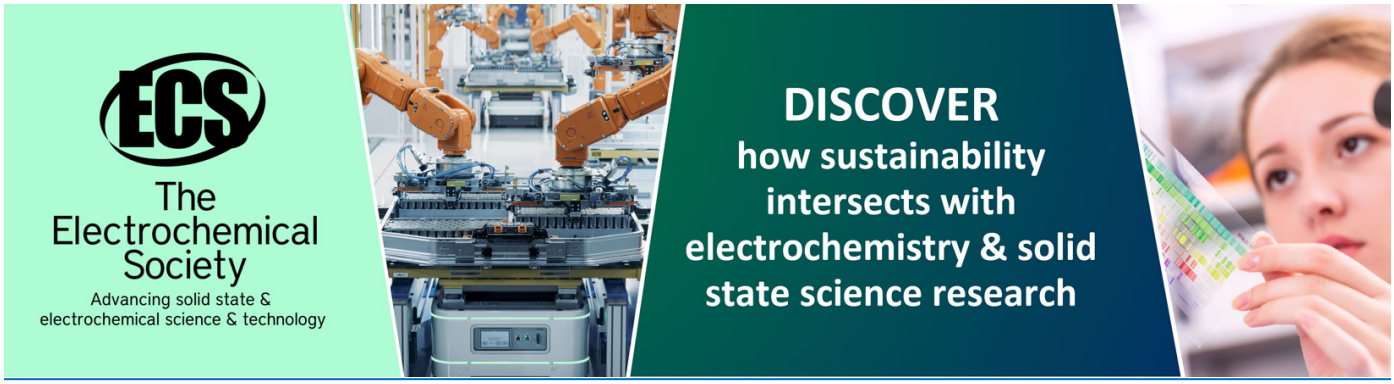
Proposed Technique for Encryption JPG and BMP Images



Proposed Technique for Encryption JPG and BMP Images

Ahlam Majead Kadhim[1], Shaimaa H. Abd muslim[2] and Huda M. Jawad[3]

[1] Physics Department / Science College / Mustansiriyah University/Iraq/ ahlammajead@uomustansiriyah.edu.iq.
[2] Physics Department / Science College/ Mustansiriyah University/Iraq / drhuda222@uomustansiriyah.edu.iq,
[3] Physics Department / Science College/ Mustansiriyah University/Iraq / Shaimaamuslim@yahoo.com

Abstract. The technique of chaotic system is considered one of the applications for high security encryption, where a color images sent is encrypted for the purpose of preserving from hacker futility. The color images which are used to study are in both formats JPG and BMP. This paper deals with the method of the numeric encryption key to encrypt each one of the two formats type images and then decrypt the result images using the same key. The measures where used to study the statistical characteristics of result images are the histogram of images, original signal divided by noise signal rate (SNR), maximum squared errors (MSE) and peak signal to the noise rate (PSNR). It is found that the chaotic key with control parameter (r) in rang (3.4567-- 4) and initial value(x) within rang (0.6716 -- 1) make high mixing. Encryption results for BMP color images are very good and efficiently, because of the decryption process given the same input image and have the same pixels values without any loosed values. The result of encryption technique for the color images in JPG format is given a little and acceptable loss because of resaving process for resaving output images using compress data in jpg format algorithm.

1. Introduction

The increasing use of the Internet among the public and the availability of public and private data and sharing of specialists and researchers in this area has led to special attention to information security. The users of social media often need to interchange, transmitted, and save their special picture information. And this private information must be protected from unauthorized access and attacks. At present, several ways of securing information have been discovered. There are three main methods used for information security: Watermarking, cryptography and steganography. The three methods are information security techniques and have a wide application. With the growth of the computer network and the Internet, information security has become a major concern and thus the technique of data concealment has attracted people all over the world [1].

So, protection of special images of people from illegal copying and distribution is being an important need. Image encryption methods try to transforming the image to another image, so that, it is hard to discovered from any one [2,3].

Image decryption retrieves the original secret image from the sending encrypted image. The encryption technique provides good confusion and diffusion characters to get high security because of mixing operation of cooler image pixels [4].

The purpose of this method is to maintain the security and confidentiality of secure locations against the process of penetration or breaking the cooler image details. There are various image processing encryption systems to safely sending secret color images, and there is many encryption algorithms to send different image types.

2. Image Encryption Techniques

Nowadays, there are different available color image encryption techniques like Arnold map, Tangram algorithm, Baker's transformation, Magic cube transformation, and affine transformation etc. Some of those algorithms, the key of security method cannot be safely and has not effective separated. This does not provide the demined requirements for the cryptographic processing method and are prone to different attacks by any person. It is desirable to develop an efficiently image secret key for new cryptosystem, especially for real-time secure cooler image transmitting over open internet networks. To satisfying this challenge, a variety type of image encryption system has been presented. One of them is the chaos-based algorithm which has suggested a new and efficient way to treatment with these problems of fast and highly secure level image encryption. The basic characters of chaotic dynamical systems such as periodicity, mixing property, sensitivity to initial conditions, system parameters that can be considered analogous to some effective cryptographic properties such as confusion, diffusion, balance, avalanche properties [5].

3. Logistic Map

Logistic map is one of the effective chaotic techniques that have been studied at last for cryptographic systems. The logistic map equation is as follows [6, 7]:

$$x_{n+1} = r\, x_n\, (1 - r) \qquad (1)$$

Where (x_n) values in rang (0, 1), the parameter (r) is a positive number taking value up to 4. Its value determines and explores the behavior of the logistic map. The system has different characteristics with different values of r which is called bifurcation parameter as shown in figure1 where the horizontal axis shows the parameter revalues of and vertical axis shows the $x_n$values [8].

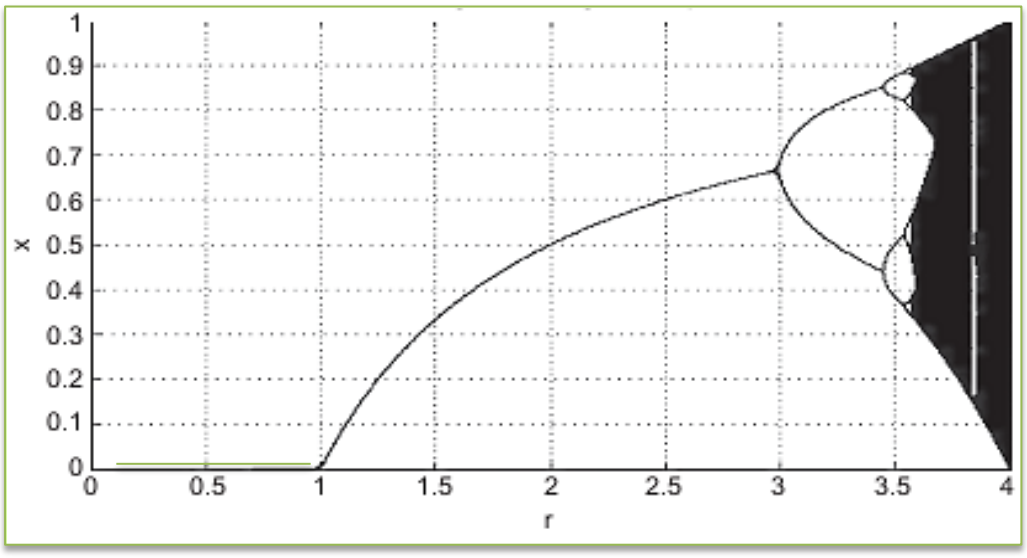


Figure 1.Bifurcation for the logistic map [8, 9]

A detailed analysis of this bifurcation diagram in figure 1 leads to the following conclusions about the logistic map [8,9,10].

1. In the state where $r \in [0, 3)$ the results come to the same number value after several iterations without any chaotic fixed point.
2. In the state where $r \in [3, 3.57)$ the system appears periodicity.
3. In the state where $r \in [3.57, 4)$ becomes a chaotic system with periodicity disappeared, larger value of parameter r is chosen to obtain a highly chaotic yet deterministic discrete time signal.

4. Key space analyses

In this work secret color image is encrypted using NEK which is having two important criteria (key space analysis and sensitivity) that are considered to analysis the encryption algorithm [10]:

a. Key space: The key space of any encryption algorithm should be very large. The initial condition and control parameter of the proposed algorithm can be take (10^7) possible values. Therefore the key space is about$((10^7)^6)$ which is large enough to resist the brute force attack.
b. Key sensitivity: The idea of key sensitivity is that any tiny change in keys used in the key encryption should be reflect clearly and largely in the cipher message. So, large key sensitivity is required for all encryption algorithms.

In this work, the color image is encrypted using NEK in order to ensure that the image arrives in safely manner. The receiver should know the same secret key which is used to decrypt the image. The initial value of NEK is 0.6716 for all images and the control parameter preform for three values (2.7567, 3.4567 and 3.9867) which are used in the proposed algorithm. The steps of algorithm that generation NEK are as follow:

Step1: Determination and select the entail value, control parameter and length of key of the chaotic key (x, r and n).

Step2: Generated sequence new numbers that represents an array with length n using equation (1).

Step3: Rearrangement array sequence number and store in an array in ascending or descending.

5. The tested images

The proposed algorithm is applying for tow format BMP and JPG of Mustansiriya University image with size300 by 199Pixels which is capturing by mobile camera iPhone 7.The camera resolution is 12 mega pixel and 1.8-inch lens and has an optical image stabilization system and a hexagonal lens. Nikon D 5200,its size is medium and the ability 24 MB and size of original image is 4000 * 6000 pixels. The images were transferred to the computer and converted to a format BMP and JPG. Figure 3displays images captured for two types BMP and JPG which were saved in a computer to preform encoding operation. Image (1) is the encrypted image for the secret key state where x, r and n of values 0.6716, 2.7567 and 179100 respectively. Image (2) is the encrypted image for the secret key state where x and n have the same values of image (1), the value of r is 3.4567. Image (3) is the encrypted image for the secret key state where x and n have the same values of image (1), the value of r is 3.9867. Decryption image for the state above is image (11), image (22) and image (33) for both images BMP and JPG. It is clear that, image (33) for the third stat is the best one.

6. Proposed Technique

In this study, an algorithm of encryption and decryption mage method will be implemented in such a way that it allows encrypting and decrypting each one of BMP or JPG images. The algorithm implemented with combination of NEK generation scheme that uses to mixing pixels of images to

improving the security. Figure 2 shows the steps of the proposed algorithm. The steps for implementing the algorithm are as follows:

Step 1: Select and read the image to be encrypted

Step 2: Convert the image into three component images.

Step 3: Convert each of the RGB images to arrays in one dimension.

Step 4: Now, generated the chaotic key using NEK algorithm and input the values (x, r and n).

Step 5: Then we had done scrambling operation for more security concern selecting one of the number to entail value and control parameter.

Step 9: Finally, we had a fully encrypted color image with the NEK algorithm.

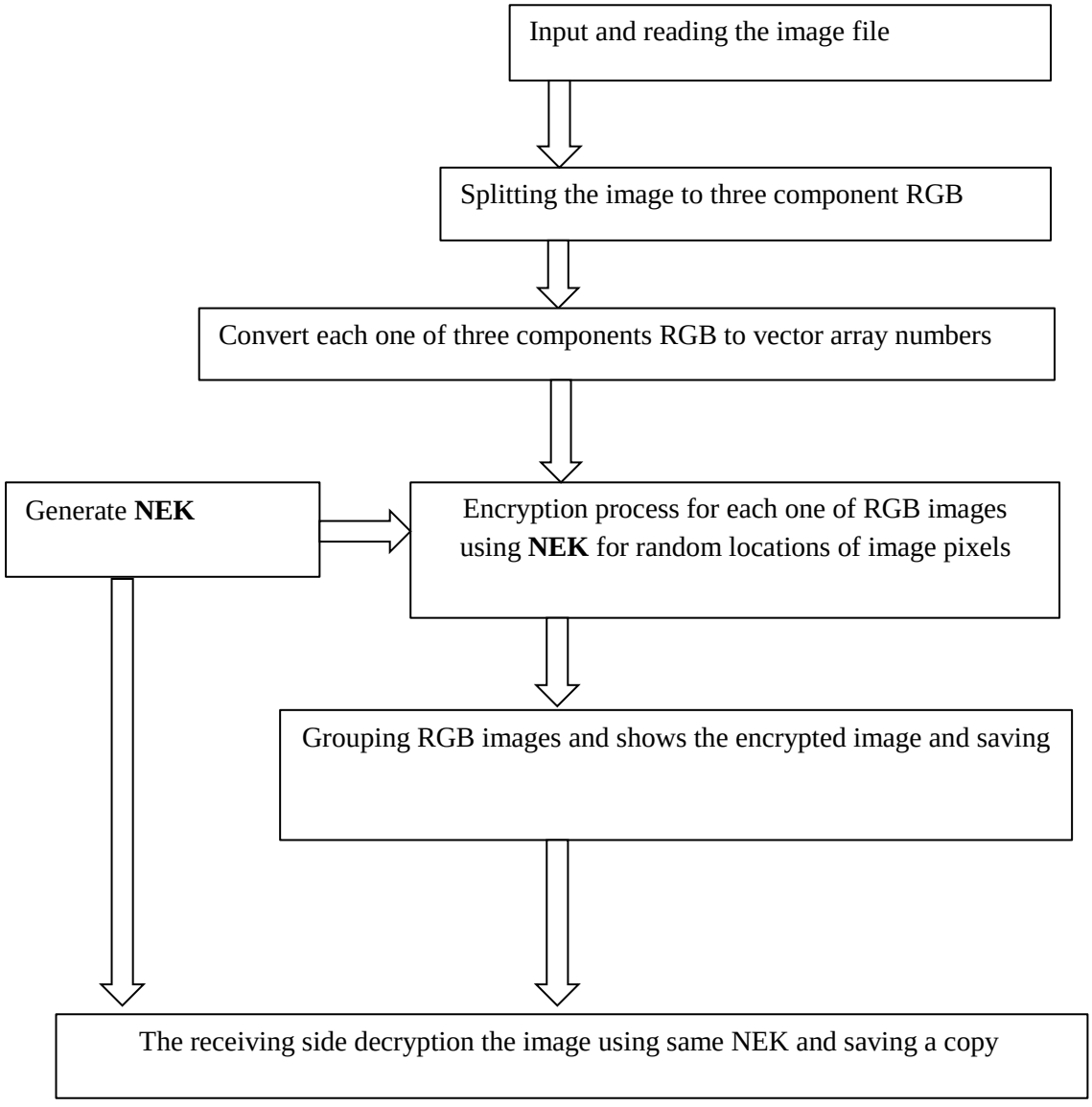


Figure2. Block diagram of proposed NEK encryption algorithm

This section discusses the performance and analysis proposed algorithms for both JPG and BMP colour images. Figures3 and 4shows the histogram of original JPG image and encrypted images using the three states of key parameters .It is concluded that, the component histogram of decrypted images similar to that one for the original and encrypted images. The result of encryption technique does not change the original values of the elements and the encryption process changed only the locations of those elements. To reconstruct the original image, the receiver should be provided the security NEK which help him to obtain the correct colour images. It then unscrambles the encrypted image using the selected the correct entail value and control parameter for the NEK algorithm. The next step is decomposes the unscrambled image to the format JPG or BMP. Arrangement of all pixels positions is restored to the original order. The reconstructed 2D image component can be obtained by combining the three component images. The encryption process does not change their efficiency with resizing the image. And the results are equal when using different both JPG and BMP for the same image.

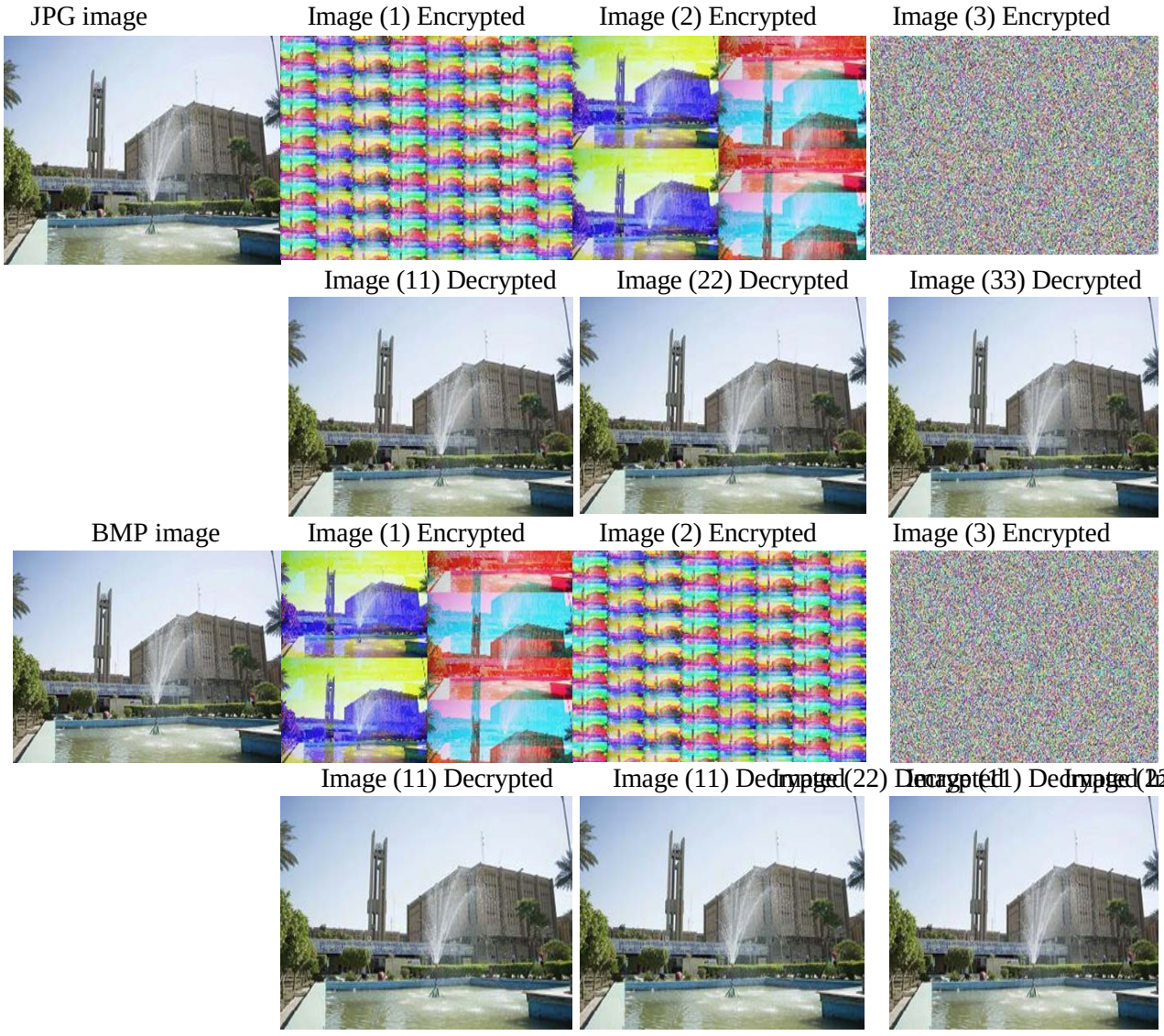


Figure3. Encrypted and decrypted Images for format JPG and BMP using NEK method.

Table 1. The result measures of JPG image.

	NEK(x,r,n)= NEK(0.6716,2.7567, 179100)					
	Encrypted Image			Decrypted Image		
COLOR	RED	GREEN	BLUE	RED	GREEN	BLUE
SNR	29.3271	28.5690	28.6532	42.2034	42.8633	40.1910
MSE	33.6453	38.5565	38.5574	1.7026	1.4741	2.7278
PSNR	32.8616	32.2698	32.2697	45.8196	46.4455	43.7726
	NEK(x,r,n)= NEK(0.6716, 3.4567, 179100)					
	Encrypted Image			Decrypted Image		
COLOR	RED	GREEN	BLUE	RED	GREEN	BLUE
SNR	28.9087	28.4921	28.2500	42.2034	42.8633	40.1910
MSE	36.5172	39.9125	41.2472	1.7026	1.4741	2.7278
PSNR	32.5058	32.1197	31.9769	45.8196	46.4455	43.7726
	NEK(x,r,n)= NEK(0.6716, 3.9867, 179100)					
	Encrypted Image			Decrypted Image		
COLOR	RED	GREEN	BLUE	RE	GREEN	BLUE
SNR	28.5810	28.1635	28.0147	42.2034	42.8633	40.1910
MSE	37.8499	41.4061	42.8283	1.7026	1.4741	2.7278
PSNR	32.3502	31.9602	31.8135	45.8196	46.4455	43.7726

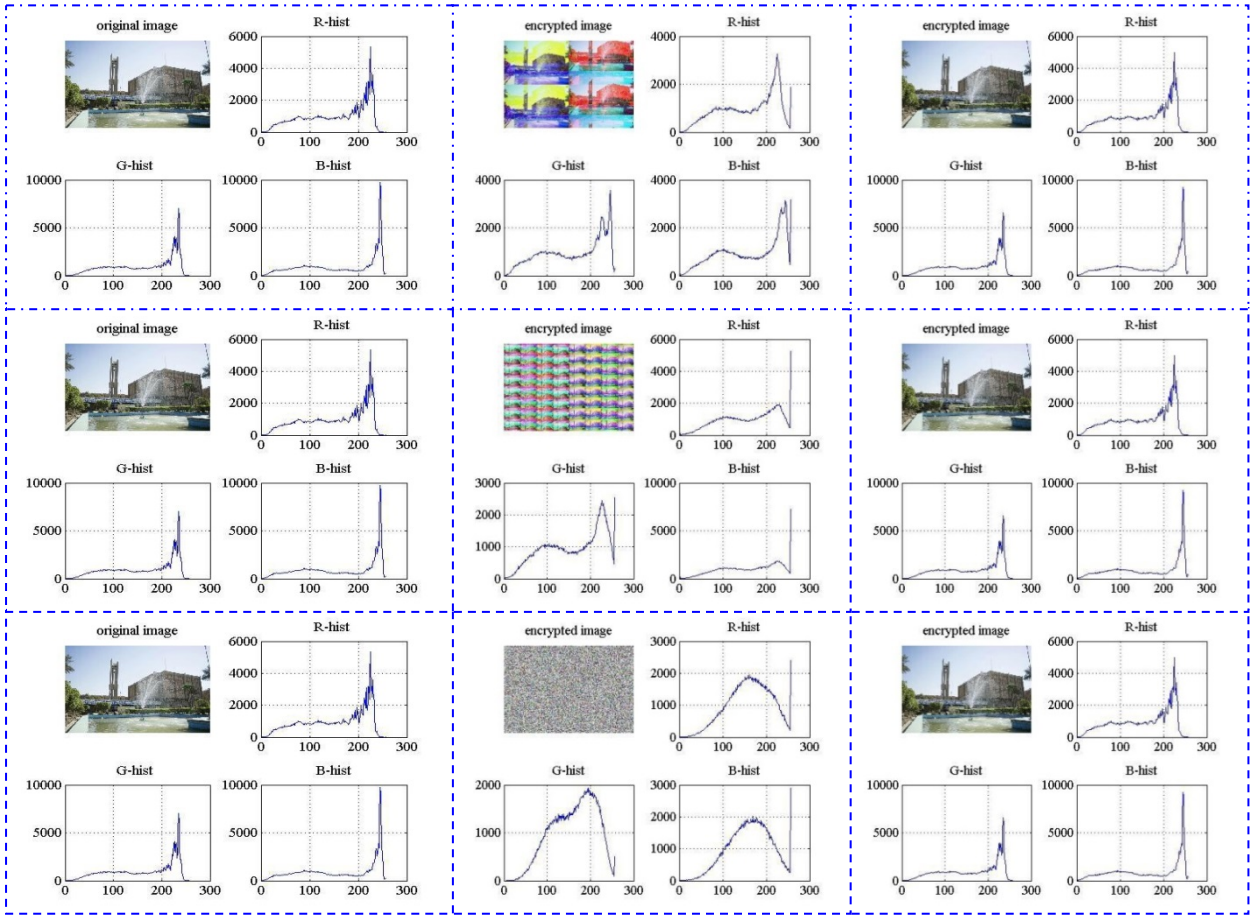


Figure4. Encrypted and decrypted Histogram of Images in format JPG (300*199) Pixels.

Table 2. The results measures for BMP image.

	NEK(x,r,n)= NEK(0.6716,2.7567, 179100)					
	Encrypted Image			Decrypted Image		
COLOR	RED	GREEN	BLUE	RED	GREEN	BLUE
SNR	32.5533	31.6494	31.8481	Inf	Inf	Inf
MSE	32.3803	38.0903	36.0858	0	0	0
PSNR	33.0280	32.3227	32.5574	Inf	Inf	Inf
	NEK(x,r,n)= NEK(0.6716, 3.4567, 179100)					
	Encrypted Image			Decrypted Image		
COLOR	RED	GREEN	BLUE	RED	GREEN	BLUE
SNR	32.1859	31.6258	31.5118	Inf	Inf	Inf
MSE	34.4690	38.7715	39.1516	0	0	0
PSNR	32.7565	32.2457	32.2033	Inf	Inf	Inf
	NEK(x,r,n)= NEK(0.6716, 3.9867, 179100)					
	Encrypted Image			Decrypted Image		
COLOR	RED	GREEN	BLUE	RED	GREEN	BLUE
SNR	31.8577	31.3937	31.1605	Inf	Inf	Inf
MSE	34.5019	38.3305	40.4729	0	0	0
PSNR	32.7524	32.2954	32.0592	Inf	Inf	Inf

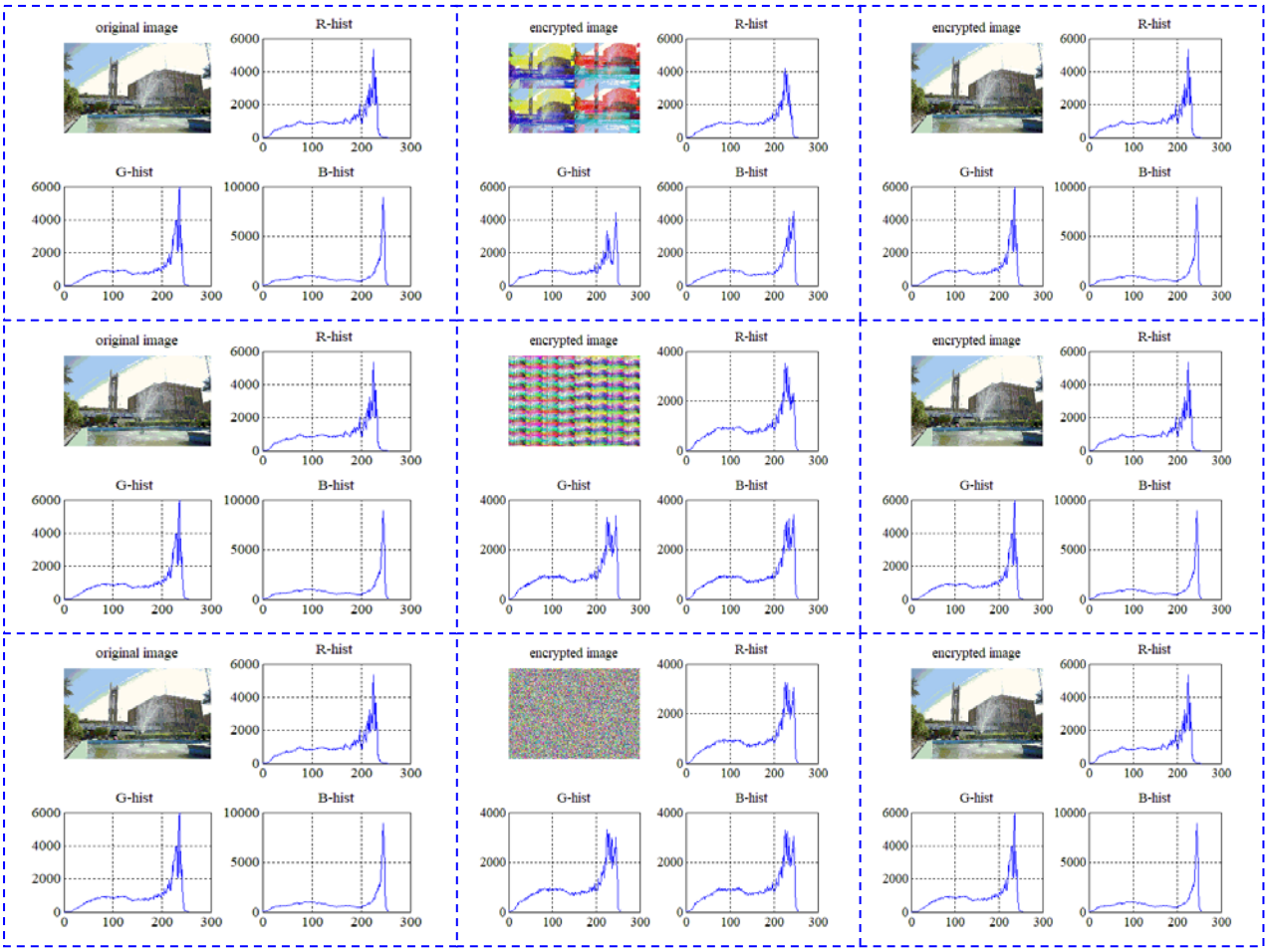


Figure5. Encrypted and decrypted Histogram of Images in format BMP (300*199) Pixels.

7. Conclusion

It was noted that the chaotic key generation is in the best results at a control parameter between (3.57- 4) where the high levels of protection are obtained. The encryption process was effective for each one of images, but, encryption process for JPG causing loss of some information at applying the decryption process. The best results getting using BMP images there was no loss of information or expansion of pixels. The results derived through the use of encryption and decryption algorithm, the testing values for each image display to comparing between original image and the encrypted image and also between the original image and the decrypted image. Analysis measures and statistical analysis (SNR, MSE and PSNR) of comparing color images before and after applying encryption algorithm, demonstrate that the proposed method has good security features.

Reference

[1] Pala Mahesh Kumar2017A New Encryption and Decryption for 3D MRT Images Asian Journal of Electrical Sciences ISSN: 2249 - 6297 **Vol. 6** No. 1 pp.1-6

[2] Cheng-Hung Chuang Zhi-Ye YenGuo-Shiang Lin2011A Virtual Optical Encryption Software System for Image Security JCIT **Vol. 6**No. 2pp.357-364

[3] Brahim Nini Chafia Melloul 2011 Pixel Permutation of a Color Image Based on a Projection from a Rotated View JDCTA **Vol. 5** No. 4pp.302-312

[4] Li. Shujun X. Zheng2002Cryptanalysis of a chaotic image encryption method Inst. of Image Process. Xi'an Jiaotong Univ., Shaanxi, This paper appears in: Circuits and SystemsISCAS 2002. IEEE International Symposium **Vol. 2** pp.708-711

[5] L. Singh and R. K. Bharti 2013 Comparative perfomance analysis of cryptographic algorithmsInternational journal of advanced research in computer science and software engineering (IJARCSSE)**Vol. 3** No. 11

[6] Tenny R. Tsimring L. S. Abarbanel H. D. I. 2006 Security of chaosbased communication and encryption. In Digital Communications Using Chaos and Nonlinear Dynamics Institute for Nonlinear Science Springer pp. 191–229

[7] Sayed Ahmad Salehi Rasoul Amirfattahi 2011 VLSI Architectures of Lifting-Based Discrete Wavelet Transform Isfahan University of Technology Iran.

[8] Jamal Nasir Hasoon January 2014 Speech Hiding Using Vector Quantization M.SC. Thesis AL-Mustansiriyh University.

[9] Eman Hato Hashim September 2013 Speech Signal Encryption Using Chaotic Maps M.Sc Thesis Al Mustansiriyah University Computer Science department.

[10] Ahlam Majead Saad Najim Al-Saad2016 Speech Steganography System Using Lifting Wavelet Transform International Information Institute Information 19.10B **4633**Tokyo