Switched-system-based four-scroll chaotic attractor generation and its application in color image encryption

Qiang Tan and Xia Huang

College of Electrical Engineering and Automation, Shandong University of Science and Technology, Qingdao 266590, China

E-mail: huangxia@sdust.edu.cn

Abstract. In this paper, a four-scroll chaotic attractor is generated based on a switched system, and moreover, it is applied to color image encryption. First, the canonical Chen system and a modified chaotic system are used as two subsystems to construct the switched system. Meanwhile, a state-dependent switching law with a threshold is designed to regulate the switching between the two subsystems. Then, a four-scroll chaotic attractor is generated by tuning the threshold value. Last, the chaotic sequence extracted from the switched chaotic system is applied to image encryption. The experimental results show that the encryption performance of this switched chaotic system is better than that of a single Chen system.

1. Introduction

With the rapid development of the Internet and multimedia technology, image encryption has become an important issue in the field of information security and attracted much attention. In the past decade, chaotic systems are widely used in the fields of image encryption [1]. Because color image has the characteristics such as large amount of data and the strong correlation of adjacent pixels, the traditional image encryption techniques cannot satisfy the requirement of the real-time image encryption. As is well known, chaotic systems possess several inherent characteristics, e.g., extreme sensitivity to initial conditions, broadband power spectrum, and random-like behavior. These outstanding features are beneficial to information security and it has attracted the attention of cryptographers to develop varieties of encryption algorithms based on chaotic systems [2].

In 1989, Matthews proposed a chaotic flow cipher scheme based on Logistic deformation mapping for the first time [3]. A new optical color image encryption technique was proposed by using spiral phase transform and chaotic pixel scrambling [4]. An image encryption algorithm was presented based on the memristive chaotic system and compressive sensing [5]. Though the image scrambling algorithm is simple, efficient and easy to implement, it can be seen that the scrambling based image encryption algorithm does not essentially change the content of the image pixel, it only rearranges the positions of each pixel, so once the set of image pixels is fixed, the permutation and combination of image pixels will be fixed. The security of the scrambling algorithm seems to be unreliable, especially when the size of the image is relatively small [6, 7]. Thus, an algorithm that could radically alter the image is very important.

On the other hand, the generation of multi-scroll chaotic attractors is of great significance. Multi-scroll chaotic attractors possess more complicated topological structure and have broad application prospects in the field of communication security. Methods of generating multi-scroll attractors can be summarized as follows: (1) non-smooth functions, such as piecewise-linear function [8], switching...
function [9], and stair function [10]; (2) smooth functions, such as sine function [11]. In a word, the basic technique of generating multi-scroll attractors is either increasing the number of equilibrium points, or realizing the equilibrium jumping. Besides, the number of scrolls equals the number of equilibrium points.

As a kind of important hybrid dynamical system, switched systems possess complex nonlinear dynamical behaviors due to the switching characteristics. In this paper, a new switched chaotic system is proposed by combining two subsystems together with a switching law to generate a four-scroll chaotic attractor by changing the threshold. Compared with the traditional high-dimensional chaotic system, the switched-system-based chaos attractor generation does not need to expand the dimension of the chaotic system. Moreover, the switched chaotic system has better randomness, which makes the encryption have larger key space and improves the security of encryption.

The contributions of this paper are: Firstly, a switched chaotic system is constructed based on the canonical Chen system and its derivative system. Then, the chaotic dynamics of the switched system is verified by Lyapunov exponent spectrum, bifurcation diagram, and Poincare section. Secondly, the color image encryption is realized based on the proposed switched chaotic system. Finally, the detailed security analysis, including key space analysis, statistical analysis and sensitivity analysis are carried out. It is shown that the encryption performance of the proposed switched chaotic system is better than that of the single Chen system.

2. The switched system
As is well known, the canonical Chen system can be described as:

$$\begin{align*}
\dot{x} &= a(y - x) \\
\dot{y} &= (c - a)x + cy - xz \\
\dot{z} &= xy - bz
\end{align*}$$

(1)

where \(a, b\) and \(c\) are real parameters.

When \(a = 39, b = 2\) and \(c = 26\), system (1) is chaotic and the chaotic attractor of system (1) is shown in Figure 1. In this paper, system (1) is taken as the subsystem A. The equilibrium points and the corresponding eigenvalues of system (1) are listed in Table 1.

When taking \(a = 50, b = 10, c = 35\), we can obtain a modified chaotic system based on system (1), and the chaotic attractor is displayed in Figure 2. In this paper, the modified chaotic system is taken as the subsystem B. The equilibrium points and the corresponding eigenvalues of subsystem B are listed in Table 2.

In this paper, we propose a 3-D switched system based on the Chen system (1) and its derivative chaotic system described as:

$$\begin{align*}
\dot{x} &= a(x)(y - x) \\
\dot{y} &= (c(x) - a(x))x + c(x)y - xz \\
\dot{z} &= xy - b(x)z
\end{align*}$$

(2)

where

$$a(x) = \begin{cases} 
39, & |x| < T \\
50, & |x| > T
\end{cases},
b(x) = \begin{cases} 
2, & |x| < T \\
10, & |x| > T
\end{cases},
c(x) = \begin{cases} 
26, & |x| < T \\
35, & |x| > T
\end{cases}$$

\(a(x), b(x)\) and \(c(x)\) are state-dependent parameters and \(T\) is the threshold. In other word, the parameter will switch from one value to the other if the state \(x\) reaches the threshold.

### Table 1. Equilibrium points and eigenvalues of system (1) with \(a = 39, b = 2, c = 26\)

| Equilibrium | Eigenvalue | Index |
|-------------|------------|-------|
| \(S_0(0,0,0)\) | \(\lambda_1 = -29.94, \lambda_2 = 16.94, \lambda_3 = -2\) | 1 |
| \(S_1(5.10,5.10,13)\) | \(\lambda_1 = 5.81 \pm 4.40j, \lambda_2 = -26.62\) | 2 |
| \(S_2(-5.10,-5.10,13)\) | \(\lambda_1 = 5.81 \pm 4.40j, \lambda_2 = -26.62\) | 2 |
Table 2. Equilibrium points and eigenvalues of system (1) with \( a = 50, b = 10, c = 35 \).

| Equilibrium       | Eigenvalue          | Index |
|-------------------|---------------------|-------|
| \( S_0(0,0,0) \)  | \( \lambda_1 = -40, \lambda_2 = 25, \lambda_3 = -10 \) | 1     |
| \( S_1(14.14,14.14,20) \) | \( \lambda_1 = 3.93 \pm 24.35 \, j, \lambda_2 = -32.86 \) | 2     |
| \( S_2(-14.14,-14.14,20) \) | \( \lambda_1 = 3.93 \pm 24.35 \, j, \lambda_2 = -32.86 \) | 2     |

Figure 1. The chaotic attractor of system (1).

Figure 2. The chaotic attractor of the modified system.

Figure 3. Lyapunov exponent spectrum.
3. Dynamical analysis of the switched system

3.1. Bifurcation analysis
In this section, we analyze the bifurcation dynamics of system (2). The Lyapunov exponent spectrum is shown in Figure 3 and the bifurcation diagram is shown in Figure 4. Therein, $T$ varies from 0 to 20 with step size 0.001. We can see that the bifurcation diagram is coincident with the Lyapunov exponent spectrum. It can be seen from the Lyapunov exponent spectrum and bifurcation diagram that the switched system (2) has complex bifurcation dynamics compared with the single system. Hence, system (2) has high potential application in the field of information security.

![Figure 4. Bifurcation diagram.](image)

3.2. Four-scroll chaotic attractor
In switched system (2), take the threshold value $T=8$. By calculation, system (2) has five equilibrium points, namely $(0,0,0)$, $(\pm 14.14, \pm 14.14, 20)$ and $(\pm 5.10, \pm 5.10, 13)$. It can be seen that the number of the equilibrium points is increased, which provides the possibility for the appearance of multi-scroll chaotic attractors. Take the initial value as $[0.1, 0.1, 0.1]^T$ and the step size as 0.001. The phase portrait of switched system (2) in x-z plane is displayed in Figure 5. When $T=8$, the Poincaré section is shown in Figure 6, in which the section is taken as $z = 15$. We can see that system (2) generates a four-scroll chaotic attractor. It has more complicated topological structure that is not found in the single chaotic system.

![Figure 5. Phase portrait of system (2) with $T=8$.](image)
![Figure 6. Poincaré section of system (2) with $T=8$.](image)
4. Encryption algorithm

In encryption algorithm, the initial values of switched system (2) are selected as the key stream and pixel scrambling is used to disturb the pixel position of the original image and to reduce the correlation between adjacent pixels. The gray scale value is used to change the pixel gray scale of the scrambled image and to disturb the original characteristics of the image.

4.1. Chaotic encryption algorithm

**Step1**: Parameters and initial values are determined.

**Step2**: Take the initial value as the secret key to generate chaotic sequence.

**Step3**: XOR operation is performed between the sequence generated by Step2 and the gray value of the image to obtain the encrypted image.

**Step4**: The decryption process also uses the initial values of the switched system to generate chaotic sequence, and then performs XOR operation with the gray value of the encrypted image to obtain the decrypted image.

4.2. Experimental analysis

Color image "Lena" with size of 256×256×3 is used as plaintext image. The simulation results are shown in Figure 7(a), 7(b) and 7(c), respectively.

![Figure 7](image)

**Figure 7.** Experimental results: (a) Plain image; (b) Encrypted image; (c) Decrypted image.

5. Security analysis

5.1. Statistical analysis

Histogram can reflect the distribution of image pixel value by counting the number of different pixels. The more uniform the histogram distribution is, the more irregular the image pixel value distribution will be. Thus, it is effective to prevent attackers from obtaining effective information from the perspective of statistical characteristics. The histogram of the original image and the encrypted image are shown in Figure 8(a) and 8(b), respectively. It can be seen from the comparison that the pixel values of the original image are distributed centrally in some points, while the pixel values of the encrypted image are uniformly distributed. In other words, when the original image is encrypted, it is more secure against potential statistical attacks.

The correlation coefficients of the original image and the encrypted image can be calculated by randomly extracting many pairs of adjacent pixel values. The following calculation formulas are adopted

\[ E(x) = \frac{1}{p} \sum_{i=1}^{p} x_i, \]  
\[ D(x) = \frac{1}{p} \sum_{i=1}^{p} (x_i - E(x))^2, \]
\[ \rho_{xy} = \frac{\text{cov}(x, y)}{\sqrt{\text{D}(x)\text{D}(y)}}. \]  

(5)

\[ \text{cov}(x, y) = \frac{1}{p} \sum_{i=1}^{p} (x_i - E(x))(y_i - E(y)). \]  

(6)

where \( x \) and \( y \) represent the gray value of two adjacent pixels, \( p \) is the total number of pixels in the image, and \( \rho_{xy} \) is the correlation coefficient of adjacent pixels.

Simulation results are shown in Figure 9(a), (b) and Table 3. By contrast, the correlation of adjacent pixels is very large for the original image, and the correlation of adjacent pixels is very small for the encrypted image. It indicates that the statistical characteristics of the original image has been scattered completely randomly. It means that the switched chaotic system has better image encryption performance than the single Chen system.

There are many criteria for judging the performance of image encryption, such as the information entropy, the mean-variance gray value, histograms of the image, and the run statistics analysis. In general, the greater the information entropy \( (H) \), the mean-variance gray value \( (G) \), the run statistics \( (R) \), and the smaller the histogram equalization \( (F) \), the better the image encryption effect will be.

![Figure 8](image8.png)

(a) (b)

**Figure 8.** (a) Histograms of the plain image and (b) the encrypted image.

| Correlation coefficients | Original image | Chen system | Switched chaotic system |
|--------------------------|----------------|-------------|-------------------------|
| plain image              | 0.8662         | 0.8662      | 0.8662                  |
| encrypted image          | ---            | -0.0180     | -0.0088                 |

**Table 3.** Correlation coefficients of the plain image and encrypted image.

![Figure 9](image9.png)

(a) (b)

**Figure 9.** Correlations of (a) the plain image (b) the encrypted image.
\[
H = -\sum_{i=1}^{n} p_i \log_2 p_i 
\]

\[
G = \sum_{i=1}^{M} \sum_{j=1}^{N} |Image(i,j) - \text{avg}| \]

\[
F = \sum_{i=1}^{255} \left( K(i) - \frac{M \times N}{256} \right)^2 \]

\[
R = \frac{\text{num}}{M \times N} = \frac{\sum_{i=1}^{M} \text{num}_i}{M \times N} 
\]

The original image used in this paper is \(256 \times 256 \times 3\). After gray level process, the gray level is 256. That is, the symbol number of the source is 256, so the ideal entropy value of the source is 8. The higher the entropy of the image, the more uniform the gray distribution of the image will be. The results are shown in Table 4. It indicates that when encryption based on the switched chaotic system, it has better encryption performance compared with a single Chen system.

**Table 4.** Information entropy of encrypted image.

| Comparison    | H     | G     | F     | R     |
|---------------|-------|-------|-------|-------|
| Initial image | 5.1973| 20.0740| 146.6743| 0.0780 |
| Chen system   | 5.3276| 30.9656| 13.1422 | 0.5062 |
| Switched system | 5.5381| 32.1763| 2.8446  | 0.5699 |

The initial values of the switched system are selected as the secret keys. As long as one key is incorrect, decryption will fail. The secret keys used in this section are all 0.1. If the secret key is \((0.1, 0.1, 0.0999)\), the decryption will also fail. The simulation results are displayed in Figure 10(a)-(c), respectively.

![Wrong decryption result](a) (b) (c)

**Figure 10.** Wrong decryption result: (a) Plain image; (b) Encrypted image with secret key of 0.1; (c) Decrypted image with secret key \((0.1, 0.1, 0.0999)\).

It can be seen that the decrypted image by using the wrong key is totally different from the original image. That is to say, the decryption will completely fail even if the key is slightly biased.

### 5.2. Noise attack analysis

Salt-and-pepper noise is conducted on the encrypted image and then decrypt to observe the anti-attack effect. As shown in Figure 11(a)-(c), the simulation results show that the original image can be decrypted after salt-and-pepper noise is added. The decrypted image contains most of original information and we can recognize the original image from the decrypted image.
Figure 11. Salt-and-pepper noise attack: (a) Plain image; (b) Encrypted image; (c) Decrypted image.

6. Conclusions
In this paper, a four-scroll chaotic attractor is generated and is applied to color image encryption. The switched system is constructed based on the famous Chen system. A state-dependent switching law with a threshold is designed to activate the switching from one subsystem to the other. Thus, a four-scroll chaotic attractor is generated from the designed switched system by selecting suitable threshold value. The four-scroll chaotic attractor is applied to image encryption. The simulation results indicate that the encryption performance of this switched chaotic system is better than that of a single Chen system.

Acknowledgement
This work was supported by the National Natural Science Foundation of China (61473178).

References
[1] Ghebleh M, Kanso A and Noura H 2014 An image encryption scheme based on irregularly decimated chaotic maps *Signal Processing: Image Communication* 29(5) 618-627
[2] Zhang Y, Xiao D, Shu Y and Li J 2013 A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations *Signal Processing: Image Communication* 28(3) 292-300
[3] Matthews R 1989 On the derivation of a 'chaotic' encryption algorithm *Cryptologia* 13(1) 29-42
[4] Kumar R and Quan C 2019 Optical colour image encryption using spiral phase transform and chaotic pixel scrambling *Journal of Modern Optics* 66(7) 776-785
[5] Chai X, Zheng X, Gan Z, Han D and Chen Y 2018 An image encryption algorithm based on chaotic system and compressive sensing *Signal Processing* 148 124-144
[6] Hou J, Xi R, Liu P and Liu T 2017 The switching fractional order chaotic system and its application to image encryption *IEEE/CAA Journal of Automatica Sinica* 4(2) 381-388
[7] Parvaz R and Zarebnia M 2018 A combination chaotic system and application in color image encryption *Optics & Laser Technology* 101 30-41
[8] Suykens J A and Vandewalle J 1993 Generation of n-double scrolls (n= 1, 2, 3, 4...) *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 40(11) 861-867
[9] Yalcin M E, Suykens J A K, Vandewalle J and Ozoguz S 2002 Families of scroll grid attractors *International Journal of Bifurcation and Chaos* 12 23-41
[10] Yalcin M E, Ozoguz S, Suykens J A K and Vandewalle J 2001 n-scroll chaos generators: a simple circuit model *Electronics Letters* 37(3) 147-148
[11] Tang W K, Zhong G Q, Chen G and Man K F 2001 Generation of n-scroll attractors via sine function *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications* 48(11) 1369-1372