A New Data Hiding Technique Based on Irreducible Polynomials

Wafaa Mustafa Abduallah[1*], Abdul Monem S. Rahma[2], and Al-Sakib Khan Pathan[1]
[1]Department of Computer Science, International Islamic University Malaysia, Gombak 53100, Kuala Lumpur, Malaysia
[2]Department of Computer Science, University of Technology, Baghdad, Iraq
Email: [1*]heevy9@yahoo.com, [2]monemrahma@yahoo.com, [1]sakib@iium.edu.my

***Abstract*—The mass diffusion of digital communication needs the special means of security. Cryptography concentrates on rendering the messages unreadable to any unauthorized person who might intercept those. In contrast, steganography is a method of concealing the existence of message to allow a secure communication in a complete undetectable manner. Digital image is the most common type of carrier used for steganography. This paper presents a new method for data hiding within transform domain of the color images which is based on dividing the image into blocks, then applying the proposed transform on specified blocks and hiding the secret message within them. In this way, the security can be increased since it depends on a different type of transform which is based on irreducible polynomial mathematics. According to our investigation in this area, our work for the first time uses this mechanism for data hiding. The results have proven increasing the capacity with maintaining reasonable level of imperceptibility.**

***Index Terms*— Column, Transform, Irreducible, Polynomial, Steganography**

I. Introduction

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. The term is derived from Greek which literally means "*covered writing*". It includes a wide range of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. In practice, steganography and cryptography are kind of "*cousins*" in the spycraft family. While cryptography scrambles a message to make it unintelligible, steganography hides the message itself so that it cannot be seen. A message in ciphertext, for instance, might arouse suspicion on the part of the recipient while an "*invisible*" message created with steganographic methods will not [1]. The cover media like digital images, audio files, video files, text files, executable files can be used for this purpose. Generally speaking, a good steganographic technique should have good visual imperceptibility and sufficient capacity of hidden secret data [2].

Steganography can be divided into different categories based upon the type of cover media chosen and the method of data embedding in it as shown at a glance in Figure 1, which is adopted from [3].

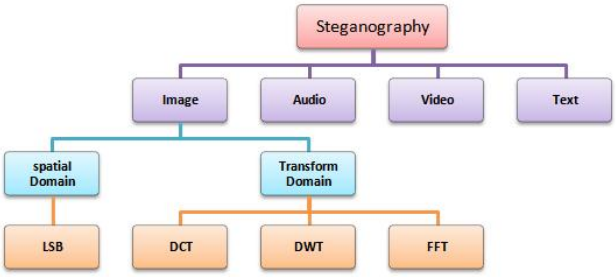

Figure 1. Various Types of Steganography Techniques.

An image steganographic scheme is one kind of steganographic systems, where the secret message is hidden in a digital image with some hiding method. It is possible to use a proper embedding procedure to embed the secret message into the cover image in such a way that it is imperceptible to a human observer. The hidden message can then be recovered using appropriate extraction procedure. The original image is called the '*cover image*' and the message-embedded image is called a '*stego-image*'. There are a number of steganographic schemes that hide secret message in a digital image. These schemes can be classified according to the method of hiding. Two popular types of hiding methods are: **spatial domain** embedding and **transform domain** embedding. The Least Significant Bit (LSB) substitution is the most commonly used spatial domain technique. The most widely used transforms are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Fast Fourier Transform (FFT) [4].

In this work, a new type of transform will be applied on the image called "*Mix Column Transform*" based on *irreducible polynomial mathematics*, which can meet the requirements of good steganographic system (i.e., high capacity, good visual imperceptibility, and reasonable level of security).

Following the introduction in Section I, in Section II we discuss some of the related works. The mathematical background of the proposed system is presented in section III. Then, in Section IV, the proposed algorithm is presented. Section V presents our results and analysis. Finally, the paper concludes in Section VI outlining the

doi:10.4304/jetwi.5.1.45-51

achievements.

II. Related Works

As noted earlier, there are two popular techniques used for image steganography in the literature: spatial domain embedding and transform domain embedding. In this section, we will look into some other works related to our approach. In [2], the authors propose a novel steganographic method based on Kohonen Neural Networks (NNs) and wavelet contrast. They embed more secret information into the dark and texture areas, and less in smooth areas. So, the proposed method hides about 1000 bytes and maintains a better visual quality of stego-image. In addition, the amount of information carried by individual pixels is decided by NNs trained, which is a secret key. Therefore, the security has been increased.

A block complexity analysis for transform domain image steganography is introduced in [5]. The authors propose works on the wavelet transform coefficients which embed secret data into the original image. In addition, the image quality has been improved through using bit plain complexity images which are obtained in embedding and extraction process.

A novel steganographic technique that combines both the spatial domain as well as the transform domain approach to achieve greater security is proposed in [6]. The authors here have chosen LSB substitution technique for spatial domain embedding and Discrete Wavelet Transform (DWT) for transform domain embedding. They also propose some technique to combine cryptography with the proposed image steganography technique. The experimental results show that the proposed steganographic technique achieves moderate embedding capacity with high level of security.

The researchers in [7] use pixel value differencing (PVD) method for secret data embedding in each of the components of a pixel in a color image. Furthermore, for providing more security, they use different number of bits in different pixel components. The results obtained with the proposed method provide better visual quality of stego-image compared to the original PVD method.

After analyzing all the relevant works and motivated by these, in this work, a new steganographic scheme based transform domain is proposed. Our adopted transform domain is different from those mentioned in the previous works since it has not been used before in steganographic technique as we have found during our investigation and literature survey. Therefore, the proposed method provides good level of security.

III. Mathematical Background: Irreducible Polynomial Mathematics

The forward Mix Column Transformation, called Mix Columns, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column [8]. The results of the Mix Column operation are calculated using $GF(2^8)$ operations. Each element of $GF(2^8)$ is a polynomial of degree 7 with coefficients in $GF(2)$ (or, equivalently Z_2). Thus, the coefficients of each term of the polynomial can take the value 0 or 1. Given that there are 8 terms in an element of $GF(2^8)$, an element can be represented by bit string of length 8, where each bit represents a coefficient. The least significant bit is used to represent the constant of the polynomial, and going from right to left, represents the coefficient of x^i by the bit b_i where b_i is i bits to the left of the least significant bit. For example, the bit string (10101011) represents ($x^7+x^5+x^3+x+1$). For convenience, a term x^i is found in the expression if the corresponding coefficient is 1. The term is omitted from the expression if the coefficient is 0. Addition of two elements in $GF(2^8)$ is simply accomplished using eight *XOR* gates to add corresponding bits. Multiplication of two elements in $GF(2^8)$ requires a bit more work. The multiplication of two elements of Z_2 is simulated with an *AND* gate. Multiplication in $GF(2^8)$ can then be accomplished by first multiplying each term of the second polynomial with all of the terms of the first polynomial. Each of these products should be added together. If the degree of the new polynomial is greater than 7, then it must be reduced modulo using one of the irreducible polynomials which are presented in Table 1. In the case of Advanced Encryption Standard (AES), the irreducible polynomial is $x^8+x^4+x^3+x+1$ [9]. So, multiplication can be performed according to the following rule [8]:

$$\mathbf{x} \times \mathbf{f(x)} = \begin{cases} (\mathbf{b_6 b_5 b_4 b_3 b_2 b_1 b_0 0}) & \textbf{if } \mathbf{b_7 = 0} \\ (\mathbf{b_6 b_5 b_4 b_3 b_2 b_1 b_0 0}) \oplus (\mathbf{00011011}) & \textbf{if } \mathbf{b_7 = 1} \end{cases}$$

TABLE 1.
LIST OF IRREDUCIBLE POLYNOMIALS [10].

No.	Irreducible Polynomial	Dec	N	Irreducible Polynomial	Dec
1	$x^8+x^4+x^3+x+1$	283	16	$x^8+x^7+x^3+x+1$	395
2	$x^8+x^4+x^3+x^2+1$	285	17	$x^8+x^7+x^3+x^2+1$	397
3	$x^8+x^5+x^3+x+1$	299	18	$x^8+x^7+x^4+x^3+x^2+x+1$	415
4	$x^8+x^5+x^3+x^2+1$	301	19	$x^8+x^7+x^5+x+1$	419
5	$x^8+x^5+x^4+x^3+1$	313	20	$x^8+x^7+x^5+x^3+1$	425
6	$x^8+x^5+x^4+x^3+x^2+x+1$	319	21	$x^8+x^7+x^5+x^4+1$	433
7	$x^8+x^6+x^3+x^2+1$	333	22	$x^8+x^7+x^5+x^4+x^3+x^2+1$	445
8	$x^8+x^6+x^4+x^3+x^2+x+1$	351	23	$x^8+x^7+x^6+x+1$	451
9	$x^8+x^6+x^5+x+1$	355	24	$x^8+x^7+x^6+x^3+x^2+x+1$	463
10	$x^8+x^6+x^5+x^2+1$	357	25	$x^8+x^7+x^6+x^4+x^2+x+1$	471
11	$x^8+x^6+x^5+x^3+1$	361	26	$x^8+x^7+x^6+x^4+x^3+x^2+1$	477
12	$x^8+x^6+x^5+x^4+1$	369	27	$x^8+x^7+x^6+x^5+x^2+x+1$	487
13	$x^8+x^6+x^5+x^4+x^2+x+1$	375	28	$x^8+x^7+x^6+x^5+x^4+x+1$	499
14	$x^8+x^6+x^5+x^4+x^3+x+1$	379	29	$x^8+x^7+x^6+x^5+x^4+x^2+1$	501
15	$x^8+x^7+x^2+x+1$	391	30	$x^8+x^7+x^6+x^5+x^4+x^3+1$	505

IV. Our Proposed Algorithm

In our work, a new type of transform will be applied on the color images to get new domain for embedding, which is more secure and can be applied for real-time applications.

A. Embedding Algorithm

The procedure of embedding is described in the following steps:

Step 1. Dividing the cover image into blocks, each block of size (4*4).
Step 2. Selecting some of the blocks for embedding the watermark according to secure key.
Step 3. Applying the proposed transform (Mix Column Transform) on each specified block individually.
Step 4. Specifying certain positions for embedding the secret message in the transformed blocks sequentially using another secret key.
Step 5. Applying an inverse transform on the transformed blocks to get back the original blocks.
Step 6. Evaluating the proposed method through using the most common measurements that have been used in the literature such as Peak Signal Noise to Ratio (PSNR) for testing the invisibility.

B. Extraction Algorithm

The proposed method is a blind algorithm so; there is no need for the original cover image during the process of extraction. To recover the secret message, the following steps should be applied:

Step 1. Dividing the stego-image into blocks, each block of size (4*4).
Step 2. Determining the selected blocks that have been used for embedding the secret message through using the same secure key.
Step 3. Applying the proposed transform on each block individually.
Step 4. Extracting the secret bits from the transformed blocks sequentially using secure key.
Step 5. Reconstructing the secret message from the extracted bits.

C. The Proposed Transform

In order to apply Mix Column Transform, it is supposed to have a block matrix taken from a cover image with size (4*4) which can be referred to as *block matrix,* and another matrix called *transformed matrix* of the same size (4*4) then, multiplying each row of the *transformed matrix* with each column of the original values of the *block matrix* as shown in Figure 2.

To perform this operation, firstly the values of both matrices should be converted to polynomial equations as shown below:

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} BF & CD & BF & 8A \\ BF & AF & C0 & AD \\ 6E & 73 & 9D & A3 \\ 85 & 82 & 89 & 86 \end{bmatrix}$$

Transformed Matrix **Block Matrix**

Figure 2. The Transformed Matrix and Block Matrix.

It is evident that the largest element appeared in this example is (x^7) because the results of the Mix Columns operation are calculated using $GF(2^8)$ operations where, each element of $GF(2^8)$ is a polynomial of degree 7 with coefficients in $GF(2)$. Thus, if the result of multiplication led to get a polynomial with degree larger than 7, then the resulted polynomial should be reduced through dividing it by the irreducible polynomial ($x^8 + x^4 + x^3 + x + 1$) to get the remainder which will be used as a resulted polynomial. So, to verify the first value 54 of the resulted matrix after applying transform in this example, it is supposed to multiply the first column of the original values of the block matrix with the first row of the transformed matrix:

$$\boldsymbol{x}.(\boldsymbol{x^7 + x^5 + x^4 + x^3 + x^2 + x + 1}) = \boldsymbol{x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x}$$

$$\boldsymbol{(x+1).(x^7 + x^5 + x^4 + x^3 + x^2 + x + 1)} = \boldsymbol{x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x + x^7 + x^5 + x^4 + x^3 + x^2 + x + 1} = \boldsymbol{x^8 + x^7 + x^6 + 1}$$

$$\boldsymbol{1.(x^6 + x^5 + x^3 + x^2 + x)} = \boldsymbol{x^6 + x^5 + x^3 + x^2 + x}$$

$$\boldsymbol{1.(x^7 + x^2 + 1)} = \boldsymbol{x^7 + x^2 + 1}$$

The result is = $\boldsymbol{x^6 + x^4 + x^2}$ → which represents (**0101 0100**) = (**54**)

The same operation can be done to get the whole values of the resultant matrix. Next, the secret message can be embedded in the least significant bit (LSB) of some of the values of the resulted matrix according to secret key randomly generated for instance; in the first and last element.

On the other hand, to get the original values of the block matrix, the resulting matrix from Mix Column Transform should be multiplied by the inverse matrix (see Figure 3, next page).

$$\begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix}$$

$$\begin{bmatrix} x^7 + x^5 + x^4 + x^3 + x^2 + x + 1 & x^7 + x^6 + x^3 + x^2 + 1 & x^7 + x^5 + x^4 + x^3 + x^2 + x + 1 & x^7 + x^3 + x \\ x^7 + x^5 + x^4 + x^3 + x^2 + x + 1 & x^7 + x^5 + x^3 + x^2 + x + 1 & x^7 + x^6 & x^7 + x^5 + x^3 + x^2 + 1 \\ x^6 + x^5 + x^3 + x^2 + x & x^6 + x^5 + x^4 + x + 1 & x^7 + x^4 + x^3 + x^2 + 1 & x^7 + x^5 + x + 1 \\ x^7 + x^2 + 1 & x^7 + x & x^7 + x^3 + 1 & x^7 + x^2 + x \end{bmatrix}$$

$$\begin{bmatrix} x^3+x^2+x & x^3+x+1 & x^3+x^2+1 & x^3+1 \\ x^3+1 & x^3+x^2+x & x^3+x+1 & x^3+x^2+1 \\ x^3+x^2+1 & x^3+1 & x^3+x^2+x & x^3+x+1 \\ x^3+x+1 & x^3+x^2+1 & x^3+1 & x^3+x^2+x \end{bmatrix}$$

$$\begin{bmatrix} x^6+x^4+x^2+x+1 & x^7+x^4+x^3+x & x^5+x^3+x & x^7+x^6+x^2+x \\ x^7+x^6+x^5+x^3+x^2+1 & x^7+x^4+x^3+x^2+x+1 & x^4+1 & x^7+x^5+x^4+x+1 \\ x^6+x^3 & x^4+x^3+1 & x^7+x^6+x^4+x^3+x^2+x & x^7+x^6+x^5+x^3+x+1 \\ x^4+x^3+x & x^7+x^3+x^2+x+1 & x^7+x^3+x^2+x & x^7+x^4+x^3+x^2+1 \end{bmatrix}$$

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} * \begin{bmatrix} 55 & 9A & 2A & C6 \\ ED & 9E & 11 & B3 \\ 48 & 19 & DE & EB \\ 1A & 8F & 8E & 9D \end{bmatrix}$$

Inverse Matrix

Figure 3. The Inverse Matrix and Block Matrix.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} B1 & CD & BF & 83 \\ B6 & AF & C0 & A0 \\ 63 & 73 & 9D & A8 \\ 8E & 82 & 89 & 88 \end{bmatrix}$$

Figure 4. The Transformed Matrix and Block Matrix.

And again all the values of both matrices should be converted to polynomial equations as explained above.

$$x + x^7 + x^6 + x^5 + x^3 + x^2 + 1$$
$$= x^{10} + x^9 + x^6 + x^4 + x^3 + x^2 + x + 1$$
$$(x^3 + x^2 + 1).(x^6 + x^3)$$
$$= x^9 + x^6 + x^8 + x^5 + x^6 + x^3$$
$$= x^9 + x^8 + x^5 + x^3$$
$$(x^3 + 1).(x^4 + x^3 + x) = x^7 + x^6 + x^4 + x^4 + x^3 + x$$
$$= x^7 + x^6 + x^3 + x$$

The result is $= x^{10} + x^9 + x^7 + x^6 + x^5 + x^3 + x + 1$ which has a degree $(10 > 7)$ so, it should be reduced through dividing it by $(x^8 + x^4 + x^3 + x + 1)$, this polynomial can be considered as a secret key because it can be changed so, the attacker cannot expect the utilized polynomial in the proposed steganographic algorithm.

$$\begin{array}{r} x^2+x \\ x^8+x^4+x^3+x+1 \;\overline{)}\; x^{10}+x^9+x^7+x^6+x^5+x^3+x+1 \\ x^{10}+x^6+x^5+x^3+x^2 \\ \hline x^9+x^7+x^2+x+1 \\ x^9+x^5+x^4+x^2+x \\ \hline x^7+x^5+x^4+1 \end{array}$$

(B1) ← (1011 0001) ←

Consequently, all other values of the original matrix can be obtained through repeating the same operation. Finally, the secret message can be retained through applying the Mix Column Transform on the final resulted matrix. As an example, taking the operation shown in Figure 4, converting to polynomials:

The first value can be got via multiplying the first row of the first matrix with the first column of the second matrix as explained below:

$$x.(x^7 + x^5 + x^4 + 1) = x^8 + x^6 + x^5 + x$$
$$(x+1).(x^7 + x^5 + x^4 + x^2 + x)$$
$$= x^8 + x^6 + x^5 + x^3 + x^2 + x^7 + x^5 + x^4 + x^2 + x$$
$$= x^8 + x^7 + x^6 + x^4 + x^3 + x$$
$$1.(x^6 + x^5 + x + 1) = x^6 + x^5 + x + 1$$
$$1.(x^7 + x^3 + x^2 + x) = x^7 + x^3 + x^2 + x$$

The result is $= x^6 + x^4 + x^2 + 1 \rightarrow$ which is equivalent to (**0101 0101**) = (**55**)

So, taking the LSB from the resulting value which represents the value of the secret bit, the original value (54) can be obtained.

V. Experimental Results and Discussion

The proposed technique is tested by using sequence of standard color images of size (512*512) with JPEG formats like (Lena, Peppers, Barbara, Baboon, and similar) as shown in Figure 5 (a, b, c, d, e, and f). and the secret information to be embedded in these images is about 7000 characters as shown in Figure 6.

The image quality of the proposed algorithm has been tested using a measurement called peak signal-to-noise ratio (PSNR), which is commonly employed in image processing research. The PSNR is estimated in decibel (dB). Table 2 and Table 3 show the results of applying proposed technique using the mentioned test images.

$$\begin{bmatrix} x & x+1 & 1 & 1 \\ 1 & x & x+1 & 1 \\ 1 & 1 & x & x+1 \\ x+1 & 1 & 1 & x \end{bmatrix}$$

$$\begin{bmatrix} x^7+x^5+x^4+1 & x^7+x^6+x^3+x^2+1 & x^7+x^5+x^4+x^3+x^2+x+1 & x^7+x+1 \\ x^7+x^5+x^4+x^2+x & x^7+x^5+x^3+x^2+x+1 & x^7+x^6 & x^7+x^5 \\ x^6+x^5+x+1 & x^6+x^5+x^4+x+1 & x^7+x^4+x^3+x^2+1 & x^7+x^5+x^3 \\ x^7+x^3+x^2+x & x^7+x & x^7+x^3+1 & x^7+x^3 \end{bmatrix}$$

(a) Lena.jpg (b) Barbara.jpg (c) Peppers.jpg

(d) Baboon.jpg (e) Parrot.jpg (f) Fruit.jpg

Figure 5. Test images for the proposed technique.

In this work, the proposed algorithm hides 7000 characters which is equivalent to 55,254 bits in the red channel of each image of the standard images as presented in Table 2. Comparing these results with [2] which only hid 1000 bytes in the cover images which is equivalent to 8000 bits (as each byte=8bit). So, it is the proof that our proposed method hides more information with maintaining good level of image quality for the stego-image which was around 40 db.

Table 3 presents the results of hiding the same amount of information in the red, green and blue colors of each image separately. The capacity payload in this case exceeds the maximum capacity that has been got by [7] which was 146,732 bits. On the other hand, the visual quality of the stego-image of our proposed method still good which is around 35db.

Moreover, the security has been increased because it uses two secret keys for embedding; one for specifying the block and the other is used for determining the pixel within the block for embedding. Besides that, the most important secure key is the utilized irreducible polynomial in the proposed scheme since we have 30 polynomials and we can use any one of those as explained earlier in Table 1 which is hard to be attacked by the intruder.

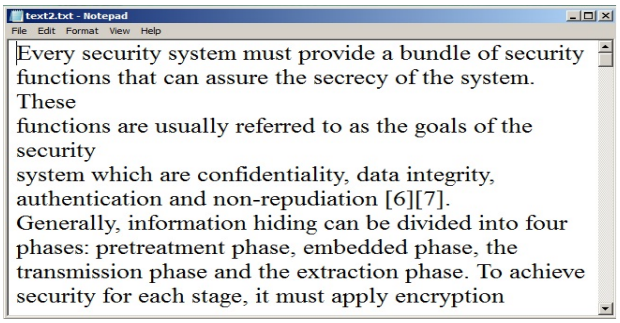

Figure 6. The Secret Message.

TABLE 2.
RESULTS OF APPLYING THE PROPOSED ALGORITHM ON THE RED CHANNEL ONLY OF EACH IMAGE.

Color Images	Message Size (Characters)	Payload (Bits)	PSNR of the Stego-image	Embedding duration time In Sec.
1. Lena.jpg	7000	55254	40.5908	78.4685
2. Barbara.jpg	7000	55254	40.8095	81.4481
3. Peppers.jpg	7000	55254	40.7339	81.2609
4. Baboon.jpg	7000	55254	40.7121	83.5385
5. Parrot.jpg	7000	55254	40.6524	82.1813
6. Fruit.jpg	7000	55254	40.6096	83.8505

(a) Lena_stego.jpg (b) Barbara_stego.jpg (c) Peppers_stego.jpg

(d) Baboon_stego.jpg (e) Parrot_stego.jpg (f) Fruit_stego.jpg

Figure 7. The stego-images after applying the proposed algorithm on the red channel only.

(a) Lena_stego2.jpg (b) Barbara_stego2.jpg (c) Peppers_stego2.jpg

(d) Baboon_stego2.jpg (e) Parrot_stego2.jpg (f) Fruit_stego2.jpg

Figure 8. The stego-images after applying the proposed algorithm on the red, green, and blue channels.

TABLE 3.
RESULTS OF APPLYING THE PROPOSED ALGORITHM ON THE RED, GREEN AND BLUE CHANNELS OF EACH IMAGE.

Color Images of size (512*512)	Message Size (Characters)	Payload (Bits)	PSNR of the Stego-image	Embedding duration time In Sec.
1. Lena.jpg	21000	165762	35.8703	247.8856
2. Barbara.jpg	21000	165762	35.9867	244.4536
3. Peppers.jpg	21000	165762	35.8396	246.8092
4. Baboon.jpg	21000	165762	35.9420	247.7296
5. Parrot.jpg	21000	165762	35.9509	243.8140
6. Fruit.jpg	21000	165762	35.8499	243.6892

Figures 7(a-f) show the stego-images after applying the proposed algorithm on the red channel only. Figures 8(a-f) show the stego-images after applying the proposed algorithm on the red, green, and blue channels.

VI. CONCLUSION

In this paper a steganographic technique is proposed based on different transform called Mix Column Transform. The proposed transform increases the security of the system since it has more than one secret key for embedding and extracting the secret message. Two types of experiments have been conducted in this work; either embedding in the red channel only or embedding in the red, green, and blue channels of each image. Both cases of embedding obtained good level of imperceptibility were PSNR values ranged between 35-40 db. In addition to that the capacity of embedding is increased compared with the existing methods. Finally, this method is also capable of extracting the secret message without the cover image.

ACKNOWLEDGMENT

This work was supported in part by NDC Lab, KICT, IIUM.

REFERENCES

[1] Johnson, N.F. and Jajodia, S., "Exploring Steganography: Seeing the Unseen", *IEEE Computer*, Volume: 31, Issue: 2, 1998, pp. 26-34.
[2] Rana, A., Sharma, N., and Kaur, A. "Image Steganography Method Based On Kohonen Neural Network", *International Journal of Engineering Research and Applications*, 2(3), 2012, pp. 2234-2236.
[3] Chutani, S. and Goyal, H., "LSB Embedding in Spatial Domain - A Review of Improved Techniques", *International Journal of Computers & Technology*, 3(1), 2012, 153-157.
[4] Kekre, H. B., Patankar, A.B., and Koshti, D., "Performance Comparison of Simple Orthogonal Transforms and Wavelet Transforms for Image", *International Journal of Computer Applications*, 44(6), 2012, 21-28.
[5] Dhanarasi, G. and Prasad, A.M., "Image Steganography Using Block Complexity Analysis", *International Journal of Engineering Science and Technology*, 4(7), 2012, 3439-3445.
[6] Joshi, S.V., Bokil, A.A., Jain, N.A., and Koshti, D., "Image Steganography Combination of Spatial and Frequency Domain", *International Journal of Computer Applications*, 53(5), 2012, 25-29.
[7] Mandal, J. K. and Das, D., "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", *International Journal of Information Sciences and Techniques*, 2(4), 2012, 83-93.
[8] Stallings, W. *Cryptography and Network Security Principles and Practice*. USA: Prentice Hall, 2006.
[9] Li, H., and Friggstad, Z., "An Efficient Architecture for the AES Mix Columns Operation", *Proceedings of IEEE International Symposium on Circuits and Systems*, Kobe, Japan, May 2005, pp. 4637-4640.
[10] Ruskey, F. Generate Polynomials. 2000. Retrieved from http://www.theory.cs.uvic.ca/~cos/gen/poly.html (last accessed December 11, 2012)

Wafaa Mustafa Abduallah received her M.Sc. in Computer Science in 2010 from University of Duhok, Iraq. She received her B.Sc. in Computer Science in 2005 from Mosul University, College of Computer Science and Mathematics, Iraq. She is currently a Ph.D. Candidate in Computer Science Department, Kulliyyah of Information and Communication Technology (KICT), International Islamic University Malaysia (IIUM), Malaysia. She previously worked as Assistant Lecturer in the College of Computer Science, Nawroz University, Duhok City, Iraq.

Abdul Monem S. Rahma was awarded his MSc from Brunel University and his PhD from Loughborough University of technology, United Kingdom in 1982, 1984 respectively. He taught at Baghdad university department of computer science and the Military Collage of Engineering, computer engineering department from 1986 till 2003. He fills the position of Dean Asst. of the scientific affairs and works as a professor at the University of Technology computer Science Department. He published 76 papers, 4 books in the field of computer science, supervised 28 PhD and 57 MSc students. His research interests include image processing, biometrics, computer security, and graphics.

Al-Sakib Khan Pathan received Ph.D. degree in Computer Engineering in 2009 from Kyung Hee University (KHU), South Korea. He received B.Sc. degree in Computer Science and Information Technology from Islamic University of Technology (IUT), Bangladesh in 2003. He is currently an Assistant Professor at Computer Science department in International Islamic University Malaysia (IIUM), Malaysia. Till June 2010, he served as an Assistant Professor at Computer Science and Engineering department in BRAC University, Bangladesh. Prior to holding this position, he worked as a Researcher at Networking Lab, KHU, South Korea till August 2009. His research interest includes wireless sensor networks, network security, and e-services technologies. He is a recipient of several awards/best paper awards and has several publications in these areas. He has served as a Chair, Organizing Committee Member, and Technical Program Committee member in numerous international conferences/workshops like HPCS, ICA3PP, IWCMC, VTC, HPCC, IDCS, etc. He is currently serving as the Editor-in-Chief of IJIDCS, an Area Editor of IJCNIS, Editor of IJCSE, Inderscience, Associate Editor of IASTED/ACTA Press IJCA and CCS, Guest Editor of some special issues of top-ranked journals, and Editor/Author of eight books. He also serves as a referee of some renowned journals. He is a member of Institute of Electrical and Electronics Engineers (IEEE), USA; IEEE Communications Society (IEEE ComSoc), USA, and IEEE ComSoc Bangladesh Chapter, and several other international organizations.