Multimed Tools Appl (2017) 76:24027–24062
DOI 10.1007/s11042-016-4090-y

A new approach for image encryption and watermarking based on substitution box over the classes of chain rings

Majid Khan [1] · **Tariq Shah** [2] · **Syeda Iram Batool** [2]

Received: 12 February 2016 / Revised: 19 October 2016 / Accepted: 24 October 2016 /
Published online: 26 November 2016

Abstract The meanings of passing information from one side to other side by a conventional way is been changed because of internet and communication technology. The issues of the security and the uprightness of information increase due to fast developments in digital world. Presently digital communication has become an important part of transmission of information securely. There are various internet applications which are utilized to convey covertly. As an outcome, the security of data against unapproved access has turned into a prime target. This leads to parts of advancement of different systems for information hiding. Cryptography and watermarking are famous techniques for hiding information accessible to conceal information safely. Our main goal here is to develop an innovative algebraic structures for the construction of nonlinear components of block cipher namely substitution boxes (S-boxes); and also use these components in image encryption and watermarking applications. Different types of S-boxes were introduced in literature based on Galois field and chaos theory in order to add confusion in any cryptosystems. The present construction is entirely based on Galois ring which enrich the existing algebraic structures of S-box theory.

Keywords Image encryption · Watermarking · S-boxes · Galois ring · Algebraic structures

1 Introduction

Information is exceptionally significant to any organization or for any individual. None of us prefers our discussion being caught as it contains the capability of being abused. Same is the situation with the information of any association or of any individual. The trading of information among two potential gatherings must be done in secured system to maintain a strategic

✉ Majid Khan
mk.cfd1@gmail.com

[1] Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad 44000, Pakistan

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

distance from any altering. Two sorts of dangers exist amid any data trade. The unintended client who may attempt to catch this discussion can either alter with this information to change its unique importance or it can attempt to listen to the message with proposition to decipher it. Both these attacks disregarded the secrecy and trustworthiness of the communication passed.

Giving planned get to and dodging unintended access is an exceptionally testing undertaking. Information hiding has been since long time. In past, individuals utilized concealed images or undetectable ink to pass on confidential data. But nowadays, we are living in the era of digital world where information security systems depends extensively on binary Boolean functions. Keeping in view the growing demands of digital security mechanism, we have devised a novel technique of image encryption and watermarking based on classes of finite chain ring to enrich existing information hiding scheme that rely on Galois field.

For valuable application and a new role, maximal cyclic subgroup of the group of units of a Galois extension ring attains a keen interest in algebraic cryptography and coding theory. In this respect, initially Shankar [30] presented a construction technique of BCH (Bose Chaudhuri Hocquenghem) codes over local commutative rings with the help of maximal cyclic subgroup of the group of units of a Galois extension of a local commutative ring $\mathbb{Z}_{p^k}$. The construction of this maximal cyclic subgroup is based on a mod $-p$ reduction map from commutative ring $\mathbb{Z}_{p^k}$ to $\mathbb{Z}_p$ (see Shankar [30]). However, the exponential sums over Galois rings and an upper bound for the hybrid sum over the Galois rings by using maximal cyclic subgroups of the groups of units of these Galois rings in a series of papers Cohen [12] and Shanbhag et al. [29]. Further, Andrade and Palazzo gave the construction of BCH codes over the Galois rings by means of maximal cyclic subgroup. In this sequel, Shah et al. [28] used maximal cyclic subgroups of the chain of groups of units in the chain of finite Galois rings to produce new class of S-boxes. In this correspondence, the proposed work presents a construction technique of a substitution box (S-box) using this maximal cyclic subgroup of the group of units in Galois rings and chain ring [3–8, 11, 12, 18–21, 28, 30]. The complexity of the problem is to construct bijective Boolean functions over this maximal cyclic subgroup adjoining zero, with the extension $0 \to 0$ and then apply permutation in order to increase the number of S-boxes in a databased to add confusion in the selection of appropriate S-boxes. These S-boxes are not so simple as compared to S-boxes which are based on Galois field. These proposed S-boxes are small in nature but having much enrich statistical and algebraic properties [9, 10, 13–15, 25, 31, 32]. The second part of this article is to utilize these structures in image encryption and data hiding techniques namely watermarking [16, 17, 22–24, 26, 27].

The paper is organized as follows: In Section 2, the algebraic structure of the maximal cyclic subgroup is presented. Section 3 consists of the algebraic expression of the proposed S-boxes over maximal cyclic subgroups of groups of units of Galois ring extensions $GR(4,2)$, $GR(4,4)$, $GR(8,4)$, $GR(16,4)$ and $GR(32,4)$ of $\mathbb{Z}_4$. In Section 4, we have added construction of S-boxes with Galois ring extensions. In Section 5, we discussed another class of chain ring and S-box construction. In Section 6, we examine the security of the projected S-box with first order texture analysis, second order texture analysis, image quality measures and image similarity metrics and section 7 is about conclusions and future directions.

2 Galois rings and their groups of unit elements

In this section, we discuss some elementary concepts, for instance; Local commutative ring with identity, Galois extension ring, unit elements, and maximal cyclic subgroup of group of invertible elements of a Galois ring.

2.1 Galois rings

We begin with some basic definitions of unitary (local) commutative rings.

Let R be a commutative ring with unity. An element u is unit in R if there exists an element v in R such that $u.\ v=1$, where 1 is the identity of R.

A commutative ring R with unity is said to be local if and only if its all non-unit elements form an additive Abelian group. For instance $\mathbb{Z}_{p^k}$, p is a prime integer and k is any positive integer, is a local ring.

Let R be a commutative ring with unity. A non-zero element a is a zero divisor in R if there exists a non-zero element b in R such that $a.\ b=0$.

Let (R, M) be a local commutative ring with unity. An irreducible polynomial $f(x)\in R[x]$ over R is said to be a basic irreducible polynomial if it is irreducible over the corresponding residue field K, where $(K=R/M)$.

Consider the finite local ring $\mathbb{Z}_{p^k}$, where p is prime and k is a positive integer with corresponding residue field $\mathbb{Z}_p$. Now $\mathbb{Z}_{p^k}[x]=\left\{a_0+a_1x+a_2x^2+\ldots+a_nx^n : a_i\in\mathbb{Z}_{p^k}, n\in\mathbb{Z}^+\right\}$ is the polynomial extension of $\mathbb{Z}_{p^k}$ in the variable x and $\mathbb{Z}_p[x]=\{a_0+a_1x+\ldots+a_nx^n : a_i\in\mathbb{Z}_p, n\in\mathbb{Z}^+\}$ is the polynomial extension of $\mathbb{Z}_{pk}$ in the variable x. Let $f(x)\in\mathbb{Z}_{p^k}[x]$ be a basic irreducible polynomial with degree h. Ideal generated by $f(x)$ is denoted as $\langle f(x)\rangle$ and defined as $\langle f(x)\rangle=\left\{a(x).f(x) : a(x)\in\mathbb{Z}_{p^k}[x]\right\}$. Let $R=\frac{\mathbb{Z}_{p^k}[x]}{\langle f(x)\rangle}=\left\{a_0+a_1x+a_2x^2+\ldots+a_{h-1}x^{h-1} : a_i\in\mathbb{Z}_{p^k}\right\}$ denote the set of residue classes of polynomial in x over $\mathbb{Z}_{p^k}$, modulo the polynomial $f(x)$. This ring, denoted by $GR(p^k, h)$, is a commutative ring with identity and is called the Galois extension of $\mathbb{Z}_{p^k}$. Also $GR(p^k, 1)$ is isomorphic to $\mathbb{Z}_{p^k}$ and $GR(p,h)=\frac{\mathbb{Z}_{p^k}[x]}{\langle f(x)\rangle}=K$ is isomorphic to $GF(p^h)$, a Galois field extension of $\mathbb{Z}_{p^k}$ having p^h elements, where $\overline{f}=r_p(f)$ polynomial f which has coefficient modulo p.

2.2 Maximal cyclic subgroup of group of units of Galois rings

Let K^* and R^* be the multiplicative group of units of field and the ring K and R, respectively. Then R^* is an abelian group and can be written in the direct product of cyclic subgroups. By the following Theorem from [1, Theorem 2], between these cyclic subgroups, there is only one cyclic subgroup of order p^h-1.

R^* has one and only one cyclic subgroup of order relatively prime to p. This cyclic subgroup has order p^h-1. The cyclic subgroup of order p^h-1 can be generated by the generator of the corresponding finite field. This cyclic subgroup is denoted by G_n, where $n=p^h-1$. Since the order of K^* and G_n is the same, i.e., p^h-1 and both will be cyclic. Therefore G_n is isomorphic to K^*.

3 Construction of S-boxes based on maximal cyclic subgroups

In order to create confusion in a data many techniques can be used to do so. One of these techniques is using an S-box. The strongest S-boxes are constructed through mathematical formulas and systematic calculations. In order to improve the quality many have worked in the Galois fields $GF(2^n)$, $1\leq n\leq 8$ and created numerous S-boxes. In [1], a 4×4 S-box over maximal cyclic subgroup of group of units of Galois ring $GR(4, 4)$ is constructed with its application in watermarking. However, as an extension to [1], in this section, a novel construction technique of 4×4 S-boxes with the utility of maximal cyclic subgroups of groups of units of the Galois rings $GR(4,4)$, $GR(8,4)$ and $GR(32,4)$ is given. While, in each three cases the maximal cyclic subgroups G_{15} of orders 15 are, respectively, isomorphic to the cyclic Galois group $GF(2,4)^*$. The association of maximal cyclic subgroups with admiring cyclic Galois group $GF(2,4)^*$, which are caused by the mod- 2 reduction maps from local commutative rings $\mathbb{Z}_4$, $\mathbb{Z}_8$ and $\mathbb{Z}_{32}$ to their common residue field $\mathbb{Z}_2$, supports in construction of the 4×4 S-boxes over maximal cyclic subgroups. Of course these newly designed S-boxes are increasing complexity during encryption and decryption.

3.1 S-box construction algorithm on Galois ring $GR(\mathbb{Z}_{2^m}, 4)$

Given below is the procedure, defining the S-box in 4 steps:

Step.1: Inversion function $I : G_n \cup \{0\} \rightarrow G_n \cup \{0\}$,
Step.2: Linear scalar multiple function $f : G_n \cup \{0\} \rightarrow G_n \cup \{0\}$,
Step.3: Take composition of $I \circ f$ to get $(n+1) \times (n+1)$ S-box,
Step.4: Apply permutations S_n to each element of S-box obtained in step 3, which gives us $n!$ S-boxes.

The map described above is nothing more than a substitution within the set $G_n \cup \{0\}$. An element of the set is substituted with the element next to its respective inverse. (In this case we define this direction with increasing power of the generator) or in other words the scalar multiplied with the inverse. In the examples below we discuss and analyze this construction method for S-boxes of size 4×4.

Let us consider the local rings $\mathbb{Z}_4 = \{0,1,2,3\}$, $\mathbb{Z}_8 = \{0,1,2,\ldots,7\}$, $\mathbb{Z}_{16} = \{0,1,2,\ldots,15\}$ and $\mathbb{Z}_{32} = \{0,1,2,\ldots,31\}$, whereas $\mathbb{Z}_2 = \{0,1\}$, is their common residue field. The monic polynomial $f(x) = x^4 + x + 1$ is basic irreducible over the local rings $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_{16}$ and $\mathbb{Z}_{32}$ such that $f(x) = f(x) \mod 2 = x^4 + x + 1$ is irreducible polynomial over $\mathbb{Z}_2$.

3.2 S-box on $GF(2^4)$

Take the polynomial ring $\mathbb{Z}_2[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_2, n \in \mathbb{Z}^+\}$ in one indeterminate x over binary field $\mathbb{Z}_2$. Let $<f(x)> = \{a(x).f(x) : a(x) \in \mathbb{Z}_2[x]\}$ be the principal ideal in $\mathbb{Z}_2[x]$, generated by $f(x)$. Then elements of Galois extension field $K = \mathbb{Z}_2[x])/(<f(x)>)$, of order 16 are given in Table 1.

Now, let us construct the S-box on the Galois field extension $GF(2^4)$ (Table 1). It can be seen in Table 2 that it is the most basic S-box and it satisfies all the fundamental properties being an S-box.

3.3 S-box on $GR(4,4)$

Let $\mathbb{Z}_4[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_4, n \in \mathbb{Z}^+\}$ is the polynomial ring with one indeterminate x and $<f(x)> = \{a(x).f(x) : a(x) \in \mathbb{Z}_4[x]\}$ is a principal ideal generated by $f(x)$. Thus $R = (\mathbb{Z}_4[x])/(<f(x)>) = \{a_0 + a_1x + a_2x^2 + \cdots a_{(4-1)}x^{(4-1)} : a_i \in \mathbb{Z}_4\}$ is the Galois ring extension of order 256 with corresponding Galois field extension $K = (\mathbb{Z}_2[x])/(<f(x)>)$ of order 16, whose elements are given in Table 1.

Table 1 Elements of Galois field $GF(2^4)$

Exp	Polynomial	Binaries representation
$-\infty$	1	0000
0	1	1000
1	$1+x$	1100
2	$1+x^2$	1010
3	$1+x+x^2+x^3$	1111
4	x	0100
5	$x+x^2$	0110
6	$x+x^3$	0101
7	$1+x^2+x^3$	1011
8	x^2	0010
9	x^2+x^3	0011
10	$1+x+x^2$	1110
11	$1+x^3$	1001
12	x^3	0001
13	$1+x+x^3$	1101
14	$x+x^2+x^3$	0111

$K^* = K\backslash\{0\}$ becomes the multiplicative group of units of the field K. Now, let R^* be the multiplicative group of units of the Galois ring R. Then the maximal cyclic subgroup of R^*, isomorphic to the cyclic Galois group K^*, of order 15 is denoted by G_{15} and it is given in Table 3.

Followed by the construction algorithm 3.1 and using maximal cyclic subgroup of Table 3. We obtain S-box given in the Table 4.

3.4 S-box on $GR(\mathbb{Z}_8, 4)$

$\mathbb{Z}_8[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_8, n \in \mathbb{Z}^+\}$ is the polynomial ring with one indeterminate x and $<f(x)> = \{a(x).f(x) : a(x) \in \mathbb{Z}_8[x]\}$ is principal ideal generated by $f(x)$. Thus $R = (\mathbb{Z}_8[x])/(<f(x)>) = \{a_0 + a_1x + a_2x^2 + \cdots a_{(4-1)}x^{(4-1)} : a_i \in \mathbb{Z}_8\}$ is the Galois ring extension of order 4096 with corresponding Galois field extension $K = (\mathbb{Z}_2[x])/(<f(x)>)$ of order 16, whose elements are given in Table 1.

$K^* = K\backslash\{0\}$ becomes the multiplicative group of the field K. Now, let R^* be the multiplicative group of units of R. Then the cyclic subgroup of R^*, isomorphic to K^* , of order 15 is denoted by c and is given in Table 5.

Followed by the construction algorithm 3.1 and using maximal cyclic subgroup of Table 5, we obtain S-box given in the Table 6.

Table 2 S-box on $GF(2^4)$

0	11	12	6
3	8	4	2
1	9	13	15
14	7	10	5

Table 3 Elements of $G_{15} \cup \{0\}$ in $GR(4, 4)$

Exp	Polynomial	
$-\infty$	0	0000
0	1	1000
2	$1+2x+x^2$	1210
4	$3x+2x^2$	0320
6	$2+x+3x^3$	2103
8	x^2	0010
10	$3+3x+x^2+2x^3$	3312
12	$2+2x+3x^3$	2203
14	$x+3x^2+x^3$	0131
16	$3+3x$	3300
18	$3+x+x^2+3x^3$	3113
20	$x+3x^2+2x^3$	0132
22	$1+3x^2+x^3$	1031
24	$3x^2+3x^3$	0033
26	$3+x^3$	3001
28	$1+3x+2x^2+x^3$	1321

3.5 Nonexistence of S-box on $GR(\mathbb{Z}_{16}, 4)$

$\mathbb{Z}_{16}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_{16}, n \in \mathbb{Z}^+\}$is the polynomial ring with one indeterminate x and $<f(x)> = \{a(x).f(x) : a(x) \in \mathbb{Z}_{16}[x]\}$ is principal ideal generated by $f(x)$. Thus $R = (\mathbb{Z}_{16}[x])/(<f(x)>) = \{a_0 + a_1x + a_2x^2 + \cdots a_{(4-1)}x^{(4-1)} : a_i \in \mathbb{Z}_{16}\}$ is the Galois ring extension of order 65535 with corresponding Galois field extension $K = (\mathbb{Z}_2[x])/(<f(x)>)$ of order 16, whose elements are given in Table 1.

$K^* = K\backslash\{0\}$ becomes the multiplicative group of the field K. Now, let R^* be the multiplicative group of units of R. Then the cyclic subgroup of R^*, isomorphic to K^*, of order 15 is denoted by G_{15} and is given in Table 5.

Followed by the construction algorithm 3.1 and using maximal cyclic subgroup of Table 7, we obtain S-box given in the Table 8.

The structure in Table 8 is not an S-Box as repetition of 1 on two positions. So, this gives us a counter example that, not every maximal cyclic subgroup of the group of units of Galois ring extension generates an S-box.

3.6 S-box on $GR(\mathbb{Z}_{32}, 4)$

$\mathbb{Z}_{32}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_{32}, n \in \mathbb{Z}^+\}$ is the polynomial ring with one indeterminate x and $<f(x)> = \{a(x).f(x) : a(x) \in \mathbb{Z}_{32}[x]\}$ is principal ideal generated by $f(x)$. Thus $R = (\mathbb{Z}_{32}[x])/(<f(x)>) = \{a_0 + a_1x + a_2x^2 + \cdots a_{(h-1)}x^{(h-1)} : a_i \in \mathbb{Z}_{32}\}$ is the Galois ring

Table 4 S-box on $GR(4, 4)$

0	67	215	159
25	240	15	16
1	113	116	198
109	45	202	44

Table 5 Elements of $G_{15} \cup \{0\}$ in $GR(8, 4)$

Exp	Polynomial	
$-\infty$	0	0000
0	1	1000
2	$1+2x+x^2$	1210
4	$3x+6x^2+4x^3$	0364
6	$2+x+3x^3$	2103
8	$4+4x+x^2+4x^3$	4414
10	$3+7x+x^2+2x^3$	3712
12	$6+6x+3x^3$	6603
14	$x+7x^2+x^3$	0171
16	$7+7x$	7700
18	$7+5x+5x^2+7x^3$	7557
20	$4x+3x^2+3x^3$	4176
22	$1+7x^2+5x^3$	1075
24	$4x^2+3x^3+3x^3$	0433
26	$7+5x^3$	7005
28	$5+7x+2x^2+5x^3$	5725

extension of order 1048576 with corresponding Galois field extension $K = (\mathbb{Z}_2[x])/(<f(x)>)$ of order 16, whose elements are given in Table 1.

$K^* = K\backslash\{0\}$ becomes the multiplicative group the field K. Now, let R^* be the multiplicative group of units of R. Then the cyclic subgroup of R^*, isomorphic to K^* of order 15 is denoted by G_{15} and is given in Table 9.

Followed by the construction algorithm 3.1 and using maximal cyclic subgroup of Table 9, we obtain S-box given in the Table 10.

So, we are not certain if G_s of every Galois ring will generate an S-box for us. This implies that with a certain polynomial and Galois ring structure we are not sure if we will get an S-box over it or not. It shows that, the method discussed in [1] is not an efficient technique to get S-boxes for use in different applications. Even though these newly designed S-boxes are increasing encryption and decryption difficulty as compare to the S-boxes constructed over Galois field $GF(2, 4)$.

4 Basic primilanaries of finite chain ring of the type $\frac{F_2[u]}{<u^k>} = F_2 + uF_2 + u^2F_2 + \cdots + u^{k-1}F_2$

Let R be a ring. An element v is unit in R if there exists an element w in R such that $vw = 1$, where 1 is the identity of R. Unit elements of a ring form a multiplicative group. A non-zero element a is a zero divisor in R if there exists a non-zero element b in R such that $ab = 0$. A

Table 6 S-box on $GR(8, 4)$

0	3	111	123
81	224	63	100
1	193	200	10
189	195	60	152

Table 7 Elements of $G_{15} \cup \{0\}$ in *GR*(16,4)

Exp	Polynomial	
$-\infty$	0	0000
0	1	1000
2	$1+2x+x^2$	1210
4	$3x+6x^2+4x^3$	0364
6	$2+x+8x^2+3x^3$	2183
8	$4+4x+9x^2+4x^3$	4494
10	$3+7x+x^2+10x^3$	371*A*
12	$14+14x+8x^2+3x^3$	*EE*83
14	$9x+15x^2+x^3$	09*F*1
16	$15+7x+8x^3$	*F*708
18	$15+13x+5x^2+15x^3$	*FD*5*D*
20	$12x+9x^2+15x^2+6x^3$	*C*9*F*6
22	$1+7x^2+13x^3$	107*D*
24	$4x^2+11x^2+11x^3$	04*BB*
26	$15+8x+8x^2+5x^3$	*F*885
28	$13+15x+2x^2+13x^3$	*DF*2*D*

nonzero element a is said to be nilpotent element in R if there exists a positive integer k such that $a^k = 0$. The least positive integer k with this property is known as the nilpotency index a.

A ring R is local if and only if its all non-unit elements form an additive Abelian group. More unambiguously a local ring R has a unique maximal ideal M and the factor ring $\frac{R}{M}$ is its residue field.

A local finite ring R is a chain ring if and only if the radical M of R is a principal ideal (consists of all multiples of a fixed element of R, and this fixed element is called the generator of the ideal), and therefore the factor ring $\frac{\mathbf{R}}{\mathbf{M}}$ is a field. Thus ideals of a chain ring form a chain. The famous examples of such rings are $\mathbb{Z}_{p^n}[x]$ the ring of integers modulo p^n where p is prime, and the Galois field $GF(p^n) = \mathsf{F}_q$ with $q = p^n$ elements. Another large class of finite chain rings is the Galois rings $GR(p^n, r) = \frac{\mathsf{Z}_{p^n}[x]}{<f(x)>}$, where $f(x) \in \mathbb{Z}_{p^n}[x]$ is monic irreducible polynomial of degree r generates the principal ideal $<f(x)>$, however $f(x)$ is also irreducible modulo the prime p, i.e. $f(x)$ is the basic irreducible polynomial. Whereas the Galois ring $R = GR(p^n, r)$ has p^{nr} number of elements and an element $\bar{a}(x)$ in $GR(p^n, r)$ has the representation $\bar{a}_0 + \bar{a}_1 x + \ldots + \bar{a}_{r-1} x^{r-1}, \bar{a}_0, \bar{a}_1, \ldots, \bar{a}_{r-1} \in \mathbb{Z}_{p^n}$. The radical M is the set of nilpotent elements of R and the residue field $\frac{\mathbf{R}}{\mathbf{M}}$ of R is the Galois extension field $GF(p^r)$. One of the typical class of chain rings is the factor ring $\frac{GF(p^r)[x]}{<x^k>}$ of Euclidean domain $GF(p^r)[x]$. The finite chain ring $\frac{GF(p^r)[x]}{<x^k>} \left(= \frac{\mathsf{F}_{p^r}[x]}{<x^k>}\right)$ has the representation $\mathsf{F}_{p^r} + x\mathsf{F}_{p^r} + \cdots + x^{k-1}\mathsf{F}_{p^r}$.

Table 8 S-box on *GR*(16, 4)

0	143	223	115
33	64	127	68
1	1	144	18
253	156	238	48

Table 9 Elements of $G_{15} \cup \{0\}$ in $GR(32, 4)$

Exp	Polynomial	
$-\infty$	0	0000
0	1	1000
4	$3x+6x^2+4x^3$	0364
8	$4+20x+9x^2+20x^2$	4*K*9*K*
12	$30+14x+8x^2+19x^3$	*UE*8*J*
16	$31+7x+24x^3$	*V*700
20	$28+9x+31x^2+6x^3$	*S*9*V*6
24	$16+4x+11x^2+11x^3$	*G*4*BB*
28	$13+15x+18x^2+13x^3$	*DFID*
32	$17+2x+17x^2+16x^3$	*H*2*HG*
36	$2+17x+8x^2+3x^3$	2*H*83
40	$3+23x+x^2+26x^3$	2*N*1*Q*
44	$16+25x+15x^2+17x^3$	*GPFH*
48	$15+29x+5x^2+31x^3$	*FT*5*V*
52	$17+16x+7x^2+29x^3$	*HG*7*T*
56	$31+8x+24x^2+5x^3$	*V*8*O*5

Let R_k be the representation of finite chain ring $\frac{\mathsf{F}_2[u]}{<u^k>} = \mathsf{F}_2 + u\mathsf{F}_2 + u^2\mathsf{F}_2 + \cdots + u^{k-1}\mathsf{F}_2$. The ring R_k has 2^k number of elements. The element u is the nilpotent element with nilpotency index k (i.e., $u^k = 0$). Thus it follows that $<0> = u^k R_k \subset u^{k-1} R_k \subset \cdots \subset u^2 R_k \subset uR_k \subset R_k$ is the ascending chain of ideals in R_k and therefore R_k is a local ring with only maximal ideal uR_k. Whereas, $\frac{R_k}{uR_k} \simeq \mathsf{F}_2$ is the residue field of the chain ring R_k. The ideals $u^i R_k$ and $u^{i+1} R_k$, where $i =$ 0, 1, 2, $\cdots$, $k-1$, respectively have the cardinality 2^{k-i} and 2^{k-i+1}. Thus the cardinality of $u^i R_k$ is 2 times the cardinality of $u^{i+1} R_k$.

Amongst the rings of four elements, earlier the Galois field F_4 , and later the integers modulo 4 ring $\mathbb{Z}_4$, are frequently used in algebraic coding theory. Recently, Abualrub and Siap [2] studied cyclic codes of an arbitrary length n over the rings $\mathsf{F}_2 + u\mathsf{F}_2 = \{0, 1, u, \overline{u} = 1+u\}$, with $u^2 = 0$, and $\mathsf{F}_2 + u\mathsf{F}_2 + u^2\mathsf{F}_2 = \{0, 1, u, u^2, 1+u, 1+u^2, u+u^2, 1+u+u^2\}$, with $u^3 = 0$. However, Al-Ashker and Hamoudeh [7] extend these results to more general rings of the form $R_k = \mathsf{F}_2 + u\mathsf{F}_2 + \cdots + u_2^{k-1}\mathsf{F}_2$, with $u^k = 0$. The ring $\mathsf{F}_2 + u\mathsf{F}_2$ share some good properties of both $\mathbb{Z}_4$ and F_4. The alphabet in the ring $\mathsf{F}_2 + u\mathsf{F}_2$ is given to all binary polynomials in indeterminate u of degree at most 1, and is closed under binary polynomial addition and multiplication modulo u^2. The multiplication and addition tables for the ring $\mathsf{F}_2 + u\mathsf{F}_2$ are given in Table 11. The multiplication table of the ring $\mathsf{F}_2 + u\mathsf{F}_2$ coincides with that of $\mathbb{Z}_4$, when u and $\bar{u}$ are replaced by 2 and 3 respectively. In this sense $\mathsf{F}_2 + u\mathsf{F}_2$ is analogous to $\mathbb{Z}_4$ and here u plays the role of 2. Whereas the addition table is

Table 10 S-box on $GR(32, 4)$

0	17	34	60
96	175	81	255
1	48	237	222
31	227	144	132

Table 11 × and + Tables for $F_2 + uF_2$

×	0	1	u	$\bar{u}$	+	0	1	$\bar{u}$	u
0	0	0	0	0	0	0	1	$\bar{u}$	u
1	0	1	u	$\bar{u}$	1	1	0	u	$\bar{u}$
u	0	$\bar{u}$	1	u	$\bar{u}$	$\bar{u}$	u	0	1
$\bar{u}$	0	u	u	0	u	u	$\bar{u}$	1	0

different and is similar to that of the Galois field $\mathsf{F}_4 = \{0, 1, \beta, \beta^2 = 1 + \beta\}$, where $\bar{u}$ and u are replaced by β and β^2, respectively (Table 12).

5 Construction of S-box through finite chain rings $\mathsf{F}_2 + u\mathsf{F}_2 + \cdots + u^{k-1}\mathsf{F}_2$

The chain ring $R_k = \frac{\mathsf{F}_2[u]}{<u^k>} = \mathsf{F}_2 + u\mathsf{F}_2 + \ldots + u^{k-1}\mathsf{F}_2$ has cardinality 2^k. As u is a nilpotent element with nilpotency index k, it follows that $<0> = u^k R_k \subset u^{k-1} R_k \subset \ldots \subset uR_k \subset R_k$. Accordingly the residue field of R_k is $\frac{R_k}{uR_k} \simeq \mathsf{F}_2$. The ring R_k shares some properties of the local ring $\mathbb{Z}_{2^k}$ and the Galois field F_{2^k}. More explicitly the multiplication binary operation of R_k coincides with of $\mathbb{Z}_{2^k}$, whereas the addition binary operation is similar to that of F_{2^k}.

A significant S-box with wide-ranging cryptographic features is of ultimate worth for the development of resilient cryptographic system. Constructing cryptographically strong S-boxes is a basic challenge. In this study we propose a method to amalgam an efficient 4 × 4 S-box based on unit elements of the chain rings $\mathsf{F}_2 + u\mathsf{F}_2 + \cdots + u^{k-1}\mathsf{F}_2$. For the purpose we fix k to $2, 3, 4, 5, 6, 7$ and 8.

The 4 × 4 S-box construction steps are given bellow:

1) Table M_{G_k}, the multiplicative group of unit elements of the ring R_k.
2) If the cardinality of M_{G_k} is a perfect square and less than or equal to 16, define an inversion map $f : M_{G_k} \rightarrow M_{G_k}$ and a linear scalar multiple function $g : M_{G_k} \rightarrow M_{G_k}$. Otherwise choose a subgroup H_{G_k} of M_{G_k} of desired size 16 and then define these two bijective maps f and g from H_{G_k} to H_{G_k}. The selection of subgroups and defined maps for each ring are explicitly explained in subsections.
3) Take the composition of the maps f and g.
4) Generate 4 × 4 S-box by arranging them row wise.
5) Apply permutations S_n to each elements of S-box obtained in step 4 which result in $n!$ S-boxes.

Table 12 Elements in chain ring R_3

S. No.	Polynomial	Binary string	S. No.	Polynomial	Binary string
1	0	000	5	$1+u$	110
2	1	100	6	$1+u^2$	101
3	u	010	7	$u+u^2$	011
4	u^2	001	8	$1+u+u^2$	111

Table 13 Elements in $f \circ g(M_{g_3})$

S. No.	Polynomial
$f \circ g(2)$	111
$f \circ g(5)$	101
$f \circ g(6)$	110
$f \circ g(8)$	100

5.1 Construction of S-box through multiplicative group of R_3

The chain ring $R_3 = \frac{\mathsf{F}_2[u]}{<u^3>} = \mathsf{F}_2 + u\mathsf{F}_2 + u^2\mathsf{F}_2$ has 8 number of elements. The chain of ideals of this ring is $<0> = u^3R_3 \subset u^2R_3 \subset uR_3 \subset R_3$ and $\frac{R_3}{uR_3} \simeq \mathsf{F}_2$ is its residue field. The multiplication binary operation of R_3 coincides with of $\mathbb{Z}_8$, whereas the addition binary operation is similar to that of F_8.

The multiplicative group of unit elements of the ring R_3 is

$$M_{G_3} = 1,\ 1+u,\ 1+u^2,\ 1+u+u^2.$$

Define $f: M_{G_3} \to M_{G_3}$ by $f(a) = a^{-1}$ and $g: M_{G_3} \to M_{G_3}$ by $g(a) = a'a$, where $a' = 1+u$. Thus $f \circ g(a) = \left(a'a\right)^{-1}$.

5.2 Construction of S-box through multiplicative group of R_4

The chain ring $R_4 = \frac{\mathsf{F}_2[u]}{<u^4>} = \mathsf{F}_2 + u\mathsf{F}_2 + u^2\mathsf{F}_2 + u^3\mathsf{F}_2$ has 16 elements. Its chain of ideals is $<0> = u^4R_4 \subset u^3R_4 \subset u^2R_4 \subset uR_4 \subset R_4$, whereas the residue field of this ring is $\frac{R_4}{uR_4} \simeq \mathsf{F}_2$. The ring R_4 shares some properties of the local ring $\mathbb{Z}_{16}$ and the Galois field F_{16}. The multiplication and addition binary operations of R_4 coincides with $\mathbb{Z}_{16}$ and F_{16} respectively.

Multiplicative group of unit elements of the ring R_4 is

$$M_{G_4} = 1,\ 1+u,\ 1+u^2,\ 1+u^3,\ 1+u+u^2,\ 1+u+u^3,\ 1+u^2+u^3,\ 1+u+u^2+u^3.$$

Take a subgroup $H_{G_4} = \{1,\ 1+u,\ 1+u^2,\ 1+u+u^2+u^3\}$ of index 2 of the group M_{G_4} and apply given procedure on subgroup rather than group M_{G_4}. Define $f: H_{G_4} \to H_{G_4}$ by $f(a) = a^{-1}$ and $g: H_{G_4} \to H_{G_4}$ by $g(a) = a'a$, where $a' = 1+u, f \circ g(a) = \left(a'a\right)^{-1}$. The following Table 16 is of $f \circ g(H_{G_4})$ in binary and decimal form, which is in fact the S-box constructed over the chain ring $R_4 = \mathsf{F}_2 + u\mathsf{F}_2 + u^2\mathsf{F}_2 + u^3\mathsf{F}_2$.

5.3 Construction of S-box through multiplicative group of R_5

The chain ring $R_5 = \frac{\mathsf{F}_2[u]}{<u^5>} = \mathsf{F}_2 + u\mathsf{F}_2 + +u^2\mathsf{F}_2 + u^3\mathsf{F}_2 + u^4\mathsf{F}_2$ has 32 number of elements. The chain of ideals is, $<0> = u^5R_5 \subset u^4R_5 \subset u^3R_5 \subset u^2R_5 \subset uR_5 \subset R_5$ and its residue field is $\frac{R_5}{uR_5} \simeq$

Table 14 S - box over $R_3 = \mathrm{F}_2 + u\mathrm{F}_2 + u^2\mathrm{F}_2$

7	5	6	4

Table 15 Elements in chain ring R_4

S. No.	Polynomial	Binary string	S. No.	Polynomial	Binary string
1	0	0000	9	$u+u^2$	0110
2	1	1000	10	$u+u^3$	0101
3	u	0100	11	u^2+u^3	0011
4	u^2	0010	12	$1+u+u^2$	1110
5	u^3	0001	13	$1+u+u^3$	1101
6	$1+u$	1100	14	$1+u^2+u^3$	1011
7	$1+u^2$	1010	15	$u+u^2+u^3$	0111
8	$1+u^3$	1001	16	$1+u+u^2+u^3$	1111

F_2. The multiplication binary operation of R_5 coincides with of $\mathbb{Z}_{2^5}$, whereas the addition binary operation is similar to that of F_{2^5}.

Multiplicative group of unit elements of the ring R_5 is

$$M_{G_5}=\left\{\begin{array}{c}1,\,1+u,\,1+u^2,\,1+u^3,\,1+u^4,\,1+u+u^2,\,1+u+u^3,\,1+u+u^4,\,1+u^2+u^3,\\ 1+u^2+u^4,\,1+u^3+u^4,\,1+u+u^2+u^3,\,1+u+u^2+u^4,\,1+u+u^3+u^4,\\ 1+u^2+u^3+u^4,\,1+u+u^2+u^3+u^4\end{array}\right\}.$$

Define $f:M_{G_5}\rightarrow M_{G_5}$ by $f(a)=a^{-1}$ and $g:M_{G_5}\rightarrow M_{G_5}$ by $g(a)=a'a$, where $a'=1+u$. Thus $(f\circ g)(a)=(a'a)^{-1}$.

The following Table 17 is of $f\circ g(H_{G_5})$ in binary and decimal form, which is in fact the S-box constructed over the chain ring $R_5=\mathsf{F}_2+u\mathsf{F}_2++u^2\mathsf{F}_2+u^3\mathsf{F}_2+u^4\mathsf{F}_2$.

5.4 Construction of S-box through multiplicative group of R_6

The chain ring $R_6=\mathsf{F}_2[u]/<u^6>=\mathsf{F}_2+u\mathsf{F}_2++u^2\mathsf{F}_2+u^3\mathsf{F}_2+u^4\mathsf{F}_2+u^5\mathsf{F}_2$ has cardinality 64. As u is a nilpotent element with nilpotency index 6 , it follows that $<0>=u^6R_6\subset u^5R_6\subset u^4R_6\subset u^3R_6\subset u^2R_6\subset uR_6\subset R_6$ and the residue field of R_6 is $\frac{R_6}{uR_6}\simeq\mathsf{F}_2$. The addition and multiplication binary operation of R_6 coincides with F_{2^6} and $\mathbb{Z}_{2^6}$ respectively.

Multiplicative group of the ring R_6 is

$$M_{G_6}=\left\{\begin{array}{c}1,\,1+u,\,1+u^2,\,1+u^3,\,1+u^4,\,1+u^5,\,1+u+u^2,\,1+u+u^3,\,1+u+u^4,\,1+u+u^5,\\ 1+u^2+u^3,\,1+u^2+u^4,\,1+u^2+u^5,\,1+u^3+u^4,\,1+u^3+u^5,\,1+u^4+u^5,\,1+u+u^2+u^3,\\ 1+u+u^2+u^4,\,1+u+u^2+u^5,\,1+u+u^3+u^4,\,1+u+u^3+u^5,\,1+u+u^4+u^5,\\ 1+u^2+u^3+u^4,\,1+u^2+u^3+u^5,\,1+u+u^2+u^3+u^4,\,1+u+u^2+u^3+u^5,\,1+u+u^2+\\ u^4+u^5,\,1+u+u^3+u^4+u^5,\,1+u^2+u^3+u^4+u^5,\,1+u+u^2+u^3+u^4+u^5\end{array}\right\}$$

The multiplicative subgroup M_{G_6} contains 32 elements, sixteen elements of order 8, 8 elements of order 4, 7 elements of order 2, and one element of order 1. Since our interest is in the subgroups of cardinality 16, so we combine these cyclic subgroups in such a way that they generate subgroups of order 16. We take subgroups $H_{G_6}=\langle 1+u^2,1+u^3+u^4,1+u^3+u^5\rangle$ of cardinality 16 of the multiplicative group M_{G_6}. Define the maps $f:H_{G_6}\rightarrow H_{G_6}$ by $f(a)=a^{-1}$

Table 16 S - box over R_4

15	10	12	8

Table 17 S-box over R_5

31	30	26	19
21	18	24	23
25	22	29	27
28	20	17	16

and $g : H_{G_6} \rightarrow H_{G_6}$ by $g(a) = a'a$, where $a' = 1 + u^4$. Thus, $(g \circ f)(a) = \left(a' a\right)^{-1}$. The following Table 18 is of $f \circ g(H_{G_6})$ in binary and decimal form, which is in fact the S-box designed over the chain ring R_6.

5.5 Construction of S-box through multiplicative group of R_7

The size of chain ring $R_7 = \frac{\mathsf{F}_2[u]/}{<u^7>} = \mathsf{F}_2 + u\mathsf{F}_2 + +u^2\mathsf{F}_2 + u^3\mathsf{F}_2 + u^4\mathsf{F}_2 + u^5\mathsf{F}_2 + u^6\mathsf{F}_2$ is 128. The chain of ideals is $<0> = u^7R_7 \subset u^6R_7 \subset u^5R_7 \subset u^4R_7 \subset u^3R_7 \subset u^2R_7 \subset uR_7 \subset R_7$. Accordingly the residue field of R_7 is $\frac{R_7}{uR_7} \simeq \mathsf{F}_2$. The ring R_7 shares some properties of the local ring $\mathbb{Z}_{2^7}$ and the Galois field F_{2^7}. The multiplicative subgroup M_{G_7} contains 64 elements, with 32 elements of order 8, 24 elements of order 4, 7 elements of order 2 and 1 element of order 1. Since we require the subgroups of size 16 , it follows that we can fulfill our requirement by above explained availability for M_{G_7}. For this purpose we choose a subgroup $H_{G_7} = \langle 1 + u^3, 1 + u^2 + u^3 \rangle$ of cardinality 16 of the multiplicative group M_{G_7}.

Define the maps $f : H_{G_7} \rightarrow H_{G_7}$ by $f(a) = a^{-1}$ and $g : H_{G_7} \rightarrow H_{G_7}$ by $g(a) = a'a$, where $a' = 1 + u^3$. Thus, $(g \circ f)(a) = (a'a)^{-1}$. The following Table 19 is of $f \circ g(H_{G_7})$ in decimal form, which is in fact the S-box constructed over the chain ring $R_7 = \mathsf{F}_2 + u\mathsf{F}_2 + +u^2\mathsf{F}_2 + u^3\mathsf{F}_2 + u^4\mathsf{F}_2 + u^5\mathsf{F}_2 + u^6\mathsf{F}_2$.

5.6 Construction of S-box through multiplicative group of R_8

The ring $R_8 = \frac{\mathsf{F}_2[u]}{<u^8>} = \mathsf{F}_2 + u\mathsf{F}_2 + +u^2\mathsf{F}_2 + u^3\mathsf{F}_2 + u^4\mathsf{F}_2 + u^5\mathsf{F}_2 + u^6\mathsf{F}_2 + u^7\mathsf{F}_2$ is a commutative chain ring of 2^8 elements. Since u is nilpotent with nilpotency index 8, it follows that $<0> = u^8R_8 \subset u^7R_8 \subset u^6R_8 \subset u^5R_8 \subset u^4R_8 \subset u^3R_8 \subset u^2R_8 \subset uR_8 \subset R_8$ and $\frac{R_8}{uR_8} \simeq \mathsf{F}_2$ is the residue field of R_8. The ring R_8 shares some properties of the local ring $\mathbb{Z}_{2^8}$ and the Galois field F_{2^8}. The multiplication binary operation of R_8 coincides with of $\mathbb{Z}_{2^8}$, whereas the addition binary operation is similar to that of F_{2^8}. We choose a subgroup $H_{G_8} = \langle 1 + u^3 + u^6, 1 + u^2 + u^4 + u^5 + u^7 \rangle$ of the group M_{G_8} having cardinality 16. Define the maps $f : H_{G_8} \rightarrow H_{G_8}$ by $f(a) = a^{-1}$ and $g : H_{G_8} \rightarrow H_{G_8}$ by $g(a) = a'a$, where we take $a' = 1 + u^4 + u^6$. Thus, $(g \circ f)(a) = (a'a)^{-1}$. The following Table 20 is of $f \circ g(H_{G_8})$ in decimal form, which is in fact the S-box designed over the chain ring $R_8 = \mathsf{F}_2 + u\mathsf{F}_2 + +u^2\mathsf{F}_2 + u^3\mathsf{F}_2 + u^4\mathsf{F}_2 + u^5\mathsf{F}_2 + u^6\mathsf{F}_2 + u^7\mathsf{F}_2$.

Table 18 S-box over R_6

34	40	42	36
39	33	47	44
43	38	37	35
45	46	41	32

Table 19 S-box over R_7

73	65	64	72
86	77	82	69
93	89	87	76
83	92	76	88

6 Applications of proposed substitution box in image encryption and watermarking

As digital image plays an important role in multimedia technology, it becomes more important for the user's to maintain privacy. And to provide such security and privacy to the user, encryption and watermarking is very important to protect from any unauthorized user access. The encryption and watermarking have applications in various fields, including internet communication, multimedia systems, medical imaging, Telemedicine and military communication. Nowadays, the prominent share of the multimedia fabrication and dissemination is carried out digitally. The rapid growth of digital media like Internet and Compact Discs has ushered in a wonderful era where the flow, duplication and modification of digital images have become all the more easier and simpler. Mega distribution of flawless replicas of multimedia data at an accelerated degree has become the order of the day. And this phenomenon has unfortunately resulted in tremendous threats to multimedia safety and copyright security. This has the effect of ringing an alarm bell for authors, when the stark reality dawned upon them, convincing that conservative safety systems, like encryption were incapable of affording the much-needed shelter. This has motivated many investigators to devise alternate methods, one of which is known by the term 'digital watermarking' which is nothing but the art of concealing data in a healthy way and without being noticed by pirates or others of the sort [29]. The classifications of information hiding techniques are cryptography, watermarking and steganography. Here we will only focus on encryption that belongs to cryptography and watermarking. Encryption protects content during the transmission of the data from the sender to receiver. However, after receipt and subsequent decoding, the data is no longer protected and is in the clear. Watermarking compliments encryption by embedding a signal directly into the data. Thus, the goal of a watermarking is to always remain present in the data. The algorithms for image encryption and watermarking schemes are presented in Figs. 1 and 2.

The results after applying the proposed image encryption and watermarking schemes are given in Figs. 3, 4, 5 and 6 respectively.

The statistical analysis plays an important role in estimating good quality information hiding. We have applies first order texture image analysis that deals with the histograms of an image which includes mean, standard deviation (Std.), skewness and kurtosis [27]. The GLCM (Gray-Level Co-Occurrence Matrix) analysis of an image consists of entropy, contrast, homogeneity, energy and correlation [15]. The correlation based statistical analyses consists of structure content, normalized cross correlation. The human visual system (HVS) fundamentally deals with the human perceptions. These analyses include universal image quality index, structure content and structure similarity index metric.

Table 20 S-box over R_8

138	153	130	136
155	175	165	186
146	177	128	173
167	184	143	179

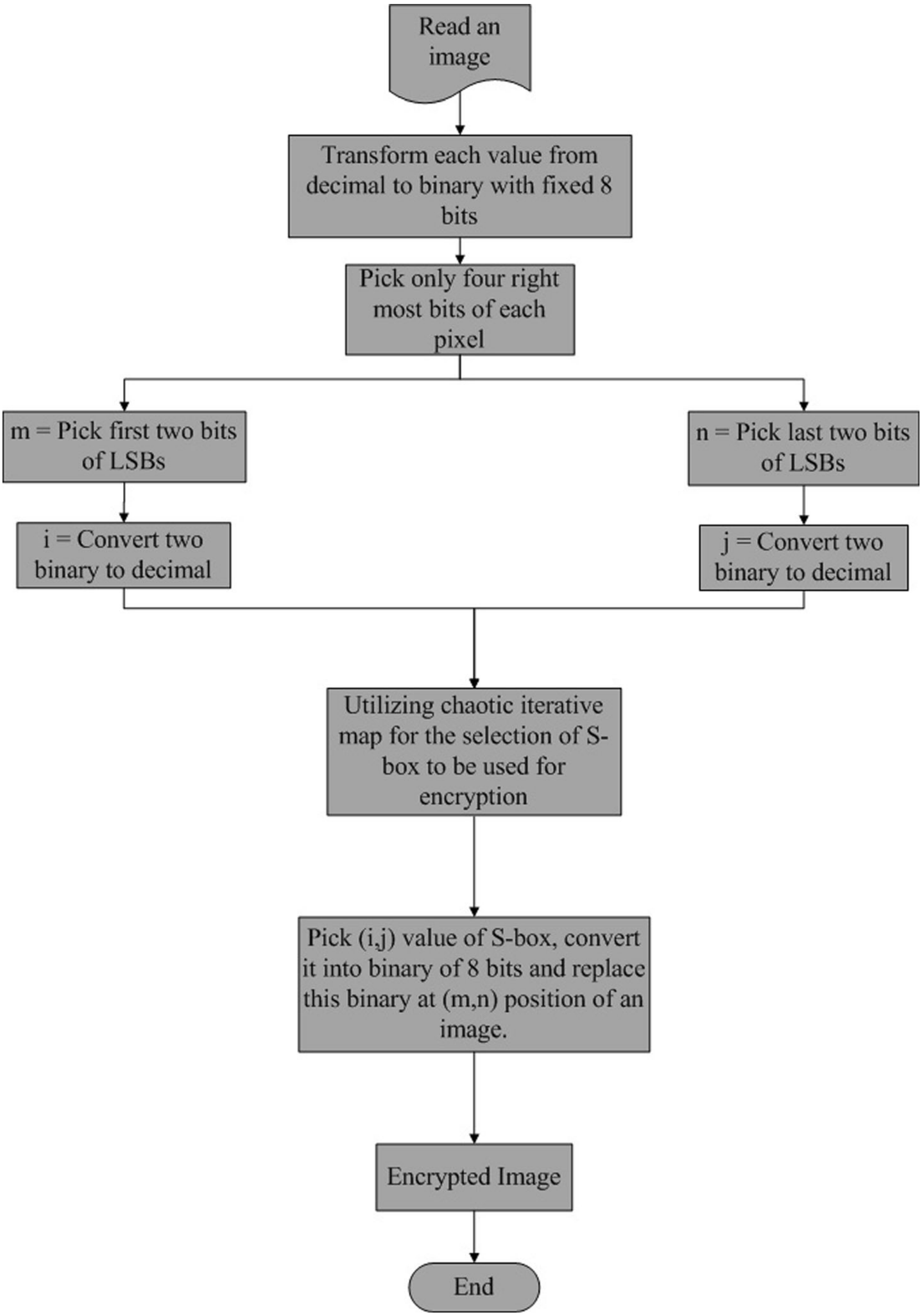


Fig. 1 Proposed image encryption algorithmbased on Galois ring

First-order statistics are quite straightforward. They are computed from a function that measures the probability of a certain pixel occurring in an image. The interpretations of first order texture analysis of an image are quite straightforward. They are computed from the

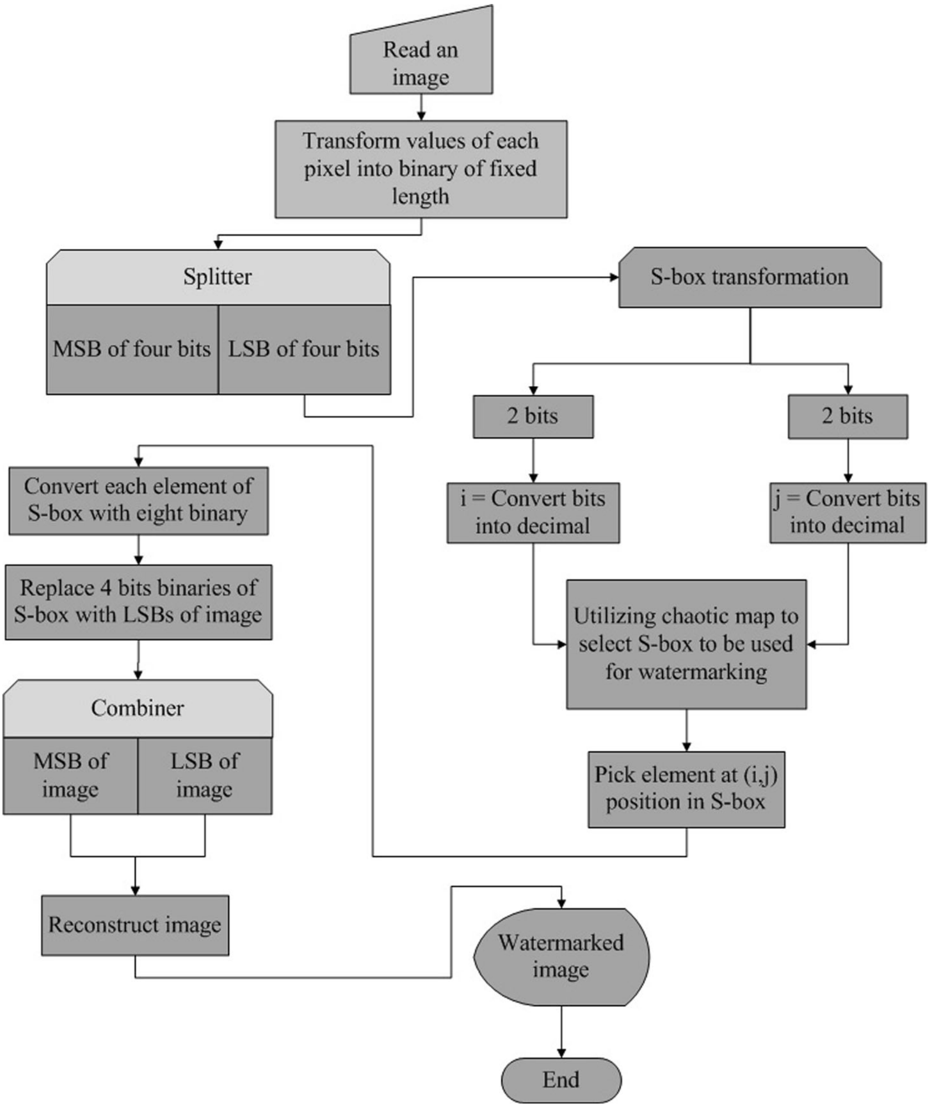


Fig. 2 Algorithm for image watermarking based on Galois ring

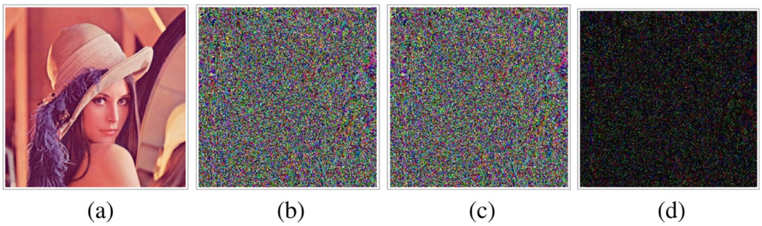
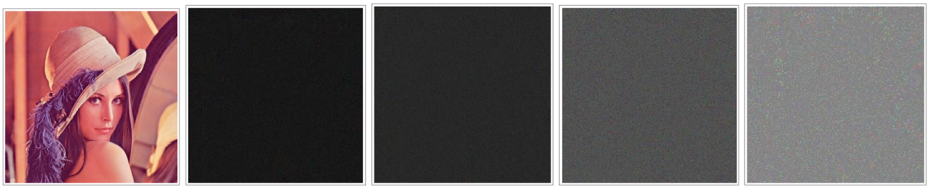


Fig. 3 (**a**) Plain Lena image, (**b**) Encrypted image using GR(4,4), (**c**) Encrypted image using GR(8,4), (**d**) Encrypted image using GR(32,4)



(a) (b) (c) (d) (e)

Fig. 4 (**a**) Plain Lena image, (**b**) Encrypted image using R_5, (**c**) Encrypted image using R_6, (**d**) Encrypted image using R_7, (**e**) Encrypted image using R_8

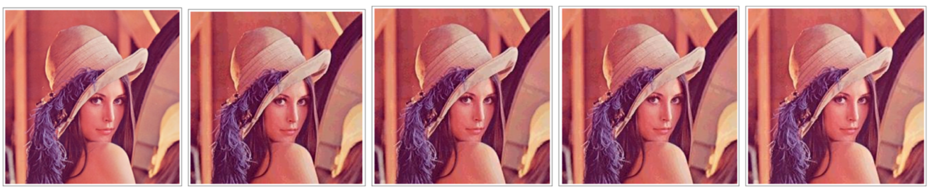
(a) (b) (c) (d)

Fig. 5 (**a**) Cover Lena image, (**b**) Watermarked image using GR(4,4), (**c**) Watermarked image using GR(8,4), (**d**) Watermarked image using GR(32,4)

mechanism which measures the pixel probabilities in an image. The analysis of first order textures like mean, standard deviation, skewness and kurtosis reflects that there are significant changes in these features for plain and encrypted images in case of Galois rings and finite chain rings (see Tables 21, 22, 23, 24, 25, 26 and 27) whereas in the case of watermarking these parameter values will remain constant with some minute changes for original and watermarked images (see Tables 56, 57, 58, 59, 60, 61 and 62).

The second order texture analysis generally deals with contrast, homogeneity, entropy, correlation and energy. The contrast measures the amount of local variations present in the image. Contrast is zero when the neighboring pixels have constant values. The values second order characteristics for plain and encrypted images are different from each other and for watermarking through Galois rings and finite chain rings are remain same or tend to cover image second order texture features (see Tables 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72 and 73).

The image error measurements and image similarity analysis in case of image encryption and watermarking are quite different. The values of the means square error and mean absolute error increases, whereas peak signal to noise ratio decreases for image encryption. As far as



(a) (b) (c) (d) (e)

Fig. 6 (**a**) Cover Lena image, (**b**) Watermarked image using R_5, (**c**) Watermarked image using R_6, (**d**) Watermarked image using R_7, (**e**) Watermarked image using R_8

Table 21 First order texture analysis of proposed encryption scheme based on S-box of *GR(4,4)*

	Plain image color components			Encrypted image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.300781	0.355469	0.292969
Std.	0.496541	0.459496	0.38138	0.459496	0.479593	0.456016
Skewness	−0.267999	0.868817	1.703557	0.868817	0.603906	0.909779
Kurtosis	1.07182	1.75484	3.90216	1.754840	1.364700	1.827700

Table 22 First order texture analysis of proposed encryption scheme based on S-box of *GR(8,4)*

	Plain image color components			Encrypted image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.261719	0.210938	0.183594
Std.	0.496541	0.459496	0.38138	0.440431	0.408773	0.387911
Skewness	−0.267999	0.868817	1.703557	1.084160	1.417060	1.634530
Kurtosis	1.07182	1.75484	3.90216	2.173900	3.008070	3.671690

watermarking is concerned, these analyses are entirely changed (Table 41). The value of mean square error and mean absolute error decreases, and peak signal to noise ratio decreases (see Tables 42, 43, 44, 45, 46, 47, 48, 70, 71, 72, 73, 74, 75 and 76).

The structural similarity image quality standard is grounded on the notion that the human visual system is extremely modified for extracting structural information from the scene, and therefore a measure of structural similarity can provide a good approximation to perceived image quality. The standard similarity measurement tests which include structure content, universal image quality index and structure similarity index metric (SSIM). The similarity coefficients values for image encryption and watermarking are computed (see Tables 49, 50, 51, 52, 53, 54, 55, 77, 78, 79, 80, 81, 82 and 83). The readings of similarity measures discloses the quality of encryption using proposed algorithms for image encryption, which is based on chain rings. The structure content values in case of image encryption are higher than unity which reveals that two images are completely different. Similarly, structure similarity index and universal image quality index measure far away from unity backwardly which guarantee the authentication of the proposed image encryption algorithm. In case of watermarking

Table 23 First order texture analysis of proposed encryption scheme based on S-box of *GR(32,4)*

	Plain image color components			Encrypted image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.101563	0.136719	0.078125
Std.	0.496541	0.459496	0.38138	0.302664	0.344223	0.268894
Skewness	−0.267999	0.868817	1.703557	2.638030	2.114870	3.144000
Kurtosis	1.07182	1.75484	3.90216	7.959200	5.472660	10.884700

Table 24 First order texture analysis of proposed encryption scheme based on S-box of R_5

	Plain image color components			Encrypted image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.578125	0.5156250	0.382813
Std.	0.496541	0.459496	0.38138	0.494826	0.5007350	0.487025
Skewness	−0.267999	0.868817	1.70357	−0.316386	−0.0625305	0.482181
Kurtosis	1.071820	1.754840	3.90216	1.100100	1.0039100	1.232500

Table 25 First order texture analysis of proposed encryption scheme based on S-box of R_6

	Plain image color components			Encrypted image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.628906	0.636719	0.597656
Std.	0.496541	0.459496	0.381380	0.484044	0.481887	0.491331
Skewness	−0.267999	0.868817	1.70357	−0.533666	−0.568542	−0.398296
Kurtosis	1.071820	1.754840	3.90216	1.284800	1.323240	1.15864

Table 26 First order texture analysis of proposed encryption scheme based on S-box of R_7

	Plain image color components			Encrypted image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.421875	0.613281	0.558594
Std.	0.496541	0.459496	0.38138	0.496541	0.487952	0.497528
Skewness	−0.267999	0.868817	1.703557	0.316386	−0.465222	−0.236001
Kurtosis	1.07182	1.75484	3.90216	1.100100	1.216430	1.055700

Table 27 First order texture analysis of proposed encryption scheme based on S-box of R_8

	Plain image color components			Encrypted image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.5090600	0.4648440	0.4960940
Std.	0.496541	0.459496	0.38138	0.5009640	0.4997400	0.5009640
Skewness	−0.267999	0.868817	1.703557	−0.0156255	0.1400974	0.0156255
Kurtosis	1.07182	1.75484	3.90216	1.0002400	1.0198700	1.0002400

Table 28 Second order texture analysis of proposed encryption scheme based on S-box of *GR(4,4)*

	Plain image color components			Encrypted image color components			
	Red	Green	Blue	Red	Green	Blue	Average
Contrast	0.3726	0.3928	0.3652	5.7166	5.9307	5.6531	5.7668
Homogeneity	0.8724	0.8712	0.8749	0.4631	0.4600	0.4637	0.4623
Entropy	7.2911	7.581	7.0794	7.7240	7.7433	7.6947	7.7207
Correlation	0.9234	0.9294	0.8538	0.07963	0.08541	0.0696	0.0782
Energy	0.1386	0.0999	0.1698	0.02470	0.02421	0.0250	0.0246

Table 29 Comparison of second order texture analysis of proposed encryption scheme based on S-box of *GR(4,4)* with some existing algorithm

	Encrypted image color components				
	Red	Green	Blue	Average	AES [9]
Contrast	5.7166	5.9307	5.6531	5.7668	7.2240
Homogeneity	0.4631	0.4600	0.4637	0.4623	0.4701
Entropy	7.7240	7.7433	7.6947	7.7207	7.9325
Correlation	0.07963	0.08541	0.0696	0.0782	0.0815
Energy	0.02470	0.02421	0.0250	0.0246	0.0211

Table 30 Second order texture analysis of proposed encryption scheme based on S-box of *GR(8,4)*

	Plain image color components			Encrypted image color components			
	Red	Green	Blue	Red	Green	Blue	Average
Contrast	0.3726	0.3928	0.3652	7.3449	7.5510	7.2945	7.3968
Homogeneity	0.8724	0.8712	0.8749	0.5238	0.5245	0.5214	0.5232
Entropy	7.2911	7.581	7.0794	7.5132	7.7389	7.0996	7.4505
Correlation	0.9234	0.9294	0.8538	0.0394	0.0450	0.0250	0.0365
Energy	0.1386	0.0999	0.1698	0.0536	0.0600	0.0509	0.0548

Table 31 Comparison of second order texture analysis of proposed encryption scheme based on S-box of *GR(8,4)* with some existing algorithm

	Encrypted image color components				
	Red	Green	Blue	Average	AES [9]
Contrast	7.3449	7.5510	7.2945	7.3968	7.2240
Homogeneity	0.5238	0.5245	0.5214	0.5232	0.4701
Entropy	7.5132	7.7389	7.0996	7.4505	7.9325
Correlation	0.0394	0.0450	0.0250	0.0365	0.0815
Energy	0.0536	0.0600	0.0509	0.0548	0.0211

Table 32 Second order texture analysis of proposed encryption scheme based on S-box of *GR(32,4)*

	Plain image color components			Encrypted image color components			
	Red	Green	Blue	Red	Green	Blue	Average
Contrast	0.3726	0.3928	0.3652	7.0918	7.1035	7.0795	7.0916
Homogeneity	0.8724	0.8712	0.8749	0.7429	0.7548	0.7410	0.7432
Entropy	7.29110	7.5813	7.0794	7.4161	7.5139	7.1015	7.343
Correlation	0.9234	0.9294	0.8538	0.0266	0.0259	0.0161	0.0228
Energy	0.1386	0.0999	0.1698	0.2835	0.3203	0.2781	0.2940

Table 33 Comparison of second order texture analysis of proposed encryption scheme based on S-box of *GR(32,4)* with some existing algorithm

	Encrypted image color components				
	Red	Green	Blue	Average	AES [9]
Contrast	7.0918	7.1035	7.0795	7.0916	7.2240
Homogeneity	0.7429	0.7548	0.7410	0.7432	0.4701
Entropy	7.4161	7.5139	7.1015	7.343	7.9325
Correlation	0.0266	0.0259	0.0161	0.0228	0.0815
Energy	0.2835	0.3203	0.2781	0.2940	0.0211

Table 34 Second order texture analysis of proposed encryption scheme based on S-box of R_5

	Plain image color components			Encrypted image color components			
	Red	Green	Blue	Red	Green	Blue	Average
Contrast	0.3726	0.3928	0.3652	7.0020	7.0009	7.0024	7.0018
Homogeneity	0.8724	0.8712	0.8749	0.4689	0.4695	0.4687	0.4690
Entropy	7.29110	7.5813	7.0794	7.3541	7.7091	7.0996	7.3866
Correlation	0.9234	0.9294	0.8538	0.1918	0.0323	0.2743	0.1661
Energy	0.1386	0.0999	0.1698	0.0254	0.0281	0.0240	0.0258

Table 35 Second order texture analysis of proposed encryption scheme based on S-box of R_1 with some well known algorithm

	Encrypted image color components				
	Red	Green	Blue	Average	AES [9]
Contrast	7.0020	7.0009	7.0024	7.0018	7.2240
Homogeneity	0.4689	0.4695	0.4687	0.4690	0.4701
Entropy	7.3541	7.7091	7.0996	7.3866	7.9325
Correlation	0.1918	0.0323	0.2743	0.1661	0.0815
Energy	0.0254	0.0281	0.0240	0.0258	0.0211

Table 36 Second order texture analysis of proposed encryption scheme based on S-box of R_6

	Plain image color components			Encrypted image color components			
	Red	Green	Blue	Red	Green	Blue	Average
Contrast	0.3726	0.3928	0.3652	7.0006	7.0005	7.000781	7.0006
Homogeneity	0.8724	0.8712	0.8749	0.4696	0.4797	0.459609	0.4696
Entropy	7.29110	7.5813	7.0794	7.4561	7.7813	7.351237	7.5295
Correlation	0.9234	0.9294	0.8538	−0.0003	0.0510	0.037352	0.0293
Energy	0.1386	0.0999	0.1698	0.01987	0.0188	0.021408	0.0200

Table 37 Comparison of second order texture analysis of proposed encryption scheme based on S-box of R_6 with some well known algorithm

	Encrypted image color components				
	Red	Green	Blue	Average	AES [9]
Contrast	7.0006	7.0005	7.000781	7.0006	7.2240
Homogeneity	0.4696	0.4797	0.459609	0.4696	0.4701
Entropy	7.4561	7.7813	7.351237	7.5295	7.9325
Correlation	−0.0003	0.0510	0.037352	0.0293	0.0815
Energy	0.01987	0.0188	0.021408	0.0200	0.0211

Table 38 Second order texture analysis of proposed encryption scheme based on S-box of R_7

	Plain image color components			Encrypted image color components			
	Red	Green	Blue	Red	Green	Blue	Average
Contrast	0.3726	0.3928	0.3652	7.0102	7.0087	7.0108	7.0099
Homogeneity	0.8724	0.8712	0.8749	0.4849	0.4856	0.4846	0.4850
Entropy	7.29110	7.5813	7.0794	7.5132	7.7389	7.0996	7.4505
Correlation	0.9234	0.9294	0.8538	0.0220	0.0091	0.0337	0.0216
Energy	0.1386	0.0999	0.1698	0.0255	0.0232	0.0208	0.0240

Table 39 Comparison of second order texture analysis of proposed encryption scheme based on S-box of R_7 with some well known algorithm

	Encrypted image color components				
	Red	Green	Blue	Average	AES [9]
Contrast	7.0102	7.0087	7.0108	7.0099	7.2240
Homogeneity	0.4849	0.4856	0.4846	0.4850	0.4701
Entropy	7.5132	7.7389	7.0996	7.4505	7.9325
Correlation	0.0220	0.0091	0.0337	0.0216	0.0815
Energy	0.0255	0.0232	0.0208	0.0240	0.0211

Table 40 Second order texture analysis of proposed encryption scheme based on S-box of R_8

	Plain image color components			Encrypted image color components			
	Red	Green	Blue	Red	Green	Blue	Average
Contrast	0.3726	0.3928	0.3652	7.6206	7.6027	7.6198	7.6143
Homogeneity	0.8724	0.8712	0.8749	0.4393	0.4526	0.4789	0.4569
Entropy	7.29110	7.5813	7.0794	7.0468	7.0203	7.0441	7.0371
Correlation	0.9234	0.9294	0.8538	0.0572	0.0437	0.0580	0.0530
Energy	0.1386	0.0999	0.1698	0.0202	0.0256	0.0200	0.0219

Table 41 Comparison of second order texture analysis of proposed encryption scheme based on S-box of R_8

	Encrypted image color components				
	Red	Green	Blue	Average	AES [9]
Contrast	7.6206	7.6027	7.6198	7.6143	7.2240
Homogeneity	0.4393	0.4526	0.4789	0.4569	0.4701
Entropy	7.0468	7.0203	7.0441	7.0371	7.9325
Correlation	0.0572	0.0437	0.0580	0.0530	0.0815
Energy	0.0202	0.0256	0.0200	0.0219	0.0211

Table 42 Image error measurements of proposed encryption scheme based on S-box of *GR(4,4)*

	Image color components						
	Red	Green	Blue	Average	Gray [9]	APA [9]	Lui [9]
Mean square error	12134.3	6068.13	4437.92				
Peak signal to noise ratio	7.29067	10.3003	11.6590	9.74999	8.1421	9.0014	9.2541
Mean absolute error	93.3373	63.2998	54.0589				

Table 43 Image error measurements of proposed encryption scheme based on S-box of *GR(8,4)*

	Image color components						
	Red	Green	Blue	Average	Gray [9]	APA [9]	Lui [9]
Mean square error	19007.1	6839.19	5523.35	–			
Peak signal to noise ratio	5.37564	9.81475	10.7428	8.64439	8.1421	9.0014	9.2541
Mean absolute error	122.514	67.7453	61.6997				

Table 44 Image error measurements of proposed encryption scheme based on S-box of *GR(32,4)*

	Image color components						
	Red	Green	Blue	Average	Gray [9]	APA [9]	Lui [9]
Mean square error	26869.2	8949.01	8245.61	–			
Peak signal to noise ratio	8.83825	8.61305	8.96858	7.13996	8.1421	9.0014	9.2541
Mean absolute error	154.441	79.2899	80.9500				

Table 45 Image error measurements of proposed encryption scheme based on S-box of R_5

	Image color components						
	Red	Green	Blue	Average	Gray [9]	APA [9]	Lui [9]
Mean square error	26938.7	8395.85	7914.18	–			
Peak signal to noise ratio	8.62704	8.89119	9.14675	8.80662	8.1421	9.0014	9.2541
Mean absolute error	156.614	76.4777	81.7981				

Table 46 Image error measurements of proposed encryption scheme based on S-box of R_6

	Image color components						
	Red	Green	Blue	Average	Gray [9]	APA [9]	Lui [9]
Mean square error	22211.3	6234.6	5573.56	–			
Peak signal to noise ratio	4.66506	10.1827	10.6695	8.50575	8.1421	9.0014	9.2541
Mean absolute error	140.6860	64.5333	66.0316				

Table 47 Image error measurments of proposed encryption scheme based on S-box of R_7

	Image color components						
	Red	Green	Blue	Average	Gray [9]	APA [9]	Lui [9]
Mean square error	12225.6	3037.64	1838.02	–			
Peak signal to noise ratio	7.2581	13.3054	15.4873	12.0169	8.1421	9.0014	9.2541
Mean absolute error	99.2633	45.0841	32.8454				

Table 48 Image error measurments of proposed encryption scheme based on S-box of R_8

	Image color components						
	Red	Green	Blue	Average	Gray [9]	APA [9]	Lui [9]
Mean square error	3269.08	6173.97	4007.07	–			
Peak signal to noise ratio	12.9866	10.2252	12.1025	11.7814	8.1421	9.0014	9.2541
Mean absolute error	50.4345	66.0888	55.0974				

Table 49 Image similarity measurements of proposed encryption scheme based on S-box of *GR(4,4)*

	Image color components		
	Red	Green	Blue
Structure content	2.67522000	0.959737000	0.9467440
Universal image quality index	−0.00329472	0.000386892	−0.0000435
Structure similarity index metric	0.013055400	0.016328500	0.0184890

Table 50 Image similarity measurements of proposed encryption scheme based on S-box of *GR(8,4)*

	Image color components		
	Red	Green	Blue
Structure content	5.5605800	2.01720000	1.96540000
Universal image quality index	−0.0016198	−0.00399473	−0.00170602
Structure similarity index metric	0.0130455	0.01506070	0.019223800

Table 51 Image similarity measurements of proposed encryption scheme based on S-box of *GR(32,4)*

	Image color components		
	Red	Green	Blue
Structure content	25.7971000	9.660140000	9.28556
Universal image quality index	0.000360266	0.000617253	−0.000210373
Structure similarity index metric	0.021377500	0.037992700	0.036532900

Table 52 Image similaritymeasurments of proposed encryption scheme based on S-box of R_5

	Image color components		
	Red	Green	Blue
Structure content	62.221	22.4185	21.9321
Universal image quality index	−0.00113042	−0.0000975	−0.00306773
Structure similarity index metric	0.119023	0.219966	0.212875

Table 53 Image similarity measurments of proposed encryption scheme based on S-box of R_6

	Image color components		
	Red	Green	Blue
Structure content	5.5605800	2.01720000	1.96540000
Universal image quality index	−0.0016198	−0.00399473	−0.00170602
Structure similarity index metric	0.0130455	0.01506070	0.019223800

Table 54 Image similaritymeasurments of proposed encryption scheme based on S-box of R_7

	Image color components		
	Red	Green	Blue
Structure content	22.3112000	7.980790000	7.90325000
Universal image quality index	0.00290522	0.000516327	0.00219534
Structure similarity index metric	0.19237900	0.301132000	0.3223110

Table 55 Image similaritymeasurments of proposed encryption scheme based on S-box of R_8

	Image color components		
	Red	Green	Blue
Structure content	5.2635300	1.8889400	1.86378000
Universal image quality index	0.0023029	−0.0020651	−0.0029209
Structure similarity index metric	0.2721280	0.3122190	0.36223600

Table 56 First order texture analysis of proposed watermarking scheme based on S-box of *GR(4,4)*

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.574219	0.296875	0.195313
Std.	0.496541	0.459496	0.38138	0.495429	0.457776	0.397218
Skewness	−0.267999	0.868817	1.70357	−0.300201	0.889181	1.53711
Kurtosis	1.07182	1.75484	3.90216	1.09012	1.79064	3.36272

Table 57 First order texture analysis of proposed watermarking scheme based on S-box of *GR(8,4)*

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.589844	0.31250	0.160156
Std.	0.496541	0.459496	0.38138	0.492825	0.46442	0.367469
Skewness	−0.267999	0.868817	1.70357	−0.365321	0.80904	1.853270
Kurtosis	1.07182	1.75484	3.90216	1.13346	1.65455	4.434600

Table 58 First order texture analysis of proposed watermarking scheme based on S-box of *GR(32,4)*

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.589844	0.3125	0.160156
Std.	0.496541	0.459496	0.38138	0.492825	0.46442	0.367469
Skewness	−0.267999	0.868817	1.70357	−0.365321	0.80904	1.85327
Kurtosis	1.07182	1.75484	3.90216	1.13346	1.65455	4.4346

Table 59 First order texture analysis of proposed watermarking scheme based on S-box of R_5

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.574219	0.28125	0.175781
Std.	0.496541	0.459496	0.38138	0.495429	0.45049	0.38138
Skewness	−0.267999	0.868817	1.70357	−0.300201	0.973067	1.70357
Kurtosis	1.07182	1.75484	3.90216	1.09012	1.94686	3.90216

Table 60 First order texture analysis of proposed watermarking scheme based on S-box of R_6

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.574219	0.28125	0.175781
Std.	0.496541	0.459496	0.38138	0.495429	0.45049	0.38138
Skewness	−0.267999	0.868817	1.70357	−0.300201	0.973067	1.70357
Kurtosis	1.07182	1.75484	3.90216	1.09012	1.94686	3.90216

Table 61 First order texture analysis of proposed watermarking scheme based on S-box of R_7

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.578125	0.289063	0.183594
Std.	0.496541	0.459496	0.38138	0.494826	0.454215	0.387911
Skewness	−0.267999	0.868817	1.70357	−0.316386	0.930620	1.634530
Kurtosis	1.07182	1.75484	3.90216	1.100100	1.866050	3.671690

Table 62 First order texture analysis of proposed watermarking scheme based on S-box of R_8

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Mean	0.566406	0.300781	0.175781	0.570313	0.296875	0.171875
Std.	0.496541	0.459496	0.38138	0.496001	0.457776	0.378011
Skewness	−0.267999	0.868817	1.70357	−0.284073	0.889181	1.739460
Kurtosis	1.07182	1.75484	3.90216	1.080700	1.790640	4.025730

Table 63 Second order texture analysis of proposed watermarking scheme based on S-box of $GR(4,4)$

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.372687	0.392816	0.365273	0.39375	0.406985	0.389338
Homogenity	0.872453	0.871262	0.874949	0.864794	0.866005	0.865558
Entropy	7.29110	7.581330	7.079450	7.32279	7.56524	7.09129
Correlation	0.923453	0.929416	0.853838	0.920109	0.926875	0.847282
Energy	0.138624	0.0999494	0.169877	0.135096	0.0973498	0.159161

Table 64 Second order texture analysis of proposed watermarking scheme based on S-box of *GR(8,4)*

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.372687	0.392816	0.365273	0.391866	0.406127	00387469
Homogenity	0.872453	0.871262	0.874949	0.865176	0.866715	0.868536
Entropy	7.29110	7.581330	7.079450	7.3227	7.5607	7.08971
Correlation	0.923453	0.929416	0.853838	0.920656	0.927186	0.846354
Energy	0.138624	0.0999494	0.169877	0.134363	0.0978212	0.161773

Table 65 Second order texture analysis of proposed watermarking scheme based on S-box of *GR(32,4)*

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.372687	0.392816	0.365273	0.391866	0.406127	00387469
Homogenity	0.872453	0.871262	0.874949	0.865176	0.866715	0.868536
Entropy	7.29110	7.581330	7.079450	7.3227	7.5607	7.08971
Correlation	0.923453	0.929416	0.853838	0.920656	0.927186	0.846354
Energy	0.138624	0.0999494	0.169877	0.134363	0.0978212	0.161773

Table 66 Second order texture analysis of proposed watermarking scheme based on S-box of R_5

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.372687	0.392816	0.365273	0.397702	0.403278	0.376716
Homogenity	0.872453	0.871262	0.874949	0.863205	0.863345	0.870555
Entropy	7.29110	7.581330	7.079450	7.30967	7.48019	7.0773
Correlation	0.923453	0.929416	0.853838	0.92072	0.926736	0.854595
Energy	0.138624	0.0999494	0.169877	0.133659	0.0969861	0.155589

Table 67 Second order texture analysis of proposed watermarking scheme based on S-box of R_6

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.372687	0.392816	0.365273	0.394225	0.395787	0.374494
Homogenity	0.872453	0.871262	0.874949	0.864685	0.867443	0.870939
Entropy	7.29110	7.581330	7.079450	7.30751	7.48453	7.07733
Correlation	0.923453	0.929416	0.853838	0.921642	0.928676	0.854764
Energy	0.138624	0.0999494	0.169877	0.135017	0.098445	0.157312

Table 68 Second order texture analysis of proposed watermarking scheme based on S-box of R_7

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.372687	0.392816	0.365273	0.382154	0.383824	0.373851
Homogenity	0.872453	0.871262	0.874949	0.869645	0.874147	0.872720
Entropy	7.29110	7.581330	7.079450	7.29890	7.499040	7.077940
Correlation	0.923453	0.929416	0.853838	0.923301	0.931268	0.853531
Energy	0.138624	0.0999494	0.169877	0.137470	0.100933	0.161723

Table 69 Second order texture analysis of proposed watermarking scheme based on S-box of R_8

	Original image color components			Watermarked image color components		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.372687	0.392816	0.365273	0.376532	0.399203	0.374295
Homogenity	0.872453	0.871262	0.874949	0.871378	0.868688	0.871490
Entropy	7.29110	7.581330	7.079450	7.282660	7.512610	7.076750
Correlation	0.923453	0.929416	0.853838	0.921681	0.928119	0.850357
Energy	0.138624	0.0999494	0.169877	0.140061	0.098777	0.168454

Table 70 Image error measurements of proposed watermarking scheme based on S-box of *GR(4,4)*

	Image color components		
	Red	Green	Blue
Mean square error	35.072	30.841	37.9247
Peak signal to noise ratio	32.6812	33.2395	32.3416
Mean absolute error	4.62018	4.33269	4.80144

Table 71 Image error measurements of proposed watermarking scheme based on S-box of *GR(8,4)*

	Image color components		
	Red	Green	Blue
Mean square error	29.9243	26.5959	32.3507
Peak signal to noise ratio	33.3706	33.8827	33.0320
Mean absolute error	4.22232	3.98900	4.40581

Table 72 Image error measurements of proposed watermarking scheme based on S-box of *GR(32,4)*

	Image color components		
	Red	Green	Blue
Mean square error	29.9243	26.5959	32.3507
Peak signal to noise ratio	33.3706	33.8827	33.0320
Mean absolute error	4.22232	3.98900	4.40581

Table 73 Image error measurments of proposed watermarking scheme based on S-box of R_5

	Image color components		
	Red	Green	Blue
Mean square error	67.7634	60.3825	67.1817
Peak signal to noise ratio	29.8206	30.3217	29.8583
Mean absolute error	7.09592	6.75697	6.99326

Table 74 Image error measurments of proposed watermarking scheme based on S-box of R_6

	Image color components		
	Red	Green	Blue
Mean square error	55.2887	48.5003	55.1235
Peak signal to noise ratio	30.7044	31.2734	30.7174
Mean absolute error	6.26427	5.9082	6.19368

Table 75 Image error measurments of proposed watermarking scheme based on S-box of R_7

	Image color components		
	Red	Green	Blue
Mean square error	31.9533	26.3285	32.6609
Peak signal to noise ratio	33.0856	33.9265	32.9905
Mean absolute error	5.65273	5.13113	5.71497

Table 76 Image error measurments of proposed watermarking scheme based on S-box of R_8

	Image color components		
	Red	Green	Blue
Mean square error	22.435	20.2259	24.6088
Peak signal to noise ratio	34.6215	35.0717	34.2199
Mean absolute error	3.65494	3.48647	3.83476

Table 77 Image similarity measurements of proposed watermarking scheme based on S-box of *GR(4,4)*

	Image color components		
	Red	Green	Blue
Structure content	1.02006	1.02876	1.03460
Universal image quality index	0.767415	0.80177	0.756734
Structure similarity index metric	0.895856	0.906332	0.885709

Table 78 Image similarity measurements of proposed watermarking scheme based on S-box of *GR(8,4)*

	Image color components		
	Red	Green	Blue
Structure content	1.01492	1.02385	1.02670
Universal image quality index	0.78181	0.812344	0.767011
Structure similarity index metric	0.906944	0.917087	0.896842

Table 79 Image similarity measurements of proposed watermarking scheme based on S-box of *GR(32,4)*

	Image color components		
	Red	Green	Blue
Structure content	1.01492	1.02385	1.02670
Universal image quality index	0.78181	0.812344	0.767011
Structure similarity index metric	0.906944	0.917087	0.896842

Table 80 Image similaritymeasurments of proposed watermarking scheme based on S-box of R_5

	Image color components		
	Red	Green	Blue
Structure content	1.0733	1.11063	1.12045
Universal image quality index	0.80846	0.837688	0.792751
Structure similarity index metric	0.927252	0.932159	0.916876

Table 81 Image similaritymeasurments of proposed watermarking scheme based on S-box of R_6

	Image color components		
	Red	Green	Blue
Structure content	1.06197	1.09256	1.10057
Universal image quality index	0.808703	0.839345	0.79333
Structure similarity index metric	0.927525	0.934201	0.917581

Table 82 Image similaritymeasurments of proposed watermarking scheme based on S-box of R_7

	Image color components		
	Red	Green	Blue
Structure content	1.03484	1.04849	1.05593
Universal image quality index	0.81822	0.85175	0.80365
Structure similarity index metric	0.93213	0.94117	0.92368

Table 83 Image similaritymeasurments of proposed watermarking scheme based on S-box of R_8

	Image color components		
	Red	Green	Blue
Structure content	0.983519	0.969268	0.970146
Universal image quality index	0.825920	0.858906	0.812379
Structure similarity index metric	0.936415	0.945399	0.927879

similarity coefficients are closed to one which elucidates the robustness of suggested watermarking algorithm constructed on the classes of chain rings (Tables 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82 and 83).

7 Conclusion

In this article, we developed new schemes for image encryption and watermarking independently that soundly depends on classes of finite chain rings. The readings of test images in case of encryption and watermarking are closed to optimal values that reflect the endorsement of our suggested data hiding technique. In future, we will combine encryption and watermarking due to the fact that cryptography provides no protection once the content is decrypted, which is required for human perception, whereas watermarking complements cryptography by embedding a message within the content.

References

1. Abu Dahrouj FM (2008) Negacyclic and constacyclic codes over finite chain rings. Master of Mathematics Thesis, The Islamic University of Gaza
2. Abualrub T, Saip I (2007) Cyclic coacquired a great consideration in algebraic coding theory over the rings F_2 + uF_2 and $F_2 + uF_2 + u^2F_2$. Des Codes Crypt 42:273–287
3. Adams C, Tavares S (1990) The structured design of cryptographically good S-boxes. J Crypt 3:27–41
4. Al-Ashker M (2005) Simplex codes over the ring $\sum_{2n=0}^{n} {}^{s}u^nF_2$. Turk J Math 29(3):221–233
5. Al-Ashker M (2005) Simplex codes over $F_2 + uF_2$. Arab J Sci Eng 3:227–285
6. Al-Ashker M, Chen J (2013) Cyclic codes of arbitrary length over $F_q + uF_q + \cdots + u^{k-1}F_q$. Palist J Math 2(1):72–80
7. Al-Ashker M, Hamoudeh M (2011) Cyclic codes over $F_2 + uF_2 + \cdots + u^{k-1}F_2$. Turk J Math 33:737–749
8. Andrade AA, Palazzo R (1999) Construction and decoding of BCH codes over finite rings. Linear Algebra Appl 286:69–85
9. Anees A, Ahmed Z (2015) A technique for designing substitution box based on van der pol oscillator. doi:10.1007/s11277-015-2295-4, Wireless Pers. Commun
10. Bilgin B, Nikova S, Nikov V, Rijmen V, Stutz G (2012) Thershold Implementations of all 3 × 3 and 4 × 4 S-boxes. Cryptographic Hardware and Embedded Systems. Springer Berlin Heidelberg 76–91
11. Bonnecaze A, Udaya P (1999) Cyclic codes and self dual codes over $F_2 + uF_2$. IEEE Trans Inf Theory 45:1250–1255
12. Cohen S, Niederreiter H (2009) Finite fields and applications. Cambridge University Press, London
13. Cui L, Cao Y (2007) A new S-box structure named Affine-Power-Affine. Int J Innov Comput Appl 3(3):45–53
14. Daemen J, Rijmen V. The block cipher Rijndael. NIST's AES
15. Khan M, Shah T (2014) A novel image encryption technique based on Hénon chaotic map and S8 symmetric group. Neural Comput Appl 25:1717–1722
16. Li X, Li B, Yang B, Zeng T (2013) General framework to histogram shifting based reversible data hiding. IEEE Trans Image Process 22:2181–2191
17. Liu Z, Zhang F, Wang J, Wang H, Huang J (2016) Authentication and recovery algorithm for speech signal based on digital watermarking. Signal Process 123:157–166
18. Naji A (2002) Linear codes over $F_2 + uF_2 + u^2F_2$ of Constant Lee weight. The second conference of the Islamic University on Mathematical Science-Gaza
19. Qian J, Li Z, Zhu S (2006) Constacyclic and cyclic codes over $F_2 + uF_2 + u^2F_2$. IEICE Trans Fundam 6:1863–1885
20. Qian J, Zhang L, Zhu S (2005) Cyclic codes over $F_p + uF_p + \cdots + u^{k-1}F_p$. IEICE Trans Fundam 3:795–779
21. Qian J, Zhang L, Zhu S (2006) (1+u) constacyclic and cyclic over $F_2 + uF_2$. Appl Math Lett 19(8):823–820
22. Qin C, Chang C-C, Chiu Y-P (2014) A novel joint data-hiding and compression scheme based on SMVQ and image inpainting. IEEE Trans Image Process 23:969–978
23. Qin C, Zhang X (2015) Effective reversible data hiding in encrypted image with privacy protection for image content. J Vis Commun Image Represent 31:154–164
24. Qin C, Chang C-C, Hsu T-J (2015) Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Multimedia Tools Appl 74:5861–5872

25. Rijmen V. Efficient Implementation of the Rijndael S-box. Katholieke Universiteit Leuven, Dept. ESAT, Kard. Mercierlaan 94, B–3001 Heverlee, Belgium
26. Sajjad M, Ejaz N, Baik SW (2014) Multi-kernel based adaptive interpolation for image super-resolution. Multimed Tools Appl 72:2063–2085
27. Selvarajah S, Kodituwakku SR (2011) Analysis and comparison of texture features for content based image retrieval. Int J Latest Trends Comput 2:108–113
28. Shah T, Qamar A, Hussain I (2013) Substitution box on maximal cyclic subgroup of units of a Galois ring. Z Naturforsch A 68a:567–572
29. Shanbhag AG, Kumar PV, Helleseth T (1996) Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation of some q-ary sequences. IEEE Trans Inf Theory 42(1):250–54
30. Shankar P (1979) On BCH codes over arbitrary integer rings. IEEE Trans Inf Theory IT-25(4):480–483
31. Tran MT, Bui DK, Doung AD (2008) Gray S-box for advanced encryption standard. Int Conf Comput Intell Secur 1:253–256
32. Yi X, Cheng SX, You XH, Lam KY (2002) A method for obtaining cryptographically strong 8×8 S-boxes. Int Conf Inf Netw Appl 2(3):14–20

Dr. Majid Khan is a prominent researcher in information security. He is the winner of the Productive Scientist Award in 2012, 2013, and 2014. He has done his PhD from Quaid-i-Azam University Islamabad, Pakistan in Dec. 2015. Recently, he is working as an Assistant Professor in the Department of Applied Mathematics & Statistics at Institute of Space Technology, Islamabad, Pakistan.

Dr. Tariq Shah is working as a Professor and head of mathematical cryptography group at Quaid-i-Azam University Islamabad, Pakistan. He has introduced number of courses at post graduate and graduate level in different institutions. He is founder of mathematical cryptography and designs different structures for the construction of nonlinear component of block ciphers and cryptosystems.

Syeda Iram Batool is a potential researcher and analyst in information hiding techniques which have been booming due to fast development in internet and online banking.