Wireless Networks (2019) 25:1491–1503
https://doi.org/10.1007/s11276-017-1606-y

A new technique of frequency domain watermarking based on a local ring

Sajjad Shaukat Jamal[1] · Tariq Shah[1] · Shabieh Farwa[2] · Muhammad Usman Khan[3]

Published online: 22 November 2017

Abstract

This paper presents a new and comparatively secure watermarking technique, in the frequency domain. Our scheme deploys a local ring-based substitution box (S-box). The algebraic algorithm used to synthesize S-box basically exploits one–one correspondence between the multiplicative group of units of the local ring $\mathbb{Z}_{512}$ and the Galois field $\boldsymbol{F}_{256}$. This S-box has high confusion creating capability due to the structural properties of the local ring and fulfills the necessary requirements to be reliably used in multimedia applications. We use this S-box in a watermarking scheme to make our technique more confusing and secure to provide more support in copyrights protection strategies. The proposed non-blind digital watermarking technique deals with the application of discrete cosine transform (DCT) in the frequency domain which is comparatively more robust than spatial domain techniques. In the proposed scheme, first the watermark image is substituted through the S-box, and the scrambled watermark is then embedded in the DCT-transformed host image.' To measure the strength of the proposed technique, simulation results and statistical analyses are made. Most significant analyses techniques including measures of homogeneity, contrast, energy, entropy, correlation, mean squared error and peak signal to noise ratio are applied which show coherent results. To determine the robustness of our is effectively strong.

Keywords Local ring · Galois field · S-box · Digital watermarking · Discrete cosine transform

List of symbols

$\boldsymbol{F}_{2^n}$	Galois field of order 2^n
DCT	Discrete cosine transform
H	The host image
W	The watermark image

1 Introduction

Rapidly increasing use of international networking offers various new openings for the design and demonstration in the form of digital data. Easy availability and access to digital contents like electronic advertising, video, audio, digital repositories, electronic libraries, web designing etc. arise many security concerns. Copyright violations and plagiarism indicate that current copyright rules are vulnerable to be used for the digital data transfer on internet. Keeping in view, the importance of copyright protection of digital contents, many researchers initiated working in the field of digital watermarking (a process of hiding data inside a digital signal), that is applied to multimedia data such as text, audio, video and digital images.

For the last three decades, different techniques for watermarking are developed and categorized into two main types named as spatial domain [1] and frequency domain techniques [2]. In the spatial domain, the process of watermarking replaces the pixels of the original image (also known as the host image), with the watermark image. However, in the frequency domain the watermarking process is applied on the coefficients' values of the image. The main feature of both these techniques is to provide digital data the integrity, authentication, copyright protection, broadcast monitoring and most importantly robustness against malicious attacks [3].

Among the aforementioned types of watermarking, spatial domain algorithms offer more capacity to insert watermark but as far as robustness is concerned, frequency

✉ Sajjad Shaukat Jamal
shaukat_sajjad@yahoo.com

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

[2] Department of Mathematics, COMSATS Institute of Information Technology, Wah Campus, Wah Cantt., Pakistan

[3] Department of Electronics, Quaid-i-Azam University Islamabad, Islamabad, Pakistan

domain watermarking is a preferably used technique (see [4] for more details).

Several techniques for digital watermarking in the frequency domain are available in literature including Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) [5], Discrete Fractional Fourier Transform (DFRFT) [6] and Discrete Wavelet Transform (DWT) [7, 8]. We, in the proposed framework, apply the Discrete Cosine Transform method to get robust watermarking. It is safe from annoying blocking artifacts as it is not a block-based transform and offers a high degree of freedom for embedding due to its multi-resolution property. DCT may be used with the combination of other transforms to obtain maximum advantages of the properties of other transforms [9, 10].

DCT-based watermarking algorithms have been widely studied [11, 12]. Recently Zhang et al. [13] proposed a digital watermarking scheme based on DCT, that involves two preprocessing steps (before watermark embedding); changing the size of the watermark and scrambling it. However, our proposed method achieves the security targets by using a comparatively simple, direct and more secure approach as compared to [13]. This algorithm is distinguished from the previous work in two senses; firstly, it enhances the security level by utilizing the S-box, secondly, the structural properties of the used local ring contribute to elevate the imperceptibility level of our technique.

In cryptography, S-box plays a vital role in the confusion creating capability of any system. It is the only nonlinear part of any cryptosystem which actually generates confusion and vagueness. Construction of stronger S-boxes is considered as a major focus of recent research as in the last few years S-boxes gained attention in further multimedia applications as well [14, 15].

In this paper, we introduce an application of S-box in digital watermarking in the frequency domain using DCT method. For the construction of our S-box, we utilize the structure of a local ring $\mathbb{Z}_{512}$ of size 512 which has a multiplicative subgroup of cardinality 256, formed by the unit elements. The bijection between the group of units and the Galois field $\boldsymbol{F}_{256}$ leads us to formulate a new S-box by applying a specific map in the corresponding field. This S-box is used to substitute the watermark before the embedding process. By the involvement of S-box, our technique becomes highly secured against any plagiarism and copyright violations. The substituted watermark image is embedded in the DCT-transformed host image, and the watermarked image is obtained by applying the inverse DCT. The algorithm for the extraction of watermark is also discussed which shows non-blind watermark technique.

The material is organized as follows; in Sect. 2, construction of proposed S-box with the help of unit elements of local ring and their bijection with Galois field is outlined. Frequency domain watermarking technique, along with the embedding and extraction algorithm, is described in Sect. 3. Section 4 deals with the performance analyses of the new S-box. Section 5 presents the detailed statistical analyses of the host and watermarked images. In Sect. 6 image processing attacks are used to examine the robustness of the proposed technique. The last section presents the conclusion.

2 Construction of substitution box

This section presents the algebraic algorithm used to structure our S-box. To understand this, we need to go through some basic facts.

A function $f : \boldsymbol{F}_{2^n} \rightarrow \boldsymbol{F}_2$ is called a Boolean function. A vector Boolean $\mathrm{F} : \boldsymbol{F}_{2^n} \rightarrow \boldsymbol{F}_{2^m}$ is defined as $\mathrm{F(x)} = (f_1(x), f_2(x), \ldots, f_m(x))$, where $x = (x_1, x_2, \ldots, x_n) \in \boldsymbol{F}_{2^n}$ and each of f_i is called a coordinate Boolean function. An $n \times n$ S-box is precisely a vector Boolean function: $\mathrm{S} : \boldsymbol{F}_{2^n} \rightarrow \boldsymbol{F}_{2^m}$.

The construction of proposed S-box depends on 3 majors steps; calculation of multiplicative inverses of the elements of the group of units $U(\mathbb{Z}_{512})$, then the construction of pseudo S-box based on $U(\mathbb{Z}_{512})$ and in the last step defining one–one correspondence between $U(\mathbb{Z}_{512})$ and $\boldsymbol{F}_{256}$. Consequently, 256 distinct values of S-box are obtained.

First step The set of unit elements $U(\mathbb{Z}_{512})$ of local ring $\mathbb{Z}_{512}$ is given as;

$$\begin{aligned} U(\mathbb{Z}_{512}) &= \{z \in \mathbb{Z}_{512} : z \, \textit{is relatively prime to} \, 512\} \\ &= \{2t + 1 : 0 \le t \le 255\} \end{aligned} \tag{1}$$

Now we introduce map, $\tau : U(\mathbb{Z}_{512}) \rightarrow U(\mathbb{Z}_{512})$, defined as

$$\tau(z) = z^{-1} \tag{2}$$

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

Second step Here we need the map, ω: $U(\mathbb{Z}_{512}) \rightarrow U(\mathbb{Z}_{512})$ represented by

$$\omega(z) = cz \quad \text{where,} \quad c \in U(\mathbb{Z}_{512}) \tag{3}$$

For calculation purposes, for instance, we choose $c = 11$ here, then the composition map

$$\begin{aligned} &v = \omega o \tau : U(\mathbb{Z}_{512}) \rightarrow U(\mathbb{Z}_{512}) \text{ gives} \\ &v(z) = 11z^{-1} \end{aligned} \tag{4}$$

Table 1 Row-wise multiplicative inverse of $2t + 1$

1	171	205	439	57	419	197	239	241	27	317	423	41	19	53	479
481	395	429	407	25	131	421	207	209	251	29	391	9	243	277	447
449	107	141	375	505	355	133	175	177	475	253	359	489	467	501	415
417	331	365	343	473	67	357	143	145	187	477	327	457	179	213	383
385	43	77	311	441	291	69	111	113	411	189	295	425	403	437	351
353	267	301	279	409	3	293	79	81	123	413	263	393	115	149	319
321	491	13	247	377	227	5	47	49	347	125	231	361	339	373	287
289	203	237	215	345	451	229	15	17	59	349	199	329	51	85	255
257	427	461	183	313	163	453	495	497	283	61	167	297	275	309	223
225	139	173	151	281	387	165	463	465	507	285	135	265	499	21	19
193	363	397	119	249	99	389	431	433	219	509	103	233	211	245	159
161	75	109	87	217	323	101	399	401	443	221	71	201	435	469	127
129	299	333	55	185	35	325	367	369	155	445	39	169	147	181	95
97	11	45	23	153	259	37	335	337	379	157	7	137	371	405	63
65	235	269	503	121	483	261	303	305	91	381	487	105	83	117	31
33	459	493	471	89	195	485	271	273	375	93	455	73	307	205	511

Third step We define bijective correspondence between $U(\mathbb{Z}_{512})$ and $\boldsymbol{F}_{256}$ by

$$l(2t + 1) = \frac{33t + 23}{12t + 9}, \tag{5}$$

where $0 \le t \le 255$. The fraction on the left side of Eq. (5) is evaluated by expressing each number in 8-bits format such as $33 = 00100001$, $23 = 00010111$, $12 = 00001100$ and $9 = 00001001$. We assign values to "t" corresponding to each of *2t + 1* in Table 2, rewrite it in 8-bits and then apply modular arithmetic as explained in [16, 17].

By the help of these calculations, Table 2 is transformed into an 8×8 proposed S-box.

3 Performance analysis of the proposed S-box

In this section, the essential performance parameters are inspected for the newly generated S-box. The assessment of the projected S-box guarantees its competence and strength [18]. In this article, best available tests are selected to assure the strength of the S-box. It includes bit independence criterion (BIC), linear approximation probability (LP), differential approximation probability (DP), nonlinearity, bit independence criterion (BIC) and strict avalanche criterion. It is proved that the new S-box fulfills all the requirements to be used in further applications. The subsections below describe the required properties in detail (Table 3).

Table 2 S-box based on $U(\mathbb{Z}_{512})$

11	345	207	221	115	1	119	69	91	297	415	45	451	209	71	149
171	249	111	381	275	417	23	229	251	201	319	205	99	113	487	309
331	153	15	29	435	321	439	389	411	105	223	365	259	17	391	469
491	57	431	189	83	225	343	37	59	9	127	13	419	433	295	117
139	473	335	349	243	129	247	197	219	425	31	173	67	337	199	277
299	377	239	509	403	33	151	357	379	329	447	333	227	241	103	437
459	281	143	157	51	449	55	5	27	233	351	493	387	145	7	85
107	185	47	317	211	353	471	165	187	137	255	141	35	49	423	245
267	89	463	477	371	257	375	325	347	41	159	301	195	465	327	405
427	505	367	125	19	161	279	485	507	457	63	461	355	369	231	209
75	409	271	285	179	65	183	133	155	361	479	109	3	273	135	213
235	313	175	445	339	481	87	293	315	265	383	269	163	177	39	373
395	217	79	93	499	385	503	453	475	169	287	429	323	81	455	21
43	121	495	253	147	289	407	101	123	73	191	77	483	497	359	181
203	25	399	413	307	193	311	261	283	489	95	237	131	401	263	341
363	441	303	61	467	97	215	421	443	29	511	397	291	305	207	501

3.1 Strict avalanche criterion

It is the highly-desired property of an S-box that single input deviation produces series of variations in the substitution- permutation network [19, 20].

If we make a single input-bit change, that is, we have two n-tuples x and $y \in F_2^n$ that differ at only one coordinate (say ith coordinate). Mathematically, let $x = (x_1, x_2, \ldots .x_n)$ and $y = x \oplus \tau_i$, where τ_i is an n-tuple, with 1 at ith position and zeros elsewhere (so that x and y differ at ith coordinate only. Let us consider an arbitrary component Boolean function f_k. Let $f_k(x)$ and $f_k(x \oplus \tau_i)$ be the outputs of f_k for a single input-bit change. We denote the corresponding output difference by ξ_k^i, i.e.

$$\xi_k^i = f_k(x) \oplus f_k(x \oplus \tau_i)$$

Let d_i represents the number of n-tuples $x \in F_2^n$, out of the total 2^n tuples in F_2^n, for which $f_k(x) \neq f_k(x \oplus \tau_i)$, then the avalanche probability P_k^i for the kth Boolean function is given by;

$$P_k^i = \frac{d_i}{2^n}$$

P_k^i can be interpreted as the probability of change of the output of f_k, when only ith bit of input x is complemented. The strict avalanche criterion P_k^i must be $\frac{1}{2}$, $\forall 0 \leq i, \ k \leq n$.

Table 4 shows the results of strict avalanche criterion and Fig. 1 provides the comparison of the proposed S-box with the prevailing S-boxes such as Gray, APA, residue prime, S8, Xyi and state of the art, AES S-box. The average value of the strict avalanche criterion comes out to be 0.5039.

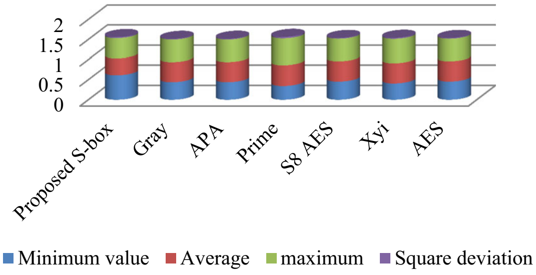


Fig. 1 Strict avalanche criteria of various S-boxes

Table 3 Proposed S-box

95	228	190	139	255	0	175	241	43	8	66	70	125	62	245	119
250	181	158	214	96	100	44	53	192	73	178	17	187	135	246	161
122	206	234	149	106	99	133	235	51	212	211	170	7	93	91	27
205	86	89	67	63	243	182	13	87	77	16	160	41	20	237	167
117	15	24	146	252	216	166	200	213	46	196	152	113	115	42	209
137	111	147	1	2	31	206	194	3	240	148	164	239	21	184	154
189	281	84	143	110	35	220	253	132	61	108	244	247	9	50	208
39	10	112	236	54	126	199	203	33	159	186	72	11	165	222	28
140	155	0	59	30	58	174	79	251	157	142	34	45	6	105	173
151	83	40	101	215	231	123	130	121	59	207	36	204	202	116	62
82	248	78	180	185	176	14	198	22	193	226	156	127	75	218	94
109	12	134	57	76	150	232	230	163	224	177	183	179	32	10	223
141	128	120	48	47	254	153	103	52	69	85	5	238	201	25	197
145	90	107	74	64	249	60	131	18	38	97	168	124	210	104	136
71	162	92	217	169	98	227	129	81	65	37	191	219	68	188	19
242	49	88	23	55	29	229	171	144	149	233	221	138	56	190	114

Table 4 Strict avalanche criterion of substitution box

0.4453	0.5391	0.4688	0.5625	0.4531	0.4922	0.4844	0.4844
0.4766	0.4609	0.5625	0.4688	0.6094	0.5234	0.5938	0.5000
0.4453	0.4922	0.4843	0.5000	0.5156	0.5547	0.5156	0.5313
0.4766	0.5391	0.5156	0.5938	0.4844	0.5391	0.4375	0.5000
0.4609	0.4922	0.5313	0.4375	0.4844	0.4453	0.5156	0.5313
0.4453	0.5703	0.5000	0.5000	0.5000	0.5547	0.5000	0.5000
0.5391	0.5703	0.5000	0.5469	0.4848	0.4609	0.4688	0.4219
0.5547	0.5078	0.4688	0.4219	0.5781	0.5391	0.4844	0.4844

3.2 Bit independence criterion

The makeup for a single plaintext bit is the basic feature of bit independence criterion (BIC). The independent behavior of the pair of variables and the variations of input bits are considered as important factors of bit independence criterion. In bit independence criterion, input bits are transformed exclusively, and then output results are scrutinized for their independency [19, 21]. Bit independence has great worth in cryptographic structures. The goal of reaching the maximum complexity and perplexity in a system can be achieved through this property of increasing independence between the bits. Table 5 presents bit independence of nonlinearity and Table 6 show the comparison of the minimum value, the average value and the square deviation of the proposed S-box with different S-boxes. The minimum value of proposed S-box is 96, the average value is 103.25 and square deviation is 2.849. Figure 2 is a pictorial representation of the comparison of numerical results of BIC applied on different S-boxes.

3.3 Nonlinearity

Nonlinearity analysis measures the distance of the reference function from all of the affine functions. Non-linearity criterion outlines the total number of bits that must be altered in the truth table of a Boolean function to get close to the nearby affine function. These calculations are given as

Table 5 The BIC of nonlinearity of proposed S-box changed

0	104	105	103	103	104	105	103
104	0	103	97	103	106	103	105
105	103	0	102	104	101	104	102
103	97	102	0	108	99	108	102
103	103	104	108	0	101	108	106
104	106	101	99	101	0	101	105
105	103	104	108	108	101	0	96
103	105	102	102	106	105	96	0

Table 6 Bit independence criterion of various substitution boxes

S-boxes	Minimum value	Average	Square deviation
Proposed S-box	96	103.25	2.849
Gray	112	112	0
APA	112	112	0
Prime	94	101.71	3.53
S8 AES	112	112	0
Xyi	98	103.78	2.743
AES	112	112	0

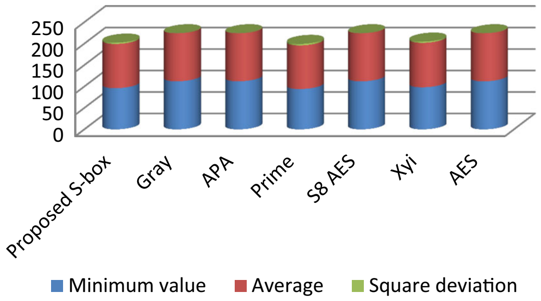


Fig. 2 Bit independence criterion of various substitution boxes

$$N_g = 2^{m-1}\left(1 - 2^{-m} max\left|S_{(g)}(w)\right|\right) \tag{6}$$

where

$$S_{(g)}(w) = \sum\nolimits_{w\epsilon F_2^m}(-1)^{g(x)\otimes\nmid w} \tag{7}$$

represents the Walsh Spectrum. For more details and calculation process see [21]. The average nonlinearity of our S-box is 104.375 that is reasonably acceptable. The nonlinearity measures of the coordinate functions of the proposed S-box and different S-boxes are given in Table 7. Figure 3 is the graphical representation of the nonlinearity comparison.

3.4 Linear approximation probability

The unevenness of an event is calculated in linear approximation method. The maximum value of imbalance of the outcome is also attained through this test. The parity of input and output bits is given by the masks Γ_l and Γ_m respectively. It is given as

$$LP = \max_{\Gamma_l,\Gamma_m \neq 0}\left|\frac{\#\{z/z \bullet \Gamma_l = S(z) \bullet \Gamma_m\}}{2^l} - \frac{1}{2}\right| \tag{8}$$

where z is the set of all possible inputs, the total number of elements is 2^l. The Linear approximation probability of the proposed S-box is 0.1094. The results are compared in Table 8. It is evident from these results that our S-box

Table 7 The nonlinearity of coordinate functions of different substitution boxes

S-boxes	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Average
Gray	112	112	112	112	112	112	112	112	112
Prime	94	100	104	104	102	100	98	94	99.5
Skipjack	104	108	108	108	108	104	104	106	105.75
Proposed	101	103	104	106	106	103	106	106	104.38
APA	112	112	112	112	112	112	112	112	112
AES	112	112	112	112	112	112	112	112	112
S8 AES	112	112	112	112	112	112	112	112	112
Xyi	106	104	106	106	104	106	104	106	105

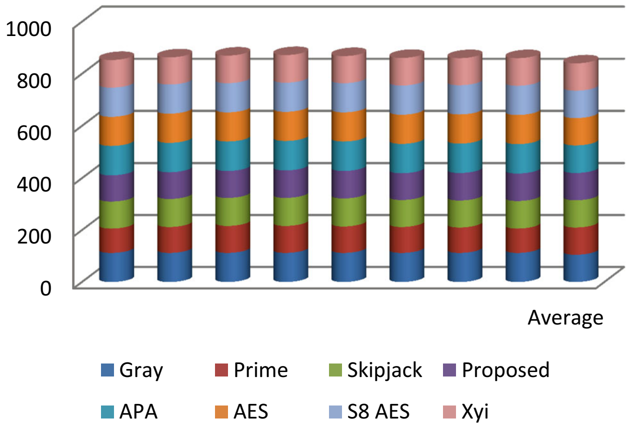


Fig. 3 Nonlinearity of proposed and other S-boxes

shows resistance to linear attacks. The graphical representation of the linear approximation of proposed S-box and different S-boxes is given in Fig. 4.

3.5 Differential approximation probability

For further analysis, we rely on the differential approximation probability test which determines the differential uniformity demonstrated by an S-box. The differential approximation probability is measured by analyzing every input bit and establishing the fact that uniform mapping is ensured. Mathematically, it is given as

$$D_{P^s}(\Delta x \to \Delta y) = \frac{[\#\{x\varepsilon X/S(l) \oplus S(x \oplus \Delta x) = \Delta y\}]}{2^m} \tag{9}$$

The results of odds of differential by applying input and output differentials are given in Table 9. The graphical analyses of proposed S-box and some well-known S-boxes are also shown in Fig. 5.

4 Watermarking algorithm using S-box

The flow chart of the new technique of watermarking using S-box and frequency domain watermarking is depicted in Fig. 1. By utilizing the multiplicative subgroup of unit elements $U(\mathbb{Z}_{512})$ of the local ring $\mathbb{Z}_{512}$, we propose a new S-box which is based on the special algebraic structure of a local ring and its relation with the Galois field. The newly developed S-box possesses reasonably acceptable performance indices as discussed in the previous section. By the help of this S-box, we substitute the watermark image first. This

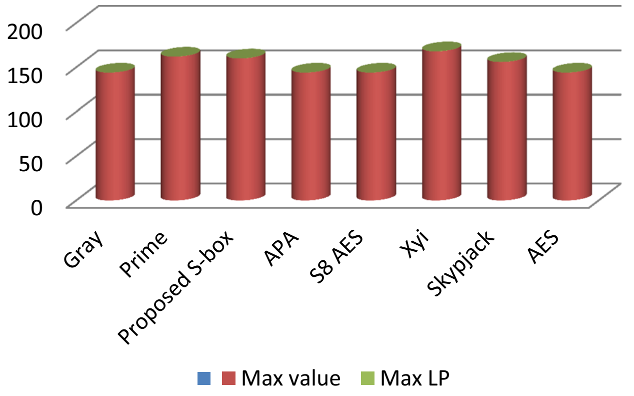


Fig. 4 Comparison of linear approximation probability

altered and secured watermark is then embedded into the DCT-transformed version of the original image. In frequency domain, almost all portions of image observe the change as the watermark is inserted in low or middle frequencies and low-frequency components contain the larger portion of energy. Due to special features of discrete cosine transform, we are applying the frequency domain technique using DCT.

Fourier series provides us the establishment of various transforms including discrete cosine transform (DCT). DCT transforms an image to the frequency domain by compression which is obtained through data quantization. This transform only uses the real part of the Fourier complex kernel and neglect complex part. The main information of the original image is concentrated into the smallest low-frequency coefficient with the help of 2D-DCT. Moreover, due to this transformation, the effect of image blocking is minified, which shows good interaction between the information centralizing and the computing complications. The embedding process is strengthened with the help of secure S-box and this altered watermark is than embedded into DCT-converted host image. For extraction of the watermark, the original host image is needed as it is the non-blind technique of frequency domain. Figures 6 and 7 represent the process of embedding and extraction of the watermark respectively.

4.1 Embedding and extraction of watermark

Let the host image is of size $H1 \times H2$ and is given by $H = \{h(x,y),\ 1 \le x \le H1,\ 1 \le y \le H2\}$ and the watermark image is of size $W1 \times W2$ be denoted as $W = \{w(i,j), 1 \le i \le w1, 1 \le j \le\ W2\}$ and (x,y), (i,j) represent the pixel coordinates of original host image and gray

Table 8 Linear approximation probability analyses of different S-boxes

S-boxes	Gray	Prime	Proposed S-box	APA	S_8 AES	Xyi	Skypjack	AES
Max value	144	162	160	144	144	168	156	144
Max LP	0.062	0.132	0.125	0.062	0.062	0.156	0.109	0.062

Table 9 Differential approximation probability of proposed S-box

0.0234	0.0313	0.0313	0.0234	0.0234	0.0313	0.0313	0.0313	0.0313	0.0313	0.0234	0.0234	0.0234	0.0313	0.0234	0.0313
0.0313	0.0313	0.0313	0.0234	0.0156	0.0234	0.0313	0.0234	0.0234	0.0313	0.0234	0.0234	0.0234	0.0234	0.0234	0.0313
0.0313	0.0234	0.0234	0.0391	0.0234	0.0234	0.0313	0.0313	0.0313	0.0234	0.0234	0.0234	0.0313	0.0313	0.0313	0.0234
0.0234	0.0391	0.0234	0.0234	0.0234	0.0313	0.0234	0.0391	0.0391	0.0313	0.0234	0.0234	0.0234	0.0313	0.0313	0.0234
0.0313	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0156	0.0234	0.0234	0.0234	0.0313	0.0234	0.0313	0.0313	0.0234
0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0313	0.0313	0.0234	0.0234	0.0234	0.0234	0.0234	0.0313	0.0234	0.0234
0.0234	0.0234	0.0234	0.0234	0.0313	0.0234	0.0156	0.0234	0.0234	0.0234	0.0234	0.0313	0.0313	0.0156	0.0234	0.0234
0.0234	0.0391	0.0234	0.0234	0.0234	0.0234	0.0234	0.0234	0.0313	0.0313	0.0391	0.0234	0.0313	0.0234	0.0234	0.0313
0.0313	0.0313	0.0313	0.0234	0.0313	0.0234	0.0313	0.0234	0.0234	0.0391	0.0234	0.0234	0.0313	0.0313	0.0313	0.0313
0.0313	0.0313	0.0234	0.0313	0.0234	0.0391	0.0313	0.0234	0.0234	0.0234	0.0313	0.0234	0.0234	0.0234	0.0234	0.0234
0.0313	0.0234	0.0234	0.0234	0.0313	0.0313	0.0234	0.0234	0.0234	0.0156	0.0313	0.0234	0.0313	0.0313	0.0234	0.0234
0.0313	0.0469	0.0234	0.0313	0.0313	0.0234	0.0234	0.0234	0.0313	0.0313	0.0234	0.0313	0.0234	0.0234	0.0313	0.0234
0.0313	0.0313	0.0313	0.0234	0.0234	0.0234	0.0391	0.0234	0.0313	0.0234	0.0313	0.0234	0.0234	0.0234	0.0234	0.0234
0.0234	0.0234	0.0234	0.0234	0.0469	0.0234	0.0234	0.0234	0.0234	0.0313	0.0234	0.0313	0.0234	0.0313	0.0234	0.0313
0.0313	0.0234	0.0313	0.0313	0.0234	0.0234	0.0234	0.0234	0.0313	0.0313	0.0313	0.0234	0.0234	0.0234	0.0234	0.0234
0.0234	0.0313	0.0234	0.0234	0.0313	0.0391	0.0234	0.0234	0.0313	0.0313	0.0234	0.0234	0.0234	0.0234	0.0234	0.0000

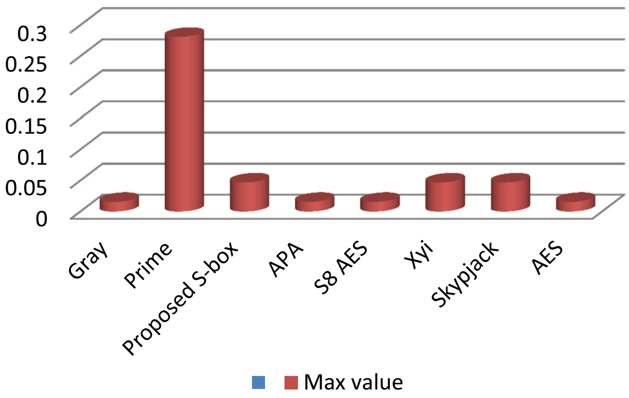


Fig. 5 Comparison of differential approximation probability

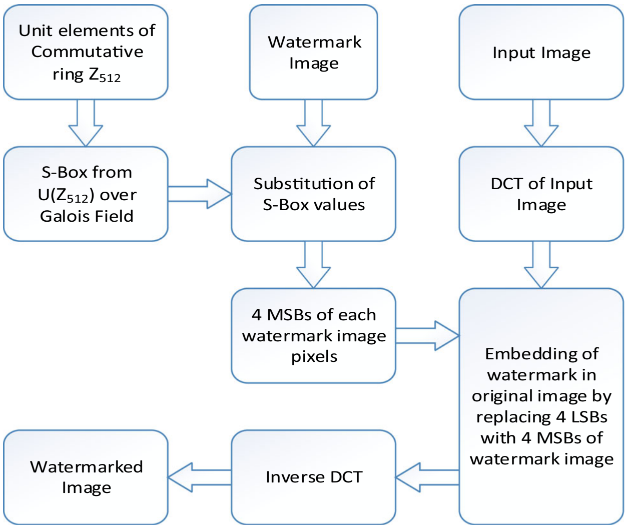

Unit elements of Commutative ring Z512
Watermark Image
Input Image
S-Box from U(Z512) over Galois Field
Substitution of S-Box values
DCT of Input Image
4 MSBs of each watermark image pixels
Embedding of watermark in original image by replacing 4 LSBs with 4 MSBs of watermark image
Watermarked Image
Inverse DCT

Fig. 6 Embedding of S-box substituted watermark in original image

watermark image respectively, If P denotes the total number of binary bits of gray level image pixels than $h(x,y)$ and $w(i,j)$ is given by $\{0,1,\ldots,2L-1\}$. The substitution of the frequency domain is almost same as that in spatial domain with an exception that the watermark is embedded into frequency coefficients of the transformed image. In this article, the scheme becomes more secure as the watermark is substituted with algebraic S-box. This provides more strength to our technique and copy right protection to support our claim at any forum. The watermark is then inserted into DCT-transformed image where we consider positive integral parts of DCT coefficients (neglecting the sign of negative DCT coefficients) and replace the LSBs of DCT coefficient with MSBs of the altered watermark. After applying IDCT on the result we attain the final watermarked image.

In embedding scheme, it must be clear that the S-box, is another hidden truth to counterfeit any plagiarism attempt. Moreover, this provides a strong mathematical foundation to our technique. Figure 8(a)–(c) represent the gray level host images of Lena, Baboon and Peppers respectively. Figure 9 represents the watermark image. The altered watermark, under the application of S-box is depicted in Fig. 10, however, Fig. 11(a)–(c) illustrate the watermarked images of Lena, Baboon and Peppers, after applying the proposed DCT-based watermarking scheme in the frequency domain. The visual results witness that the final watermarked images have the identical appearance as in Fig. 8 of the original images.

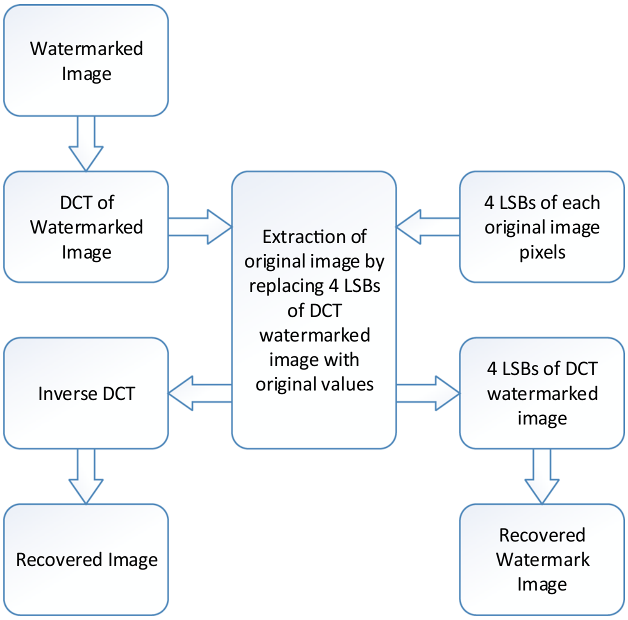

Watermarked Image
DCT of Watermarked Image
Extraction of original image by replacing 4 LSBs of DCT watermarked image with original values
4 LSBs of each original image pixels
Inverse DCT
4 LSBs of DCT watermarked image
Recovered Image
Recovered Watermark Image

Fig. 7 Extraction of watermark

Following the inverse process of embedding, it is possible to extract the watermark image from the original image. The watermarked image is then subjected to DCT and extraction of the original image is done by replacing 4 LSBs of DCT watermarked image with original values. By this process, we are able to extract the watermark from the original image. The extraction process involves the inverse S-box algorithm as well. Figure 12 represent the extracted S-box substituted image and Fig. 13 shows the successfully extracted watermark. The extracted original images of Lena, baboon and Peppers are represented in Fig. 14(a)–(c) respectively.

5 Simulation results and statistical analysis of host and watermarked image

The assessment of both the original image and the s-box substituted, watermarked image with certain statistical tests is performed in this section. We perform frequently used tests including homogeneity, contrast, correlation, entropy,

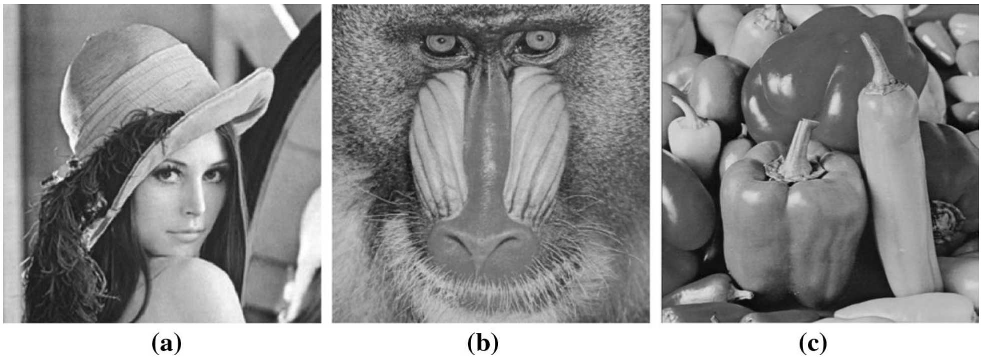
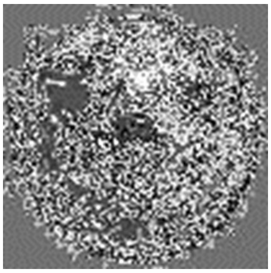


Fig. 8 Host images. **a** Lena. **b** Baboon. **c** Peppers

Fig. 9 Watermark

Fig. 10 S-box substituted watermark



energy, mean square error and peak signal to noise ratio on both the images. These analyses are made on 256 × 256 image of Lena, baboon and pepper along with 50 × 50 watermark image. The results of all above-mentioned analyses are presented in Table 10 and Fig. 15.

Fig. 12 Extracted S-box substituted watermark

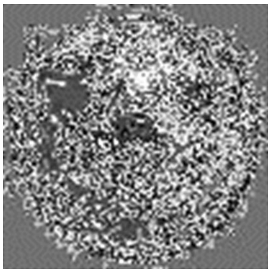
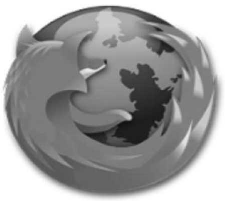


Fig. 13 Extracted watermark



5.1 Homogeneity

Gray level co-occurrence matrix (GLCM) indicates the ability of combinations of pixel brightness results in tabular form. The closeness of the distribution in the (GLCM) to its diagonal is measured in homogeneity. GLCM table gives gray levels frequency. The homogeneity is given as:

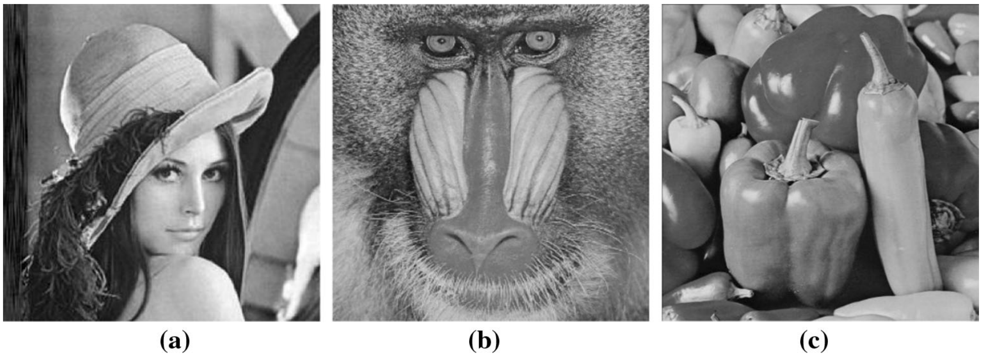


Fig. 11 Watermarked images. **a** Lena. **b** Baboon. **c** Peppers

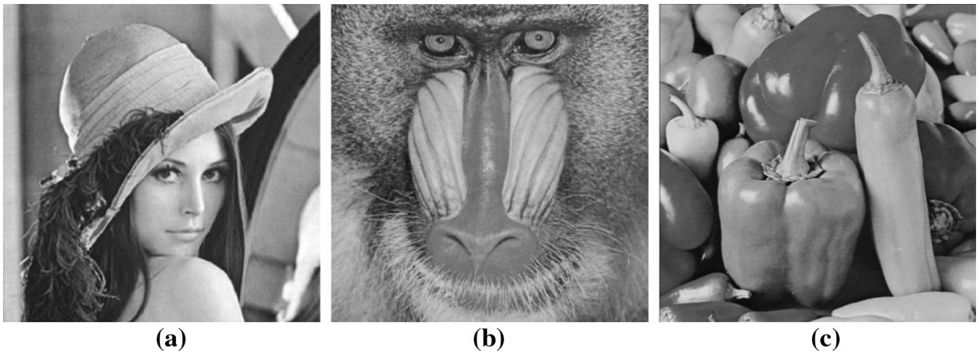


Fig. 14 Extracted images. **a** Lena. **b** Baboon. **c** Peppers

Table 10 Statistical analyses of host image and watermarked image

Statistical	Pepper		Lena		Baboon	
	Host	Watermarked	Host	Watermarked	Host	Watermarked
Homogeneity	0.9317	0.9279	0.8651	0.8625	0.7848	0.7839
Contrast	0.2219	0.2295	0.4141	0.4194	0.6159	0.6194
Energy	0.1560	0.1537	0.0942	0.0934	0.0655	0.0653
Entropy	0.7856	0.7579	0.5859	0.5859	0.6962	0.6962
Correlation	0.9484	0.9467	0.9444	0.9437	0.8994	0.8989

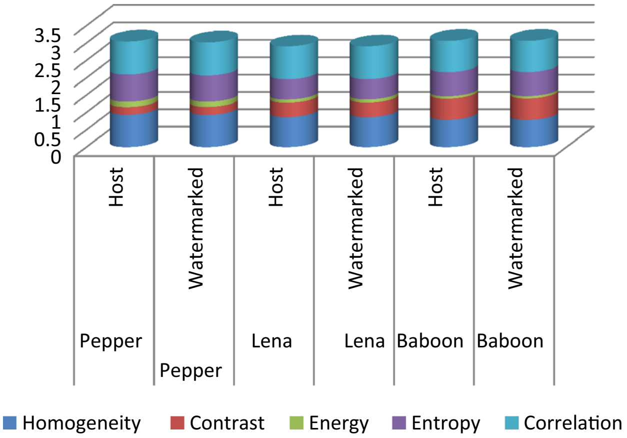


Fig. 15 Comparison of MLC for different images

$$Hom = \sum \frac{p(i,j)}{1 + |i - j|} \tag{10}$$

5.2 Contrast

The Contrast analysis is used to measure the sensitivity of the image textures in relation to intensity alterations. It is defined as

$$C = \sum |i - j|^2 p(i,j) \tag{11}$$

5.3 Energy

For the energy analysis, initially squares of all *ith* row and *jth* column values of gray pixels is calculated and then added to get mathematical representation given as follows

$$E = \sum p(i,j)^2 \tag{12}$$

5.4 Entropy

Entropy helps to determine whether the approximation of the digital image is same as the original image. Entropy specifies the uncertainty of the digital image as it is the magnitude of the randomness. Mathematically,

$$C = -\sum p(x_i) log_2 p(x_i) \tag{13}$$

5.5 Correlation

The similarity between the original image and the watermarked image helps to analyze the quality of scheme which is obtained from correlation. Mathematically it is represented as:

$$Corr = \sum \frac{(i - \mu i)(j - \mu j) p(i,j)}{\sigma_{i\sigma_j}} \tag{14}$$

In above equation, μ and σ denote the mean and the standard deviation respectively and P(i,j) represents the *ith* row and *jth* column pixel value.

5.6 Mean squared error

The dissimilarity between two digital images is calculated with the help of the mean squared error. Table 11 gives the result of MSE. Mathematically it is given by the equation

$$MSE = \frac{1}{n}\sum \left(x_i - x_i^*\right)^2 \tag{15}$$

5.7 Peak signal to noise ratio

The logarithm of the ratio between the signal strength and difference between the images (MSE) gives peak signal to noise ratio. It provides the best relative statistical analysis. Table 11 gives the result of PSNR. It is given as:

$$PSNR = 10log_{10}\frac{MAX_I^2}{MSE} \tag{16}$$

5.8 Complexity analysis

For the application of the proposed technique, the most important factors are the improved security and the embedding, extraction speed of watermark along with the space complexity. In this regard, speed analysis is performed with the help of MATLAB 7.9.0 (R2009b) on a laptop having Windows 7 working structure, Intel(R) Core(TM) i5-2520 M, CPU@ 2.50 GHz and RAM of 4 GB. One can see that the speed of our embedding and extraction process is pretty close to the other DCT-based schemes, however the security level attained by the proposed scheme is highly improved than the recently known techniques. It is worth mentioning that the sequence of operations used for the proposed algorithm requires no additional space. Table 12 provides elapsed time for embedding and extraction of watermark with different image sizes and picture qualities.

6 Robustness test based on image processing operations

The mathematical approximation of two watermarks is the similarity between the extracted and the original watermark [22]. High correlation between the both leads to robustness. The close correlation between two watermarks is observed when the result of similarity is on the higher side. It is represented as,

$$Sim = \frac{\sum t_i.s_i}{\sqrt{\sum t_i^2.\sum s_i^2}} \tag{17}$$

where t_i, s_i represents the corresponding *ith* element of the extracted and the original watermark respectively. The numerical value for confidence measure in our simulation results is 99.92. It demonstrates the ideal correlation between extracted and original watermarks. The watermarked image and extracted watermark are gone through well-known image processing operations which are given in the following subsections. Similarity analysis of different images is given in Table 13.

6.1 Noise attack

The watermark image can be attacked by different noise attacks. Here we add salt noise. Gaussian, Poisson and speckle can also be used for this purpose.

6.2 Compression attack

Joint Photographic Experts Group (JPEG) is measured for compression attack.

6.3 Cropping attack

In cropping attack either extracted image is distorted or offers fewer information than the original image. The outcomes of all image processing attacks are given in

Table 11 MSE and PSNR values of proposed watermarking technique

Image	MSE	PSNR
Pepper	1.4786	46.4814
Lena	1.4665	46.5741
Baboon	1.4644	46.4742

Table 13 Similarity analysis of different Images

Image	SIM
Pepper	0.9964
Lena	0.9937
Baboon	0.9987

Table 12 Elapsed time for Embedding and Extraction of watermark

Serial No	Size	JPEG			PNG		
		Baboon (s)	Pepper (s)	Lena (s)	Baboon (s)	Pepper (s)	Lena (s)
01	512 × 512	5.3631	5.3579	5.6291	5.4792	5.4385	5.6820.
02	256 × 256	1.7309	1.2096	1.7533	1.6618	1.9459	1.9154

Table 14 Confidence measure values against different image processing attacks

Attacks	Pepper	Lena	Baboon
Compression	33.0563	36.4937	22.5401
Noise	18.5720	18.3259	18.7559
Cropping	30.1589	32.4309	28.0296

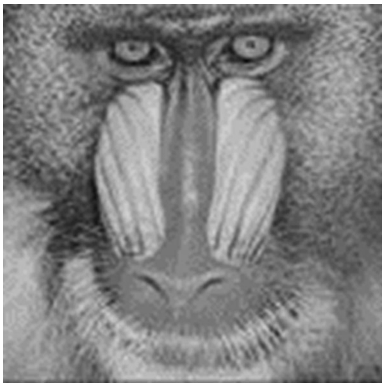


Fig. 16 Pictures of image processing effects. Compression attack

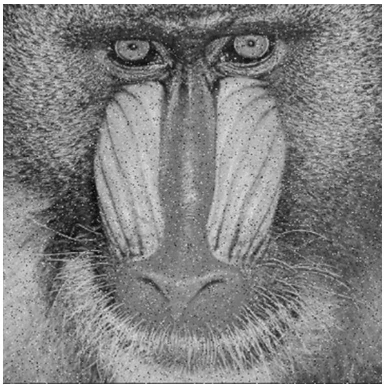


Fig. 17 Pictures of image processing effects. Salt and Pepper attack

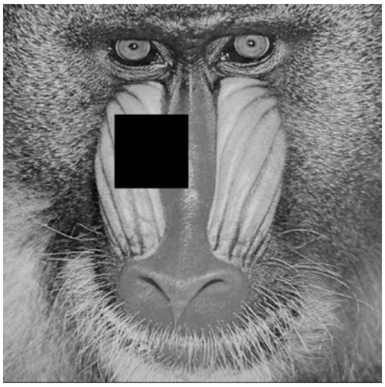


Fig. 18 Pictures of image processing effects. Cropping attack

Table 14 and Figs. 15, 16 and 17 represent the compression, noise and cropping attacks respectively.

7 Conclusion

With certain weaknesses, the best-offered technique for safe copyrights of multimedia data is digital watermarking. In this paper, a new idea is presented for watermarking that mainly relies on a newly designed 8 × 8 S-box from a local ring instead of a Galois field. The involvement of S-box in the scheme, where we substitute the values of watermark image, not only develops confusion in understanding the used scheme but also provides more security and support to our argument for copy right protection of digital data. This technique of watermarking is based on frequency domain Discrete Cosine Transform. The complexity of the algebraic structure of the S-box and then frequency domain technique makes almost impossible to identify watermark. Moreover, the outcomes of statistical analyses and robustness tests really support the new idea of watermarking. The numeric results of similarity, after the application of the image processing tests, lie in the range 40–79%, (78.92% in our case) which makes us conclude that our technique is a semi-fragile watermarking technique (Fig. 18).

References

1. Mukherjee, D. P., Maitra, S., & Acton, S. T. (2004). Spatial domain digital watermarking of multimedia objects for buyer authentication. *IEEE Transactions on Multimedia, 6*(1), 1–15.
2. Lin, S. D., & Chen, C. F. (2000). A robust DCT-based watermarking for copyright protection. *IEEE Transactions on Consumer Electronics, 46,* 415–421.
3. Caronni, G. (1995). Assuring ownership rights for digital images. In *Proceedings of reliable IT systems* (pp. 251–263).
4. Vasudev, R. (2016). A review on digital image watermarking and its techniques. *Journal of Image and Graphics, 4*(2), 150–153.
5. Kitamytra, I., Kanai, S., Kanai, T., & Kishinami, T. (2001). Copyright protection of vector map using digital watermarking method based on discrete Fourier transform. In *Proceedings of IEEE international symposium on geosciences and remote sensing* (pp. 1191–1193).
6. Hong, W. D., Ming, L. D., Jun, Y., & Xiong, C. F. (2007). An improved chirp typed blind watermarking algorithm based on wavelet and fractional Fourier transform. In *Proceedings of IEEE international conference on images and graphics* (pp. 291–296).
7. Lai, C. C., & Tsai, C. C. (2008). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transaction on Instrumentation and Measurement, 59*(11), 3060–3063.
8. Safabakhsh, R., Zaboli, S., & Tabibiazar, A. (2004). Digital watermarking on still images using wavelet transform. In *Proceedings of international conference on information technology: coding and computing-ITCC*.

9. Kang, X., Huang, J., Shi, Y. Q., & Lin, Y. (2003). A DWTDFT composite watermarking scheme robust to both affine transform and JPEG compression. *IEEE Transactions on Circuits and Systems for Video Technology, 13*(8), 776–786.
10. Kaur, S., & Sidhu, R. K. (2016). Robust digital image watermarking for copyright protection with SVD–DWT–DCT and Kalman filtering. *International Journal Emerging Technologies in Engineering Research, 4*(1), 59–63.
11. Wang, G. M., & Hou, Z. F. (2008). Watermarking scheme based on DCT. *Computer Engineering and Design, 29*(21), 5635–5637.
12. Liu, F., & Yang, F. (2009). An improved blind watermarking algorithm based on DCT. *Computer Engineering and Applications, 45*(13), 124–126.
13. Zhang, Q., Li, Y., & Wei, X. (2012). An improved robust and adaptive watermarking algorithm based on DCT. *Journal of Applied Research and Technology, 10*(3), 405–415.
14. Xu, Z. H., Shen, G., & Lin, S. (2011). Image encryption algorithm based on chaos and S-boxes scrambling. *Advanced Materials Research, 171172,* 299–304.
15. Jamal, S. S., Shah, T., & Khan, M. U. (2016). A watermarking technique with chaotic fractional S-box transformation. *Wireless Personal Communications, 90*(4), 2033–2049.
16. Farwa, S., Shah, T., & Idrees, L. (2016). A highly nonlinear S-box based on a fractional linear transformation. *SpringerPlus,* 5(1), 1658. https://doi.org/10.1186/s40064-016-3298-7.
17. Benvenuto, C. J. (2012). *Galois field in cryptography*. Washington: University of Washington.
18. Adams, C., & Tavares, S. (1989). In *Advances in cryptology: proceedings of CRYPTO*. Lecture notes in computer science (Vol. 89, pp. 612–615).
19. Webster, A. F., & Tavares, S. E. (1986). On the design of S-boxes. In *Advances in cryptology: proceedings of CRYPTO'85* (pp. 523–534). Berlin: Springer.
20. Sattar, F., & Mufti, M. (2011) Spectral characterization and analysis of avalanche in cryptographic substitution boxes using Walsh-Hadamard transformations. *International journal of Computer Applications*, *28*(6), 0975–8887.
21. Wang, Y., Xie, Q., Wu, Y., & Du, B. (2009) A software for S-box performance analysis and test. In *International conference on electronic commerce and business intelligence* (pp. 125–128).
22. Cox, J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing, 6*(12), 1673–1687.

Sajjad Shaukat Jamal is currently a Ph.D. candidate in the Department of Mathematics at Quaid-i-Azam University. He has done his masters and M.Phil. from the same university. His research interests are fluid and analytical methods, cryptography and digital watermarking.

Tariq Shah received his Ph.D. in Mathematics from University of Burcharest, Burcharest Romania and is currently serving as Associate Professor in Department of Mathematics at Quaid-i-Azam University. His topics of research are commutative algebra, algebraic coding theory, cryptography, wireless communication, generalization of algebraic structure, fuzzy and soft structures, development of economics.

Shabieh Farwa is currently serving at COMSATS Institute of Information Technology as an Assistant Professor in the Department of Mathematics. She completed her Ph.D. degree from the University of Sheffield, UK in 2012. She has been awarded TM Flett Prize in Pure Mathematics for her Ph.D. research. She is Presidential Award holder and Gold Medalist in Masters and M.Phil. from Quaid-i-Azam University Islamabad Pakistan.

Muhammad Usman Khan has completed his M.Phil. from department of Electronics, Quaid-i-Azam University, Islamabad. His research interests are Image Processing, Digital Image Watermarking, Machine/Computer Vision and Pattern Recognition.