Erzincan Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
2019, 12(2), 687-694
ISSN: 1307-9085, e-ISSN: 2149-4584
Araştırma Makalesi

Erzincan University
Journal of Science and Technology
2019, 12(2), 687-694
DOI:10.18185/erzifbed.477525
Research Article

Higher Dimensional Chaotic Linear Transformations of Colored Image Encryptions

Deniz ELMACI[1], Nursin BAS CATAK[2*]

[1]Department of Computer Technology, Bergama Vocational School,
Dokuz Eylul University, Izmir, Turkey
[2]Department of Mathematics, Ege University, Izmir, Turkey

Geliş / Received: 01/11/2018, Kabul / Accepted: 08/05/2019

Abstract

In this study, a well-known chaotic transformation namely Arnold's CAT map is used to extend 2-dimensional mapping to a higher dimension. This extension is achieved by means of the planar extension and Multinacci series. The demonstration of a 3-dimensional Arnold's CAT map is performed by RGB component substitution of a colored image. For this purpose, the colored image is converted from a standard RGB space into an intensity-hue-saturation (IHS) space. Consequently, both Chebyshev and Hadamard map is employed for encryption of the intensity component. Besides, CAT map is engaged to encrypt the hue and saturation components. According to the results, the proposed method has a great potential to be an efficient tool for data encryption.

Keywords: Image Encryptions, Arnold's CAT Map, Chebyshev Map, Hadamard Map.

Renkli Resimlerin Yüksek Boyutlu Kaotik Lineer Dönüşümlerle Şifrelenmesi

Öz

Bu çalışmada, 2 boyutlu dönüşümü daha yüksek bir boyuta genişletmek için Arnold'ın CAT dönüşümü olarak bilinen kaotik bir dönüşüm kullanılmıştır. Bu boyut artırma işlemi düzlemsel genişleme ve Multinacci serisi ile elde edilir. 3 boyutlu bir Arnold'ın CAT dönüşümünün gösterimi, renkli bir görüntünün RGB bileşen değişimi ile gerçekleştirilir. Bu amaçla, renkli görüntü standart bir RGB uzayından yoğunluk-ton-doygunluk (IHS) aralığına dönüştürülür. Sonuç olarak, hem Chebyshev hem de Hadamard dönüşümü, yoğunluk bileşeninin şifrelenmesi için kullanılmaktadır. Ayrıca, ton haritası ve doygunluk bileşenlerini şifrelemek için CAT dönüşümü kullanılmıştır. Elde edilen sonuçlara göre, önerilen yöntem veri şifreleme için etkin bir yöntem olma potansiyeline sahiptir.

Anahtar Kelimeler: Resimlerin şifrelenmesi, CAT dönüşümü, Chebyshev dönüşümü, Hadamard dönüşümü.

1. Introduction

Due to the progress of science and technologies, the multimedia data such as image, video etc. can be transferred rapidly. However, many attempts to steal the data can be made during the transfer. To overcome this disadvantage many expensive affords has been made to protect the data [1]. For that reason, chaotic encryption systems become important in terms of improving the security level. As it is dependent on initial conditions and system parameters. Cryptography is a

*Corresponding Author: nursin.catak@ege.edu.tr

commonly used technique which protects the contents of the messages that are from insecure channels. But most of its algorithms have disadvantages such as small key space and low level of security. To meet these challenges, many chaos-based algorithms have been suggested [1-11]. The chaotic behavior is a cure part of a nonlinear system. Although this system seems random, it is not originated from stochastic behavior. The basis of the chaotic behavior is related with deterministic processes. Therefore, chaos based communication and chaotic cryptography has been utilized for secure communication and data storage. Accordingly, the chaos based cryptographic algorithms are promising and efficient route to develop secure image encryption techniques. Encryption schemes use chaotic systems for key generation, and the key is furtherly used for generation of chaotic sequences. A dynamical chaotic system is defined by V. I. Arnold in 1960. He used a continuous automorphism on the torus, namely CAT map. In his work, V. I. Arnold used an image of a cat to build a transformation which changes the order of pixels of the image in randomized order [2]. This work concerns with a colored image encryption technique which uses both Arnold's CAT map (ACM) - Chebyshev map and ACM - Hadamard map in the intensity-hue-saturation (IHS) color space. The standard Red-Green-Blue (RGB) color image is transformed into the IHS color space. Each component is then encrypted independently with different approaches. For the I component, Chebyshev and Hadamard maps are used for the encryption, separately. Chebyshev and Hadamard maps are such encryption for the value and position of the pixel. H and S components which are position mixing technique are encrypted using ACM.

2. Material and Methods

2.1. Chaotic Linear Transformations

2.1.1. Arnold's CAT Map

In ACM, an image is divided into an appropriate number of pixels to constitute an N×N matrix of pixels in which the coordinates is represented by an ordered pair (X, Y) of real numbers in the interval [0, 1).

The transformation of all pixels is achieved by the multiplication of each pixel by a special matrix A of ACM as follows:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \tag{1}$$

The resultant matrix is taken in mod 1 to normalize each coordinates in the interval [0, 1) [3]. ACM induces a discrete-time dynamical system in which the evolution of pixels is given by each iteration of the transformation [3].

The next position of any pixel exposed by the transformation is given by the following equation:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \Gamma_{cat} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \ (mod\ 1) \tag{2}$$

Planar extension can be used for generalized CAT map which is given in Eq. 2 by the following equations:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & p_z & 0 \\ q_z & p_z q_z + 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} \ (mod\ N) \tag{3}$$

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & p_x \\ 0 & q_x & p_x q_x + 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} \ (mod\ N) \tag{4}$$

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & p_y \\ 0 & 1 & 0 \\ q_y & 0 & p_y q_y + 1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \\ z_n \end{pmatrix} \ (mod\ N) \tag{5}$$

$$A = \begin{pmatrix} 1 & p_z & 0 \\ q_z & p_z q_z + 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & p_x \\ 0 & q_x & p_x q_x + 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & p_y \\ 0 & 1 & 0 \\ q_y & 0 & p_y q_y + 1 \end{pmatrix} \ (mod\ N) \tag{6}$$

The matrix A obtained in Eq. 6 can be used as a 3-dimensional Arnold's CAT map. The other method of extension is Multinacci series, which can be implemented as [4-5]:

$$A = M^n, \qquad M = \begin{bmatrix} 1 & 1 & 1 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 1 & 0 \end{bmatrix} \ (mod\ N) \tag{7}$$

It can be expressed matrix of M as Tribonacci matrix for 3-dimensional ACM.

$$t_{n+1} = t_n + t_{n-1} + t_{n-2} \tag{8}$$

$t_0 = t_1 = 0, \ t_2 = 1$

Tribonacci numbers are obtained by using Eq. 8. The matrix can be written [4-5]:

$$M = \begin{pmatrix} t_4 & t_3 & t_2 \\ t_3 + t_2 & t_2 + t_1 & t_1 + t_0 \\ t_3 & t_2 & t_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \tag{9}$$

which is the n[th] power:

$$M^n = \begin{pmatrix} t_{n+2} & t_{n+1} & t_n \\ t_{n+1} + t_n & t_n + t_{n-1} & t_{n-1} + t_{n-2} \\ t_{n+1} & t_n & t_{n-1} \end{pmatrix} \tag{10}$$

In Eq. 7, N is used to define matrix A.

$$A = \begin{pmatrix} 4 & 3 & 2 \\ 2 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix} \tag{11}$$

2.1.2. Chebyshev Map

The private keys are generated by using Chebyshev polynomial in the proposed algorithm and Chebyshev polynomial is defined as $T_n(x)$ by the following relation [6]:

$$T_n(x) = \cos(n\theta) \tag{12}$$

where $x = \cos(\theta)$. For n = 0, 1, 2, 3, 4, …

$\cos(0\theta) = 1 \ \Rightarrow \ T_0(x) = 1$

$\cos(1\theta) = \cos\theta \ \Rightarrow \ T_1(x) = x$

$$\cos(2\theta) = \cos^2\theta - 1 \quad \Rightarrow \quad T_2(x) = x^2 - 1$$

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta \quad \Rightarrow$$

$$T_3(x) = 4x^3 - 3x$$

$$\cos(4\theta) = 8\cos^4\theta - 8\cos^2\theta + 1 \quad \Rightarrow$$

$$T_4(x) = 8x^4 - 8x^2 + 1 \qquad (13)$$

2.1.3. Hadamard Map

A Hadamard map H_m is a $2^m \times 2^m$ matrix. The Hadamard matrix, H_m, is a square matrix of order m = 1, 2, or 4k where k is a positive integer. The elements of H are either +1 or 1 and $H_m H_m^T = mI_m$, where H_m^T is the transpose of H_m, and I_m is the identity matrix of order m.

A Hadamard matrix is said to be normalized if all of the elements of the first row and first column are +1. $H_0 = 1$, and then H_m is defined by for m > 0 [6-7]:

$$H_{m-1} = \frac{1}{\sqrt{2}}\begin{pmatrix} H_{m-1} & H_{m-1} \\ H_{m-1} & -H_{m-1} \end{pmatrix} \qquad (14)$$

where the $\frac{1}{\sqrt{2}}$ is a normalization that is sometimes omitted. For m > 1, H_m is defined by:

$$H_m = H_1 \otimes H_{m-1} \qquad (15)$$

where $\otimes$ represents the Kronecker product.

3. Resarch Findings

3.1. The Encryption Method of a Colored Image

Each pixel of the image is represented by three RGB values in a standard RGB color image. Color models are mathematical represented by a set of colors that can be divided in RGB and IHS models. The RGB model utilized by many visual systems is based on a Euclidean coordinate system and all colors are included in a cube. On the other hand, a color space that has three constituent components is defined in IHS model in which RGB color space is transformed nonlinearly. These two models can be transformed with each other. Many published studies show that various IHS transformations [8-9]. Transformations which are used in this study are expressed by the following steps of equations.

First, it is converted RGB color space image to IHS space beginning with normalizing RGB values [9-10]:

$$r = \frac{R}{R+G+B}\ ,\ \ g = \frac{G}{R+G+B}\ ,\ b = \frac{B}{R+G+B} \qquad (16)$$

$$i = \frac{R+G+B}{3\times 255}\ ;\quad i \in [0,1] \qquad (17)$$

$$h = \cos^{-1}\frac{0.5[(r-g)+(r-b)]}{[(r-g)^2+(r-b)(g-b)]^{\frac{1}{2}}}\ ;$$

$$h \in [0,\pi] \quad for\ b \le g$$

$$h = 2\pi - \cos^{-1}\frac{0.5[(r-g)+(r-b)]}{[(r-g)^2+(r-b)(g-b)]^{\frac{1}{2}}}\ ;$$

$$h \in [0,\pi] \quad for\ b > g \qquad (18)$$

$$s = 1 - 3\min(r,g,b)\,;\quad s \in [0,1] \qquad (19)$$

For simplicity, h, s and i values are converted in the ranges of [0, 360], [0, 100], [0, 255], respectively, by:

$$H = h \times \frac{180}{\pi}\ ;\quad S = s \times 100\ ;\quad I = i \times 255 \qquad (20)$$

Then it is converted the IHS image back to RGB by following equations:

$$x = i.(1-s)$$

$$y = i.\left[1 + \frac{s.\cos(h)}{\cos\left(\frac{\pi}{s} - h\right)}\right] \qquad (21)$$

$$z = 3i - (x+y)$$

$$h < \frac{2\pi}{3} \quad \Rightarrow \quad r = y,\ g = x,\ b = z$$

$$\frac{2\pi}{3} \leq h < \frac{4\pi}{3} \quad \Rightarrow r = x,\ g = z,\ b = y \quad (22)$$

$$\frac{4\pi}{3} \leq h < 2\pi \quad \Rightarrow r = z,\ g = y,\ b = x$$

The result r, g and b are normalized values, which are in the ranges of [0, 1], therefore, they should be multiplied by 255 for displaying.

3.2. Encryption scheme

To initiate the scheme, the original RGB image should be transformed into IHS space. The intensity I component which is the gray information of the color image is encrypted into I_{new} by Chebyshev and Hadamard maps separately. For the hue H component, ACM is used for ω_H iterative numbers to get a mixed image H_{new}. Conveniently, S component is mixed into S_{new} after ω_S iterative number ACM. In these two steps, the iterative numbers ω_H, ω_S and the period T of ACM are called as encryption keys. Ultimately, the encrypted color image can be obtained when the inverse IHS transformation is taken. The transformation scheme is illustrated in Fig. 1.

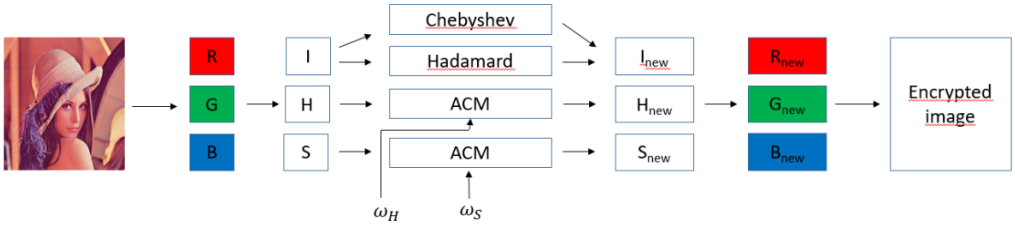


Figure 1: The transformation scheme

The decryption process is the inverse process of the above scheme. For the H and S components, after (T – ω_H) and (T – ω_S) iterative numbers ACM, the decrypted H and S can be obtained, respectively. The decrypted I, H and S components are transformed into RGB space to get the decrypted color image [9].

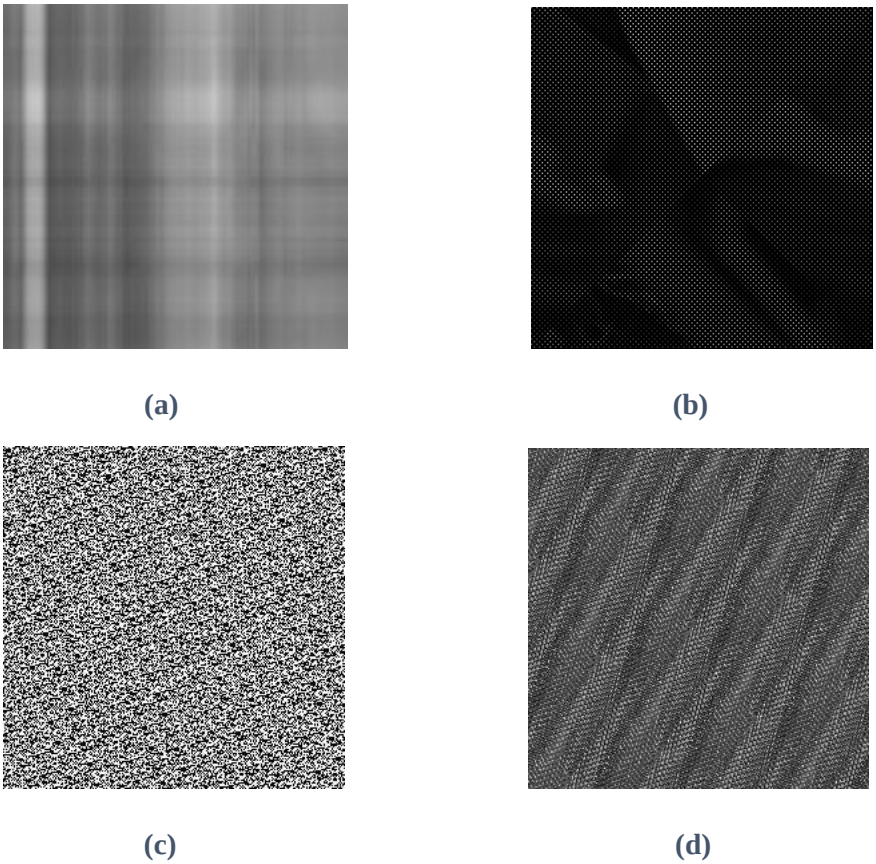
4. Results

By using Matlab® [12], a 512 × 512 pixels of Lena picture is converted to 256 × 256 pixels of the image. Then, the above-mentioned encryption process was performed. Accordingly, Chebyshev map and ACM, a digital scheme of colored image encryption is suggested in IHS color space as shown in Fig. 2(a), the other proposed encryption method which is on the basis of Hadamard map an ACM is showed in Fig. 2(b).

(a) **(b)**

Figure 2: (a) Encrypted with Chebyshev map. **(b)** Encrypted with Hadamard map.

When the Chebyshev map is applied, $T_2(x)$ is used to encryption for the normalization and easy decryption process $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is used 4 times for encryption with Hadamard map. ACM is used for ω_H =75 iterative numbers for the H component and ω_S = 125 iterative numbers for the S component both encryption method. The obtained results are given in Fig. 3.



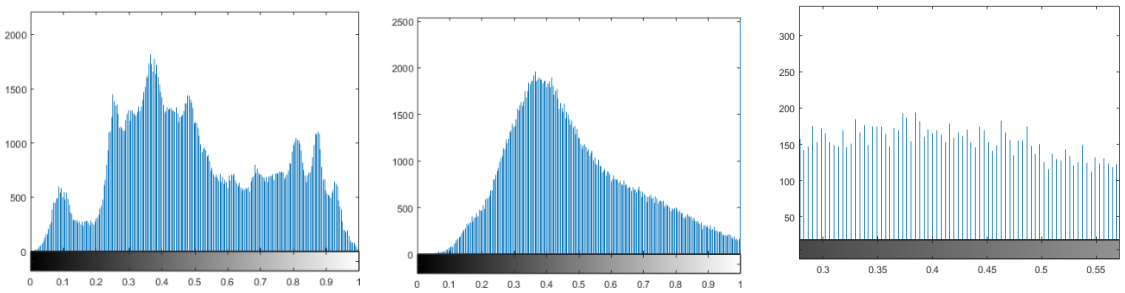
(a) **(b)**

(c) **(d)**

Figure 3: (a) Intensity component which is encrypted with Chebyshev map. **(b)** Intensity component which is encrypted with Chebyshev map. **(c)** Hue component which is encrypted with ACM for 75 times. **(d)** Saturation component which is encrypted with ACM for 125times.

4.1. Analysis of Histograms

Histogram analysis is a commonly used technique in image processing area. An image histogram shows the distribution of pixels in an image by plotting the number of pixels at each color intensity level. It shows the efficiency of the encryption process. For an efficient encryption, the histogram of the encrypted image will be nearly uniform. When Fig 4(a) shows the histogram of Lena's picture, Fig. 4(b) and 4(c) shows the histogram of two encrypted images which is encrypted using Chebyshev map and Hadamard map, respectively.



(a) **(b)** **(c)**

Figure 4: Histogram Analysis of **(a)** Lena's picture. **(b)** encrypted image with Chebyshev map. **(c)** encrypted image with Hadamard map

For an efficient encryption, the histogram of the encrypted image should almost be uniformly distrubuted. According to the results shown in Fig. 4, the method employed Hadamard map supplies better encryption than Chebyshev map method based on histogram analysis. While Chebyshev method result in very close to a Gaussian distrubution, Hadamard mapping gives nearly perfect uniform distribution.

4.2. Conclusion

In this work, a hybrid method is used for encrypt of a colored image through 3-dimensional CAT map. This hybrid method is proposed by using Arnold's CAT map, Chebyshev and Hadamard maps in the HIS color space whose three components (intensity, hue and saturation) are encrypted seperately by using ACM - Chebyshev and ACM - Hadamard maps, respectively. Each pixel of the image comprises a value and a position.

Moreover the results from the simulation of both Chebyshev and Hadamard maps are compared. It was seen that Chebyshev and Hadamard maps resulted in different distrubution of intensity level. This shows that Chebyshev and Hadamard maps can be considered as an encryption value and position of pixels simultaneously. Furthermore, it has been observed that ACM could drive a good positon mixing results, which yields more security for decryption of an image. Additionally, the decryption of the image is ensured accurately and easily by good periodicity property of ACM.

4.3. Acknowledgement

The authors would like to acknowledge to TUBITAK for their financial support.

5. References

Masuda N. and Aihara K., "Cryptosystems with discretized chaotic maps," IEEE Trans. on Circuits and Systems - I: Fundamental Theory and Applications, 2002, vol. 49, no. 1, page(s): 28-40. DOI: 10.1109/81.974872.

V. Arnold and A. Avez, "Ergodic Problems of Classical Mechanics," Benjamin, 1968. DOI:10.1002/zamm.19700500721.

F. Svanstrom, "Properties of a generalized Arnold's discrete cat map," 2014.

R.L. Devaney, "An Introduction to Chaotic Dynamical Systems," Second Edition, Addison-Wesley, 1987. DOI: 10.1063/1.2820117.

Brugia O., Filipponi P., Mazzarella F., "Applications of Fibonacci Numbers," Springer, 1991. DOI: 10.1007/978-94-011-3586-3-7.

J. Rosen, Z. Scherr, B. Weiss, and M. E. Zieve, "Chebyshev mappings of finite fields," Amer. Math. Monthly, 119(2):151-155, 2012.

K. J. Horadam, "Hadamard Matrices and Their Applications," Princeton University Press, ISBN: 9780691119212, 2007.

S. S. Agaian, "Hadamard Matrices and Their Applications," Springer, ISBN: 978-3-540-16056-4. DOI: 10.1007/BFb0101073, 1985.

Q. Guo, Z. Liu, S. Liu, "Color image encryption by using Arnold and discrete fractional random transforms in IHS space," Optics and Lasers in Engineering, 48,1174–1181, 2010.

R.C. Gonzalez, R.E.Woods, "Digital Image Processing," Second Edition, ISBN:0-201-11026-1, 1987.

D. Elmaci and N. Bas Catak, "An Efficient Image Encryption Algorithm for the Period of Arnold's CAT Map," Internaional Journal of Intelligent Systems and Applications in Engineering, 2018, vol. 6 no. 1, page(s): 80-84. DOI: 10.18201/ijisae.2018637935.

Matlab 2017a, https://www.mathworks.com