Multidimensional Systems and Signal Processing (2020) 31:885–905
https://doi.org/10.1007/s11045-019-00689-w

A novel efficient image encryption algorithm based on affine transformation combine with linear fractional transformation

Dawood Shah[1] · Tariq Shah[1] · Sajjad Shaukat Jamal[2]

Received: 20 April 2019 / Revised: 11 July 2019 / Accepted: 28 October 2019 / Published online: 6 November 2019

Abstract
Algebraic structures and their hardware–software implementation gain considerable attention in the field of information security and coding theory. Research progress in the applications of arithmetic properties of algebraic structures is being frequently made. These structures are mostly useful in improvement of the cryptographic algorithms. A novel technique is given to design a cryptosystem responsible for lossless for image encryption. The proposed scheme is for the RGB image whose pixels are considered as 24 binary bits, accordingly a unique arrangement for the construction of S-boxes over a Galois field $GF(2^9)$ is employed. Consequently, it generates multiple different S-boxes with excellent cryptographic characteristic and hence confusing process of the cryptosystem has been working. Whereas the diffusion process in this cryptosystem is based on Affine transformation over a unit elements of an integers modulo ring $\mathbb{Z}_n$. The scrambling of the image data through the Affine transformation escalate the security asset, avoid computational effort and abbreviated the time complexity. In addition, the simulation test and comparative scrutinize illustrate that the proposed scheme is highly sensitive, large keyspace, excellent statistical properties and secure against differential attacks. Therefore, the proposed algorithm is valuable for confidential communication. Furthermore, due to the arithmetic properties of algebraic structures, the proposed scheme would be easily implemented, secure and fast enough to be utilized in real-world applications.

Keywords Galois field · Substitution boxes · Affine transformation · LFT

1 Introduction

Nowadays, the rapid expansion of internet and digital media, data can easily be shared and store among interconnected parties. However, due to the openness of the network, the sharing or storing of that information is threatened. Cryptography is the study of techniques,

✉ Dawood Shah
dawoodshah@math.qau.edu.pk

[1] Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

[2] Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

which are used to protect digital information and control access toward it. Many cryptographers have come up with numerous cryptosystems which include data encryption standard (DES) and advanced encryption standard (AES) (Tuchman 1979; Daemen and Rijmen 2002). AES is the most popular and effective algorithm using broadly to cryptographic applications. This algorithm was submitted by Joan Daemen and Vincent Rijmen to the National Institute of Standards (NIST) which has been formally accepted in October 2000 (Tuchman 1979). AES algorithm built on four steps, round key addition, byte substitution, shift row, and the mix column. Byte substitution is the most significant, use to produce confusion between key and ciphertext by means of substitution box (S-box). Accordingly, the robustness of the cryptosystem has been deeply associated with the quality of S-box. The S-box used in AES is based on the Galois field of order 256, which comprises good cryptographic properties. In view of that AES is the most secure and widely used cryptosystem for confidential communication. However, the cryptosystems like AES is not appropriate for multimedia data due to strong correlation, bi-dimensionality and high redundancy of data. Keeping this in mind, Fridrich proposed cryptosystem on the chaotic map in 1998 (Fridrich 1998). Later researcher elaborates that the foremost properties of a chaotic map like sensitivity to the initial condition and control parameters are equivalent to the desired cryptographic properties, thus the image encryption algorithms established on the chaotic map have been widely studied (Li et al. 2005, 2008; Lian et al. 2005; Wang et al. 2009a, b; Amin et al. 2010; Pisarchik et al. 2006; Wong et al. 2008; Alvarez and Li 2006; Naseer et al. 2019a; Chiaraluce et al. 2002; Gao and Chen 2008; Patidar et al. 2009; Behnia et al. 2008; Shah et al. 2018). Afterward, the cryptographers reveals the defect in the internal structure of different chaos-based cryptosystems (Li et al. 2012; Zhang et al. 2012, 2014, 2015; Liu et al. 2016). Li et al. studied the cryptosystem given in Li et al. (2012) and expose that the only permutation substitution part can be demolished with the chosen plain text attack (Wang et al. 2012). Zhang et al. have examined that the security strength of an image encryption algorithm is based on perception model (Wang et al. 2015) and established that the analogous secret key can be reassembled with only single pair of identified plaintexts or ciphertexts (Zhang et al. 2012). The hyperchaotic system-based image cipher with the single round diffusion process is given in Norouzi et al. (2014). The fact that known and chosen-plaintext attacks are valuable to break this scheme is revealed by Zhang et al. (2014b). Image encryption scheme depends on three cells chaotic system blend with DNA was introduced by Saberi et al. (2014). Zhang et al. recently scrutinized and disclose the weakness of the scheme against chosen-plaintext attack (Zhang et al. 2015). Liu et al. (2016) has studied the cryptosystems which practice on one round revised permutation–diffusion and reported that this type of systems hurt from the weakness against the chosen plaintext attack. Therefore, the need for designing better cipher schemes based on S-boxes and chaos is essential for encryption applications and stimulating further development. In Zhu et al. (2011), Fridrich proposed a new cryptosystem which involves the bit level permutation. This replacement of pixel permutation with bit level permutation enables the change in both the position and value of the pixel. Wang et al. identified that if the plaintexts consists of identical pixels, then the confusion and diffusion are considered as two independent processes. So, it is necessary to keep the parameters for both confusion and diffusion must be fixed (Li et al. 2005). This will not only remove the effect of confusion but put an extra burden on diffusion and hence the cryptosystem becomes vulnerable to many malicious attacks. The Fridrich confusion-diffusion model has three loopholes which can allow invaders to attack this cryptosystem. Firstly, the effect of confusion is eliminated by the selection of a homogeneous image having identical pixels. Moreover, the chosen plaintext attacks help to obtain the key-stream of the diffusion phase and lastly, with the help of chosen-plaintext attacks the permutation

only cipher image is proven to be insecure (Pisarchik et al. 2006; Liu et al. 2016; Wang et al. 2012; Norouzi et al. 2014). The encryption schemes that used one round adapted permutation diffusion are analyzed in Liu et al. (2016). The author assumed that the scheme which uses single round modified permutations are weak against the chosen plain text attack. Therefore good quality S-box is essential for the secure encryption scheme. In the recent decade, many algorithms for the construction of S-box and image encryption algorithms amalgamate S-box with the different chaotic system as represented in Gan et al. (2018a), Shah and Shah (2019), Naseer et al. (2019b), Hussain et al. (2012), Liu et al. (2015), Zhang et al. (2014a), Belazi et al. (2016), Hussain and Gondal (2014), Wang and Wang (2014). A color image encryption technique using one-time S-boxes is being proposed by Liu et al. (2015) and these S-boxes were constructed with the help of a chaotic system. The Chen chaotic system has been used for the construction of S-boxes for image encryption technique by Zhang et al. (2014a). Moreover, a novel chaotic image encryption technique is presented in Belazi et al. (2016) whereas the S-boxes are used for block cipher substitution to obtain confusion. The chaotic coupled map and linear fractional S-boxes have been used by Hussain and Gondal (2014). On the other hand, these image encryption techniques have certain flaws which affect the validity of these schemes. For example, Wang and Wang (2014) proposed an image encryption scheme using S-boxes constituted through Logistic and Tent maps. Though this technique survives against chosen-plaintext attacks as this technique follows group substitution encryption hence, the correlation between adjacent pixels in a group cannot be reduced completely. Similarly, many other drawbacks prompt researchers to develop such image encryption techniques which are flawless and survive against different attacks.

In this paper, an efficient algorithm for the construction of multiple S-boxes is proposed based on the finite field of order 512. Then by utilizing the proposed method, a new algebraic cryptosystem for image encryption based on substitution-permutation is presented. First, the RGB image is split into three components Red (R), Green (G) and Blue (B). Then Affine transformation is used to shuffle the components of the image. To produce confusion, the suggested multiple S-boxes construction method is deployed to substitute the shuffle components of the image. Finally, a rough sequence is generated using the multiplicative operation of finite field and carried out Xor operation to produce more randomness in the substituted components of the image. The proposed scheme is tested over different analysis and compare the analysis with the existing schemes. The results show that the proposed scheme is quite better and suitable for secure communication.

The rest of the paper is organized as follows: The S-boxes construction method and performance analyses are given in Sect. 2. Section 3 is devoted to image encryption algorithm. Section 4 elaborates the performance analysis of the planned cryptosystem. In the last Sect. 5, we conclude the discussion.

2 S-boxes construction methods

In this study, the extension filed of order 2^9 has special attention. For the synthesis of Galois field $\mathbb{F}_{512}$ we select a degree-9 primitive irreducible polynomial (PIP) $r(x)$ in the Euclidean domain (ED) $\mathbb{Z}_2[x]$. The PIP generates the maximal ideal of the ED. The quotient group $\frac{\mathbb{Z}_2[x]}{\langle r(x)\rangle}$ is isomorphic to $\mathbb{Z}_2[\alpha]$, where α is the root of irreducible polynomial $r(x)$. The designing technique of the multiple S-boxes is based on the action of projective general linear group $PGL\left(2, \frac{\mathbb{Z}_2[x]}{\langle r_i(x)\rangle}\right)$ on a Galois field $\frac{\mathbb{Z}_2[x]}{\langle r_i(x)\rangle}$), called linear fractional transformation (LFT). Thus, the LFT operated for the invention of S-boxes. Mathematically, defined as;

$$g_i : PGL\left(2, \frac{\mathbb{Z}_2[x]}{\langle r_i(x)\rangle}\right) \times \frac{\mathbb{Z}_2[x]}{\langle r_i(x)\rangle} \to \frac{\mathbb{Z}_2[x]}{\langle r_i(x)\rangle}$$
$$g_i(z) = \frac{az+b}{cz+d} \text{ where } a, b, c, d \in \frac{\mathbb{Z}_2[x]}{\langle r_i(x)\rangle}. \tag{1}$$

The order of degree 9 PIP in the ED $\mathbb{Z}_2[x]$ is 48, so one can choose any of them. For the construction of multiple S-boxes, the method initiates with the action of $PGL\left(2, \frac{\mathbb{Z}_2[x]}{\langle r(x)\rangle}\right)$ on $\frac{\mathbb{Z}_2[x]}{\langle r_i(x)\rangle}$, for any fixed i, the mapping g_i is the bijective mapping from the Galois field $\mathbb{F}_{512}$ to $\mathbb{F}_{512}$. Then use the inclusion map, which is defined as follows:

$$I_{\mathbb{F}_{256}} : \mathbb{F}_{512} \to \mathbb{F}_{256}$$

$$I_{\mathbb{F}_{256}}(x) = \begin{cases} x & if\ x \le 255 \\ 0 & if\ x > 255 \end{cases} \tag{2}$$

$$I'_{\mathbb{F}_{256}}(x) = \begin{cases} x - 256 & if\ x \ge 255 \\ 0 & if\ x < 255 \end{cases} \tag{3}$$

Ultimately, the composition map $I_{\mathbb{F}_{256}} o g_i$ generates the S-box denoted as S_1. Similarly, the composition of $I'_{\mathbb{F}_{256}} o g_i$ generates the second S-box signify as S_2. The third S-box is obtained by substituting S_1 over S_2. Further, the details procedure of the multiple S-box constructions is shown in Table 1. In Table 1, column 1 denotes the elements of $\frac{\mathbb{Z}_2[x]}{\langle r_i(x)\rangle}$ ranging from 0 to 511. Column 2 represents the analytical details of the linear fractional transformation and the results from the evaluation of g_i(z) are listed. Columns (3–5) shows the elements of the S-boxes (1–3) respectively.

3 Proposed algorithm

The proposed S-box construction technique generates good quality S-boxes, which are suitable for image encryption application. In this section, we introduced a novel image encryption scheme named algebraic algorithm as the algebraic operation is used in their internal structure. The input of the algorithm is an RGB 24-bit image. Initially, the image is divided into three color components, each component is a data matrix with $N \times M$ size. The color components are encrypted individually using the S-boxes and the affine transformation over a finite ring.

Table 1 S-box construction based on linear fraction transformation

$GF(2^9)$	$f_M(x) = 100x + 160/189x + 198$	$GF(2^9)$	S_1	S_2	S_3
0	$f_M(0) = 100(0) + 160/189(0) + 198 = 167/501$	497	0	241	226
1	$f_M(1) = 100(0) + 160/189(0) + 198 = 257/399$	68	68	0	12
.	.	.	.	.	.
.	.	.	.	.	.
255	$f_M(254) = 100(0) + 160/189(0) + 198 = 257/399$	90	184	0	56
.	.			.	.
.	.			.	.
510	$f_M(510) = 100(0) + 160/189(0) + 198 = 166/481$	143	143	0	.
511	$f_M(511) = 100(0) + 160/189(0) + 198 = 256/411$	444	0	188	.

Ultimately, after encrypting all components are combined with each to form a new encrypted image. The proposed scheme is performed in two stages comprising confusion and diffusion that are elaborated as follows:

3.1 Diffusion

The digital image data have robust correlations between any two adjacent pixels. The statistical analysis on considerable images elaborates that usually 8–16 adjacent pixels be correlative in the vertical diagonal and horizontal direction for computer graphical images and natural images as well. In this study, we used affine transformation to embezzle the position of the pixels in the plain image to disturb the high correlation among the adjacent pixels. We assume the dimension of the image $N \times M$. The affine transformation is described as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} x \times p_1^{R,G,B} + q_1^{R,G,B} \bmod N \\ y \times p_2 + q_2 \bmod M \end{bmatrix} \quad \text{if} \quad \begin{matrix} x \times p_1^{R,G,B} + q_1^{R,G,B} \bmod N \neq 0 \\ y \times p_2^{R,G,B} + q_2^{R,G,B} \bmod M \neq 0 \end{matrix} \tag{4}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} x \times p_1^{R,G,B} + q_1^{R,G,B} \bmod N \\ M \end{bmatrix} \quad \text{if} \quad \begin{matrix} x \times p_1^{R,G,B} + q_1^{R,G,B} \bmod N \neq 0 \\ y \times p_2^{R,G,B} + q_2^{R,G,B} \bmod M = 0 \end{matrix} \tag{5}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} N \\ y \times p_2^{R,G,B} + q_2^{R,G,B} \bmod M \end{bmatrix} \quad \text{if} \quad \begin{matrix} x \times p_1^{R,G,B} + q_1^{R,G,B} \bmod N = 0 \\ y \times p_2^{R,G,B} + q_3^{R,G,B} \bmod M \neq 0 \end{matrix} \tag{6}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} N \\ M \end{bmatrix} \quad \text{if} \quad \begin{matrix} x \times p_1^{R,G,B} + q_1^{R,G,B} \bmod N = 0 \\ y \times p_2^{R,G,B} + q_3^{R,G,B} \bmod M = 0 \end{matrix} \tag{7}$$

where p_1 and p_2 the positive prime number, q_1 and q_2 are any positive integer. The prime number avoid the zero divisors, accordingly, the affine transformation for the prime number is bijective over a finite ring. Thus the position (x, y) of all pixels of the original image is swap to (x', y'). The images once applying the affine transformation is shown in the Fig. 2b.

3.2 Confusion

The xor operation is essential to ensure that the proposed scheme is secure against the histogram attack. Hence we generate the chaotic matrices x_n and y_n and of size $N \times M$ using Ginger breadman map in the condition of initial x_1 and y_1. Formerly chaotic matrices are the map from $[-4, 8]$ to the set $\{0, 1, 2, \ldots 255\}$ using Eqs. (10) and (11).

$$x_{i+1} = 1 + y_i + |x_i| \tag{8}$$

$$y_{i+1} = x_i \tag{9}$$

$$x_i = mod(x_i \times 10^{10}, 256) \tag{10}$$

$$y_i = mod(x_i \times 10^{10}, 256) \tag{11}$$

$$z_i = bitxor(x_i, y_i) \tag{12}$$

Then carried out the xor operation. A substitution operation is essential to ensure that the proposed scheme is secure against the chosen plain text attack. The three S-boxes

is generated denoted by S_1, S_1 and S_3 employing the procedure described in Sec. 2. The scrambled RGB components of the image are then substituted by S_1, S_1 and S_3 respectively, to obtain three substituted components. Eventually, combine the scrambled component of the image, which is the required ciphered image. The decryption process of our novel scheme is identical to the encryption process but with the converse operational order. Further, the detail of the proposed scheme is shown in the Fig. 1

Encryption	*Decryption*
Start	*Start*
Input Image ← [image name. format]	*Input Image ← [image name. format]*
Input key←Input: $[p_1, p_2, a_1, a_2, a_3, a_4, q_1, q_2, x_0, y_0\ p(x)]$	*Input key←Input:* $[p_1, p_2, a_1, a_2, a_3, a_4, q_1, q_2, x_0, y_0\ p(x)]$
I← imread(Input image);	*C← imread(Input image);*
[A]← size(I);	*[A]← size(C);*
for j←1 to A(1)	$Modpoly \leftarrow$ *Dec2bin (p(x));*
for k ←1 to A(2)	*Declare set 'a' ←[0 to 512];*
if $I_{i*p_1+q_1, j*p_2+q_2} \leftarrow 0$	*for* $j \leftarrow 0$ *to 511*
$T_{j,k} \leftarrow I_{A(1),A(2)}$	$x_j \leftarrow$ *bitxor(poly mult*$(a_1, j,$ *Mod poly),* $a_2)$
else	$y_j \leftarrow$ *bitxor(poly mult*$(a_3, j,$ *Mod poly),* $a_4)$
$T_{j,k} \leftarrow I_{i*p_1+q_1,\ j*p_2+q_2}$	$S \leftarrow$ *polymult*$(x_j$*,find inverse*$(y_j, Mod\ poly)$*, Mod poly)*
end	*if*
end	$S_i >\leftarrow 256$
*for i← 1:A(1)*A(2)*	$S^1{}_i \leftarrow S_i$
$x_{i+1} \leftarrow 1 + y_i + abs(x_i)$	*else*
$y_{i+1} \leftarrow x_i$	$S^2{}_i \leftarrow 256 - S_i$
end	*end*
$X \leftarrow$ $bitxor(bitxor(floor(x_{i+1}), 256), (floor(x_{i+1}), 256), \quad T)$	$S^3 \leftarrow$ *substitute* (S^1, S^2)*;*
$Modpoly \leftarrow$ *Dec2bin (p(x));*	$Inv\ S^i{}_{S^1{}_i} \leftarrow i$
Declare set 'a' ←[0 to 512];	$X \leftarrow$ *substitute (C, inv* S^i*);*
for $j \leftarrow 0$ *to 511*	*for i← 1:A(1)*A(2)*
$x_j \leftarrow$ *bitxor(poly mult*$(a_1, j,$ *Mod poly),* $a_2)$	$x_{i+1} \leftarrow 1 + y_i + abs(x_i)$
$y_j \leftarrow$ *bitxor(poly mult*$(a_3, j,$ *Mod poly),* $a_4)$	$y_{i+1} \leftarrow x_i$
$S \leftarrow$ *polymult*$(x_j$*,find inverse*$(y_j, Mod\ poly)$*, Mod poly)*	*end*
if	$T \leftarrow$ $bitxor(bitxor(floor(x_{i+1}), 256), (floor(x_{i+1}), 256), \quad X)$
$S_i >\leftarrow 256$	*for j←1 to A(1)*
$S^1{}_i \leftarrow S_i$	*for k ←1 to A(2)*
else	*if* $I_{i*p_1{}^{-1}-q_1, j*p_2{}^{-1}-q_2} \leftarrow 0$
$S^2{}_i \leftarrow 256 - S_i$	$I_{j,k} \leftarrow T_{A(1),A(2)}$
End	***else***
$S^3 \leftarrow$ *substitute* (S^1, S^2)*;*	$I_{j,k} \leftarrow T_{i*p_1{}^{-1}-q_1,\ j*p_2{}^{-1}-q_2}$
$C \leftarrow$ *substitute (X,* S^i*);*	*end*
Cipher image $\leftarrow uint8(C)$	*end*
	plain image $\leftarrow uint8(I)$
End	*End*

.

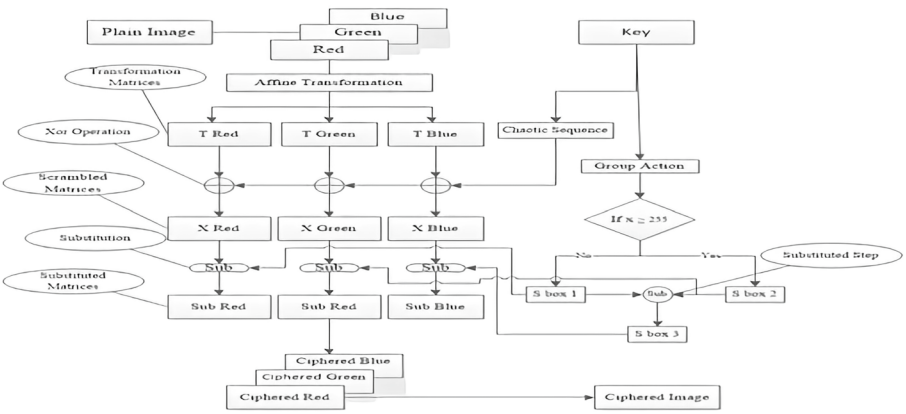

Fig. 1 The flowchart of the encryption process of the proposed scheme

4 Security and performance analyses

A well-organized encryption algorithm should have capablility to convert various dissimilar images into unrecognized cipher-images. The decryption of the images will possible only one has the knowledge of the complete correct key. In the case of a wrong key, one is unable to decrypt the complete image or obtained any useful information from the cipher image. The encryption process of a grayscale color and binary image are shown in Fig. 2. The key selected for the experiment is as follows, the elements a, b, c, and d of the Galois field $GF\left(2^9\right)$ are 422, 167, 122 and 501 respectively and the primitive irreducible polynomial $r_i(x) = x^9 + x^4 + x^3 + x + 1$ are chosen for the S-boxes generation step. The prime elements of the ring $p_1^{R,G,B}, p_2^{R,G,B}, q_1^{R,G,B}, q_2^{R,G,B}$ are selected 113, 149, 100 and 234 respectively. The initial conditions and chaos perimeters are 0.30.5. It can be seen in the Fig. 2a that all the original images have several arrangements that make them hard to be treated. However, the corresponding encrypted images are completely random and their pixel values are uniformly distributed, which are shown in Fig. 2c. Accordingly, the attackers are unable to get any valuable data about the plain images from their uniform pixel distributions.

4.1 Performance analysis of the generated S-box

The cryptographic strength of the generated S-boxes used in the encryption process is inspected through the most commonly used analyses such as nonlinearity, SAC, BIC, DP and LP. The performance index of the generated S-boxes are given below.

4.1.1 Nonlinearity

The Nonlinearity of a Boolean function h can be defined as the least Hamming distance among and the set of all affine Boolean functions and the function h, we denoted the nonlinearity of h by N_h and mathematically it can be written as;

$$N_h = \min\{d(h, a) : a \in A\} \tag{13}$$

where $d(h, a)$ denote the hamming distance between h and a and A signify the set of affine Boolean functions. Accordingly, all affine functions are linear have nonlinearity 0. The maximum probable N_h value of $n \times n$ S-box is equal to $2^{n-1} - 2^{\frac{n}{2}-1}$. Thus, the case for $n = 8$ the promising value is 120. The nonlinearity result of the proposed S-box is shown in Table 2.

4.1.2 Strict avalanche criterion

In 1985, Webster and Tavares described the analysis of strict avalanche criterion (SAC) and the concept of completeness and avalanche are developed. This criterion studied to inspect the performance of the output bits once changes applied to the input bits. The SAC result of the proposed S-boxes is shown in Table 3. In the table, it can be seen that the least value of the analysis is 0.437500, the maximum value of the analysis is 0.562500 and the average value is 0.502686. Thus the proposed S-boxes satisfied the need of the sac test.

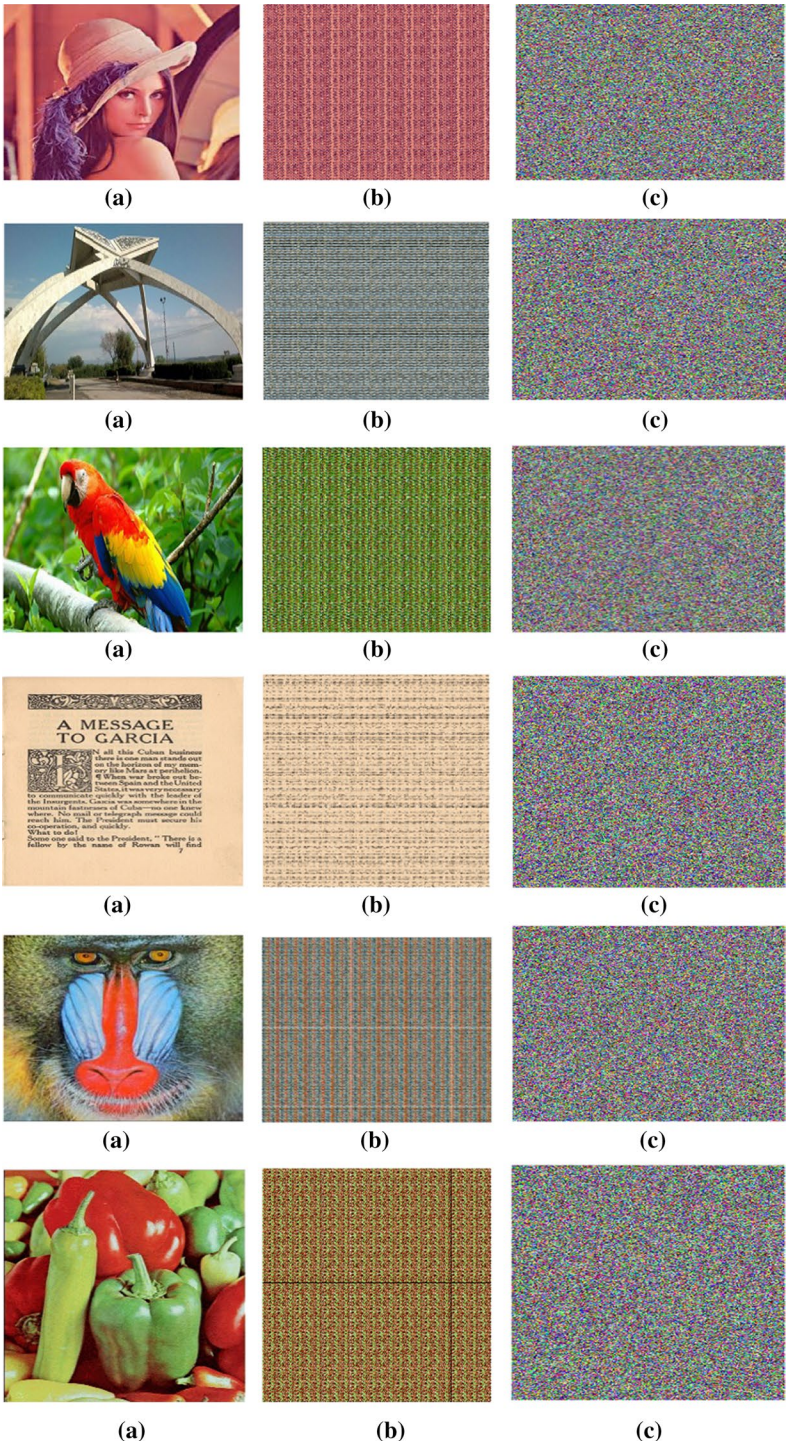

Fig. 2 **a** The original images: Lena image, QAU image, Perrot image, a Message image, Mandrill image, Peppers image. **b** The Affine Permuted images, **c** the encrypted image

Table 2 Nonlinearity of S-boxes

Functions	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Average
S_1	102	104	108	104	104	106	106	104	104
S_2	104	106	104	104	106	106	104	106	105
S_3	100	100	104	104	102	106	98	104	102

Table 3 Strict avalanche criterion

S-boxes	Maximum value	Minimum value	Average value	SD
S_1	0.625000	0.421875	0.498535	0.040794
S_2	0.625000	0.421875	0.510254	0.043861
S_3	0.625000	0.406250	0.500977	0.046072

4.1.3 Bit independent criterion

Webster and Tavares also present the important property of Boolean function called bit independent criterion. (BIC) in 1985. The BIC is used to compare the individual's bits that are produced via the eight-constitution function. This criterion used to measure the correlation effect of nth and mth output bits whenever slight change carried out in the input ith bits. Initially in this analysis change the ith bit from 1 to n and fixed ith and kth bits, and similarly, in the next step change the value of nth and mth in the range of 1 to n. The BIC result of the proposed S-boxes is shown in Table 4.

4.1.4 Linear approximation probability

Linear approximation probability (LP) analysis is used to investigate the maximum value of imbalance of the scheme. Let L_i and L_o denote the input and the output mask respectively. According to the Mastui original definition of LP, The order of equal output bits selected by the mask L_o is equivalent to the equality of the input bits select by the mask L_i. Mathematically it can be written as follows:

$$LP = \max_{L_i, L_o \neq 0} \left| \frac{\left\{ \#i \in Z | i \cdot L_i = S(i) \cdot L_o \right\}}{2^n} - \frac{1}{2} \right| \tag{14}$$

where the set input bits of order 2^n is denoted by Y. In Table 5 the performance result of LP analysis show that the proposed S-boxes are successfully secure against linear cryptanalysis.

4.1.5 Differential approximation probability

Differential approximation probability (DP) analysis is used to measure the differential uniformity of the S-box. Mathematically DP can be defined as follows:

$$DP^s(\Delta i \rightarrow \Delta o) = \left[\frac{\#\{ i \in K | S(i) \pm S(i \pm \Delta i = \Delta o) \}}{2^m} \right] \tag{15}$$

Table 4 BIC and SAC-BIC

S-boxes	BIC			SAC-BIC		
	Max value	Min value	SD	Min value	Ave value	SD
S_1	98	103	2.449	0.46289	0.50181	0.01582
S_2	96	102.857	2.278	0.47266	0.50049	0.01628
S_3	98	103.500	2.344	0.48633	0.50565	0.01106

Table 5 Linear approximation probability

S-boxes 1		S-box 2		S-box 3	
LP	Max count	LP	Max count	LP	Max count
0.1328125	162.0	0.140625	164.0	0.125	160.0

In the above equation, the input differential Δi_j would map exclusively to the output differential, to confirm the uniform mapping probability for each j. The result of the DP analysis of the generated S-boxes over the proposed construction method is closed to the optimum value as shown in Table 6.

4.2 Performance analysis and simulation result

4.2.1 Keyspace analysis

A brute-force attack is also called exhaustive key search that is the attacker is able to check all the possible keys of the key space till they recover the ciphertext. The viability of the brute-force attack depends on the order of the set of all valid keys. The parameters used as a key in the proposed cryptosystem are given below:

(a) The element of a Galois field a, b, c, d and degree 8 primitive irreducible polynomial in principle ideal domain $\mathbb{Z}_2[x]$.
(b) The unite elements p_1^R, p_1^G, p_1^B,p_2^R, p_2^G, p_2^B any others elements q_1^R, q_1^G, $q_1^B q_2^R$, q_2^G, q_2^B of a ring $\mathbb{Z}_N$.
(c) The initial conditions x_0 and y_0 of Gingerbreadman map

Since the elements a, b, c and $d \in GF\left(2^9\right)$. By Theorem 2.9, in Gan et al. (2018a) the total number of possible different pair a, b, c and d which can be used as a secret key is 6.8595×10^{10}, for a fixed primitive irreducible polynomial and the integers a, b and c are the elements of the ring $\mathbb{Z}_{512}\backslash\{0, 1\}$and the total number of a, b and c which can also be used a part of a secret key 16194277. So for a fixed $p_1^{R,G,B}$, $q_1^{R,G,B}$ and the initial condition x_0 and y_0 the key space is 6.8595×10^{10}. Therefore, the proposed scheme is able to resist all kind of brute force attack.

4.2.2 Histogram analysis

The histogram plot of the image represents the distribution of pixel values through graphing the total number of pixels intensity. A well-organized algorithm should produce cipher image with uniform pixels distribution and must be expressively dissimilar from that of the plaintext image. Figure 3 presents the histogram plots of the original images and their corresponding encrypted images. Here, with the first to the fifth column are plaintext images, histograms of plaintext images, ciphertext images, histograms of ciphertext images, deciphered images, respectively. The histograms plots of the original images are uniform and fairly distinct from the histogram of their corresponding cipher image.

4.2.3 Correlation analysis

The pixels of the plain image are usually correlated with their adjacent pixels either in the vertical, diagonal or horizontal direction. The high correlation of the pixels is also helpful to break the cryptosystems. Therefore, a secure cryptosystem must terminate the correlation of the neighbor pixels. In order to calculate the correlation among the adjacent pixels, 4000 pairs of the adjacent pixels in horizontal, vertical and diagonal directions are randomly selected from the original image and their corresponding encrypted image. Then used the following equation and calculate the correlation coefficients.

$$C_{\alpha\beta} = \frac{\mathrm{E}(\alpha - \mathrm{E}(\alpha))\mathrm{E}(\beta - \mathrm{E}(\beta))}{\sqrt{\mathrm{B}(\alpha)}\sqrt{\mathrm{B}(\beta)}} \tag{16}$$

$$\mathrm{E}(\alpha) = \frac{1}{\mathrm{M}} \sum_{j=1}^{\mathrm{M}} \alpha_j \tag{17}$$

$$\mathrm{B}(\alpha) = \frac{1}{\mathrm{M}} \sum_{j=1}^{\mathrm{M}} (\alpha_j - \mathrm{E}(\alpha))^2 \tag{18}$$

In the above equation M denote the number of sample and α_j and β_j are the gray values of the jth pair of the chosen two neighbor pixels. The correlation distribution of the Lena plain image in horizontal, diagonal and vertical are shown in Fig. 4a–c and d–f display the correlation distribution of horizontally, diagonally and vertically adjacent pixels of the ciphered Lena image, respectively. The result of the correlation analysis is listed in Table 7. From table we observed that the value correlation coefficients of the encrypted images closely equal to 0 while the correlation coefficient of their original image close to 1. Figure 4 and Table 7 reveal that the correlation of the adjacent pixels

Table 6 Differential approximation probability

S-boxes 1		S-box 2		S-box 3	
DP	Max value	DP	Max value	DP	Max value
0.046875	12	0.039062	10	12	0.046875

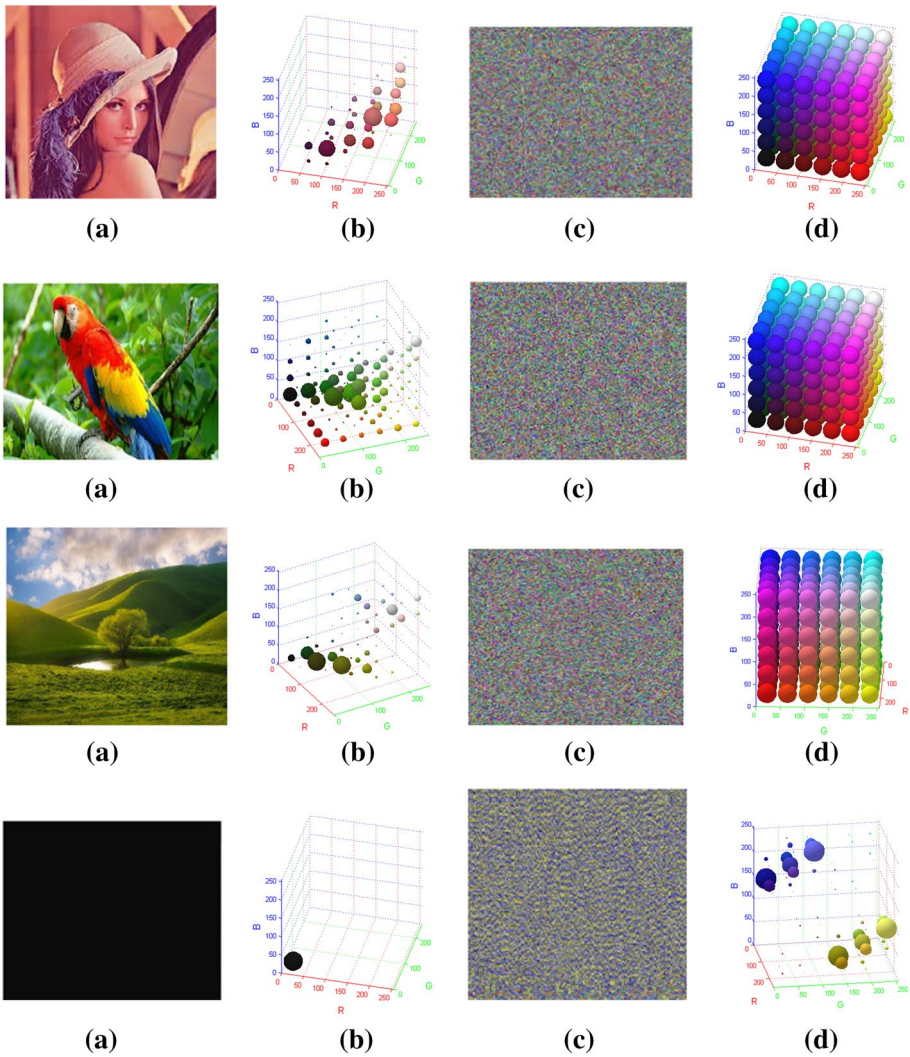

Fig. 3 **a** The original images: Lena image, QAU image, Perrot image, nature image, binary black image. **b** The histogram of original images, **c** the encrypted image, **d** the histogram of encrypted images

in the encrypted images are demolished so that the neighboring pixels in the encrypted images have no correlation.

4.2.4 Information entropy analysis

For digital data, the quantity of randomness is measured with the help of information entropy analysis. Mathematically entropy is defined as:

$$\mathrm{H}(S) = -\sum_{j=1}^{2^K-1} \mathrm{P}\left(S_j\right) log_2 \mathrm{P}\left(S_j\right) \tag{19}$$

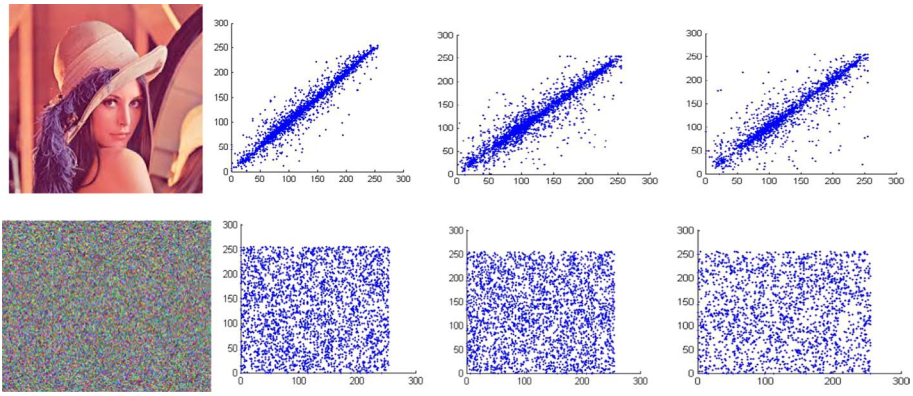

Fig. 4 Correlation plots of two adjacent pixels, from the first to fourth column illustrates: the image, horizontal, vertical, and diagonal adjacent pixels, respectively

Table 7 Correlation coefficient analysis

Images	Original image			Ciphered image		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Lean	0.9851	0.9673	0.9478	−0.0116	−0.0083	0.0056
QAU	0.9707	0.9478	0.9390	−0.0105	−0.0055	−0.0055
Parrot	0.9440	0.9462	0.9239	−0.0220	0.0370	−0.0263
Message	0.6882	0.6292	0.5048	−0.0087	−0.0177	−0.0066
Mandrill	0.9476	0.9517	0.9036	−0.0039	0.0074	−0.0084
Peppers	0.9672	0.9597	0.9348	−0.0046	−0.0030	−0.0031

where K denotes the total number of bits to signify the notation S_j and $\mathrm{P}(S_j)$ represent its probability. The genuine random source consists of 2^K symbols. Therefore, the optimum value of the entropy analysis with 256 gray-level would be 8. The information entropy of different plain images and their corresponding encrypted images are calculated. The result is listed in Table 8. In the last row of the table, the average result of the information entropy analysis of different images is given. We observed from the table that the average result of information entropy analysis of all encrypted images is approximately equal to the theoretical maximum 8, implies that the encrypted images are near to a random source, thus the information leakage in the encryption procedure is insignificant. Thus, the proposed algorithm is more secure against the entropy attack as compared to the other scheme as shown in Table 9.

4.2.5 Differential attacks

The differential cryptanalysis is a type of chosen-plaintext attacks. This attack attempt to ascertain the relationship between the ciphertext and the plaintext, through tracing, how the small change in the plaintexts can influence the ciphertexts. Subsequently, the building

Table 8 Information entropy analysis of different images

Images	Original image			Ciphered image		
	Red	Green	Blue	Red	Green	Blue
Lena	7.29970	7.5825	7.07090	7.99721	7.9973	7.99698
QAU	7.6758	7.6379	7.4152	7.9974	7.9964	7.9968
Parrot	7.8343	7.8070	7.1404	7.9974	7.9970	7.9971
Message	5.9665	5.9665	5.9665	7.9967	7.9967	7.9967
Mandrill	7.6539	7.3782	7.656	7.9974	7.9970	7.9969
Peppers	7.3808	7.6445	7.1886	7.9973	7.9969	7.9969

Table 9 Comparing entropy for Lena (256×256) image

Images	Red	Green	Blue	Average
Proposed	7.99721	7.9973	7.99698	7.9971
Chai et al. (2018)	7.9973	7.9969	7.9971	7.9971
Wu et al. (2015)	7.9893	7.9896	7.9903	7.9897
Wu et al. (2017)	7.9973	7.9972	7.9969	7.99713
Liu and Kadir (2015)	7.9896	7.9893	7.9896	7.98964
Dong (2014)	7.9901	7.9912	7.9921	7.91133
ur Rehman et al. (2018)	7.9892	7.98987	7.9899	7.98963

relationship is used to retrieve the ciphertext without a secret key. The security strength of the encryption algorithm against differential attacks can be examined utilizing the number of pixels changing rate (NPCR) and the unified averaged changed intensity (UACI). The NPCR and UACI for the two ciphered images C_1 and C_2 corresponding to the two plain-images of one-bit difference are defined as:

$$NPCR_{R,G,B} = \frac{1}{L \times K} \sum_{J=1}^{L} \sum_{J=1}^{K} H_{R,G,B}(x, y) \times 100\% \tag{20}$$

$$UACI_{R,G,B} = \frac{1}{L \times K} \sum_{J=1}^{L} \sum_{J=1}^{K} \frac{|C_1(x, y) - C_2(x, y)|}{255} \times 100\% \tag{21}$$

where $L \times K$ represent the size of the image and $H_{R,G,B}(x, y)$ is calculated by the rule as follows:

$$H_{R,G,B}(x, y) = \begin{cases} 1 & if\ C_1(x, y) = C_2(x, y) \\ 0 & if\ C_1(x, y) \neq C_2(x, y) \end{cases} \tag{22}$$

To calculate the plaintext sensitivity of our new encryption method, we perform the following process: Initially, we encrypt the original plain image. Then select and change an arbitrarily bit of the original image. Subsequently, we encrypt the modified image via the same secret keys and compute the $NPCR_{R,G,B}$ and $UACI_{R,G,B}$. We execute the same test with different color images. Accordingly, *NPCR* and *UACI* outcomes of the proposed scheme are given below in Table 10. As can be seen that the average value of *NPCR* and *UACI*

are 99.6119% and 33.4789%, respectively. The result determines that the proposed cryptosystem has an ability for resisting different malicious differential attacks. Moreover, the comparison of the result listed in Table 11 demonstrates that the proposed scheme is more efficient as compared to the existing scheme.

4.3 Robustness

It is often observed that errors may occur during the transmission of information through the internet. It has been observed that even a single error in a pixel may lead to losing the host image (Awad and Awad 2010; Ur Rehman et al. 2015). Moreover, the decryption process can majorly be disfigured due to slight modification in the ciphered image. For this reason, the standard cryptosystem must be architecture to counter the domino effect in the decryption process. The expected randomness by Gaussian noise makes it the most desired robustness test.

4.3.1 Noise addition

While communication, the noise addition may result in alteration, deprivation and corrupted form of data. In order to counter such situations, the robustness of our scheme is evaluated with the help of Gaussian Noise and Salt and Pepper Noise added in peppers encrypted image shown in Fig. 2c. The parameters mean is given, value as $\mu = 0$ and variance has $\sigma = 0.0005$, 0.005, 0.05 and 0.3. These noise added images are then decrypted, the decryption results of PSNR, UACI, and NPCR of noisy decrypted images are given in Table 12. The resultant noisy encrypted images are shown in Figs. 5a–d and 6a–d while corresponding decrypted images shown in Figs. 5e–h and 6e–h.

4.3.2 Occlusion attack

n many cases, a portion of an image can vanish during transmission of data from one place to another. To handle such a situation, the proposed scheme must have the tendency to recover these lossy images. For the proposed technique, we have removed certain portions of Peppers image i.e. 64×64, 64×128 and 128×128 pixels of red, green and all channels. These removed portion images are shown in Fig. 7a. By seeing the deciphered images shown in Fig. 7e, it is clear that the proposed scheme helps to get back the original data and image can easily be visualized. Moreover, the different proportion of encrypted images have been removed as given in Fig. 7a–d and after going through the occlusion attack the

Table 10 Differential analyses for proposed

Images	NPCR			UACI		
	Red	Green	Blue	Red	Green	Blue
Lean	99.612	99.5345	99.5578	32.117	33.459	34.644
QAU	99.6345	99.6117	99.6543	34.251	31.269	34.251
Parrot	99.5012	99.521	99.4978	33.4583	32.373	33.832
Message	99.7085	99.745	99.839	33.4933	33.761	34.187
Peppers	99.6513	99.641	99.6432	32.106	29.895	35.700

Table 11 Comparing differential analyses for proposed and different existing encryption schemes for 256×256 Lena image

Schemes	NPCR			UACI		
	Red	Green	Blue	Red	Blue	Green
Proposed	99.612	99.5345	99.5578	32.117	33.459	34.644
Chai et al. (2018)	99.60	99.61	99.61	33.56	33.45	33.49
Wu et al. (2015)	99.61	99.60	99.60	33.46	33.50	33.47
Wu et al. (2017)	99.60	99.60	99.60	33.36	33.43	33.37
Liu and Kadir (2015)	99.63	99.60	99.60	33.60	33.30	33.40
Dong (2014)	99.60	99.59	99.59	33.44	33.46	33.47
ur Rehman et al. (2018)	99.66	99.54	99.67	33.12	34.00	33.90

original images are given in Fig. 7e–h. Table 13 depicts the outcomes of PSNR, UCI and NPCR results of the lossy decrypted image.

4.4 Complexity analysis and speed performance

The running speed is also an important feature for a well-organized encryption algorithm. The scheme is coded on Windows 10, 64-bit operating system and compiled under MATLAB 8.2.0.701 (R2013b). The experiments are carried out on Intel (R) Core (TM) i7-4770 CPU @ 3.40 GHz with 8 GB RAM personal computer. The number of steps and operation desirable to complete the process of encryption. Some of the steps are ignored such as programming language, framework, programming capacity, the calculation running tools, moreover, the spee performance of the proposed encryption are totaled in Table 14. The time-consuming part of the confusion portion is the number of the affine transformation based on integer addition and multiplication module n, thus the time complexity is $\Theta(3 \times N \times M)$. The diffusion portion of the scheme is consisting of two steps. So, the time-consuming part of the first step is the total number of the points operation for the generation of 2D chaotic sequence accordingly the complexity is $\Theta(N \times M)$. The second time consuming part of the diffusion portion is the generation of multiple S-boxes and the substitution the image data, thus the time complexity of the substitution step is $\Theta(6 \times N \times M)$. Since the cost of the computational time complexity depends on all operations of the scheme, so the time complexity of the proposed encryption scheme is $\Theta(6 \times N \times M)$.

Comparing the computational complexity of our scheme with the existing image encryption algorithms such as Chai et al. (2016), Gan et al. (2018b), the proposed encryption

Table 12 PSNR, NPCR and UACI of different decrypted image

Variane	Salt and pepper noise			Gussian noise		
	PSNR	NPCR	UACI	PSNR	NPCR	UACI
0.0005	40.910	52.99	11.022	14.1150	98.052	12.472
0.005	31.333	61.23	15.40	14.121	98.052	12.472
0.05	21.115	65.67	19.205	13.708	98.261	13.304
0.3	13.3522	78.85	20.08	9.5691	99.587	26.528

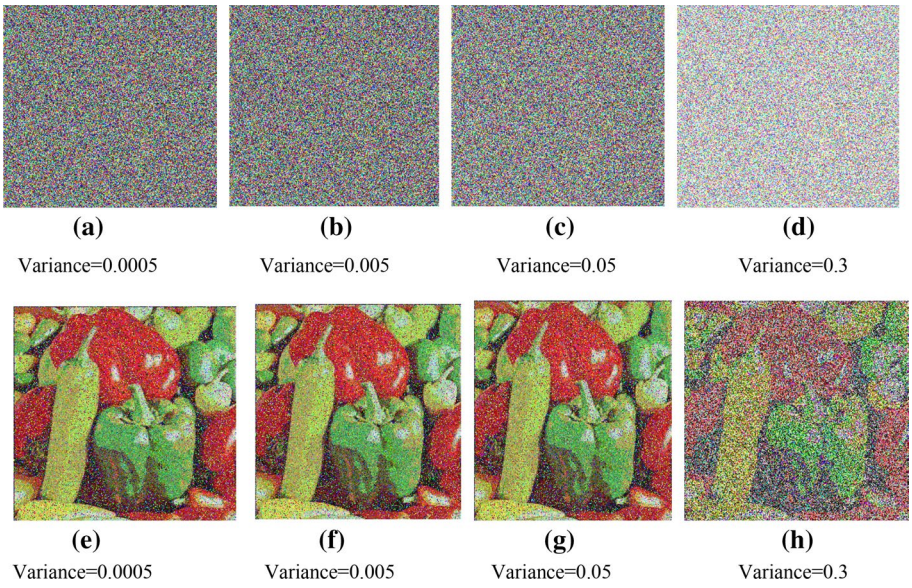

Fig. 5 Test of Gusian noise, **a** encrypted with density 0.0005; **b** polluted with density 0.005; **c** polluted with density 0.05; **d** polluted with density 0.3; **e** decrypted pepper image from **a**; **f** decrypted pepper image from **b**; **g** decrypted pepper image from **c**; **h** decrypted pepper image from **d**

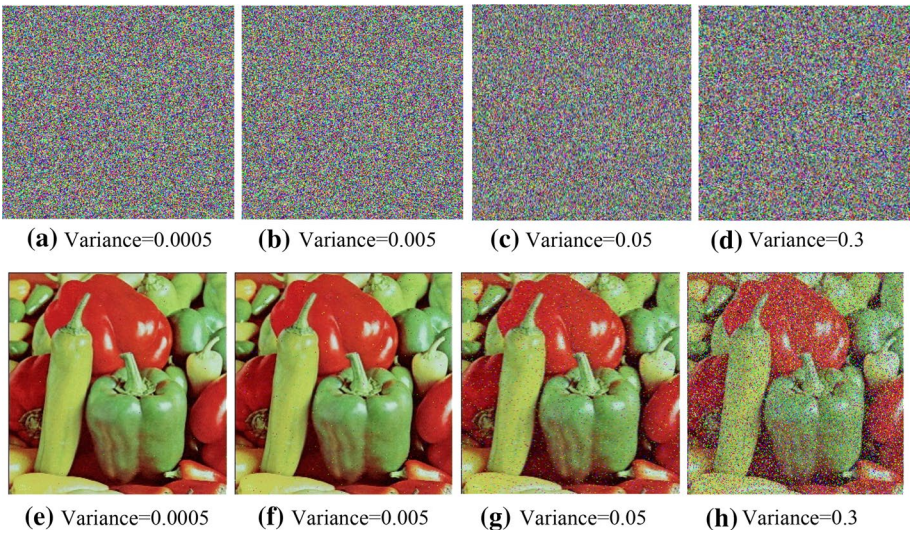

Fig. 6 Test of Salt and Peppers, **a** encrypted with density 0.0005; **b** polluted with density 0.005; **c** polluted with density 0.05; **d** polluted with density 0.3; **e** decrypted pepper image from **a**; **f** decrypted pepper image from **b**; **g** decrypted pepper image from **c**; **h** decrypted pepper image from **d**

scheme has smaller time complexity. Because Step 1 of the proposed scheme which is described in Sect. 3.1 there are simple affine transformations are used to disturb the pixels of the image. In step 2 three S-boxes are generated, and a simple substitution process is

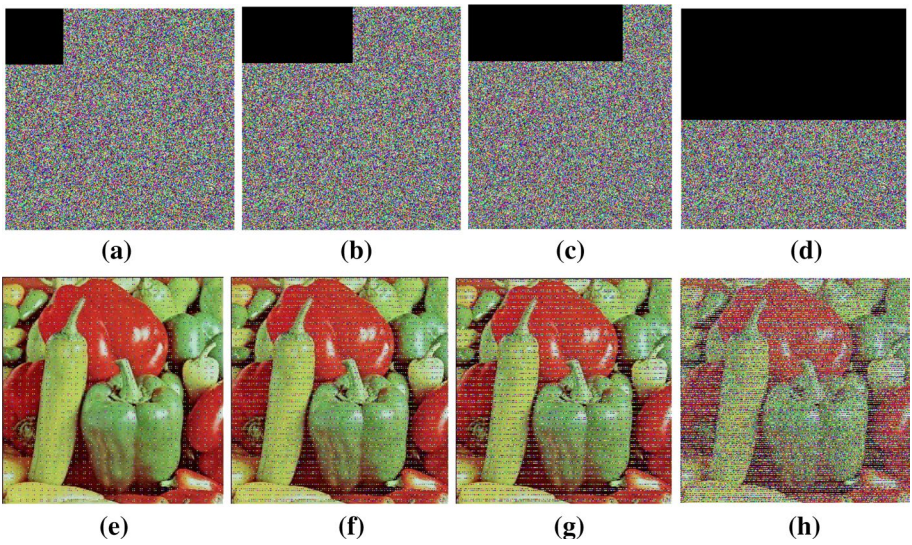

Fig. 7 Occlusion attack analysis by removing a part **a** 1/16 of encrypted Pepper; **b** 1/8 of encrypted Pepper; **c** 3/16 of encrypted Pepper; **d** 1/2 of encrypted Pepper; **e** decrypted image of **a**; **e** decrypted image of **a**; **f** decrypted image of **b**; **g** decrypted image of **c**; **h** decrypted image of **h**

Table 13 PSNR, NPCR and UACI of different decrypted image

Clipping size	PSNR	NPCR	UACI
1/16	20.176	10.636	10.202
2/8	17.161	21.273	19.404
3/16	15.3945	31.910	21.607
1/2	11.1112	50.38	20.955

Table 14 Speed performance analysis

Image size	Encryption time (s)
$512 \times 512 \times 3$	0.078
$1024 \times 1024 \times 3$	3.854

used. Ultimately, two-dimensional chaotic sequences are iterated and the xor operation is used.

5 Conclusion

In this paper for the construction of multiple S-boxes a novel algorithm is introduced. This S-box construction algorithm is obtained by employing action of projective general linear group over the Galois field $GF(2^9)$. Performance results of these S-boxes are examined

by different analyses, the results show that the S-boxes are nonlinear, successfully satisfied SAC, and capable to resist linear and differential attacks. Since the algorithm generates multiple S-boxes, thus we designed an algorithm for image encryption employing the construction method in the substitution part of the algorithm. The permutation step is performed by the Affine transformation over the ring of integers modulo n. Simulation results show that this algorithm can efficiently encrypt different kind of an image into random-like ones. Security analysis shows that this algorithm can resist the common attacks, such as statistical, brute-force, differential, known plaintext attack and chosen plaintext attack. Efficient analysis indicates that it has low computation and time complexity. Thus it has excellent application prospect.

Acknowledgements The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under Grant Number R.G.P. 2/58/40.

References

Alvarez, G., & Li, S. J. (2006). Some basic cryptographic requirements for a chaos-based cryptosystem. *International Journal of Bifurcation and Chaos, 16*(8), 2129–2151.

Amin, M., Faragallah, O. S., & Abd El-Latif, A. A. (2010). A chaotic block cipher algorithm for image cryptosystems. *Communications in Nonlinear Science and Numerical Simulation, 15*(11), 3484–3497.

Awad, A., & Awad, D. (2010). Efficient image chaotic encryption algorithm with no propagation error. *ETRI Journal, 32*(5), 774–783.

Behnia, S., Akhshani, A., Mahmodi, H., & Akhavan, A. (2008). A novel algorithm for image encryption based on a mixture of chaotic maps. *Chaos, Solitons & Fractals, 35*(2), 408–419.

Belazi, A., El-Latif, A. A. A., & Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing, 128,* 155–170.

Chai, X., Fu, X., Gan, Z., Lu, Y., & Chen, Y. (2018). A color image cryptosystem based on dynamic DNA encryption and chaos. *Journal of Signal Processing, 155*(2019), 44–62.

Chai, X. L., Gan, Z. H., Lu, Y., Zhang, M. H., & Chen, Y. R. (2016). A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system. *Chinese Physics B, 25*(10), 100503.

Chiaraluce, F., Ciccarelli, L., Gambi, E., Pierleoni, P., & Reginelli, M. (2002). A new chaotic algorithm for video encryption. *IEEE Transactions on Consumer Electronics, 48*(4), 838–844.

Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES—the advanced encryption standard*. Berlin: Springer.

Dong, C. (2014). Color image encryption using one-time keys and coupled chaotic systems. *Signal Processing: Image Communication, 29,* 628–640.

Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos, 8*(6), 1259–1284.

Gan, Z., Chai, X., Yuan, K., & Lu, Y. (2018a). A novel image encryption algorithm based on LFT based S-boxes and chaos. *Multimedia Tools and Applications, 77*(7), 8759–8783.

Gan, Z., Chai, X., Zhang, M., & Lu, Y. (2018b). A double color image encryption scheme based on three-dimensional Brownian motion. *Multimedia Tools and Applications, 77*(21), 27919–27953.

Gao, T. G., & Chen, Z. Q. (2008). A new image encryption algorithm based on hyper-chaos. *Physics Letters A, 372*(4), 394–400.

Hussain, I., & Gondal, M. A. (2014). An extended image encryption using chaotic coupled map and S-box transformation. *Nonlinear Dynamics, 76*(2), 1355–1363.

Hussain, I., Shah, T., & Gondal, M. A. (2012). Image encryption algorithm based on PGL (2, GF (2^8)) S-boxes and TD-ERCS chaotic sequence. *Nonlinear Dynamics, 70*(1), 181–187.

Li, S., Chen, G., & Zheng, X. (2005). *Chaos-based encryption for digital images and videos. Multimedia security handbook, chapter 4* (pp. 133–167). Boca Raton: CRC Press.

Li, S. J., Li, C. Q., Chen, G. R., Bourbakis, N. G., & Lo, K. T. (2008). General quantitative cryptanalysis of permutation-only multimedia ciphers against plain-image attacks. *Signal Processing: Image Communication, 23*(3), 212–223.

Li, C., Zhang, L. Y., Ou, R., Wong, K.-W., & Shu, S. (2012). Breaking a novel color image encryption algorithm based on chaos. *Nonlinear Dynamics, 70*(4), 2383–2388.
Lian, S. G., Sun, J. S., & Wang, Z. Q. (2005). A block cipher based on a suitable use of the chaotic standard map. *Chaos, Solitons & Fractals, 26*(1), 117–129.
Liu, H. J., & Kadir, A. (2015). Asymmetric color image encryption scheme using 2D discrete-timemap. *Signal Processing, 113,* 104–112.
Liu, H., Kadir, A., & Gong, P. (2015). A fast color image encryption scheme using one-time S-boxes based on complex chaotic system and random noise. *Optics Communications, 338,* 340–347.
Liu, Y., Zhang, L. Y., Wang, J., Zhang, Y., & Wong, K.-W. (2016). Chosen-plaintext attack of an image encryption scheme based on modified permutation-diffusion structure. *Nonlinear Dynamics, 84*(4), 2241–2250.
Naseer, Y., Shah, D., & Shah, T. (2019a). A novel approach to improve multimedia security utilizing 3D mixed chaotic map. *Microprocessors and Microsystems*. https://doi.org/10.1016/j.micpro.2018.12.003.
Naseer, Y., Shah, T., Shah, D., & Hussain, S. (2019b). A novel algorithm of constructing highly nonlinear sp-boxes. *Cryptography, 3*(1), 6.
Norouzi, B., Mirzakuchaki, S., Seyedzadeh, S.-M., & Mosavi, M.-R. (2014). A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion. *Multimedia Tools and Applications, 71*(3), 1469–1497.
Patidar, V., Pareek, N. K., & Sud, K. K. (2009). A new substitution–diffusion-based image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation, 14*(7), 3056–3075.
Pisarchik, A. N., Flores-Carmona, N. J., & Carpio-Valadez, M. (2006). Encryption and decryption of images with chaotic map lattices. *Chaos, 16*(3), 033118.
Saberi, K. M., Mohammad, D., Rahim, M., & Yaghobi, M. (2014). Using 3-cell chaotic map for image encryption based on biological operations. *Nonlinear Dynamics, 75*(3), 407–416.
Shah, T., & Shah, D. (2019). Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over $\mathbb{Z}$ 2. *Multimedia Tools and Applications, 78*(2), 1219–1234.
Shah, D., ul Haq, T., & Shah, T. (2018). Image encryption based on action of projective general linear group on a galois field GF (2^8). In *2018 international conference on applied and engineering mathematics (ICAEM)*. https://doi.org/10.1109/ICAEM.8536281.
Tuchman, W., IV. (1979). Hellman presents no shortcut solutions to the DES'. *IEEE Spectrum, 16*(7), 40–41.
ur Rehman, A., Liao, X. F., Ashraf, R., Ullah, S., & Wang, H. W. (2018). A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik, 159,* 348–367.
Ur Rehman, A., Liao, X., Kulsoom, A., & Abbas, S. A. (2015). Selective encryption for gray images based on chaos and DNA complementary rules. *Multimedia Tools and Applications, 74*(13), 4655–4677.
Wang, X., Teng, L., & Qin, X. (2012). A novel colour image encryption algorithm based on chaos. *Signal Processing, 92*(4), 1101–1108.
Wang, X., & Wang, Q. (2014). A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. *Nonlinear Dynamics, 75*(3), 567–576.
Wang, Y., Wong, K. W., Liao, X. F., & Xiang, T. (2009a). A block cipher with dynamic S-boxes based on tent map. *Communications in Nonlinear Science and Numerical Simulation, 14*(7), 3089–3099.
Wang, Y., Wong, K. W., Liao, X. F., Xiang, T., & Chen, G. R. (2009b). A chaos-based image encryption algorithm with variable control parameters. *Chaos, Solitons & Fractals, 41*(4), 1773–1783.
Wang, X. Y., Yang, L., Liu, R., & Kadir, A. (2015). A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynamics, 62*(3), 615–621.
Wong, K. W., Kwok, B. S. H., & Law, W. S. (2008). A fast image encryption scheme based on the chaotic standard map. *Physics Letters A, 372*(15), 2645–2652.
Wu, X. J., Kan, H. B., & Kurths, J. (2015). A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Applied Soft Computing, 37,* 24–39.
Wu, J. H., Liao, X. F., & Yang, B. (2017). Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. *Signal Processing, 141,* 109–124.
Zhang, Y., Li, C., Li, Q., Zhang, D., & Shu, S. (2012). Breaking a chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynamics, 69*(3), 1091–1096.
Zhang, Y., Li, Y., Wen, W., Wu, Y., & Che, J.-X. (2015). Deciphering an image cipher based on 3-cell chaotic map and biological operations. *Nonlinear Dynamics, 82*(4), 1831–1837.
Zhang, X., Mao, Y., & Zhao, Z. (2014a). An efficient chaotic image encryption based on alternate circular S-boxes. *Nonlinear Dynamics, 78*(1), 359–369.

Zhang, Y., Xiao, D., Wen, W., & Li, M. (2014b). Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Nonlinear Dynamics, 76*(3), 1645–1650.
Zhu, Z. L., Zhang, W., Wong, K. W., & Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences, 181*(6), 1171–1186.