International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015
ISSN 2091-2730

WAVELET BASED ADVANCED ENCRYPTION STANDARD ALGORITHM FOR IMAGE ENCRYPTION

Ajish S , Assistant Professor
Department of Computer Science and Engineering
College of Engineering, Perumon, Kollam, India, ajishs2014@gmail.com

Abstract— With the fast evolution of digital data exchange, security of information becomes much important in data storage and transmission. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. As encryption process is applied to the whole image in AES ,it is difficult to improve the efficiency. In this paper, wavelet decomposition is used to concentrate the main information of image to the low frequency part. Then dynamic S-Box based AES encryption is applied to the low frequency part. In Dynamic chaotic S-BOX Based AES the Substitute bytes provide security because the S-Box is constructed from the key. The high frequency parts are XORed with the encrypted low frequency part and a wavelet reconstruction is applied. Theoretical analysis and experimental results show that the proposed algorithm has high efficiency, and satisfied security suits for image data transmission.

Keywords— Image encryption; Wavelet Transforms; Advanced Encryption Standard; dynamic S-Box; High frequency wavelet coefficients; Haar- Discrete wavelet transforms.

I. INTRODUCTION

With the rapid development of network and through which information transmission is widely used, the protection of information becomes a crucial issue. Multimedia information, as an important information carrier, how to confirm the confidentiality, integrity and usability when transmitted on the network becomes a research hotspot in recent years.

Wavelet analysis [6] is a mathematical tool, which has been developed only in recent decades, but has been quickly applied to many research areas, such as image processing and audio analysis. Wavelet transform time-domain and frequency-domain or the space-domain and frequency domain have a good local optimization features, as well as the Multi-Resolution Analysis features make wavelet transform suitable for image processing on transform domain.

The S-Box is a substitution box [2] and the only nonlinear component assuring the confusion property of the Advanced Encryption Standard (AES). The strength of the AES algorithms depends on the design of cryptographically strong S-Box. In recent years, chaos has attracted a great deal of attention in many fields especially in cryptography. Using chaos may have potential benefits such as added security and low complexity due its random like behavior that exhibits sensitive dependence on initial conditions [5]. According to the chaotic systems properties it seems to be convenient and simple to obtain ”good” S-Boxes by modifying slightly the initial conditions or system parameters. Many approaches for obtaining S-Boxes based on chaos have been presented, and they severely rely on iterating and discretization chaotic maps.

In this paper, a new image encryption algorithm is proposed which is based on wavelet transform and dynamic S-box based AES algorithm. First of all, wavelet decomposition is used for concentrating original image in low-frequency wavelet coefficients [7], then dynamic S-Box based AES algorithm is applied to encrypt the low-frequency wavelet coefficients. In dynamic S-Box based AES algorithm[3] the S-Box is generated from the key by using pairwise linear chaotic maps. Secondly, an XOR operation is used for high-frequency wavelet coefficients and the encrypted low-frequency wavelet coefficients (as a key stream), so that the image information contained in high-frequency wavelet coefficients is hidden; Thirdly, a wavelet reconstruction is used for spreading the encrypted low-frequency part to the whole image.

II. HAAR -DISCRETE WAVELET TRANSFORMS

The frequency domain transform applied in this algorithm is Haar-DWT [1], the simplest DWT. A 2-dimensional Haar-DWT [1] consists of two operations: One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:
Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 1.

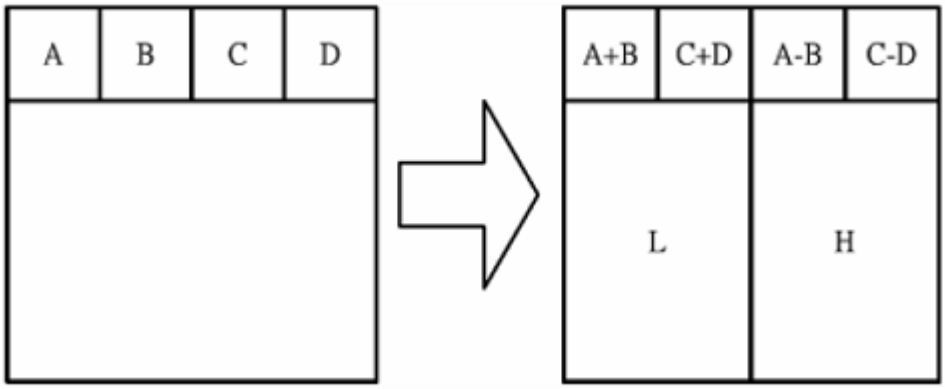

Figure 1. The horizontal operation on the first row.

Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Figure 2. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image.

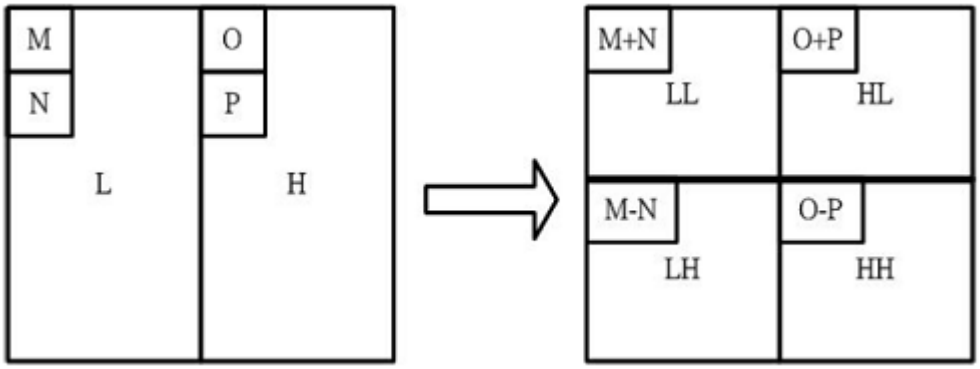

Figure 2. The vertical operation

The whole procedure described above is called the first-order 2-D Haar-DWT. The first-order 2-D Haar-DWT applied on the image "Lena" is illustrated in Figure 3.

III. WAVELET BASED AES ENCRYPTION ALGORITHM

The AES algorithm [3] is divided into four different phases, which are executed in a sequential way forming rounds. The encryption is achieved by passing the plaintext through an initial round, 9 equal rounds and a final round. The four phases are SubByte Transformation, Shiftrows Transformation, Addroundkey Transformation and Mixcolumns Transformation. The structure of AES algorithm [3] is shown in Figure 4.

A. SubByte Transformation

After the wavelet decomposition the maximum value in each column is 1024. So the S-Box used in AES algorithm can't be used in the Wavelet Based AES Encryption Algorithm. In the SubByte Transformation dynamic S-Boxes based on one-dimensional chaotic maps are used. A piece-wise linear chaotic map (PLCM) [2] is given by

$$F(x,p) = \begin{cases} \frac{x}{p} & 0 \le x \le p \\ \frac{x-p}{\frac{1}{2}-p} & p < x \le 1/2 \\ F(1-x,p) & 1/2 < x \le 1 \end{cases}$$

(a) (b)

Figure 3. (a)Original image-Lena, (b) Result after the first-order 2-D Haar-DWT

where 0< p< 1/2, x serves as an initial condition, and p is the control parameter for the map F.

Step 1. Divide the output range [0.1, 0.9] into 1024 intervals of equal length. During the iteration of the chaotic map, the output of the PLCM that occurs outside the considered range will be neglected. This is done to generate more chaotic numbers, since initial conditions close to 0 and 1 are not good starting points.

Step 2. Label each region sequentially from 0 to m, where m is equal to 1023. Let the length of each region be denoted by ΔL. Let us denote the first region by R0 =[0.1, 0.1+ ΔL], and the last region by Rm =[0.1+mΔL, 0.1+(m+1)ΔL]. Now, label each region sequentially, that is, R0 → 0, R1 →1, R2 → 2, and Rm → m.

Step 3. Calculate the arbitrary initial condition, IC from the Key using the logistic maps.

Logistic map:

$$x_{n+1} = 1 - \mu x_n,\ \mu \in (0,2), x_n \in [-1,1]$$

Chebyshev map:

$$x_{n+1} = \cos\left(k cos^{-1}(x_n)\right), k \geq 2, x_n \in [-1,1]$$

The 128 bit key is divided into 4 32-bit unsigned integer keys: key1, key2, key3, key4. In the initial condition generation process u0 = 1.9999.

x01 = (key0+key1)/(0xffffffff*2)

x02 =(key2+key3)/(0xffffffff*2)

x21 and x22 are calculated after 100 rounds iteration using Logistic map with the initial value x01 and x02, x2= (x21+x22)/2. The initial condition IC for the dynamic S-Box is calculated after 100 rounds iteration using Chebyshev map with x2 as the initial value

Step 4. Iterate the PLCM using the initial condition. Whenever the PLCM visits a particular region, store that number in an array S. If the PLCM has already visited a particular region, then do not store the assigned number to that region in the array S.

Step 5. Stop iterating the PLCM when it traverses all regions.

Step 6. Rearrange the array S in the form of a table by filling rows sequentially.

B. Shift Rows

The ShiftRows step operates on the rows of the state, it cyclically shifts the bytes in each row by a certain offset as shown in Figure 4. The first row is left unchanged. For the second row, a 1-byte circular left shift is performed. For the third row, a 2-byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed. The inverse shift row transformation, called InvShiftRows, used in the decryption, performs the circular shifts in the opposite direction for each of the last three rows, with a one-byte circular right shift for the second row, and so on.

C. Mix Columns

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. The transformation can be defined by the following matrix multiplication on State.

The inverse mix column transformation, called InvMix- Columns, is defined by the following matrix multiplication Where the C matrix used in inverse mix column should be the inverse of A matrix used in forward mix column transformation. That is, the inverse transformation matrix times the forward transformation matrix equals the identity matrix.

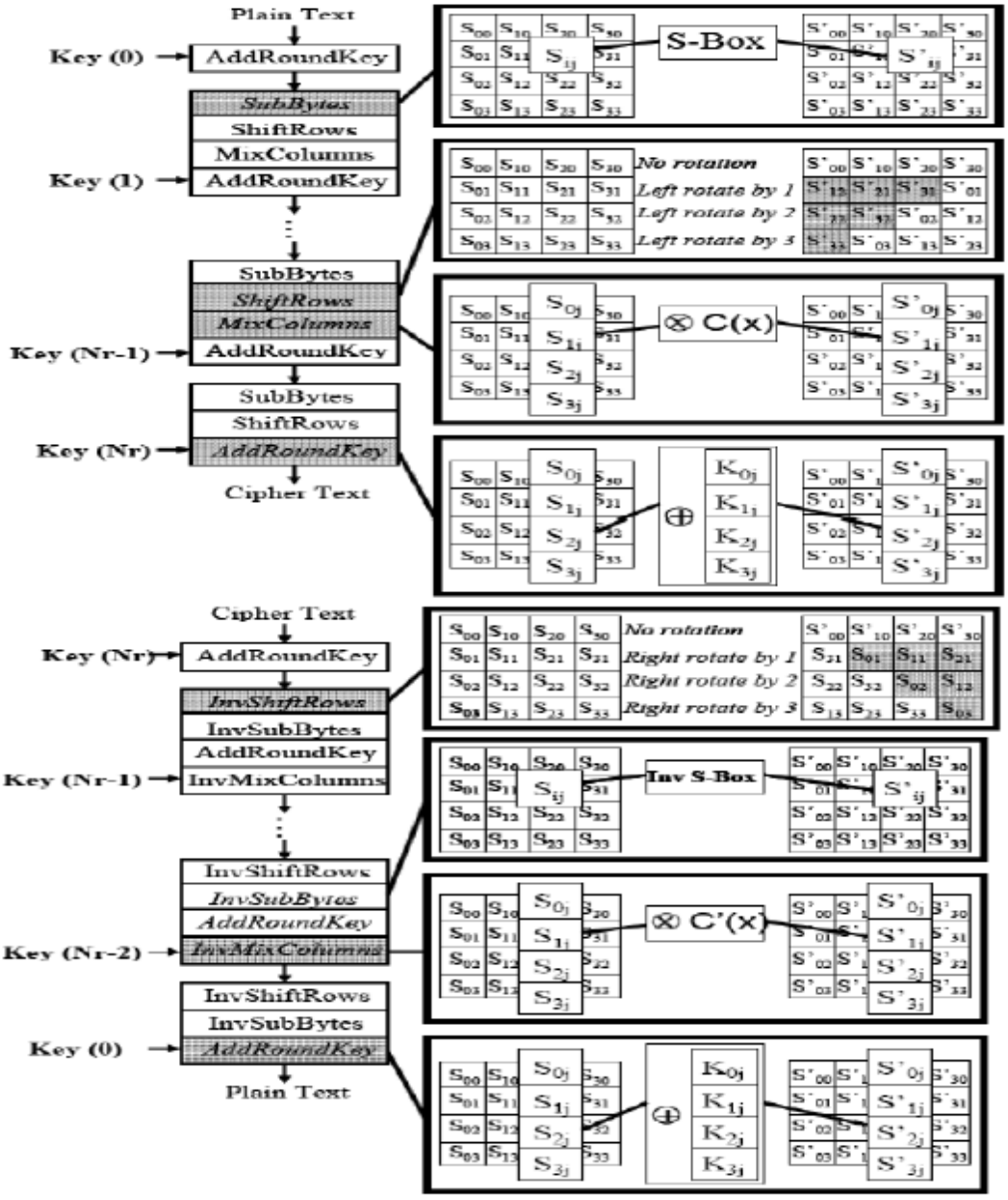

Figure 4. Description of the AES cryptographic algorithm

D. Add Round Key

In the AddRoundKey step [3], the sub-key is combined with the state. For each round, a sub-key is derived from the main key using AES key schedule, each sub-key is the same size as the state. The sub-key is added by combining each byte of the state with the corresponding byte of the sub-key using bitwise Exclusive OR (XOR).

The inverse add round key transformation is identical to the forward add round key transformation, because the XOR operation is its own inverse.

E. Encryption of High-Frequency Wavelet Coefficients

The low frequency wavelet co-efficient (LL part) is encrypted using the modified AES algorithm. The high frequency wavelet co-efficients (LH,HL,HH) are encrypted by EXORing the high frequency parts with the encrypted low frequency part. After that a wavelets reconstruction is used for spreading the encrypted low-frequency part to the whole image.

IV. PERFORMANCE ANALYSIS

A. Efficiency

The Wavelet Based AES image encryption algorithm is tested and evaluated based on software and hardware simulation. Different standard images have been used ”lena” and ”cheetah” (greyscale format) in the simulations which are encrypted with wavelet Based AES and AES algorithms. Table I shows the average time required by Wavelet Based AES and AES for each image. From the Table it is clear that Wavelet Based AES algorithm is much faster than AES algorithm.

Image(Size)	AES Encryption Time	Wavelet Based AES Encryption Time
Lena(256*256)	31.75 ms	8.2 ms
Cheetah(200*320)	29.25 ms	7.52 ms

Table I: AVERAGE TIME REQUIRED BY AES AND WAVELET AES FOR DIFFERENT IMAGES

B. Differential Approximation Probability

The nonlinear transformation S-box should ideally have differential uniformity. An input differential Δxi should uniquely map to an output differential Δyi, thereby ensuring a uniform mapping probability for each i. The differential approximation probability of a given S-box, DPs, is a measure for differential uniformity and is defined as

$$DP^{s}(\Delta x \rightarrow \Delta y) = \left(\frac{\#x \in X | S(x) \oplus S(x + \Delta x) = \Delta y}{2^{m}}\right)$$

where X is the set of all possible input values, and 2m is the number of its elements.

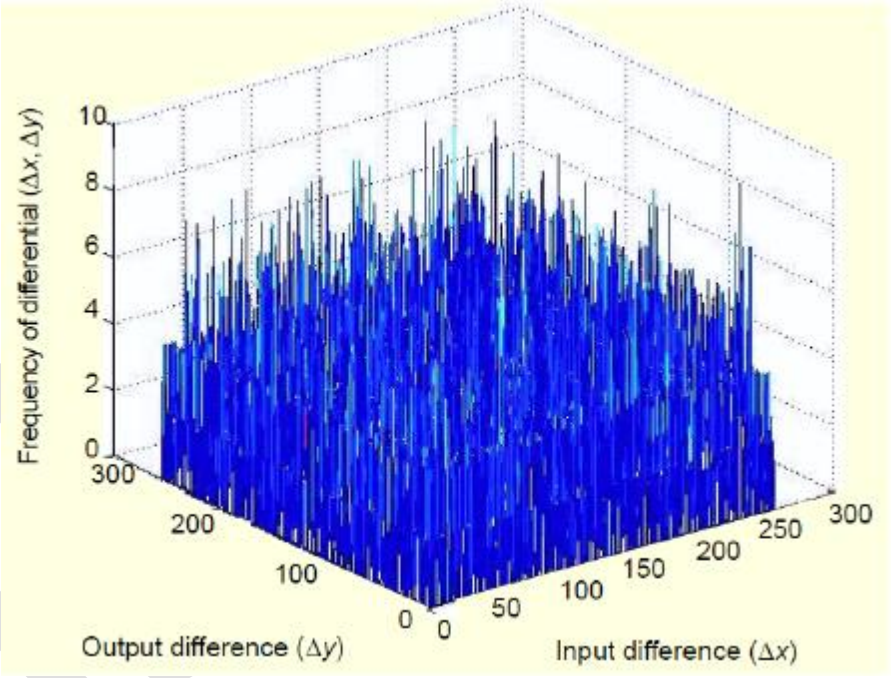

Figure 5:. Differential distribution of S-box in Table 1

In Figure 5, the distribution of the differentials for the S-box constructed by On Dynamic chaotic S-BOX [2] is shown, where the x-axis represents the input differentials Δx, the y-axis represents the corresponding output differentials Δy, and the z-axis represents the number of occurrences of the particular input and output differential (Δx, Δy). Table I shows those differentials that occur with the maximum probability of 10/256. The rest of the differentials occur with a probability of less than 10/256. The maximum differential probability, DPs, is 12/256 in case of [2]. Also, more input and output differential pairs occur with the maximum probability of 10/256 as compared to PLCM S-box.

C. Histograms of Encrypted Images

To prevent the leakage of information to an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each

colour intensity level. The histograms of the several encrypted images as well as its original images that have widely different content are calculated and analyzed. One typical example among them is shown in Figure 6.

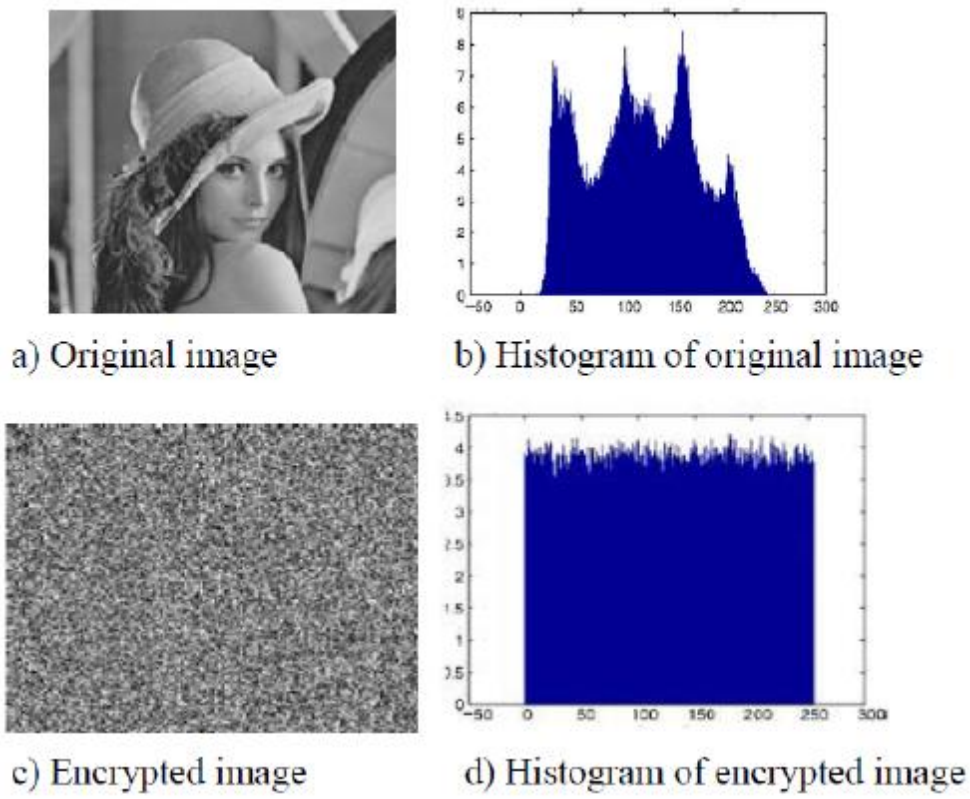

Figure 7. Histograms of the plain image and ciphered image

The histogram of a plain image Lena image (Figure 6a) of size 256x256 pixels) contains large spikes. The histogram of the cipher image as shown in Figure 6d, is uniform, significantly different from that of the original image, and bears no statistical resemblance to the plain image. It is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.

D. Correlation Property Test

The following method is used to test the pixel correlation property. First, 1000 couples of pixels are randomly chosen (horizontally, vertically and diagonally) from the cipher image. Second, the correlation coefficient of adjacent pixels of the cipher image obtained using the following formulas:

$$E(x) = \frac{1}{N}\sum_{1}^{N} xi$$

$$D(x) = \frac{1}{N}\sum_{1}^{N}(x_i - E(x))2$$

$$Con(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)(y_i - E(y))$$

$$\gamma_{xy} = \frac{Con(x,y)}{\sqrt{D(x)\sqrt{D(y)}}}$$

In which x, y are gray value of two adjacent pixels, γ_{xy} is the correlation coefficient. Adjacent pixels of original image are usually highly correlated, that is, the correlation coefficient is close to 1. Figure 7 shows the results of correlation property analysis. Ideally,

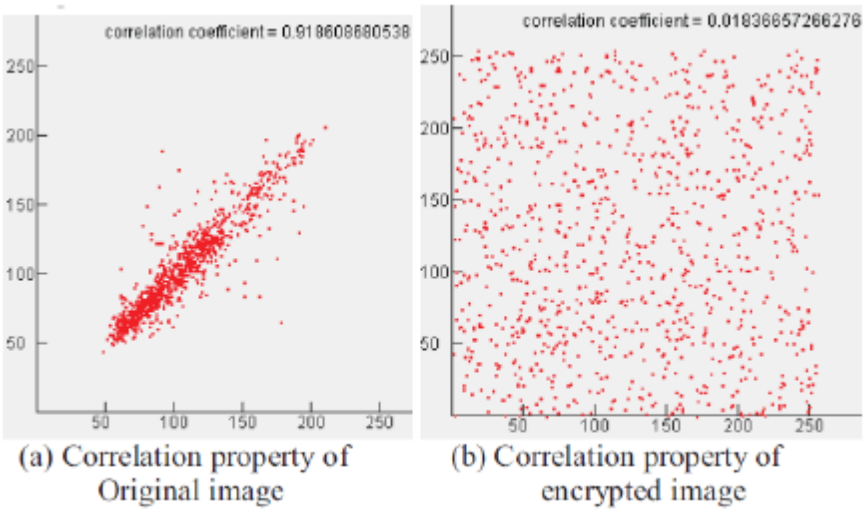

Figure 8. Pixel correlation analysis

encryption algorithm should make the adjacent pixels correlation coefficient of cipher image close to 0, that is, pixels are basically uncorrelated, which illustrates the statistical properties of original image have been randomly diffused into cipher image.

V. CONCLUSION

To improve the efficiency of AES wavelet decomposition is used to concentrate the main information of image to the low frequency part. Then dynamic S-Box based AES encryption is applied to the low frequency part. In Dynamic chaotic S-BOX Based AES the Substitute bytes provide security because the S-Box is constructed from the key. The high frequency parts are XORed with the encrypted low frequency part and a wavelet reconstruction is applied.

REFERENCES:

[1] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of AppliedScience and Engineering.

[2] Ghada Zaibi, Abdennaceur Kachouri , "On Dynamic chaotic SBOX", 2009 IEEE.

[3] William Stallings, "Cryptography and Network Security Principles and Practice", Prentice Hall.

[4] Liu, J., B. Wei and X. Wang, "An AES S-box to increase complexity and cryptographic analysis", Proc. of the 19th International Conference on Advances Information Networking and Application, Taiwan, pp.724-728, 2005.

[5] J.J. Amador, R. W.Green, "Symmetric-Key Block Cipher for Image and Text Cryptography", International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188.

[6] Shuo Zhang, Ruhua Cai, Yingchun Jiang," An Image Encryption Algorithm Based on Multiple Chaos and Wavelet Transform", 2009 IEEE pp. 178-188.

[7] Long Bao, Yicong Zhou, and C. L. Philip Chen, "Image Encryption in the Wavelet Domain", Mobile Multimedia/Image Processing, Security, and Applications 2013.

[8]Faiz Yousif Mohammad Alaa Eldin Rohiem, Ashraf Diaa Elbayoumy "A Novel S-box of AES Algorithm Using Variable Mapping Technique" Aerospace Sciences & Aviation Technology. - cairo : Military Technical College, 2009.

[9] Razi Hosseinkhani,H. Haj Seyyed Javadi, "Using Cipher Key to Generate Dynamic S-Box in AES" Cipher System - 2012. - Issue (1): Vol. (6). - pp. 19-28.

[10] Faiz Yousif Mohammad Alaa Eldin Rohiem, Ashraf Diaa Elbayoumy "A Novel S-box of AES Algorithm Using Variable

Mapping Technique" Aerospace Sciences & Aviation Technology. - cairo : Military Technical College, 2009.

[11] Abd-ElGhafar A. Rohiem, A. Diaa, F. Mohammed "Generation of AES Key Dependent S-Boxes using RC4 Algorithm" Sciences & Aviation Technology ASAT-13". - cairo : Military Technical College, 2009.

[12] Rhee, Man Young. "Internet Security Cryptographic Principles, Algorithms and Protocols". England: John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,West Sussex PO19 8SQ, 2003