Color Image Encryption in the Spatial Domain Using 3-D Chaotic System

Hanan Salem Alzreghi[1], Osama A S Alkishriwo[2]

hanansalem52@yahoo.com, alkishriewo@yahoo.com

[1, 2] Department of Electrical and Electronic Eng., Faculty of Eng., University of Tripoli, Libya

*Corresponding author email: alkishriewo@yahoo.com

Received: 00 April 2018 / Accepted: 00 May 2018

ABSTRACT

Users of Internet daily send and receive many images through social media. These images are vulnerable to hack by attackers. Therefore, it is necessary to develop methods to protect these images against attackers. A nontraditional encryption method for encrypting color images in the spatial domain is proposed. The main idea in this work is based on building strong encryption algorithm through implementing the permutation and diffusion operations on the pixels, where every pixel composed of three values red, green and blue. These operations are implemented depending on extracting three chaotic sequences from the 3-D chaotic system, where each chaotic sequence is used to shuffle and diffuse each color in the plaintext image. The proposed system is tested on well-known images like Lena and Mandrill. Experiments and security analysis prove that the algorithm has an excellent performance in image encryption.

Keywords: Color image encryption, spatial domain, 3-D chaotic system, permutation, diffusion..

1 Introduction

Nowadays information security is a vital problem in information communication. With the advancements of information technology, lots of digital contents are being stored and transmitted in various forms. As a result, the protection of digital contents data against irregular phenomena, such as illegal copying, and guarantee of their secure utility has become an important issue. In particular, compared to text data, some intrinsic features of image data, such as big size, high redundancy of data and strong correlation among neighbouring pixels are different with ordinary information. Therefore, an encryption method with fast speed and high security is needed. But the traditional block encryption being widely used now is found to be inefficient for real-time communication. Hence a lot of image encryption methods using chaotic maps with high sensitivity to their initial conditions and system parameter values and simple structures are proposed [1, 2].

2 Proposed Algorithm

The aim of this work is to design and implement a novel and highly secure method which is essential for confidentiality and to solve the problems of some previous chaotic image encryption schemes. Figure 1 depicts the main algorithm executed in this paper and includes three operations which are permutation, diffusion, and linear transformation.

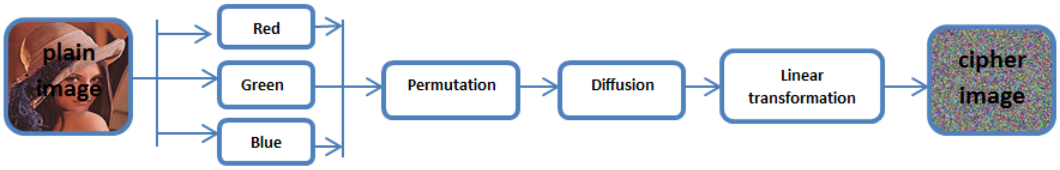


Figure 1: *Block diagram of proposed image encryption scheme.*

The original color images is divided into three images with Red ,Green and Blue channels, respectively. The encryption steps can be summarized as follows:

(1) permutation process by scrambling operation on all pixels in the image with chaotic sequence. (2) diffusion process by a sequential XOR operation on all the bits of pixels in the image. (3) linear transformation process by rotated the image to the left by amount of ℓ_p, where ℓ_p using as a security key, then we decrypte the image using inverse these process. These operations are implemented depending on extracting three chaotic sequences from the 3-D chaotic system, where each chaotic sequence is used to shuffle and diffuse each color in the plaintext image.

3 Chaotic System

The 3-D chaotic system used in this paper can be expressed as follows:

3. 1 Logistic-Logistic map

$$x_{n+1} = u\times x_n\times(1-x_n)\times 2^{14} - floor(u\times x_n\times(1-x_n)\times 2^{14}) \qquad (1)$$

3. 2 Sine-Sine map

$$x_{n+1} = u\times \sin(\pi\times x_n)\times 2^{14} - floor(u\times \sin(\pi\times x_n)\times 2^{14}) \qquad (2)$$

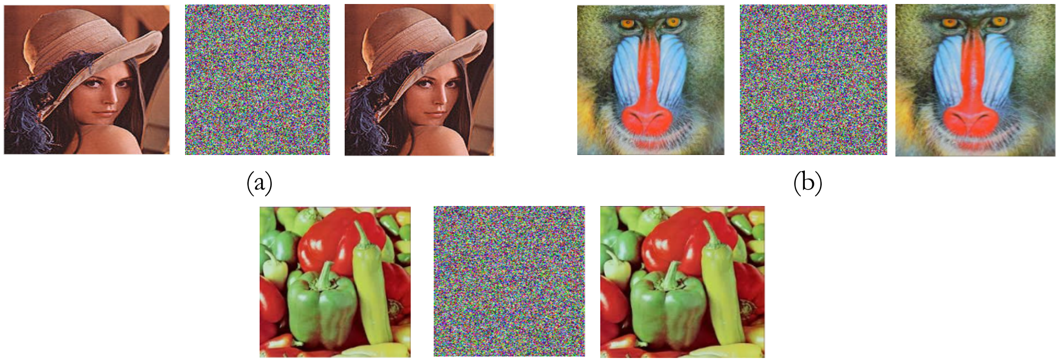
3. 3 Chebyshev-Chebyshev map

$$x_{n+1} = \cos\big((u+1)\cos^{-1}(x_n)\big)\times 2^{14} - floor\big(\cos\big((u+1)\cos^{-1}(x_n)\big)\times 2^{14}\big) \qquad (3)$$

where the control parameter $u \in (0, 10)$ and x_n is the initial value of the sequence.

4 Experimental Results and Performance Analysis

A good quality encryption scheme should be robust against all types of attack, involves security attack and statistical attack. The proposed procedure is implemented in some color images to demonstrate its efficiency. The results of encryption and decryption are shown in Figure 2. This shows that all encrypted images are noise-like ones and can be efficiently applied to images of various forms such as grayscale images, color images and binary images [3].



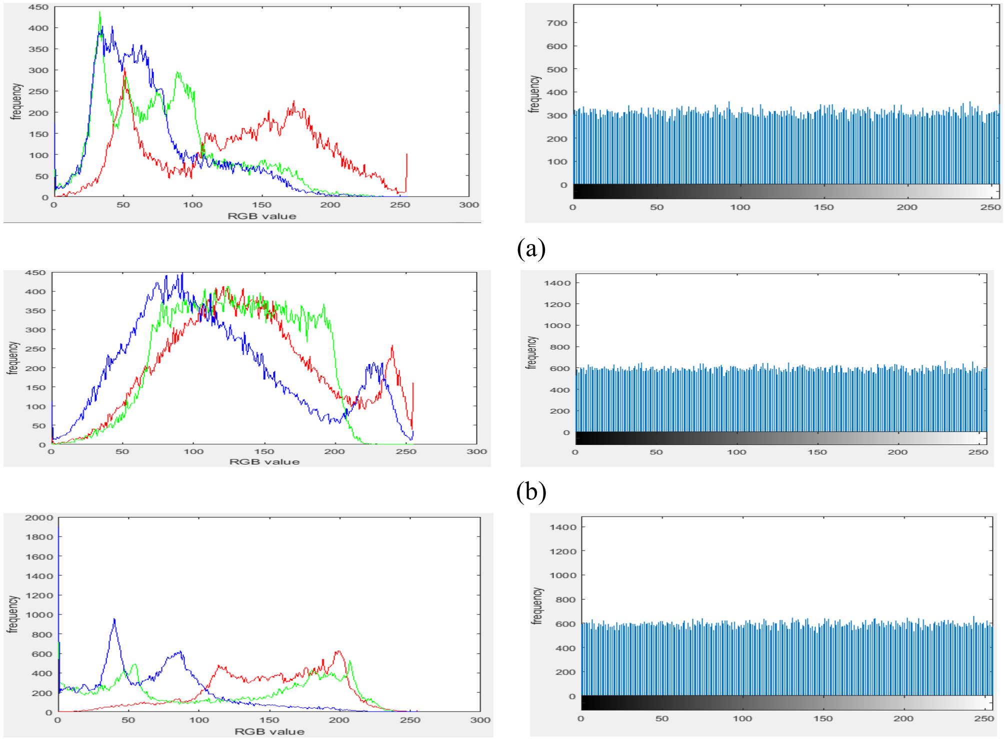
(a) (b)

(c)

Figure 2: *Encryption result of some images.*

4.1 Histogram Analysis

Image histogram reflects the distribution of pixel values of an image. To resist statistic attacks, the image histogram should be flat. Figure 3 shows the histograms of the some images and the histograms of their encrypted images. The histogram of the encrypted image has a good uniform distribution, so that it is enough to resist statistical attacks [4].



(a)

(b)

(c)

Figure 3: *(a) the histogram of the original and encrypted Lena images; (b) the histogram of the original and encrypted Mandril images; (c) the histogram of the original and encrypted Pepper images.*

4.2 Correlation of Two Adjacent Pixels

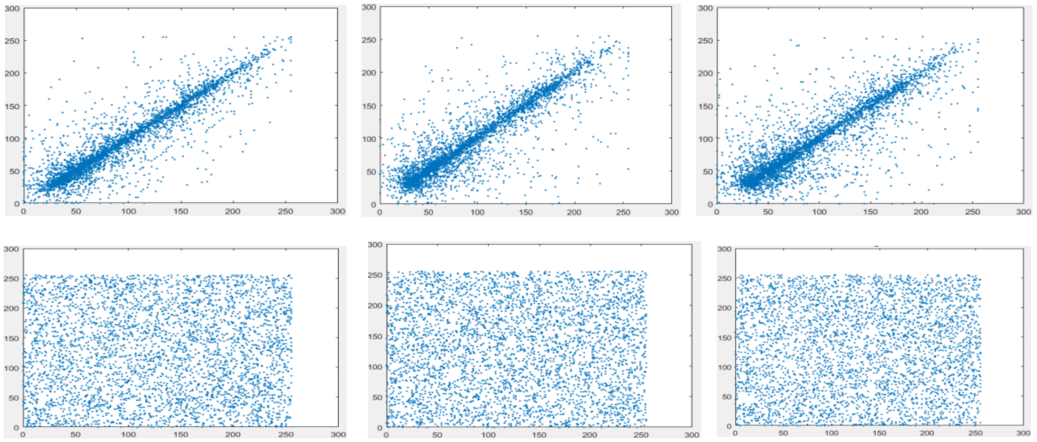
Image data generally has some intrinsic features. We analysed the correlations between two adjoining pixels of the plain-image and the cipher image at horizontal, vertical and diagonal directions for original and encrypted images [5]. The correlation coefficient is calculated by the following equations:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)\times D(y)}}$$

$$\text{where } cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad \text{and} \quad E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

where x and y are color values of two adjacent pixels in the images. Figure 4 shows the correlation analysis of Lena image.



(a) (b) (c)

Figure 4*:* *Correlation analysis of Lena image. (a) horizontal correlation of original and encrypted images; (b) vertical correlation of original and encrypted images; (c) diagonal correlation of original and encrypted images.*

Table 1: *Correlation coefficients of original Lena, Koala, Mandrill and Pepper images.*

Image	Original image			Encrypted image		
	Vertical	Horizontal	Diagonal	Vertical	Horizontal	Diagonal
Lena	0.9062	0.8722	0.8387	0.0036	0.0012	0.00032
Mandrill	0.8592	0.8876	0.8360	0.00075	-0.0016	0.0017
Pepper	0.9767	0.9696	0.9551	0.0004	0.0016	0.0025

As seen in Table 1, the correlation coefficient of the original images comes near to 1, but the correlation coefficient of the encrypted images comes near to 0. This means that the encrypted image has no correlation property with original image.

4.3 Data Loss and Noise Attack

Digital images can be easily influenced by noise and data loss during transmission through the network and storage in physical media. An image encryption algorithm should have an ability of resisting these abnormal phenomena. To test the ability of resisting the attack, we did some experiments on a data loss and a noise attack as shown in Figures 5 and 6. An original image is first encrypted by our proposed algorithm. The encrypted image is attacked by a data cut of size 15%, 30% and 40% and with 3%, 10% and 20% "salt & pepper" noise, respectively. The decryption process is then applied to these encrypted images.

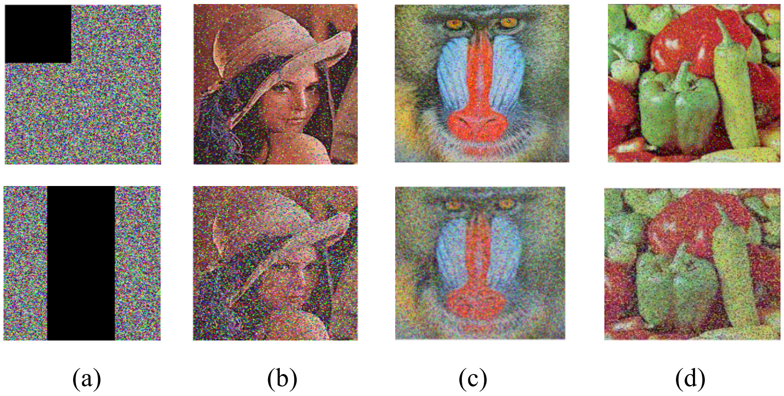


Figure 5: Data loss. (a) The encrypted images with data loss; (b) the decrypted Lena image with different data loss; (c) the decrypted Mandrill image with different data loss; (d) the decrypted Pepper image with different data loss.

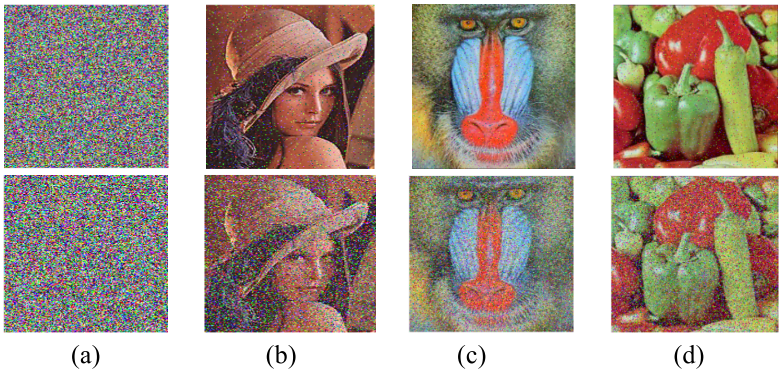


Figure 6: Noise attack. (a) the encrypted images added with 'salt & pepper' noise; (b) the decrypted Lena image of (a); (c) the decrypted Mandrill image of (a); (d) the decrypted Pepper image of (a).

The restoring ability of an image is evaluated by peak signal to noise ratio (PSNR) as expressed in the followimg equation.

$$PSNR = 10\times \log\left(\frac{255}{MSE}\right) \quad (dB)$$

where $MSE = \frac{1}{W\times H} \sum_{i=1}^{H} \sum_{j=1}^{W} (OI(i,j) - DI(i,j))^2$

where $W\times H$ is the size of image, $OI(i,j)$ a pixel of the original image and $DI(i,j)$ a pixel of the decrypted image. Table 2 shows the PSNR values for some images.

Table 2: *The peak signal to noise ratio of some encrypted images.*

Image	Lena			Mandrill			Pepper		
	Red	**Green**	**Blue**	**Red**	**Green**	**Blue**	**Red**	**Green**	**Blue**
loss 15%	35.3900	37.7780	38.4302	35.2594	35.6046	36.2049	34.9495	36.1639	38.7565
loss 40%	31.0203	33.4110	34.2228	30.7908	31.0408	31.7175	30.3950	31.5676	34.2500
Noise 3%	39.5836	42.2247	42.3936	39.3673	39.8392	40.1186	38.9030	39.9778	42.5033
Noise 20%	31.7474	34.2945	34.8950	31.4815	31.8250	32.3980	31.2189	32.4015	35.0655

5 Conclusions

In this paper, a scheme for image encryption using 3D chaotic system is presented. The encryption method involves scrambling, diffusion, and linear transformation techniques to make it more confident. The experimental analysis and results of the proposed system includes histogram analysis, correlation analysis, and peak signal to noise ratio. The results show that the graphical shape of histogram for cipher image is uniformly distributed, so the proposed algorithm is protected from frequency analysis attack. Also, the low correlation coefficient of encrypted image is near to the ideal value zero. Thus the experimental results and statistical analysis demonstrate the security, flexibility, correctness, effectiveness, and robustness of the proposed cryptosystem.

6 References

[1] C. Pak and L. Huang, “A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129-137, Sep. 2017.

[2] O. A. Alkishriwo, “An image encryption algorithm based on chaotic maps and discrete linear chirp transform,” *Almadar Journal for Communications Information Technology and Applications*, vol. 5, no. 1, pp. 14-19, Jun. 2018.

[3] A.B. Abugharsa, A..Basari, and H. Almangush, “A New Image Scrambling Approach using Block-Based on Shifted Algorithm,” *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 7, pp. 570-579, 2013.

[4] Y. Zhang and X. Wang, “A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice,” *Information Science*., vol. 273, pp. 329–351, Jul. 2014.

[5] H. Huang and S. Yang, “Colour image encryption based on logistic mapping and double random-phase encoding,” *IET Image Processing*, vol. 11, no. 4, pp. 211-216, Mar. 2017.