A Chaotic Cryptosystem for Color Image with Dynamic Look-Up Table

Med Karim Abdmouleh(✉), Ali Khalfallah, and Med Salim Bouhlel

University of Sfax,
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology, Sfax, Tunisia
medkarim.abdmouleh@isggb.rnu.tn, ali.khalfallah@enetcom.rnu.tn,
medsalim.bouhlel@enis.rnu.tn

Abstract. The chaotic cryptosystems have been widely investigated to provide fast and highly secure image encryption. In this paper, we introduce a novel cryptosystem for color image based on chaos by using a dynamic Look-Up Table (LUT). We utilized the Logistic Map chaotic system in order to benefit from its sensitivity to initial conditions.

The result shows that the proposed cryptosystem have many characteristics such as high security, high sensitivity and high speed that can be applied in the encryption of color images. It is demonstrated that the NPCR = 99.6140 %, the UACI = 33.5448 % and entropy = 7.9984 can satisfy security and performance requirements. Simulations show that the proposed cryptosystem has high security and resist various typical attacks.

Keywords: Color image encryption · Chaotic system · Look-Up Table · Logistic map

1 Introduction

In recent years, with the fast exchange and transmission of digital images over the internet, researchers have focused on the image encryption [1]. Chaotic systems have been widely used in the image encryption algorithms [2–22]. Chaotic systems have many particular properties, such ergodicity, sensitivity to initial conditions and to control parameters and randomness [23]. These properties are very important in cryptography. Recently, a variety of chaotic cryptosystem for gray-scale image have been proposed [2–13]. However, a few researches have focused on color image [14–22].

In [15], a novel color image encryption algorithm based on chaos was proposed. The authors used a chaotic system to encrypt the R, G, B components of a color image at the same time and make these three components affect one other. Therefore, the correlations between the R, G, B components can be reduced and the security of algorithm is increased. Wang et al. [16] introduced a new image encryption algorithm based on iterating the chaotic maps. Using the pseudorandom sequence generated by a group of one-dimensional chaotic

A. Mansouri et al. (Eds.): ICISP 2016, LNCS 9680, pp. 91–100, 2016.
DOI: 10.1007/978-3-319-33618-3_10

maps, the proposed algorithm realizes fast encryption and decryption of both a gray-scale image and a true color image. Moreover, the rounds of encryption could be set by the user. In [19] the authors designed a stream-cipher algorithm based on one-time keys and robust chaotic maps, in order to get high security and improve the dynamical degradation. We utilized the piecewise linear chaotic map as the generator of a pseudo-random key stream sequence. The initial conditions were generated by the true random number of generators and the MD5 of the mouse positions. We applied the algorithm to encrypt the color image. In [20], Benjeddou et al. proposed a new color image encryption technique using two multidimensional chaotic maps: a three dimensional chaotic map for the key expansion and a two dimensional chaotic map for the generation of two chaotic Look-Up Tables.

The rest of this paper is organized as follows. Section 2 describes the cryptosystem for color image. Section 3 presents the simulation and the experimental results to prove the performance of encryption algorithm. Finally, Sect. 4 concludes the paper.

2 Color Image Encryption Scheme Based on Chaos

We convert every image I with size (M × N) in 24-bit true color into its 3 components (R, G and B). The size of each color's (R, G or B) matrix is (M × N) and contains integers between 0 and 255, then each matrix will be encrypted. In this paper, we use the Logistic Map as the chaotic system which is widely used in chaotic cryptosystem for its simplicity and high sensitivity to initial conditions. It is defined by:

$$X_{n+1} = \mu \ \mathrm{X_n} \ (1 - X_n) \tag{1}$$

where μ is a control parameter, X_n is a real number in the range [0, 1] and X_0 is an initial condition. When $3.569955672 < \mu \leq 4$, the system becomes chaotic [24].

In the rest of this section we provide the process of encryption algorithm.

Step 1. The RGB color image I with size (M × N) is divided into three separate images I_R, I_G and I_B (i.e., every image represents one of the three color components (red, green and blue)) as follows:

$$\begin{gathered} I_R(x,y) = I(x,y,1);\ \ I_G(x,y) = I(x,y,2); \\ I_B(x,y) = I(x,y,3) \\ where\ 1 \leq x \leq M\ and\ 1 \leq y \leq N \end{gathered} \tag{2}$$

Step 2. Firstly, we generate a chaotic matrix using the Logistic Map function LM_1 with the parameters (x_{0XOR} and μ_{0XOR}). We mix the obtained chaotic matrix with the original image (I_R, I_G or I_B) using the logical function XOR $\oplus$ to obtain the initial encrypted image I_1 (Fig. 1(a)).

Then, for each pixel P_1 from I_1, we generate a chaotic LUT using the second Logistic Map function (LM_2) having as parameters ($x_0(P_c)$ and μ_0). Where P_c is the value of the previous encrypted pixel by our cryptosystem. The initial condition $x_0(P_c)$ depends on the previous value of the ciphered pixel and x_0 with $x_0(P_c) \in [0.1, 0.9]$ (Fig. 1(b)).

Finally, we apply the New LUT to P_i to obtain the final encrypted pixel. We repeat this process for each pixel from the initial encrypted image to get the final encrypted one (Fig. 1(c)).

Step 3. We apply **the steps in Step 2** for each component (R, G and B) of the original image I. We obtain three encrypted images (I_{CR} is the encrypted image of I_R, I_{CG} is the encrypted image of I_G and I_{CB} is the encrypted image of I_B).

Step 4. Grouping the three encrypted images (I_{CR}, I_{CG} and I_{CB}) in order to have the encrypted image I_C.

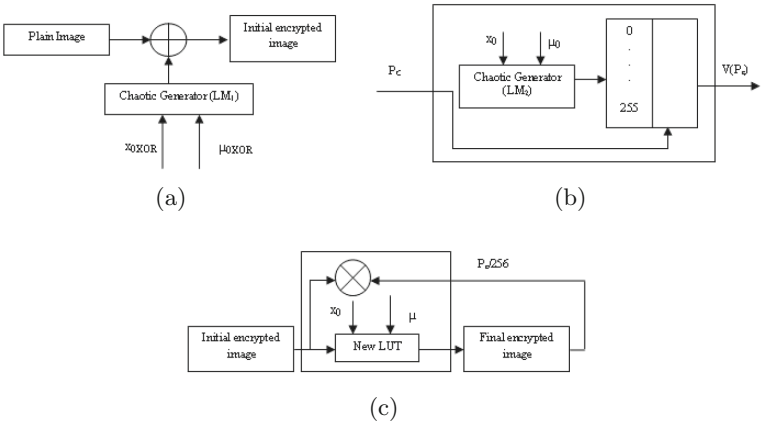


Fig. 1. Architecture of the proposed method: (a) XOR Chaotic encryption (b), Chaotic Dynamic Look-Up Table (c), Chaotic Look-Up Table encryption.

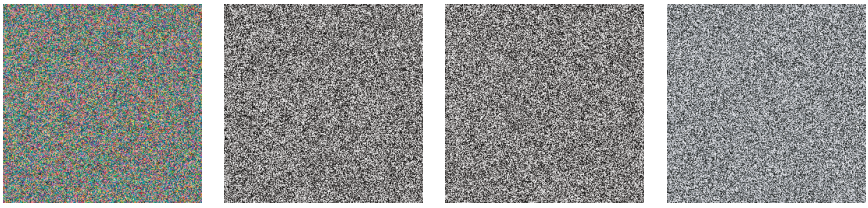
The decryption procedure is identical to that of the encryption algorithm except that the order is reversed.

3 Experimental Results

An image cryptosystem should be robust against all types of attacks (cryptanalytic and statistical attacks). In what follows, we present the different results obtained by statistical analysis of our cryptosystem [25]. These experiments include key space analysis, sensitivity analysis, histogram analysis of the original and the encrypted images, information entropy analysis, correlation coefficient analysis and differential analysis. The Lena color image of size (256×256) is

(a) (b) (c) (d)

Fig. 2. Original color image and its R, G, B components: (a) Original image, (b) R component of the original image, (c) G component of the original image, (d) B component of the original image.



(a) (b) (c) (d)

Fig. 3. Encrypted image and its R, G, B components: (a) Encrypted image, (b) R component of the encrypted image, (c) G component of the encrypted image, (d) B component of the encrypted image.

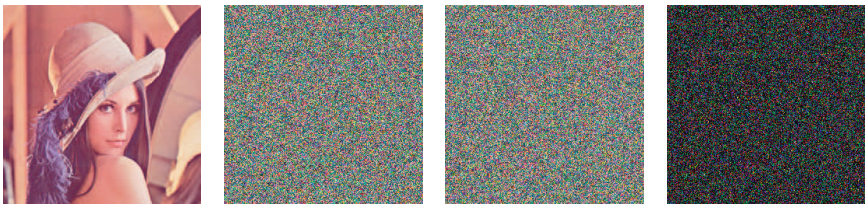
opted for encryption. Figure 2(a) shows the color original image. Figure 2(b)–(d) show the R, G, B components of the original image. The encrypted image and its R, G, B components are shown in Fig. 3(a)–(d).

3.1 Key Space Analysis

A good encryption algorithm should not only be sensitive to the secret key, but also the key space should be large enough to make brute-force attacks infeasible. In this cryptosystem, the initial conditions and parameters $\{x_0, \mu_0, x_{0XOR}, \mu_{0XOR}\}$ can be used as key. In our simulations we use MATLAB 8.3. This mathematical tool codes real in 8 bytes. Therefore, all the parameters are presented in 64 bits. Then, for each component of the color image we have $\{2^{64} \times 2^{64} \times 2^{64} \times 2^{64}\} = 2^{256}$ combinations. Our secret key has 2^{256} different combinations.

3.2 Sensitivity Analysis

1. **Key Sensitivity Analysis in the Encryption Phase**
   Figure 4(a) shows the original Lena image. Figure 4(b) shows the encrypted image of Lena with the correct encryption key $k_0 = \{0.25, 3.8701, 0.4, 3.9\}$. We change key k_0 by adding 10^{-15} for real x_0, then, the difference between the



(a) (b) (c) (d)

Fig. 4. Key sensitivity analysis in encryption phase: (a) Original image of Lena, (b) Encrypted image with key k_0, (c) Encrypted image with key k_1, (d) Difference between (b) and (c).

(a) (b) (c) (d)

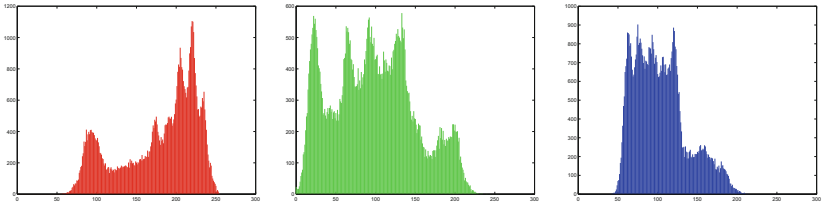
Fig. 5. Key sensitivity analysis in decryption phase: (a) Original image of Lena, (b) Encrypted image with key k_0, (c) Decrypted image with key k_0, (d) Decrypted image with key k_1.

two corresponding encrypted images is calculated. The encrypted Lena image with key $k_1 = \{0.250000000000001, 3.8701, 0.4, 3.9\}$ is shown in Fig. 4(c). Figure 4(d) is a plot of the difference between the two encrypted images.

2. **Key Sensitivity Analysis in the Decryption Phase**
   In addition, decryption using key with slight change above is also performed so as to evaluate the key sensitivity. The original image is encrypted with the original key $k_0 = \{0.25, 3.8701, 0.4, 3.9\}$, and the encrypted image is obtained, it shown in Fig. 5(b). The original key is modified slightly (order of 10^{-15} for real x_0). The encrypted image obtained by key k_0 is decrypted with the modified key $k_1 = \{0.250000000000001, 3.8701, 0.4, 3.9\}$. The results are plotted in Fig. 5. Figure 5(d) shows that the reconstructed image is noisy even when the key has only a tiny modification.
   Therefore, it can be concluded that the proposed algorithm is sensitive to the key, a small change of the key will generate a completely different decryption result and cannot get the correct original image.

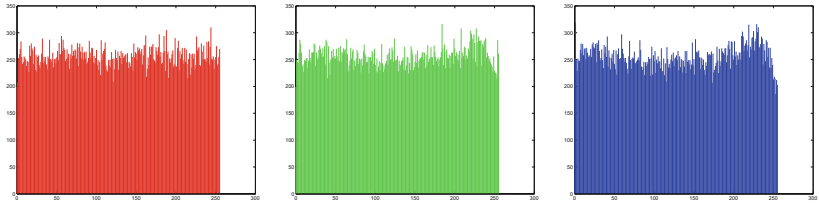
3.3 Histogram Analysis

The histograms of the original and the encrypted image are shown in Figs. 6 and 7. Referring to the obtained results, we can see that histogram of the



(a) (b) (c)

Fig. 6. Histogram of the original image R, G, B components: (a) Histogram of R component, (b) Histogram of G component, (c) Histogram of B component.



(a) (b) (c)

Fig. 7. Histogram of the encrypted image R, G, B components: (a) Histogram of R component, (b) Histogram of G component, (c) Histogram of B component.

encrypted image Fig. 7(a)–(c) is fairly uniform and is significantly different from that of the original image.

3.4 Information Entropy Analysis

The entropy, which was proposed by Shannon in 1948 [26], is defined as:

$$H(m) = -\sum_{i}^{2^M-1} P(m_i)\ \log_2 P(m_i) \tag{3}$$

Here, $P(m_i)$ represents the probability of symbol m_i. The entropy H(m) is expressed in bits.

For a purely random source emitting 2^M symbols, the entropy is H(m) = M.

Table 1 shows the entropy of the three color components R, G and B. The values obtained are very close to the theoretical value H(m) = 8 bits/pixel. From this result, it is clear that our encryption image scheme is robust against the entropy attack.

3.5 Correlation Between Neighboring Pixels

It is well known that adjacent image pixels are highly correlated in the original image. In order to resist a statistical attack, we must decrease the correlation of

Table 1. Results of information entropy.

Component	R	G	B
Entropy	7.9945	7.9956	7.9954

two adjacent pixels in the encrypted image [27]. We calculate the correlation for a sequence of adjacent pixels using the following formula:

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4}$$

Here, x and y are the intensity values of two adjacent pixels in the image. r_{xy} is the correlation coefficient. The cov(x,y), E(x) and D(x) are given as follows:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} [x_i - E(x_i)] \tag{6}$$

$$\text{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} [(x_i - E(x_i))(y_i - E(y_i))] \tag{7}$$

N is the number of adjacent pixels selected from the image to calculate the correlation.

To calculate the correlation coefficient, we have randomly chosen 2500 pairs of two adjacent pixels from the original image and the encrypted image.

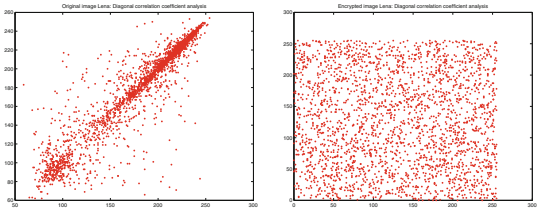
It's clear from Fig. 8 and Tables 2 and 3 that the correlation between two adjacent pixels for the encrypted Lena image is much smaller than that of the original image. This little correlation between two neighboring pixels in the encrypted image makes the brook of our cryptosystem difficult.

Table 2. Correlation coefficients of two adjacent pixels in the original image.

Correlation direction	Original image		
	R Component	G Component	B Component
Horizontal	0.9523	0.9355	0.9175
Vertical	0.9759	0.9665	0.9478
Diagonal	0.9278	0.9102	0.8883

Table 3. Correlation coefficients of two adjacent pixels in the encrypted image.

Correlation direction	Encrypted image		
	R Component	G Component	B Component
Horizontal	0.0014	0.0003	0.0003
Vertical	0.0015	−0.0044	0.0032
Diagonal	0.0034	0.0024	−0.0067



(a) (b)

Fig. 8. Correlation of diagonal adjacent two pixels: (a) R component of the original image, (b) R component of the encrypted image.

3.6 Differential Analysis

The objective of this analysis is to prove that a small change in the original image introduces a major change to the encrypted image. This difference can be measured by means of two criteria namely, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI). The theoretical values for an ideal cryptosystem are close to 100 % to the value of NPCR while the value of UACI must be very close to 33 %.

Let I_2 be the changed original image on one pixel. C_1 and C_2 are the ciphered images of the original images I and I_2. D is a matrix having the same size as the image figures C_1 and C_2. D(i,j) is determined as follows:

$$D(i,j) = \begin{cases} 1 \; if \; C_1(i,j) \neq C_2(i,j) \\ 0 \; else \end{cases} \tag{8}$$

The NPCR is defined by:

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100 \tag{9}$$

M and N are the height and width of encrypted images C_1 and C_2.
The UACI is defined by:

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100 \tag{10}$$

Two images are used in the tests. The first image is the original image, and the other is obtained by changing the first pixel value of R component from '224' to '225'. Then the two images are encrypted with the same key k_0 to generate the corresponding encrypted images C_1 and C_2.

The results obtained are NPCR = 99.6140 % and UACI = 33.5448 %. The results show that a small change in the plain image introduces a high alteration on the encrypted one. Hence, the proposed cryptosystem is robust against the differential attacks.

4 Conclusion

In this paper, we introduced a new color image encryption algorithm based on chaotic systems called Look-Up Table. This new cryptosystem uses the "Logistic Map" function to generate a dynamic LUT. The performance of this LUT is introduced to the cryptosystem feedback because this LUT depends on the encrypted previous pixel.

Simulation results demonstrate that satisfactory performance (sensitivity and security) is achievable in our proposed cryptosystem. The results show that the cryptosystem can encrypt the color image effectively.

References

1. Uhl, A., Pommer, A.: Image And Video Encryption: From Digital Rights Management To Secured Personal Communication (Advances in Information Security). Springer-Verlag TELOS, Santa Clara (2004)
2. Chen, J.X., Zhu, Z.L., Fu, C., Zhang, L.B., Zhang, Y.: An efficient image encryption scheme using lookup table-based confusion and diffusion. Nonlinear Dyn. **81**(3), 1151–1166 (2015)
3. Abdmouleh, M.K., Khalfallah, A., Bouhlel, M.S.: A new watermarking technique for medical image using hierarchical encryption. Int. J. Comput. Sc. Issues (IJCSI) **11**(4), 27–32 (2014)
4. Abdmouleh, M.K., Khalfallah, A., Bouhlel, M.S.: Dynamic chaotic Look-Up Table for MRI medical image encryption. In: International Conference on Systems, Control, Signal Processing And Informatics (SCSI), pp. 241–246 (2013)
5. Chen, J.X., Zhu, Z.L., Fu, C., Yu, H.: An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism. Opt. Express **21**(23), 27873–27890 (2013)
6. Abdmouleh, M.K., Khalfallah, A., Bouhlel, M.S.: Image encryption with dynamic chaotic Look-Up Table. In: 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp. 331–337 (2012)
7. Liao, X., Lai, S., Zhou, Q.: A novel image encryption algorithm based on self-adaptive wave transmission. Signal Process. **90**(9), 2714–2722 (2010)
8. Masmoudi, A., Bouhlel, M.S., Puech, W.: A new image cryptosystem based on chaotic map and continued fractions. In: 18th European Signal Processing Conference (EUSIPCO), pp. 1504–1508 (2010)
9. Wang, X.Y., Yang, L., Liu, R., Kadir, A.: A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn. **62**(3), 615–621 (2010)

10. He, B., Zhang, F., Luo, L., Du, M., Wang, Y.: An image encryption algorithm based on spatiotemporal chaos. In: 2nd International Congress on Image and Signal Processing (CISP), pp. 1–5 (2009)
11. Gao, T., Chen, Z.: A new image encryption algorithm based on hyper-chaos. Phys. Lett. A **372**(4), 394–400 (2008)
12. Sun, F., Liu, S., Li, Z., Lu, Z.: A novel image encryption scheme based on spatial chaos map. Chaos, Solitons Fractals **38**(3), 631–640 (2008)
13. Xiang, T., Wong, K.W., Liao, X.: Selective image encryption using a spatiotemporal chaotic system. Chaos: Interdisc. J. Nonlinear Sci. **17**(2), 023115 (2007)
14. Abu Zaid, O.M., Demba, M.: A proposed cryptosystem algorithm based on two different chaotic systems (PCA2CS) for securing the colored images. Int. J. Comput. Sci. Issues (IJCSI) **11**(2), 159–166 (2014)
15. Wang, X., Teng, L., Qin, X.: A novel colour image encryption algorithm based on chaos. Signal Process. **92**(4), 1101–1108 (2012)
16. Wang, X., Zhao, J., Liu, H.: A new image encryption algorithm based on chaos. Optics Commun. **285**(5), 562–566 (2012)
17. Gupta, K., Silakari, S.: New approach for fast color image encryption using chaotic map. J. Inf. Secur. **2**(4), 139–150 (2011)
18. Mazloom, S., Eftekhari-Moghadam, A.M.: Color image cryptosystem using chaotic maps. In: IEEE Symposium on Computational Intelligence for Multimedia, Signal and Vision Processing (CIMSIVP), pp. 142–147 (2011)
19. Liu, H., Wang, X.: Color image encryption based on one-time keys and robust chaotic maps. Comput. Math. Appl. **59**(10), 3320–3327 (2010)
20. Benjeddou, A., Taha, A.K., Fournier-Prunaret, D., Bouallegue, R.: A fast color image encryption scheme based on multidimensional chaotic maps. In: Global Information Infrastructure Symposium (GIIS), pp. 1–4 (2009)
21. Rhouma, R., Meherzi, S., Belghith, S.: OCML-based colour image encryption. Chaos, Solitons Fractals **40**(1), 309–318 (2009)
22. Pareek, N., Patidar, V., Sud, K.: Image encryption using chaotic logistic map. Image Vis. Comput. **24**(9), 926–934 (2006)
23. Kocarev, L.: Chaos-based cryptography: a brief overview. IEEE Circuits Syst. Mag. **1**(3), 6–21 (2001)
24. Li, J., Feng, Y., Yang, X.: Discrete chaotic based 3D image encryption scheme. In: Symposium on Photonics and Optoelectronics (SOPO), pp. 1–4 (2009)
25. Abdmouleh, M.K., Khalfallah, A., Bouhlel, M.S.: An overview on cryptography and watermarking. In: International Conference on Computers, Automatic Control, Signal Processing and Systems Science, pp. 99–104 (2014)
26. Shannon, C.E.: A mathematical theory of communication. Bell Syst. Tech. J. **27**(3), 379–423 (1948)
27. Behnia, S., Akhshani, A., Mahmodi, H., Akhavan, A.: A novel algorithm for image encryption based on mixture of chaoticmaps. Chaos, Solitons Fractals **35**(2), 408–419 (2008)