An Efficient Information Hiding Mechanism Based on Confusion Component over Local Ring and Moore-Penrose Pseudo Inverse

NABILAH ABUGHAZALAH [a,1], MAJID KHAN [b,c]

[a] Mathematical Sciences Department, College of Science, Princess Nourah bint Abdulrahman University, Riyadh, SAUDI ARABIA
[b] Cyber and Information Security Lab, Institute of Space Technology, Islamabad, PAKISTAN
[c] Department of Applied Mathematics & Statistics, Institute of Space Technology, Islamabad, PAKISTAN

*Abstract***:** The basic requirement by adding confusion is to ensure the confidentiality of the secret information. In the present article, we have suggested new methodology for the construction of nonlinear confusion component. This confusion component is used for enciphering the secret information and hiding it in a cover medium by proposed scheme. The proposed scheme is based on ring structure instead of Galois field mechanism. To provide multi-layer security, secret information is first encrypted by using confusion component and then utilized three different substitution boxes (S-boxes) to hide into the cover medium.

Keywords**:** Confusion, Diffusion, Encryption, Hiding.

Received: January 14, 2021. Revised: February 24, 2021. Accepted: February 26, 2021.
Published: March 2, 2021.

1. Introduction

With the increasing demands of online internet services security of digital information become one of the utmost needs across the globe. Undoubtedly, security of digital information plays an important role in advanced era of communication. The sphere of information security become enormous with vary next day.

The fast and secure transmission of information is one of the mandatory components of national and multinational organizations. In twenty first century which is fundamentally a century of hybridization. A huge number of digital contents are now accessed through different web links. From last some decades, the privacy and confidentiality of information can only be limited to military organization specifically. But now it is not limited to military but other national organizations. The privacy of digital contents can be addressed through different information security techniques for instance cryptography and information hiding. The confidentiality can be achieved through encryption algorithm in which actual contents of information can be transformed meaningless format. The encryption algorithms can be classified according to encryption keys namely symmetric and asymmetric key algorithms. In symmetric encryption algorithm utilized only one key whereas asymmetric encryption algorithm uses two or more than two keys. The symmetric encryption algorithms can further be classified as block ciphers and stream ciphers. In block cipher, algorithms can work on fixed size of bitstream whereas in stream ciphers operate on individual bits of digital information. The modern block ciphers are based are based on substitution and permutation network (SP-network). Further SP-network is categorized into two kinds of methods specifically Feistel and Non- Feistel. The layers of confusion and diffusion are incorporated

with the help of substitution and permutation in modern ciphers which added nonlinear and linear structures algebraically. Substitution box (S-box) is an integral part of modern block cipher which is responsible of adding confusion in encryption algorithm. Modern block ciphers for instance international data encryption standard (IDEA), data encryption standard (DES) and advanced encryption standard (AES) were utilizing confusion components in their structures [1-7].

Generally, there are three types of nonlinear components namely bijective or straight, compressed and expansion. A nonlinear confusion component is said to be straight if the number of input and output are same. This type of nonlinear confusion component is utilized in advanced encryption standard (AES). Another class of nonlinear confusion component take larger number of inputs as compared to its output. It means number of inputs are greater than number of outputs. Date encryption algorithm (DES) is good example for such nonlinear confusion components. It may be possible to have nonlinear confusion component where number of inputs are smaller as compared to its yields. Different designing techniques were developed for the construction of these nonlinear components. These construction mechanisms were based on chaotic dynamical systems, Galois fields and rings, optimization schemes, neural networks, and DNA sequences [15-30]. All these mechanisms were designed to construct a straight (bijective) S-boxes to add up further confusion ability in modern-day block ciphers. There are some structural problems associated with compressible and expansible nonlinear components. The fundamental problem with either of S-boxes is reversibility. By utilizing either type of confusion component changes the total number of input and output bitstreams which make it quite difficulty to reverse the process. In general, working with either compression or expansion S-boxes will introduce significant complexities in nonlinear component design.

Information hiding is generally used to hide the secret data into some information carriers. The information carriers are generally those part of digital content which are invariant under certain transformation. These transformations may be insertion or substitution of any binary bit to some digital medium. The digital information hiding is further classified into two major branches namely, digital watermarking and steganography. Process of adding any digital mark (logo, visible/invisible) to some digital content which preserve the actual for copyright protection is watermarking, whereas in steganography, hide the secret message to deceive the intruder to pass information through insecure line of communication [31-32]. The aim of our article is twofold, firstly we have introduced a new mechanism for the construction of compression based nonlinear component and secondly, we have suggested a mechanism to hide our secret information in a digital media. Through this twofold scheme, we have achieved double layer security to our secret information.

The present article is consisting of seven sections. Section 2 describes the basic steps of AES S-box. Section 3 describes the proposed methodology of nonlinear component. In section 4, proposed information hiding scheme is added. The algebraic and statistical analyses for proposed confusion component and steganographic schemes presented in sections 5 and 6. Finally, the present article is ended with conclusion in section 7.

2. Construction of AES S-box

S-box utilized in AES is based on Galois field $GF(2^8)$ of 256 elements whose each component is written in 8-bits. The Galois field of 256 elements can be generated with eight-degree primitive irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. Three different transformations were utilized to generate the AES S-box namely, linear transformation, affine transformation and inverse transformation respectively. The mathematical expression for AES S-box is defined as follow:

$$S : \mathrm{F}_2^8 \to \mathrm{F}_2^8 , \qquad (1)$$

$$S - box_{AES} = H \circ L \circ I , \qquad (2)$$

$$S-box_{AES} = S(x) = H(L(I(x))) = H(L(x^{-1})) = H(Ax^{-1}) = Ax^{-1} \oplus b, \quad (3)$$

where H is affine transformation, L is linear transformation, and I is inverse transformation.

3. Construction of S-boxes Using Ring $\mathbf{Z}_{p^n}$

In this segment of the chapter, we will first define some basic mathematical structures used for the construction of confusion component of block cipher [1-7].

3.1 Proposed Scheme for Confusion Component

This section presents the mathematical terms and basic algebraic algorithm used to structure our confusion component namely S-box. To understand this, we need to go through some basic facts. A function $g: \mathrm{F}_{2^n} \to \mathrm{F}_2$ is called a Boolean function. A vector Boolean $G: \mathrm{F}_{2^n} \to \mathrm{F}_{2^m}$ is defined as $G(x) = (g_1(x), g_2(x), ..., g_m(x))$, where $x = (x_1, x_2, ..., x_n) \in \mathrm{F}_{2^n}$ and each of f_i is called a coordinate Boolean function. An $n \times m$ S-box is precisely a vector Boolean function $S: \mathrm{F}_{2^n} \to \mathrm{F}_{2^m}$. The construction of proposed pseudo inverse S-box depends on four steps; calculation of multiplicative inverses of the elements of the group of units $U(\mathbf{Z}_{p^i})$, then the construction of pseudo S-box based on $U(\mathbf{Z}_{p^i})$, defining the arrangement of linear and inverse transformations and in the last step defining one-one correspondence between $U(\mathbf{Z}_{p^i})$ and F_{p^j}. Therefore p^j distinct values of S-box are obtained. The following are the main steps of our proposed algorithm for the construction of nonlinear component of block cipher:

- The set of unit elements $U(\mathbf{Z}_{p^i})$ of local ring $\mathbf{Z}_{p^i}$ is given as;

$$U_{p^i} = U(\mathbf{Z}_{p^i}) = \{z \in \mathbf{Z}_{p^i} : \gcd(z, p^i) = 1\} = \{2t+1 \ : 0 \le t \le p^j - 1\}. \quad (6)$$

Now we introduce map, $I: U_{p^i}^n \to U_{p^i}^n$, defined as:

$$I(z) = z^{-1}. \quad (7)$$

So, we can give the table of multiplicative inverse of each $2t+1$ element row-wise (Table 1).

- Here we need the linear map, $\omega: U_p^m \to U_p^n$ represented by

$$L(z) = Az \text{ where, } A \in PSI(n \times m, \mathrm{F}_p). \quad (8)$$

- For calculation purpose, we have combined the inverse and linear transformation with the help of composition map:

$$\psi = LoI: U_p^m \to U_p^n. \quad (9)$$

gives

$$\psi(x) = Ax^{-1}. \quad (10)$$

- We define bijective affine transformation,

$\varphi = Ho\psi: U_p^n \to U_p^n$ by

$$\varphi(x) = Ax^{-1} \oplus b. \quad (11)$$

We will have to elaborate the above construction with small example. Let us consider $U(\mathbf{Z}_{2^5})$ then the construction of pseudo S-box based on $U(\mathbf{Z}_{32})$ and in the last step defining one-one correspondence between $U(\mathbf{Z}_{32})$ and F_{2^4}. Consequently 2^4 distinct values of S-box are obtained.

First Step:

The set of unit elements $U(\mathbf{Z}_{32})$ of local ring $\mathbf{Z}_{32}$ is given as:

$$U_{32} = U(\mathbf{Z}_{32}) = \{z \in \mathbf{Z}_{32} : \gcd(z, 32) = 1\} = \{2t+1 \ : 0 \le t \le 15\}. \quad (12)$$

Now we introduce map, $I: U_{32}^5 \to U_{32}^5$, defined as

$$I(z) = z^{-1}. \quad (13)$$

We can give the table of multiplicative inverse of each $2t+1$ element row-wise (Table 1).

Second step:

Here we need the linear map, $\omega : U_2^5 \to U_2^4$ represented by

$$L(z) = Az \text{ where } A \in PSI(4\times 5, \mathrm{F}_2). \quad (14)$$

For calculation purpose, for instance, we choose the composition map:

$$\psi = LoI : U_2^5 \to U_2^4. \quad (15)$$

gives

$$\psi(x) = Ax^{-1}. \quad (16)$$

Third step:

We define bijective affine transformation $\varphi = Ho\psi : U_2^4 \to U_2^4$ by

$$\varphi(x) = Ax^{-1} \oplus b, \quad (17)$$

where

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix} \text{ and } b = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

The proposed nonlinear component of block cipher is given in the Table 1 as follow:

Table 1: Anticipated confusion component.

(k,l)	0	1	2	3
0	6	13	9	2
1	8	12	7	3
2	11	15	4	0
3	10	1	5	14

The proposed nonlinear component is tested against different cryptographic characteristics. We will have to utilize the anticipated technique in information hiding scheme namely steganography. For that we needed three different S-boxes with same cryptographic capabilities. The final expression for the other two designed nonlinear component of block cipher, discussed later in statistical analysis [2-3]:

$$\varphi_2(x) = A_2(A_1 x \oplus b_1) \oplus b_2. \quad (18)$$

4. Proposed Hiding Scheme

As proposed technique is applied on images for better analysis of results. At first, generating a unique matrix of S-box using Galois ring such that not a single component of S-box is repeated. Then by using that S-box encryption (Substitution) is done on an image to be hide. Further by using Galois ring four 2×2 small S-boxes ($G_1G_2G_3G_4$) are generated where 16 values (0 to 15) are stored. Taking the first pixel of encrypted image converted into 8-bit binary e.g. 217 values for first pixel of encrypted image, converted into 8-bit binary '11011001'. Divide 8-bit binary into four, 2-bit group as '11', '01', '10', '01' then mapping these generated 2-bits group to small S-boxes as '11' approaching the value of 1st row and 1st column of G_1 similarly '01', '10', '01' to the values of G_2, G_3, G_4 respectively. Then taking the first pixel of cover image (image in which encrypted image to be hide) converted into 8-bit binary e.g. 198 value for first pixel of cover image, converted into 8-bit binary '11000110'. Splitting 8-bit binary into 4-bit MSBs and 4-bit LSBs as MSBs = '1100' and LSBs= '0110'. As a value e.g. 12 picked from G_1 converted into 4-bit binary '1100' then placed into LSBs of first pixel of cover image as MSBs = '1100' and LSBs = '1100' presenting in 8-bit now the value for the 1st pixel of cover image is '11001100' decimal representation as 204 (converted from 198). Similarly, same operation is done for 2nd, 3rd and 4th pixels of cover image using values picked from

G_2, G_3, G_4 respectively next again for 5th, 6th , 7th and 8th pixels of cover image using values picked from G_1, G_2, G_3, G_4 respectively. The complete steps of proposed scheme are represented in section 4.1 (see Fig. 1).

4.1 System Model

The flowchart of the proposed image steganography technique method is shown in Fig. 1. The proposed method divided into two phases: in the first phase, a S-box is generated using Galois ring and an image to be hide is encrypted by using that S-box. In the second phase generating four S-boxes are generated by using these Steganography is done i.e. encrypted image has been hiding in another image (cover image). Our proposed steganography technique is discussed in detail step by step as below:

First Phase:

Step 1: Generating a G_{S-box} 16×16 matrix from Galois ring i-e.,

$$G_{S-box}=\begin{pmatrix} G_{1,1} & \cdots & G_{1,16} \\ \vdots & \ddots & \vdots \\ G_{16,1} & \cdots & G_{16,16} \end{pmatrix}. \qquad (19)$$

Step 2: Encrypt *Image* of size $256\times256\times3$ i.e. Each pixel of image is substituted with G_{S-box} values:

$$Image_{Subs} = Image\,\textbf{substitute}\,G_{S-box}. \qquad (20)$$

Second Phase

Step 3: Generating four 2×2, small S-boxes as G_1, G_2, G_3, G_4 from Galois ring:

$$G_1=\begin{pmatrix} G_{1_{1,1}} & G_{1_{1,2}} \\ G_{1_{2,1}} & G_{1_{2,2}} \end{pmatrix} \quad G_2=\begin{pmatrix} G_{2_{1,1}} & G_{2_{1,2}} \\ G_{2_{2,1}} & G_{2_{2,2}} \end{pmatrix},$$

$$G_3=\begin{pmatrix} G_{3_{1,1}} & G_{3_{1,2}} \\ G_{3_{2,1}} & G_{3_{2,2}} \end{pmatrix} \quad G_4=\begin{pmatrix} G_{4_{1,1}} & G_{4_{1,2}} \\ G_{4_{2,1}} & G_{4_{2,2}} \end{pmatrix}. \qquad (21)$$

Step 4: Each decimal pixel of $Image_{Subs}$ is converted into binary of 8-bit at index *i* and *j*:

$$Image_{bin} = decimal2binary\left(Image_{Subs}(i,j)\right), \qquad (22)$$

Step 5: Each 8-bit binary pixel of $Image_{bin}$ is split into 2,2 bits part*:*

$$P_1 = Image_{bin}(1:2) \qquad (23)$$

$$P_2 = Image_{bin}(3:4) \qquad (24)$$

$$P_3 = Image_{bin}(5:6) \qquad (25)$$

$$P_4 = Image_{bin}(7:8) \qquad (26)$$

Step 6: Pick $G_{1_{i,j}}$ as according to P_1 position in G_1 similarly for G_2, G_3, G_4 according to P_2, P_3, P_4 respectively.

$$G_{P_1} = \left(G_{1(i,j)}\text{:value according to } P_1 \text{ position in } G_1\right) \qquad (27)$$

Step 7: Each decimal value G_{P_1} is converted into binary of 4-bit.

$$G_{P_1 bin} = decimal2binary\left(G_{P_1}\right). \qquad (28)$$

$$G_{P_1 bin} = G_{P_1 bin}(1:4). \qquad (29)$$

Step 8: After getting these values inserting these values into cover image. As each decimal pixel of cover image $Image_{cover}$ of size $512\times512\times3$ is converted into binary of 8-bit at index i and j.

$$Cover_{bin} = decimal2binary\left(Image_{cover}(i,j)\right). \qquad (30)$$

Step 9: Each 8-bit binary pixel of $Cover_{bin}$ is split into *4 MSBs* and *4 LSBs.*

$$MSB_{cover} = Cover_{bin}(1:4), \qquad (31)$$

$$LSB_{cover} = Cover_{bin}(5:8). \qquad (32)$$

Step 10: Substituting $G_{P_1 bin}$ in $LSBs_{cover}$ as

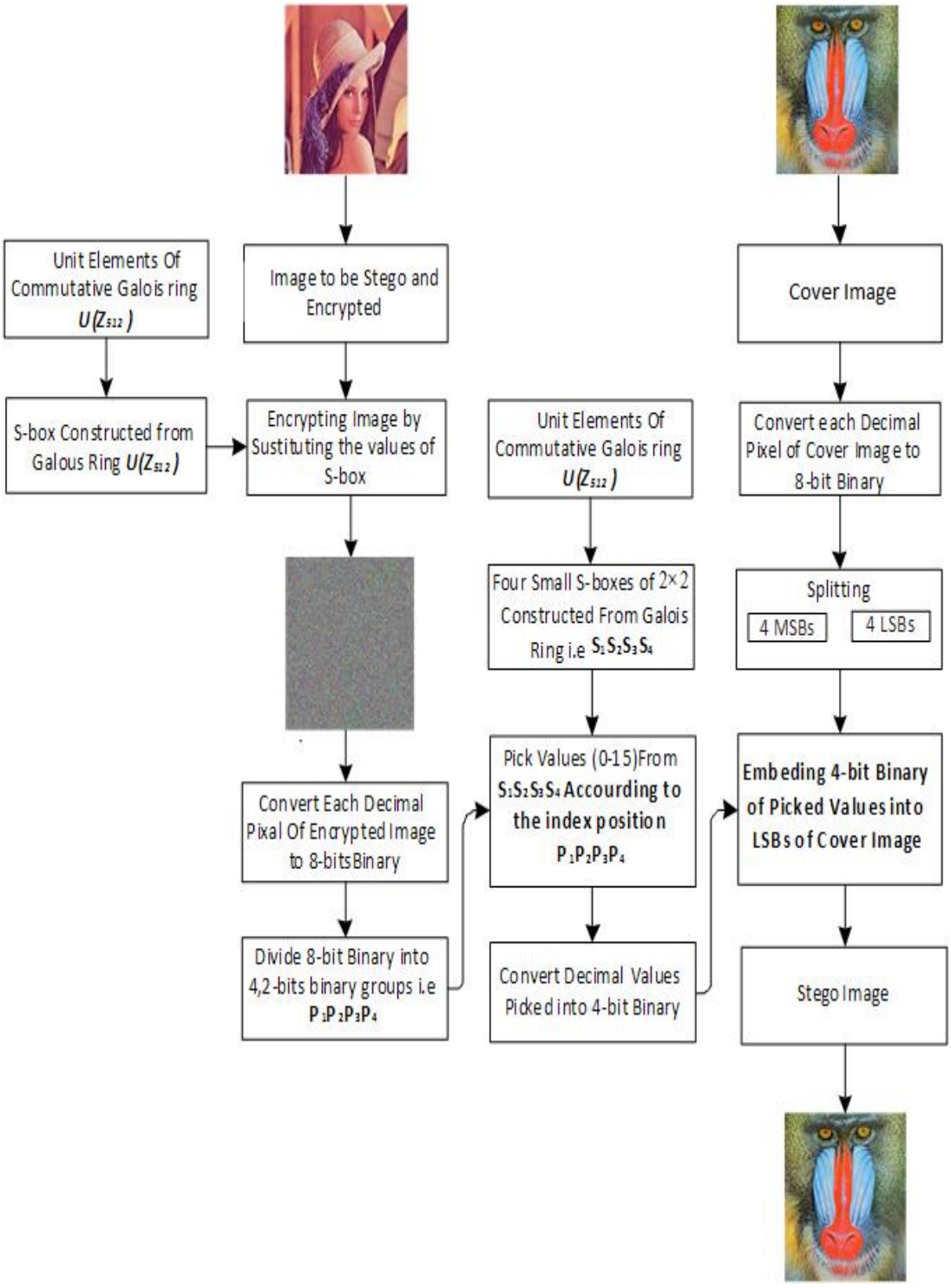


Fig. 1: Proposed algorithm for Steganography of digital image of Baboon of size 512×512×3.

$$LSBs_{cover} = G_{P_1 bin} \quad (33)$$

Now,

$$MSB_{cover} = Cover_{bin}(1:4), \quad (34)$$

$$G_{P_1 bin} = Cover_{bin}(5:8). \quad (35)$$

Step 11: Concatenate new modified $LSBs_{cover}(G_{P_1 bin})$ with MSB_{cover} to get final stego image $Image_{stego}$ of size $512 \times 512 \times 3$.

$$Image_{stego} = concatenate\left[MSB_{cover}, G_{P_1 bin}\right]. \quad (36)$$

5. Cryptographic Characteristics of Confusion Component

In this section, we will discuss the cryptographic characteristics which are necessary to satisfy to qualify for a good confusion component [4-7, 26-30].

5.1 Nonlinearity

The minimum hamming distance between Boolean function f and all affine Boolean function over F_2^n. Mathematically it can be defined as [4]

$$N_f = \min_{a \in A_n} d(f, a), \quad (37)$$

where A_n is the set of all affine function over $GF(2^n)$ and d is hamming distance. In the term of Walsh spectrum, the non-linearity of a function can be defined as follows:

$$N_f = 2^{n-1} - 2^{-1} \max |Walsh\ Spectrum|. \quad (38)$$

The nonlinearity is an algebraic criterion to ensure the confusion capability of Boolean functions quantitatively.

5.2 Bit Independent Criteria

Bit independence criterion (BIC) examined those contribution bits that stay unchanged. The alteration of unchanged contribution bits and the avalanche vectors' independent performance of pairwise variables are the properties of this measure. In the symmetric cryptosystem, BIC is an operative belonging as, by accumulative independence between bits, it is almost difficult to guess and identify the configuration of the scheme. A Boolean function $g : \mathrm{F}_2^n \to \mathrm{F}_2^n$ satisfies the BIC if $\forall\ l, p, q \in \{1, 2, ..., n\}$, with $p \neq q$, transforming input bits p and q to change independently. The avalanche vector V^{ei} which is the correlation coefficient among p^{th} and q^{th} parts of yield dissimilarity sequence is desirable to measure the bit independence criteria. A bit independence parameter connecting to the impact of the l^{th} input bit change on the p^{th} and q^{th} bits of V^{ei} is characterized as [5]:

$$BIC(b_p, b_q) = \max_{1 \le i \le n} \left| corr(b_p^{e_l}, b_q^{e_{l'}}) \right|. \quad (39)$$

The bit independence criterion (BIC) parameter for the S-box function g is defined as follows:

$$BIC(g) = \max_{\substack{1 \le p,q \le n \\ p \neq q}} BIC(b_p, b_q), \quad (40)$$

which establishes how close f is to satisfying the BIC. $\mathrm{BIC}(f)$ takes values in $[0,1]$.

5.3 Linear approximation probability

The variableness of an occasion between input and output bits is examined by the linear approximation probability test which is also known as LP. In LP, the likeness of the information bits given by a specific mask δ_x and the equality of the yield bits δ_y are utilized to decide the probability of predisposition. Mathematically LP can be defined as [6]:

$$LP = \max_{\delta x, \delta y \neq 0} \left| \frac{\#\{x / x \cdot \delta_x = S(x) \cdot \delta_y\}}{2^n} - \frac{1}{2} \right|, \quad (41)$$

where δ_x and δ_y shows the input/output masks utilized in calculating the linear approximation probability.

5.4 Differential approximation probability

Differential cryptanalysis (DC) is one important criterion for the selection of best nonlinear confusion component of block cipher. This cryptographic attack is fall in the category of chosen plaintext attack, which means that that the invader is capable to choose responses and investigate yields to obtain possible encryption key. The differential approximation probability (DP) is one of the measurements used to quantify the strength of nonlinear confusion component against the differential attack. The minor the DP more noteworthy the function of nonlinear part of the block cipher to demonstrate protection alongside the differential kind of cryptanalysis assaults. The mathematical expression for *DP* is given below [7]:

$$DP_{f(\Delta x_i \to \Delta y_i)} = \left[\frac{\#\{x_i \in X \,/\, f(x_i \oplus \Delta x_i) = \Delta y_i\}}{2^n} \right]. \quad (42)$$

5.5 Strict Avalanche Criterion

Webster and Teveres (1985) presented the strict avalanche criterion (SAC) by merging the two important cryptographic characteristics namely avalanche and completeness of Boolean function. SAC is confirmed through small change in input of Boolean function generate a significant change in corresponding output of the Boolean function. An input bit m is changed; each output bit will change with probability of 0.5 which shows half of the output will be changed. To achieve this effect, we will need a function that has an approximately 50% dependency on each of its n input bits. Mathematical expression of SAC can be clarified as [6]

$$\mathrm{wt}(x \oplus e_1) \oplus g(x) = \sum_{j=1}^{2^m-1} [g(x^j \oplus e_1) \oplus g(x^j)] = 2^{m-1}, \quad (43)$$

where affine function $e_1 \in \mathrm{F}_2^m$ with hamming weight $\mathrm{wt}(e_1) = 1$ and $\oplus$ signify the XOR operation. The cryptographic characteristics of S-box are basic principle to construct a robust secure nonlinear component of block ciphers. The most useful algebraic characteristics of cryptographically strong Boolean functions are nonlinearity, SAC, BIC, DP and LP respectively. These characteristics are equally applied for nonlinear component namely S-boxes since each S-box is consisting of Boolean functions. In our case, we have taken 4-bits confusion component and compared with already existing benchmarks (see Table 2). It is quite evident from the investigations of Table 2 that our suggested scheme has high nonlinearity as compared to other existing 4-bits confusion component. The projected scheme is immune against linear attacks which can easily be confirmed by linear approximation probability values. The linear approximation probability is quite low for our offered nonlinear components (S_1, S_2, S_3) as compared to other results available in literature [18-22]. The diffusion characteristic of the proposed confusion component is satisfied with the help of avalanched, strict avalanche criteria (SAC) and bit independent criteria (BIC). Informally, the avalanche effect is defined as small changes in inputs should always lead to large changes in outputs (see Table 2). In the avalanche criterion our preference is to look at the output as a whole whereas in strict avalanche criterion, we have to look at each bit one by one and must verify that whatever the other bits will change, it will have a 50% probability to switch. The SAC is satisfied in case of our proposed confusion component as the SAC and BIC-SAC in case of our offered scheme are 0.5 and 0.4844 and comparable to the standard lightweight S-boxes (see Table 2). The values of DP and LP are quite low and comparable to the S-boxes available in literature which clearly reveals that our suggested construction scheme is quite competent of immunize against linear and differential attacks [27-30].

6. Difference Analyses

The contents of an image and its texture is characterized by its analysis. Basically, the assessment metrics can be classified into three different classes. All these analysis categories the successfulness of proposed work. The first class is based on pixel difference-based quality metrics (peak signal to noise ratio (PSNR), means square

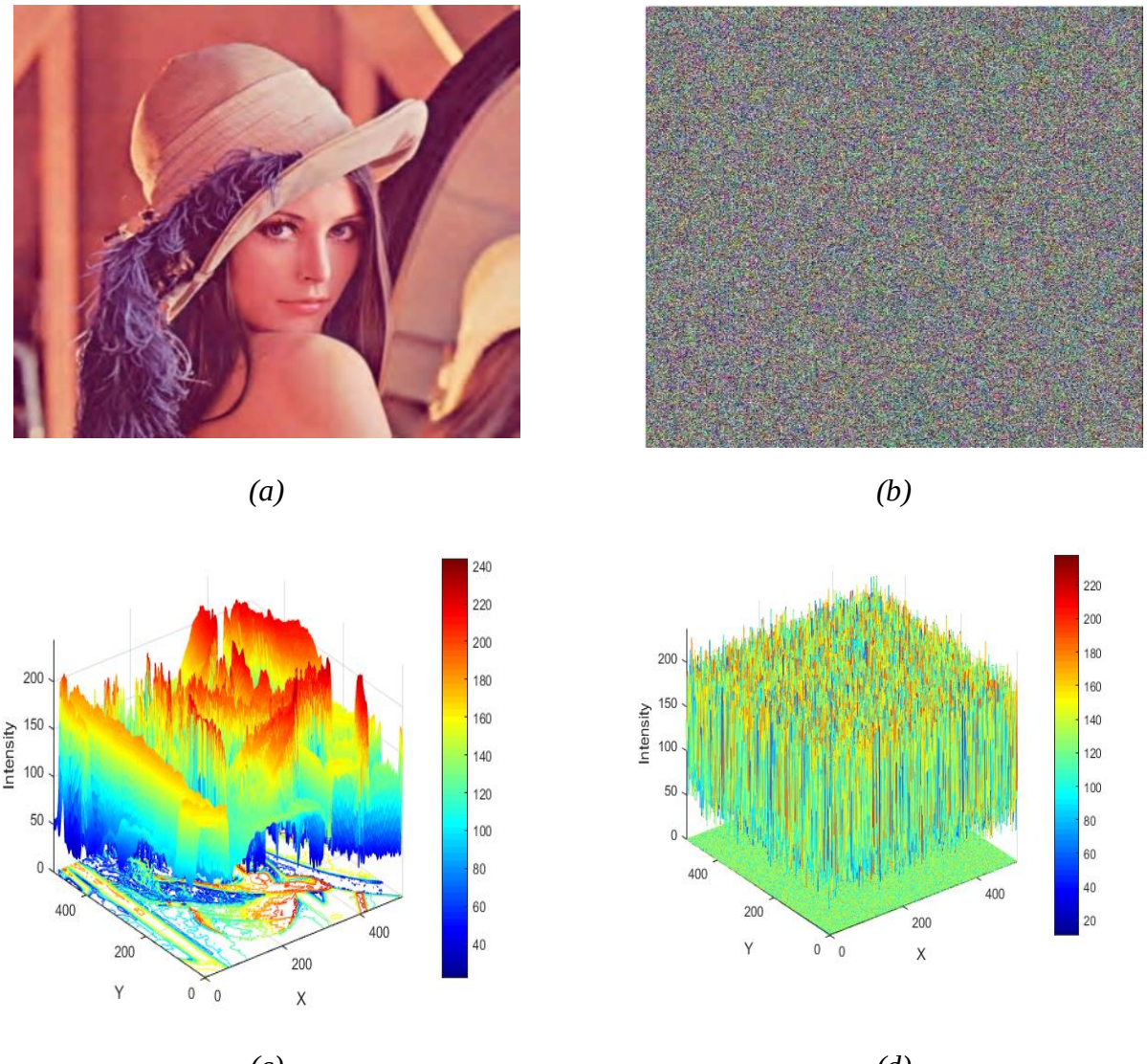
error (MSE), maximum difference (MD), normalized absolute error (NAE)) where we need two digital mediums, the second classification is based on correlation among the neighboring pixels, which includes (structure content (SC), structure similarity index measure (SSIM), normalized correction coefficient (NCC)) and third one is based on human vision system which is fundamentally based on similarity detection. All these difference analyses already discussed in detail in [2-3, 15-17]. We have conducted these analyses for our proposed steganography technique as image quality analysis in Table 3 as follow:

Table 2: Cryptographic characteristics of suggested confusion component.

		S_1	S_2	S_3	[18]	[20]	[21]	[22]	[19]
BIC-NL	Min.	0	0	0	0	0	0	0	0
	Max.	4	4	4	4	4	4	4	4
	Avg.	2.5	2.5	2.5	2.5	2.5	2.5	2.5	3.0
BIC-SAC	Min.	0.3750	0.4166	0.4166	0.4167	0.4167	0.4167	0.4167	0.4167
	Max.	0.6250	0.6250	0.5833	0.6250	0.5833	0.5833	0.5417	0.5417
	Avg.	0.4844	0.4895	0.500	0.5052	0.4688	0.5000	0.5000	0.4739
NL	Min.	4	4	4	2	2	2	4	2
	Max.	4	4	4	4	4	4	4	4
	Avg.	4	4	4	3.5	3.5	3.5	4	3.5
LP	Min.	0.250	0.250	0.250	0.375	0.250	0.375	0.375	0.3750
	Max.	0.250	0.250	0.250	0.375	0.250	0.375	0.375	0.3750
	Avg.	0.250	0.250	0.250	0.375	0.250	0.375	0.375	0.3750
DP	Min.	0.125	0.125	0.125	0.250	0.250	0.250	0.125	0.125
	Max.	1	1	1	1	1	1	1	1
	Avg.	0.3203	0.3203	0.3203	0.3672	0.3672	0.3516	0.3046	0.3125
SAC	Min.	0.3750	0.3750	0.3750	0.3750	0.2500	0.3750	0.2500	0.2500
	Max.	0.6250	0.6250	0.6250	0.6250	0.7500	0.6250	0.6250	0.7500
	Avg.	0.5000	0.5162	0.4843	0.4922	0.5000	0.4531	0.4375	0.4688

Table 3: Image quality analysis measure of steganography image.

Classifications of statistical analyses		Color Component of stego image			
		RGB	Red	Green	Blue
Pixel Difference Based	MSE	8.769	11.0910	10.4100	11.45
	PSNR	34.2656	33.7782	34.0805	33.7752
	MD	39	38	39	39
	NAE	0.0156	0.0141	0.0214	0.0270
Correlation Based	SC	1.0056	0.9905	1.0060	1.0037
	SSIM	0.9667	0.9645	0.96676	0.96675
	NCC	0.9990	1.0041	0.9963	0.9973



(a) *(b)*

(c) *(d)*

Fig. 2: 3D surface plot of original image to be hide (a) and encrypted image (b) of (a). (c) Combined 3D surface plot of original image (a), (d) Combined 3D surface plot of encrypted image(b).

If there should be an occurrence of stego image the estimations of pixel difference-based estimation for example PSNR, MSE, MD and NAE is little which shows the invariant idea of offered data hiding plan which is one of the vital qualities of implanting plan. The consequences of these distance estimations explain that the foreseen procedure does not influences real substance by embeddings the secret data in cover digital medium (see Fig. 3). Besides, we have added the correlation estimations for our recommended plot. When all is said in done, the correlation-based estimations are used to research the direct connections among the pixels of the advanced image. For plain data, the correlation-based amounts are shut to solidarity while if there should be an occurrence of encrypted data the qualities diminishing to zero because of high randomness (see Fig. 2). The proposed plot does not influence the real substance of cover medium by adding the encrypted secret image. The high level of this twofold layer data hiding plan is very helpful for constant encryption over information interface layer. Over the correspondence channel, it tends to be handily anticipated that whether a plain or encrypted data is passing because of entropy test. The cipher substance has high entropy though the plain data entropy is not high. In this manner, by beguiling the dynamic snoop in correspondence channel, we need to use the proposed plan to shroud our secret data in plain cover image which safe

transmission through insecure line of communication.

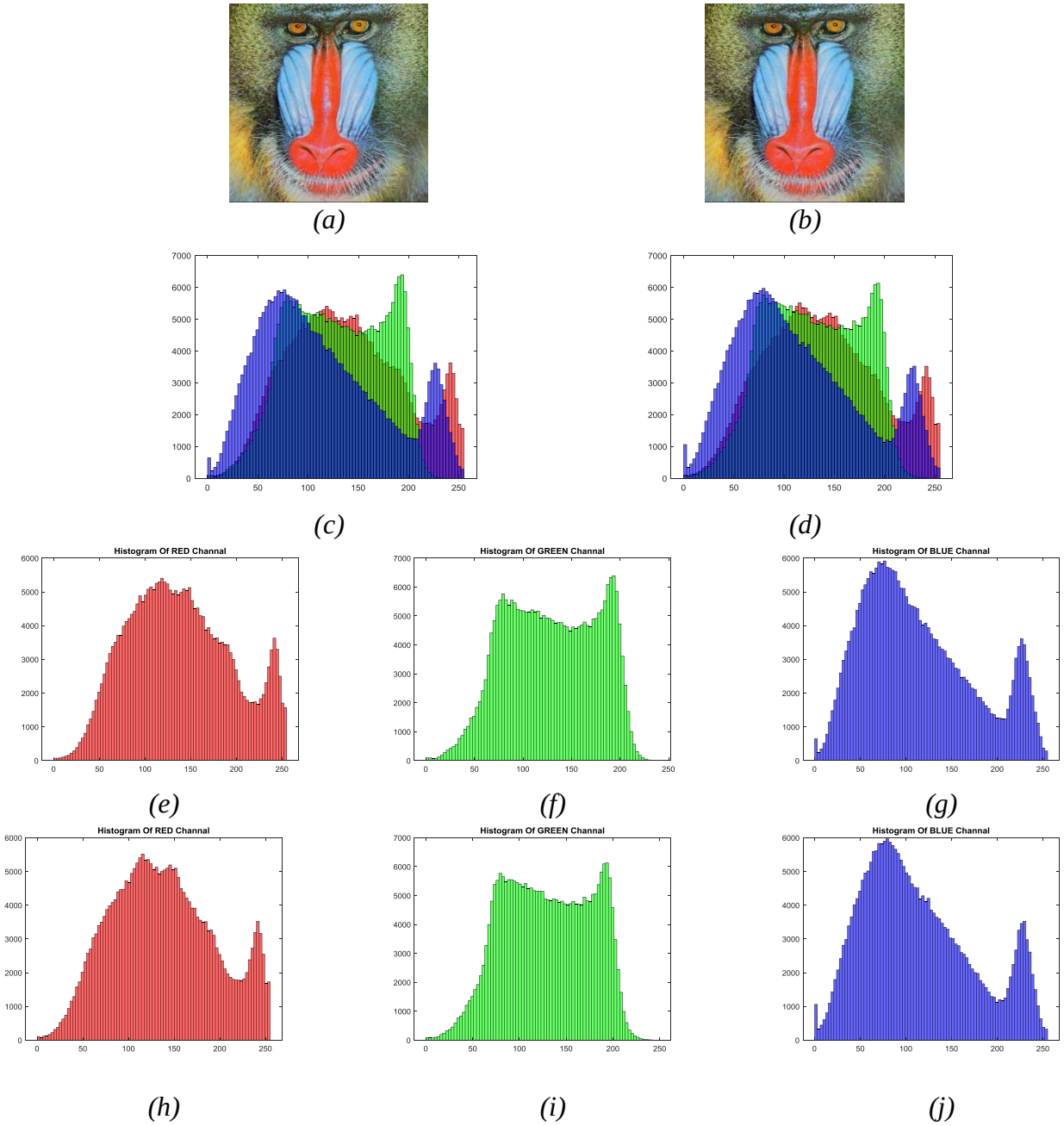


Fig. 3: Histograms analyses of cover (a) and steganographic cover image (b) of Baboon with size 512×512×3, (c) Histogram of cover image (d) Histogram of steganographic cover image. RGB Layer wise histograms of cover image and steganographic cover image, RGB layers of cover image (e, f, g) Red, green, and blue layers of steganographic cover image (h, i, j).

7. Conclusion

In this research article, we have designed a new mechanism for the construction of confusion component of modern block cipher. The proposed scheme is based on rectangular matrices which leads to notion of pseudo inverses. The proposed confusion component is equally utilized in encryption of the secret content and then hided it in cover medium without disturbing the actual content which is one of the most important and challenging issue of the information hiding. Our proposed information hiding scheme can be used for copyright protection of audios and videos too. In future, we will try to design an extended version of our proposed work for audio and video files.

Acknowledgement

The first author extends her gratitude to Deanship of Scientific Research at Princess Nourah bint Abdulrahman University for funding this work through the Fast-track Research Funding Program.

Funding

The first author extends her gratitude to Deanship of Scientific Research at Princess Nourah bint Abdulrahman University for funding this work through the Fast-track Research Funding Program.

References

[1]. Majid Khan, Tariq Shah and Syeda Iram Batool [2015] "Texture analysis of chaotic coupled map lattices based image encryption algorithm," 3D Research, 15 (3) 1–5.

[2]. Majid Khan, Tariq Shah and Syeda Iram Batool [2017] "A new approach for image encryption and watermarking based on substitution box over the classes of chain rings," Multimedia Tools and Applications, 76 (22) 24027–24062.

[3]. Majid Khan, Tariq Shah [2015] "A copyright protection using watermarking scheme based on nonlinear permutation and its quality metrics," Neural Comput & Applic., 26 (4) 845-855.

[4]. Syeda Iram Batool, Majid Khan and Tariq Shah [2014] "A color image watermarking scheme based on affine transformation and S4 permutation," Neural Comput. & Applic., 25,2037–2045.

[5]. Majid Khan, Tariq Shah [2014] "A construction of novel chaos base nonlinear component of block cipher," Nonlinear Dynamics, 76,377–382.

[6]. Majid Khan, Tariq Shah, Hasan Mahmood, M. A. Gondal [2013] "An efficient method for the construction of block cipher with multi-chaotic systems," Nonlinear Dynamics,Volume 71,493-504.

[7]. Majid Khan, Tariq Shah, M. A. Gondal [2013] "An efficient technique for the construction of substitution box with chaotic partial differential equation," Nonlinear Dynamics, 73,1795-1801.

[8]. M. Iizulca [1987] "Quantitative evaluation of similar images with quasi-gray levels," Computer Vision, Graphics, and Image Processing, 38, 342-360.

[9]. Ming Si, Jibo Si [2007] "Research on Embedding and Extracting Methods for Digital Watermarks Applied to QR code Images," New Zealand Journal of Agricultural Research, 50,861-867.

[10]. R.M. Haralick, K. Shanmugam, and I. Dinstein, [1973] "Textural Features for Image Classification," IEEE Trans. On Systems, Man and Cybernetics, 3,610-621.

[11]. R.M. Haralick and K. Shanmugam [1973] "Computer Classification of Reservoir Sandstones," IEEE Trans. on Geo. Eng., 11, 171-177.

[12]. R.W. Conners and C.A. Harlow [1980] "A theoretical comparison of texture algorithms," IEEE Trans. on Pattern Analysis and Machine Intell., 2 -204- 222.

[13]. R.W. Conners, M.M. Trivedi, and C.A. Harlow [1984] "Segmentation of a High-Resolution Urban Scene Using Texture Operators," Computer Vision, Graphics, and Image Processing, 25,273-310.

[14]. S. W. How, J. J. LI [2011] "Chaotic System and Factorization based Robust Digital Image Watermarking Algorithm," Journal of Central South University of Technology, 18 (1) 116-124.

[15]. Hafiz Muhammad Waseem, Majid Khan, A new approach to digital content

privacy using quantum spin and finite-state machine, Journal of Applied Physics B, (2019) 125: 27. https://doi.org/10.1007/s00340-019-7142-y.

[16]. Irfan Younas, Majid Khan, A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi Group and Lorenz Chaotic System, International Journal of Entropy, Accepted, 2018.

[17]. Majid Khan, Hafiz Muhammad Waseem, A Novel Image Encryption Scheme Based on Quantum Dynamical Spinning and Rotations, PLoS ONE 13(11): e0206460.

[18]. Cid C, Murphy S, Robshaw MJB (2005) Small scale variants of the AES, Proceedings of FSE 2005, LNCS, 145–162. Springer.

[19]. El-Sheikh HM, El-Mohsen OA, Elgarf T, Zekry A (2012) A new approach for designing key-dependent S-Box defined over GF(2^4) in AES. Int J Comput Theory Eng 4(2):158–164.

[20]. Nakahara J Jr, de Freitas DS (2009) Mini-ciphers: a reliable testbed for cryptanalysis, "symmetric cryptography", seminar 09031. In: Dagstuhl S (ed) Dagstuhl Seminar Proceedings. Leibniz-Zentrum fuer Informatik, Germany, pp 1862–4405

[21]. Mihajloska H, Gligoroski D (2012) Construction of optimal 4-bit S-boxes by Quasigroups of order 4. In: The 6th international conference on emerging security information, systems and technologies, SECURWARE 2012, Rome, Italy

[22]. Phan RC-W (2002) Mini advanced encryption standard (Mini-AES): A testbed for cryptanalysis students. Cryptologia XXVI(4):283–306.

[23]. Sajjad Shaukat Jamal, Tariq Shah, Shabieh Farwa, Muhammad Usman Khan. "A new technique of frequency domain watermarking based on a local ring", Wireless Networks, 2017.

[24]. Anchal Jain, Pooja Agarwal Rashi Jain, Vyomesh Singh, Chaotic Image Encryption Technique using S-box based on DNA Approach, International Journal of Computer Applications, 92 (2014) 30-34.

[25]. Li shuai, Lina wang, Li miao, Xianwei zhou, Construction Based on the Cayley Graph of the Symmetric Group for UASNs, 7 (2019) 38826- 38832.

[26]. Amjad Hussain Zahid, Muhammad Junaid Arshad, An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping, Symmetry 2019, 11(3), 437; https://doi.org/10.3390/sym11030437.

[27]. Zahid, Amjad Hussain, Muhammad Junaid Arshad, and Musheer Ahmad. "A Novel Construction of Efficient Substitution-Boxes Using Cubic Fractional Transformation." Entropy 21, no. 3 (2019): 245.

[28]. Alzaidi, Amer Awad, Musheer Ahmad, Hussam S. Ahmed, and Eesa Al Solami. "Sine-Cosine Optimization-Based Bijective Substitution-Boxes Construction Using Enhanced Dynamics of Chaotic Map." Complexity 2018 (2018).

[29]. Ahmad, Musheer, Mohammad Zaiyan Alam, Zeya Umayya, Sarah Khan, and Faiyaz Ahmad. "An image encryption approach using particle swarm optimization and chaotic map." International Journal of Information Technology 10, no. 3 (2018): 247-255.

[30]. Ahmad, Musheer, M. N. Doja, and MM Sufyan Beg. "ABC optimization based construction of strong substitution-boxes." Wireless Personal Communications 101, no. 3 (2018): 1715-1729.

[31]. Žiljak, V., Golubić, L. T., Gršić, J. Ž., & Jurečić, D. Hidden Messages with Pigments in Dual Print for a Visual and Infrared Spectrum, International Journal of Circuits, Systems and Signal Processing, 13, 484-487.

[32]. Yuan He, Liqi Ou, Xiaofei Pu, Yunfei Li, Yuyuan Zhao, E-commerce Network Security Protection Technology based on Mixed Data Encryption Strategy, International Journal of Circuits, Systems and Signal Processing, pp. 727-731, Volume 13, 2019.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)