreducible polynomial is a polynomial that is in the Galois field (GF 2^8) and has two factors, i.e., one and itself. The Irreducible polynomial in this study was taken from previous research, i.e., the optimal irreducible polynomial $x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$ [5], [6].

Multiplicative Inverse Matrix

The Multiplicative Inverse matrix is obtained from the calculation of the optimal irreducible polynomial $x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$. The multiplicative inverse matrix is presented in Table 1.

Table 1. The multiplicative inverse matrix

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

Affine matrix

An affine matrix measures 8 X 8, where the elements only consist of 0 and 1. An affine matrix is used for transformation in the formation of an S-box. The affine matrix used in this study is the optimal matrix based on previous research [5]–[7] found in Equations (1), (2), and (3).

$$A0 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad (1)$$

$$A1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (2)$$

$$A2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} \quad (3)$$

The 8-Bit Additional Constants

The additional 8-bit constants are part of the transformation in forming the S-box. The additional 8-bit constants consist of an 8 X 1 matrix whose elements only consist of the numbers 0 and 1. This study uses the additional 8-bit constants from the AES algorithm [1], as stated in Equation (4). The 8-bit additional constant is intended to provide initial values in the 0*th* row and 0*th* column of the resulting S-box.

$$C = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad (4)$$

S-box Construction

The formulation used to build the S-box uses the AES S-box formulation:

1. The multiplication inverse in a polynomial field GF(2^8) is a function that maps 8-bit input to 8-bit output, which is the inverse of the finite field elements. Each bit in a byte represents a polynomial coefficient.
2. Affine transformation (affine mapping) in the mapped state. Affine mapping, if it is mapped in matrix form, is presented as Equation (5)

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1\,1\,0\,0\,0\,0\,0\,1 \\ 1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\,0\,0\,0 \\ 0\,0\,0\,1\,1\,1\,0\,0 \\ 0\,0\,0\,0\,1\,1\,1\,0 \\ 0\,0\,0\,0\,0\,1\,1\,1 \\ 1\,0\,0\,0\,0\,0\,1\,1 \end{bmatrix} \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \text{mod } 2 \quad (5)$$

$b_7\ b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0$ is the sequence of bits in the state element or byte array where b_7 is the most significant bit or the bit with the leftmost position. Bits b_7, b_6, b_5, b_4, b_3. b_2, b_1, and b_0 are polynomial coefficients x_7, x_6, x_5, x_4, x_3, x_2, x, and x_0 respectively.

AES Algorithm Implementation

In this study, the AES algorithm used is the AES-128 version which uses ten rounds and has a fixed block size of 128 bits and a key size of 128. The process of encrypting data using the AES algorithm can go through the following four stages:

1. Add Round Key is a combination process of existing ciphertext with cipherkey with XOR relationship.
2. Sub Bytes is the process of exchanging the contents of an existing matrix/table with another matrix/table called the S-Box.
3. Shift Rows is a process that performs shifts or shifts on each block/table element carried out in each row.
4. Mix Columns is the process of transferring each element from the cipherblock to the matrix.

Image Encryption
Image encryption is a process to secure an image by randomizing the pixels contained in the image. If in image steganography [24] a secret message is inserted, in the AES Algorithm, the message is in the form of a secret image that is secured so unwanted parties cannot guess it. This process can be explained in Figure 2.

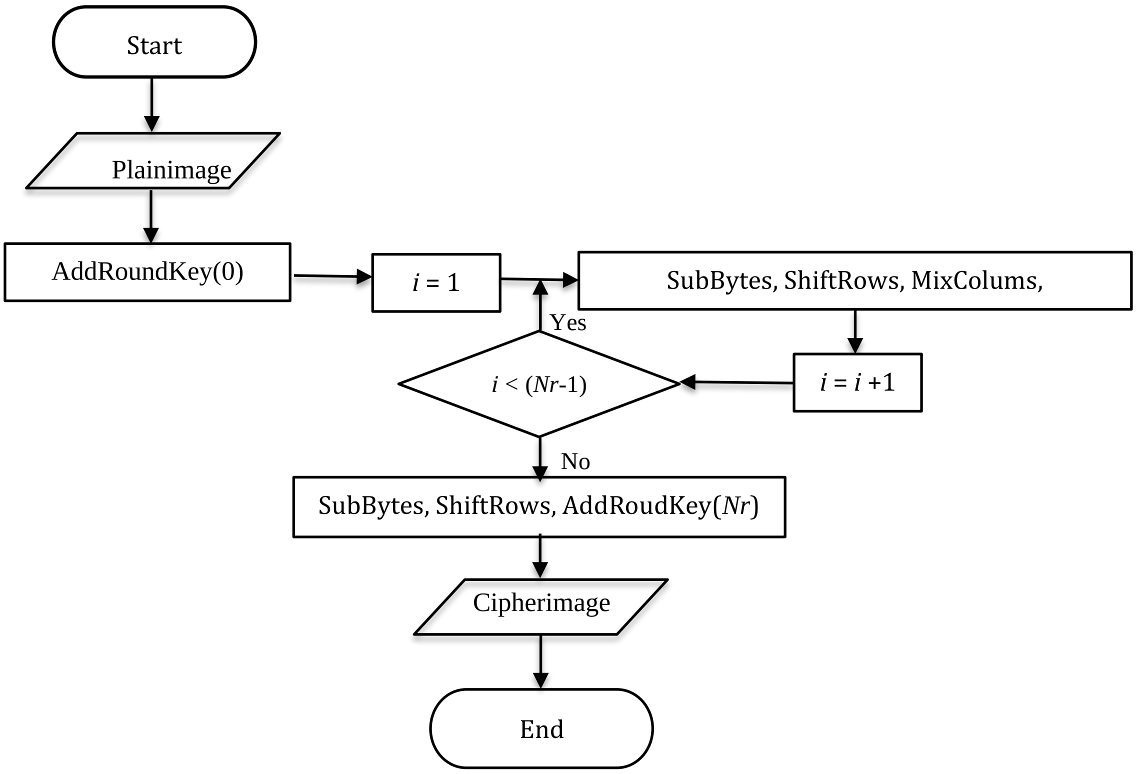


Figure 2. Image encryption process

Histogram Analysis Test
In the field of image processing, the histogram shows the distribution of pixel values in an image. The histogram is used to carry out attacks on encrypted images by utilizing the frequency of occurrence of pixels in the histogram. The attack can be in the form of matching the pixel values that frequently appear in the original image with those that frequently appear in the encrypted image. The attack will be difficult if a significant difference exists between the histogram on the original image and the histogram on the encrypted image. A good histogram on encrypted images is flat or statistically has a (relatively) uniform distribution.

Analysis Entropy Test
Entropy is the level of randomness of information that can interpret information or sources evenly. In this study, an analysis of entropy tests [20] was carried out to ensure that the image encryption process runs optimally. The entropy formulation is mathematically presented in Equation (6).

$$H(m) = \sum_{i=0}^{2m-1} P(m_i) log_2 \frac{1}{P(m_i)} \quad (6)$$

Where $P(m_i)$is the symbol probability (m_i) in the message, and entropy is expressed in bit units. The ideal value of the entropy test is 8. The closer to the value 8 is in the entropy value of the encrypted image, the more difficult it is to predict the image.

Number of Pixels Change Rate (NPCR) Test
The NPCR test is a type of sensitivity analysis [20] that functions to calculate the significant value of a ciphertext with a cipherkey or plaintext with a minimum difference presented in Equation (7)

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M*N}\ 100\% \quad (7)$$

where

$$D(i,j) = \begin{cases} 0, if\ C1(i,j) = C2(i,j) \\ 1, if\ C1(i,j) \neq C2(i,j) \end{cases}$$

M = image width

N = image length

$D(i,j)$ = the value of the two images being compared (0 or 1)

$C1(i,j)$= cipher-image1

$C2(i,j)$= cipher-image2

The ideal NPCR value is 100%. The closer to 100% the NPCR value, the stronger the resulting image encryption against various attacks.

RESULTS AND DISCUSSIONS

S-Box Construction Results

The results of the S-Box construction are obtained by using the inverse multiplicative matrix in Table and applying the formulation to Equation (5) and modifying it into Equations (8), (9), and (10) by substituting the affine matrices [5] $A0$, $A1$, and A.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \quad (8)$$

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \quad (9)$$

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \bmod 2 \quad (10)$$

The results are S-box$_1$ listed in Table 2, S-box$_2$ listed in Table 3, and S-box$_3$ listed in Table 4.

Table 2. S-box$_1$

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

Table 1. S-box$_2$

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

Table 4. S-box$_3$

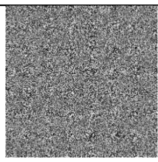
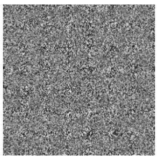
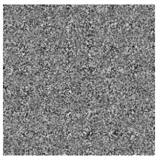
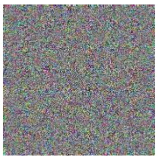
Y

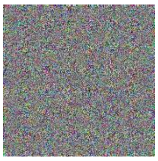
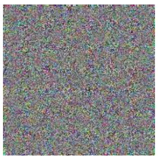
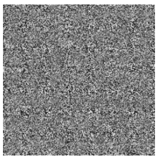
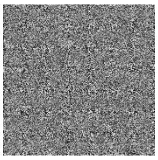
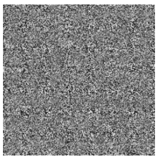
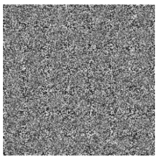
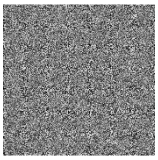
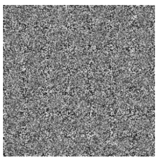
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	99	151	166	26	62	158	223	31	114	157	34	190	130	211	93	29
	1	84	182	163	240	195	85	141	38	147	209	132	28	124	40	92	115
	2	248	185	137	104	188	131	170	90	51	94	120	13	20	156	193	86
	3	164	110	133	5	144	18	220	88	83	117	198	145	252	101	212	142
	4	174	199	14	27	22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

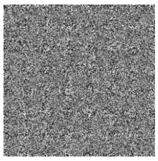
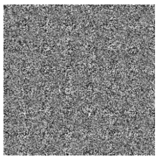
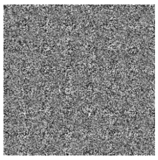
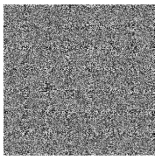
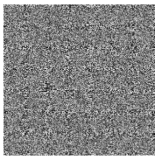
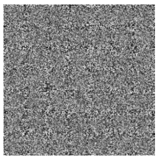
Image Encryption Results

The results of image encryption use seven images, i.e., cameraman, lena_color_512, livingroom, mandril_color, pirate, woman_blonde, and woman_darkhair. The S-boxes used are S-box$_1$, S-box$_2$, and S-box$_3$, made in a table listed in Table 5.

Table 5. Image encryption results

Image	**Plain image**	**S-box**	**Cipherimage**
cameraman		S-box$_1$	
cameraman		S-box$_2$	
cameraman		S-box$_3$	
lena_color_512		S-box$_1$	

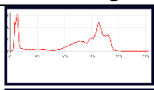
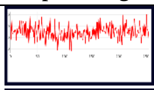
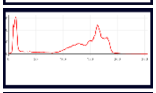
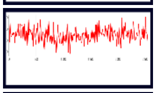
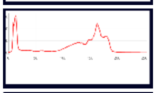
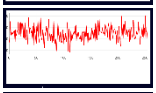
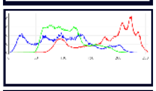
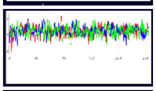
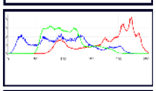
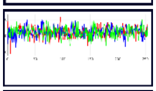
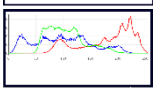
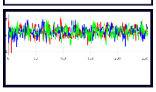
lena_color_512		S-box$_2$	
lena_color_512		S-box$_3$	
livingroom		S-box$_1$	
livingroom		S-box$_2$	
livingroom		S-box$_3$	
mandril_color		S-box$_1$	
mandril_color		S-box$_2$	
mandril_color		S-box$_3$	
pirate		S-box$_1$	
pirate		S-box$_2$	
pirate		S-box$_3$	

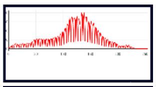
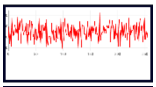
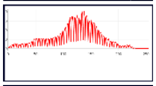
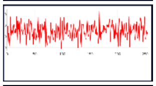
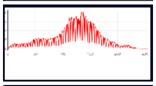
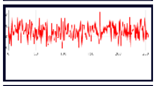
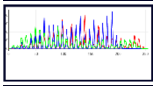
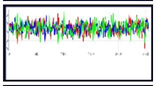
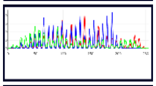
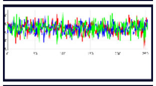
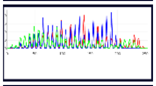
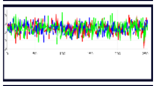
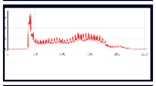
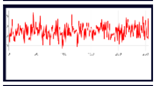
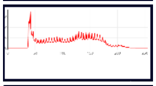
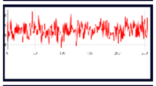
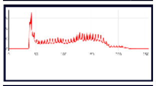
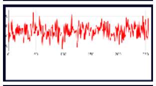
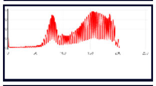
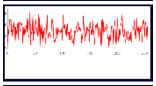
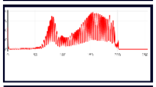
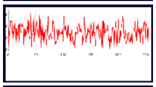
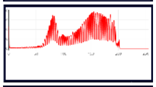
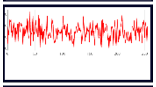
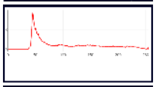
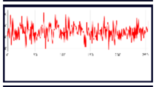
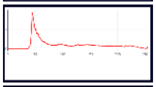
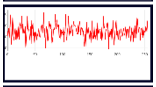
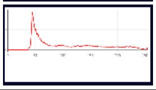
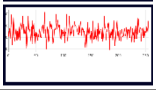
woman_blonde		S-box$_1$	
woman_blonde		S-box$_2$	
woman_blonde		S-box$_3$	
woman_darkhair		S-box$_1$	
woman_darkhair		S-box$_2$	
woman_darkhair		S-box$_3$	

Histogram Analysis Test Results

The original image histogram test results and image encryption using seven images, i.e., cameraman, lena_color_512, livingroom, mandril_color, pirate, woman_blonde, and woman_darkhair. The S-boxes used are S-box$_1$, S-box$_2$, and S-box$_3$, made in a table listed in Table 6.

Table 6 Original image and image encryption histogram test results

Image	S-box	Histogram Analysis					
		Plain image	Cipherimage	GR	R	G	B
cameraman	S-box$_1$			256	-	-	-
cameraman	S-box$_2$			256	-	-	-
cameraman	S-box$_3$			256	-	-	-
lena_color_512	S-box$_1$			-	256	255	256
lena_color_512	S-box$_2$			-	256	255	256
lena_color_512	S-box$_3$			-	256	255	256

livingroom	S-box$_1$			256	-	-	-
livingroom	S-box$_2$			256	-	-	-
livingroom	S-box$_3$			256	-	-	-
mandril_color	S-box$_1$			-	256	256	256
mandril_color	S-box$_2$			-	256	256	256
mandril_color	S-box$_3$			-	256	256	256
pirate	S-box$_1$			256	-	-	-
pirate	S-box$_2$			256	-	-	-
pirate	S-box$_3$			256	-	-	-
woman_blonde	S-box$_1$			256	-	-	-
woman_blonde	S-box$_2$			256	-	-	-
woman_blonde	S-box$_3$			256	-	-	-
woman_darkhair	S-box$_1$			256	-	-	-
woman_darkhair	S-box$_2$			256	-	-	-
woman_darkhair	S-box$_3$			256	-	-	-

Based on Table 6, the histogram test results show a significant difference between the original and encrypted images. Encrypted images tend to be flatter, indicating that encrypted images are difficult to guess.

Entropy Analysis and NPCR Test Results

Entropy Analysis and NPCR Test Results used seven images, i.e., cameraman, lena_color_512, livingroom, mandril_color, pirate, woman_blonde, and woman_darkhair. The S-boxes used are S-box$_1$, S-box$_2$, and S-box$_3$, made in a table listed in Table 7.

Table 7. Entropy analysis and NPCR test results

Image	S-box	Entropy Analysis		NPCR
		Plain image	Cipherimage	
cameraman	S-box_1	7.0480	7.9994	99.6231
cameraman	S-box_2	7.0480	7.9994	99.6231
cameraman	S-box_3	7.0480	7.9994	99.6231
lena_color_512	S-box_1	7.2719	7.9993	99.6056
lena_color_512	S-box_2	7.2719	7.9993	99.6056
lena_color_512	S-box_3	7.2719	7.9993	99.6056
livingroom	S-box_1	7.2952	7.9992	99.6208
livingroom	S-box_2	7.2952	7.9992	99.6208
livingroom	S-box_3	7.2952	7.9992	99.6208
mandril_color	S-box_1	6.8455	7.9993	99.6115
mandril_color	S-box_2	6.8455	7.9993	99.6115
mandril_color	S-box_3	6.8455	7.9993	99.6115
pirate	S-box_1	7.2367	7.9992	99.5934
pirate	S-box_2	7.2367	7.9992	99.5934
pirate	S-box_3	7.2367	7.9992	99.5934
woman_blonde	S-box_1	6.9542	7.9993	99.6288
woman_blonde	S-box_2	6.9542	7.9993	99.6288
woman_blonde	S-box_3	6.9542	7.9993	99.6288
woman_darkhair	S-box_1	7.2767	7.9994	99.6235
woman_darkhair	S-box_2	7.2767	7.9994	99.6235
woman_darkhair	S-box_3	7.2767	7.9994	99.6235

The entropy testing process on the original image and the image resulting from the analysis shows a significant difference in value. The results of the entropy test on encrypted images have increased significantly and are close to the ideal number, which is 8.00. The S-box selection factor does not affect the resulting entropy value. Every use of a different S-box, S-box_1, S-box_2, and S-box_3 still produces the same entropy value. Likewise, with the type of image, both color and black-and-white (grayscale) images tend to have nearly the same entropy value. Based on Table 7, the entropy test results are very close to the ideal number of 8.00. Entropy test results on encrypted images have the highest value of 7.9994 and the lowest of 7.9992. This shows that the resulting image encryption is strong against entropy attacks.

The NPCR testing process on the encrypted images has the same value for each S-box used. Based on Table 7, the NPCR test results are all close to the ideal value of 100%. This shows that the resulting image encryption results are very difficult to predict. The NPCR test results on encrypted images have the highest value of 99.6288% and the lowest value of 99.5934%.

Performance Comparison Analysis

To find out the performance of the resulting algorithm, a comparison is made with the results of previous research by selecting one of the tests carried out on the same dataset. Performance comparisons were made with studies that took the same test model, i.e., entropy and NPCR tests. A comparison of entropy and NPCR values are presented in Table 8.

Table 8. Performance comparison of entropy and NPCR test results

Cipherimage	Entropy	NPCR (%)
In [25]	7.9954	99.5834
In [8]	7.9974	99.6048
Proposed Method	7.9994	99.6288

Based on Table 8, the proposed method obtains higher entropy and NPCR test results than previous studies that applied the same test model.

CONCLUSION

The S-Box construction design using a modified affine matrix produces three new S-boxes called S-box$_1$, S-box$_2$, and S-box$_3$. The results of implementing S-box$_1$, S-box$_2$, and S-box$_3$ can improve image security after testing. An indicator of an increase in image security can be seen from histogram testing results, which have a uniform (flat) tendency, entropy with a value of 7.9994, and NPCR with a value of 99.6288%. These results indicate that strong S-box construction can improve the security of image encryption.

REFERENCES

[1] J. Daemen and V. Rijmen, *The Design of Rijndael*. Springer-Verlag Berlin Heidelberg New York, 2002. doi: 10.1007/978-3-662-04722-4.

[2] J. Daemen and V. Rijmen, “New criteria for linear maps in AES-like ciphers,” no. November 2007, 2008, doi: 10.1007/s12095-008-0003-x.

[3] W. Stallings, *C Ryptography and Network Security: Principles and Practice*, Seventh Ed. Pearson, 2017.

[4] C. Paar and J. Pelzl;, *Understanding Cryptography*, 1st ed., vol. 1. Springer-Verlag Berlin Heidelberg, 2010. doi: 10.1017/CBO9781107415324.004.

[5] Alamsyah, A. Bejo, and T. B. Adji, “The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box,” *Nonlinear Dyn.*, vol. 93, no. 4, pp. 2105–2118, 2018, doi: 10.1007/s11071-018-4310-2.

[6] Alamsyah, “Improving the Quality of AES S-box by Modifications Irreducible Polynomial and Affine Matrix,” 2020. doi: 10.1109/ICIC50835.2020.9288567.

[7] Alamsyah, “A Novel Construction of Perfect Strict Avalanche Criterion S-box using Simple Irreducible Polynomials,” *Sci. J. Informatics*, vol. 7, no. 1, pp. 10–22, 2020, doi: 10.15294/sji.v7i1.24006.

[8] J. Zheng and Q. Zeng, “An image encryption algorithm using a dynamic S-box and chaotic maps,” *Appl. Intell.*, vol. 52, no. 13, pp. 15703–15717, 2022, doi: 10.1007/s10489-022-03174-3.

[9] A. Mahboob, M. Asif, M. Nadeem, A. Saleem, S. M. Eldin, and I. Siddique, “A Cryptographic Scheme for Construction of Substitution Boxes using Quantic Fractional Transformation,” *IEEE Access*, vol. PP, p. 1, 2022, doi: 10.1109/ACCESS.2022.3230141.

[10] A. Alkhayyat, M. Ahmad, N. Tsafack, M. Tanveer, D. Jiang, and A. A. Abd El-Latif, “A Novel 4D Hyperchaotic System Assisted Josephus Permutation for Secure Substitution-Box Generation,” *J. Signal Process. Syst.*, vol. 94, no. 3, pp. 315–328, 2022, doi: 10.1007/s11265-022-01744-9.

[11] H. Zhu, X. Tong, Z. Wang, and J. Ma, “A novel method of dynamic S-box design based on combined chaotic map and fitness function,” *Multimed. Tools Appl.*, vol. 79, no. 17–18, pp. 12329–12347, 2020, doi: 10.1007/s11042-019-08478-0.

[12] A. H. Zahid *et al.*, “Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation for Security Applications,” *IEEE Access*, vol. 9, pp. 98460–98475, 2021, doi: 10.1109/ACCESS.2021.3095618.

[13] R. Hoseini, S. Behnia, S. Sarmady, and S. Fathizadeh, “Construction of dynamical S-boxes based on image encryption approach,” *Soft Comput.*, vol. 26, no. 24, pp. 13985–13997, 2022, doi: 10.1007/s00500-022-07443-8.

[14] S. Ibrahim and A. M. Abbas, “A Novel Optimization Method for Constructing Cryptographically Strong Dynamic S-Boxes,” *IEEE Access*, vol. 8, pp. 225004–225017, 2020, doi: 10.1109/ACCESS.2020.3045260.

[15] W. J. Jun and T. S. Fun, “A New Image Encryption Algorithm Based on Single S-Box and Dynamic Encryption Step,” *IEEE Access*, vol. 9, pp. 120596–120612, 2021, doi: 10.1109/ACCESS.2021.3108789.

[16] X. Wang and J. Yang, “A novel image encryption scheme of dynamic S-boxes and random blocks based on spatiotemporal chaotic system,” *Optik (Stuttg).*, vol. 217, no. May, p. 164884, 2020, doi: 10.1016/j.ijleo.2020.164884.

[17] A. Shafique and F. Ahmed, “Image Encryption Using Dynamic S-Box Substitution in the Wavelet Domain,” *Wirel. Pers. Commun.*, vol. 115, no. 3, pp. 2243–2268, 2020, doi: 10.1007/s11277-020-07680-w.

[18] R. H. Sani, S. Behnia, and J. Ziaei, “Construction of S-box based on chaotic piecewise map: Watermark application,” *Multimed. Tools Appl.*, 2022, doi: 10.1007/s11042-022-13278-0.

[19] R. H. Sani, S. Behnia, and A. Akhshani, “Creation of S-box based on a hierarchy of Julia sets: image encryption approach,” *Multidimens. Syst. Signal Process.*, vol. 33, no. 1, pp. 39–62, 2022, doi: 10.1007/s11045-021-00786-9.

[20] Y. Su, X. Tong, M. Zhang, and Z. Wang, “A new S-box three-layer optimization method and its application,” *Nonlinear Dyn.*, vol. 9, 2022, doi: 10.1007/s11071-022-07956-9.
[21] C. Yang, I. Taralova, S. El Assad, and J. J. Loiseau, “Image encryption based on fractional chaotic pseudo-random number generator and DNA encryption method,” *Nonlinear Dyn.*, vol. 109, no. 3, pp. 2103–2127, 2022, doi: 10.1007/s11071-022-07534-z.
[22] F. Masood *et al.*, “A new color image encryption technique using DNA computing and Chaos-based substitution box,” *Soft Comput.*, vol. 26, no. 16, pp. 7461–7477, 2022, doi: 10.1007/s00500-021-06459-w.
[23] M. Tanveer *et al.*, “Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box,” *IEEE Access*, vol. 9, pp. 73924–73937, 2021, doi: 10.1109/ACCESS.2021.3081362.
[24] Alamsyah, M. A. Muslim, and B. Prasetiyo, “Data hiding security using bit matching-based steganography and cryptography without change the stego image quality,” *J. Theor. Appl. Inf. Technol.*, vol. 82, no. 1, pp. 106–112, 2015.
[25] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, “A novel image encryption scheme based on DNA sequence operations and chaotic systems,” *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, 2019, doi: 10.1007/s00521-017-2993-9.