A Simple Chaotic Image Cryptography Algorithm Based on New Quadratic Chaotic Map

Saad Muhi Falih
Department of Computer Technical Engineering, Islamic University College
saadmuheyfalh@gmail.com

Abstract

The chaos based cryptographic methods have been suggested some new and efficient algorithms to develop image encryption techniques because of its exceptionally desirable properties of sensitivity to initial condition and parameters of chaotic map. However, this paper proposes a new symmetric image encryption system (SIES) that based on a new class of quadratic chaotic map. In this proposed scheme, the image is converted to a stream of serial bits which modulo-2 added with the stream of binary chaotic sequence generated using a new class of quadratic chaotic map. Finally, the proposed system is tested under Matlab environment and results show that the proposed technique is efficient and has high security features.

Keywords: chaos, chaotic map, chaotic sequence generated, Image cryptographic.

الخلاصة

اقترحت العديد من خوارزميات التشفير المعتمدة على النظم الفوضوية الجديدة والفعالة لتطوير تقنيات تشفير الصور لما تمتلكه هذه النظم من خصائص ومميزات تصميمية جيدة كحساسيتها المفرطة للشروط الابتدائية ولقيم معاملات المخططات الفوضوية. على كل حال، اقترح هذا البحث طريقة جديدة للتشفير المتماثل للصور مستنداً الى نوع جديد من المخططات الفوضوية التربيعية. في هذه الخوارزمية المقترحة، الصورة تحول الى سلسلة من الاعداد الثنائية والتي تجمع مودولو−2 (modulo-2) مع سلسلة الاعداد الثنائية الفوضوية المولدة باستخدام المخطط الفوضوي التربيعي. وفي ختام البحث تم اختبار الخوارزمية المقترحة بعد بنائها في بيئة ماتلاب (Matlab) وأظهرت النتائج أن التقنية المقترحة تتمتع بفعالية عالية ولها ميزات أمان متميزة.

الكلمات المفتاحية: الفوضى ، المخططات الفوضوية ، مولدات الاشارة الفوضوية ، تشفير الصور.

1. Introduction

With the rapid development of communication systems and Internet, digital images and other multimedia are more commonly and frequently transmitted in the public communication network. Therefore, the protection of digital information against illegal copying and distribution has become extremely important, and image encryption technology becomes an important issue in the encryption field. Many new encryption schemes have been proposed in literature (Chang, 2001;Guan, 2005). Some researchers proposed conventional encryption methods for encrypting images and multimedia. However, this is not efficient method due to the large data size and real-time constraints of image data. The conventional encryption methods require a lot of time to directly encrypt thousands of image pixels value. On the other hand, textual data, a decrypted image is mostly acceptable although it contains small levels of distortion. Therefore, for these two mentioned reasons, the algorithms that function well for textual data may not be suitable for multimedia data (Soleymani, 2012). On the other hand, the chaotic encryption algorithms has been suggested as a new, fast, and efficient way to deal with highly secure image encryption, and it has been proved that in many proposed chaotic encryption algorithms has analogous but different characteristics as compared with conventional algorithms (Jakimovski, 2001;Mao,2004).

The chaos has been introduced to cryptography all the credits to its ergodicity, pseudo-randomness and sensitivity to initial conditions and control parameters, which are close to confusion and diffusion in cryptography. However, these properties make chaotic systems as a potential choice for constructing cryptosystems (Ye, 2011).

One of the remarkable features of chaotic algorithm is their sensitivity to initial conditions. In other words, for a typical chaotic algorithm, even when there is a very minor variation in the initial conditions, the system dynamics will be varied tremendously. Based on this concept, when a chaotic data generator is used as the key(s)

in a cryptosystem, this system sensitivity to initial conditions will substantially increase the complexity for a hacker to guess (and hack) the system.

The studies on chaos-based image cryptosystems can be classified into two categories. In the first one; a pixel is considered as the smallest element, and a digital image is considered as a collection of pixels. On the other hand, in the second category; a pixel can be further divided into a number of bits, on which bit-level operations are performed. However, in this study the second category are chosen because of the superior performance compared to the first one (Fu, 2014). In this paper, an image encryption scheme based on a new class of quadratic chaotic map is proposed and built under Matlab environment. However, the good performance and the simple procedure design are the main advantages of this proposed method.

The rest of the paper is organized as follows: Section 2 looks at the generating chaotic binary sequence based on quadratic chaotic map and gives some discussion on it; Section 3 reports the proposed design procedure; the experimental results and security analysis of the proposed encryption and decryption algorithms are discussed in section 4; Finally, the conclusion is summarized in section 5.

2. The Proposed Chaotic System and Its Properties

a. Chaotic Map

The chaotic map is a simple nonlinear model, but it has a complicated dynamic behavior. The chaotic sequence produced by the chaotic map is extremely sensitive to the change of its initial value. Any chaotic map can be defined as (Azou, 2002):

$$x_n = f(x_{n-1}) \quad , \quad k = 0, 1, 2, \ldots \tag{1}$$

Where x_n is called the state, and $f(x_{n-1})$ maps the state x_{n-1} to the next state x_n . However the chaotic map proposed here can be written as:

$$x_n = 1 - r(x_{n-1})^2 \tag{2}$$

This system exhibits a great variety of dynamics, depending upon the value of the bifurcation parameter *(r)*.

A complete picture of the chaotic map behaviors can be got by studying the bifurcation diagram, which is a graphical depiction of the relationship between the values of one parameter and the behavior of the system in which the parameter is being measured (Pratt, 2008), and The magnitude of the Lyapunov exponent, which is an indicator of the behavior of the system, if the value of Lyapunov exponent is negative then this refer to the stable behavior of the system, on the other hand, the positive value refer to the chaotic behavior (Diks, 1999).

Figure (1) is showing the bifurcation diagram of the proposed chaotic map, it is clear from the figure that the bifurcation parameter *(r)* must be greater than 1.43 to get the chaotic behavior. However, there is some stable islands in this chaotic margin located at *r*= 1.477, 1.631, and 1.75. These stable islands must be avoided to get a good chaotic signal from this map.

On the other hand, the Lyapunov exponent for one dimension map is defined as (Diks, 1999):

$$\lambda = \lim_{n\to\infty} \left(\frac{1}{n} \sum_{i=0}^{n-1} \ln \left| \acute{f}(x_i) \right| \right) \tag{3}$$

Where $\acute{f}(x_i)$ is the first derivative of $f(x_i) = x_{n+1}$ which is equal to $(1 - r(x_n)^2)$ in the proposed chaotic map.

$$\therefore \lambda = \lim_{n\to\infty} \left(\frac{1}{n} \sum_{i=0}^{n-1} \ln(|-2rx_i|) \right) \tag{4}$$

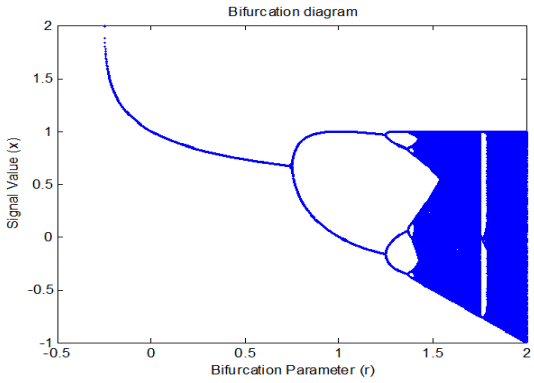

Figure 1: Bifurcation diagram of the proposed chaotic map.

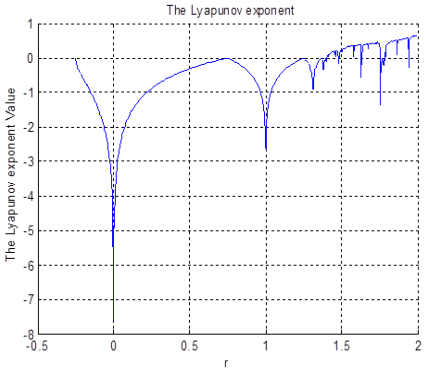

Figure 2: Lyapunov exponent value as a function of bifurcation parameter of the proposed chaotic map.

Figure (2) shows the value of Lyapunov exponent with respect to bifurcation parameter *(r)*. In this figure the location of the stable islands and the chaotic region are very clear in the diagram depending on the value of Lyapunov exponent as described previously.

b. Chaotic Binary Sequence Generator

The block diagram for the proposed chaotic sequence generator is shown in Figure (3). The chaotic sequence generator shown in the block diagram generates random chaotic signal from chaotic quadratic map for different initial values x_o and the bifurcation parameter *r*. the random chaotic signal is mapped to binary to generate the final chaotic binary sequence.

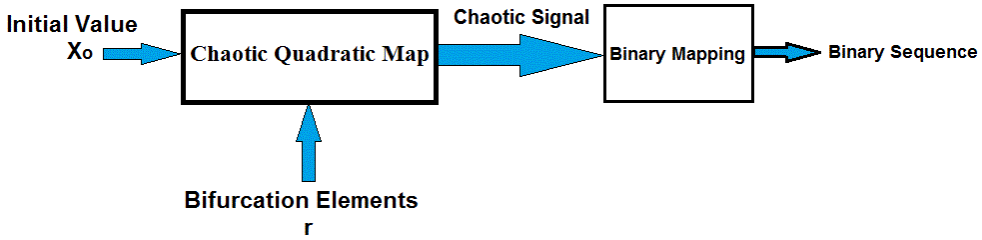

Figure 3: Block diagram for chaotic sequence generator.

The proposed chaotic sequence generator shown in Figure (3) is built in Matlab environment. However, the initial conditions of the chaotic map used in this simulation program has been taken as *xo=0.2* and *r=2*.

Figure (4) is showing the chaotic binary sequence generated by using the proposed chaotic map.

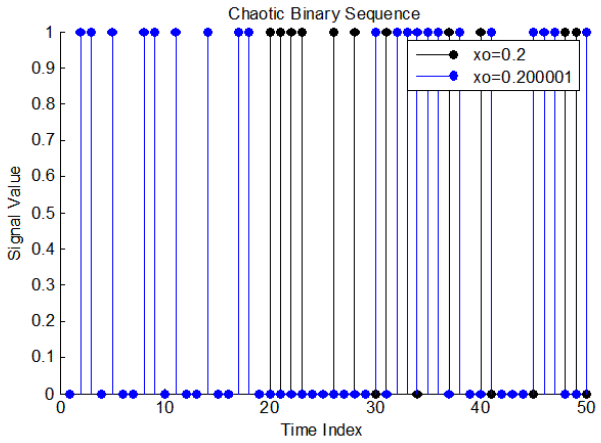

Figure 4: The chaotig binary sequence genration by the proposed genrator.

3. The Proposed Design algorithm

In this section, we are introducing the step-by-step procedure of the proposed algorithm for encryption and decryption algorithm as shown in Figure (4) and Figure (5), respectively. Let $Imag$ be an image of size $\times N$. The pixel of $Imag$ is denoted by $Imag(i,j)$, where i and j is in the range of $1 \leq i \leq M$ and $1 \leq j \leq N$. Basically, $Imag(i,j)$ denotes the gray levels in the range 0 to 1 at the pixel position (i,j) of an image, however, this pixel value is represented by 8-bit binary notation.

Step No.	Operation	Description
Step 1	$Imag \leftarrow Read\ an\ image$	Read an image
Step 2	$Stream\ bit\ Image \leftarrow convert\ Imag$	Convert image to stream bit
Step 3	$Key \leftarrow Generate\ the$ chaotic sequence as discused in previose section	Generate key sequence
Step 4	$Cipher\ Image \leftarrow Stream\ bit\ Image \oplus Key$	Determine cipher image

Figure 4: The proposed encryption algorithm.

Step No.	Operation	Description
Step 1	$Cipher\ Image \leftarrow Read\ an\ Cipher\ Image$	Read cipher image
Step 2	$Key \leftarrow Generate\ the$ chaotic sequence as discused in previose section	Generate key sequence
Step 3	$Stream\ bit\ Image \leftarrow Cipher\ Image \oplus Key$	Convert stream bit image to matrix pixel image
Step 4	$Image \leftarrow convert\ Stream\ bit\ Image$	Determine image

Figure 5: The proposed decryption algorithm.

4. The Experimental Results and Security Analysis

The experimental results of the suggested encryption and decryption algorithms have been fully discussed here. The suggested algorithm is built under the Matlab environment and the test done on personal computer has a core i5 CPU operates in clock speed equal to 2.53 GHz. However, the selected images used in these experiments are "Flowers.bmp", "Cameraman.bmp", and "Mountain.bmp" which are 640 × 480, 512 × 512, and 640 × 480 gray images. The operation of the proposed algorithm is shown in Figure (5), where the original, encrypted and decrypted images are shown.

In the next subsections, several tests have been done on the proposed algorithm to check the security. Some of these tests done on the encrypted key to measure its strength, and the other done on the cipher image and the original image, which can be described as statistical analysis, to extract the relationships between them.

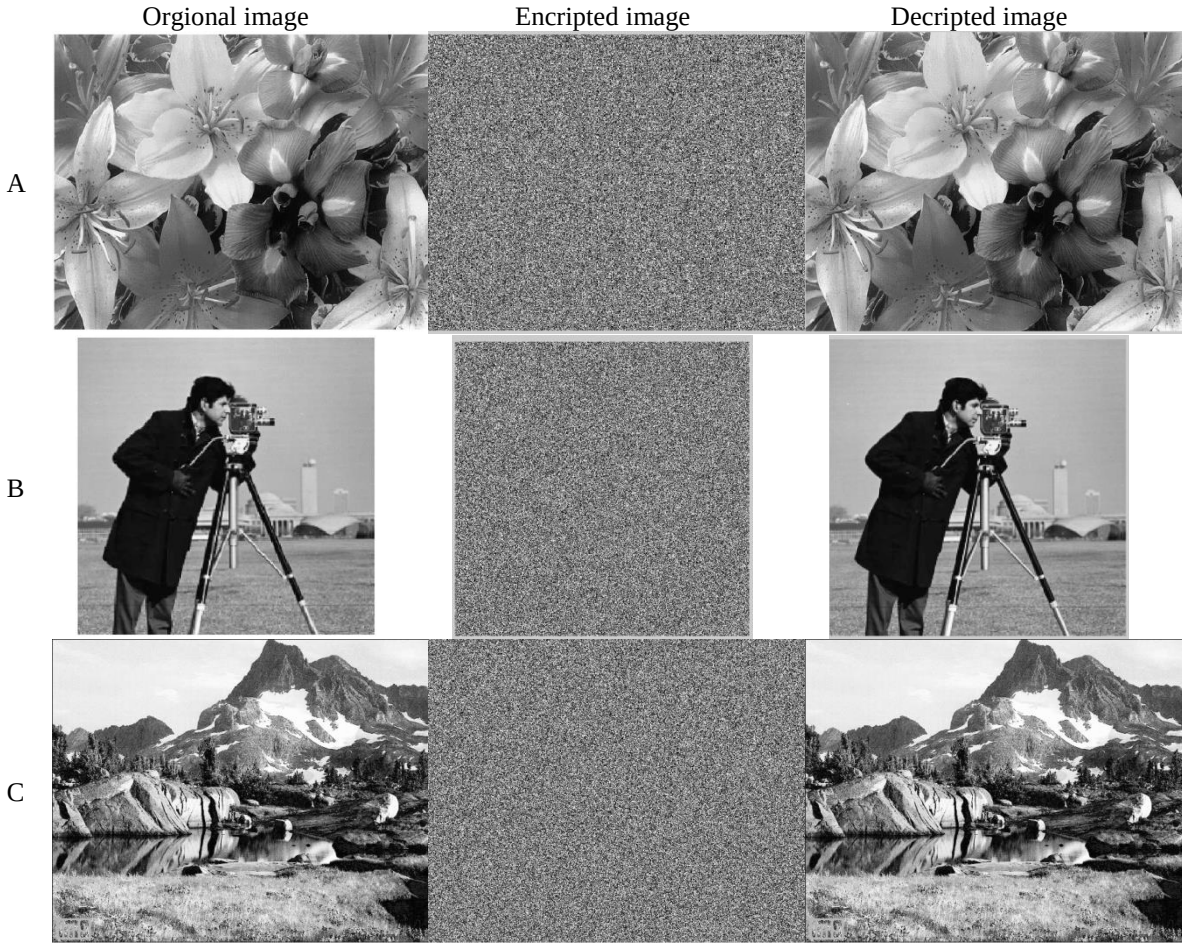

Figure 5: operation of encryption and decryption algorithms using a) Flowers.bmp, b) Cameraman.bmp, and c) Mountain.bmp.

4.1 Encryption Key Space Test

The encryption key space of any encryption system is defined as the total number of the possible keys which can be used as encryption key. Therefore, the security of any encryption system is increase with increase the key space. In the suggested algorithm, the initial value (x_o) of the quadratic chaotic map and the defragment parameter (r) were used as the encryption keys. The test result is shown in Table (1), which is reported the accepted bound value for each variable and calculate the overall number of the possible keys may be used. However, the total key space produce from two parameters will be approximately 2^{106} (or 1.14×10^{32}) which is very good key space compared with key space of the Data Encryption Standard (DES) which has only 2^{56} (or 7.2058×10^{16}) (Srinivas, 2014).

Table 1: Range of parameter value and key space

The acceptable range of (x_0)	**-1 - 1**
Smallest change in x_0 change encryption key	**10^{-16}**
The acceptable range of (r)	**1.43 - 2**
Smallest change in r change encryption key	**10^{-16}**
Total No. of trails needed (key space)	**2^{106} (or 1.14×10^{32})**

4.2Encryption Key Sensitivity Test

The key sensitivity can be defined as the magnitude of the difference between two encryption images encrypted by two keys differs between them by very small change. However, the strength encryption algorithm should have high sensitive to any change in encryption key.

In this test, the encryption key is a little changed by adding 1 to the 16^{th} digit after the decimal point of the original value, i.e., modified (x_o=0.2000000000000001, and r=2) to (x_o=0.2000000000000002, and r=2), and the variation in the corresponding decryption images is calculated. The original flowers image is display in Figure 6(a), and the encryption image by (x_o=0.2000000000000001, and r=2) is depicted in Figure 6(b), Figures 6(c) and 6(d) are displaying the decryption images using (x_o=0.2000000000000001, and r=2) and (x_o=0.2000000000000002, and r=2), respectively. However, the results are proved that the suggested encryption algorithm has very high sensitivity to the change of the encryption key.

4.3Histogram Analysis

The histogram of any image is a chart showing the distribution of the pixel intensity values. For example, in the 8-bit gray scale image, there are 256 different possible intensities. Therefore, the histogram of it will be display 256 numbers showing the distribution of the pixels amongst those intensities values. However, the histogram of a good cipher image must have a fairly uniform shape for any plain images.

The histograms of the several original images which have widely different content as well as the histograms of its encrypted images are shown in Figure (7). However, the nearly uniform histograms of the encrypted images refer to no information about the plain images that can be gathered through histogram analysis and this attributed to the good encryption process.

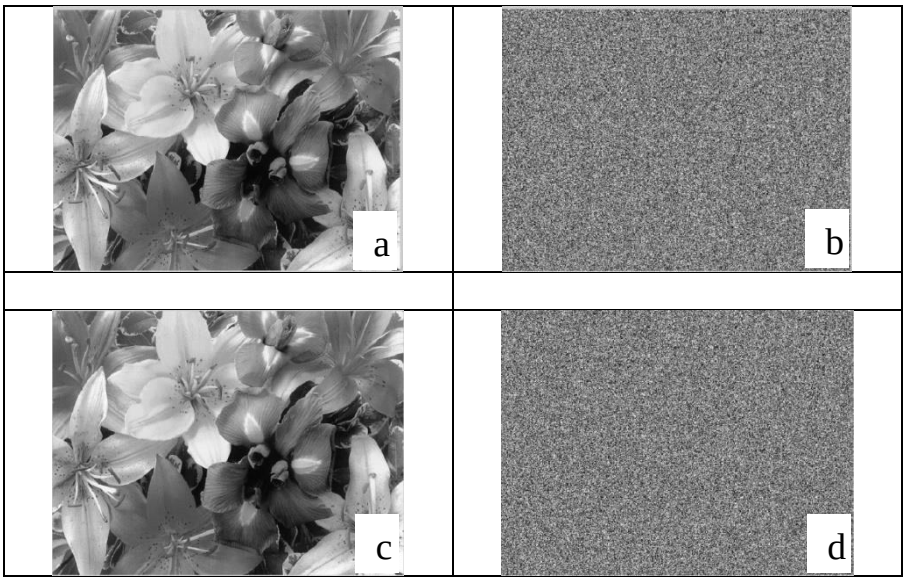

Figure 6: Key Sensitivity test; a) original image, b) cipher image, c) decryption image with the same encryption key, and d) decryption image with slightly change in encryption key.

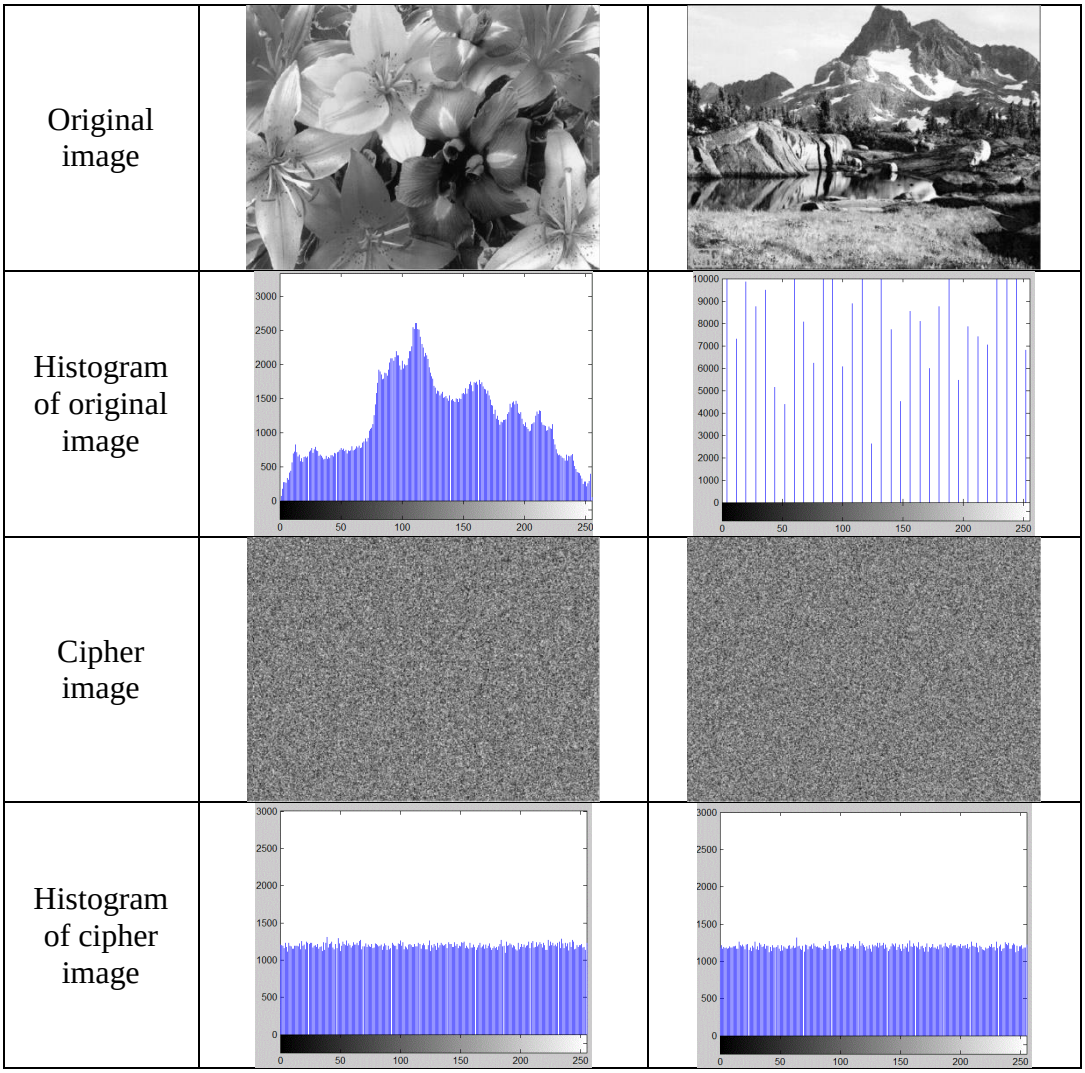

Figure 7: Histogram analysis of the proposed encryption algorithm.

4.4Correlation Coefficient

The correlation coefficient can be defined as a coefficient represents the statistical dependents between two measured quantities. However, the correlation coefficient (Cor) was the first widely used authoritative correlation measure in the image processing. The correlation coefficient for monochrome digital images is defined as (Rodgers, 1988):

$$Cor = \frac{\sum_{i=1}^{N}[(x_i - x_m)(y_i - y_m)]}{\sqrt{\sum_{i=1}^{N}(x_i - x_m)^2}\sqrt{\sum_{i=1}^{N}(y_i - y_m)^2}} \quad (1)$$

Where, N is the number of pixels in the image, x_i and y_i are intensity values of i^{th} pixel in 1st and 2nd image respectively. Also, x_m and y_m are mean intensity values of 1st and 2nd image respectively. The correlation coefficient equal to *1* if the two images are completely identical, on the other hand, if the correlation coefficient equal to *0* this means they are completely different, finally, if the correlation coefficient equal to *-1* indicate to that the two images are completely anti-correlated (Jen, 2012).

The correlations coefficient between the original image and the encryption image was computed using the above formulas and the results are shown in Table (2).

From the correlations coefficient values calculated, one can be said that the encryption images are completely different from the original images.

Table 2: Correlation coefficient test

Image	Correlation Coefficient
Flowers	0.0013
Cameraman	0.0046
Mountain	0.0021

4.5 Information Entropy Analysis

The entropy *H(m)* is statistical measure of uncertainty in information theory, defined as (Zhang, 2014):

$$H(m) = -\sum_{i=0}^{255} p(m_i) log_2(m_i)$$

where $p(m_i)$ is the probability mass function of the occurrence of symbol m_i. We consider that there are 256 states of the information in image with the same probability. We can get the perfect $H(m) = 8$, which indicate to a true random source. Table 3 is shown the calculated values of the information entropy of the original gray scale images and their corresponding encrypted images. The calculated results is indicate to that all the entropies values of the encrypted images are very close to the theoretical value of 8, which proved that the proposed chaotic cryptographic scheme is robust against entropy analysis.

Table 3: the entropy of the orgional and cipher images

Image name	Entropy of the original image	Entropy of the encryption image
Flowers	7.8171	7.9993
Cameraman	7.0941	7.9993
Mountain	4.7981	7.9995

5. Conclusion and suggestion for future works

In this work a new image encryption algorithm have been proposed. This algorithm is based on a new quadratic chaotic map. The encryption key stream is generated from quadratic chaotic map by choosing initial condition and defragment parameter, and then the encryption process can be done by adding (*modulo-2*) the stream pits of image to the encryption key generation from quadratic chaotic map. The study is shown that the suggested algorithm gives a good performance under the key space analysis, key sensitivity analysis, histogram analysis, correlation coefficient and information entropy tests. Finally, to the future works, a new binary random generator based on the chaotic linear feedback shift register will be proposed to modify the performance of the encryption system.

6. References

Azou, S. , Burel G. , and Pistre C., 2002, "A Chaotic Direct-Sequence Spread-Spectrum System for Underwater Communication", IEEE-Oceans'2002, Biloxi, Mississippi, October 29-31.

Chang C. C. , Hwang M. S., and Chen T. S., 2001, "A new encryption algorithm for image cryptosystems", Journal of Systems and Software, Vol.58, pp. 83–91.

Diks C. ,1999, "Nonlinear Time Series Analysis: Methods and Applications", Word Scientific Publishing Co. Pte. Ltd., Singapore, Vol.4, pp. 27-31.

Fu, C. , Huang J.-B., Wang N.-N., Hou Q.-B., and Lei W.-M., 2014, "A symmetric chaos-based image cipher with an improved bit-level permutation strategy," Entropy, Vol. 16, No. 2, pp. 770–788.

Guan, Z. H. , Huang F.J., Guan W.J., 2005, "Chaos-based Image Encryption Algorithm", Physics Letters A, Vol. 346, pp. 153–157.

Jakimovski G. and Kocarev L., 2001, "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps", IEEE Trans. on Circuits and Systems, Part I, Vol. 48, No. 2, pp.163- 169.

Jen, E. K . , Johnston R. G., 2012, "The Ineffectiveness of Correlation Coefficient for Image Comparisons", Research Paper prepared by Vulnerability Assessment Team, Los Alamos National Laboratory, New Mexico.

Mao Y. B. , Chen G., Lian S.G. ,2004, "A novel fast image encryption scheme based on the 3D chaotic Baker map", International Journal of Bifurcation and Chaos, Vol. 14, pp. 3613-362.

Pratt S. S. , 2008, "Bifurcations Are Not Always Exclusive", An International Journal of Complexity and Education, Vol. 5, No. 1, pp. 125-128.

Rodgers, J. L. , Nicewander W.A., 1988, "Thirteen Ways to Look at the Correlation Coefficient", The American Statistician, Vol. 42, No. 1, pp.59-66.

Soleymani A. , Ali Z. and Nordin M., 2012, "A survey on principal aspects of secure image transmission," in Proceedings of World Academy of Science, Engineering and Technology, pp. 247–254.

Srinivas B. L. ,*et.al.* , 2014, "A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, Vol 2, No.5, pp.77-88.

Ye, R. , Zhou W., 2011, "An Image Encryption Scheme Based on 2D Tent Map and Coupled Map Lattice", International Journal of Information and Communication Technology Research, Vol. 1, No. 8, pp. 344-348.

Zhang X. and Cao Y., 2014, "A Novel Chaotic Map and an Improved Chaos-Based Image Encryption Scheme", The Scientific World Journal, Vol. 2014, Article ID 713541.