Open Mathematics **Open Access**

Research Article

Zhenghong Guo, Jie Yang, and Yang Zhao*

Double image multi-encryption algorithm based on fractional chaotic time series

DOI 10.1515/math-2015-0080
Received January 24, 2015; accepted November 3, 2015.

Abstract: In this paper, we introduce a new image encryption scheme based on fractional chaotic time series, in which shuffling the positions blocks of plain-image and changing the grey values of image pixels are combined to confuse the relationship between the plain-image and the cipher-image. Also, the experimental results demonstrate that the key space is large enough to resist the brute-force attack and the distribution of grey values of the encrypted image has a random-like behavior.

Keywords: Image encryption scheme, Fractional chaotic time series, Matlab

MSC: 68U10

1 Introduction

With the rapid growth of multimedia production systems, electronic publishing and widespread dissemination of digital multimedia data over the Internet, protection of digital information against illegal copying and distribution has become extremely important[1, 4, 5, 8]. To meet this challenge, a variety of encryption schemes have been illustrated [2, 3, 7, 11, 14]. Recently, along with the rapid development of theory and application of chaos, many researchers are now focusing on the chaotic cryptography, since it has shown some exceptionally good properties in many concerned aspects regarding security, complexity, speed, computing power and computational overhead, etc [9, 10, 12].

Fractional calculus, which dates back to the 17th century, has been applied to physics and engineering in recent decades [18, 19]. A fractional-order system is characterized by a dynamical system described by fractional derivatives and integrals. It has been found that most systems can be elegantly described with the help of fractional-order systems, especially the description of memory and hereditary properties of various materials and processes. Meanwhile, it has been shown that the chaotic behaviour of an integer order nonlinear system is maintained when the order becomes fraction. In comparison with their integer-order counterparts, fractional-order nonlinear systems in general show higher nonlinearity and more degrees of freedom in the model due to the existence of fractional derivatives. In fact, fractional derivatives have a complex geometrical interpretation for their nonlocal (or long-range dependence) effects either in space or time (for more details one can refer to [6, 13]).

Due to the excellent properties of fractional-order nonlinear systems, in this article we will use the logistic chaotical map to generate the time series, which was investigated by Li and Chen in [16, 17]. In their papers they introduced and discussed the fractional logistic chaotical map and gave the fractional logistic chaotical time series form as follows

Zhenghong Guo: School of Information Science and Engineering, Heibei North University, Zhangjiakou 075000, China
Jie Yang: School of Information Science and Engineering, Heibei North University, Zhangjiakou 075000, China
***Corresponding Author: Yang Zhao:** Department of Electronic and Information Technology, Jiangmen Polytechnic, Jiangmen 529090, China, E-mail: zhaoyang19781023@gmail.com

$$x(n) = x(0) + \frac{\mu}{\Gamma(v)} \sum_{i=1}^{n} \frac{\Gamma(n-i+v)}{\Gamma n - i + 1} x(i-1)(1-x(i-1)). \tag{1}$$

This paper is organized as follows. In Section 2, some basic preliminaries about fractional calculus (FC) are mentioned. In Section 3, a new kind of image encryption algorithm by fractional chaotic time series shall be introduced. Finally, in Section 4, we shall show some experimental results, statistical analysis and key secure analysis to demonstrate that the key space is large enough to resist the brute-force attack and the distribution of grey values of the encrypted image has a random-like behavior.

2 Preliminaries

In this section we shall recall some preliminaries of the fractional calculus (FC), which provides an useful tool for nonlinear problems.

Definition 2.1 ([6, 13]). *According to the Riemann-Liouville approach, the fractional integral of order $\alpha > 0$ with lower limit a of a function $f : [a, \infty] \to \mathbb{R}$ is defined by*

$$I_t^{\alpha} f(t) := \int_a^t \frac{(t-s)^{\alpha-1}}{\Gamma(\alpha)} f(s)ds,\ t \geq a,$$

provided that the right-hand side is point-wise defined, where Γ is the Ruler gamma function.

Definition 2.2 ([6, 13]). *Let $\alpha > 0$ and m be the smallest integer greater than or equal to α. The Riemann-Liouville fractional derivative of order α with lower limit 0 for a function $f : [a, \infty) \to \mathbb{R}$ is defined by*

$${}_a^R D_t^{\alpha} := \frac{1}{\Gamma(m-\alpha)} \frac{d^m}{dt^m} \int_a^t (t-s)^{m-\alpha-1} f(s)ds,\ t \in J,$$

provided that the right-hand side is point-wise defined.

Definition 2.3 ([6, 13]). *Let $\alpha > 0$ and m be the smallest integer greater than or equal to α. The Caputo fractional derivative of order α with lower limit 0 for a function $f : [a, \infty) \to \mathbb{R}$ is defined by*

$${}_a^C D_t^{\alpha} := {}_a^R D_t^{\alpha} \left(f(t) - \sum_{k=0}^{m-1} \frac{t^k}{k!} f^{(k)}(0) \right),$$

provided that the right-hand side is point-wise defined.

In the sequel, we notate $\mathbb{N}_a = \{a, a+1, a+2, ...\}$, where $a \in \mathbb{R}$ be given.

Definition 2.4 ([16, 17]). *Let $x : \mathbb{N}_a \to \mathbb{R}$ and $0 < \alpha \leq 1$ be given.*
(1) *The fractional sum of order v is defined by:*

$$\triangle_a^{-\alpha} := \frac{1}{\Gamma(\alpha)} \sum_{s=a}^{t-v} [t-s-1]^{\alpha-1} x(s), t \in \mathbb{N}_{a+\alpha}; \tag{2}$$

(2) *The Caputo-like delta difference is defined by:*

$${}^C \triangle_a^{\alpha} := \frac{1}{\Gamma(1-\alpha)} \sum_{s=a}^{t-v} [t-s-1]^{-\alpha} x(s), t \in \mathbb{N}_{a+1-\alpha}. \tag{3}$$

Remark 2.5. *In fact, if $\alpha = 1$ then we consider the classical logistical map by*

$$\dot{x}(t) = \mu x(t)(1-x(t)), \tag{4}$$

then, with the corresponding discrete logistic map as:

$$x_{n+1} = \mu x_n(1 - x_n), \tag{5}$$

where μ is the control parameter of discrete logistic map, and if $\mu \in (2.57, 3]$, then logistic map is reduced to a chaotic map.

However, by the Definition 2.4, Wu and Baleanu in [16, 17] presented the discrete fractional chaotical time series by

$${}^{C}\triangle_a^{\alpha} x(t) = \mu x(t + \alpha - 1)(1 - x(t + \alpha - 1)),$$

then, we easily get

$$x(n) = x(0) + \frac{\mu}{\Gamma(\alpha)} \sum_{i=1}^{n} \frac{\Gamma(n - i + \alpha)}{\Gamma(n - i + 1)} x(i - 1)(1 - x(i - 1)), t \in \mathbb{N}_{a+1-\alpha}. \tag{6}$$

The dynamics behaviors are numerically discussed for the varied parameters μ and α.

3 Image encryption algorithm

In this paper, we assume that f is a $m \times n$ (the size of gray values) plain image (P-image shorthand), where $f(i, j)$ defines the gray value of the pixel at i-th row and j-th column of the P-image. Also, let g be another key image (K-image) (or cover image) with size the same size.

We now introduce the amounts of information of an image k which size is $m \times n$, where the average gray value of k is defined by

$$avg_k = \frac{sum_k}{m \times n},$$

where sum_k is the sum of all pixel values of k, i.e.,

$$sum_k = \sum_{i=1}^{m} \sum_{j=1}^{n} k(i, j).$$

The proposed scheme is a cascade of the following steps:

Step 1: Input the parameters $\alpha_1 \in (0, 1)$, $\alpha_2 \in (0, 1)$, μ_1, μ_2, m_1 and n_1;

Step 2: Divide P-image and K-image into some small blocks and they both have $m_1 \times n_1$ blocks, where the size of each block is $m/m_1 \times n/n_1$ (m and n are divisible by m and n, respectively), thus we have:

$$P - image = \begin{bmatrix} P_1, & P_2, & \cdots, & P_{n/n_1} \\ P_{n/n_1+1}, & P_{n/n_1+2}, & \cdots, & P_{2n/n_1} \\ \vdots & & & \\ P_{(m/m_1-1)\times n/n_1+1}, & P_{(m/m_1-1)\times n/n_1+2}, & \cdots, & P_{m/m_1\times n/n_1} \end{bmatrix}$$

and

$$K - image = \begin{bmatrix} K_1, & K_2, & \cdots, & K_{n/n_1} \\ K_{n/n_1+1}, & K_{n/n_1+2}, & \cdots, & K_{2n/n_1} \\ \vdots & & & \\ K_{(m/m_1-1)\times n/n_1+1}, & K_{(m/m_1-1)\times n/n_1+2}, & \cdots, & K_{m/m_1\times n/n_1} \end{bmatrix}$$

Step 3: Calculate the average gray values of each block of P-image and K-image by

$$avg_{P-image} = \{avg_{P_1}, avg_{P_2}, \cdots, avg_{P_{m/m_1\times n/n_1}}\},$$

and

$$avg_{K-image} = \{avg_{K_1}, avg_{K_2}, \cdots, avg_{K_{m/m_1 \times n/n_1}}\},$$

Step 4: Sort the sequence $avg_{P-image}$ and $avg_{K-image}$ by increasing

$$avg'_{P-image} = \{avg'_{P_1}, avg'_{P_2}, \cdots, avg'_{P_{m/m_1 \times n/n_1}}\},$$

and

$$avg'_{K-image} = \{avg'_{K_1}, avg'_{K_2}, \cdots, avg'_{K_{m/m_1 \times n/n_1}}\};$$

Step 5: Change the position of the blocks of P-image and K-image, thus we get:

$$P-image' = \begin{bmatrix} P'_1, & P'_2, & \cdots, & P'_{n/n_1} \\ P'_{n/n_1+1}, & P'_{n/n_1+2}, & \cdots, & P'_{2n/n_1} \\ \vdots & & & \\ P'_{(m/m_1-1)\times n/n_1+1}, & P'_{(m/m_1-1)\times n/n_1+2}, & \cdots, & P'_{m/m_1 \times n/n_1} \end{bmatrix}$$

and

$$K-image' = \begin{bmatrix} K'_1, & K'_2, & \cdots, & K'_{n/n_1} \\ K'_{n/n_1+1}, & K'_{n/n_1+2}, & \cdots, & K'_{2n/n_1} \\ \vdots & & & \\ K'_{(m/m_1-1)\times n/n_1+1}, & K'_{(m/m_1-1)\times n/n_1+2}, & \cdots, & K'_{m/m_1 \times n/n_1} \end{bmatrix}$$

Step 6: Get the average gray values $avg_{P-image}$ of P-image and denote $c_1^{(1)} = avg_{P-image} - floor(avg_{P-image})$. By the E.q. (1), we calculate the chaotic sequence

$$c^{(1)} := \{c_1^{(1)}, c_n^{(1)}, \cdots, c_{m\times n}^{(1)}\}.$$

Step 7: Retain only the integer part of $c_i^{(1)} \times 10^4$ as $\hat{c}_i^{(1)}$ for each $i \in \{1, 2, \cdots, m \times n\}$. Then, consider the modular arithmetic mod between 256 and $\hat{c}_i^{(1)}$. Denote the results as

$$\tilde{c}_i^{(1)} = mod(\hat{c}_i^{(1)}, 256), i = 1, 2, ..., m \times n;$$

Step 8: Change one-dimensional array $\tilde{c}^{(1)}$ into two-dimension matrix $G_{P-image}$ of the m rows and n columns.

$$G_{P-image} = \text{reshape}(\tilde{c}^{(1)}, m, n);$$

Step 9: Apply the Xor operation $\oplus$ between $K-image(i, j)$ and $G(i, j)$ leading to the encryption result

$$h_{K-image}(i, j) = K-image(i, j)' \oplus G(i, j), i = 1, 2, ..., m, j = 1, 2, ..., n;$$

Step 10: Apply $h_{K-image}$ instead of P-image and P-image instead of K-image. Also, apply the same processes in Steps 6–8 to generate the encryption image $h_{P-image}$ of P-image.

The decryption algorithm is similar to the encryption.

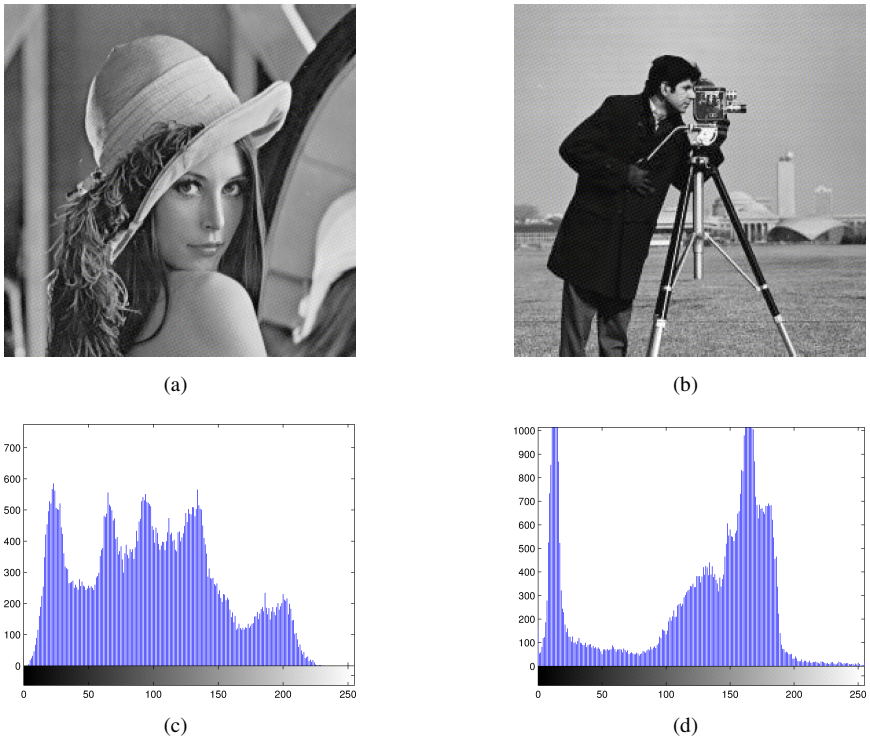
4 Experimental results and statistical analysis

In this section, some simulation results of double image multi-encryption algorithm are demonstrated. All the work is being done by software Matlab 2012(b) in a DELL Ins14VD-586. Computational platform is Microsoft Windows 7 (64 bit) with intel(R) Core(TM) I5-2450M, CPU 2.50GHz, and memory 2.0 GB.

4.1 Experimental results

We choose gray-scale "Lena" (Fig. 1 (a)) sized 256×256 as the P-image, "Cameraman" (Fig. 1 (b)) sized 256×256 as K-image. Fig. 1 (c) and Fig 1 (d) are corresponding histograms of "Lena" and "Cameraman".

Fig. 1. Lena and Cameraman.



We input the parameters $m_1 = 4, n_1 = 4, \alpha_1 = 0.6$, and $\alpha = 0.7$. Firstly, P-image and K-image are divided into blocks of 2×2. Then, we calculate the average gray values each block

$$avg_{P-imgae} = \{avg_1 = 94.9156, avg_2 = 114.3188, avg_3 = 70.9384, avg_4 = 114.5331\},$$
$$avg_{K-imgae} = \{avg_1 = 119.9196, avg_2 = 153.7616, avg_3 = 75.7767, avg_4 = 125.4131\},$$

and get the Fig. 2 by sorting them as

$$avg'_{P-imgae} = \{avg_3 = 70.9384, avg_1 = 94.9156, avg_2 = 114.3188, avg_4 = 114.5331\},$$
$$avg'_{K-imgae} = \{avg_3 = 75.7767, avg_1 = 119.9196, avg_4 = 125.4131, avg_2 = 153.7616\},$$

Next, by the parameters we obtain the chaotical sequence $c^{(1)}$ by the E.q. (1)

$$c^{(1)} := \{c_1^{(1)}, c_n^{(1)}, \cdots, c_{m\times n}^{(1)}\}.$$

we also have

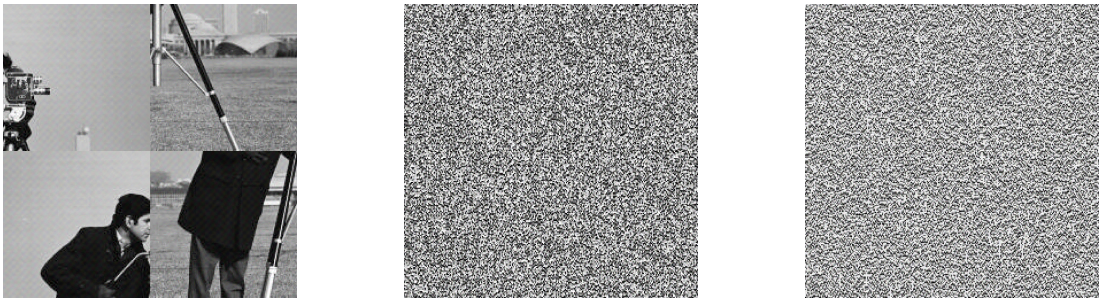
$$\tilde{c}_i^{(1)} = mod(\hat{c}_i^{(1)}, 256), i = 1, 2, ..., m \times n.$$

Hence, we change the size of $\tilde{c}^{(1)}$ into $m \times n$ and get the Fig. 3 (b). Moreover, we combine the K-image' and G to get $h_{K-image}$ which is shown in Fig. 3 (c). Finally, we directly utilize Step 9 to obtain Fig. 4. In the meantime, the hist diagrams of Lena and its encryption are obtained in Fig. 5.

Fig. 2. The results of Step 5.

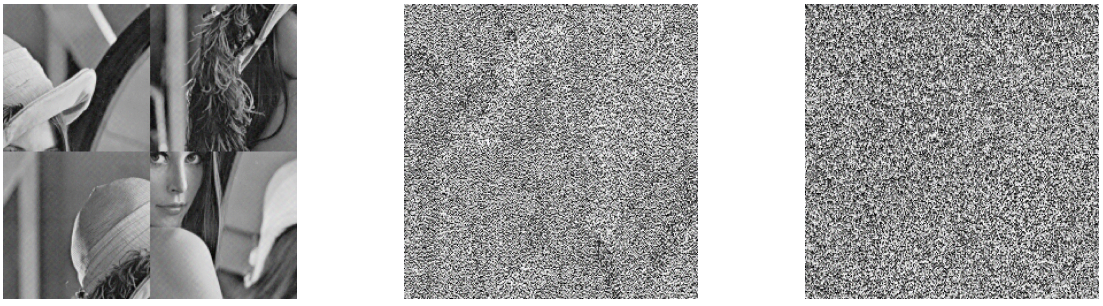
(a) Lena (b) Cameraman

Fig. 3. The results of Step 7 and Step 8.



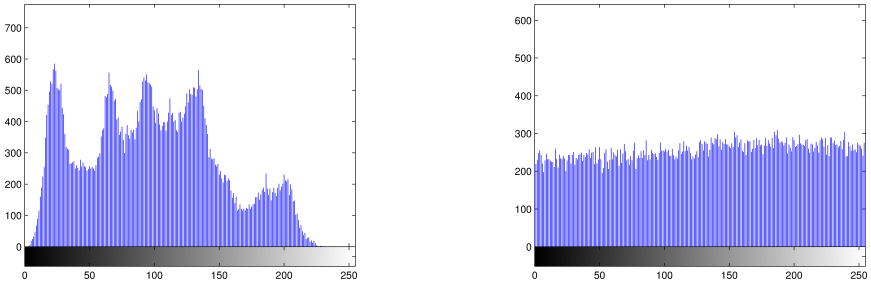
(a) (b) (c)

Fig. 4. The results of Step 9.



(a) (b) (c)

Fig. 5. The corresponding histograms of Fig. 4 (a) and (c).



(a) (b)

4.2 Statistical analysis

In order to determine whether the encryption is successful, we now apply the correlation between the two vertically and horizontally adjacent pixels in the plain image and its encrypted images, and receive the following:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x(i), \tag{7}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x(i) - E(x))^2, \tag{8}$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N} [x(i) - E(x)] \cdot [y(i) - E(y)], \tag{9}$$

$$r(x, y) = \frac{cov(x, y)}{\sqrt{D(x) \cdot D(y)}}, \tag{10}$$

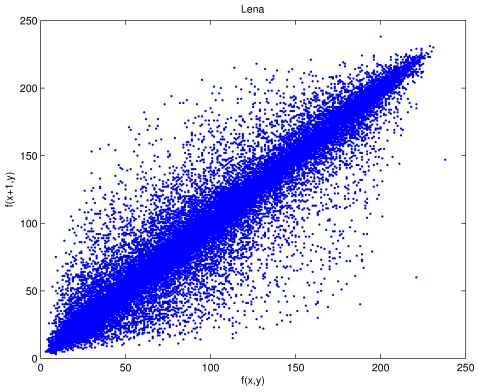
where x, y are the values of two adjacent pixels in the image, and N is the total number of pixels. In fact, we have formulas (7)-(10) that the statistical variables of P-image are obtained as follows:

$$\begin{aligned} E_{P-image}(x) &= 98.6765, \\ D_{P-image}(x) &= 119.4442, \\ r_{P-image}(x+1, y) &= 0.96934, \\ r_{P-image}(x, y+1) &= 0.93998. \end{aligned}$$

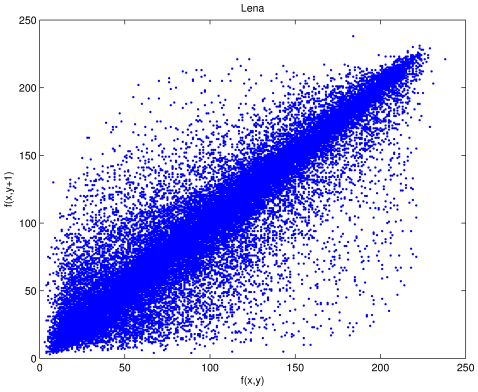
On the other hand, Fig. 6 illustrates the horizontal and vertical correlations of P-image. In fact, by the correlation coefficients $r_{P-image}(x+1, y) = 0.96934$, $r_{P-image}(x, y+1) = 0.93998$ (they almost approximate to 1) and the Fig. 6, we easily see that for the P-image the relationship between horizontal and vertical directions is almost linear. However, for the encryption image we also have

$$\begin{aligned} E_{E-image}(x) &= 2.4359, \\ D_{E-image}(x) &= 127.5431, \\ r_{E-image}(x+1, y) &= 0.00094021, \\ r_{E-image}(x, y+1) &= -0.00103427. \end{aligned}$$

Fig. 6. The horizontal (a) and (b) vertical correlations of the P-image (lena).



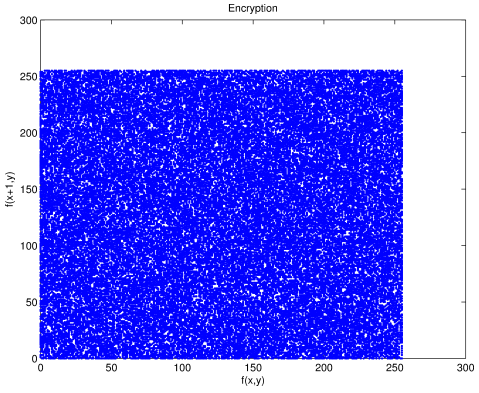
(a)



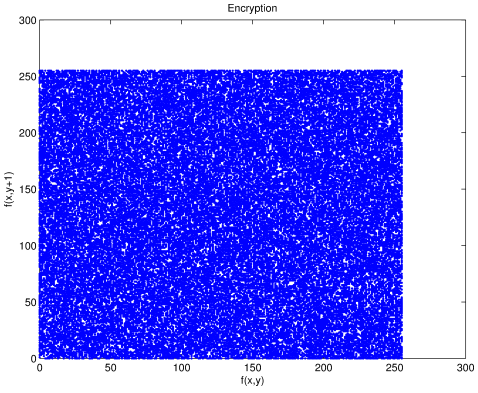
(b)

It is of course from the mean gray values $E(x)$ and covariance values that the encryption results are stable and safe. Moreover, combining the Fig. 7, we demonstrate that the correlation coefficients of encryption image are in stochastic relationship (less than 0.001). Therefore, we can conclude that the encryption is successful and exhibits promising result.

Fig. 7. The horizontal (a) and (b) vertical correlations of the encryption image.



(a)



(b)

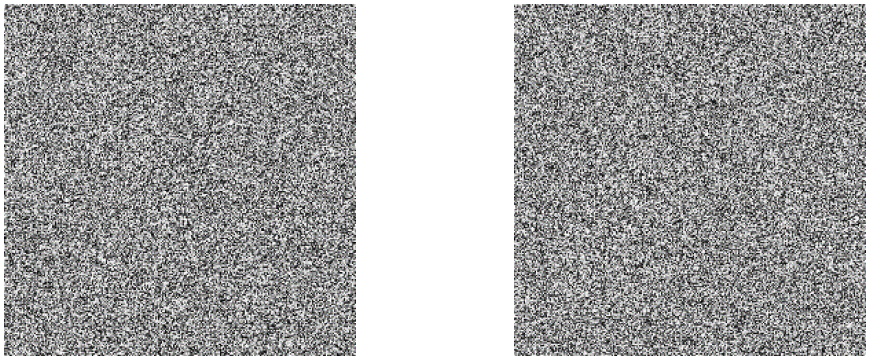
In the end, we further evaluate the effect of encryption image by two exponents of the peak signal to noise rate (PSNR) and the structural similarity (SSIM), which are most often used in the effect analysis of quality of images and image encryption algorithm. In fact, we calculate $PSNR = 8.7247$ and $SSIM = 0.00683$, thus our algorithm is quite efficient.

4.3 Key Secure Analysis

Key sensitivity is an essential property for the encryption algorithm. A good encryption algorithm should be sensitive to the initial secret keys even if it has subtle change. In order to check out the sensitivity of the proposed algorithm, use one of the keys that is only slightly different form the original one. We try to decrypt Fig. 4 (c). The resulting images, obtained by using key chains $key_{error} = key + 10^{-16}$ and and $key_{error} = key + 10^{-16}$, are in

Fig. 8. These images with slightly changed key are not visible, so that we can conclude that the proposed encryption algorithm provides a high key sensitivity.

Fig. 8. Image decryption with incorrect keys.



(a) $key_{error} = key + 10^{-16}$ (b) $key_{error} = key - 10^{-16}$

References

[1] M.S. Baptista, Cryptography with chaos. Physics Letters A, 1998; 240: 50–54.

[2] H.K.C. Chang, J.L. Liu, A linear quadtree compression scheme for image encryption. Signal Process Image Commun. 1997; 10: 279–90.

[3] C.C. Chang, M.S. Hwang, T.S. Chen, A new encryption alogorithm for image cryptosystems. J. Syst. Softw. 2001; 58: 83-91.

[4] J. Daemen, B. Sand, V. Rijmen, The Design of Rijndael: AES–The Advanced Encryption Standard. Springer-Verlag, Berlin, 2002.

[5] X.L. Huang, Image encryption algorithm using chaotic chebyshev generator. Nonlinear. Dyn. 2012; 64: 2411–2417.

[6] A.A. Kilbas, H.M. Srivastava, J.J. Trujillo, Theory and Applications of Fractional Differential Equations. in: North-Holland Mathematics Studies, vol. 204, Elsevier Science B.V, Amsterdam, 2006.

[7] L. Kocarev, Chaos-based cryptography: a brief overview. IEEE Circ. Syst. Mag. 2001; 1: 6–21.

[8] S. Lian, J. Sun, Z. Wang, A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons and Fractals, 2005; 26: 117–29.

[9] A.N. Pisarchik, M. Zanin, Image encryption with chaotically coupled chaotic maps. Physica D, 2008; 237: 2638–2648.

[10] R. Rhouma, S. Meherzi, S. Belghith, OCML-based colour image encryption. Chaos, Solitons and Fractals, 2009; 40: 309–318.

[11] J. Scharinger, Fast encryption of image data using chaotic Kolmogorov flows. J Electron Imaging, 1998; 7: 318–25.

[12] B. Schneier, Applied Cryptography–Protocols, Algorithms, and Source Code. second ed., C. John Wiley and Sons, Inc., New York, 1996.

[13] V.V. Uchaikin, Fractional Derivatives for Physicists and Engineers. Springer, New York, 2012.

[14] X.Y. Wang, C.H. Yu, Cryptanalysis and improvement on a cryptosystem based on a chaotic map. Computers and Mathematics with Applications, 2009; 57: 476–482.

[15] J. Wei, X. Liao, K.W. Wong, T. Zhou, Cryptanalysis of a cryptosystem using multiple one-dimensional chaotic maps. Commun Nonlinear Sci Numer Simul. 2007; 12: 814–22.

[16] C.G. Li, G.R. Chen, Chaos and hyperchaos in the fractional-order Rossler equations. Physica A-Statistical Mechanics and Its Applications, 2004; 341: 55–61.

[17] C.G. Li, G.R. Chen, Chaos in the fractional order Chen system and its control. Chaos Solitons Fractals, 2004; 22: 549–554.

[18] Y. Zhou, F. Jiao, Existence of mild solutions for fractional neutral evolution equations. Comput. Math. Appl. 2010; 59: 1063–1077.

[19] Y. Zhou, F. Jiao, Nonlocal Cauchy problem for fractional evolution equations. Nonlinear Anal. 2010; 11: 4465–4475.