Image Encryption using Resilient Boolean Function and DCT

Dr. Hussam A. Darweesh*, Dr. Ekbal H. Ali*
&Azhar Malik*

Received on: 24/4/ 2011
Accepted on: 21/7/ 2011

Abstract

The information security is becoming more important in data storage and transmission, where images are widely used in it. The Stream cipher cryptosystems are extensively used for provide a reliable and efficient method of security. The new propose system image encryption investigated by encrypt the powerful frequency coefficients in DCT by used saturated best resilient Boolean function that constructed by Zhang's constructions that implement Maiorana-McFarland like constructions technique and its modifications. The simulation results of the proposal system calculate correlation test ***(Corr1)*** and **PSNR1** to compare between original and encrypted image as parameter of robustness, and correlation test ***(Corr2)*** and **PSNR2** as correlation parameter between original and decrypted image as parameter of quality in reconstruct image.

Keywords: Image encryption, discrete cosine transform (DCT), resilient Boolean function (RB), Zhang's constructions, and Maiorana-McFarland

تشفير الصور باستخدام الدوال البوليانية الطيعة مع الـ DCT

الخلاصة

اخذت امنية المعلومات اهمية كبيرة خصوصا في خزن ونقل المعلومات ومن ضمنها الصور, و تجهزنا انظمة التشفير الانسيابي بطرق اكثر دقة وموثوقية لتشفير المعلومات وبامنية عالية. ان النظام المقترح لتشفير الصورة يتحقق عن طريق تشفير معاملات التردد القليلة والتي تكون ذات معلوماتها مهمه في (DCT) باستخدام الدوال البوليانية المرنة او الطيعة ذات الاشباع العالي (SRB) التي تبنى بطريقة (Zhang’s construction) والتي تستخدم تقنية الـ (Maiora-Mcfarland). ان برنامج المحاكاة لهذا النظام المقترح يقوم بحساب (Corr1) و PSNR1 كعامل لدقة الصورة الاصلية مع الصورة المشفرة, كما يقوم بحساب (Corr2) و PSNR2 كعامل ارتباط بين الصورة الاصلية والمسترجعة.

1. Introduction

Theinformation security is becoming more important in new word special in transmit data, where the images are widely used in several processes. Image encryption plays a significant role in the field of information hiding image hiding or encrypting

methods and algorithms range from simple spatial domain

methods to more complicated and reliable frequency domain ones. It is argued that the encryption algorithms, which have been originally developed for text data, are not suitable for securing

* Computer Engineering Department, University of Technology /Baghdad

https://doi.org/10.30684/ etj.29.12.14
University of Technology-Iraq, Baghdad, Iraq/2412-0758

many real-time multimedia applications because of large data sizes. Software implementations of ciphers are usually too slow to process image and data in commercial systems [1]. A major recent trend is to minimize the computational requirements for secure multimedia distribution by "*selective encryption*" where only parts of the data are encrypted.

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 at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption [2].

Stream cipher cryptosystems [3] are extensively used for 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.(1).

Construction of resilient Boolean functions (**RB**) has been an interesting research area from mid 1980. Siegen haler was the first to point out that if the Boolean function is not chosen properly then the whole system is susceptible to divide-and-conquer attack [4]. The Walsh transform is an important tool was used for the analysis of Boolean functions. 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 we mean an *n*-variable, *m*-resilient, with degree *d* and nonlinearity $nl(f)$.

The new propose system select DC and AC coefficients from DCT sub-blocks image by zigzag permutation applicable as shown in Fig.(2) for encryption. The cipher Key that encrypt the coefficients of DCT has been generated by resilient Boolean function, which given perfect desirable properties to with stand crypt analysis attacks.

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. In Eq. (1) resulting a block with the same dimension, containing the DCT coefficients [6].

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

Where:

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

X (i,j): image in spatial domain (pixel)

n: sub-block dimension.

3. Stream Ciphers

Stream ciphers form an important class of symmetric-key encryption schemes. Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry. In situations where transmission errors are highly probable, stream ciphers are advantageous because they have limited or no propagation [7].

Linear Feedback Shift registers (LFSRs) are used in many of the keystream generators due to several reasons:

-They are well-suited to hardware implementation.

-They can produce sequences of large periods. -They can produce sequences with good statistical properties.

4. Cryptographic Boolean unctions

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 these 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. Such a function should posses certain desirable properties to withstand known cryptanalytic attacks. These important properties are resiliency, algebraic degree and nonlinearity. Construction of resilient Boolean functions achieving the upper bound on nonlinearity can show by [3]

$$x = (x_1,...,x_n),$$

$$\omega = (\omega_1,...,\omega_n) \quad ....(2)$$

both belong to $\{0,1\}^n$ and

$$x.\omega = x_1.\omega_1 \oplus ... \oplus x_n.\omega_n \quad ...(3)$$

Let $f(x)$ be a Boolean function on n-variables. Then the ***Walsh transform*** of $f(x)$ is a real valued function that can be defined as

$$W_f(\omega) = \sum_{x\in\{0,1\}^n} (-1)^{f(x)\oplus x.\omega} \quad (4)$$

The *linear complexity* of an infinite binary sequence *s*, denoted L(*s*), is defined as follows **[7]**

- if *s* is the zero sequence *s* = 0, 0, 0, … , then L(***s***) = 0

- if no LFSR generates *s*, then L(***s***) = ∞

-otherwise, L(***s***) is the length of the shortest LFSR that generates ***s***.

5. Properties of the Cryptographic Boolean Functions

For practical stream cipher systems, security is judged by the ability of the system to guard against the currently known attacks. Cryptographic Boolean functions must have ***high algebraic degrees***. High algebraic degree provides high linear complexity of the resulting key stream [5]. The minimum Hamming distance between f and all affine functions must be *high*. This is called the ***nonlinearity*** of n-variable function f and denoted by

$$nl(f) = \min_{g\in A(n)} (d(f, g)) \quad ..(5)$$

Where

A(n): set of all n-variable affine functions.

n-resilient: ***resiliency*** order of f

Cryptographic functions must be *balanced* for avoiding statistical dependence between the input and output, which can be used in attacks. Only resilient functions are of practical interest as cryptographic functions **[3].**

6. Construction the sequences of saturated Best Resilient Function SBRS (*i*)

The construction of the sequences of saturated best resilient functions has been presented, in define of SBRS function, that an SBRS must be an SBR function [3].

Let $f_{i,j}$ be a *j*-th function of SBRS(*i*). Then the function

$$f_{i,j+1} = X \oplus f_{i,j} \;\ldots\ldots\; (6)$$

Where

X : is the $f_{i,j+1}$ function of SBRS(*i*) (does not in $f_{i,j}$).

Consequently, if one can construct $f_{i,j}$, then one can construct $f_{i,k}$ for all $k > j$.

For SBRS(1), it is easy to construct $f_{1,1}$ and since $f_{1,0}$ is (5,1,3,12) (i.e. 5-varaibles,1-resilient, 3-degee, 12-nonlinearity) SBR function. Note that all functions in SBRS(*i*) have the same degree **2+*i***.

This shows that if one can construct any one of the functions in SBRS(*i*), then it is possible to construct any function in the succeeding part of the sequence with increase number of variable, resiliency, nonlinearity and same the degree and this due to make the keystream difficult for the cryptanalyst to predict. Thus it is enough if the initial function of each sequence is constructed.

To construct the function (6,2,3,24), we take an initial (5,1,3,12) SBR function which construct by Zhang's constructions:

$$f_1(x_1,\ldots,x_5) = x_2x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_5 \oplus x_3x_5 \oplus \mathrm{x}_1 \oplus x_2 \oplus x_3 \quad (7)$$

This function can be testing by using Walsh transform to ensure that it is 1-resilent Boolean function.

$$f_2(x_1,\ldots,x_6) = f(x_1,\ldots,x_5) \oplus \mathrm{X}_6 \quad .\ (8)$$

Then

$$f_2(x_1,\ \ldots,x_6) = x_2x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_5 \oplus x_3x_5 \oplus \mathrm{x}_1 \oplus x_2 \oplus x_3 \oplus x_6 \quad (9)$$

Then $nl\ (f_{0,1}) = 2nl\ (f_{0,0}) = 24$ according to theorem 2 in [3] **.** Then the function (6,2,3,24) is SBR function. Table (1) shows some resilient functions.

Consider the 3-resilient function f_3 with 7-variables, nonlinearity 48 and algebraic degree 3 (7, 3, 3, 48) that are obtained from f_2 .

$$f_3(x_1,\ \ldots,x_7) = f_2(x_1,\ \ldots,x_6) \oplus x_7$$

$$f_3(x_1,\ \ldots,x_7) = x_2x_4x_5 \oplus x_1x_4 \oplus x_1x_5 \oplus x_2x_5 \oplus x_3x_5 \oplus \mathrm{x}_1 \oplus x_2 \oplus x_3 \oplus x_6 \oplus x_7 \quad (10)$$

The two function *f₁* and *f₂* shown in table (1) has been used to encrypt image in this propose system.

7. The Proposed system

The Encrypted system block diagram shown in Fig.(2). The proposed method based on decomposed the image into n×n sub-blocks, the coefficients of 2-dimension DCT (2DCT) re-arranges into vector by zigzag order as shown in Fig.(3), then the DCT coefficients of the image block are encrypted using resilient Boolean functions (stream cipher) as implement in the encrypted algorithm.

-Algorithm Encrypt Image

```
Input: - Gray level file Bmp or JPG format.
       - Resilient Boolean function
         (Stream cipher) (Mat format).
Output: Encrypted Image.
BEGIN
    OPEN image file.
    OPEN stream cipher file.
  While not eof (image and stream cipher) file
    do
      - OPEN image file x(i,j).
      - OPEN stream cipher file C(k).
      - Divided image into n×n sub-block
      - Apply 2DCT to sub-block X(u,v).
      - Convert into vector (W) by zigzag order then convert
        into corresponding K bits $W_b(u)$ as shown in Fig.(4).
      - Encrypted the selected coefficients by XORing the
        generated bitstream don't used sign bit $W_E(u)$ after
        divide into sub-block K bit.
          $W_E(u) = W_b(u) \oplus C(k)$.
      - 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 image file.
    Close stream cipher file.
    Close encrypted image file.
END
```

-Algorithm Decrypt Image

The Decrypted system block diagram shown in Fig.(4), the decrypt algorithm is

```
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 C(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 bitstream don't
        used sign bit $V_E(u)$ after
        divide into sub-block K bit.
            $V_D(u) = V_b(u) \oplus C(k)$.
        - Convert from K bit into
          decimal X(u).
        - Convert vector X(u) into 2-
          Dim. matrix X(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
```

8. Fidelity Criteria

There are two types of image fidelity criteria namely, the objective and subjective criteria. The first one depends on equations that are used to measure the amount of the error in the reconstructed image. While the second require the definition of qualitative scale to assess image quality and this scale can then be used by human test subjective to determine image fidelity [9]

I. The Similarity Test

Similarity test is the correlation compare between original, encrypted image as parameter of robustness, and between orignal and decrypted image as parameter of quality in reconstruct image.

The correlation can be calculated as shown below [9]

$$Corr. = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j)-\bar{x})(y(i,j)-\bar{y})}{\sqrt{\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j)-\bar{x})^2\right]\left[\sum_{i=1}^{M}\sum_{j=1}^{N}(y(i,j)-\bar{y})^2\right]}} \quad ..(11)$$

where:

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

i and *j*: row and column numbers.

x(i, j): the original image.

y(i,j): modified image.

$\bar{x}, \bar{y}$: Mean of original and modified image, respectively. And calculated by

$$\bar{x} = \frac{\sum_{i}^{M}\sum_{j}^{N} x(i,j)}{M \times N} \quad \dots (12)$$

$$\bar{y} = \frac{\sum_{i}^{M}\sum_{j}^{N} y(i,j)}{M \times N} \quad \dots (13)$$

II. Peak Signal to Noise Test (PSNR)

According to the human visual system, some amount of distortion between the original image and the modified one is allowed. Here the *PNSR* is employed to indicate the performance of the method. *PSNR* is usually measured in *db*[10].

$$PSNR = 10\log_{10}\frac{(L-1)^2}{\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[y(i,j)-x(i,j)\right]^2} \quad (14)$$

where:

L-1: maximum gray level.

9. Simulation Results

This section presents simulation results for some images to provide the performance of the proposed encryption system. The system program was built by Matlab-2008a M.file.

Four gray-level (256 gray-level 8 bit/pixel) images of size 128×128 have been used to compare the encrypted and decrypted results in different images. Fig.(5a-d) show the original image, encrypted image by using resilient functions f_2 with selected coefficients $C_{0,5}$ (DC plus five AC), and decrypted image for Cameraman, Bag, Circuit, and Tire images, respectively.

Table (2) shown the objective testing for image cameraman with different numbers of encrypted DCT coefficients used resilient functions f_1 in $C_{0,0}$ are Corr.1= 0.270265, PSNR.1 = -4.7921 dB and Corr.2= 0.99715, PSNR.2 = 39.2698 dB when in $C_{0,4}$ are Corr.1= 0.15994, Corr.2= 0.999464, and PSNR = 36.5273 dB, the encrypted image give stronger result when number of coefficient increased with little improved in reconstructed image.

The objective result by used resilient functions f_2 in $C_{0,0}$ are Corr.1= 0.154005, PSNR1 = -10.7417 dB and Corr.2= 0.99963 PSNR2 = 48.1380 dB, when in $C_{0,4}$ are Corr.1= 0.108366, PSNR2 = -17.7363 dB and Corr.2= 0.999844, PSNR2 = 42.1817 dB. The f_2 function gives results strong than f_1 although the two functions have the same degree, with the same number of DCT coefficients, this proves the Zhang's constructions. Table (3) shown the objective test in deferent images used function f_2 and different numbers of coefficients $C_{0,0}$ and $C_{0,5}$. The propose systems success to encrypted and decrypted different type of images with the same properties of cameraman.

10. Conclusions

In the stream cipher model, the Boolean function must be so chosen that it increases the linear complexity of the resulting key stream. So high algebraic degree provides high linear complexity. As shown in the result encerupted system be stronger when the resiliency, nonlinearity and linear complexity of the Boolean functions increased.

In DCT there is a huge spectrum of applications that demands security on a lower level that ensured by selective encryption (SE). Such approaches reduce the computational requirements in networks.

The experiment results show that we can encrypt the images by resilient Boolean function with smaller correlation compare with original image and reconstruct the image by decipher algorithm with high fidelity criteria (correlation test and PSNR).

The result has been improved when the number of encrypted coefficients (DC plus number of AC) increased. The improvement will be decreased when the number of selected coefficients increased.

11. References

[1] L. Krikor, S.Baba, T.Arif and Z.Shaaban, "Image Encryption Using DCT and Stream Cipher", European Journal of Scientific Research, , ISSN 1450-216X Vol.32 No.1 pp.47-57, (2009).

[2] 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.

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

[4] T. Siegenthaler, “Decrypting a class of Stream Ciphers Using

Cipher text Only". IEEE Transactions on Computers, C-34(1): 81-85, January 1985.

[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).

[6] 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.

[7] A. Menezes, P.van Oorschot, & S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996. www.cacr.math.uwaterloo.ca/hac.

[8] Qichun Wang,Jie Peng,Haibin Kan and Xiangyang Xue. “Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials”, Will appear in IEEE Transactions on Information Theory, Vol. 56, No.6, June 2010.

[9] Hussam A. Darweesh and Ahmmed A.A. Hussain “High Capacity Secret Image Steganography using DC|T”, Second Edition, Information Technology Conference, Iraq 2010.

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

Table (1): Some saturated best functions

	SBR functions (*n*,*m*,*d*, $nl(f)$)	**The upper bound on the nonlinearity**	**degree**	**Linear complexity**
f_1	(5,1,3,12)	12	3	100
f_2	(6,2,3,24)	24	3	104
f_3	(7,3,3,48)	48	3	108
f_5	(7,2,4,56)	56	4	675
f_6	(8,3,4,112)	112	4	678

Table (2) the result of corr. And PSNR For image 1(cameraman)

No. of coefficients Encrypted	f_1		f_2	
	Corr.1 %	PSNR1	Corr.1 %	PSNR1
C_{0-0} (DCT+0ac)	0.270265	-4.7921	0.154005	-10.7417
C_{0-1} (DCT+1ac)	0.20265	-7.8164	0.123433	-13.7611
C_{0-2} (DCT+2ac)	0.179105	-9.5764	0.114261	-15.5194
C_{0-3} (DCT+3ac)	0.162938	-10.8296	0.110172	-16.7690
C_{0-4} (DCT+4ac)	0.151825	-11.7989	0.108366	-17.7363
C_{0-5} (DCT+5ac)	0.145994	-12.5899	0.108723	-18.5264
No. of coefficients Decrypted	**Corr.2 %**	**PSNR2**	**Corr.2 %**	**PSNR2**
C_{0-0} (DCT+0ac)	0.999715	39.2698	0.999963	48.1380
C_{0-1} (DCT+1ac)	0.999843	41.8638	0.999885	43.2023
C_{0-2} (DCT+2ac)	0.999464	36.5550	0.999913	44.4412
C_{0-3} (DCT+3ac)	0.999589	37.6801	0.999908	44.1736
C_{0-4} (DCT+4ac)	0.999464	36.5273	0.99984	42.1817
C_{0-5} (DCT+5ac)	0.998710	32.7088	0.999932	45.5095

Table (3) the results of images used resilient function f_2 & no. of coefficient C_{0-0} and C_{0-5}.

Images	No. of coefficients	Encrypted		Decrypted	
		Corr.1%	PSNR1	Corr.2%	PSNR2
Cameraman	C_{0-0}	0.154005	-10.7417	0.999963	48.1380
	C_{0-5}	0.108723	-18.5264	0.999932	45.5095
bag	C_{0-0}	0.183003	-12.2895	0.999971	46.7957
	C_{0-5}	0.162806	-20.0663	0.999910	41.9254
circuit	C_{0-0}	0.115347	-14.28821	0.999994	42.4114
	C_{0-5}	0.88868	-22.053	0.998985	32.6051
tire	C_{0-0}	0.151717	-15.0274	0.999913	40.0214
	C_{0-5}	0.90589	-22.8068	0.999801	36.4529

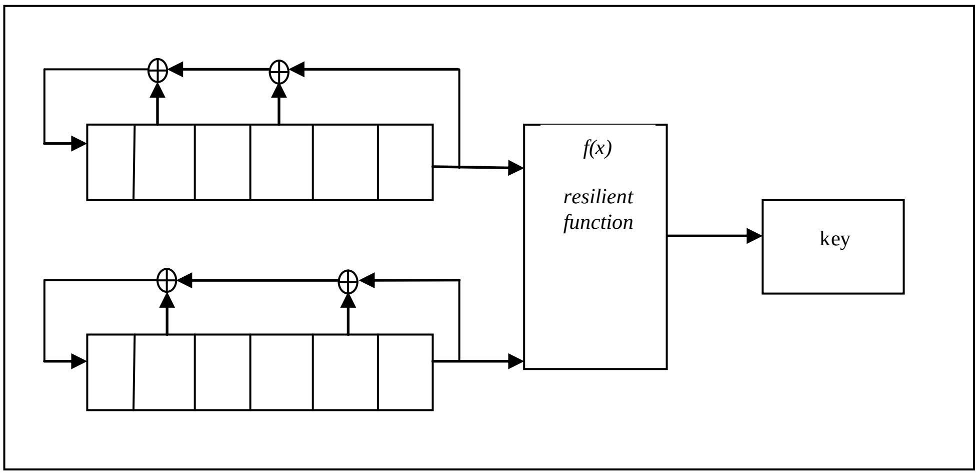


Figure (1) Stream cipher (resilient Boolean function (RB)).

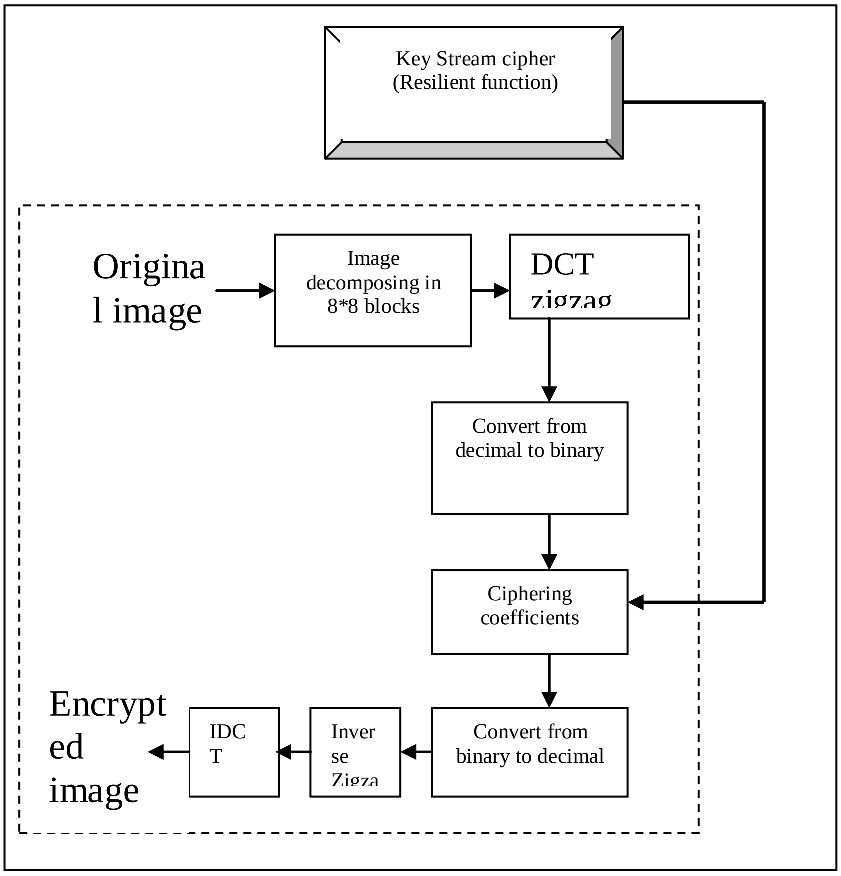


Figure (2) Block diagram of encrypted System.

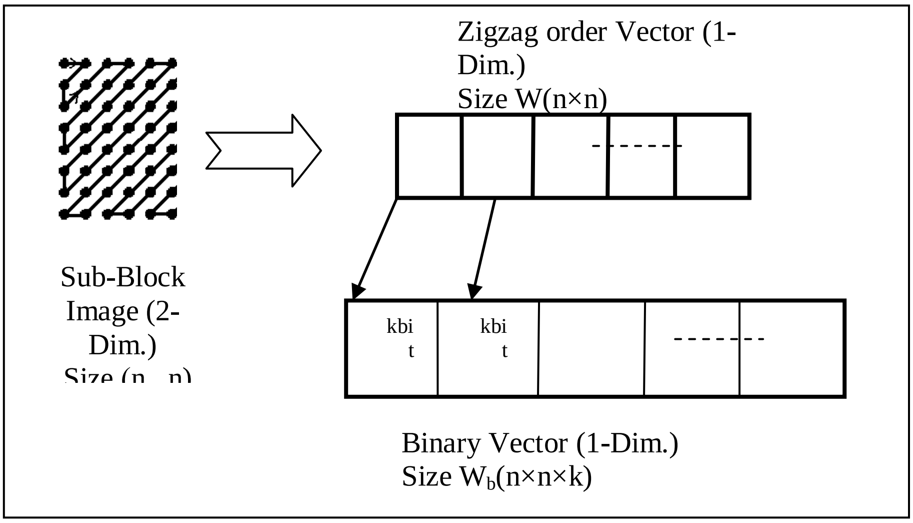


Figure (3) Convert into vector zigzag and K bits

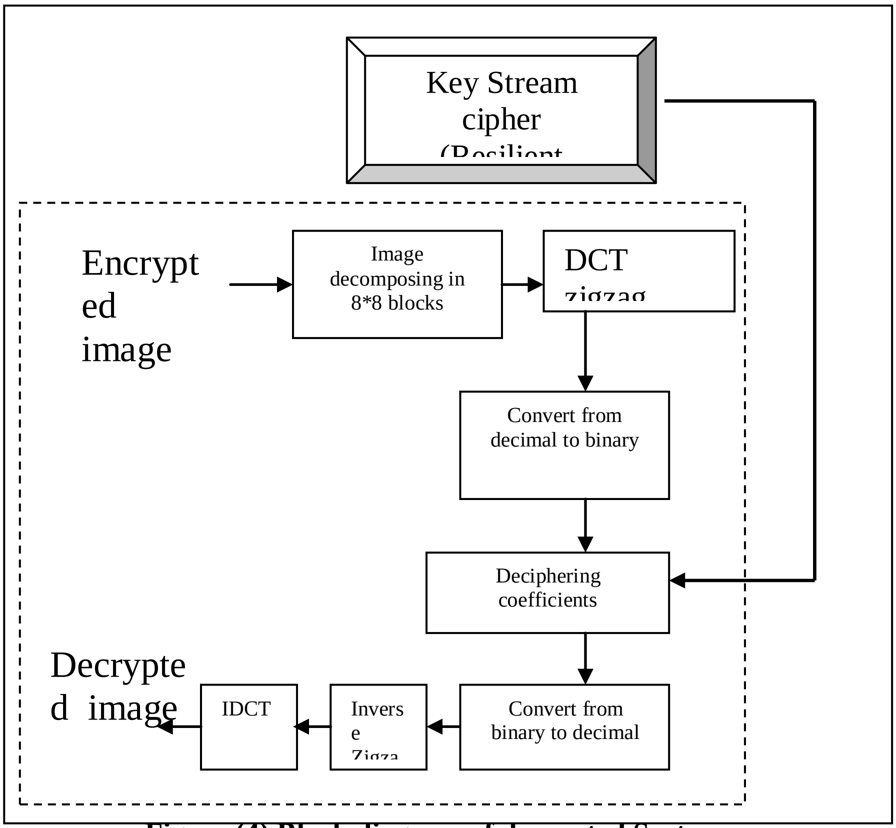
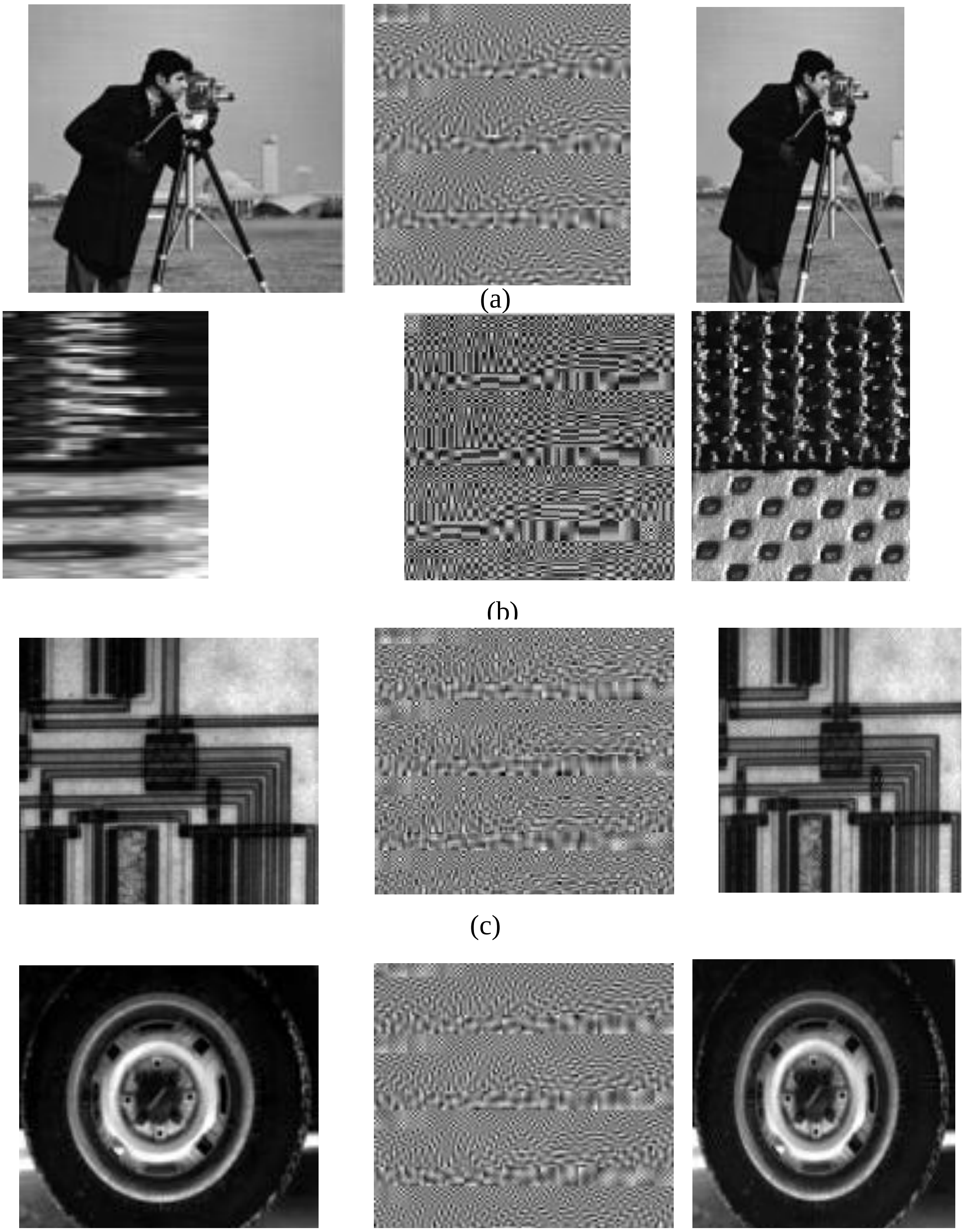

Key Stream cipher (Resilient
Encrypted image
Image decomposing in 8*8 blocks
DCT zigzag
Convert from decimal to binary
Deciphering coefficients
Convert from binary to decimal
Inverse Zigza
IDCT
Decrypted image

Figure (4) Block diagram of decrypted System.



(a)

(b)

(c)

(d)

Figure (6): The result of different images (original, encrypted and Decrypted) used using f_2 & no. of coefficient C_{0-0} and C_{0-5} for a- cameraman image b- Bag