https://doi.org/10.20965/jaciii.2019.p0805

Short Paper:

Image Encryption Algorithm Based on a Hyperchaotic System and Fractional Fourier Transform

Yang Liu

College of Information and Electronic Engineering, Hunan City University
Yiyang, Hunan 413000, China
E-mail: 58522659@qq.com

[Received June 29, 2018; accepted November 5, 2018]

An image encryption scheme that combines a hyperchaotic system with standard weighted fractional Fourier transform theory is proposed. Simulation results showed that grayscale distribution of the encrypted image was balanced, correlation coefficients of adjacent pixels were highly irrelevant, and the encrypted image was highly sensitive to the secret key, offering good robustness against attacks and a larger key space.

Keywords: hyperchaotic system, standard weighted class, fractional Fourier transform, image encryption, information security

1. Introduction

With the rapid development of network and information technology, digital images have become a means of expressing information. However, in the process of their dissemination, digital images need to be encrypted for security or for sensitive factors that cannot be directly transmitted. Therefore, digital image encryption methods have become an important research area in information security. Both mathematics and algorithm theory lie at the foundation of these methods. Compared with ordinary text information, digital images have several unique characteristics: They contain a large amount of data, there are strong correlations between pixels, and there is high redundancy. Therefore, traditional encryption methods can only be used for reference and cannot be copied. So far, research on image encryption has mainly focused on the spatial domain, the transform domain, and chaotic systems. However, simply using a certain encryption method has the disadvantages of a simple system structure, fewer parameters and variables, and a small key space. The high-dimension hyperchaotic system above has more than four invariants and two positive Lyapunov exponents. Its key space is larger, and its nonlinear system behavior is more complex, making it more suitable for digital image encryption. The standard weighted fractional Fourier transform contains both time information and frequency information. Therefore, digital image encryption using these two methods has far-ranging application value, and the improvement of computer performance provides technical support for the implementation of the algorithms.

This article, based on the hyperchaotic system method proposed in References [1–5], proposes a new image encryption method based on the combination of a hyperchaotic system and weighted fractional Fourier transform theory. The key to the method not only has chaotic parameters and initial values but also the order of the fractional Fourier transform, greatly increasing the key space and making it more difficult to decrypt the digital image. Finally, the safety of the algorithm is analyzed from several aspects, such as an image histogram, adjacent pixel correlation, and key sensitivity. The numerical results show that this method can effectively resist many kinds of attacks such as statistics, exhaustion, and difference and has good security.

2. Theoretical Basis of Double Image Encryption Method

2.1. Hyperchaotic System

The hyperchaotic system can be described as follows:

$$\begin{cases} \dfrac{dx_1}{dt} = a(x_2 - x_1), \\ \dfrac{dx_2}{dt} = bx_1 + cx_2 - x_1x_3 + x_4, \\ \dfrac{dx_3}{dt} = x_2^2 - dx_3, \\ \dfrac{dx_4}{dt} = -ex_1. \end{cases} \quad \ldots\ldots \quad (1)$$

Where a, b, c, d, and e are the system control parameters and $x = [x_1, x_2, x_3, x_4]$ represents the state quantity of the hyperchaotic system. When the control parameters are $a = 27.5$, $b = 3$, $c = 19.3$, $d = 2.9$, and $e = 3.3$, giving the initial value $x_0 = [x_1(0), x_2(0), x_3(0), x_4(0)]$ of a set of hyperchaotic states to be the original key, then model Eq. (1) has two positive Lyapunov exponents, which are in a hyperchaoticstate. Eq. (1) are iterated according to a fourth order Runge–Kutta algorithm, which produces four sets of original hyperchaotic sequences. However, this chaotic sequence is not suitable for image encryption directly, and there is no correlation with plaintext images, so it needs

optimal reformation.

2.2. Standard Weighted Fractional Fourier Transform

The standard weighted fractional Fourier transform is derived from the weighted fractional Fourier transform defined by H. Ozaktas and it mainly studied in its extended form [6–8]. It can be defined as follows:

$$F^{\alpha}\left[f(x)\right] = F^{\alpha}(m,M)\left[f(x)\right] = \sum_{l=0}^{M-1} A_l(\alpha,m) f_l(x).$$

The expressed weighting factor is

$$A_l(\alpha,m) = \frac{1}{M}\sum_{k=0}^{M-1} \exp\left\{-\frac{2\pi i}{M}\left[\alpha(k+m_k M) - kl\right]\right\},$$

where $\alpha \in \mathrm{R}$ is the order of the fractional Fourier transform and $m = (m_0, m_1, \ldots, m_{M-1}) \in z^M$ is the l-th Fourier transform of $f_l(x)$.

The weighted fractional Fourier transform satisfies the following four properties:

1. Continuity:
   For the two functions $f(x), g(x)$ in $L^2(R)$, if $\int_{-\infty}^{+\infty} \left\| f(x) - g(x) \right\|^2 dx \to 0$, then $F^{\alpha}(f(x)) \to F^{\alpha}(g(x))$.
2. Linearity:
   $$F^{\alpha}\left[af(x) + bg(x)\right] = aF^{\alpha}\left[f(x)\right] + bF^{\alpha}\left[g(x)\right].$$
3. Order additivity and exchangeability:
   $$\begin{aligned} F^{\alpha+\beta}\left[f(x)\right] &= F^{\alpha}\left[f(x)\right]F^{\beta}\left[f(x)\right] \\ &= F^{\beta}\left[f(x)\right]F^{\alpha}\left[f(x)\right] \\ &= F^{\beta+\alpha}\left[f(x)\right]. \end{aligned}$$
4. Awkwardness:
   $$F^{\alpha} \cdot \left(F^{\bar{\alpha}}\right)^H = I,$$
   where I is the identity matrix and H represents the conjugate transpose.

3. Double Image Encryption Algorithm

(1) The original image is preprocessed and is represented by P. $M \times N$ is its size, and R, G, and B represents its three primary color plane layered matrix.

(2) Two-dimensional discrete standard weighted fractional Fourier transforms for R, G, and B are performed, that is,

$$Q_1 = F^{\alpha}(R)F^{\overline{\alpha}},\ Q_2 = F^{\alpha}(G)F^{\overline{\alpha}},$$
$$Q_3 = F^{\alpha}(B)F^{\overline{\alpha}},$$

where F^{α} is a discrete real vector-weighted transformation matrix of $X \times X$.

(3) Hierarchical chaos scrambling is performed.

Let the four sets of original sequences generated by the hyperchaotic system be $\{x_j(i)\}$ $(j = 1,2,3,4;\ i = 1,2,\ldots,L/4)$, where L is the sum of the number of pixels in the image to be encrypted. To prevent chaotic iterative transient effects, the results of the previous iteration are discarded. The elements of the hyperchaotic sequence are transformed into integers in the range $[0,255]$ according to

$$x_j = \mathrm{mod}\Big(floor\big(\big(|x_j| - floor\left(|x_j|\right)\big) \times 10^{14} + S \times 10^6\big), 256\Big), \quad (2)$$

where floor represents a negative direction rounding, mod represents a spare, and S is the sum of the grayscale values of each pixel in the image to be encrypted. If S is multiplied by the number of operations (e.g., 10^5–10^6 times), the sensitivity of the original image pixel to the key can be enhanced. Combining this with the modified sequence

$$k_1 = \left\{x_1(1), \ldots, x_1\left(\frac{L}{4}\right), \ldots, x_j\left(\frac{L}{4}\right)\right\}, \quad j = 1,2,3,4, \quad (3)$$

will yield a key sequence k_1 with a length of L (grayscale replacement key sequence). Then the following binary key sequence k_2 is obtained:

$$k_2 = \begin{cases} 0, & k_1(i) > 127.5 \\ 1, & k_1(i) < 127.5 \end{cases} \quad \ldots\ldots \quad (4)$$

based on k_1 (separate scrambling key sequences).

The sequence satisfies an ideal random sequence, because it has three characteristics: Its mean is zero, its autocorrelation is the impulse function, and its cross-correlation is zero.

Q_1, Q_2, and Q_3 are then separately scrambled. The scrambling method for Q_1 is defined as follows:

A. If $k_2(i) = 0$, pixels $Q_1(i)$ are stored in the sequence p_{1r}; if $k_2(i) = 1$, pixels $Q_1(i)$ are stored in the sequence p_{2r}.

B. p_{1r} and p_{2r} are then combined and scanned in rows into matrix P_1, which is equal to the original image. If the connection point between p_{1r} and p_{2r} is L_0, which is the length of sequence p_{1r}, then L_0 can be saved as a key and then G_2 and G_3 are separately scrambled according to the above scrambling method. The resulting matrices are P_2 and P_3, because the chaotic sequence generated by the chaotic scrambling is the same, and the key L_0 is the same.

(4) The three layers are merged, and the scrambled matrices P_1, P_2, and P_3 are merged to obtain the encrypted dense map M.

The specific encryption process is represented by **Fig. 1**, and the decryption process simply reverses the above process.

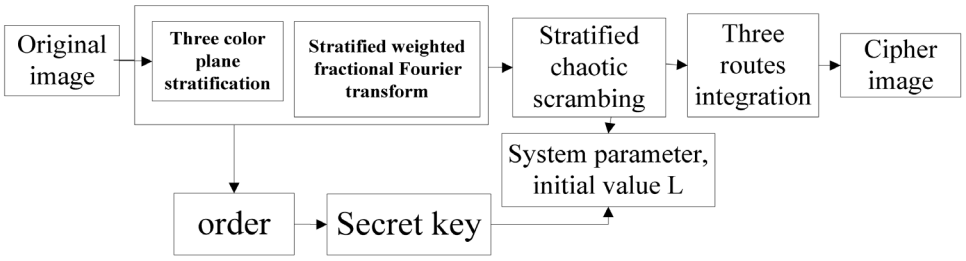


Fig. 1. Diagram of the encryption scheme.

4. Numerical Simulation and Performance Analysis

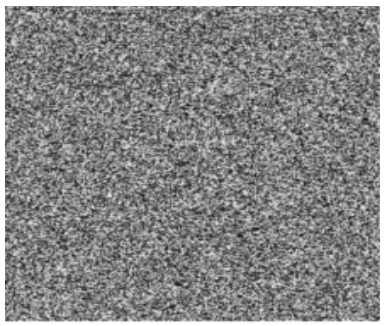
4.1. Encryption Algorithm Simulation

The original image is chosen as lena.bmp with a size of 256×256. The orders of the standard weighted fractional Fourier transforms are 0.3 and 1.3. The parameters and four initial values in the chaotic system are $a = 27.5$, $b = 3$, $c = 19.3$, $d = 2.9$, and $e = 3.3$ and $[0.5, 0.5, 0.3, 0.5]$. If $L_0 = 32887$, the simulated effect diagram is shown in **Fig. 2**.

From a visual point of view, no matter which order is selected for encryption, the encrypted image does not carry the information of the original image at all and thus has a better encryption effect.

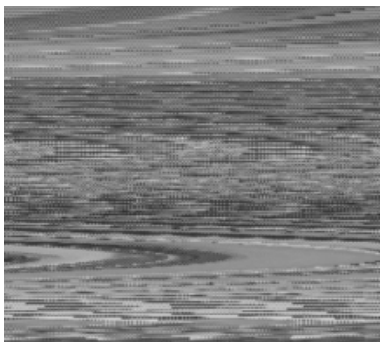
(a) Original image

An encrypted graph with a transformation order of 1.3



(b) Image with an order of 1.3

An encrypted graph with a transformation order of 0.3



(c) Image with an order of 0.3

Fig. 2. Comparison between the double encryption image and the encryption map.

4.2. Mean Square Error Analysis (Key Sensitivity Analysis)

The mean squared error (MSE) for an image with a pixel size of $N \times M$ is defined as

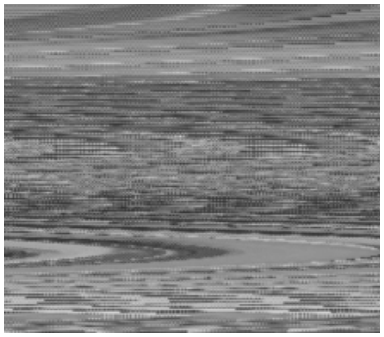
$$MSE = \|p - \omega\|^2 = \frac{1}{N \times M} \sum_{i=1}^{N} \sum_{j=1}^{M} |p(i,j) - \omega(i,j)|^2 \quad . \quad . \quad . \quad (5)$$

where p is the original image and ω is the decrypted image. Without knowing the decryption key, the size of the MSE can represent the degree of similarity between the decrypted image and the original image [9, 10]. When $MSE = 0$, the speculative decryption key is consistent with the actual decryption key. When $MSE \neq 0$, the estimated decryption key does not match the correct decryption key, and the image cannot be decrypted correctly. The larger the value of the MSE, the greater the difference between the image decrypted by the decryption key and the image before encryption. From **Figs. 3** and **4**, it can be seen that the MSE values of the decrypted image and the original image caused by small changes of the secret key are very different. It can be seen that the encrypted image is extremely sensitive to the secret key.

4.3. Analysis of Grayscale Histogram

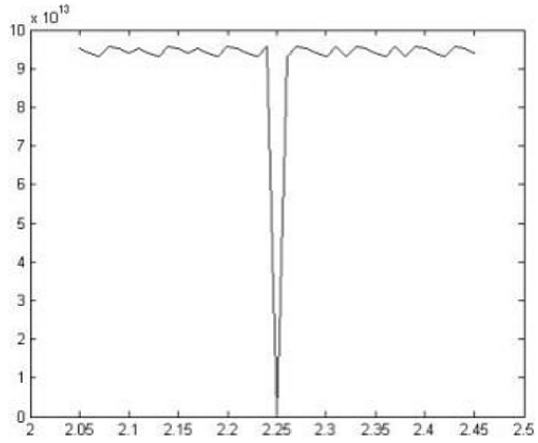
To show the probability of occurrence of each grayscale in an image, a two-dimensional grayscale histogram is constructed. The abscissa represents the gray level of the pixel in the image and the ordinate represents the probability of occurrence of each pixel in the gray level. From the histogram of the original image and the encrypted histogram in **Fig. 5**, it can be seen that the encrypted density histogram is more evenly distributed than that of the

(a) Correct decryption

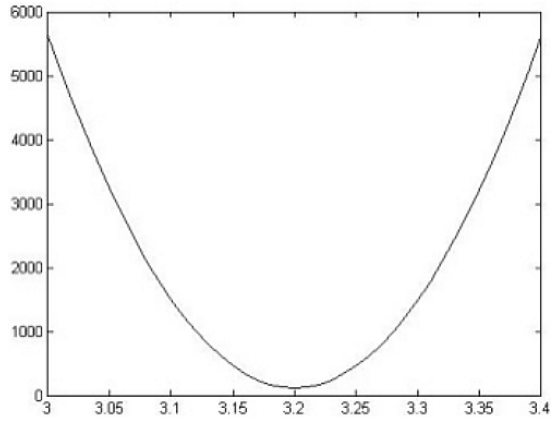


(b) Error decryption

Fig. 3. Correct decryption and error decryption of images.

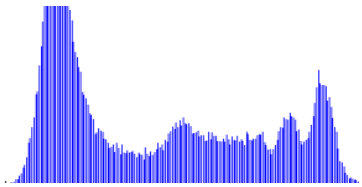


(a) Change of chaotic parameter

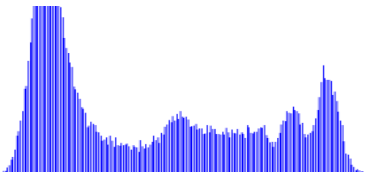


(b) Change of transformation order

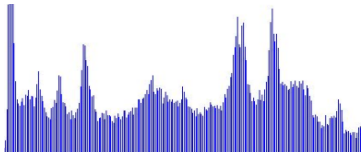
Fig. 4. MSEs for encryption scheme of a single decryption key change.



(a) Original image



(b) Image with an order of 0.3



(c) Image with an order of 1.3

Fig. 5. Comparison of the original image and the encrypted image histogram.

original image. Moreover, there is no similarity to the grayscale distribution of the original image. It is difficult to get the correct information of the original image from the encrypted grayscale histogram.

4.4. Correlation Analysis Between Adjacent Pixels

For a general digital image, correlations between adjacent pixels in the horizontal, vertical, and diagonal directions are often very large. By using this feature, the original image information can be obtained from statistical characteristics. To prevent statistical analysis attacks, the correlation between adjacent pixels of the image after encryption must be relatively low. Adjacent pixels in the horizontal direction are randomly selected from the original image and their correlation coefficients are calculated by using the following equations:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad \ldots\ldots\ldots\ldots (6)$$

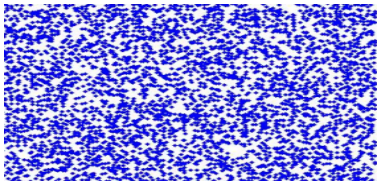
$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left[x_i - E(x)\right]^2, \quad \ldots\ldots\ldots (7)$$

$$conv(x,y) = \frac{1}{N}\sum_{i=1}^{N} \left[x_i - E(x)\right]\left[y_i - E(y)\right], \quad \ldots (8)$$

where (x_i, y_i) represents a pair of adjacent pixel gray values, N represents the number of adjacent pixel pairs for which the correlation coefficient is calculated, and two adjacent pixel correlation coefficients are represented as $r_{x,y} = conv(x,y)/(\sqrt{D(x)}\sqrt{D(y)})$. The correlation coefficients between adjacent pixels in the vertical and diago-

(a) Original image

Correlation coefficient between pixels in the original horizontal direction of original images



(b) Encrypted image

Correlation coefficient between pixels in the horizontal direction of encrypted images

Fig. 6. Correlation chart for the horizontal direction.

Table 1. Correlation analysis of adjacent pixels.

Pixel relation	Horizontal direction	Vertical direction	Diagonal direction
Original image	0.9761	0.9523	0.9394
Encrypted image	0.0649	0.0174	0.0466

nal directions can be calculated in the same manner. All adjacent pixel pairs of theoriginal image and of the encrypted image were selected for correlation analysis, and a comparison of the calculation results is shown in **Fig. 6** and listed in **Table 1**. It can be seen from the table that the correlation coefficients for the encrypted images in all directions are obviously small, being close to 0.

5. Conclusion

This work is based on using a double encryption scheme that combines a hyperchaotic system with the standard weighted fractional Fourier transform for image encryption. The original image is first stratified into three primary colors. A standard weighted fractional Fourier transform is performed on each layer, and then the four sequences of the hyperchaotic system are modified. Separation and scrambling in the three-level image fractional Fourier transform domain according to separate scrambling secret key sequences are used to reduce the correlations of the image. Finally, the three primary color planes are combined to obtain the encrypted image. In addition, simulations were performed from the three aspects of key sensitivity, histograms, and adjacent pixels in the image. The results show that the combination of the sensitivity of chaos scrambling and the robustness of the fractional Fourier transform encryption method offers stronger attack resistance, greater information security, and potential application value.

References:

[1] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," Nonlinear Dynamics, Vol.62, Issue 3, pp. 615-621, 2010.

[2] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," Signal Processing, Vol.97, pp. 172-182, 2014.

[3] X. Wang and H.-L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," Nonlinear Dynamics, Vol.83, Issue 1-2, pp. 333-346, 2016.

[4] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," Applied Soft Computing, Vol.26, pp. 10-20, 2015.

[5] X. Wang, C. Liu, D. Xu, and C. Liu, "Image encryption scheme using chaos and simulated annealing algorithm," Nonlinear Dynamics, Vol.84, Issue 3, pp. 1417-1429, 2016.

[6] M. J. Rostami, S. Saryazdi, H. Nezamabadi-pour, and A. Shahba, "Chaos-Based Image Encryption Using Sum Operation Modulo 4 and 256," IETE J. Research, Vol.62, Issue 2, pp. 179-188, 2016.

[7] H. Khanzadi, M. Eshghi, and S. E. Borujeni, "Design and FPGA Implementation of a *Pseudo* Random Bit Generator Using Chaotic Maps," IETE J. Res., Vol.59, Issue 1, pp. 63-73, 2013.

[8] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," IBM J. of Research Development, Vol.38, Issue 3, pp. 243-250, 1994.

[9] H. Williams, "A modification of the RSA public-key encryption procedure," IEEE Trans. on Information Theory, Vol.26, Issue 6, pp. 726-729, 1980.

[10] Y.-Q. Zhang and X.-Y. Wang, "Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation," Nonlinear Dynamics, Vol.77, Issue 3, pp. 687-698, 2014.

Name:
Yang Liu

Affiliation:
Lecturer, College of Information and Electronic Engineering, Hunan City University

Address:
Yiyang, Hunan 413000, China

Brief Biographical History:
2008 M.S., Central South University
2008- Lecturer, College of Information Science and Engineering, Hunan City University

Main Works:
• Cloud computing and intelligence computing. He has published 25 journal papers and about 5 conference papers.