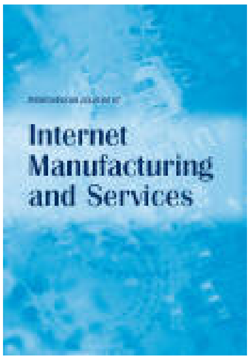
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



Internet Manufacturing and Services

International Journal of Internet Manufacturing and Services

ISSN online: 1751-6056 - ISSN print: 1751-6048
https://www.inderscience.com/ijims

A data encryption technology for serial communication of multi degree of freedom manipulator based on chaotic sequence

Yan-Qin Zhang, Xiao-Xing Shi, Yunqing Qu

DOI: 10.1504/IJIMS.2022.10052232

Article History:

Received:	26 April 2022
Accepted:	20 July 2022
Published online:	03 March 2023

A data encryption technology for serial communication of multi degree of freedom manipulator based on chaotic sequence

Yan-Qin Zhang, Xiao-Xing Shi* and Yunqing Qu

Department of Electrical and Electronic Engineering,
Shijiazhuang University of Applied Technology,
Shijiazhuang, 050081, China
Email: 5546378@qq.com
Email: xiaoxshi@mls.sinanet.com
Email: 3998744@qq.com
*Corresponding author

Abstract: In order to effectively improve the security of serial communication data encryption of manipulator and shorten the encryption time, a multi degree of freedom serial communication data encryption technology of manipulator based on chaotic sequence is proposed. The serial communication data of the manipulator is obtained by using the logistic chaotic map, and the chaotic sequence of the communication data is generated. Based on the binary sequence generated by the logistic chaotic map, the serial communication data encryption key of each wheel is generated. The serial communication data obtained is forward XOR or reverse XOR with the sub key to realise the serial communication data encryption of the mechanical arm. The experimental results show that the maximum value of the cross-correlation function of the proposed method is closer to 0, and the data encryption time is only 15.2 s, which effectively improves the security of data encryption.

Keywords: chaotic sequence; logistic chaotic map; multi-degree-of-freedom manipulator; serial communication data; data encryption.

Reference to this paper should be made as follows: Zhang, Y-Q., Shi, X-X. and Qu, Y. (2023) 'A data encryption technology for serial communication of multi degree of freedom manipulator based on chaotic sequence', *Int. J. Internet Manufacturing and Services*, Vol. 9, No. 1, pp.32–43.

Biographical notes: Yan-Qin Zhang received her Master's in Communication and Information System from Shenyang Ligong University in 2010. She is currently an Engineer and Lecturer in the Department of Electrical and Electronic Engineering of Shijiazhuang University of Applied Technology. Her research interests include wireless communication technology, communication engineering, and electronic application.

Xiao-Xing Shi received her Master's in Mechanical Engineering from Hebei University of Technology in 2011. She is currently a Lecturer in the Department of Electrical and Electronic Engineering of Shijiazhuang University of Applied Technology. Her research interests include mechanical engineering.

Yunqing Qu is an Associate Professor, and graduated from Hebei Normal University in 2001 with a Master's degree. She is currently an Associate Professor of Electrical and Electronic Engineering Department of Shijiazhuang University of Applied Technology. Her research interests are electronic and electrical, and high precision sensor micro-displacement measurement.

1 Introduction

With the rapid development of network technology, people's demand for information transmission, storage and processing is increasing day by day, and the security of The Internet is also attracting people's attention (Zhang, 2021; Wei and Wang, 2020; Gao, 2020). Due to its many advantages, multi degree of freedom manipulator has gradually become a hot topic in robot research. Multi degree of freedom manipulator is widely used in engineering field because of its advantages of high reliability, large workspace and high flexibility (Wei et al., 2020; Wang and Liu, 2020). However, the content of serial communication data of multi degree of freedom manipulator can be analysed through network monitoring software, and there is a serious threat to the serial communication data of the mechanical arm. Therefore, it is of great significance to encrypt the serial communication data of multi degree of freedom manipulator.

Qi et al. (2021) proposed a real-time communication encryption method of manipulator based on ROS and can protocol. The serial communication data of the mechanical arm is obtained through ROS system, the serial communication data of the mechanical arm is analysed by CAN protocol, the hash dynamic transmission protocol is used for data access control, and the elliptic linear mapping method is used to realise the secure encryption of serial communication data of the mechanical arm, This method improves the transmission performance of network communication data, but the overall encryption effect is not ideal. Wang and Li (2021) proposed an encryption control method of manipulator communication databased on deep reinforcement learning, built a mechanical arm simulation control module, obtained the serial communication data of the mechanical arm through the deep reinforcement learning method, reduced the dimension of the communication data through two-dimensional discrete wavelet transform, and used the improved ddpg algorithm for interactive training with the simulated manipulator to obtain the serial communication data control model of the manipulator, So as to realise the accurate control of the communication data of the manipulator and protect the data in the channel. Wang (2019) proposed a data encryption method of 7-DOF manipulator communication network based on CAN bus. The data sequence of DOF Manipulator is obtained through merlay state machine, the can communication network of DOF Manipulator is established, the sinusoidal function data transmitted between nodes is obtained, the data control of DOF Manipulator communication network is realised through can bus, and the sub key is generated by specific threshold function to complete the communication data encryption of manipulator. This method can effectively improve the effect of serial communication data encryption, but the encryption takes a long time.

To solve the above problems, this paper proposes a serial communication data encryption technology of the mechanical arm based on chaotic sequence. The overall research scheme of this technology is as follows:

1 The serial communication data of the mechanical arm is mapped by logistic chaos, and the chaotic sequence of serial communication data of the mechanical arm is generated. Based on the binary sequence generated by Logistic chaotic map, the serial communication data encryption key of the mechanical arm is generated.

2 The serial communication data of the mechanical arm is XORed with the sub key in the forward or reverse direction to realise the serial communication data encryption of the mechanical arm.

3 Experimental verification, taking the encryption effect, encryption security and encryption time as the experimental comparison index, this method is compared with different traditional methods.

2 Chaotic sequence

2.1 Concept and characteristics of chaos

If a real physical system still has similar randomness after excluding the influence of all randomness, it is called chaos (Shailaja and Ningappa, 2021; Sabir et al., 2021). Chaotic system is a nonlinear dynamic system with the following characteristics:

1 Chaotic signal is a kind of deterministic random signal. Given the system parameters and initialisation conditions, chaotic signal can be reproduced accurately. True random signal can ensure the absolute security of 'one secret at a time', but it cannot be copied and decrypted properly. Chaotic signal can effectively solve the above problems.

2 Under chaotic conditions, chaotic systems are highly sensitive to system parameters and initial values. If the parameters and initial values of the same chaotic system are slightly different, it will soon become two distinct states, resulting in the change of chaotic signals. This shows that chaotic signals can not be predicted for a long time.

3 Continuous spectrum: the spectrum of chaotic signal is similar to that of random signal.

4 Singular attractor: in phase space, the attractor of chaotic signal presents a very complex geometric structure. There is a singular fractional attractor, and the Lyapunov exponent of chaotic attractor is positive (Mohammadi, 2020; You and Leung, 2021).

5 The analysis, reconstruction and prediction of chaotic sequence are very difficult, and chaotic sequence is a kind of nonlinear sequence. At present, it is limited to reconstruction in some specific cases, and there is no good general algorithm in theory.

In short, chaotic system can provide many random, uncorrelated and complex pseudo-random numbers. It is a good information encryption method. Therefore, the in-depth study of chaotic system is of great significance both in theory and practice.

2.2 Logistic chaotic mapping

On this basis, a one-dimensional discrete nonlinear dynamic system z_{k+1} is defined:

$$z_{k+1} = f(z_k) \tag{1}$$

Suppose H is a compact metric space of continuous mapping f: $H \to H$, if the following conditions are met:

1 Sensitive dependence on the initial value

2 Topological transitivity

3 The periodic points of f are dense in H, and f is called the chaotic image on H.

Logistic mapping belongs to a very simple but widely studied dynamic system z_{k+1} (Ahmmed et al., 2021; Zhang. and Guo, 2021; Wang et al., 2021), which is defined as follows:

$$z_{k+1} = 1 - \varphi z_k^2 \tag{2}$$

In equation (2), $\varphi \in 0, 2$. When $\varphi \to = 1.40115$, the $N \to \infty$ cycle is quickly reached, that is, chaos is entered, and its probability distribution density function x is as follows:

$$\vartheta(x) = \frac{1}{\pi\sqrt{1-x^2}}, -1 < x < 1 \tag{3}$$

Through x, combined with logistic mapping, some important features of chaotic sequences can be easily obtained. If the average time of x, that is, the trajectory point of the chaotic sequence, its average value x is:

$$\overline{x} = \frac{1}{N}\sum_{i=0}^{N-1} x_i = \int_0^1 x\vartheta(x)dx = 0 \tag{4}$$

In the correlation function, two initial values p_0 and u_0 are selected respectively, and the relationship is:

$$t(l) = \frac{1}{N}\sum_{i=0}^{N-1} (x_i - \overline{x})(p_0 - u_0) \tag{5}$$

Therefore, the correlation function mapping relationship of serial communication data of the mechanical arm is obtained.

2.3 Chaotic sequence generation

So far, there are mainly the following chaotic sequences (Zhang et al., 2020; Das and Kar, 2021; Yu and Wang, 2021) commonly used for encryption:

1 The sequence of real numbers, that is, $\{z_k: k = 0, 1, 2, \ldots\}$. This is a series of chaotic maps.

2 Binary sequence: A function $\delta(x)$ generated by the real-valued chaotic sequence described above is defined, and its operation results are as follows:

$$\delta x = \{0 - 1 \leq x < 0\ 1 \quad 0 \leq x \leq 1 \tag{6}$$

A series of chaotic sequences are generated by this method.

3 Bit sequence: It is also obtained from a chaotic sequence of real numbers. Unlike the binary sequence, z_k is rewritten into L-bit in the form of a floating point number, that is:

$$|z_k| = \beta_1(z_k)\beta_2(z_k), \cdots, \beta_i(z_k) \tag{7}$$

The generated sequence $\beta_i(z_k)$is:

$$\{\beta i(z_k); i = 0,1,2, \cdots L; k = 0,1,2, \cdots\} \tag{8}$$

4 Four-value chaotic sequence: The generation of the chaotic sequence is similar to the generation of the chaotic sequence. The interval I:–1, 1 is divided into 4 sub-intervals I_j:j = 0, 1 ,2, 3, so that the probability of z_k entering each sub-area is equal, so it can be divided into:

$$g0 = -1, g_1 = \frac{-\sqrt{2}}{2}, g_3 = \frac{-\sqrt{2}}{2}, g_4 = 1 \tag{9}$$

If $x_k = j$, then $\{x_k$: $k = 0, 1, 2, 3, \ldots\}$ is the desired chaotic sequence.

3 DOF manipulator serial communication data encryption method

3.1 Chaotic mapping of serial communication data of the mechanical arm

On the surface, the serial communication data of the mechanical arm has no rules and is similar to random, but there are actually certain rules. For this reason, logistic chaos is used to map the serial communication data of the mechanical arm to prepare for data encryption. The specific mapping process is as follows:

Assuming that the serial communication data of the mechanical arm at time point t is q_n, and the serial communication data of the mechanical arm at time point $t + 1$ is q_{n+1}, the relationship between the two time points can be expressed by the following a form of representation:

$$q_{n+1} = F(q_n) \tag{10}$$

In equation (10), $F(q_n)$ represents a specific functional relationship, and the value range of n is 0,1 ,2,…, ∞.

Using the Logistic chaotic sequence mapping conversion equation (10), the serial communication data mapping relationship of the mechanical arm is obtained as:

$$q_{n+1} = q_n(\alpha - \beta q_n) \tag{11}$$

In equation (11), α represents the growth rate of serial communication data between multiple degrees of freedom manipulators, and β represents the saturation of a mapping relationship including external factors.

In order to reduce the computational complexity of equation (11) and make the parameter $\alpha = \beta = \gamma$ equation (12) is rewritten as:

$$q_{n+1} = \gamma q_n \left(1 - q_n\right) \tag{12}$$

Through the above steps, the chaotic mapping of serial communication data of the mechanical arm is completed.

3.2 Chaotic sequence generation of serial communication data of multi degree of freedom manipulator

Based on the chaotic mapping of serial communication data of the mechanical arm, the chaotic sequence of serial communication data of multi degree of freedom manipulator is established and simplified.

The sequence of real numbers is composed of the trajectory points of the chaotic map, and the sequence of real numbers is represented by w_n, $n = 0, 1, 2, \ldots, \infty$. The bit sequence is in the actual number sequence, the sequence element becomes a floating point number, which is represented by $|w_n| = \beta_1(w_n), \beta_2(w_n), \ldots, \beta_i(w_n)$, and $\beta_i(w_n)$ is the i bit element of $|w_n|$, and its value is [0, 9]. The binary sequence is obtained by defining the threshold function δ, and the set threshold function is expressed as:

$$\delta(w_n) = \{0 - 1 \le w_n < 0 \; 1 \quad 0 \le w_n \le 1 \tag{13}$$

Then the binary sequence element is $\{\delta(w_n), n = 0, 1, 2 \ldots, \infty\}$. The results show that the binary sequence is more consistent with the encryption of the serial communication data of the mechanical arm. Therefore, equation (13) is the chaotic sequence of the serial communication data of the mechanical arm.

3.3 Generation of serial communication data encryption sub key of multi degree of freedom manipulator

Logistic chaotic mapping uses the same parameter as its input, and the binary sequence generated by a specific number of Logistic chaotic mapping is transformed into a binary sequence by the $sign(w_n)$threshold function, and its $sign(w_n)$threshold equation (Lin et al., 2020) is expressed as follows:

$$sign(w_n) = \{0 \quad 0 \le w_n < 0.5 \; 1 \quad 0.5 \le wn \le 1 \tag{14}$$

The original key is obtained by XOR transformation of 64 bit binary sequence stream and 64 bit plaintext sequence, so as to realise the synchronisation and variability of the original key for serial communication data encryption and decryption of the mechanical arm.

3.4 Realisation of serial communication data encryption of multi degree of freedom manipulator

Forward and reverse XOR the serial communication data of the mechanical arm obtained above with the sub key. The working steps are as follows:

1 Positive XOR is expressed as:

$$E_n = \delta\left(w_{n-1}\right) \oplus R_n \oplus sign(wn) \tag{15}$$

In equation (15), R_n represents the XOR parameter.

2 Reverse XOR is expressed as:

$$En = \delta\left(w_{n+1}\right) \oplus Rn \oplus sign(w_n) \tag{16}$$

3 After XOR is completed, the forward and reverse modes are extracted, and the expression is as follows:

$$\begin{aligned} &\{E_n = \left(\delta\left(w_{n-1}\right) \oplus Rn \oplus sign\left(w_n\right)\right)\ mod127\ E_n = wn \\ &\quad \left(\delta\left(w_{n-1}\right) \oplus R_n \oplus sign\left(w_n\right)\right)\ mod127 \end{aligned} \tag{17}$$

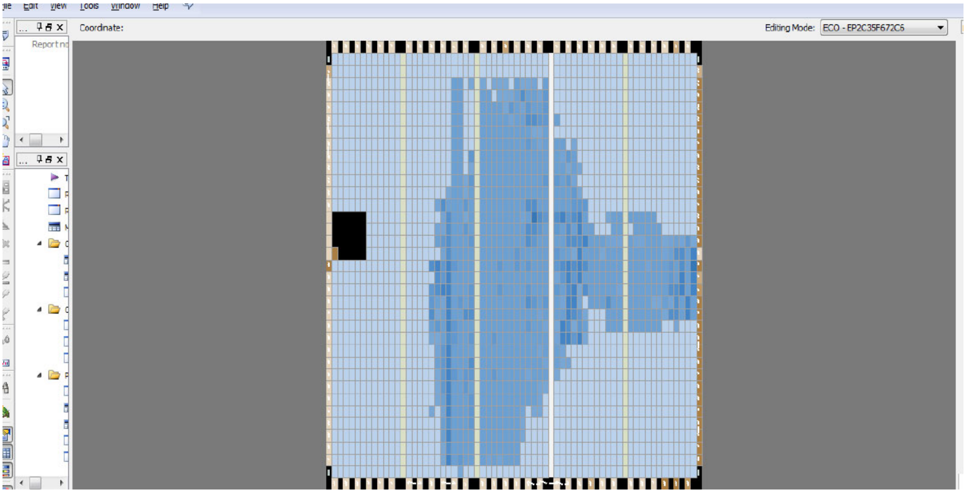
The result obtained by forward and reverse modelling is the encrypted serial communication data of the mechanical arm, which realises the encryption of serial communication data of multi degree of freedom manipulator, and provides a more efficient guarantee for the security of serial communication of the mechanical arm.

4 Experimental simulation and analysis

4.1 Setting the experimental environment

In order to verify the effectiveness of serial communication data encryption technology of the mechanical arm based on chaotic sequence, the experimental platform selects XUP Virtex-IIPro development platform. Virtex-II Pro Series has Virtex-II with PowerPC 405 core built in. The whole design scheme uses VHDL language to describe RTL level, and is simulated on Virtex-2 Pro.

Figure 1 Resource share and routing chart of chip planner (see online version for colours)



ile Edit View Tools Window Help
Coordinate:
Editing Mode: ECO - EP2C35F672C6
Report n

This paper describes the FPGA implementation process of MD5 encryption algorithm through iterative loop and pipeline design, and compares and analyses the accuracy, resource occupancy, execution speed, power consumption and throughput of the two methods to optimise the process of the designed encryption algorithm. Xilinx ISE is used as a comprehensive development tool. The autocorrelation and cross-correlation between binary sequences generated by Logistic chaotic system are used, and the autocorrelation and cross-correlation functions between randomly selected subsequences are used to make it have an interval of 0–3200.Understand the resources used in detail by analysing the resource share. The design uses Quartus II compiler, which has the chip planner function. It uses the graphical interface to express the occupation of resources and the layout of Chip Planner in a more humanised, intuitive and detailed way. Chip planner compiles and displays the connection between resource occupancy and routing, as shown in Figure 1.

As can be seen from Figure 1, each small cell represents a series of digital logic units. The light part is the unused logic unit, the dark part is the logic unit occupied by the system, and the black square is the unusable logic unit to maintain the normal operation of the chip. It can be seen intuitively from Figure 1 that the logical resources used in the system design account for the total proportion. By opening each small cell, we can understand the routing and delay between devices. It plays a guiding role in improving the speed.

4.2 Experimental scheme

According to the above experimental environment, in order to improve the effectiveness of the experimental results and reduce the experimental error, taking the communication data encryption effect, communication data encryption security and communication data encryption time as the experimental comparison indicators, this method is compared with the methods of Qi et al. (2021) and Wang and Li (2021).

1 Encryption effect: Taking the *ASII* code value as the evaluation index, the more stable the change of ASII code value is, indicating that the serial communication data encryption effect of the multi degree of freedom manipulator of the method is better. The calculation formula of *ASII* code value is:

$$ASII = log\frac{n_{qj}}{n_q}, +n_k \tag{18}$$

where the cluster numbers of communication data of multi degree of freedom manipulator are q and j; The degree of fit between q and j is n_{qj}; The sample sizes existing in q and j are n_q and n_k; The total number of samples is n.

2 Encryption security: the subsequence autocorrelation and cross-correlation functions are used as evaluation indexes. The smaller the subsequence autocorrelation and cross-correlation function, the larger the key space and the higher the initial value sensitivity, which indicates that the method has higher data encryption security for serial communication of multi degree of freedom manipulator. The maximum value H_I of autocorrelation function and the maximum value R_I of cross-correlation function are calculated as follows:

$$H_I = \frac{E_0 + E_1}{n(n-1)/2} \tag{19}$$

RI is calculated as follows:

$$RI = \frac{E_0 + E_1}{n(n+1)/2} \tag{20}$$

where, the number of pairs with different labels and different classes is E_0; There are consistent labels in the data, and the number of pairs in the same category is E_1.

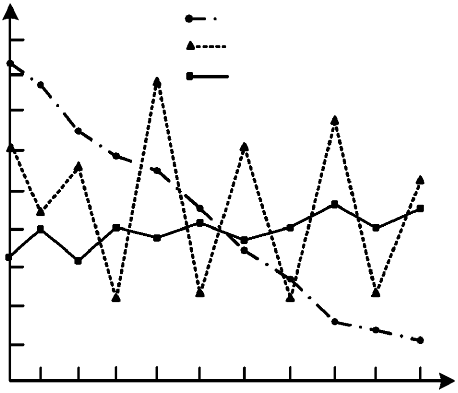
3 Encryption time consumption: encryption time consumption refers to the time consumed by different methods for encryption when the amount of data is the same. The shorter the time consumption, the faster the efficiency of the method.

4.3 Experimental results

4.3.1 Data encryption effect of serial communication of the mechanical arm

In order to verify the data encryption effect of serial communication of the mechanical arm, ASII code value is taken as the evaluation index. The more stable the change of ASII code value is, the better the data encryption effect of serial communication of the mechanical arm is. By comparing the method of Qi et al. (2021), the method of Wang and Li (2021) and the proposed methods, the data encryption effect of serial communication of the mechanical arm with different methods is obtained, as shown in Figure 2.

Figure 2 Data encryption effect of serial communication of the mechanical arm with different methods



As can be seen from Figure 2, the overall state of the character change curve of the proposed method is relatively stable, which shows that when encrypting the serial communication data of the mechanical arm, this paper effectively makes use of the advantages of chaotic sequence to ensure the uniform distribution of relevant sub key sequence and ensure that it can effectively complete the communication data encryption even in the case of dense and complex communication data. However, the overall state of the character change curve of the method of Qi et al. (2021) and the method of Wang and Li (2021) fluctuates greatly, and the problem of uneven distribution caused by the serial communication data of the mechanical arm is not considered. As a result, when the amount of encrypted data increases, the corresponding sub key cannot be evenly distributed, which affects the encryption quantity and cannot ensure the encryption effect.

It can be seen that the serial communication data encryption effect of the mechanical arm of the proposed method is better.

4.3.2 Security of serial communication data encryption of the mechanical arm

On this basis, the security of serial communication data encryption of the mechanical arm is verified, and the subsequence autocorrelation and cross-correlation functions are used as evaluation indexes. The smaller the subsequence autocorrelation and cross-correlation functions, the larger the key space, and the higher the initial value sensitivity, indicating that the serial communication data encryption security of the mechanical arm of the method is higher. By comparing the method of Qi et al. (2021), the method of Wang and Li (2021) and the proposed method respectively, the serial communication data encryption security of the mechanical arm of different methods is shown in Table 1.

Table 1 Data encryption security of serial communication of the mechanical arm with different methods

Different methods	*Maximum value of autocorrelation function*	*Maximum value of cross correlation function*
The proposed method	0.0138	0.0074
The method of Qi et al. (2021)	0.0149	0.0086
The method of Wang and Li (2021)	0.0163	0.0091

It can be seen from Table 1 that the maximum values of autocorrelation and cross-correlation functions of the proposed method are 0.0138 and 0.0074 respectively, which are significantly lower than those of the method of Qi et al. (2021) and the method of Wang and Li (2021), and the maximum value of cross-correlation function of the proposed method is closer to 0. Therefore, the subsequence autocorrelation and cross-correlation functions of the proposed method are small, its sensitivity, randomness and correlation advantages are obvious, and the key space is further expanded. The results show that the data encryption security of serial communication of the mechanical arm is high.

4.3.3 Data encryption time of serial communication of the mechanical arm

Further verify the serial communication data encryption time of the mechanical arm, randomly select 1000 communication data sequences, and compare them with the method of Qi et al. (2021), the method of Wang and Li (2021) and the proposed methods respectively. The serial communication data encryption time of the mechanical arm with different methods is shown in Table 2.

According to the analysis of Table 2, with the increase of communication data sequence, the serial communication data encryption time of the mechanical arm with different methods increases. When the communication data sequence is 1000, the encryption time of serial communication data of the mechanical arm in the method of Qi et al. (2021) is 23.4s, the encryption time of serial communication data of the mechanical arm in the method of Wang and Li (2021) is 28.2s, while the encryption time of serial communication data of the mechanical arm in the proposed method is only 15.2s. The above results show that the proposed method can improve the encryption efficiency of serial communication data.

Table 2 Data encryption time of serial communication of the mechanical arm with different methods

Communication data sequence/piece	*The proposed method/ s*	*The method of Qi et al. (2021)/s*	*The method of Wang and Li (2021)/ s*
200	5.2	8.9	11.6
400	8.6	8.6	12.5
600	10.2	15.8	19.7
800	12.8	19.1	23.5
1,000	15.2	23.4	28.2

5 Conclusions

In this paper, the serial communication data of the manipulator is encrypted based on chaotic sequence. Chaotic sequence of communication data is generated by Logistic chaos mapping. Forward XOR or Reverse XOR is used to encrypt the communication data. It has high encryption security and short encryption time.The following conclusions are drawn through experiments:

1 The overall state of the character change curve of the proposed method is relatively stable. In the case of dense and complex communication data, it can also effectively complete the communication data encryption. The data encryption effect of serial communication of the mechanical arm based on the proposed method is good.

2 The maximum values of autocorrelation and cross-correlation functions of the proposed method are 0.0138 and 0.0074 respectively, and the maximum value of cross-correlation function is closer to 0. It shows that the proposed method has obvious advantages in sensitivity, randomness and correlation, and the key space is further expanded. It is shown that the proposed method is more secure in serial communication data encryption.

3 The serial communication data encryption time of the proposed method is only 15.2s, which reflects that the proposed method can meet the requirements of the serial communication data encryption of the manipulator.

In the following research, data hiding and data encryption technology can be organically combined to provide a more reliable guarantee for the data encryption security of serial communication of manipulator.

References

Ahmmed, T., Raha, I.T., Safwat, F. and Turzo, N.A. (2021) 'Impact of message size on least significant bit and chaotic logistic mapping steganographic technique', *International Journal of Advanced Scientific Research and Development* (IJASRD), Vol. 5, No. 4, pp.1100–1104.

Das, A. and Kar, N. (2021) 'A metamorphic cryptography approach towards securing medical data using chaotic sequences and Ramanujan conjecture', *Journal of Ambient Intelligence and Humanized Computing*, Vol. 25, No. 10, pp.12652–12659.

Gao, K. (2020) 'Research on the application of computer remote network communication technology under big data technology', *Journal of Physics Conference Series*, Vol. 1648, No. 23, pp.42–48.

Lin, C.C., Liu, C.H., Chen, Y.C. and Wang, C.Y. (2020) 'A new necessary condition for threshold function identification', *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 39, No. 12, pp.5304–5308.

Mohammadi, S. (2020) 'LYAPROSEN: MATLAB function to calculate Lyapunov exponent', *Statistical Software Components*, Vol. 18, No. 26, pp.741502–741510.

Qi, H., Zhou, Y. and Zhang, C. (2021) 'Design and implementation of manipulator real-time communication mechanism based on ROS and can protocol', *Industrial Control Computer*, Vol. 34, No. 8, p.42.

Sabir, M., Ahmad, S. and Marwan, M. (2021) 'HOPF bifurcation analysis for liquid-filled Gyrostat chaotic system and design of a novel technique to control slosh in spacecrafts', *Open Physics*, Vol. 19, No. 1, pp.539–550.

Shailaja, A., Ningappa, K.G. (2021) 'A low area VLSI implementation of extended tiny encryption algorithm using Lorenz chaotic system', *International Journal of Information and Computer Security*, Vol. 4, No. 1, pp.112205–112208.

Wang, H. and Liu, S. (2020) 'Position servo control method for multi-degree-of-freedom pneumatic manipulators based on delayed feedback', *Automatic Control and Computer Sciences*, Vol. 54, No. 1, pp.10–18.

Wang, J. and Li, K. (2021) 'A manipulator control method based on deep reinforcement learning', *Journal of Henan University of science and Technology* (*NATURAL SCIENCE EDITION*),Vol. 42, No. 3, pp.19–24+3.

Wang, X., Guan, N. and Yang, J. (2021) 'Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map', *Chaos Solitons and Fractals*, Vol. 150, No. 3, pp.111117–111126.

Wang, Y. (2019) 'Research on communication network of 7-DOF manipulator based on CAN bus', *Journal of Longdong University*, Vol. 30, No. 2, pp.11–15.

Wei, D., Gao, T., Mo, X., Xi, R. and Zhou, C. (2020) 'Flexible bio-tensegrity manipulator with multi-degree of freedom and variable structure', *Chinese Journal of Mechanical Engineering*, Vol. 33, No. 1, pp.83–93.

Wei, P. and Wang, B. (2020) 'Multi-sensor detection and control network technology based on parallel computing model in robot target detection and recognition – ScienceDirect', *Computer Communications*, Vol. 159, No. 26, pp.215–221.

You, G. and Leung, S. (2021) 'Computing the finite time Lyapunov exponent for flows with uncertainties', *Journal of Computational Physics*, Vol. 425, No. 15, pp.109905–109909.

Yu, W. and Wang, H. (2021) 'Analysis of trigonometric chaotic sequence by proposing an index-based bit level scrambling image encryption', *Modern Physics Letters B*, Vol. 35, No. 24, pp.2150406–2150415.

Zhang, B. (2021) 'Research on the application of speech recognition in computer network technology in the era of big data', *International Journal of Speech Technology*, Vol. 25, No. 11, pp.10772–10778.

Zhang, S. and Guo, Q. (2021) 'Fixed frequency hysteresis current control of power filter based on chaos algorithm', *Computer Simulation*, Vol. 38, No. 9, pp.124–128.

Zhang, X., Zhang S. and Ma, L. (2020) 'an encrypted polar coding scheme based on chaotic sequences', *2020 27th International Conference on Telecommunications* (ICT), Vol. 13, No. 1540–956.