Construction of New S-Boxes Over Finite Field and Their Application to Watermarking

Iqtadar Hussain[a], Tariq Shah[a], Muhammad Asif Gondal[b], and Hasan Mahmood[c]

[a] Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
[b] Department of Sciences and Humanities, National University of Computer and Emerging Sciences, Islamabad, Pakistan
[c] Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan

Reprint requests to I. H.; E-mail: iqtadarqau@gmail.com

Z. Naturforsch. **67a,** 705 – 710 (2012) / DOI: 10.5560/ZNA.2012-0090
Received February 13, 2012 / revised August 13, 2012 / published online November 14, 2012

In this work, we develop an imperceptible watermarking technique for images that employ substitution boxes constructed over Galois field GF(2^4). The strength of the proposed substitution box (S-box) is analyzed and its suitability is investigated for watermarking applications by applying statistical methods, which include entropy, contrast, correlation, energy, homogeneity, mean of absolute deviation (MAD), mean square error (MSE), peak-to-peak signal to noise ratio (PSNR), and structural similarity (SSIM) paradigm analysis. The application of the proposed S-box is presented for embedding copyright information in images.

Key words: Block Ciphers; S-Box; Watermarking; MSE; PSNR; SSIM.

1. Introduction

The substitution box (S-box), in combination with a permutation network, is used to encrypt data by a series of nonlinear mappings and permutations [1]. The application of the S-box is widely seen in various ciphers, such as, data encryption standard (DES), advanced encryption standard (AES), international data incryption standard (IDES), etc., and it provides a nonlinear mapping of plaintext to the encrypted data [2 – 4]. While the application of S-box to encryption applications is widely practiced, an interesting methodology to digital watermarking process is presented in this paper [5 – 8]. In this watermarking technique, a pattern of bits is inserted into a digital image, which assists in identifying the copyright information or the ownership rights [9, 10]. The intellectual property is protected by the imperceptible watermarking technique from the application of nonlinear transformation on the original data. The proposed S-box, which is constructed over GF(2^4) and tailored for watermarking applications, is analyzed through various testing criteria.

In this work, we present a technique for the construction of substitution boxes for block ciphers over finite field GF(2^4) [11]. We analyze the strength of the proposed box by applying statistical methods such as entropy analysis, contrast analysis, correlation analysis, energy analysis, homogeneity analysis, and mean of absolute deviation analysis [12 – 15]. Furthermore, we developed a new watermarking method that uses the proposed S-box in creating images with embedded copyright information. At the end, we analyze the strength of the proposed watermarking technique with mean of absolute deviation (MAD) analysis, mean square error (MSE) analysis, peak-to-peak signal to noise ratio (PSNR) analysis, structural similarity (SSIM) paradigm analysis, and discuss the properties of the proposed method of watermarking [7 – 10].

This paper is structured as follows. Section 2 presents the construction of a S-box over finite field, and Section 3 describes the method for the new watermarking technique by the application of the proposed S-box. The statistical analysis of the new S-box is presented in Section 4. Simulation results are discussed in Section 5, and the conclusions are presented in Section 6.

2. Construction of New S-Box Over Finite Field

This section presents details for the construction of the proposed S-box. The method used to define the proposed S-box is similar to the AES S-box construc-

tion [16, 17]. The S-box is constructed from a finite field, with a couple of transformations and permutation functions in Galois field of order 16, GF(2^4). The algebraic structure of the proposed S-box is articulated with a Galois field GF(2^4), whereas the AES S-box is constructed over GF(2^8). The following equation describes the algebraic expression of GF(2^4) used in the proposed formulation:

$$\begin{aligned}\mathrm{GF}(2^4) &= \frac{Z_2[X,Z_0]}{(x^4+x+1)}\\ &= a_0+a_1x+a_2x^2+a_3x^3+P,\end{aligned}$$

where $a_0,a_1,a_2,a_3 \in Z_2$ and $P=(x^4+x+1)$. Furthermore, we need to define three more functions (transformations) in GF(2^4) to formally elucidate the proposed S-box. These three mandatory functions consist of two transformations and one permutation. The first transformation $I(x)$ is a multiplicative inverse transformation in the finite Galois field GF(2^4), with an exception of mapping the '0' element to itself as an inverse transformation:

$$I(x)=\begin{cases}x^{-1}, & x\neq 0,\\ 0, & x=0.\end{cases}$$

The second essential transformation $A(x)$ is a composite transformation of two constitutive functions, $L(x)$ and $H(x)$, where $L(x)$ is a linear permutation in GF(2^4) and $H(x)$ is the affine part of the transformation. The permutation $L(x)$ is a Z_2 linear mapping in GF(2^4), therefore it can be expressed as a linearized polynomial with the following terms:

$$L(x)=\sum_{i=0}^{4}\lambda_i x^{2^i}.$$

The above expression can be described by a matrix multiplication as

$$L(x)=\begin{pmatrix}y_0\\y_1\\y_2\\y_3\end{pmatrix}=\begin{pmatrix}1&0&1&1\\1&1&0&0\\1&1&1&0\\0&0&1&1\end{pmatrix}\times\begin{pmatrix}x_0\\x_1\\x_2\\x_3\end{pmatrix},$$

where x_i is the ith bit of the byte x (x_0 is the least significant bit) and y_i is the ith bit of the byte y. Finally, we define the affine transformation function in GF(2^4) as

$$H(x)=x+C,$$

where C is any element from GF(2^4). Now we have all the functions required to characterize the proposed S-box with a similar method used in the construction of AES S-box. The combination of the power function $I(x)$, the linear transformation $L(x)$, and the affine transformation $H(x)$ models the S-box:

$$\text{S-box}_{\text{AES}}=H\circ L\circ I.$$

The permutation of S_4 (symmetric group) is applied to the AES S-box. Finally the algebraic expression of the proposed S_4 AES S-box over GF(2^4) is as follows:

$$\text{S-box}_{S_4\text{AES}}=\pi(H\circ L\circ I),$$

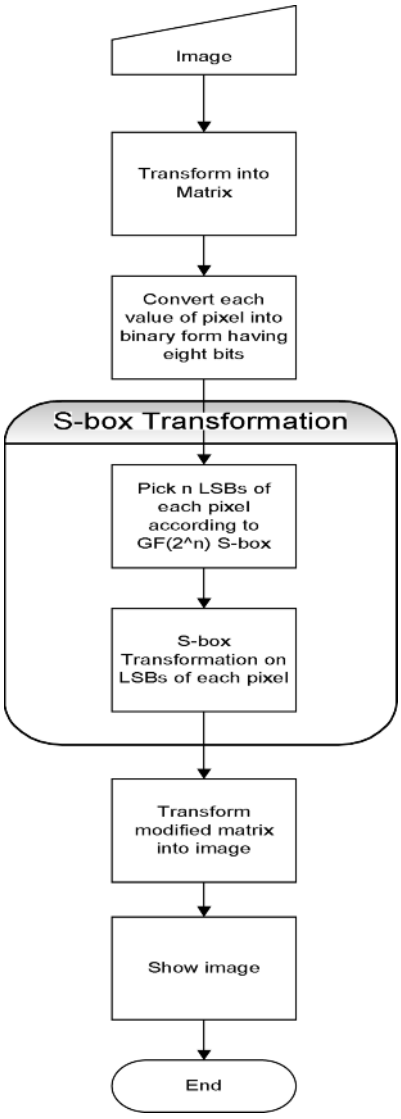

Fig. 1. Watermarking algorithm using S-box transformation.

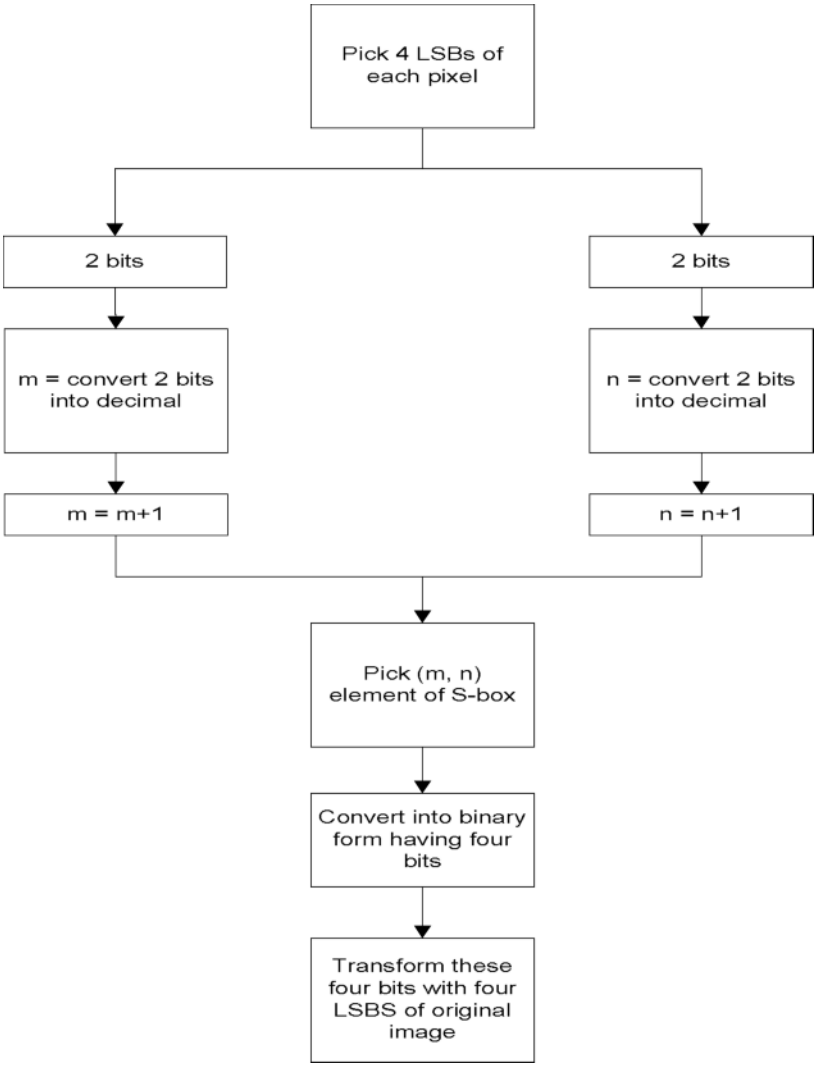

Fig. 2. Transformation of four LSBs of each pixel by using two-dimensional S-box.

where $\pi \in S_4$ (symmetric group of order 2^4). The final matrix of GF(2^4) S-box is shown in Table 1 [18 – 22].

In the next section, we present the secure watermarking technique that uses the S_4 AES S-box to modify the least significant bits in an image.

Table 1. Two-dimensional S-box over GF(2^4).

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

3. Watermarking Algorithm

The flowchart of the watermarking algorithm is illustrated in Figure 1. This flowchart describes the steps for the watermarking process, whereas the actual S-box transformation algorithm details are presented in Figure 2.

The image is processed by creating a matrix, which consists of the constituent pixels. The algorithm presented in this paper induces watermarks on images consisting of 8 bits per pixel. The algorithm can be modified to any number of bits per pixel. The S-box

Table 2. Results of statistical analyses: entropy, contrast, correlation, energy, homogeneity, and mean of absolute deviation (MAD).

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

transformation of one dimensional GF(2^4) S-box is applied to the four least significant bits (LSB) of each pixel of the image. Although the LSBs are replaced by a nonlinear transformation, the change in the bits does not affect the image perception as the LSBs contribute less as compared to the bits with higher significance. After the application of S-box transformation, the image is ready to use and contains embedded watermark that provides copyright information if required.

S-box transformations are mostly used for encryption of the data, but in this work, we present another potential watermarking application of the proposed S-box defined in Table 1. In Figure 2, it is shown that the four LSBs are separated in to pairs of two LSBs. The range of possible values of these pairs of two bits is $\{0,1,2,3\}$. These values are used to select the column and row of the S-box in order to identify the value of the element to be substituted. The corresponding bits in the image are replaced with the bits from the S-box, thus completing the nonlinear transformation. The process is repeated for every pixel in the image.

4. Statistical Analysis of the S-Boxes

Several statistical analyses are used to characterize the watermarked image. These analyses exhibit some interesting properties that assist in evaluating the transformed images with watermarks. The entropy analysis provides information about the amount of randomness in an image, which in turn determines the strength of the encryption. The contrast analysis assists in determining the level of diffusion induced in the image. In general image encryption applications, it is desirable that the cipher is capable of creating high levels of contrast, whereas, in watermarking applications, the least significant bits are processed and thus the influence on the image perception is minimal. The correlation analysis determines the relationship between the original image and the watermarked image. The results of this analysis are used to quantize the changes performed in the original image. The energy analysis is also used to determine the strength of the encryption used in the watermarking process. In homogeneity analysis, the relationship of the distribution of the corresponding pixels in plain image and watermarked image is analyzed. The mean of absolute deviation analysis is a useful method in determining vulnerability of the watermark in an image. In an extension to these analyses, the majority logic criterion (MLC) is applied where the suitability of the substitution box is determined for a particular application. The results of all the analyses discussed in this section are used in MLC [3, 18].

The results of the statistical analysis used in this work are listed in Table 2.

5. Simulation Results

The proposed watermarking technique is applied to grey scale and color images, and the resulting his-

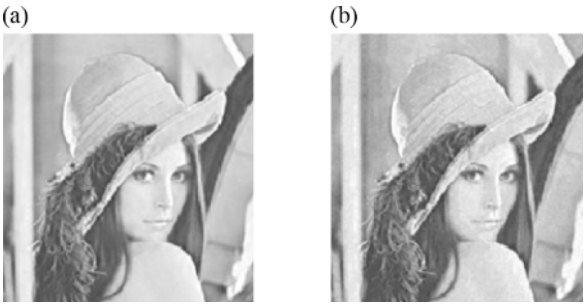

Fig. 3. Grey scale image: (a) original image and (b) watermarked image, watermarked in four LSBs by S-box.

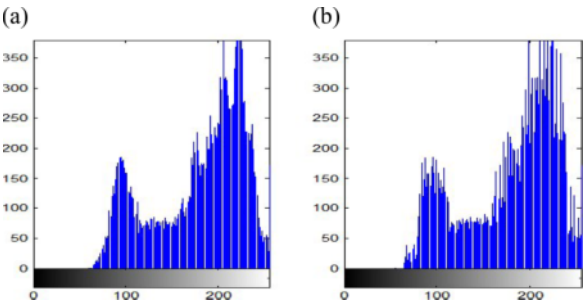

Fig. 4 (colour online). Histogram of images in Figure 3, respectively.

tograms are analyzed for comparison. The picture of Lena is used as a sample image for embedding the watermark. In Figure 3a, the original image is shown and the watermarking algorithm is applied to obtain an image shown in Figure 3b.

In Figure 4, the histograms show the distribution of intensities of pixels in the image before and after the watermarking, Figure 4a and Figure 4b, respectively. It is evident from this figure that there is little difference between the shapes of the two histograms, due to the fact that the transformation is applied only to the four LSBs of the original image.

The maximum change in the pixel intensity by the proposed watermarking algorithm is of fifteen grey levels (i. e. $2^4 - 1$), but the human eye can differentiate forty or more grey level variations, hence the distortions generated by the watermarking are virtually never perceived by the human observer.

Similar to the grey scale watermarking, Figures 5 and 6 show histograms of a coloured plain image and the corresponding watermarked image, respectively. Once again, due to the fact that watermarking is performed only to the LSBs of the image pixels, there is no perceptive change in the image.

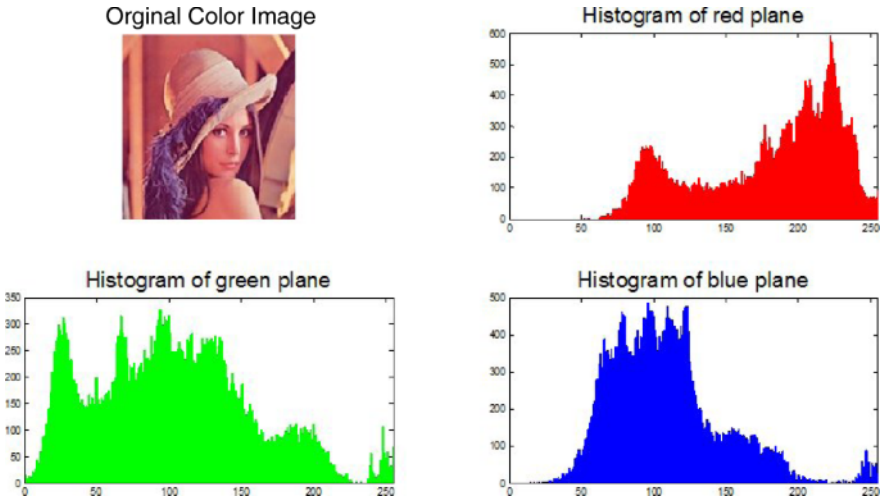

Fig. 5 (colour online). Original colour image along with histogram of each colour layer, red, green, and blue (RGB).

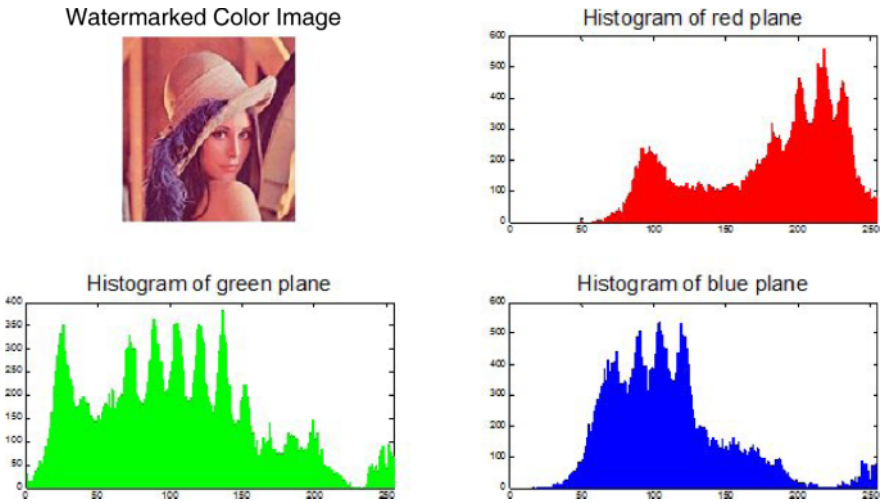

Fig. 6 (colour online). Watermarked colour image along with histogram.

Table 3. Statistical analysis used in watermarking.

Watermarking Analysis	Grey Scale Image	Colour Image
MSE	11.7755	11.6538
PSNR	86.1651	86.2689
SSIM	0.9145	0.9124

The results of mean square error analysis, peak-to-peak signal to noise ratio analysis, and structural similarity paradigm analysis are shown in Table 3. These statistical analyses are applied to the watermarked image.

6. Conclusions

The proposed algorithm is a useful algorithm in terms of content authentication and proving ownership. An attractive feature of this algorithm is the complexity and robustness in the identification of watermark by statistical methods or visual perception. The watermarking algorithms, which rely on embedding company logo or unique image templates, are relatively easy to identify, remove or modify. In this work, the presented algorithm operates on LSBs making it difficult to visually perceive any changes in the image.

[1] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, Neural Comput. Appl. (2012) doi:10.1007/s00521-012-0870-0.
[2] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, Z. Naturforsch. **67a**, 327 (2012).
[3] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, Z. Naturforsch. **67a**, 282 (2012).
[4] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, Neural Comput. Appl. (2012) doi:10.1007/s00521-012-0914-5.
[5] Y. Zaho, Dual Domain Semi-Fragile Watermarking for Image Authentication, Master's Thesis, University of Toronto 2003.
[6] J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann Pub., Elsevier Inc. 2008.
[7] M. Barni and F. Bartolini, Watermarking Systems Engineering, Marcel Dekker Inc., New York 2004.
[8] J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, IEEE Transact. Image Proc. **6**, 1673 (1997).
[9] M. Vatsa, R. Singh, A. Noore, M. M. Houck, and K. Morris, IEICE Elec. Expr. **3**, 23 (2006).
[10] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, IEEE Trans. Image Proc. **13**, 600 (2004).
[11] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, Nonlin. Dyn. (2012). doi:10.1007/s11071-012-0440-0
[12] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, Neural Comput. Appl. **21**, 377 (2012).
[13] I. Hussain, T. Shah, and H. Mahmood, Comput. Math. Appl. **64**, 2450 (2012).
[14] I. Hussain, T. Shah, and M. A. Gondal, Opt. Commun. **285**, 4887 (2012).
[15] I. Hussain, T. Shah, M. A. Gondal, and Y. Wang, World Appl. Sci. J. **13**, 2385 (2011).
[16] I. Hussain, T. Shah, M. A. Gondal, and W. A. Khan, World Appl. Sci. J. **13**, 2389 (2011).
[17] I. Hussain, T. Shah, M. A. Gondal, W. A. Khan, and M. Khan, World Appl. Sci. J. **14**, 1779 (2011).
[18] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, Int. J. Phys. Sci. **6**, 4110 (2011).
[19] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, Proc. Pakistan Acad. Sci. **48**, 111 (2011).
[20] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, Int. J. Contemp. Math. Sci. **5**, 1263 (2010).
[21] I. Hussain, T. Shah, H. Mahmood, and M. Afzal, Int. J. Comp. Appl. **2**, 975 (2010).
[22] I. Hussain, T. Shah, and K. S. Aslam, Adv. Algeb. **3**, 57 (2010).