Chaos Image Encryption based on DCT Transforms and Henon Map

Abdullah M. Awad
University of Anbar
Ramadi, Iraq

Rehab F. Hassan
University of Technology
Baghdad, Iraq

Ali M. Sagheer
University of Anbar
Ramadi, Iraq

ABSTRACT
The study of cryptography applications in chaotic system have been exponentially increasing in the recent years. Depending on the sensitivity to initial conditions, chaotic systems are characterized, similarity to continuous broad-band power spectrum and random behavior. The chaotic system is high sensitive to the initial condition and is a high complex nonlinear dynamic system. The chaotic sequence is unpredictable and extreme sensitivity to initial conditions. There are many applications to the chaotic system in several methods, image compression, encryption, modulation and digital communication system. In this paper, an algorithm based on Discrete Cosine Transform (DCT) has been introduced by using Henon map to get the scheme of chaos image encryption. The level of security is very high and this algorithm can improve small key space.

A new chaotic algorithm is presented to get rid of the problem of the weakness of security in one dimensional chaotic cryptosystems and small key space based on a new chaotic algorithm, which uses two dimension linear functions instead of one dimension.

Keywords
Chaos theory, chaotic encryption, AES, DWT, image encryption

1. INTRODUCTION
In recent years, information's security becomes an essential factor in different applications such as, multimedia, military communications, internet security and medical images. However, most applications face some problems such as security and lack of robustness. The security of encrypted image for this algorithms can be evaluated to show the correlation between the two adjacent pixels differentiated attack the key space analysis were performed. Two processes should be composed in a chaotic image encryption , the first process is a chaotic confusion and the second is pixel diffusion. The pixels permutation are achieved to image with two dimensions chaotic map but the value of each pixel alternates in a sequential manner. The traditional architecture of cipher like RSA, AES, DES and IDEA are used for binary data or text but not used in image encryption because it is not suitable to the digital image which are usually with large size. The image data encryption is too expensive with traditional cipher. The digital image characteristics suffer from poor security and high redundancy. A light encryption reserves information for many applications. A new algorithm for image encryption was used by combining chaos encryption theory with Discrete Cosine Transform (DCT). The analysis of encryption security algorithm can be used from the key space perspective, key sensitivity analysis and statistical analysis. The results will show effectively image encryption, which is faster than traditional techniques, the transmitted amount of information, is low according to DCT and resists the brute-force attack and good key space is large enough encryption effect.

This paper is organized as follow; Section 2 surveys some significant related work. Section 3 shows the basic concepts of chaos cryptography. Section 4 presents the RC4 encryption method. Section 5 summarizes the DCT. The proposed model is illustrated in Section 6, while Section 7 discusses the results. Finally, Section 8 delivers the main conclusions.

2. RELATED WORKS
Since the last decade, chaos encryption has been investigated. There are several papers discussed the chaos which used encryption in many applications such as, communications, images, video and optical data. There are also many algorithms proposed in chaotic image encryption. According to some chaotic functions, several algorithms are used to manipulate them and scattering the position of pixels. Two chaotic image encryption algorithms are proposed by Yen, and Guo [8-10] where the pixels of image are rearranged by using a chaotic system method to generate a binary sequence randomly. Alvarez et al Li has suggested a new algorithm for a chaotic encryption, which was improved by et al and Cai, Y. [13]. Fridrich has suggested a new algorithm in chaotic encryption image, which does not need a chaotic random number generator by using a 2D Baker's map transforms instead of the permutation of the pixel's position [11-12]. The proposed algorithms by Yen, Guo and Fridrich have one similarity that is to encrypt a square image. Sasidharan et al proposed a new algorithm as scheme of fast partial wavelet transform (DWT) and stream cipher (RC4) for image encryption. According to their technique, the lowest frequency band is carried out by the stream cipher to get the encryption [27]. A random combinational image encryption approach with bit, pixel and block permutations have presented by Mitra[21] A et al. Zhi-Hong Guan et al. have presented a new chaotic image encryption by changing the grey values and shuffling the image pixels positions combined to confuse the cipher image and the plain image relationship[23]. A. Sinha, K. Singh have proposed a chaotic image encryption based on JigSaw Transform (JST) and Fractional Fourier Transform (FRFT) in bit plane images proposed in [20]. The chaotic key based Algorithm (CKBA) as an encryption method is generated a binary sequence key by using a chaotic system proposed by Yen, J.C. and Guo, J.I when the binary sequence are generated and according to this the selected key then Xored with the arranged image pixel [5]. Rahma, A.S. and Yacob, B. Z have proposed Real-Time Partial Encryption of Digital Video Using Symmetric Dynamic Dual Keys Algorithm (SDD [6]. Rahma, A.S. and Ali, M. A have presented Modify the Partial Audio

Cryptography for Haar Wavelet Transform by Using AES Algorithm [7].

3. CHAOTIC CRYPTOGRAPHY

3.1 Background

Cryptography is the science of protecting the security of information during communication under antagonistic conditions. These days, cryptography has an important in information technology development and communication via computer networks. Current cryptographic methods are used of number theoretic or mathematical concepts. Chaos is another ideal model, which appears to be promise. Chaos is one of the possible systems, which have characteristics, or behaviors associated with development of a nonlinear dynamic system and occur for parameters of specific values of system.

The chaotic characteristic is a delicate behavior of a nonlinear system, which looks as irregular or random. The disclosure of this pseudo-random specification happening as a result of deterministic systems turned out to be quite revolutionary which prompt numerous issues interconnecting stability theory, new signatures and new geometrical features characterizing dynamical performances.

At the point when the chaotic state is observed by the existence in phase space of a chaotic attractor or fractal where in all the system trajectories evolve following a certain pattern but are never the same. In a more logical analytical design, the chaotic state can be extensively studied by the Lyapunov exponents that globally characterize the behavior of dynamical systems.

Chaos can exist just when there is no less than one positive Lyapunov exponents and the total sum of all exponents is negative, this means the dynamical system has a stable but random like state called chaotic state [13].

Chaos theory has acquired a lot of consideration from the cryptographic community in the last two decades. Both physical and mathematical, a remarkable number of chaotic systems, were designed in both hardware and software equipments for realizing encryption and decryption of messages.

Chaos cryptography might not have particularly exact parallelism to ideas and concepts of traditional cryptographic and cryptanalysis approaches as it is still in its childhood stage. Cryptographic algorithms and chaotic maps have some similar properties: Pseudo-random number generator behavior, with long time unstable orbits, very sensitive to initial conditions and parameters, depending upon the numerical implementation precision. Diffusion and confusion properties in a cryptographic algorithm depend on encryption rounds. In the same time, the initial region over the entire phase space is spread the iterations of the chaotic map [13].

3.2 Basic Concepts of Chaos

Chaotic confusion by permutation process spread of pixel positions and by diffusion process diffusion of pixel grey values wherein the former permutes an image with chaotic systems. The latter changes to pixel values sequentially leads to a small change for a singular pixel can spread out to all pixels in the whole image. These are the two processes, which made the chaos-based image encryption schemes. A reliable permutation procedure must display good missing effect and a good diffusion procedure that causes greatly modifies over the encrypted image even if only a mirror change for one pixel in the plain-image [13].

3.3 Special Properties of Chaotic Systems

Systems which are basically nonlinear and exhibiting an apparently random behavior for certain range of values of system parameters is referred to as chaotic. However, the solutions or trajectories of the system remain bounded within the phase space. This unstable state has a strong dependence on the values of the parameters and the way the system begins.

The following properties characterize chaotic dynamics. In general, nonlinear system the initial state of a deterministic system can be given by the sensitivity to initial conditions and, the future states of the system can be predicted. Long-term prediction in chaotic systems is impossible. It is very close initial condition to diverge exponentially in a short time, there are two trajectories for the specific values of parameters, and the system is completely lost the initial information.

- Ergodicity

The property when in phase space trajectory comes arbitrarily close to the first earlier states is called ergodicity. This property essentially reflects that it finally is confined to a spatial object and there are a set of points, which is called an attractor. The essential property to cryptography that the density of points which is time invariant.

- Mixing

Initial condition in a small interval has a characteristic that the system spread in its asymptotic evolution over the full phase space.

- Initial conditions

It is an arbitrary interval that a chaotic system spreads over the phase space and which part to the trajectory asymptotically can be confined. Thus, any region becomes into every other region of the phase space spatial attractor.

3.4 Henon Map

Michel Henon introduced the map of the Poincare section as a simplified model of the Lorenz model. An initial point for the canonical map of the plane, a set of either points known as diverge to infinity will approach, or the Henon strange attractor.

The Hénon map attractor is a Cantor set and smooth, fractal in one direction in another. Numerical estimates a Hausdorff dimension of 1.261 ± 0.003 and correlation dimension of 1.25 ± 0.02 for the canonical map attractor [26].

The Henon map is good dynamical systems that achieve chaotic specifications and behaviors. Two equations can be defined the Henon map. There are two parameters a and b that the Henon map equations depend on. For a = 1.4 and b = 0.3 the system achieves a strange attractor.

One point (x, y) takes in a Henon map and maps this point to get a new point in the plane (see Figure 1).

$$X_{n+1} = Y_n + 1 - aX_n \quad (1)$$

$$Y_{n+1} = bX \quad (2)$$

Fig 1: Henon map attractor, a = 1.4 and b = 0.3

The Henon map is a dynamical system discrete-time. The Henon map is achieved chaotic behavior in the most examples of dynamical systems are studied [26].

The map may converge to a periodic orbit, chaotic or intermittent for other a and b values. From the Henon map, the map type of orbit diagram behavior can be obtained for different parameters.

3.4.1 RC4

Ron Rivest from MIT designed RC4, which has its place among the most popular ciphers for RSA Data Security Encryption. RSA considered it as its trade secret until it was leaked in the early mid-90s. Researchers who can reach out to RC4's real implementation have confirmed its authenticity [4].

RC4's major usage, a part of its numerous applications, is in SSL (also known as TLS). It is used to secure majority of the world's e-commerce over WWW. Its function is also made available in WEP, IEEE 802.11 wireless networking security standard. Email encryption products are another example.

3.4.2 RC4 Algorithm

The key stream is completely independent of the plain content utilized as a part of the RC4 encryption algorithm. A 8 * 8 S-Box (S0 to S255) is utilized, where each number is a permutation from 0 to 255. The permutation is an element of the length key. There is variables i and j which used as two counters, both instated to 0 utilized as a part of the algorithm [4].

The state table is 256-bytes because the calculation utilizes a length key variable from 1 to 256 bytes. This table is used to get of pseudo-random bytes is trailed by produced of pseu-random stream .The produced stream is XORed with the plaintext to achieve the ciphertext. The element in the state table is swapped at least once.

The key is 40 bits because of restriction but it is utilized as a 128 bit key. This system has the ability to utilize keys from 1 to 2048 bits. Lotus Notes and Prophet secure SQl use RC4 and these are a couple of cases of its numerous business-programming bundles.

The algorithm works in two phases, key setup and ciphering. Key setup is the first and most troublesome part in the encoding calculation. The key of encryption is utilized to create an encoding variable utilizing two exhibits, key, N-number and state of mixing operations amid N-bit key setup (N mean key length). The different approaches to mix operations are swapping bytes, utilizing different equations or modulo operation and so forth the procedure which gives a remaining value from a division is known as a modulo operation [4]**.**

3.4.3 Strengths of RC4

The strength of RC4 constitutes the following:

- The efforts to know that where any value is in the table.
- The effort to know which location in the table is utilized to choose every value in the succession.
- A particular RC4 Calculation key can be utilized just once.
- Encryption is 10 times speeder than DES.

3.4.4 Limitations of RC4

Any one key of 256 available keys can be a weak key. This key is recognized by cryptanalysis, which is able to find conditions under which one of more produced bytes is powerfully associated with a few bytes of the key [4].

4. DISCRETE COSINE TRANSFORM

Discrete Cosine Transform (DCT) is used in image and video coding since early 1970s.

The block 8x8 pixels in two-dimensional DCT are used in forward DCT for 64 pixel values and gets 64 DCT coefficients. The coefficient in the top left corner is called DC component of the DCT coefficient matrix and the other DCT coefficients are called AC components.

The DCT transformation can be achieved by using 8x8 pixels block to sum of cosine signals weighted. These weights are represented by the matrix DCT coefficient [24].

The coefficients, which represent to the low spatial domain frequencies, are near to the top left corner and the coefficients, which represent to the high spatial domain frequencies, are near to the bottom right corner. The low frequencies are gradual changes and slow representation, and the high frequencies are sharp changes and fast representation in the pixel domain. There is a spatial domain redundancy and the low frequency dominates the high frequency. The energy or information can be concentrated in the forward DCT contained in 8*8 block coefficient matrix in the top left side. The coefficients in the matrix near the DC coefficient differ a lot from zero and the other high coefficients are very close to zero.

DCT is a lossless transformation. Because of the quantization of the DCT coefficients, the information is lost in transformation-based data compression techniques [24].

The mathematical equations for a two-dimensional DCT are;

$$y(k,l)=\frac{c(k)c(l)}{4}\sum_{i=0}^{7}\sum_{j=0}^{7}x(i,j)\cos\left\{\frac{(2i+1)k\pi}{16}\right\}\cos\left\{\frac{(2j+1)l\pi}{16}\right\} \quad (3)$$

Where, k, l = 0, …, 7 and

$$C(k,l)=\begin{cases}\frac{1}{\sqrt{2}}, & k,l=0\\ 1, & k,l\neq 0\end{cases}$$

There is an Inverse DCT (IDCT):

$$x(k,l)=\sum_{i=0}^{7}\sum_{j=0}^{7}y(i,j)\frac{c(k)c(l)}{4}\cos\left\{\frac{(2i+1)k\pi}{16}\right\}\cos\left\{\frac{(2j+1)l\pi}{16}\right\} \quad (4)$$

The input matrix (8*8) from an image consists of values of pixels of Gray scale image and these values randomly spread from 123 to 140 range. The output matrix is created below when the input values are fed to the discrete cosine transform algorithm.

Table 1. Input matrix

137	137	137	134	129	131	131	132
137	137	137	141	133	132	132	133
138	138	138	134	134	131	131	129
138	138	138	132	130	127	133	134
140	140	140	134	139	133	136	128
135	135	135	129	133	131	133	123
130	130	130	129	136	134	129	129
135	135	135	131	129	132	129	129

Table 2. Output matrix

1064	17	0	-2	-4	-1	0	2
8	3	2	-7	2	2	-1	-4
-6	-4	-1	-1	1	-1	3	-7
-2	-5	14	-15	-8	-3	-3	8
-3	10	8	1	-11	18	18	15
4	-2	-18	8	8	-4	1	-7
9	1	-3	4	-1	-7	-1	-2
0	-8	-2	2	1	4	-6	0

The output matrix consists of DCT Coefficients, which is arranged in a way that coefficients containing useful and important data for representation of the image to be in the upper left of the matrix and in the lower right coefficients containing less useful information. The DC coefficient is at position (0,0) in the upper left-hand corner of the matrix and it represents the average of the other 63 values in the matrix [24].

5. THE PROPOSED CHAOTIC ENCODING MODEL

Chaos is a complex non-linear non-equilibrium dynamics process, characterized as follows:

- Chaotic system pattern is an assortment of many methodical acts and each part does not play a leading role under normal conditions.
- Chaos mirrors randomness and hence impulsiveness.
- It is sensitive to necessity on first condition. Even with two identical chaotic systems, if they are in two marginally different first states, they will quickly grow to ward completely diverse states. In the field of information security, the close association between chaotic systems and cryptography is used elaborately. Shadow of the chaotic encoding technology is used in technological applications such as information encryption, secure communications, smart card encryption and digital watermarking. Sine carrier signal plays a major role in modulation and demodulation of information signals in traditional method of confidential communications.

A new proposed image encryption algorithm was set ahead by using and mixing Discrete Cosine Transform DCT with chaotic theory, However, the, researcher is able to study encryption algorithm based on security analysis through viewpoint to Sensitivity analysis of the key, key space and statistical analysis. In DCT the information transmission is very low and key space is great enough to face the aggressive attack with acceptable encryption result.

Now the suggested procedure clarifies the method of encryption and decryption in that order (see Figure 2 and 3). Encryption process is started with transform the image by utilizing Forward Discrete Cosine transform. At that time, the DCT coefficients values are chosen to encrypt using RC4 with the input undisclosed means.

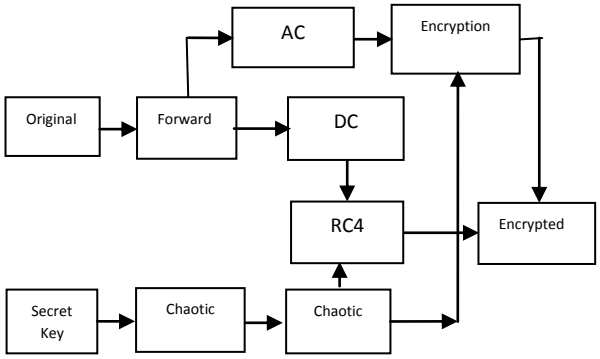

Fig 2: The proposed image encryption model

After that, the chaotic sequence is generated using Henon map method to encrypt the image. Finally, the output of these two encryption operations is merges by swapping its values to get encryption image. The inverse of each operation is done in the decryption model as shown below to decrypt each block and inverse transform to get the reconstructed image.

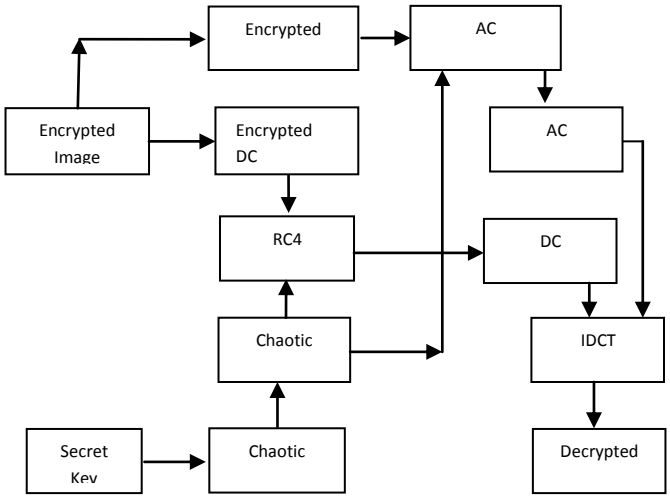

Fig 3: The proposed image decryption model

The following algorithms show the main basic encryption operations:

Algorithm 1: Image Encoding

Input: Original Image I, Parameters and Secret Chaotic Keys

(a, b, X_0, Y_0), where a and b are constants.

Output: Encoded Image I.

- Compute of Forward DCT for Image I.

(DC, AC) = DCT (I)

DC = lowest frequency part, AC = High frequency parts.

- Generate Chaotic Sequence according Henon map:

$$X_{n+1} = Y_n + 1 - aX_n$$
$$Y_{n+1} = bX_n$$

- Convert the sequence Xi, Yi into integer value.
- Encrypt DCT low coefficients using RC4 by Xi:

CDC=RC4_Encryption (DC, *X*)

- Encrypt DCT high coefficients using Chaotic sequence:

CAC= Chaotic Encryption (AC, Y)

- Spread each pixel in DC into each block of the AC according the following chaotic swapping:

C = Chaotic Swap (DC, AC)

- Output C.

The DCT transform is used to transform the input image into frequency domain.

The process is as follows:

- The image is divided into blocks of 8x8 pixels.
- The DCT is achieved for each block and the working is started from left to right and from top to bottom.
- The quantization is performed for each block.
- The compressed block in array is stored in a reduced space.

The top left value is denoted by DC coefficient as a lowest frequency block and the other DCT coefficients are called AC components.

The block is encrypted by the chaotic technique according to Henon map. The chaotic sequence is generated according to the following equation:

$$X_{n+1} = Y_n + 1 - aX_n$$
$$Y_{n+1} = bX_n$$

Where, initial X_0, Y_0 and a, b also input as secret values, these values are converted into integer values to generate secret chaotic sequence X.

The DC coefficients are encrypted by using RC4. The secret key of RC4 is generated from chaotic sequence directly. The cipher value is computed as CDC=RC4_Encryption (DC, X).

The AC coefficient block of transformed image is encrypted, by the chaotic sequence,

The AC coefficient block of transformed image AC is encrypted, where CAC = Chaotic Encryption (AC, Y). The encryption operation is:

$$CAC_i = AC_i \oplus Y_i$$

The final operation of encoding is merging of CDC and CAC by spread each pixel in CDC into each block of the CAC according the following chaotic swapping:

C = Chaotic Swap (CDC, CAC)

The chaotic swapping parameters are:

Ir = $\lfloor X_0 \times 8 \rfloor$

Ic = $\lfloor Y_0 \times 8 \rfloor$

Where Ir and Ic represent the location shifting index of row r and column c for each pixel CDC (i, j).

The CAC is separated into blocks of 8×8 pixels; the first pixel of CDC is swapped with pixel of the first 8×8 block of CAC of indexes Ir and Ic. Suppose CAC represent the first block of AC, then, the first pixel CDC (0, 0) is swapped as follows:

Swap (CDC (0, 0), CAC1 (Ir, Ic))

Swap (CDC (0, 1), CAC2 (Ir, Ic))

and repeat for other CDC pixels. The encrypted image is sent to receiver. The inverse operation of encryption must be processed on receiver side.

The following algorithm shows the decryption operations:

Algorithm 2: Image Decryption

Input: Encryption Image C and Secret Chaotic Keys

(a, b, X_0, Y_0), where a and b are constants.

Output: The Reconstructed Image (RI)

- Separate pixel of C into lowest pixel in CDC and CAC according the invers chaotic swapping:

(CDC, CAC) = Chaotic Swap (C).

- Generate Chaotic Sequence according Henon map:

$$X_{n+1} = Y_n + 1 - aX_n$$
$$Y_{n+1} = bX_n$$

Convert the sequence Xi and Yi into integer value.

- Decrypt CDC and CAC using Chaotic Decryption:

AC = Chaotic Decryption (CAC, Y)

- Decrypt CDC using RC4 by Secret Key X:

DC = RC4_Decryption (CDC, X)

- Compute the inverse of DCT
- Output RI.

The received enciphered image is isolated into lowest frequency parts CDC and CAC according inverse of chaotic swapping.

(CDC, CAC) = Chaotic Swap (C).

With swapping parameter

Ir = $\lfloor X_0 \times 8 \rfloor$

Ic = $\lfloor Y_0 \times 8 \rfloor$

The CAC will be decrypted using chaos decryption. The CDC are decrypted by using RC4 encryption sequence where is generated in the encryption way from secret input values CDC and key X. The inverse of the reconstruction of original image can be implemented when the result of decryption is processed with inverse IDCT transform.

6. SIMULATION RESULTS

The proposed system is implemented using C#.Net with PC with Intel coreTM2 dual processor 2GH, 4GB RAM and 2GB video card based on Windows 8.1 operating system. This system is repeatedly implemented and tested for five pictures;

Lena, children, bear, hours and city (see Figure 4 Lena image and its histogram).

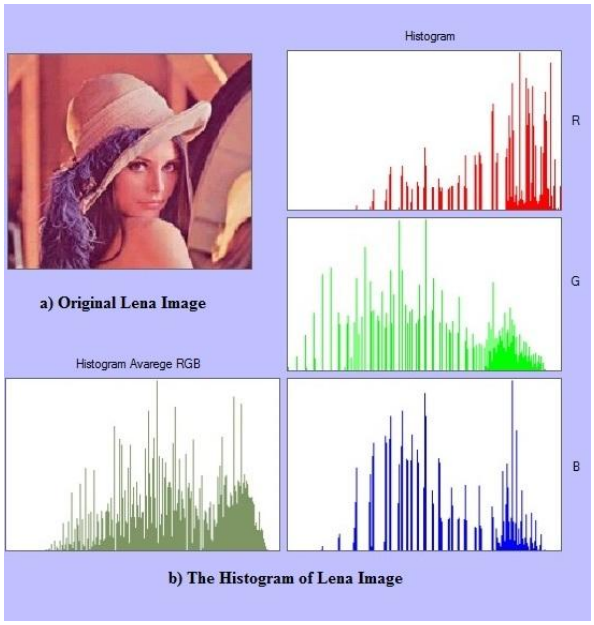

Fig 4: The original image histogram

Figure 5 shows the encryption image and the histogram of it. The encryption image appears as scramble image. In addition, the histogram do not indicate any information for the original image, the randomness characteristics covered the image information. In addition, the histogram of the original image has randomness, but after encryption these randomness covered.

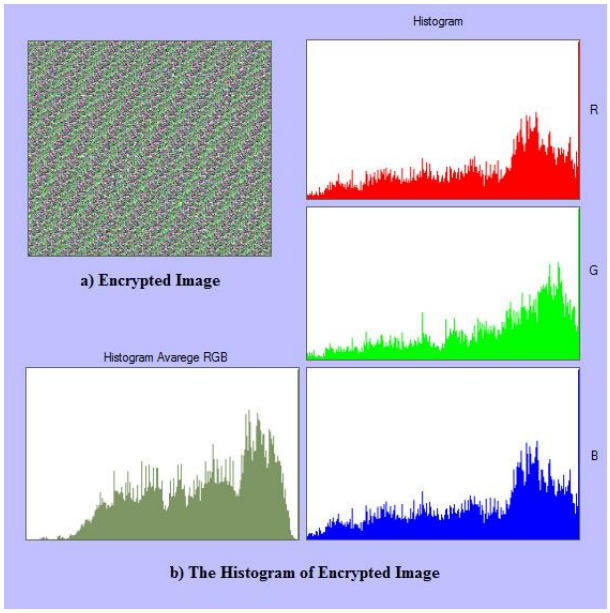

Fig 5: The encoded image histogram

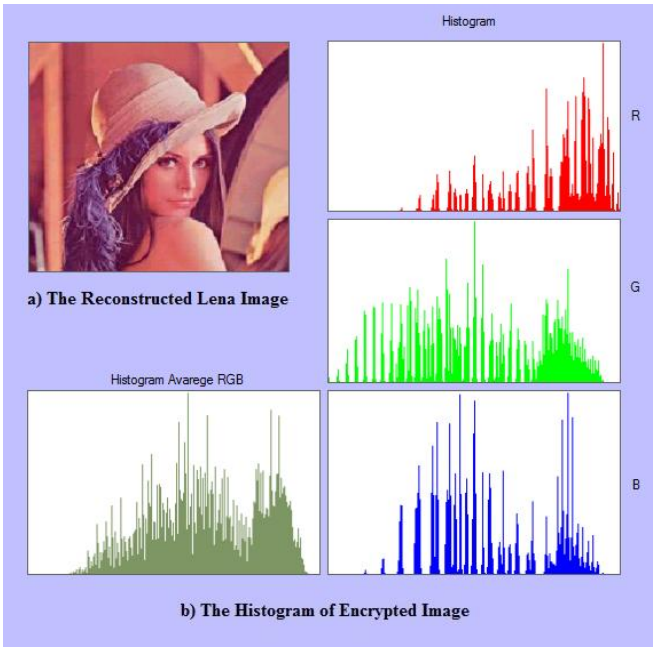

Fig 6: The Reconstructed Image Histogram

In Figure 6, the reconstructed image is computed by decryption. Reversing each processing step in image encryption will achieve decryption. There is small difference between original and reconstructed images as shown in the histogram. Table 3 shows the peak signal to noise ratio (PSNR).

Table 3. PSNR of five tested image

Image	PSNR
Lena	44.27
Children	44.50
Bear	44.43
Hourses	44.41
City	44.36
Average	44.42

All values greater than 28 dB, which indicated to good quality for reconstructed image. Table 4, shows the mean of execution time of each operation in the encryption and decryption stages. The time execution is computed by seconds. The execution time of inverse of discrete cosine transform always less than foreword cosine transform due to its operations. In addition, the execution time of most decryption operation is less than encryption operation. Finally, the execution time of decryption stage is less than execution time of encryption stage.

Table 4. Execution time of five-tested image

Image	Image Transform Time		Image Encryption / Decryption Time	
	DCT	IDCT	Encryption	Decryption
Lena	1.86	2.68	0.0068	0.0068
Children	1.85	2.68	0.0068	0.0068
Bear	1.85	2.68	0.0063	0.0064
Hourses	1.85	2.68	0.0062	0.0063
City	1.86	2.68	0.0065	0.0066
Average	1.85	2.68	0.0065	0.0065

7. CONCLUSIONS

The obtained results show the effectiveness of the proposed image encryption technique. The DCT transform is used to encrypt DC by RC4 and the most important information (lowest frequency values) can be isolated because Henon map have two keys, the first key is used to encrypt the DC values in block and the second key is used to encrypt the remaining AC values in block. The key space is enough to protect this method and refuse the brute force attack with high security. Chaotic encryption application provides by using two secret keys as a primitive key to generate secret chaotic key sequence of pseudo-random key to encrypt the DC and AC rest image blocks. It is fast technique where the average of each encryption or decryption stag. The reconstructed image has good quality compared to original image, where the average of PSNR is about 44.4 dB. For future works, the size of key can be increased to avoid most of image encryption attacks. The powerful encryption like AES and RSA can be used instead of RC4 to increase the complexity of encryption or used public key cryptosystem.

8. REFERENCES

[1] Matthews, R A J., On the Derivation of a Chaotic Encryption Algorithm, Cryptologia, 1989, 13(1), 29-42.

[2] Shannon, C., Communication Theory of Secrecy Systems, Bell System Technical Journal, 1949, 28(4), 656–715.

[3] Baptista, M.S., Cryptography with Chaos, Physics Letters A, 1998, 240, 50–54.

[4] "RC4 Encryption Algorithm. htm ",vocal Technologies, Ltd. 520 Lee Entrance, Suite 202 Amherst New York 14228Email: sales@vocal.com.

[5] Yen, J.C. and Guo, J.I., A New Chaotic Key Based Design for Image Encryption and Decryption, Proceedings of the IEEE International Symposium Circuits and Systems, 2000, 49-52 Vol.4.

[6] Rahma, A.S. and Yacob, B. Z, Real-Time Partial Encryption of Digital Video Using Symmetric Dynamic Dual Keys Algorithm (SDD), Eng.& Tech. Journal ,2012, 30(5).

[7] Rahma, A.S. and Ali, M. A., To Modify the Partial Audio Cryptography for Haar Wavelet Transform by Using AES Algorithm, Eng. & Tech. Journal, 2014, 32(1).

[8] Yen, J.C and J. I. Guo, A New Chaotic Image Encryption Algorithm, Proceedings of National Symposium on Telecommunications, 1998, 358-362.

[9] Yen, J. C. and J. I Guo., A New Chaotic Mirror-Like Image Encryption Algorithm and Its VLSI Architecture, Pattern Recognition and Image Analysis, 2000, 10(2), 236-247.

[10] Yen, J. C. and J. I. Guo., Efficient Hierarchical Chaotic Image Encryption Algorithm and Its VLSI Realization, Proceedings of IEEE Vision, Image and Signal Processing, 2000, 147(2).

[11] Fridrich, J., Symmetric Ciphers Based on Two-Dimensional Chaotic Maps, Int. J. Bifurcation and Chaos. 1998, 8(6).

[12] Fridrich, J., Image Encryption Based on Chaotic Maps, Proceedings of IEEE Conference on Systems,Man, and Cybernetics, 1997, 1105-1110.

[13] Alireza Jolfaei (Corresponding author) 2011. "Image Encryption Using Chaos and Block Cipher". Computer and Information Science Vol. 4, No. 1; January 2011.

[14] Logistic aps, https://en.wikipedia.org/wiki/Logistic_map, Accessed Sep. 2015.

[15] Naess, A., Chaos and Nonlinear Stochastic Dynamics, Probabilistic Engineering Mechanics, 2000, 15, 37-47.

[16] Sheng, Y., Wavelet Transform, CRC Press LLC, 2000.

[17] S., Gilbert and N., Truong, Wavelets and Filter Banks, Wellesley-Cambridge Press, 1997.

[18] Giesl, J. andVlcek, K., Fractal Image Compression using the wavelet transformation,Proceedings of International Workshop Control and Information Technology, 2007.

[19] Podoba, T, Giesl, J., and Vlcek, K., Image Encryption In Wavelet Domain Based on ChaoticMaps, Proceedings of International Congress on Image and Signal Processing, 2009, 1-5.

[20] A. Sinha, K. Singh, Image Encryption by using Fractional Fourier Transform and Jigsaw Transform in Image Bit Planes, Optical Engineering, Optical Engineering, 44(5), 2005, 15-18.

[21] A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna,A New Image Encryption Approach using Combinational Permutation Techniques, Int. J. on Electrical and Computer Eng.,2006, 1(2), 127- 132.

[22] Li. Shujun, X. Zheng, Cryptanalysis of a Chaotic Image Encryption Method, Proceedings of IEEE InternationalSymposium on Circuits and Systems, 2002, II-708 - II-711 Vol.2.

[23] G. Zhi-Hong, H. Fangjun, and G. Wenjie, Chaos-based image encryption algorithm, Physics Letters A, Vol. 346, Iss. 1–3, 2005, 153–157.

[24] PanuRanta, Adapting Media Elements of MMS Messages Using Digital Signal Processor, Master thesis,Helsinki University of Technology.

[25] PianHui Wu, Research on Digital Image Watermark Encryption Based on Hyper Chaos, PhD Thesis, 2013, University of Derby.

[26] Maqableh, Mahmoud, Mohammad (2012) ."Analysis and Design Security Primitives Based on Chaotic Systems for e Commerce", Durham theses, Durham University. Available at Durham E-Theses Online: http://etheses.dur.ac.uk/738/

[27] Sapna Sasidharan , Deepu Sleeba Philip, "A FAST PARTIAL IMAGE ENCRYPTION SCHEME WITH WAVELET TRANSFORM AND RC4 ", The College of Information Sciences and Technology © 2007-2015 The Pennsylvania State University.