Entropy **2015**, *17*, 28-38; doi:10.3390/e17010028

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

A Color Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System

Xia Huang [1,*], Tiantian Sun [1], Yuxia Li [1] and Jinling Liang [2,3]

[1] College of Electrical Engineering and Automation, Shandong University of Science and Technology, Qingdao 266590, China; E-Mails: yuchen38@163.com (T.S.); yuxiali2004@126.com (Y.L.)

[2] Department of Mathematics, Southeast University, Nanjing 210096, China; E-Mail: jinlliang@seu.edu.cn

[3] CSN Research Group, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia

* Author to whom correspondence should be addressed; E-Mail: huangxia_qd@126.com; Tel.: +86-13969832984; Fax: +86-0532-86057153.

Academic Editors: Guanrong Chen, C. K. Michael Tse, Mustak E. Yalcin, Hai Yu and Mattia Frasca

Received: 24 October 2014 / Accepted: 13 December 2014 / Published: 23 December 2014

Abstract: In this paper, a new color image encryption algorithm based on a fractional-order hyperchaotic system is proposed. Firstly, four chaotic sequences are generated by a fractional-order hyperchaotic system. The parameters of such a system, together with the initial value, are regarded as the secret keys and the plain image is encrypted by performing the XOR and shuffling operations simultaneously. The proposed encryption scheme is described in detail with security analyses, including correlation analysis, histogram analysis, differential attacks, and key sensitivity analysis. Experimental results show that the proposed encryption scheme has big key space, and high sensitivity to keys properties, and resists statistical analysis and differential attacks, so it has high security and is suitable for color image encryption.

Keywords: color image encryption; fractional-order; hyperchaotic system

1. Introduction

With the rapid development of the Internet and multimedia technology, multimedia communication has become an important issue. According to the statistics of the US National Security Agency, image information accounts for over 70% of the total information, and it is the principal means of information exchange between people, therefore, the security and confidentiality of image information are becoming increasingly important, and image encryption has become a research hotspot in the field of information security. Each pixel of an original color image is composed of three basic colors—R, G, and B. Compared with gray images, color images provide more information and attract more attention.

Chaos arises from deterministic nonlinear systems. As is well known, chaotic systems possess several intrinsic characteristics, such as extreme sensitivity to initial conditions, broadband power spectrum, and random-like behaviors. Owing to the abovementioned characteristics, chaos has been applied to a variety of disciplines and the most promising application of chaos is in secure communication. In recent years, a number of scholars have proposed several image encryption methods based on chaotic systems [1–6].

However, as the authors in [7,8] pointed out, low-dimensional chaotic sequences have many problems, for example, the password cycle is short and low accuracy, and therefore, the security of the image encryption algorithm is difficult to guarantee. A hyperchaotic attractor can show richer dynamic phenomena, and the randomness is higher compared with the chaotic attractor. Therefore, encryption algorithms based on hyperchaotic systems have become a research focus in recent years [9–15] On the other hand, fractional chaotic systems have potential applications in chaotic secure communication. Compared with integer-order chaotic systems, fractional chaotic systems show higher nonlinearity and more degrees of freedom in the models due to the existence of fractional derivatives. Thus, a fractional chaotic system has a bigger key space and an encrypted system using a fractional-order chaotic attractor is more difficult to copy [6,16].

A neural network system is substantially a nonlinear dynamical system that possesses complex chaotic characteristics. Moreover, the fractional-order hyperchaotic neural network system has the advantages of complex structure, large secret key space, *etc.* [17]. Motivated by the abovementioned reasons, a new color image encryption algorithm on the basis of a fractional-order hyperchaotic neural network system is proposed in this paper. In the traditional image encryption methods, the image cannot fully diffuse among the keys, however, the newly-proposed encryption algorithm can overcome this shortcoming. The algorithm can effectively resist statistical attacks, brute force attacks and possesses higher security.

This paper is organized as follows: in Section 2, the fractional-order hyperchaotic neural network system is introduced. A new color image encryption algorithm is developed in Section 3. The experimental results, analysis, and comparison are presented in Section 4. Finally, Section 5 concludes the paper.

2. Hyperchaotic System

The model of a fractional-order four-cell neural network system is described by [17]:

$$\begin{cases} D_t^\alpha x(t) = -z - w, \\ D_t^\alpha y(t) = 2y + z, \\ D_t^\alpha z(t) = 14x - 14y, \\ D_t^\alpha w(t) = 100(x - g(w)), \end{cases} \tag{1}$$

where $g(w) = w - (|w - 0.4| - |w - 0.8| - |w + 0.4| + |w + 0.8|)$, $D_t^\alpha x_i(t)$ represents the fractional derivative which is defined by Caputo definition [18–20] and α represents the derivative order. The numerical method used for solving system (1) is described in [21].

The initial value is set as $(0.1, 0.1, -0.1, 0.1)^T$. When $\alpha = 0.97$, the Lyapunov exponent of system (1) can be calculated as $LE_1 = 0.2187$, $LE_2 = 0.0828$, $LE_3 = 0$, $LE_1 = -85.2329$. The two positive Lyapunov exponents show that system (1) is hyperchaotic, and the hyperchaotic attractors are shown in Figure 1.

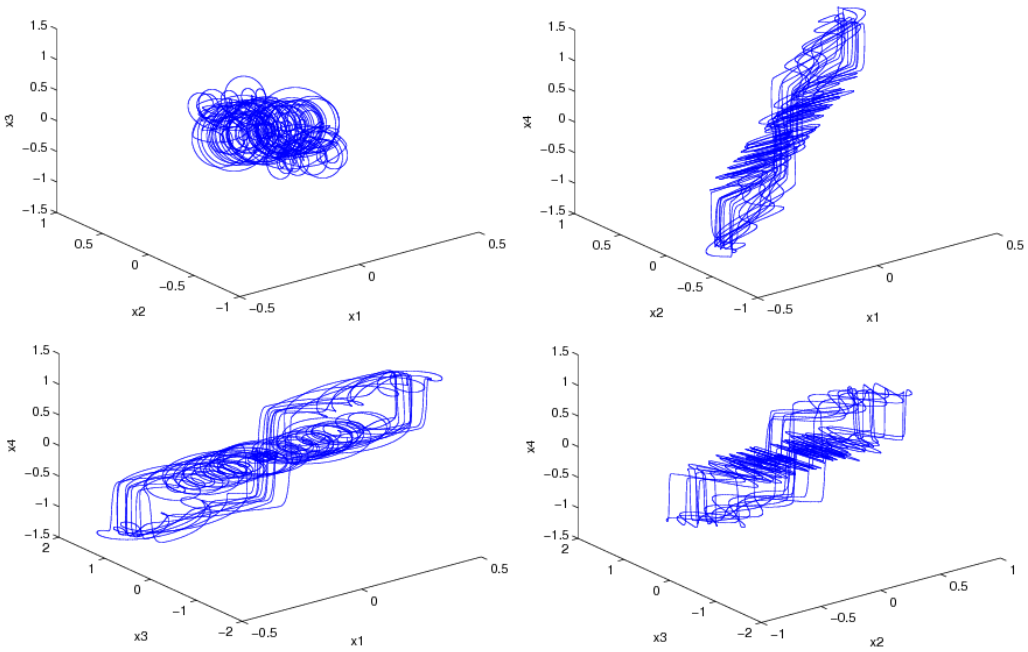

Figure 1. Phase portraits of system (1) when $\alpha = 0.97$.

3. Encryption Algorithm

In this paper, the plain image is the color image which is $256 \times 256 \times 3$, denoted by E. The color image is composed of three primary colors R, G, B, which are expressed by the three monochromatic images, denoted by E_R, E_G, E_B, and $E_R = E(:,:,1)$, $E_G = E(:,:,2)$, $E_B = E(:,:,3)$. The encryption process can be described by the following step-by-step procedure:

***Step 1*:** Produce four chaotic sequences $\{x_n\}, \{y_n\}, \{z_n\}, \{w_n\}$ with the hyperchaotic system (1), where $n = 1, 2, 3, \cdots, M \times N$, $M \times N$ represents the numbers of pixels to be encrypted. Update $\{w_n\}$ by:

$$w_i = 10^{10} \times w_i - Round\left(w_i \times 10^{10}\right) \tag{2}$$

where the function $Round(\cdot)$ is to rounded to the nearest integer.

***Step 2*:** Expand E_R, E_G, E_B to one-dimensional row vectors ER, EG, EB with length $M \times N$. Let $selE=\left(\left|x_i\right|\times 10^{14}\right) \bmod 6$, $selLen=\left(\left|z_i\right|\times 10^{14}\right) \bmod 3$. Local scrambling rules depend on the values of $selE(i)$. For example, if $selE(i)=3$, the pixel value beginning from pos with *length* in ER is replaced by the corresponding value in EB. Similarly, the pixel value beginning from *pos* with *length* in EG is replaced by the corresponding value in ER; the pixel value beginning from pos with *length* in EB is replaced by the corresponding value in EG. The replacement rules are shown in Table 1, where R, G, B represent the diagram layers of the color components of the plain image.

Table 1. The local scrambling replacement rules.

$selE(i)=0$	$R \to R, G \to G, B \to B$	$selE(i)=3$	$R \to B, G \to R, B \to G$
$selE(i)=1$	$R \to R, G \to B, B \to G$	$selE(i)=4$	$R \to G, G \to B, B \to R$
$selE(i)=2$	$R \to G, G \to R, B \to B$	$selE(i)=5$	$R \to B, G \to G, B \to R$

According to the above rules, the length of next local scrambling ($1 \le length \le 64$) is determined by the value of $selLen(i)$ as follows:

$$length=\left(sum\left(ER\left(pos:pos+length-1\right)\right) \bmod 64\right)+1, \text{ if } selLen(i)=0;$$

$$length=\left(sum\left(EG\left(pos:pos+length-1\right)\right) \bmod 64\right)+1, \text{ if } selLen(i)=1;$$

$$length=\left(sum\left(EB\left(pos:pos+length-1\right)\right) \bmod 64\right)+1, \text{ if } selLen(i)=2.$$

***Step 3*:** Continue to step 4 if $pos+length-1 \le M \times N$, otherwise, execute step 6.

***Step 4*:** Sort the $M \times N$ values of chaotic sequences $\{y_n\}$ in descending order. Use IY to denote the positional index of the corresponding elements in the original chaotic sequence. Chaotic sequences $\{z_n\}, \{w_n\}$ can be handled in the same way, and we use IZ, IW to record the positional index in the original chaotic sequences. Rearrange the elements of ER, EG, EB, by using IY, IZ, IW. Namely, $ER(j) = ER(IY(j))$, $EG(j) = EG(IZ(j))$, $EB(j) = EB(IW(j))$, where j = 1, 2, 3,…, $M \times N$. The scrambling of plain images is thus completed.

Step 5: Let $SX = round((x_i) \times 10^{14}) \bmod 256$, $SY = round((y_i) \times 10^{14}) \bmod 256$, $SZ = round((z_i) \times 10^{14}) \bmod 256$. Use SX, SY, SZ to execute diffusion transformation for pixel values after scrambling:

$$HR(k)=SX(k) \oplus \left\{\left[ER(k)+SX(k)\right] \bmod 256\right\} \oplus HR(k-1)$$

$$HG(k)=SY(k) \oplus \left\{\left[EG(k)+SY(k)\right] \bmod 256\right\} \oplus HG(k-1)$$

$$HB(k)=SZ(k) \oplus \left\{\left[EB(k)+SZ(k)\right] \bmod 256\right\} \oplus HB(k-1)$$

where $ER(k)$, $EG(k)$, $EB(k)$ are pixel values after scrambling encryption. $HR(k)$, $HG(k)$, $HB(k)$ are pixel values after diffusion transformation. $HR(k\text{-}1)$, $HG(k\text{-}1)$, $HB(k\text{-}1)$ are values after diffusion transformation of the former pixel. $CR(0)=SX(M \times N)$, $CG(0)=SY(M \times N)$, $CB(0)=SZ(M \times N)$, $k=1,2,3,\cdots,M \times N$.

***Step 6*:** Replace the three vectors HR, HG, HB with length MN into three $M \times N$ matrices HR', HG', HB', $M=cat(3,HR',HG',HB')$ and combine the three two-dimensional images into a three-dimensional image. Thus, M is the encrypted image. The decryption process is just the reverse of the encryption process, therefore, we do not describe it.

4. Experimental Analysis

In this section, we provide some experimental results to illustrate the performance of the proposed encryption algorithm. We select secret keys with the initial values $t_f = 300$, $\alpha = 0.97$, $h = 0.005$, $x_0 = [0.1, 0.1, -0.1, 0.1]^T$. According to the proposed algorithm, we encrypt the Lena image, and the plain image and the corresponding cipher image are depicted in Figure 2a,b.

Figure 2. Experimental results. (**a**) Plain image (**b**) Cipher image.

In order to show that the proposed image encryption algorithm is secure against the most common attacks, security analyses are performed, including the correlation between adjacent pixels, distribution histogram, differential attack analysis, and the sensitivity of the secret key.

4.1. Correlation of Adjacent Pixels

We choose vertical and horizontal directions of the plain image and its ciphered image, and randomly select 3000 pairs of adjacent pixels in the opposite angle direction to test the correlation between adjacent pixels before and after the encryption. The following formulas are adopted:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \,, \tag{3}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \tag{4}$$

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right), \tag{5}$$

$$\rho_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)D(y)}}. \tag{6}$$

$E(x)$ is the estimation of mathematical expectations of x, $D(x)$ is the estimation of variance of x, x and y are the values of two adjacent pixels in the image, N is the total number of pixels selected from the image. Each pixel in an ordinary image is highly correlated with its adjacent pixels either in

horizontal or vertical. An ideal encryption design should produce cipher images with no such correlation to the adjacent pixels. We compute the correlation coefficients for horizontally and vertically adjacent pixels, respectively. Figure 3 shows the correlation of the plain image and the cipher image. It can be easily found that the correlation of the initial image is an obvious linear relationship, whereas the correlation of the cipher image shows a stochastic relationship. Table 2 shows the vertical and horizontal correlation of the plain image and the cipher image. The results show that the correlation coefficients of the plain image are all close to 1. However, the correlation coefficients of the cipher image is close to 0. This indicates that the proposed encryption algorithm possesses high security against statistical attacks.

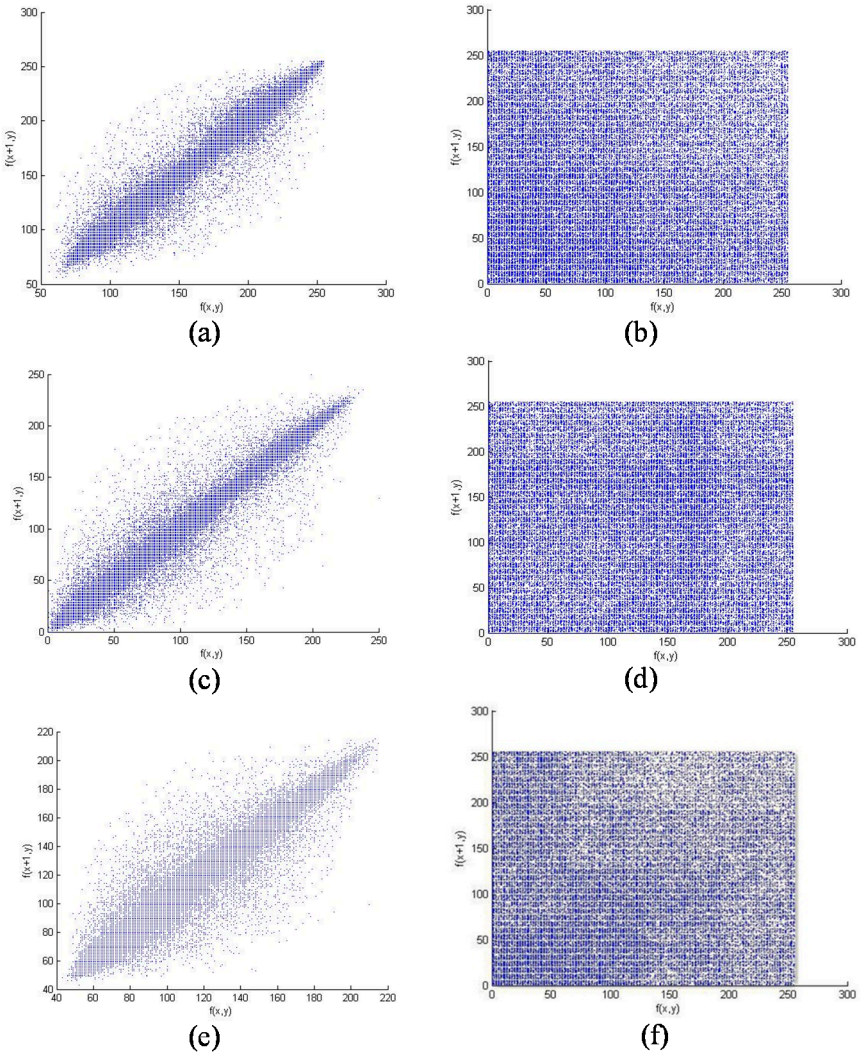

Figure 3. Horizontal and vertical correlation of the plain image and the cipher image. (**a**) horizontal correlation of the plain image (R); (**b**) horizontal correlation of the cipher image (R); (**c**) horizontal correlation of the plain image (G); (**d**) horizontal correlation of the cipher image (G); (**e**) horizontal correlation of the plain image (B); (**f**) horizontal correlation of the cipher image (B).

Table 2. Correlation coefficients of the plain image and cipher image.

Direction	Plain image			Cipher image		
	Red	**Green**	**Blue**	**Red**	**Green**	**Blue**
Horizontal	0.9420	0.9406	0.8971	0.0085	−0.0157	0.0054
Vertical	0.9669	0.9725	0.9450	0.0079	0.0002	0.0072
Diagonal	0.9185	0.9120	0.8517	0.0167	0.0081	0.0034

4.2. Histogram of the Image

The comparison of the distribution histogram before and after the encryption is as follows. From Figure 4, we can see that the histograms of the encrypted image are fairly uniform and significantly different from the histograms of the original image and hence they do not provide any clues that could be employed for any statistical analysis attack on the encrypted image.

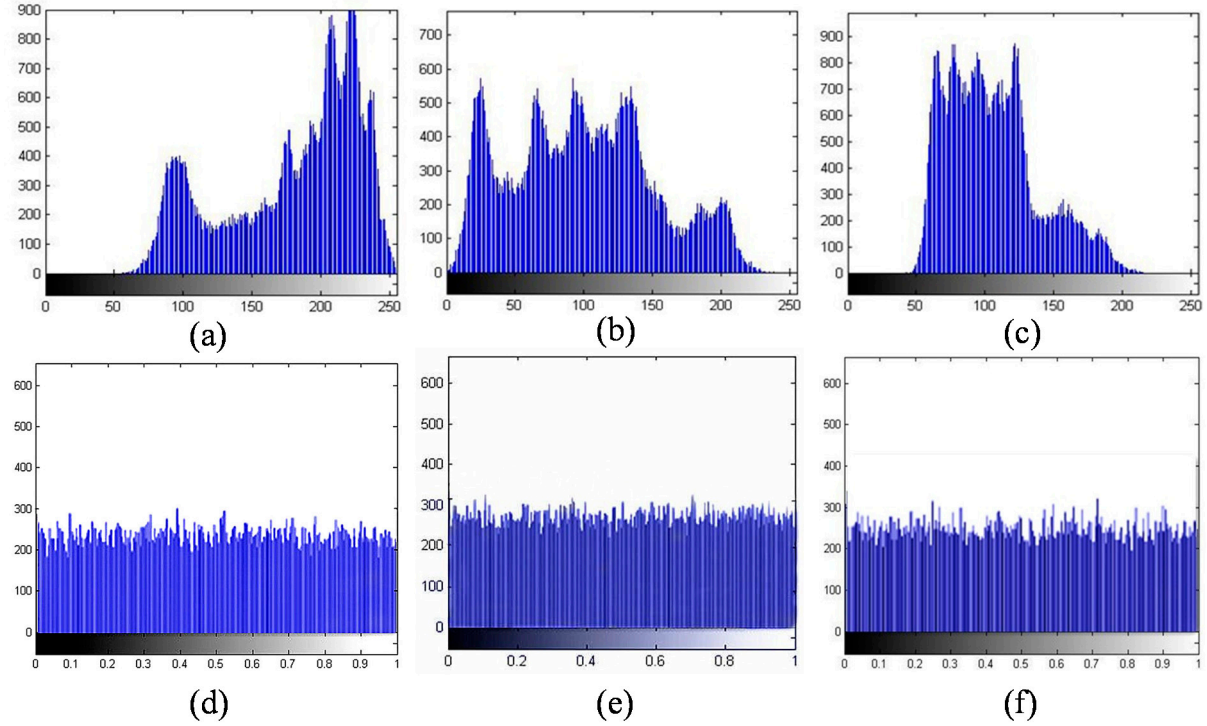

Figure 4. Histogram of the plain image and the encrypted image. (**a**)–(**c**) Histograms of the plain R, G and B images, respectively; (**d**)–(**f**) Histograms of the cipher R, G and B images, respectively.

4.3. Differential Attack Analysis

In order to obtain the correlation of the plain image and the cipher image, an attacker often makes a small alteration in the plain image to observe the change in the resulting cipher image. This attack is called the differential attack. If an encryption algorithm can guarantee that the cipher image undergoes a substantial change if the plain image undergoes a small change, then such an encryption algorithm would be good against differential attacks. Number of Pixels Change Rate (NPCR) [22] and Unified Average Changing Intensity (UACI) [23] are two common quantitative measures, which are defined as:

$$NPCR_{R,G,B}=\frac{\sum_{i,j} D_{R,G,B}(i,j)}{M\times N}\times 100\% \tag{7}$$

$$UACI_{R,G,B}=\frac{\sum_{i,j} \frac{\left|C_{R,G,B}(i,j)\text{-}C'_{R,G,B}(i,j)\right|}{255}}{M\times N}\times 100\% \tag{8}$$

where M and N mean the width and height of the image, $C_{R,G,B}(i,j)$ and $C'_{R,G,B}(i,j)$ are the initial ciphered image and the ciphered image that is changed some grey level of the pixels. Matrix $D_{R,G,B}(i,j)$ is defined as: if $C_{R,G,B}(i,j)=C'_{R,G,B}(i,j)$, then $D_{R,G,B}(i,j)=0$, otherwise, $D_{R,G,B}(i,j)=1$.

The test results of NPCR and UACI are shown in Table 3. They indicate that compared with some existing algorithms, the proposed algorithm could effectively resist plain text attacks and differential attacks.

Table 3. NPCR and UACI for different encryption algorithms.

Encryption algorithm	NPCR(%)	UACI(%)
The proposed algorithm	99.6013	33.4134
Ref. [24]	99.5207	26.7948
Ref. [25]	99.5946	33.3756
Ref. [26]	99.2173	33.4055

4.4. Key Sensitivity Analysis

A good cryptosystem should be sensitive to the secret keys. That is to say, if the attacker uses two slightly different keys to decrypt the same plain image, the two encrypted images should be completely independent of each other. We test the key sensitivity by using one of the keys, which is a little different from the original one. If we take $x_0=0.10000000001$ to decipher and $y_0=0.10000000000$, $z_0=-0.10000000000$, $w_0=0.10000000000$ remain the same.

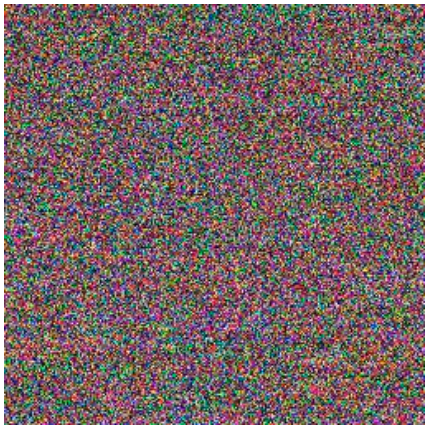

Figure 5. Wrong decryption result.

The resulting decrypted image is shown in Figure 5. Obviously, the decrypted image produced by using a slightly different key is completely different from the original one shown in Figure 2a. When the decryption operator has only 10^{-10} deviation, the decryption result has a great deviation with the original

image. The key space for this encryption algorithm is $O(10^{70})$, which is greater than that of the algorithm proposed in [6,26]. For a computer with a computation speed of 1 quadrillion operations per second, the decryption time would be $10^{54} s \approx 3.17 \times 10^{46}$ years. Therefore, large-scale exhaustive searches are useless for this kind of encryption algorithm. This suggests that the proposed algorithm has higher security.

5. Conclusions

In this paper, a novel encryption algorithm based on a fractional-order hyperchaotic system which can effectively enhance the cryptosystem security is presented. The scheme is described in detail. Security analyses, including correlation analysis, histogram analysis, and key sensitivity analysis are carried out to verify the security of the proposed encryption scheme. The experimental results demonstrate that the encryption algorithm has high security.

Acknowledgments

This research was supported by the National Natural Science Foundation of China (Grant Nos. 61473178, 61174136 and 61473177).

Author Contributions

During the development of this paper, we benefited from the suggestions and critical insights provided by Yuxia Li and Jinling Liang. Xia Huang designed the research and Tiantian Sun performed the experiment, analyzed the data and plotted the figures, and Xia Huang wrote the paper. Correspondence and requests for materials should be addressed to Xia Huang. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Boriga, R.; Dăscălescu, A.C.; Diaconu, A.V. A new one-dimensional chaotic map and its use in a novel real time image encryption scheme. *Adv. Multimed.* **2014**, *2014*, 409586.
2. Huang, C.K.; Liao, C.W.; Hsu, S.L.; Jeng, Y.C. Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. *Telecommun. Syst.* **2013**, *52*, 563–571.
3. Diaconu, A.V.; Loukhaoukha, K. An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher. *Math. Probl. Eng.* **2013**, *2013*, 848392.
4. Ghebleh, M.; Kanso, A.; Noura, H. An image encryption scheme based on irregularly decimated chaotic maps. *Signal Process Image Commun.* **2014**, *29*, 618–627.
5. El-Latif, A.A.; Li, L.; Wang, N.; Han, Q.; Niu, X. A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces. *Signal Process.* **2013**, *93*, 2986–3000.

6. Wang, Z.; Huang, X.; Li, Y.; Song, X. A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system. *Chin. Phys. B* **2013**, *22*, 010504.
7. Zhang, Y.; Huang, X.W.; Liu, J.S. New encryption scheme for color images based on 3D chaotic system. *Comput. Eng. Appl.* **2008**, *44*, 202–205. (in Chinese)
8. Tong, X.J.; Cui, M.G. Feedback image encryption algorithm with compound chaotic stream cipher based on perturbation. *Sci. China Inf. Sci.* **2010**, *53*, 191–202.
9. Boriga, R.; Dăscălescu, A.C.; Priescu, I. A new hyperchaotic map and its application in an image encryption scheme. *Signal Process. Image Commun.* **2014**, *29*, 887–901.
10. Mirzaei, O.; Yaghoobi, M.; Irani, H. A new image encryption method: parallel sub-image encryption with hyper chaos. *Nonlinear Dyn*. ***2012***, *67*, 557–566.
11. Ye, G.; Wong, K.W. An image encryption scheme based on time-delay and hyperchaotic system. *Nonlinear Dyn.* **2013**, *71*, 259–267.
12. Li, C.; Liu, Y.; Xie, T.; Chen, M.Z.Q. Breaking a novel image encryption scheme based on improved hyperchaotic sequences. *Nonlinear Dyn.* **2013**, *73*, 2083–2089.
13. Zhu, H.; Zhao, C.; Zhang, X. A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem. *Signal Process. Image Commun.* **2013**, *28*, 670–680.
14. Zhang, Y.; Xiao, D.; Shu, Y.; Li, J. A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations. *Signal Process. Image Commun.* **2013**, *28*, 292–300.
15. Cang, S.; Qi, G.; Chen, Z. A four-wing hyper-chaotic attractor and transient chaos generated from a new 4-D quadratic autonomous system. *Nonlinear Dyn.* **2012**, *59*, 515–527.
16. Wang, Z.; Huang, X.; Li, N.; Song, X. Image encryption based on a delayed fractional-order chaotic logistic system. *Chin. Phys. B* **2012**, *21*, 050506.
17. Huang, X.; Zhao, Z.; Wang, Z.; Li, Y. Chaos and hyperchaos in fractional-order cellular neural networks. *Neurocomputing* **2012**, *94*, 13–21.
18. Podlubny, I. Fractional Differential Equations: An Introduction to Fractional Derivatives, Fractional Differential Equations, to Methods of Their Solution and Some of Their Applications; Academic Press: New York, NY, USA, 1998.
19. Shen, J.; Lam, J. State feedback H_∞ control of commensurate fractional-order systems. *Int. J. Syst. Sci.* **2014**, *45*, 363–372.
20. Hilfer, R. *Applications of Fractional Calculus in Physics*; World Scientific: Danvers, MA, USA, 2001.
21. Diethelm, K.; Ford, N.J.; Freed, A.D. Detailed error analysis for a fractional Adams method. *Numer. Algorithms* **2004**, *36*, 31–52.
22. Chen, G.R.; Mao, Y.B.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals* **2004**, *21*, 749–761.
23. Rhouma, R.; Meherzi, S.; Belghith, S. OCML-based color image encryption. *Chaos Solitons Fractals* **2009**, *40*, 309–318.
24. Huang, C.K.; Nien, H.H. Multi chaotic systems based pixel shuffle for image encryption. *Opt. Commun.* **2009**, *282*, 2123–2127.
25. Liu, H.; Wang, X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt. Commun.* **2011**, *284*, 3895–3903.

26. Wei, X.; Guo, L.; Zhang, Q.; Zhang, J.; Lian, S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *J. Syst. Softw.* **2012**, *85*, 290–299.