IJCCCE Vol.13, No.2, 2013

A Technique for Image Steganography Based on Optimal Resilient Boolean Functions and DCT

Azhar Malik

Computer Engineering Dept., University of Technology, Baghdad – Iraq
azharmalik1310@yahoo.co.uk

Received: 12/5/2013
Accepted: 12/11/2013

Abstract: One of the methods introduced for accomplishing hidden communication is the steganography technique. Steganography is an important area of research in recent years involving a number of applications. It is the science of embedding information into the cover image, text and video without causing statistically significant modification to the cover image. This paper proposes an image steganography system; it hides the gray level image on another gray level image by using optimal resilient Boolean functions. First, it starts by encrypting secret image by using optimal resilient function then embedding encrypted image inside a cover image by using DCT. The new proposal system of image encryption has been investigated by encrypting the powerful frequency coefficients in DCT using a saturated best resilient Boolean function (SRB) that constructed by Zhang's construction. The simulation results of the proposal system have calculated the peak signal to noise ratio (**PSNR)** and the correlation test in order to compare between the cover image and the stego image and the results have also calculated the correlation test between the secrete image and the extraction image as a parameter of robustness. The experimental results have showed that the images can be embedded by steganography and optimal resilient Boolean function with smaller correlation compared to the original secret image and the extraction image. Finally, it is observed that for all images, PSNR is greater than 55.

Keywords: Steganography, Image encryption, optimal resilient Boolean function (RB), Discrete Cosine Transform (DCT) and echo hiding.

1. Introduction

Steganography comes from Greek words steganos (covered or secret) and the graphy (writing). Steganography in these days refers to information or a file that has been concealed inside a digital picture, video or audio file [1]. The purpose of steganography is not to keep others from knowing the hidden information; it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has been failed [2]. Figure (1) shows the block diagram of a simple steganographic method.

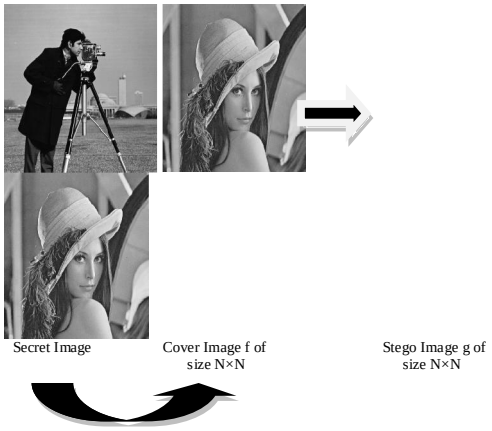


Figure. 1 The block diagram of a simple steganographic system

There are two levels of security for digital image encryption: low level and high-level security encryption. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all. Selective encryption aims to avoid the encryption of all bits of a digital image and yet ensuring a secure encryption [3].

Stream cipher cryptosystems [4] are extensively used to provide a reliable and efficient method of secure communication. In the standard model of stream cipher the outputs of several independent Linear Feedback Shift Register (LFSR) sequences are combined using a nonlinear Boolean function to produce the key stream as shown in Fig.(2).

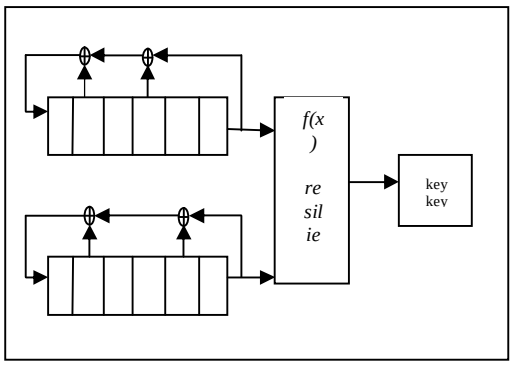


Fig. (2) Stream cipher (resilient Boolean function (RB))

It is generally accepted that for a Boolean function to be used in stream cipher system it must satisfy several properties such as high algebraic degree, high nonlinearity, and high order of resiliency [5]. By an $(n,m,d,\ nl(f))$ function which means an n-variable, m-resilient, with degree d and nonlinearity $nl(f)$.

In this paper, a frequency domain steganography technique has been proposed for hiding a large amount of data with high security, a good invisibility and no loss of secret encryption image. The basic idea to hide information in the frequency domain is to alter the magnitude of all of the DCT coefficients of the cover image. The (8*8 blocks) 2-D DCT converts the image blocks from spatial domain to frequency domain.

2. Related Work

Po-Yueh Chen*, Wei-En Wu [15] proposed a modifying scheme to improve the side match method. The major merit of the proposed method is the increase of the embedding capacity without scarifying the image quality. The experimental results ensure the superiority of the proposed modifications. Like the original sides match method, it also provides respectable security since the embedding procedures are not as straight as the LSB scheme. Babita Ahuja and Manprecet Kaur [2] proposed an image based on steganographic algorithm named as High Capacity Filter Based Steganography (HCFBS) that combines Least Significant Bit (LSB) method for data hiding, and the filtering techniques for image enhancement. A. Nag, and D. Sarkar [11] proposed a novel technique for image steganography based on Block-DCT and Huffman encoding. H.S. Manjunatha [14] proposed High Capacity and Security Steganography using Discrete Wavelet Transform (HCSSD).

3. Methods of Concealing Data in Digital Images:

3.1 Echo Hiding:

In this method the secret image is embedded into cover as an echo. Three parameters of the echo of the cover signal namely amplitude, decay rate and offset from original signal are varied to represent the encoded secret binary message. The original cover image represented by C(m,n) and (m,n) are the row and column indices of the pixels, respectively. The binary secret image denoted by M(m,n) is embedded into the cover. M(m,n) is defined over the same domain as the host C(m,n). The stego-image signal is represented by equation (1) [6].

$$S(m,n) = C(m,n) + \alpha(m,n)M(m,n) \quad ....(1)$$

where α is a scaling factor.

3.2 Discrete Cosine Transform (DCT)

The Discrete Cosine Transform (DCT) is a mathematical transformation that takes a signal and transforms it from spatial domain into frequency domain. Eq. (2) is resulting a block with the same dimension, containing the DCT coefficients [7].

$$X(i,j) = \frac{1}{\sqrt{2n}} c(u)c(v) \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} x(i,j) \cos\left(\frac{(2i+1)u\pi}{2n}\right) \cos\left(\frac{(2j+1)v\pi}{2n}\right) \quad ..... (2)$$

Where:

$$c(u), c(v) = \begin{cases} \frac{1}{\sqrt{2}} & u,v = 0 \\ 1 & u,v \neq 0 \end{cases}$$

x(i,j): image in spatial domain (pixel)
n: sub-block dimension.

3.3 Stream Ciphers

Stream ciphers form an important class of symmetric-key encryption schemes. Stream cipher cryptosystems [4] are extensively used to provide a reliable and efficient method of secure communication. In the standard model of stream cipher the outputs of several independent Linear Feedback Shift Register (LFSR) sequences are combined using a nonlinear Boolean function to produce the key stream as shown in Fig.(2).

Boolean functions play a central role in the design of most symmetric cryptosystems and in their security. There are several construction methods for constructing resilient Boolean functions. The most common of all is the Maiorana-McFarland construction technique [8].

The purpose of the nonlinear combining function f is to make the key stream difficult for the cryptanalyst to predict. According to the correlation attacks, the strength of stream cipher systems depends on the selection of the RB functions. If these functions are not chosen properly then the whole system is susceptible to a divide–and–conquer attacks. A notion of optimality for resilient Boolean functions provides better security against correlation attacks.

4. A Notion of Optimality

Motivated by Theorem (1) [4], a notion of optimality for resilient Boolean functions provides better security against correlation attacks. This notion consists of *two classes* of resilient functions: **Type-I** and **Type-II** optimal resilient functions.

Given an *n*-variable function, *m*-resilient with algebraic degree *d* and nonlinearity $nl(f)$:

- An $(n, m, d, nl(f))$ function is said to be **Type-I** optimal if $nl(f)$ is the upper bound on *nl(n,m)* provided in Theorem (1).
- An $(n, m, d, nl(f))$ function is said to be **Type-II** optimal if the function is Type-I optimal and further for any $p > m$ the upper bound on *nl(n,p)* in Theorem (1) [4] is strictly less than $nl(f)$.

5. Saturated Best Resilient Function (SBR)

The best function is said to be ***saturated*** if its spectra is three valued according to corollary (1) **[4]**. Thus an $(n, m, n-m-1, nl(f))$-function is called *optimal saturated best* resilient function (**SBR**) if it's best function and its spectra are three valued. For such a function, must necessarily have $m > \left\lfloor \frac{n}{2} \right\rfloor - 2$.

These optimal **SBR** functions are better than the resilient functions in designing stream cipher systems because it achieves trade off among the parameters: *number of variables, order of resiliency, algebraic degree* and *nonlinearity*.

Consider a 2-resilient Boolean function of 6-variables with nonlinearity 24, (6 , 2 , 3 , 24) that are constructed by Zhang & Zheng's construction method:

$$f(x_1,\ldots,x_6) = x_1 \oplus x_2 \oplus x_3 \oplus x_2x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6 \oplus x_2x_5x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \quad \ldots(3)$$

This function is Type-I optimal since $nl(f) = 24$ is the upper bound on *nl(n,m)* provided in Theorem (1) [4].

Moreover, for any $p=3 > m$, the upper bound on *nl(n,p)* is $16\,(2^{n-1} - 2^{p+1})$ which is strictly less than $nl(f) = 24$. Then it is Type-II optimal function.

These notions of optimality can be further strengthened by requiring the degree to be the maximum possible $d=n-m-1$.

Thus $(n, m, n-m-1, nl(f))$ Type-II optimal functions achieve the best possible trade-off among the parameters: *number of variables, order of resiliency, algebraic degree and nonlinearity*. Type-II optimal resilient functions achieve the maximum possible algebraic degree n-*m*-1, which are called the ***best functions*** [**4**].

The way of defining the notion of optimality is not guaranteed whether it is possible to construct functions satisfying the notions of Type-I and Type-II optimality introduced above. The tightness of the upper bounds in Theorem

(1) [4] is dependent on the existence of such functions. Function *(3)* has been used to encrypt image in this proposed system.

6. The Proposed system

The embedded system block diagram is shown in Fig.(3). The proposed algorithm based on decomposed the image into n×n sub-blocks, the coefficients of 2-dimension DCT (2DCT) re-arranges into vector by zigzag order, then the DCT coefficients of the image block are encrypted using optimal resilient Boolean functions (stream cipher). In this paper, a frequency domain steganography technique is used based on echo hiding for hiding a large amount of data with high security, a good invisibility and no loss of secret image as implement in the embedded algorithm.

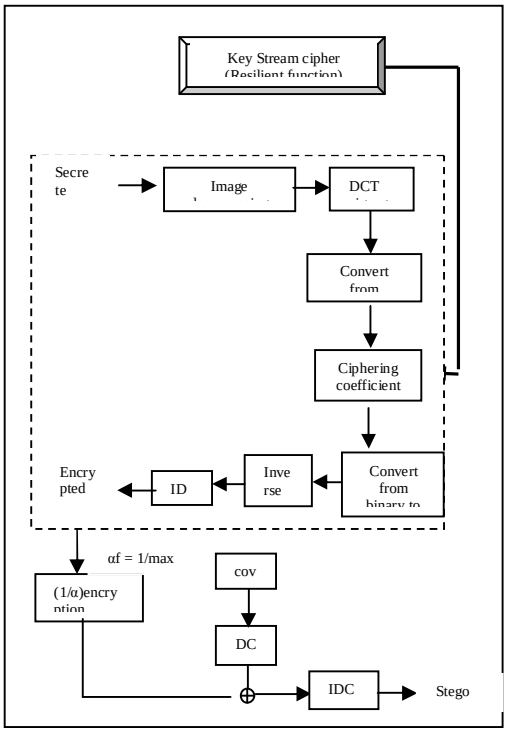


Figure (3) Block diagram of Stegano System

Embedded Algorithm

Input : Cover Image file, Secret image file
[Gray level file Bmp or JPG format.
- Resilient Boolean function
(Stream cipher)].

Output: Stego-image file.

BEGIN

Step 1: Select the secret image.

Step 2: OPEN Secrete image file.
OPEN Stream cipher file.

While (secret image and stream cipher) file **do**

- **OPEN** secret image file M(i,j).
- **OPEN** stream cipher file X(k).
- Divide image into n×n sub-block
- Apply 2DCT to sub-block M(u,v).
- Convert into vector (W) by zigzag order then convert into corresponding K bits $W_b(u)$ as shown in Fig.(4).
- Encrypte the selected coefficients by XORing the generated bit stream don't used sign bit $W_E(u)$ after divide into sub-block K bit.

$$W_E(u) = W_b(u) \oplus X(k).$$

- Convert from K bit into decimal Y(u).
- Convert vector Y(u) into 2-Dim. matrix Y(u,v) by Zigzag order.
- Perform an inverse DCT (IDCT) y(i,j) to generate encrypted image.

End

Close secret image file.

Close stream cipher file**.**

Close encrypted image file.

Step 3: Open cover image file C(i,j)

- Divide image into n×n sub-block.
- Apply 2DCT to sub-block C(u,v).
- Calculate
  S(i.j)=DCT C(i,j) +(1/αf)*Y(i,j).
- Inverse DCT S(I,j) =Stg(i,j).
- Output Stg(i,j)

Close stegano image file.

END

7. Extraction of the Secret Image

The stego-image is received in spatial domain. DCT is applied on the stego-image using the same block of size 8 × 8 to transform the stego-image from spatial domain to frequency domain. The size of the encoded bit stream and the encoded bit stream of secret image are extracted along with the resilient function of the

secret image. The block diagram of the extracting process is given in Fig.(4) and the extracting algorithm is also given as follows:

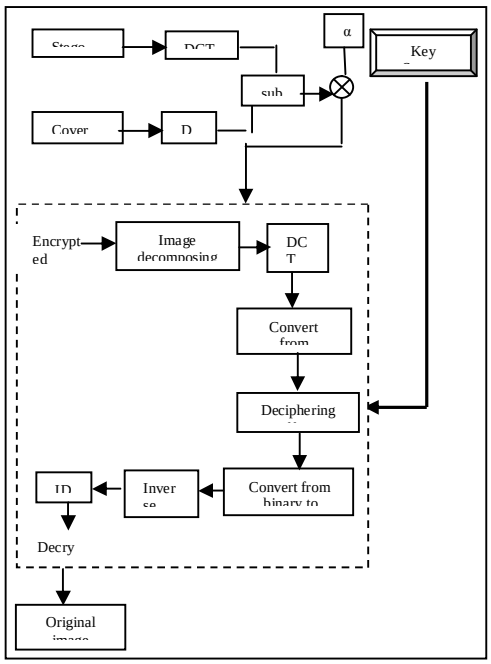


Figure (4) Block diagram of the extracting algorithm

Extraction Algorithm

Input: Stego-image.

Output: Secret image.

(1) Divide the stego-image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks of the stego-image.

(2) Divide the cover-image into non overlapping blocks of size 8×8 and apply DCT on each of the blocks of the cover-image.

(3) Apply subtraction on steps (1) and (2).

(4) Multiply the result in step (3) by (αf).

(5) Obtain encryption (secrete) image

(6) **Input:** - encryption image file JPG format.

- Resilient Boolean function (Stream cipher) (Mat format).

Output: decrypted Image.

BEGIN

OPEN encrypted image file.

OPEN stream cipher file.

While not eof (encrypted image and stream cipher) file

do

- **OPEN** encrypted image file y(i,j).
- **OPEN** stream cipher file X(k).
- Divided encrypted image into n×n sub-block
- Apply 2DCT to sub-block Y(u,v).
- Convert into vector (V) by zigzag order then convert into corresponding K bits $V_b(u)$.
- Encrypted the selected coefficients by XORing the generated bit stream don't used sign bit $V_E(u)$ after divide into sub-block K bit.

$V_D(u) = V_b(u) \oplus X(k)$.

- Convert from K bit into decimal X(u).
- Convert vector X(u) into 2-Dim. matrix M(u,v) by Zigzag order.
- Perform an inverse DCT (IDCT) x(i,j) to generate decrypted image.

End

Close encryption image file.

Close stream cipher file**.**

Close decrypted image file.

END

End.

Algorithm represents embed function for a 8x8 block nonoverlabing example in MATLAB® code

```
functionYstg = Embed(xa,xa1)
xa=imresize(xa,[192,192]); % secrete image
xa1=rgb2gray(xa1);
xa1=imresize(xa1,[192,192]); % cover image
[R,C]=size(xa);
k=1;
fori=1:8:R
for j=1:8:C
    Y(i:i+7,j:j+7)=dct2(xa(i:i+7,j:j+7)); %
Discrete cosine transform
Y1(k:k+63)=zmat2vect(Y(i:i+7,j:j+7)); %
Convert into vector by zigzag
    k=k+64;
end
end
encyr % this function in order to generate key
using resilient  Boolean functions
V=1;k=1;ss=1;
fori=1:R*C
ss=ss+1;
YB(k:k+11)=de2bi(round(abs(Y1(i))),12);
Convert  to binary and shift using round
if(ss==64)
ss=1;
    V=1;
```

```
end
if(ss<=64&&V<=6)
     YB(k:k+11)=xor(YB(k:k+11),fx);% encrypt
screte sub image with resilient key using xor
function
     V=V+1;
end
 k=k+12;
end
k=1;
fori=1:R*C
    YR(i)=(bi2de(YB(k:k+11)))*sign(Y1(i));%
convert  vector  into decimal
   k=k+12;
end
k=1;
fori=1:8:R
for j=1:8:C
YR1(i:i+7,j:j+7)=zvect2mat(YR(k:k+63));

YR2(i:i+7,j:j+7)=round(idct2(YR1(i:i+7,j:j+7)));
% inverse DCT
      k=k+64;
end;
end;
df=1/max((mat2vect(YR2)));
fori=1:8:R
for j=1:8:C
      Ystg1(i:i+7,j:j+7) =dct2(xa1(i:i+7,j:j+7));%
Yst(i:i+7,j:j+7)=df*(YR2(i:i+7,j:j+7))+Ystg1(i:i+
7,j:j+7);% function to stegano operation
Ystg(i:i+7,j:j+7) =idct2(Yst(i:i+7,j:j+7));  %
stagano image
End
End
end  function
```

Peak Signal to Noise Test (PSNR)

The measurement of the quality between the cover image *f* and stego image *g* of size N×N that shown in Fig.(1) is defined below. PSNR is expressed in [9].

$$PSNR = 10\log_{10}\frac{(S)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[C(i,j)-S(i,j)\right]^2} \quad ...(4)$$

where:
C: cover image.
S: stegano image.

$$S^2 = \sum_{i=1}^{M}\sum_{j=1}^{N} S^2(i,j)$$

The larger PSNR indicates higher image quality i.e. there is only little difference between the cover image and the stego image. On the other hand, a smaller PSNR means there is huge distortion between the cover image and the stego image.

The Similarity Test

Similarity test is the correlation compared between cover image and stego image as a parameter of robustness, and between secrete and extraction image as a parameter of quality in reconstruct image.

The correlation can be calculated as shown below [10]

$$Corr. = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(c(i,j)-\bar{c})(s(i,j)-\bar{s})}{\sqrt{\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(c(i,j)-\bar{c})^2\right]\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(s(i,j)-\bar{s})^2\right]}} \quad ...(5)$$

where:
M and N: the height and width of the two images (because the two images must be of the same size).

i and *j*: row and column numbers.
c(i, j): the cover image.
s(i,j): stegano image.
$\bar{c}, \bar{s}$: mean of cover and stegano image, respectively, which is calculated by

$$\bar{c} = \frac{\sum_{i}^{M}\sum_{j}^{N} c(i,j)}{M \times N} \quad ...(6)$$

$$\bar{s} = \frac{\sum_{i}^{M}\sum_{j}^{N} s(i,j)}{M \times N} \quad ...(7)$$

8. Simulation Results

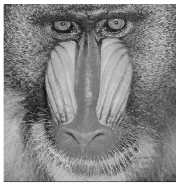
In this section, some experiments are carried out to prove the efficiency of the proposed scheme. The proposed method has been simulated using the MATLAB 2009 program. A set of 8- bit grayscale images of size 192 × 195 are used as the cover image to form the stego-image. The new proposed system image encryption

has been investigated by encrypting the powerful frequency coefficients of the secret image (cameraman) in DCT by using DCT and optimal saturated best resilient Boolean function that constructed by Zhang's construction and then embedded this encrypted image inside four cover images (Lenna, Babban, Airplane and Boat) by using steganography based Echo hiding.

In the Embedded and Extraction Algorithms the output of the key (12 bits) should be known, so this type of stegano hiding with gray image is non-blind.

Figure (5 (a – d)) shows the original cover (carrier) images, Fig.(5-e) shows the original secret image and Fig.(5-f) shows the encrypted of secret image.

(a) Lena

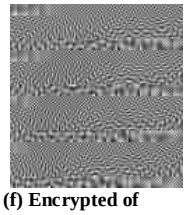


(b) Babban

(c) Airplane

(d) Boat

(e) Secret image



(f) Encrypted of secret image

Figure (5) Four cover-image for simulations

The hiding capacity of secret images is about 3×10^4 bits into a 192 × 195 cover (carrier) image. Here, 8-bit grayscale image of size 192 × 195 embedded into an 8-bit grayscale images. Table (1) exhibits the capacity, correlation test and PSNR of four cover and stego images.

From table (1), it is observed that for all images, PSNR is greater than 55 and the hidden capacity is about 299520 bits.

Table (2) shows the correlation test between secret and extraction image (cameraman).

Table (3) shows that the PSNR of our proposed algorithm is better than the one in reference [11].

Table (1) The PSNR and correlation of cover and stego four images (capacity 299520).

Images	Corr.	PSNR
Lenna	0.9977	55.4715
Babban	0.9963	55.4716
Airplane	0.9976	55.4715
Boat	0.9998	55.4716

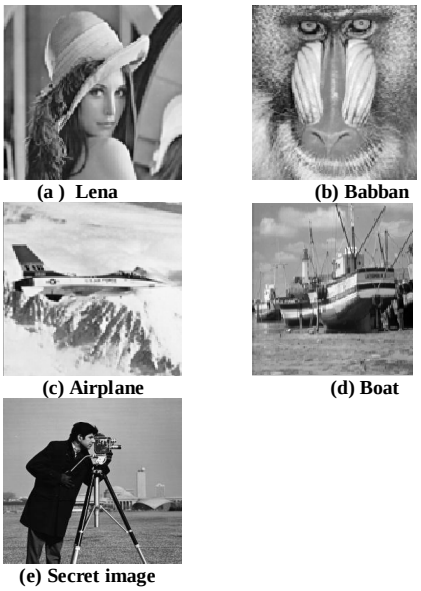
Table (2) The correlation between secret and extraction image (Cameraman).

Images	Corr.	PSNR
Lenna	0.994	52.0731
Babban	0.983	53.0731
Airplane	0.996	57..0731
Boat	0.999	55.0731

Table (3) The PSNR of cover and stego. comparison with an algorithm in reference [11].

Images	PSNR Algorithm in reference [11]	PSNR Proposed algorithm
Lenna	50.48	55.4715
Babban	50.28	55.4716
Airplane	50.91	55.4715
Boat	50.36	55.4716

Figure (6 (a - d)) shows the resulted stego-images of the proposed methods. Fig.(6 - e) also shows the original secret image retrieved from the stego-images.



(a) Lena **(b) Babban**

(c) Airplane **(d) Boat**

(e) Secret image

Figure (6) Stego-images of the proposed method

The experimental results show embedding the images by steganography and optimal resilient Boolean function with smaller correlation which compared between original secret image and extraction image. Also it is observed that for all images, PSNR is greater than 55.

9. Conclusion

In this paper, a steganography process in frequency domain has been proposed to improve security and image quality. The experiment results show that it is possible to encrypt the image by optimal resilient Boolean function with smaller correlation compared with the original image then embedded this encrypted image by using steganography based Echo hiding and reconstruct the image by decipher algorithm with high fidelity criteria (PSNR) and correlation test.

It is observed that for all images, PSNR is greater than 55 and the hidden capacity is about 299520 bits. Also the correlation test between secret and extraction image (cameraman) is smaller. This result provides additional layers of security by means of transformation (2-dim DCT and Inverse DCT) of cover image and optimal resilient Boolean functions of secret image which keep images away from destroying.

References

[1] Dr. Ekta Walia, Payal Jain and Navdeep, “An Analysis of LSB and DCT based Steganography”, Global Journal of Computer Science and Technology, Vol.10 Issue 1 (Ver 1.0), April 2010.

[2] Babita Ahuja and Manprecet Kaur, “High Capacity Filter Based Steganography”, International Journal of Recent Trends in Engineering, Vol.1, No.1, May 2009.

[3] Fonteneau C., Motsch J., Babel M., and D´eforges O., "A hierarchical selective encryption technique in a scalable image codec", International Conference in Communications, Bucharest, Romania 2008.

[4] P. Sarkar, & S. Maitra, “New Directions in Design of Resilient Boolean Functions”. Cryptology ePrint Archive: Report 2000/009, Mar. 22, 2009 www.IVSL.org.

[5] P. Sarkar and S.Maitra, "Construction of Nonlinear Resilient Boolean Functions Using Small Affine Functions". IEEE Transactions on Information Theory 50(9): 2185-2193 (2004) www.IVSL.org.

[6] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal, “Steganography and Steganalysis: Different Approaches”. 13 Aug, 2011. www.IVSL.org.

[7] C. Coconu, V. Stoica, F. Ionescu, and D. Profeta, "Distributed implementation of discrete cosine transform algorithm on a network of workstations", Proceedings of the International Workshop Trends & Recent Achievements in IT, Romania, pp. 116-121, May 2002.

[8] Qichun Wang, Jie Peng, Haibin Kan and Xiangyang Xue. “Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials”, IEEE Transactions on Information Theory ISSN, Vol. 57, ISSUe:7 page, 2011 www.IVSL.org.

[9] L.R. Hussain, "Image Identification Using DSP Techniques", PH.D., Thesis. Computer Science dept. College of Science, University of Technology, 2002.

[10] Eugene T. Lin and Edward J. Delp "Review of Data Hiding in Digital Images" Purdue University, west Lafayehe, Indiana, 1999.

[11] A. Nag, S. Biswas, D. Sarkar, P.P. Sarkar, "A Novel Technique for Image Steganography based on Block-DCT and Huffman Encoding", International Journal of Computer Science and Information Technology, Vol.2, No.3, June 2010 www.IVSL.org.

[12] Shahana T "A Secure DCT Image Steganography based on Public-Key Cryptography", International Journal of Computer Trends and Technology (IJCTT), Vol.4, Issue 7-July 2013.

[13] Shahana T "An Enhanced Security Technique for Steganography using DCT and RSA", International Journal of Advanced Research in Computer Seince and software Engineering, Vol.3, Issue 7-July 2013.

[14] H.S. Manjunatha Reddy, K.B. Raja "High Capacity and Security Steganography using Discrete Wavelet Transform" International Journal of Computer Science and Security 01/2009.

[15] Po-Yueh Chen*, Wei-En Wu "A Modified Side Match Scheme for Image Steganography" International Journal of Applied Science and Engineering 7, 1: 53-60 2009.