Substitution Box on Maximal Cyclic Subgroup of Units of a Galois Ring

Tariq Shah, Attiq Qamar, and Iqtadar Hussain

Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

Reprint requests to I. H.; E-mail: iqtadar.hussain@nu.edu.pk

Z. Naturforsch. **68a,** 567 – 572 (2013) / DOI: 10.5560/ZNA.2013-0021
Received October 26, 2012 / revised February 21, 2013 / published online July 17, 2013

In this paper, we construct a new substitution box (S-box) structure based on the elements of the maximal cyclic subgroup of the multiplicative group of units in a finite Galois ring instead of Galois field. We analyze the potency of the proposed S-box by using the majority logic criterion. Moreover, we illustrate the utility of the projected S-box in watermarking.

Key words: S-Box; Watermarking; Galois Field; Galois Ring; Maximal Cyclic Subgroup.

1. Introduction

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 coding theory. In this respect, initially Shankar [1] presented a construction technique of Bose–Chaudhuri–Hocquenghem (BCH) 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 Z_{p^k}. The construction of this maximal cyclic subgroup is based on a mod-p reduction map from commutative ring Z_{p^k} to Z_p (see Shankar [1]). However, the exponential sums over Galois rings and an upper bound for the hybrid sum over the Galois ring are obtained by using maximal cyclic subgroups of the groups of units of these Galois ring one can see in a series of papers Cohen [2] and Shanbhag et al. [3]. Further, Andrade and Palazzo [4] gave the construction of BCH codes over the Galois rings by means of maximal cyclic subgroup. In this sequel, Shah et al. [5, 6] present a sequence of BCH codes using the chain of maximal cyclic subgroups of the chain of groups of units in the chain of finite Galois rings and finite unitary commutative rings.

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. The complexity of the problem is to construct bijective Boolean functions over this maximal cyclic subgroup adjoining zero, with the extension $0 \to 0$.

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) and GR(4,4) of Z_4. In Section 4, we examine the security of the projected S-box with the majority logic criterion (MLC). Section 5 presents the usefulness of the proposed substitution box in watermarking and Section 6 is about conclusions and future directions.

2. Construction of Maximal Cyclic Subgroup

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

Definition 1 (Unit elements)**.** 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 $u \cdot v = 1$, where 1 is the identity of R.

Definition 2 (Local ring)**.** 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 Z_{p^k}, p is a prime integer and k is any positive integer, is a local ring.

Definition 3 (Zero divisors)**.** 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 $a \cdot b = 0$.

Definition 4 (Basic irreducible polynomial)**.** 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 $(= R/M)$.

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

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 $p^h - 1$.

Theorem 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^*.

Example 1. The corresponding residue field of the ring is $Z_2 = \{0,1\}$. Let $f(x) = x^2 + 3x + 1$ be a monic and basic irreducible polynomial over Z_4 and $\bar{f}(x) = x^2 + x + 1$ is an irreducible polynomial over Z_2. Now $Z_2[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in Z_2, n \in Z^+\}$ is the polynomial ring in one indeterminate x and ideal generated by $\bar{f}(x)$ is denoted and defined as $\langle \bar{f}(x)\rangle = \{a(x)\cdot \bar{f}(x) :\ a(x) \in Z_2[x]\}$. Similarly, $Z_4[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n :\ a_i \in Z_4,\ n \in Z^+\}$ and ideal generated by $f(x)$ is denoted and defined as $\langle f(x)\rangle = \{a(x)\cdot f(x) :\ a(x) \in Z_4[x]\}$. Now, the Galois ring of order 16 becomes $R = \frac{Z_4[x]}{\langle x^2+3x+1\rangle}$ and the corresponding Galois field of order 4 becomes $K = \frac{Z_2[x]}{\langle x^2+x+1\rangle}$. The multiplicative group of units of K is $K^* = \{1, \bar{u}, \bar{u}+1\}$, where $\bar{u}$ denotes the residue class containing $\{x\}$. The elements of $\mathrm{GF}(2^2)$ are given in Table 1.

Similarly, the multiplicative group of units of R is R^* and its cyclic subgroup is $G_3 = \{1, 3u, u+3\}$, where u is the residue class containing x. We can write it in tabular form as in Table 2.

Example 2. Let $Z_4 = \{0,1,2,3\}$ be a ring with residue field $Z_2 = \{0,1\}$. Let $f(x) = x^4 + x + 1$ be a monic and irreducible polynomial over Z_4 and $\bar{f}(x) = x^4 + x + 1$ is irreducible over Z_2. Now $Z_2[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n :\ a_i \in Z_2,\ n \in Z^+\}$ and ideal generated by $\bar{f}(x)$ is denoted and defined as $\langle \bar{f}(x)\rangle = \{a(x)\cdot \bar{f}(x) : a(x) \in Z_2[x]\}$. Similarly $Z_4[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n :\ a_i \in Z_4,\ n \in Z^+\}$ and ideal generated by $f(x)$ is denoted and defined as $\langle f(x)\rangle = \{a(x)\cdot f(x) : a(x) \in Z_4[x]\}$. Now a Galois ring of order 256 becomes $R = \frac{Z_4[x]}{\langle x^4+x+1\rangle}$ and its corresponding Galois field of order 16 becomes $K = \frac{Z_2[x]}{\langle x^4+x+1\rangle}$. The elements of $\mathrm{GF}(2^4)$ can be obtained in Table 3 using the identity $\bar{u}^4 + \bar{u} + 1 = 0$ and modulo 2.

The multiplicative group of units of K is $K^* = K\backslash\{0\}$. Similarly a multiplicative group of units of R is R^* and its cyclic subgroup is G_{15}. Since the corre-

Table 1. Elements of Galois field of order 4.

Exp.	Polynomial		Calculation
$-\infty$	0	00	
0	1	10	
1	$\bar{u}$	01	
2	$1+\bar{u}$	11	$\bar{u}^2 = 1+\bar{u}$

Table 2. Elements of cyclic subgroup of order 3.

Exp.	Polynomial		Calculation
$-\infty$	0	00	
0	1	10	
2	$3+\bar{u}$	31	$u^2 = 3+u$
4	$3\bar{u}$	03	$u^4 = u^2\cdot u^2 = 1+2u+u^2$ $= 1+2u+3+u = 3u$

Table 3. Elements of Galois field of order 16.

Exp.	Polynomial		Calculation
$-\infty$	0	0000	
0	1	1000	
1	$1+\bar{u}$	1100	
2	$1+\bar{u}^2$	1010	$(\bar{u}+1)^2=\bar{u}^2+1$
3	$1+\bar{u}+\bar{u}^2+\bar{u}^3$	1111	$(\bar{u}+1)^3=(\bar{u}+1)(\bar{u}+1)^2$ $=(\bar{u}+1)(\bar{u}^2+1)$ $=\bar{u}^3+\bar{u}^2+\bar{u}+1$
4	$\bar{u}$	0100	$(\bar{u}+1)^4=(\bar{u}+1)^2(\bar{u}+1)2$ $=(\bar{u}^2+1)(\bar{u}^2+1)=\bar{u}^4+1$ $=\bar{u}+1+1=\bar{u}$
5	$\bar{u}+\bar{u}^2$	0110	$(\bar{u}+1)^5=(\bar{u}+1)(\bar{u}+1)^4$ $=(\bar{u}+1)(\bar{u})=\bar{u}^2+\bar{u}$
6	$\bar{u}+\bar{u}^3$	0101	$(\bar{u}+1)^6=(\bar{u}+1)(\bar{u}+1)^5$ $=(\bar{u}+1)(\bar{u}^2+\bar{u})=\bar{u}^3+\bar{u}$
7	$1+\bar{u}^2+\bar{u}^3$	1011	$(\bar{u}+1)^7=(\bar{u}+1)(\bar{u}+1)^6$ $=(\bar{u}+1)(\bar{u}^3+\bar{u})=\bar{u}^3+\bar{u}^2+1$
8	$\bar{u}^2$	0010	$(\bar{u}+1)^8=(\bar{u}+1)^4(\bar{u}+1)^4$ $=\bar{u}\cdot\bar{u}=\bar{u}^2$
9	$\bar{u}^2+\bar{u}^3$	0011	$(\bar{u}+1)^9=(\bar{u}+1)(\bar{u}+1)^8$ $=(\bar{u}+1)\bar{u}^2=\bar{u}^3+\bar{u}^2$
10	$1+\bar{u}+\bar{u}^2$	1110	$(\bar{u}+1)^{10}=(\bar{u}+1)^2(\bar{u}+1)^8$ $=(\bar{u}^2+1)\bar{u}^2=\bar{u}^2+\bar{u}+1$
11	$1+\bar{u}^3$	1001	$(\bar{u}+1)^{11}=(\bar{u}+1)(\bar{u}+1)^{10}$ $=(\bar{u}+1)(\bar{u}^2+\bar{u}+1)=\bar{u}^3+1$
12	$\bar{u}^3$	0001	$(\bar{u}+1)^{12}=(\bar{u}+1)^4(\bar{u}+1)^8$ $=\bar{u}\cdot\bar{u}^2=\bar{u}^3$
13	$1+\bar{u}+\bar{u}^3$	1101	$(\bar{u}+1)^{13}=(\bar{u}+1)(\bar{u}+1)^{12}$ $=(\bar{u}+1)(\bar{u}^3)=\bar{u}^4+\bar{u}^3$ $=\bar{u}^3+\bar{u}+1$
14	$\bar{u}+\bar{u}^2+\bar{u}^3$	0111	$(\bar{u}+1)^{13}=(\bar{u}+1)^2(\bar{u}+1)^{12}$ $=(\bar{u}^2+1)(\bar{u}^3)=\bar{u}^3+\bar{u}^2+\bar{u}$

sponding element of $\bar{u}+1$ is $u+1$ and the order of that element $u+1$ is 30 so the generator of the cyclic group G_{15} is $(u+1)^2$, where $\bar{u}$ is the residue class containing $\bar{u}$ in K and u is the corresponding residue class containing u in R. The elements of the cyclic subgroup of order 15 are shown in Table 4.

3. Construction of the Substitution Box over G_n

The substitution box is the only component of many block ciphers which is capable to create confusion in the data that is why many researchers have paid attention to improve the quality of the S-box. In this paper, we construct a new S-box structure based on G_n. To the best of the authors knowledge, this is the first time to construct a bijective S-box on a cyclic group instead of Galois field. The procedure is explained below:

Table 4. Elements of cyclic subgroup of order 15.

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

Step 1: Define an inversion function I from $G_n\cup\{0\}$ to $G_n\cup\{0\}$.

Step 2: Define a linear scalar multiple function f from $G_n\cup\{0\}$ to $G_n\cup\{0\}$.

Step 3: Take the composition of I and f and get a $n\times n$ S-box.

Some examples are given below.

Example 3. Now take $I: G_3\cup\{0\}\to G_3\cup\{0\}$ such that

$$I(u)=\begin{cases}u^{-1} \text{ if } u\neq 0,\\ 0 \text{ if } u=0,\end{cases}$$

and $f: G_3\cup\{0\}\to G_3\cup\{0\}$ such that

Table 5.

Exp.	Polynomial	
$-\infty$	0	00
4	$3u$	03
2	$3+u$	31
0	1	10

$$f(u)=\begin{cases} au \text{ if } u\neq 0, \\ 0 \text{ if } u=0, \end{cases}$$

where $a=3u=(03)$ then Table 5 is $I\circ f$.

Now for the S-box the decimal form of the above table is

0	3	14	4

Finally, the S-box will be

	0	1	2	3
1	0000	0011	1101	0100

Example 4. Now take $I: G_{15}\cup\{0\}\to G_{15}\cup\{0\}$ such that

$$I(u)=\begin{cases} u^{-1} \text{ if } u\neq 0, \\ 0 \text{ if } u=0, \end{cases}$$

and $f: G_{15}\cup\{0\}\to G_{15}\cup\{0\}$ such that

$$f(u)=\begin{cases} au \text{ if } u\neq 0, \\ 0 \text{ if } u=0, \end{cases}$$

where $a=(u+1)^2=(1210)$ then Table 6 is $I\circ f$.

Table 6.

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

Now for the S-box, Table 6 becomes (under mod 256)

0	193	215	246
100	15	240	4
64	77	29	147
121	30	163	56

and its S-box will be (under mod 2)

	0	1	2	3
0	00000000	11000001	11010111	11110110
1	01100100	00001111	11110000	00000100
2	01000000	01001101	00011101	10010011
3	01111001	00011110	10100011	00111000

4. Majority Logic Criterion for the Analysis of Substitution Boxes

In [7], Hussain et al. have given a majority logic criterion to analyze the statistical strength of an S-box in image encryption application. This criterion is used to analyze the statistical strength of the S-box in image encryption application. The encryption process produces distortions in the image, and the type of these distortions determines the strength of the algorithm.

The results of MLC, arranged in Table 7, show that the proposed S-box satisfies all the criteria up to the standard and can be used for secure communication.

5. Application of Proposed Substitution Box in Watermarking

One possible application of the proposed S-box is that it can be used in watermarking of an image. One of the prime aspects of watermarking is that it does not affect the quality of the image. So keeping that point in mind, the S-box transformation has been applied to the least significant bits (LSBs) of each pixel of an image which will not alter the class of the image. The procedure is explained in Figure 1.

Table 7. Entropy, Contrast, Correlation, Energy, Homogeneity and MAD analysis of proposed sheme.

S-Box	Proposed
Entropy	4.73018
Contrast	3.322085
Correlation	0.087904
Energy	0.024477
Homogeneity	0.483523
MAD	36.3631

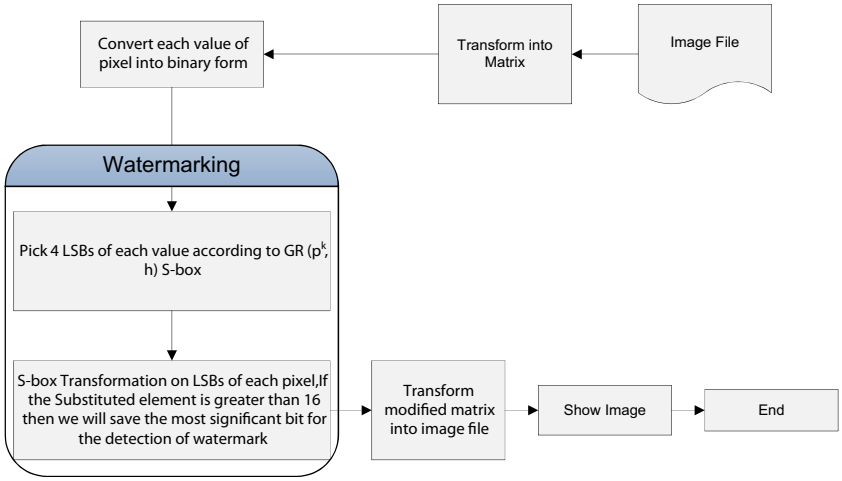

Fig. 1 (colour online). Proposed scheme.

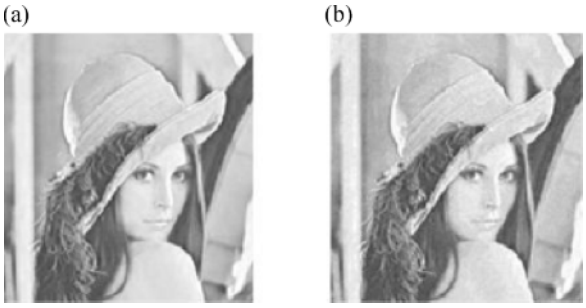

Fig. 2. Grey scale image (two-dimensional matrix of picture elements (pixels) having intensities between 0 and 255) comparison of (a) original image and (b) watermarked image, having a watermark in the four least significant bits (LSBs) of each pixel of the original image by the transformation of the two-dimensional S-Box having four rows and four columns.

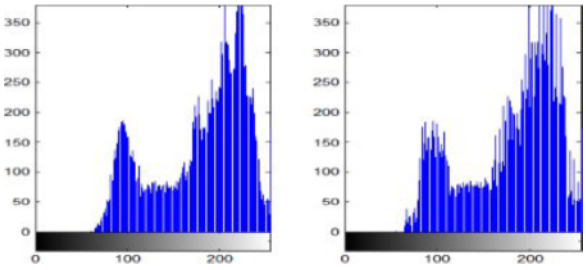

Fig. 3 (colour online). Histogram of Figure 1.

The simulation results are achieved using MATLAB software. The watermarking has been applied to the grey scale, and the comparison of their histograms is analyzed.

In Figure 3, the histograms show the distribution of the intensities of picture elements. We can see that there is not much difference between the two histograms due to the fact that the transformation is applied only to the four LSBs of the original image, so the maximum alteration of a pixel is to the extent of fifteen intensity values. This effect is visualized in Figure 2: the watermark does not affect much the quality of the original image because the human eye can differentiate only forty grey scale levels, so the change of six or less than six grey scale levels cannot be distinguished by the human eye.

Watermarking Analysis	Grey Scale Image
MSE	11.7755
PSNR	86.1651
SSIM	0.9145

6. Conclusion

Some important findings of the proposed work:

(i) In the construction of the S-box, we used the maximal cyclic subgroup of the group of units in a Galois ring instead of a Galois field, and we used a mod p-reduction map to construct maximal cyclic subgroup.

(ii) Since we used a maximal cyclic subgroup under multiplication, so the operation of addition in this construction is removed as in the case of a field.

(iii) In the proposed work, we constructed a 4×4 S-box instead of a 8×8 S-box.

(iv) The mapping of the proposed S-box is one-one from $G_n \cup \{0\}$ to GF(2^8), but in the S-box construc-

tion over a Galois field, the mapping is bijective from GF(2^4) to GF(2^4).

(v) The proposed S-box satisfies the MLC with optimal values and gives a good worth as compared to the other ones.

(vi) We used the propose S-box in watermarking scheme which robust the original image while the watermarked image is almost similar.

(vii) MAD, SSIM, and peak signal to noise ratio (PSNR) analyses of watermarking are very reasonable.

[1] P. Shankar, IEEE Trans. Inform. **25**, 480 (1979).
[2] S. Cohen, Finite Fields and Applications, Cambridge University Press, Cambridge, England 2009.
[3] A. G. Shanbhag, P. V. Kumar, and T. Helleseth, IEEE Trans. Inform. Theory **42**, 250 (1996).
[4] A. A. Andrade and R. Palazzo Jr., Lin. Alg. Appl. **286**, 69 (1999).
[5] T. Shah, A. Qamar, and A. A. Andrade, Math. Sci. Res. J. **16**, 234 (2012).
[6] T. Shah T, A. Qamar A, and A. A. Andrade, Math. Sci. **6**, 51 (2012).
[7] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, Z. Naturforsch. **67a**, 282 (2012).