Image Encryption Based on Fractional-order Chaotic Model of PMSM

Wei Xue\textsuperscript{1}, Mei Zhang\textsuperscript{6}, Shilong Liu, Xue Li
Department of Automation, Tianjin University of Science and Technology, 1038 Daguanlu Road, Hexi District, Tianjin 300222, PR China

E-mail:* xuewei@tust.edu.cn; \textsuperscript{6}zhangmeifuwei@163.com
www.tust.edu.cn

Abstract

The permanent magnet synchronous motor (PMSM) is a nonlinear system with multi-variable and significant coupling. When PMSM works in certain conditions, the chaotic behavior will occur. In this paper, the application of image encryption based on fractional-order chaotic model of PMSM is investigated. By the mean of drawing histogram, adjacent pixels correlation, key sensitivity of the cipher-text were analyzed. The results show that image encryption based on fractional-order chaotic model of PMSM have a large key space and high security.

Keywords: Fractional-order chaotic model; Permanent magnet synchronous motor (PMSM); Image encryption; Algorithm.

1. Introduction

In the nonlinear system described by the equation of state, when motion of the system is far from the equilibrium state, with the changing of the system parameters, the dynamic behavior of the system enter into the dissipative structure state with time-space order and symmetry through bifurcation or chaotic state more disorder.\textsuperscript{1} In recent years, many new chaotic systems have been proposed.\textsuperscript{2-8} In 1999, the Chen system was successfully constructed by Chen et al.\textsuperscript{3} In 2002, the Lü system was further discovered by Lü et al.\textsuperscript{4} In 2003, Liu et al. discovered a three-dimensional continuous autonomous chaotic system of four-helical chaotic attractors, named as Liu system.\textsuperscript{5} In 2005, a new four-wing autonomous chaotic system, the Qi system was proposed by Qi et al.\textsuperscript{6,8} Those researches have made great progress in chaotic dynamics analysis. When the chaotic system is described by fractional-order model, the system can still show the chaotic state, it is found that the fractional-order chaotic model can accurately describe the real physical phenomena.\textsuperscript{9-10} Some practical nonlinear systems are chaotic in the process of operation sometime. For example, there has chaotic behavior in permanent magnet synchronous motor (PMSM) when it works under certain condition.\textsuperscript{11-12} Some scholars have studied the fractional-order chaotic model of PMSM.\textsuperscript{13-14} As the fractional-order increases, the PMSM system enters the chaotic motion through the fixed point and quasi-periodic state.\textsuperscript{15} In general, the existence of chaos is harmful in the actual systems, it is controlled to eliminate its chaotic behavior. But the chaotic characteristics have good effects in some aspects, we can use chaotic characteristics to achieve secure communication and image encryption.

The basic theoretical research of chaotic dynamics has been great development in the field of confidential communication and image encryption. Fractional-order chaotic system provides more key parameters for the encryption algorithm and increases the key space, in order to improve the security of the system.\textsuperscript{16} Digital image pixel location scrambling is an important encryption method, the characteristics of the histogram are not changed, it also reflects the information system and memory the information. In addition, the nonlinearity and complexity are enhanced by the fractional-order chaotic system, which increases the key space. By the mean value of histogram, the correlation of adjacent pixels and the key sensitivity of cipher-text, the image encryption effect based on the fractional-order chaotic model of PMSM is analyzed in this paper.

© The 2017 International Conference on Artificial Life and Robotics (ICAROB 2017), Jan. 19-22, Seagaia Convention Center, Miyazaki, Japan
2. Numerical analysis of fractional–order chaotic model of PMSM

The fractional-order PMSM chaotic model is as follows:

\[
\begin{align*}
D^\alpha x &= -x + yz \\
D^\alpha y &= -y - xz + \gamma z \\
D^\alpha z &= \sigma(y - z)
\end{align*}
\]

(1)

Where the dimensionless state variables \( x, y, z \) represent the stator current, the rotator current and the mechanical angular velocity respectively; \( \sigma \) and \( \gamma \) are the system parameters related to the motor damping and permanent flux; \( \alpha \in (0,1) \) is the fractional order.

When \( \alpha = 0.95, \sigma = 20, \) and \( \gamma = 300, \) phase portraits are shown in Fig.1. Lyapunov exponent spectrum is shown in Fig.2.

It is showed clearly that system (1) has complex dynamic characteristics.

![Phase portraits of system (1) with \( \alpha = 0.95, \sigma = 20, \) and \( \gamma = 300: \](a) \( x-y \), (b) \( x-y-z \)).

![Lyapunov exponent spectrum of system](image)

3. Application of fractional-order chaotic model of PMSM in image encryption

A message is called a plaintext, in order to hide content, the process of concealing messages in some way is called encryption. Encrypted messages are called cipher-text, and the process of converting cipher-text to plaintext is called decryption. Digital image pixel location scrambling change is an important document encryption method. Color images are described by R, G and B primary color, and it stores in a matrix format of \( m \times n \times 3 \) in computer. Fractional-order chaotic model of PMSM is a system with three state variables, the \( y \) chaotic sequence is used to perform one-dimensional time-domain scrambling sequence on the digital image. And then the three-dimensional sequence matrix is used to realize the spatial encryption algorithm by performing XOR operation. Encryption flow chart is shown in Fig.3, decryption flow chart is shown in Fig.4.

![Encryption flow chart](image)

![Decryption flow chart](image)

3.1. Encryption process

The system (1) parameters are still chosen as \( \alpha = 0.95, \sigma = 20, \) and \( \gamma = 300, \) the initial states are assumed as \( x_0 = 0.1, y_0 = 0.2, z_0 = 0.3, \) then the digital image is encrypted. The encryption process steps are as follows:

1) The plain text is divided into three primary colors: R component image, G component image and B component image. The results are shown in Fig.5.

© The 2017 International Conference on Artificial Life and Robotics (ICAROB 2017), Jan. 19-22, Seagaia Convention Center, Miyazaki, Japan
2) The y sequence is sorted to obtain a sequence y change, and then transform R, G, B corresponding components. After that, the R, G and B components of color image are calculated by using chaotic sequences. Due to space constraints, here only the encryption result of the G component is given. The result of the encryption of G component is shown in Fig.6.

3) The encrypted three-color matrix is used to synthesize the encrypted image. The result is shown in Fig.7.

3.2. Decryption process

The image decryption process based on system (1) is the reverse operation of its encryption. And the plaintext will not repeat. Decryption result is shown in Fig.8.

3.3. Algorithm security analysis

3.3.1. Histogram analysis

Fig.9 is the gray histogram of G component. It can be seen from the figure: Before encryption, the pixel distribution is obvious in each gray level, the difference between the highest point and the lowest point is very large; after encryption, the number of pixels is almost the same, and the frequency of the pixels is basically the same in each gray level. The pixel distribution of the original image is hidden in a large degree, which can be a good resistance to the statistic.

3.3.2. Adjacent pixel correlation analysis

One row and one column of pixels are selected from the original image and the encrypted image. The correlation coefficients of its adjacent pixels are calculated in Tab.1. The encryption algorithm of this method has good performance of diffusion and aliasing, and the encryption algorithm of fractional-order chaotic model of PMSM has better security for statistical analysis attacks.

<table>
<thead>
<tr>
<th>Different directions</th>
<th>Different images</th>
<th>Horizontal direction</th>
<th>Vertical direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The original image R pixel matrix</td>
<td>0.97303</td>
<td>0.97327</td>
<td></td>
</tr>
<tr>
<td>The original image G pixel matrix</td>
<td>0.9753</td>
<td>0.97538</td>
<td></td>
</tr>
<tr>
<td>The original image B pixel matrix</td>
<td>0.98807</td>
<td>0.98861</td>
<td></td>
</tr>
<tr>
<td>Encrypted image R pixel matrix</td>
<td>0.0025357</td>
<td>0.00088599</td>
<td></td>
</tr>
<tr>
<td>Encrypted image G pixel matrix</td>
<td>0.00036788</td>
<td>0.00060489</td>
<td></td>
</tr>
<tr>
<td>Encrypted image B pixel matrix</td>
<td>0.00068514</td>
<td>0.00061357</td>
<td></td>
</tr>
</tbody>
</table>

3.3.3. Key sensitivity analysis

Given the system (1) parameter: \( \alpha = 0.95, \sigma = 20, \) and \( \gamma = 300. \) When the initial states are assumed as \( x_0 = 0.1, \) \( y_0 = 0.2, \) \( z_0 = 0.3 \) to the system key, the image is encrypted. When the correct key is input, the decrypted image can be obtained successfully. If we change the initial value as \( x_0 = 0.1000000000001 \) and the other parameter values are unchanged, the image
decryptions fail. Unsuccessful decryption results are shown in Fig.10. As long as the key changes, the original figure can not be decrypted. This shows that the sensitivity of the encryption system on the key requirements is high.

Fig.10 Decryption results of the wrong key

4. Conclusion

In this paper, the fractional-order chaotic model of PMSM is used as the key to encrypt the digital image. The phase trajectories and Lyapunov exponent spectrum of fractional-order chaotic model of PMSM are drawn. Furthermore, the chaotic model is applied to image encryption, and the flow chart of image encryption and decryption process are given. By means of histogram, adjacent pixel correlation and key sensitivity, the cipher-text is analyzed. The results show that the digital image encryption algorithm based on the fractional-order chaotic model of PMSM has the characteristics of large key space and high security, and indicates that it is feasible and effective to use the model for image encryption.

5. Acknowledgement

This work is supported by the Young Scientists Fund of the National Natural Science Foundation of China (Grant No.11202148).

6. References