Color and gray images encryption algorithm using chaotic systems of different dimensions

S. N. Lagmiri[1], N. Elalami[2], J. Elalami[3]

[1,2] SIP, LAII Mohammadia School Engineering
Mohamed V University in Rabat, Morocco

[3] LASTIMI, Higher School of Technology of Sale,
Mohamed V University in Rabat, Morocco

Summary
The data confidentiality, integrity, security and the authenticity has become an important issue for communication via insecure channel for information includes text, audio, video, image etc. When information is transferred through various networks, there is high chance of unauthorized access. The available encryption algorithms which are mainly used for text data may not be adequate for multimedia data like images. Most of the encryption techniques have some security and performance issues.
Due to the random-like property and high sensitivity for initial values and parameters, chaotic systems are usually proposed as a solution to image encryption.
This work deals with the encryption of a color and gray images using chaotic systems of different dimensions. The proposed chaotic systems show excellent chaotic behaviors. To demonstrate its application in image processing, the two systems are applied with an algorithm based on key generation based on initial conditions for encryption and decryption.
The simulations results and security analysis demonstrate that the proposed systems have excellent encryption performance, high sensitivity to the security keys.

Key words:
Chaotic / hyperchaotic systems, Histogram, Image encryption, Decryption, Correlation.

1. Introduction

Nowadays, digital image information exchanges have increased so rapidly, so security has become an essential issue for safe transmission. To make the transmission secure over the internet, encryption of image is very important [1]. Image encryption is an effective method to protect images by transforming them into an unrecognized format. A wide variety of cryptographic algorithms have been proposed to meet to secure data and its transmission and also to identify the required levels of security depending on the purpose of the communication. Traditional ciphers methods are less efficient in securing real-time multimedia data encryption systems and exhibit some drawbacks and weakness in high stream data encryption [3,4]. Contrariwise, the chaos-based image encryption algorithms have many advantages for the random properties of chaotic systems, such as sensitivity to initial conditions and state ergodicity [2].

Manuscript received January 5, 2018
Manuscript revised January 20, 2018

Current research into the development of new chaotic and hyperchaotic systems is highlighting the benefits of real-time encryption and communication applications. They show that chaotic systems are good schemes for designing cryptosystems. For these prominent features, this paper introduces the three and four dimensional chaotic systems have been explored and utilized in the design of the color image and gray image encryption algorithm.

The paper is divided into five parts. In Section II, the chaotic and hyperchaotic systems are introduced and its chaotic property has also observed. Then in Section III, the image encryption using proposed chaotic and hyperchaotic systems are presented. Simulation results and security analysis are shown in Section IV. In Section V, a conclusion will be reached.

2. The proposed chaotic systems

The chaotic and hyperchaotic systems consist of a encryption chaotic sequence generator. In the part of the chaotic sequence generator, the system is used to generate the output chaotic sequence. The function in Eqn. (1) and (2) represent the three and four dimensional chaotic system.

2.1 Three dimensional chaotic system

The novel chaotic system introduced in this paper is described as the following autonomy differential equations [6] and its attractor is shown in figure 1:

$$\begin{cases} \dot{x}_1 = -25x_1 + 17x_2 + x_2x_3 \\ \dot{x}_2 = 39x_1 - 4x_2 - x_1x_3 + x_2x_3 \\ \dot{x}_3 = 5(x_1 - x_3) + 7x_1x_2 + 1 - x_2^2 \end{cases} \quad (1)$$

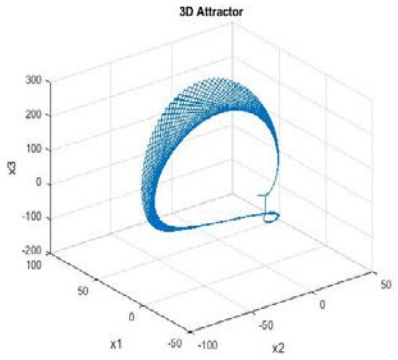
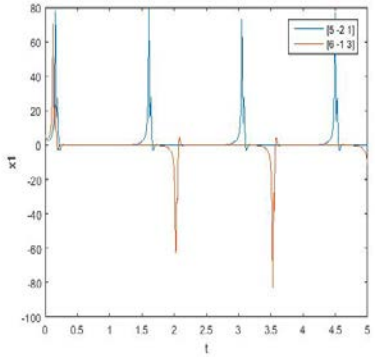


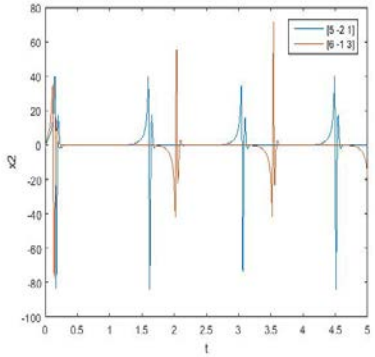
Fig.1 Novel chaotic 3D attractor

2.1.1 Sensitivity to initial conditions

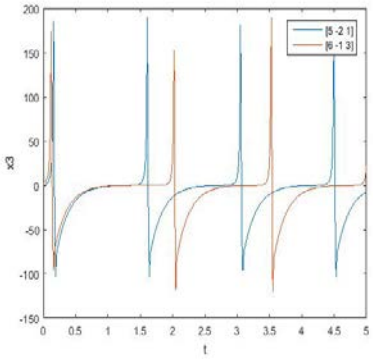
Sensitivity to initial conditions means that each point in a chaotic system is arbitrarily closely approximated by other points with significantly different future paths, or trajectories. Thus, an arbitrarily small change, or perturbation, of the current trajectory may lead to significantly different future behavior. The figure 2 compares the time series for two litely different initial conditions. The two time series stay close together, but after that, they are pretty much on their own.



(a)



(b)



(c)

Fig. 2 Sensitivity to two initial conditions [5, - 2, 1] and [6, -1, 3]: (a): x_1 (b): x_2 (c): x_3

2.2 Four dimensional hyperchaotic system

The four hyperchaotic system is described by the following equations and his attractor is represented in figure 3:

$$\begin{cases} \dot{x}_1 = 35 * (x_2 - x_1) + x_2 * x_3 * x_4 \\ \dot{x}_2 = 10 * (x_1 + x_2) - x_1 * x_3 * x_4 + 8 \\ \dot{x}_3 = -x_3 + x_1 * x_2 * x_4 \\ \dot{x}_4 = -10 * x_4 + x_1 * x_2 * x_3 \end{cases} \quad (2)$$

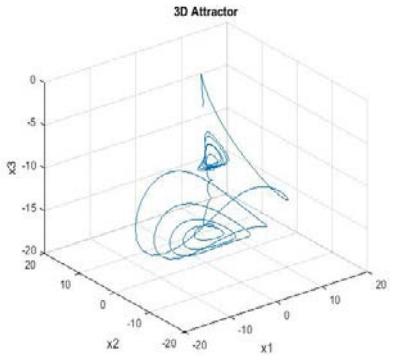
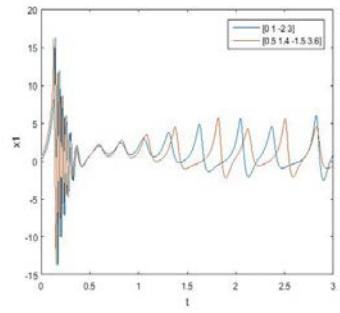


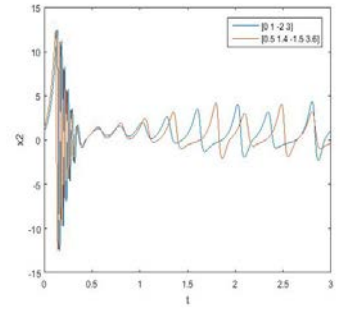
Fig. 3 Hyperchaotic 4D attractor

2.2.1 Sensitivity to initial conditions

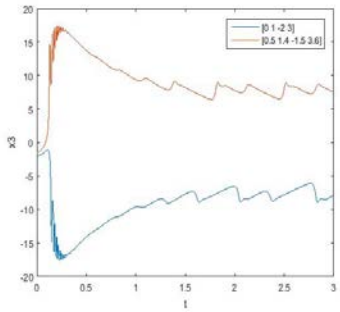
As it defined in section 2.1.1 the sensitivity to initial conditions for the four hyperchaotic system is shown in figure 4.



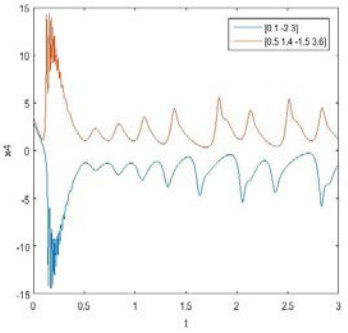
(a)



(b)



(c)



(d)

Fig. 4 Sensitivity to two initial conditions [0, 1, -2, 3] and [0.5, 1.4, -1.5, 3.6] : (a): x_1 (b): x_2 (c): x_3 (d): x_4

3. Proposed encryption scheme

This section introduces a chaos-based image encryption algorithm. It is based on the permutation pixel position only without changing the pixel value. The initial conditions for each system allow generating the output chaotic encryption sequence. Thereafter the image encryption steps are quoted. The image decryption is done by simply reversing the process using the same key.

This encryption algorithm contains five steps:

Step 1: Load the original image I [M, N];

Step 2: Initializing the chaotic/ hyperchaotic system;

*Step 3: Generating the chaotic sequences at length of M*N, then starts to generate the chaotic sequences for image encryption;*

Step 4: Calculating the new index pixel position based on key sequence;

Step 5: Permute the pixel positions on the original image then gat the encrypted one;

4. Simulation results and security analysis

4.1 Simulation results

The encryption and decryption algorithms are implemented in MATLAB. The simulation results demonstrate that the proposed algorithm shows good performances in image encryption. For the performance evaluation of the proposed method, we used “Alice.bmp” and “Moon.jpg” images of size 384x450. The initial conditions for 3D and 4D chaotic systems are respectively $x0_{3D} = [0.1; 0.2; 0.05]$ and $x0_{4D} = [0.001; 0.1; 0.02; 0.6]$. The encrypted image in Figure 5 (b) is completely different from the original image and cannot be recognized. The decrypted image in Figure 5(c), getting from the decryption process, is the same as the original image in Figure 5(a). The Figure 6 shows the same process of gray image. This shows the success of the encryption and decryption algorithm for both color and gray images.

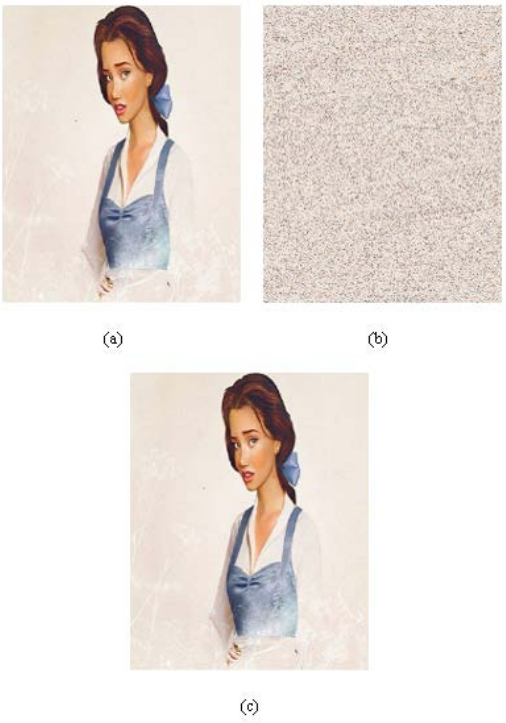


Fig. 5 (a) shows the original image, (b) shows encrypted image, (c) shows decrypted image with the same key

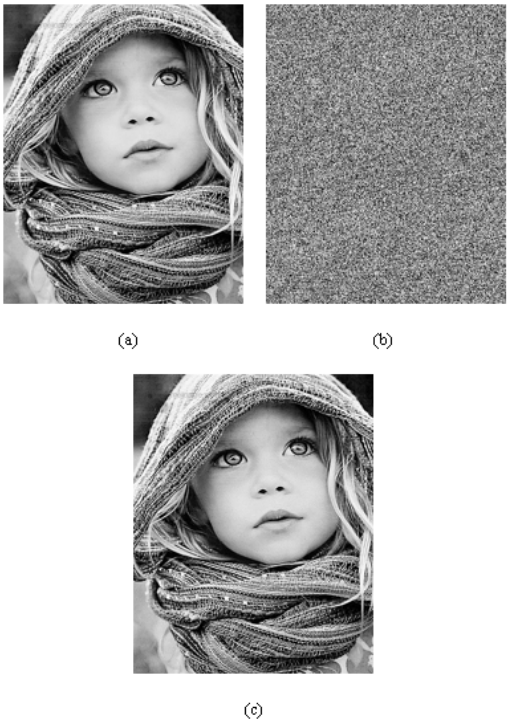


Fig. 6 (a) shows the original image, (b) shows encrypted image, (c) shows decrypted image with the same key

4.2 Statistical analysis

In order to resist attacks, the encrypted images should possess certain random properties. To prove the robustness of the proposed algorithm, a statistical analysis has been performed by calculating the histograms, the correlation coefficients, PSNR, NPCR and UACI. For the two images that have been tested, it has been determined that their quality is good.

4.2.1 Histogram Analysis

An image histogram is a commonly used method of analysis in image processing. The advantage of a histogram is that it shows the shape of the distribution for a large set of data. Thus, an image histogram illustrates how pixels in an image are distributed by plotting the number of pixels at each color intensity level. It is important to ensure that the encrypted and original images do not have any statistical similarities [7].

The experimental results of the original image and its corresponding encrypted image and their histograms are shown in figure 7 and figure 8. It is clear that the histogram of the encrypted image is significantly different from the respective histograms of the original image.

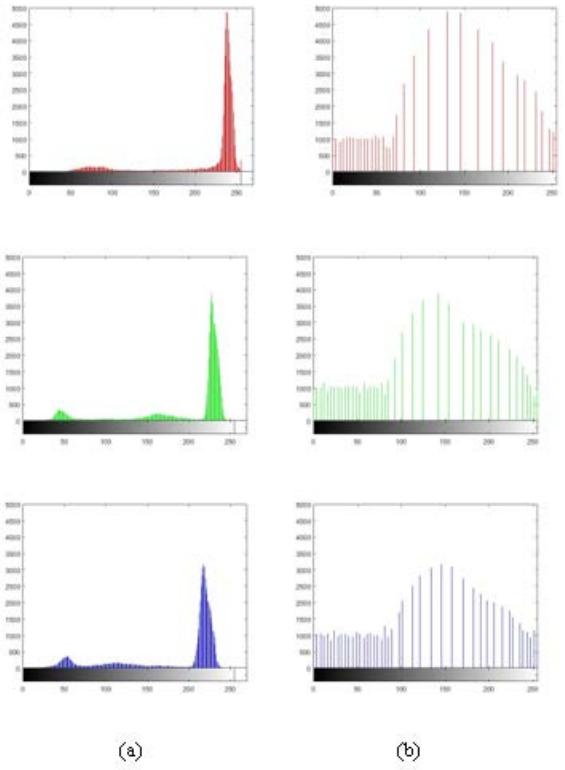
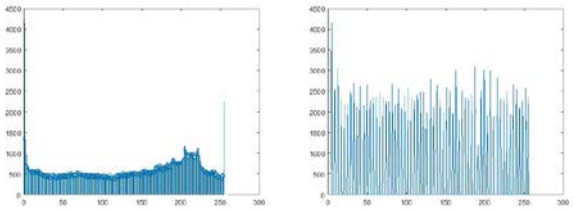


Fig. 7 (a) Original and (b) encrypted image histogram of three channels RGB



(a) (b)

Fig. 8 (a) Original and (b) encrypted image histogram of the gray image

4.2.2 Correlation of two adjacent pixels

In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain image and cipher image respectively.

A correlation is a statistical measure of security that expresses a degree of relationship between two adjacent pixels in an image or a degree of association between two adjacent pixels in an image. The aim of correlation measures is to keep the amount of redundant information available in the scrambled image as low as possible [8], [9].

Equation (3) is used to study the correlation between two adjacent pixels in the horizontal, vertical, diagonal and anti-diagonal orientations:

$$C_r = \frac{N\sum_{j=1}^{N}(X_j \times Y_j) - \sum_{j=1}^{N} X_j \times \sum_{j=1}^{N} Y_j}{\sqrt{(N\sum_{j=1}^{N} X_j^2 - (\sum_{j=1}^{N} X_j)^2) \times (N\sum_{j=1}^{N} Y_j^2 - (\sum_{j=1}^{N} Y_j)^2)}} \qquad (3)$$

where x and y are the intensity values of two adjacent pixels in the image and N is the number of adjacent pixels selected from the image to calculate the correlation. Results for the correlation coefficients of two adjacent pixels are shown in tables 1and 2.

The results of the correlation coefficients for horizontal, vertical and diagonal adjacent pixels for the original images and its encrypted images show that there is very good correlation between adjacent pixels in the image data [10], [11], while there is only a small correlation between adjacent pixels in the encrypted image.

Table 1: correlation coefficient for "Alice" color image

		Horizontal	***Vertical***	***diagonal***
Original image		0.9759	0.9855	0.9677
3D	***Encrypted***	0.0071	-0.0066	-0.0007
	Decrypted	0.9637	0.9681	0.9487
4D	***Encrypted***	0.0015	-0.0020	0.0001
	Decrypted	0.9617	0.9688	0.9494

Table 2: correlation coefficient for "Moon" gray image

		Horizontal	***Vertical***	***diagonal***
Original image		0.7195	0.6947	0.6060
3D	***Encrypted***	-0.0006	-0.0004	-0.0013
	Decrypted	0.7335	0.7101	0.6259
4D	***Encrypted***	0.00142	0.0012	0.00148
	Decrypted	0.7195	0.6947	0.6060

4.2.3 PSNR analysis

Peak Signal to Noise Ratio (PSNR) criterion is used to test the unobservable factor. This measure indicates the degree of similarity between the watermark images and a watermark images. PSNR is expressed mathematically in the following form [12]:

$$PSNR[dB] = 10\log_{10}\left(\frac{255^2}{EQM(I_o, I_R)}\right) \qquad (4)$$

where EQM is the mean square error between the two images (I_o original , I_R recovered).

$$EQM(I_o, I_R) = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}(I_o(x,y) - I_R(x,y))^2$$

Table 3: PSNR coefficient for "Alice" color image

		PSNR(:,:,1)	***PSNR(:,:,2)***	***PSNR(:,:,3)***
3D	***Photo/ Encrypted***	16.8220	16.0716	16.1744
	Photo/ Decrypted	Inf	Inf	Inf
	Photo/ Decrypted with Noise	38.6607	Inf	Inf
4D	***Photo/ Encrypted***	16.8172	16.0787	16.1879
	Photo/ Decrypted	Inf	Inf	Inf
	Photo/ Decrypted with Noise	38.5462	Inf	Inf

Table 4: PSNR coefficient for "Moon" gray image

	3D			***4D***		
	E	***D***	***DN***	***E***	***D***	***DN***
PSNR	12.056	Inf	Inf	12.063	Inf	Inf

E: Encrypted, D: Decrypted, DN: Decrypted with Noise

PSNR high means: Mean square error between the original image and reconstructed image is very low. It implies that the image been properly restored. In the other way, the restored image quality is better; in our case, the value of PSNR is as follow:

PSNR (Original/Decrypted) = Inf

PSNR (Original/DecryptedNoise) = Inf

Contrariwise, a low PSNR means: Mean square error between the original image and encrypted image is very high. It implies that the image been correctly encrypted. In our case the value of PSNR is as follow:

PSNR(Original/Encrypted) = 12.056

PSNR(Original/Encrypted) = 12.063

The result is much closed with the correlation coefficient.

- The correlation coefficients for the original and decrypted image are identical. The value of PSNR (Original/Decrypted) means that the decrypted image is identical to original image.

- The correlation coefficients for the original and encrypted image are very different. The PSNR(Original/Encrypted) means that the encrypted image is totally different of the original image.

4.2.4 NPCR and UACI analysis

NPCR stands for the number of pixels change rate while one pixel of plain image changed. UACI stands for the average intensity of differences between the plain image and ciphered image. The NPCR and UACI measure tested the different range between two images. Calculate using the following formulas [5]:

$$\boldsymbol{NPCR}_{R,G,B} = \frac{\sum_{ij} D_{R,G,B}(i,j)}{W \times H} \times 100\%$$

$$\boldsymbol{UACI}_{R,G,B} = \frac{1}{W \times H}\left[\frac{\sum_{ij}\left|C_{R,G,B}(i,j) - C'_{R,G,B}(i,j)\right|}{255}\right] \times 100\%$$

Where W, H are the width and height of the image, $C_{R,G,B}(i,j)$and$C'_{R,G,B}(i,j)$ are the two encrypted images before and after one pixel of the plain image is changed respectively. $D_{R,G,B}(i,j)$ is determined by the following rules: when $C_{R,G,B}(i,j) = C'_{R,G,B}(i,j)$, then $D_{R,G,B}(i,j) = 0$; otherwise it is 1. The results are shown in table 2. We can find that the is over 99% and the is over 33%; the results show that the algorithm was very sensitive to tiny changes in the plain image, even if there is only one bit difference between the two plain images, the decrypted images will be different completely. Thus, the algorithm is robust against differential attack.

Table 5: NPCR AND UACI RESULT

	NPCR %		***UACI %***	
	3D	***4D***	***3D***	***4D***
Alice	99.60	99.61	33.46	33.47
Moon	99.52	99.49	35.01	34.95

4.3 Error Decrypted image

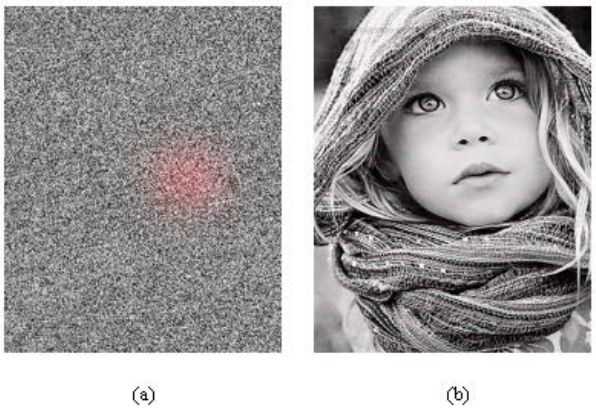
To recover images "Alice" and "Moon", we apply the inverse of the algorithm proposed in section 3. For a good decryption, we used the same key as the encryption. The result is already shown in section 4.1. But in the practical case we find situation where the encrypted image will be attacked. In this part of work we present two cases.

4.3.1 Cannel attack: white noise

In practice, the transmission of information is done through the Channel with noise. So to analysis the performance of our algorithm and our chaotic systems, we have added a white noise to the encrypted image, then we have decrypted it with the same key in the encryption. The results are shown in figures 9 and 10.

(a) (b)

Fig. 9 (a) Color Encrypted image with added white noise, (b) Decrypted image



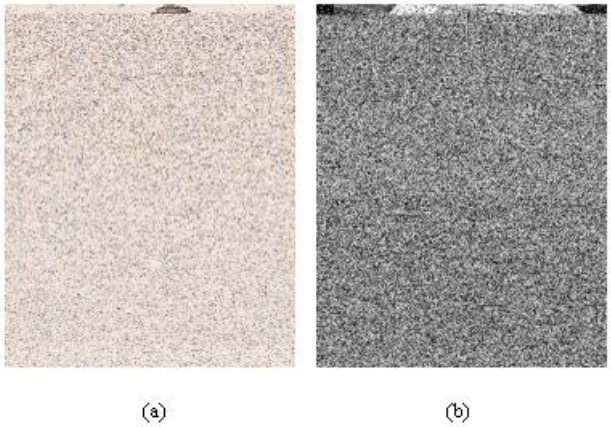
(a) (b)

Fig. 10 (a) Gray encrypted image with added white noise, (b) Decrypted image

We observe that the decrypted image is the same as the original one. That is confirmed by the *PSNR* value equal to Inf.

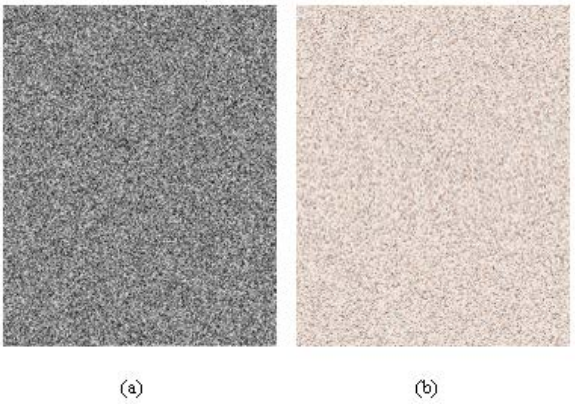
4.3.2 Unauthorized access: Error in initial conditions

Another case is when an unauthorized person tries to decrypt the image with another key. In our key, we have chosen a decryption key with an error of 10^{-6}. The results show that the decrypted images are totally different of the original images as shown in figures 11 and 12. These results confirm performance of our algorithm using chaotic and hyperchaotic systems sensitive to initial conditions.



(a) (b)

Fig. 11 Decrypted image with 3D and $x0_{3D} = [0.000001;\ 0.2;\ 0.05]$. (a) Color image (b) gray image



(a) (b)

Fig. 12 Decrypted image with 4D system $x0_{4D} = [0.001;\ 0.000001;\ 0.02;\ 0.6]$ (a) Color image (b) gray image

4.4 Processing encryption/decryption time

Processing time for encryption and decryption is also an important issue in real-time multimedia applications. To estimate the execution time of the proposed encryption scheme, different tests are performed. Tests results of encryption time and decryption time are shown in tables 6 and 7. We conclude from the results of input images that the proposed encryption system is of high-speed and flexible for various applications.

Table 6: Time Encryption and Decryption (Color image)

	Encryption	***Decryption***
3D	0.18206	0.17776
4D	0.18698	0.21102

Table7: Time Encryption and Decryption (Gray image)

	Encryption	***Decryption***
3D	0.17317	0.27097
4D	0.31521	0.34365

5. Conclusion

In this paper, an algorithm for color image and gray image encryption was designed utilizing the proposed chaotic and hyperchaotic systems. The simulation results showed that this algorithm was capable of achieving in terms of encryption and decryption process. The proposed scheme provides sensitivity to very small change in the initial conditions (10-6). We analyzed the basic dynamic characteristics of the proposed systems. The chaotic sequences of the proposed systems are generated on based of the initial conditions. Then we proposed image encryption based on permutation. The security analysis, including histogram, Correlation of two adjacent pixels, PSNR, NPCR and UACI shows that the proposed system

has good security and complexity. It is observed that image encryption using this technique given good results.

References

[1]. S. Jaryal, C. Marwaha. “Comparative Analysis of Various İmage Encryption Techniques”. International Journal of Computational Intelligence Research, Vol 13, Num 2 (2017), pp. 273-284.

[2]. S. Lian, Y. Mao, and Z. Wang, "3D Extensions of Some 2D Chaotic Maps and Their Usage in Data Encryption," in Control and Automation, 2003. ICCA '03. Proceedings. 4th International Conference on, 2003, pp. 819-823.

[3]. M. Y. Roueida , “ A Cryptographic Scheme For Color Images” , M.Sc. Thesis, Iraqi Commission For Computers & Informatics, Informatics Institute For Postgraduate Studies 2006.

[4]. C. Yun, Q. Runhe, F. Yuzhe , “Color Image Encryption Based On Hyper-Chaos“ ,Information And Technology Department, Donghua University, Shanghai, China, pp.1-6, IEEE 2009.

[5]. N. F. Elabady, H. M .Abdalkader , M. I. Moussa ,S. F. Sabbeh .” Image Encryption Based on New One-Dimensional Chaotic Map”. International Conference on Engineering and Technology (ICET), 2014, Cairo.

[6]. S. N. Lagmiri, N, Elalami, J, Elalami. "Novel Chaotic System for Color Image Encryption Using Random Permutation”. International Journal of Computer Networks and Communications Security. Vol 6, Issue 1, January 2018.

[7]. Abderrahim, N.W., F.Z. Benmansour, and O. Seddiki, “Integration of chaotic sequences uniformly distributed in a new image encryption algorithm.” 2012.

[8]. Burger, W. and M. Burge, “Digital image processing: “an algorithmic introduction using Java”. 2008: Springer-Verlag New York Inc.

[9]. D. L, “Color image encryption algorithm based on chua's circuit and chen's hyper-chaotic system,” Journal of Information & Computational Science, vol. 12, pp. 1021-1028, 2015.

[10]. H. El-din. H. Ahmed, H.M.K., O. S. Farag Allah, “Encryption quality analysis of the RC5 block cipher algorithm for digital images”. Optical Engineering, 2006. 45 (10).

[11]. L. Abraham, N. Daniel, “An improved color image encryption algorithm with Pixel permutation and bit substitution” International Journal of Research in Engineering and Technology. Vol: 02, Issue: 11, Nov-2013.

[12]. L. Abraham, N. Daniel, “An improved color image encryption algorithm with Pixel permutation and bit substitution” International Journal of Research in Engineering and Technology. Vol: 02, Issue: 11, Nov-2013.