Vol. 9(33), Jul. 2019, PP. 4228-4240

Contents list available at IJMEC

International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)

Journal Homepage: www.aeuso.org

PISSN: 2411-6173 - EISSN: 2305-0543

# Image Cryptography Based on Multi-Ciphering Chaotic Process

*Abbas Salman Hameed* and WeaamTalaat Ali*

*College of Engineering, University of Diyala, Diyala, Iraq*

****Corresponding Author's E-mail:** abbasfuture@yahoo.com*

***Abstract***

With the development of computing techniques, digital image security become an ever-increasing issue of daily life. As computer software and hardware evolves and as more of it becomes accessible of an Internet application or services, image security has gone from simple image protection into complex levels of image encryption. Recently, the chaotic signals are increasingly used in cryptography systems. The systems which generate chaotic signals have many desirable properties such nonlinearity, randomness and sensitivity to initial conditions. All these properties owned by chaotic systems are guarantee a highly secure and robustness for encryption process. In this project, Logistic map and Modified Arnold Cut mapping as chaotic signal generators are used to encrypt the digital gray scale and color images. A multi-ciphering process based on chaotic maps are used to generate high secure encryption scheme. The simulation results show that, the proposed algorithm has a large key space (more than $2^{230}$) to resist all kinds of brute-force attacks and encryption algorithm which are very sensitive to the secret keys. When any small change in any of the system parameters occur, a low Peak Signal to Noise Ratio PSNR (around 8.2 dB) is obtained for the decrypted image. Also, perfect PSNR is obtained when use the same system parameters. The histogram of the encrypted image is fairly uniform, the low normalized correlation which shows a good statistical property for the cipher-image and high NPCR (Number of Pixel Change Rate) is around 99.62%. Therefore, high complicated image security is offered using the proposed encryption scheme.

***Keywords:*** *Cryptography, chaotic system, Logistic map,* Arnold cut map*.*

## 1. Introduction

Nowadays, the widely communicated of digital image information over the Internet and wireless networks has become the protection of digital image against third parity an important issue. The employing of encryption algorithm is a direct and obvious way to protect image data from unauthorized eavesdropping. Unfortunately, the renowned block ciphers, such as DES, AES, and IDEA, are not suitable for practical image encryption [1]. This is because the security of these algorithms is mainly ensured by their high computational cost, making them hard to meet the demand for online communications when dealing with digital images characterized by bulk data capacity. To meet this challenge, many different encryption technologies have been proposed. Among these technologies, the chaos-based algorithms provide an optimal trade-of between security and efficiency. Fridrich was suggest a first chaos-based image encryption scheme in 1998 [2]. After that, many cryptosystem based chaos are proposed [3-7]. Chaotic systems are characterized by extremely sensitive to initial conditions



**Article History:**
**Received Date: Feb. 18, 2019**
**Accepted Date: Mar. 15, 2019**
**Available Online: Jul. 01, 2019**

and control parameters and mathematically is defined as randomness governed by simple deterministic rules [6]. Therefore, chaotic signals are very suitable to be used in encryption algorithms.

This paper demonstrates image cryptography based on three chaotic keys extracted from two chaotic maps. The proposed system depicts the advantages of the used multiple maps in encryption scheme. Also, it offers increasing in the key space for cryptosystem by enlarging the parameters number which controls the response of chaotic signal used in encryption and decryption processes. Therefore, the security level of cryptosystem will be increase. Many permutation and diffusion processes use in the proposed system which leads to a great reduction in the correlation among neighboring pixels and generates unpredictable image.

The paper is organized as follows; section 2 describes chaotic maps and keys. In section 3, the proposed system model. The Statistical Factors, Results and Simulation are presented in section 4. Finally, conclusions are clarified in section 5.

## 2. Chaotic maps and keys:

### 2.1. Logistic and Arnold Cat Maps

Logistic map is one of the simplest nonlinear systems introduced by Pierre Franois Verhulst in 1838 [8]. The logistic map is defined as: $x_{n+1} = r x_n(1 - x_n)$, where $x_n$ and $r$ are the system variable and control parameter, respectively. Logistic signal can demonstrate a wide range of behaviors, from a stationary when $r$ is close to 0, to a chaotic when $r$ is close to 4, all with values of $x_n \in (0,1)$. Logistic signal will be in chaos state if $r \in [3.57,4]$.

Arnold Cat Map (ACM) is another chaotic map used in encryption process in order to shuffled the image pixels which leads to secure images. Which when applied to a digital image randomizes the original organization of its pixels and the image becomes imperceptible or noisy. In this way, it is becoming exponentially hard to recover the initial image without knowing the original transformation or the secret key. However, ACM has a cycles $p$ to shuffle image pixels and if iterated $p$ number of times, the original image reappears [4].

The generalized form of ACM can be given by the transformation: [4].

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{M} \quad (1)$$

where, x, y {0, 1, 2 … $M$ −1} and $M$ is the size of a digital image.

It can easily be seen that the original Arnold transformations given by Equation (1) can be modified to produce a sequence of Modified Arnold Cat Map (MACM) [4] by introducing new three parameters (a,b,c) to increase and ensure high security implementation as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & b + c^2 \\ a & 1 + a\,b + a\,c^2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{M} \quad (2)$$

where a,b and c are positive integer values considered as a control parameters and (a, b, c)$\in$ R, x' and y' are the coordinate values of the shuffled pixel.

### 2.2. Structures of Encryption Keys

With proposed scheme, many chaotic maps are used to generate chaotic keys. These keys applied on original image to demonstrate the confusion and diffusion processes.

**a) key 1 (Confusion process):**

The Modified Arnold cut mapping is used to permutation pixels location as first security process to generate encrypted image according to equation (2). This key is very sensitive to ***a, b, c***, and ***p*** parameters of MACM.

**b) key 2 (Diffusion process):**

The second key which is used to encrypt image generates by convert a logistic chaotic sequence with specific parameters to integer numbers. After that, the chaotic real sequences are XORing with the pixel's values to diffusion it and generate new diffused image. Equation (3) is used to transform real logistic sequence (between 0 and 1) to an integer sequence, where individual integer's range is from 0 to 255, by magnifying, rounding and modulo $10^i$using the formulas: -

$$V_{Int}(n)= \text{mod}\ (\text{floor}(\ V_{Real}(n) \times 10^{i}),256) \quad (3)$$

where:- i number which depends on chaotic type, for logistic map i=14.

As example, assume pixels have value = [3 5 66 77 155 88 90 255 1], and the key2 have [44 5 23 54 56 76 12 11 76], the diffusion pixels will be [47 0 85 123 163 20 86 244 77].

**c) key 3 (Confusion process):**

The third key generates by take the order of other logistic sequence with specific parameters and applied it to shuffled image pixels. To generate that, many steps will be done as:

1- generate a random chaotic sequence with specific parameters from logistic map, as example let assume the sequence is:

[0.4000 0.8880 0.3680 0.8605 0.4444 0.9134 0.2926 0.7658 0.6636 0.8259]

2- Rearrangement the generated sequence with ascending arrangement with saving the old location for each sample in the sequences as:

[0.2926 0.3680 0.4000 0.4441 0.6636 0.7658 0.8259 0.8605 0.8880 0.9134]

3- The generated site vector used to permutation image's pixels according to new location as:

[ 7 3 1 5 9 8 10 4 2 6].

## 3. Proposed System Model:

The proposed image cryptography based chaotic maps mainly consists of two stages. The confusion stage is the permutation of pixel's image where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable. Another stage is diffusion processing. Diffusion refers to the process of rearranging or spreading out the bit of the message so that redundancy in the plaintext is spread out over the complete ciphertext. these stages aim to changing the value and location of each pixel in the whole image to protect image from attackers. The confusion and diffusion ciphering are done based on randomness signals which are generated by chaotic maps. The chaotic behavior is controlled by the initial conditions and control parameters. The image ciphering which is proposed here is performance by three keys driving from chaotic maps. The block diagram of proposed system used to Encrypt and decrypt Gray scale image shows in Figure (1). Also, Figure (2) shows the block diagram of proposed system which is used in encrypted and decrypted color image.

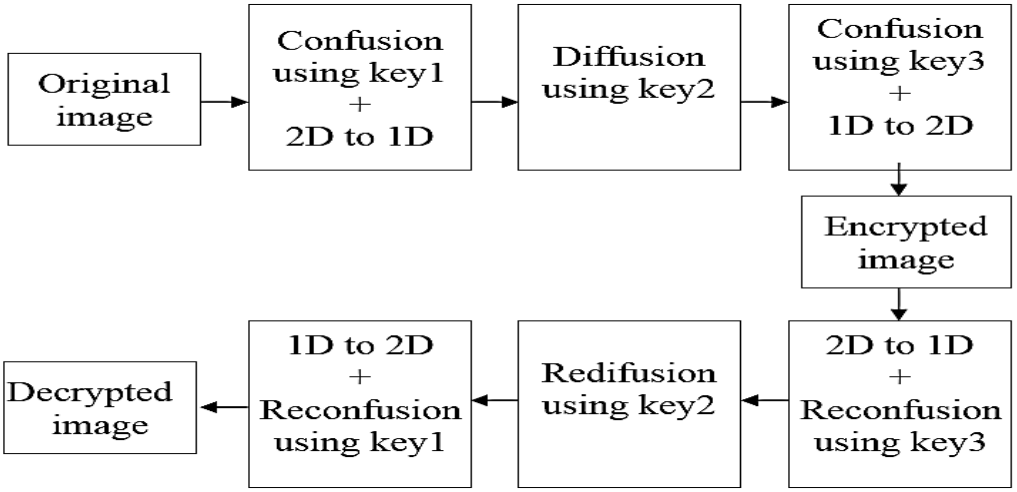


**Figure 1:** The block diagram of proposed system used to Encrypt and decrypt Gray scale image

In the following steps, the encryption of Gray scale images is illustrated:
**Input:** Target Image to be encrypted and the parameters values of all keys.
**Output:** Encrypted Image

Step1: Read the image with size (M×N).
Step 2: Shuffled image pixels depending on key 1.
Step 3: Rearrange the Image pixels as (MNx1).
Step 4: Generate Chaotic sequences (using two Logistic maps) with length (MN) then generate two keys (key2 and key3).
Step 5: Diffusion image pixels depending on key 2.
Step 6: Shuffled image pixels depending on key 3.
Step 7: Rearrange the final modified Image pixels as (MxN) to generate the encrypted image.

To decrypt the image, all steps used in encryption will be performed with inverse order.

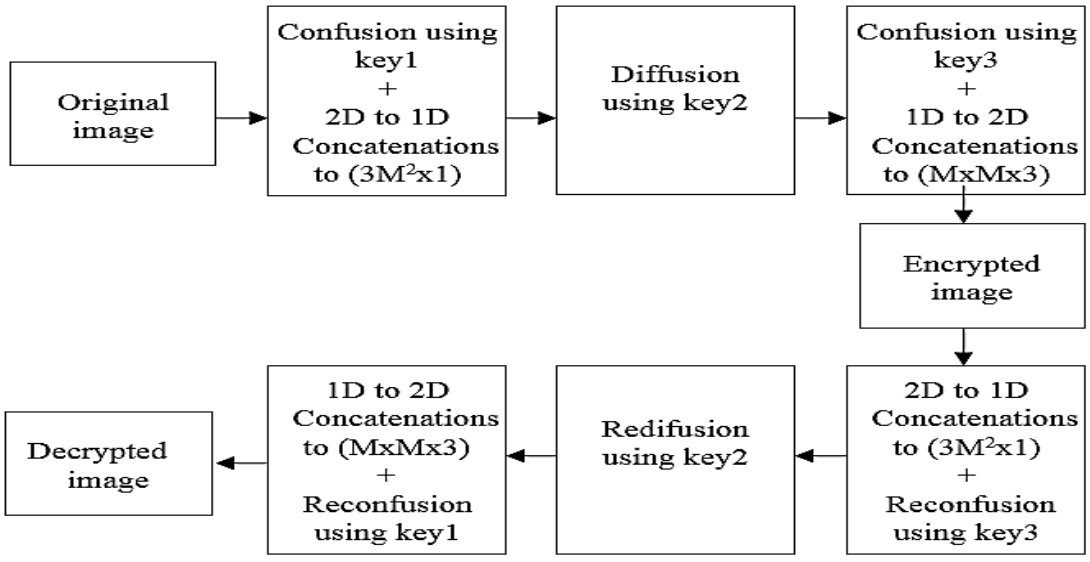


**Figure 2:** The block diagram of proposed system used to Encrypt and decrypt Color image

Also, the encryption of RGB images can be illustrated by the following steps:
**Input:** Target Image to be encrypted and the parameters values of all keys.
**Output:** Encrypted Image

Step1: Read the image with size (M×Nx3).
Step 2: Shuffled each image pixels layer depending on key 1.
Step 3: Rearrange the three layer of Image pixels as ($M^2$x1) for each layer to generate one array as [layer1, layer2, layer3] with ($3M^2$x1) dimension.
Step 4: Generate chaotic sequences (using two Logistic maps) with length ($3M^2$) then generate two keys (key2 and key3).
Step 5: Diffusion image pixels depending on key 2.
Step 6: Shuffled image pixels depending on key 3.
Step 7: Rearrange the final modified array as (MxMx3) to generate the encrypted image.

To decrypt the image, all steps used in encryption will be performed with inverse order.

## 4. Statistical Factors, Results and Simulation

The simulation uses Peppers image with 512x512 dimension as gray scale image and with 512x512x3 dimension as color image. To measure the test image some of statistical analysis will be used as:

**The Similarity Test:** The similarity is computed using normalized correlation *NC* between them according to Equation (4).

$$NC = \frac{\sum_{k=1}^{QN} M(K)M\prime(K)}{\sqrt{\sum_{k=1}^{QN} M(K)^2}\sqrt{\sum_{k=1}^{QN} M\prime(K)^2}} \quad (4)$$

where M and M**'** are original and extracted secret speech messages respectively, QN represents number of samples in each one of them [4]**.**

**Peak Signal to Noise Ratio (PSNR) Test:** According to the human visual system, some amount of distortion between the original image and the modified one is allowed [9], an expression for the ratio between the maximum possible value (power) of a signal and the power of distortion noise that affects the quality of its representation. Because many signals have a very wide dynamic range, the PSNR is usually expressed in terms of the logarithmic decibel scale. The peak signal to noise ratio can be computed as [6, 9]**:**

$$\boldsymbol{PSNR = 10log_{10}\frac{M\times N\times(L-1)^2}{\sum\sum[S(r,c)-C(r,c)]^2}} \quad (5)$$

where:

L: is the number of gray scales in the image, $\boldsymbol{S(r,c)\ and\ C(r,c)}$ are the pixels values for original and encrypted images, M and N are the dimensions of image.

**Number of Pixel Change Rate (NPCR)** is used to test the influence of one pixel change on the whole cipher-image NPCR means the change rate of the number of pixels of ciphered image while one pixel of original image is changed. The NPCR is defined as **[1,7]:**

$$\boldsymbol{NPCR = \frac{\sum_{i,j} D(i,j)}{2M\times N}\times 100\%} \quad (6)$$

where D(i, j) = 0, at pixel (i,j) of original and decrypted image is different. And D(i, j) = 1, at pixel (i,j) of original and decrypted image is same.

Also, information entropy [1,10] and correlation of adjacent pixels [10] are presented as another measurement analysis factors used to test the proposed cryptography scheme.

## 4.1: Sensitivity Testing of Chaotic Maps:

### 4.1.1: Logistic map:

Two identical Logistic maps (*a* & *b*) are taken with the same control parameter but starting from different initial condition (nearly identical however). The difference in initial condition taken between two Logistic variables $x_a$ and $x_b$ is chosen to be $10^{-15}$. Figure (3) depicts the time series of variables $x_a$ and $x_b$ for two Logistic maps. After some period, the two variables quickly diverge from each other even though they start from identical initial condition.

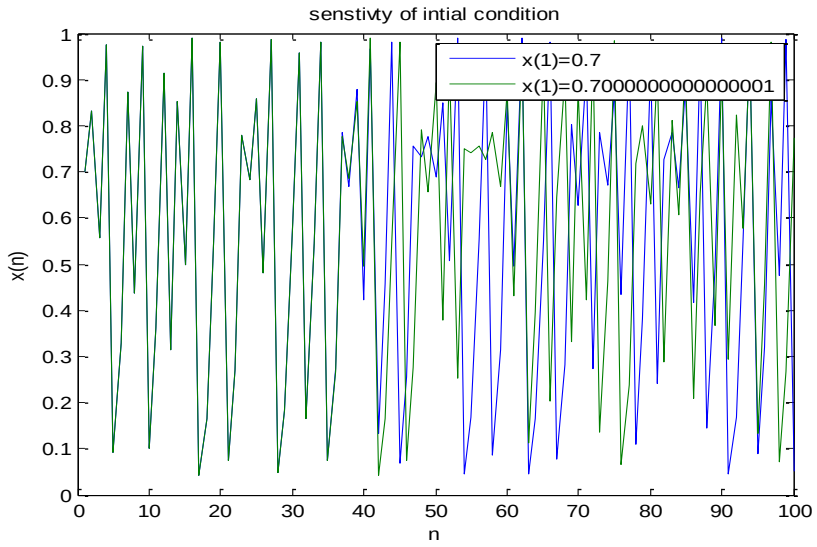


**Figure 3:** The sensitivity of Logistic map to a tiny change in initial condition

When any tiny change in control parameter (r) for a Logistic map, it yields a high different in the response of Logistic map compared with the previous state as shown in the Figure (4) .

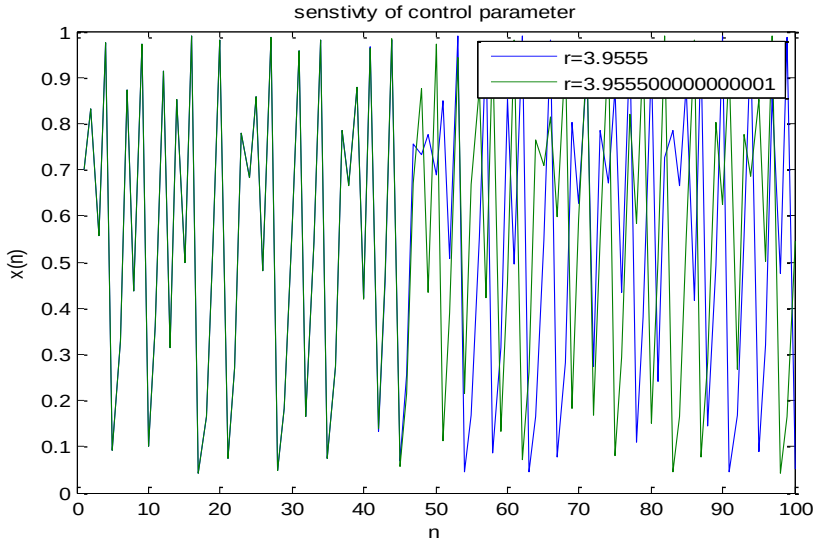


**Figure 4:** The sensitivity of Logistic map to a tiny change in control parameter

### 4.1.2: Modified Arnold cat map (MACM):

Any change in the number of cycles (*p*) or any other parameters (a, b, c) of the modified Arnold cut maps will be obtained a large different in the location of tested pixel. Example below shows the difference in pixel location with respect to the number of cycles (*p*):

Original

| | | | | |
|---|---|---|---|---|
| 1 | 255 | 200 | 100 | 44 |
| 55 | 45 | 23 | 44 | 30 |
| 105 | 205 | 66 | 7 | 45 |
| 88 | 255 | 154 | 207 | 88 |
| 55 | 33 | 22 | 11 | 10 |

*p* =3

| | | | | |
|---|---|---|---|---|
| 1 | 7 | 33 | 30 | 154 |
| 200 | 105 | 11 | 45 | 88 |
| 44 | 66 | 55 | 44 | 255 |
| 255 | 45 | 22 | 55 | 207 |
| 100 | 205 | 10 | 23 | 88 |

*p* =6

| | | | | |
|---|---|---|---|---|
| 1 | 44 | 205 | 88 | 22 |
| 33 | 44 | 23 | 105 | 207 |
| 154 | 55 | 100 | 45 | 45 |
| 7 | 255 | 10 | 200 | 55 |
| 30 | 66 | 88 | 11 | 255 |

*p* =8

| | | | | |
|---|---|---|---|---|
| 1 | 154 | 30 | 33 | 7 |
| 100 | 88 | 23 | 10 | 205 |
| 255 | 207 | 55 | 22 | 45 |
| 44 | 207 | 55 | 22 | 66 |
| 200 | 88 | 45 | 11 | 105 |

## 4.2: simulation results of gray scale image:

Figure (5) shows the original encryption and decryption gray scale image and its histogram, generated by used proposed Encryption system.

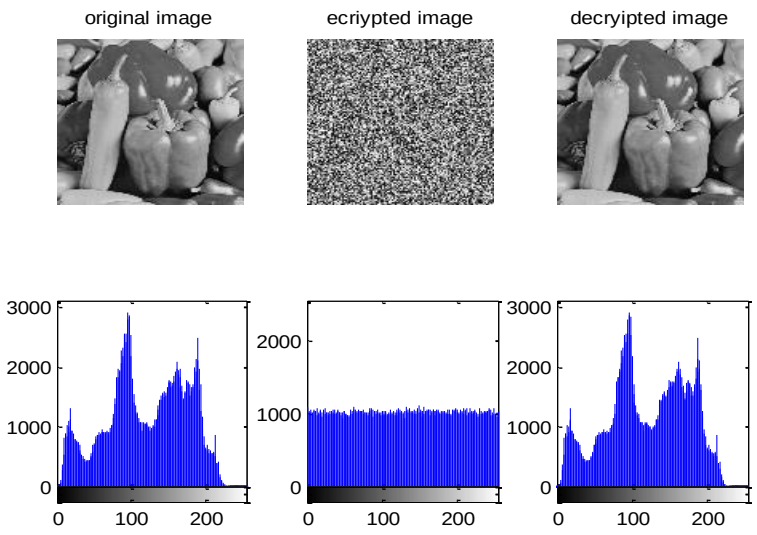


**Figure 5:** The original encryption and decryption gray scale image and its histogram.

### 4.2.1: Sensitivity for change in keys

The sensitivity of the three keys for any tiny change of any parameter causes a large different in generated of these keys. In this paragraph one parameter of Arnold or logistic map which are produced the encryption keys is changed while all parameters still the same:

**4.2.1.1: sensitivity of Key 1 (MACM):** when any parameter is changed, as example the number of cycle (*p*) changed by ±1, in the decryption process with respect to its value in the encryption process, the decrypted image will be high different compared with the original image as shown in Figure (6) .

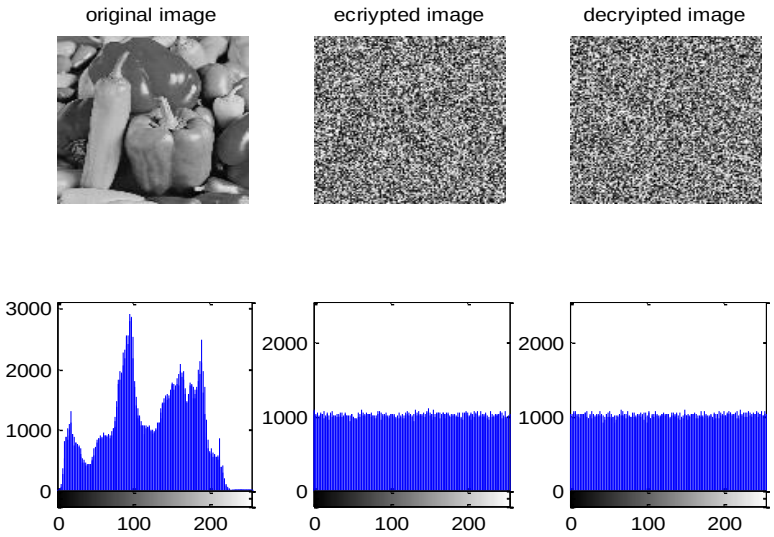


**Figure 6**: The sensitivity of change *p* parameter of key 1 on decryption process

**4.2.1.2: sensitivity of Key 2 and Key 3 (logistic map):** Figure (7) shows the original encryption and decryption gray scale image and its histogram, with sensitivity of change the initial condition of key **2** by $\pm 10^{-10}$.

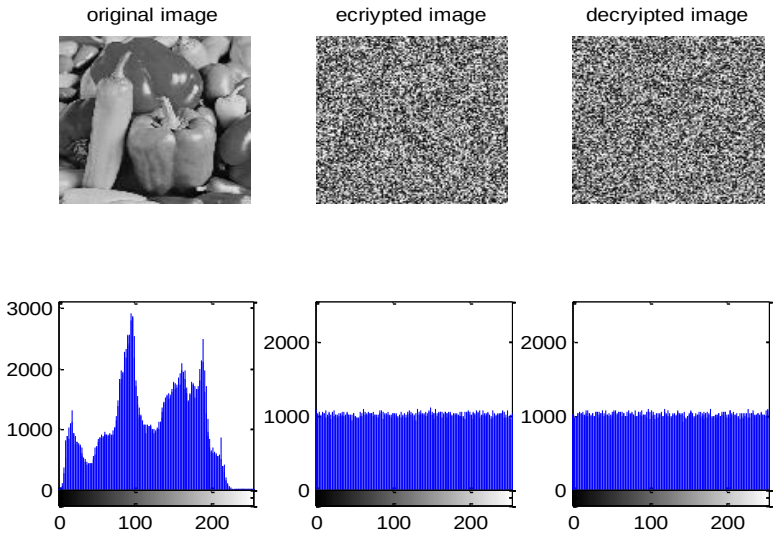


**Figure 7:** The sensitivity of change key 2 on decryption process

Also, Figure (8) shows the original encryption and decryption gray scale image and its histogram, with sensitivity of change the control parameter of key **3** by $\pm 10^{-10}$.

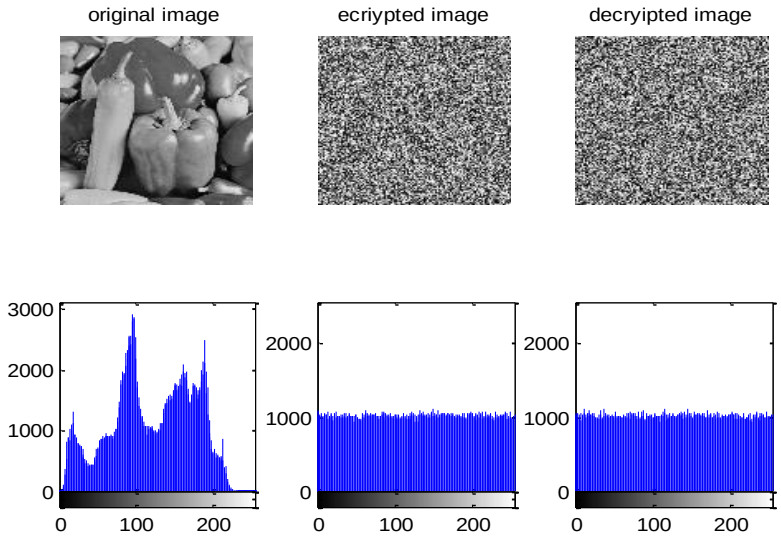


**Figure 8:** The sensitivity of change key 3 on decryption process

Table (1), shows the analyses measurements of encrypted and decrypted gray scale images with and without change of any chaotic keys in the decryption process.

**Table 1:** Analyses measurement of gray scale image

| Peppers Image | Parameter Change | NC | NPCR | PSNR |
|---|---|---|---|---|
| Encrypted | No parameter | 0.0017 | 99.62% | 8.16 |
| | No parameter | 1 | 0 | Infinity |
| | ***a*** parameter of Key 1 | 0.026 | 99.61% | 10.01 |
| | ***b*** parameter of Key 1 | 0.115 | 99.11% | 10.61 |
| | ***c*** parameter of Key 1 | 0.1118 | 99.1% | 10.91 |
| | ***p*** parameter of Key 1 | 0.00957 | 99.58% | 9.8809 |
| | Initial parameter for key2 | 0.00127 | 99.62% | 8.8913 |
| | Control parameter for key2 | -0.00179 | 99.60% | 8.8879 |
| | Initial parameter for key3 | -0.00051 | 99.61% | 8.887 |
| | Control parameter for key3 | 0.000255 | 99.59% | 8.8979 |

This table illustrates that the NC=1 for decryption image, same of original, with used same chaos parameters that are used in encryption process. Also, it shows the high sensitivity for a tiny change in any parameters of chaotic keys that is depicted with low NC, very high NPCR and small PSNR for the decrypted image.

## 4.3: simulation results of RGB image:

In this section, the Peppers color image with 512x512x3 dimensions will be analytic as a test image to the proposed encryption scheme, Figure (9) shows the original, encrypted images and its three layers histogram

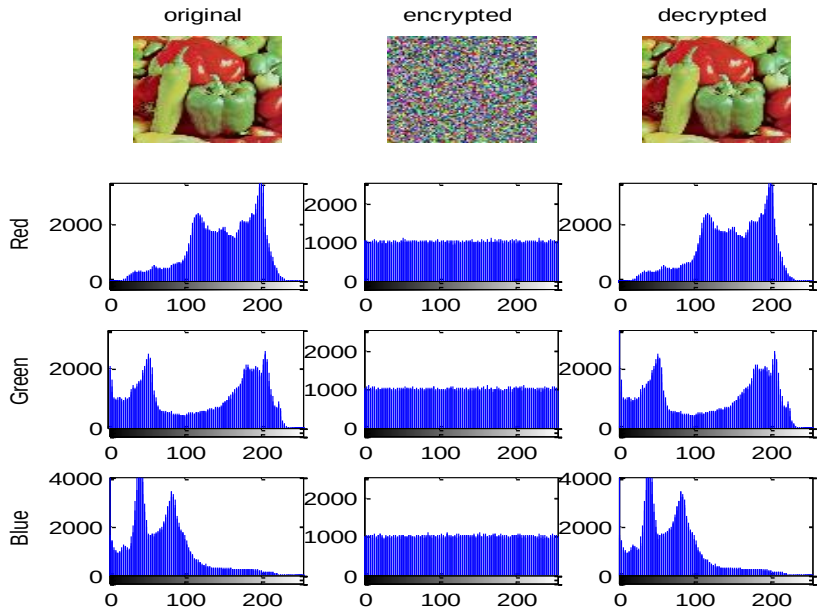


**Figure 9:** The original, encrypted, decrypted color images and its histogram

**4.3.1: sensitivity of Key 1 (MACM):** Figure (10) shows the decrypted image with its histograms when change the b parameter of MACM by **±**1 in key 1 at the decryption side.

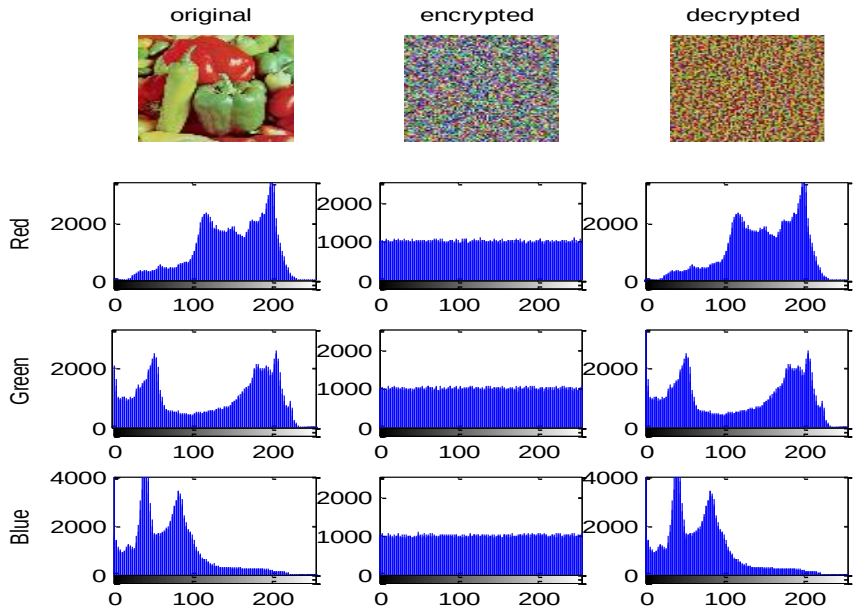


**Figure 10:** The sensitivity of change *b* parameter of key 1 on decryption process

**4.3.2: sensitivity of Key 2 and Key 3 (logistic map):** Figure (11) shows the original encryption and decryption Peppers RGB image and its histogram, with sensitivity of change the initial condition of key **2** by $\pm 10^{-10}$.

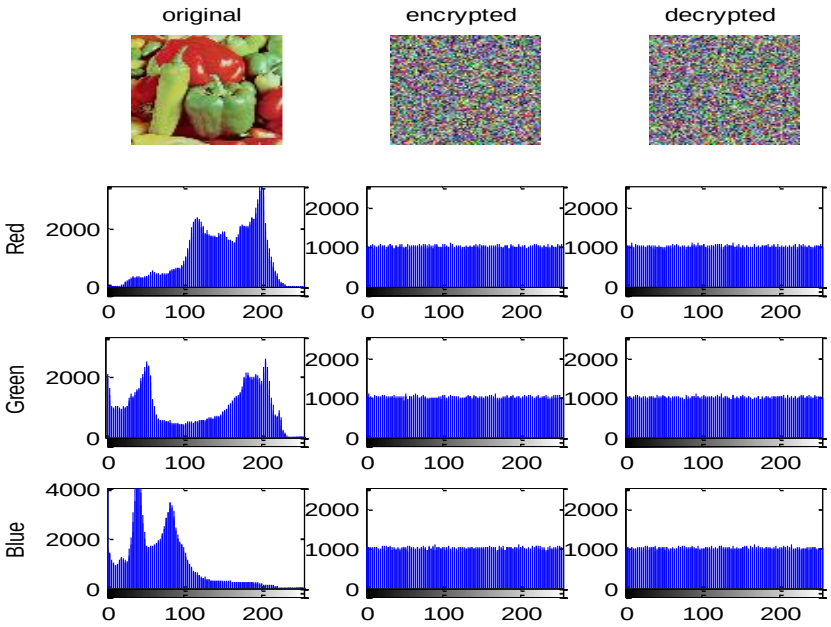


**Figure 11:** The sensitivity of change key 2 on decryption process

Also, Figure (12) shows the original encryption and decryption Peppers RGB image and its histogram, with sensitivity of change the control parameter of key **3** by $\pm 10^{-10}$.

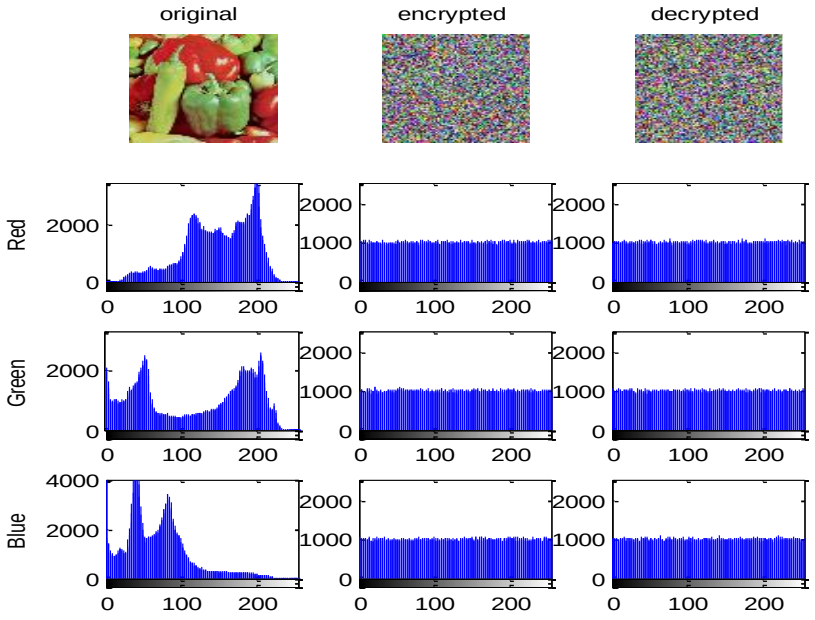


**Figure 12:** The sensitivity of change key 3 on decryption process

Table 2, shows the analyses measurements of encrypted and decrypted Peppers RGB image with and without change of any chaotic keys in the decryption process.

**Table 2:** shows the sensitivity of change keys for color image

| Image | Parameter Change | PSNR | NPCR | NC |
|---|---|---|---|---|
| Encrypted | No parameter change | 8.10 | 99.6% | 0.00069 |
| | No parameter change | Infinity | 0 | 1 |
| | ***a*** parameter of Key 1 | 10.12 | 99.31% | 0.269 |
| | ***b*** parameter of Key 1 | 10.11 | 99.32% | 0.2677 |
| | ***c*** parameter of Key 1 | 10.12 | 99.22% | 0.268 |
| | ***p*** parameter of Key 1 | 10.20 | 99.22% | 0.2816 |
| | Initial parameter for key2 | 8.110 | 99.62% | 0.00104 |
| | Control parameter for key2 | 8.110 | 99.6% | 0.00081 |
| | Initial parameter for key3 | 8.117 | 99.6% | 0.00257 |
| | Control parameter for key3 | 8.106 | 99.61% | 0.00107 |

To indicate the high quality for the proposed encryption method and for both gray scale and RGB images, correlation of adjacent pixels will be used by take 2000 pairs of random pixels organized in horizontal, vertical or diagonal directions. In each direction, correlation coefficient calculated as in [10]. Also, to distribution of pixel values can be further quantitatively determined by calculating the information entropy of the image. Information entropy is a key measure of the randomness or unpredictability of information content [1]. When the entropy very near from 8, that means the encrypted image is unpredictable.

**Table 3:** correlation of adjacent pixels of gray scale and color Peppers image

| Image type | Original Image | | | Encrypted Image | | |
|---|---|---|---|---|---|---|
| | horizontal | vertical | diagonal | horizontal | vertical | diagonal |
| Gray scale Proposed | 0.9816 | 0.9839 | 0.9669 | -0.00046 | -0.00015 | -0.00086 |
| Gray scale Ref. [5] | 0.9816 | 0.9839 | 0.9669 | 0.00078 | 0.00076 | 0.0048 |
| Red | 0.9756 | 0.9786 | 0.9564 | 0.00025 | -0.000046 | -0.00022 |
| Green | 0.9882 | 0.9901 | 0.9787 | -0.000073 | -0.00034 | -0.0008 |
| Blue | 0.9777 | 0.9769 | 0.9572 | 0.00032 | -0.000011 | -0.00016 |
| Red | 0.9756 | 0.9786 | 0.9564 | 0.0133 | 0.0146 | 0.0008 |
| Green | 0.9882 | 0.9901 | 0.9787 | 0.0016 | −0.0082 | −0.0255 |
| Blue | 0.9777 | 0.9769 | 0.9572 | −0.0112 | 0.0115 | 0.0109 |

**Table 4:** Information Entropy of Encrypted gray scale and color Peppers image

| Peppers Image | Information Entropy of Encrypted Image |
|---|---|
| Gray scale Proposed | 7.99931 |
| Gray scale Ref. [5] | 7.997 |
| RGB Proposed | 7.99983 |
| RGB Ref. [1] | 7.99978 |
| RGB Ref. [7] | 7.99423 |

Table (3) show correlation coefficients for original and cipher Peppers image. Outcomes of correlation coefficients computed in [1] and [5] references also mention here to illustrate the

advantage of proposed method. Table (4) show the entropy valued of encrypted Peppers image and the values that are computed in [1] , [5] and [7] references as comparisons results.

## 4.4: Key Space Analysis:

Key space size is the total number of different keys that are used in the encryption. For a secure image encrypted, the key space should be large enough to make the brute force attack infeasible. For proposed system, there are four variables for two Logistic maps with $10^{15}$ space for each variable, and no less than $10^2$ spaces for each four parameters of modified Arnold. Therefore, the key space for the system equal to $10^{70} \approx 2^{230}$.

## Conclusion

A high secure and efficient cryptography scheme of gray scale and color images using Logistic and Arnold chaotic maps is presented in this project. The important points that are noted during simulation and discussion of the results of Image Encryption using chaotic maps are given below:

1- Confusion and diffusion of image's pixels using MACM and Logistic map as chaos signal generators make the proposed system high robust and complex to recovered the original image without have the secret parameters.
2- Complicated chaotic encryption keys with high key space is very important to frustrate malicious attacks from unauthorized parties.
3- Low PSNR, low NC, high NPCR and high entropy for encrypted image depicts the big difference between original and encrypted images.

Therefore, from all security analysis which were carried out on the cryptography algorithm and simulation results, a high security and robustness image encryption is produced by proposed cryptography scheme.

## References


[1] Fu, Chong, et al. "A New Chaos-Based Color Image Encryption Scheme with an Efficient Substitution Keystream Generation Strategy." *Security and Communication Networks* 2018 (2018).

[2] Fridrich, Jiri. "Symmetric ciphers based on two-dimensional chaotic maps." *International Journal of Bifurcation and chaos*8.06 (1998): 1259-1284.

[3] Wang, Jiayan, and Geng Chen. "Design of a chaos-based digitlal image encryption algorithm in time domain." *Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on*. IEEE, 2015.

[4] Hameed, Abbas Salman. "Hiding of Speech based on Chaotic Steganography and Cryptography Techniques." *International Journal of Engineering Research* 4.4 (2015): 165-172.

[5] Mannai, Olfa, et al. "A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity." *Nonlinear Dynamics* 82.1-2 (2015): 107-117.

[6] Hameed, Abbas Salman. "IMAGE ENCRYPTION BASED ON FRACTIONAL ORDER LORENZ SYSTEM AND WAVELET TRANSFORM." *DIYALA JOURNAL OF ENGINEERING SCIENCES* 10.1 (2017): 81-91.

[7] Ahmad, Musheer, M. N. Doja, and MM Sufyan Beg. "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system." *Journal of King Saud University-Computer and Information Sciences* (2018).

[8] Kanso, Ali, and Nejib Smaoui. "Logistic chaotic maps for binary numbers generations." *Chaos, Solitons & Fractals* 40.5 (2009): 2557-2568.

[9] Ali, Weaam Talaat, H. Abbas S. "Data Hiding Using Steganography and Cryptography Techniques." Journal of Mechatronics, Electrical and Computer Technology 8.30 (2018): 3988-4001.

[10] Ahmad, Musheer, and Omar Farooq. "A multi-level blocks scrambling based chaotic image cipher." *International Conference on Contemporary Computing*. Springer, Berlin, Heidelberg, 2010.