Research Article

Application of Image Encryption Algorithm for Wireless Sensor Network in the Security Analysis of Public Big Data

Qiang Geng and Huifeng Yan

1 School of Big Data & Software Engineering, Chongqing College of Mobile Communication, Chongqing City 401520, China
2 Chongqing Key Laboratory of Public Big Data Security Technology, Chongqing City 401420, China
3 School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing City 400065, China

Correspondence should be addressed to Huifeng Yan; yanhf@cqupt.edu.cn

Received 1 March 2022; Revised 25 March 2022; Accepted 4 April 2022; Published 23 April 2022

Academic Editor: Haibin Lv

Copyright © 2022 Qiang Geng and Huifeng Yan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

To improve the security of the Wireless Sensor Network (WSN), the image encryption algorithm is studied. Firstly, the shortcomings of current image encryption algorithms are compared. Secondly, based on the chaotic system, the color image encryption algorithm of double chaotic cross-diffusion is built, and the encryption platform is constructed in combination with the current development of intelligent equipment. Finally, the performance of the constructed algorithm and platform is evaluated, and the correlation of adjacent pixel pairs in different color channels and different directions of image encryption is verified. The results indicate that in the designed image encryption platform, the channels of different colors are encrypted in different directions, and the encryption effect is good. Compared with the evaluation platform, the practicability of the encryption algorithm is good. After the image is encrypted, the correlation between adjacent pixels is significantly reduced. The information entropy of the red, green, and blue channels after encryption is higher than before encryption. For the index values of Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR), the average UACI of the algorithm is 99.62%, while the average of the UACI of the literature algorithm is 98.33%. The NPCR value of the algorithm is 33.52%, while the NPCR value of the literature algorithm is 31.23%. The encryption and decryption time of the algorithm is shorter than that of the literature algorithm. The constructed algorithm has high efficiency of encryption and decryption. It provides a reference for the enhancement of the security of image data in the WSN.

1. Introduction

The Wireless Sensor Network (WSN) is a subset of the Internet of Things (IoT) and is also the basic component of the IoT [1]. In the era of the rapid progress of IoT technology, the development of WSN has also received extensive attention. The WSN is composed of nodes and sensor nodes connected by infinite channels, and its main role is in the data collection and processing of distributed networks [2]. The WSN has a wide range of applications, including precision agriculture, vehicle traffic management, medical imaging, disaster prediction, and automation [3]. The wide application of WSN also involves certain privacy issues, and ensuring the security of public big data in many fields is the focus of privacy protection in WSN [4]. For example, Lv and Qiao emphasized the security of medical big data in their research [5]. Chen et al. also illustrated the importance of cybersecurity in smart city research [6]. At present, the privacy right of the WSN is not clearly defined. The privacy right of WSN is defined as the right of data information that is not wanted to be known by others in the data information fed back by the WSN, such as the medical images of patients’ privacy and the private data of vehicles and drivers in intelligent transportation systems and others [7].
The encryption method is one of the main methods to protect private information. Since the WSN is more and more involved in image data in applications of life [8, 9], the image encryption algorithm will be studied. With the popularity of mobile devices, smartphones carry the security of image information, so image algorithms are mainly used in mobile devices [10]. Digital image data has the characteristics of a strong correlation between adjacent pixels, high redundancy, and a large amount of information [11]. The encryption algorithms of traditional data and images, such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) encryption algorithms, have the characteristics of poor security and low efficiency [12]. The chaotic system has the characteristics of pseudorandomness, chaos, and ergodicity, so the image encryption algorithm based on a chaotic map is considered to have high security and high efficiency [13]. At present, image encryption algorithms based on the chaotic map are rarely used in smart mobile devices.

Now, the security of image data in WSN needs to be improved, so the chaotic system is introduced to design the image encryption algorithm. Due to the popularity of smart devices, the application of image encryption algorithms on the Android platform will also be evaluated. The overall frame is shown in Figure 1.

In Figure 1, the research background of wireless sensors is firstly analyzed. Secondly, the image encryption algorithm and security analysis system based on the chaotic map are designed, and finally, the performance of the image encryption algorithm is evaluated. The innovation of the research lies in the proposed color image encryption algorithm of double chaotic cross-diffusion suitable for the intelligent mobile platform. The research satisfies people’s needs for image encryption algorithms for public big data with high security and efficiency and has very important research significance for promoting image information security and the rapid development of artificial intelligence.

2. Literature Review

Image scrambling in image encryption algorithm was first proposed in 1991. Image scrambling can disrupt the spatial position of image pixels and hide the original image by clustering the image [14]. Image scrambling was subsequently applied to more image encryption and decryption algorithms by many scholars [15]. The main function of image scrambling is to transform the original image for a limited number of times, so there are certain loopholes. When an image attacker obtains the ciphertext and performs the same operation for a limited number of times, the original image can be easily cracked [16]. Subsequently, the image encryption technology in the transform domain was born, which is mainly encrypted by transforming the image in the frequency domain. This image encryption technology requires a large amount of calculation. The encryption technology based on image secret segmentation and sharing completes image encryption through segmentation and merging [17]. Ahmad et al. completed the storage, hiding, and transmission of shadow images through image segmentation and sharing [18]. Liang et al. proposed a more economical and effective encryption processing method by studying image secret sharing technology [19]. Huang et al. designed a new image encryption algorithm based on a two-dimensional (2D) chaotic map and image segmentation, which is highly secure [20]. There is a certain amount of resource waste in the technology based on image secret segmentation [21]. Image encryption technology based on information hiding was proposed in the 21st century, which is mainly based on the insensitivity of human vision [22]. Based on this algorithm, scholars have designed a reversible information hiding algorithm based on double chaotic encryption and obtained high lossless image restoration [23]. However, the image encryption technology based on information hiding often has the problem of excessive load and low security [24]. Doanh proposed an image encryption algorithm based on a chaotic neural network, which has a large key space and strong security [25]. Sansone et al. studied the application of chaotic sequences in image encryption and found that chaotic sequences are suitable for image encryption, which can make the encryption method more secure and reliable [26].

Based on the above description, the conventional image encryption algorithms have certain shortcomings, such as a large amount of computation, low security, and degraded image quality. The chaotic sequence has been proved to be suitable for image encryption, so the image encryption algorithm will be designed based on the chaotic sequence. The research will be applied to the security management of public big data and is expected to provide a reference for the development of the privacy protection field of the WSN.

3. Image Encryption Algorithm Based on Chaos System

3.1. Research Basis of the WSN. The WSN is a data support technology in the IoT technology, and its main function is to collect, store, and manage data [27]. The wireless network is composed of many tiny sensor devices, mainly deployed in the field environment [28]. The connection methods of sensors in wireless networks are distributed and centralized [29]. The node of the sensor is the bottom layer of the WSN, and the performance of the node is the decisive factor for the stability and speed of data acquisition in the entire WSN [30]. The structure and characteristics of the WSN are shown in Figure 2 [31].

In Figure 2(a), the components of a WSN include raw data, aggregated data, leaf nodes, aggregation nodes, and base stations. Nodes of sensors are able to convert certain physical parameters sensed into electrical signals, which are sent to the base station by radio. A WSN consists of a large number of hardware nodes. Figure 2(b) denotes the characteristics of the WSN, including that the WSN is a peer-to-peer network; the position between the nodes of the WSN will not change after the topology is constructed; the data processing of the nodes requires a simpler algorithm; the random distribution is relatively dense; the main communication method between the nodes of the WSN is
broadcasting; the WSN has the function of automatic topology, and the focus in the WSN is data [32].

The structure of nodes of the wireless sensor is shown in Figure 3.

In Figure 3, the nodes of the wireless sensor include four modules, namely, an energy supply module, a wireless communication module, a Central Processing Unit (CPU) module, and a sensor module. Each node of a wireless sensor is similar to a microcomputer. In the specific implementation, the specific architecture is different, but the characteristics are similar. All are composed of a huge number of hardware nodes, which are eventually used to collect surrounding information. The study is carried out on the basis of Figure 3.

New ideas and new algorithms are constantly being proposed in WSN. For example, Lv and Kumar proposed a software-defined solution for WSN [33]. The basic characteristics of the algorithms need to be verified with the help of the simulation platform of the WSN. The commonly used simulation software includes Tiny OS Simulator (TOSSIM), Network Simulator Version2 (NS2), and AvroraZ [34]. Based on the characteristics of TOSSIM, which can provide visualization tools and easy parameter setting [35], the algorithm simulation is carried out under the TOSSIM platform.

3.2. Design of Image Encryption Algorithm. Image encryption belongs to the new field of cryptography and information security. Cryptography includes cryptanalysis and cryptography, and the components of cryptographic encryption algorithms include decryption algorithm, ciphertext, key, and plaintext [36]. Cryptanalysis is the technology and science of deciphering passwords. The commonly used
methods of cryptanalysis attack are as follows: ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack. In this research, the ciphertext in image encryption refers to the encrypted image, and the plaintext in image encryption refers to the original image.

Chaos systems have the characteristics of orbit unpredictability, good pseudorandomness, and parameter sensitivity and can be well combined with cryptography. Chaos cryptography has become a new research field of current cryptography. Chaos encryption is to superimpose one or more chaotic signals on the plaintext. The chaos generator will generate a chaotic sequence, which is the encryption key of the plaintext. Finally, the ciphertext is transmitted through the transmission channel.

The image encryption algorithm uses a chaotic map, including a Logistic map, Chebyshev map, and Cat map. A Logistic map is a typical nonlinear chaotic equation, and the generated chaotic sequence has good randomness. Its definition is shown in equation (1).

\[
x_{n+1} = \delta x_n (1 - x_n), \quad x_n \in [0, 1].
\]  

In equation (1), \(x_n\) represents the \(n\)th iteration of the Logistic chaotic map, and \(\delta\) is the system parameter. The sequence \(\{m_n\}\) of the Logistic chaotic map is randomly distributed in the interval \([0, 1]\).

The Chebyshev chaotic map has long-term unpredictability and good initial value sensitivity of chaotic sequences and is suitable for generating chaotic sequences controlled by keys. The definition of the Chebyshev chaotic map is shown in equation (2).

\[
x_{n+1} = \cos (\arccos(x_n)), \quad x_n \in [-1, 1].
\]  

Cat map is a chaotic system that iterates the plaintext as the initial value of the chaotic system. The dynamic equation of the Cat map is shown in (3).

\[
\begin{bmatrix}
x_{n+1} \\
y_{n+1}
\end{bmatrix} = \begin{bmatrix}
1 & c \\
d & cd + 1
\end{bmatrix} \begin{bmatrix}
x_n \\
y_n
\end{bmatrix} \mod D.
\]  

In equation (3), \(c\) and \(d\) are positive integers, \(0 \leq n \leq D - 1\), and \(D\) is the width of the image matrix. Mod represents the remainder function. Cat map has good chaotic properties, and its inverse matrix is shown in equation (4).

\[
\begin{bmatrix}
x_{n+1} \\
y_{n+1}
\end{bmatrix} = \begin{bmatrix}
1 & -c \\
-d & 1
\end{bmatrix} \begin{bmatrix}
x_n \\
y_n
\end{bmatrix} \mod D.
\]  

Image encryption technology under a chaotic system has faster encryption and decryption speed and larger key space. The steps of encrypting the image by the chaotic system are as follows: firstly, the chaotic sequence generated by the chaotic system is used as the key; secondly, the key is used to diffuse and scramble the plaintext image through the chaotic map; finally, the ciphertext image is obtained.

3.3. The Color Image Encryption Algorithm Based on Double Chaotic Cross-Diffusion. A color image encryption algorithm
based on double chaotic cross-diffusion is proposed. Since most of the images to be encrypted in daily life are color images, such as Hu et al. pointed out that for medical image processing research, the samples are all color images [37]. And people often use mobile platforms in daily life. The proposed algorithm is only suitable for color image encryption on mobile platforms.

Due to the limited processing power and computing power of mobile devices, a chaotic sequence is generated by crossing the Chebyshev chaotic map and the Logistic chaotic map. The keys of the chaotic system are the chaotic sequence and control parameters. Color image pixel encryption is performed based on the key, and the encryption channel is three channels of Red Green Blue (RGB), and then, the cross operation of the three channels is performed. Finally, the diffusion is realized. The encryption principle of the Logistic-Chebyshev cross-diffusion is shown in Figure 4.

Both the Logistic map and the Chebyshev map in Figure 4 require control parameters of initial values, so there are two “control parameters of initial value” in Figure 4. Since the Logistic-Chebyshev is a low-dimensional hybrid chaotic encryption algorithm, it is suitable for encrypting digital images on mobile devices.

The studied mobile device uses the Android operating system, so considering the requirements for image encryption security and encryption and decryption speed, this research designs a color image encryption algorithm based on the dual-chaotic cross-diffusion of the Android platform.

The process of the encryption algorithm is as follows: first, the initial keys and control parameters of the Chebyshev chaotic map and the Logistic chaotic map are randomly generated; then, the two chaotic maps are used for \( n \) iterations, respectively, until the transient effect is eliminated and the avalanche effect is enlarged. The Chebyshev chaotic map is used to iterate the absolute value and the Logistic chaotic map for 3 more iterations, and the iteration result is an initial key of the RGB channel encryption. The pixels in the image are taken to confirm the parity of the corresponding value of the pixel position. If it is an even number, the Logistic chaotic map iteration is used to finally obtain the encryption key. If it is an odd number, the Chebyshev chaotic map iteration is used to finally obtain the encryption key. The current color channel and the last encrypted color channel are combined to perform an exclusive OR operation. After all pixel points are processed, the final encrypted image is obtained.

The specific steps of the designed color image encryption algorithm based on double chaotic cross-diffusion are as follows. (1) The digital image is taken, and its pixel values are converted into a one-dimensional matrix. (2) The control parameters of the Chebyshev chaotic map and the system parameters of the Logistic chaotic map are randomly generated, and the two maps are in a chaotic state. (3) The initial keys of the two chaotic maps are randomly generated. (4) The initial key of the Logistic chaotic map in the previous step is iterated, the Logistic chaotic map is iterated \( n \) times,
the Chebyshev chaotic map is iterated 3 times, and then, the Logistic chaotic map is iterated 3 times and saved. (5) The initial key of the Chebyshev chaotic map in the previous step is iterated, the Chebyshev chaotic map is iterated \( n \) times, the Logistic chaotic map is iterated 3 times, and then, the Chebyshev chaotic map is iterated 3 times and saved. (6) The pixel points are taken according to the order of the pixel points, and the parity of the pixel points is determined. If it is an odd number, the result generated in step (4) is used as the key iteration, the iteration result is recorded and saved. XOR operation is performed on each color channel, and the encrypted pixel points are diffused. If it is not the first pixel point, the pixel point component being encrypted is XORed with the pixel point component of the previous position, respectively. (7) If the pixel is an even number, the result generated in step (5) is used as key iteration, and other operations are the same as step (6). (8) Steps (6) and (7) are repeated until all pixels are processed, and the ciphertext image is finally output.

The equations involved in step (6) are shown in (5)–(10).

\[
I_g(R) = \text{Chebyshev}'[0] \oplus I_g(R). 
\] (5)

In equation (5), \( I_g(R) \) represents a digital image, \( g \) means the position of the current pixel is odd, \( R \) expresses red, and \( \text{Chebyshev}'[0] \) is the result of the first iteration in step 6.

\[
I_g(R) = \text{Chebyshev}'[1] \oplus I_g(R). 
\] (6)

In equation (6), \( \text{Chebyshev}'[1] \) is the second iteration result in step 6.

\[
I_g(R) = \text{Chebyshev}'[2] \oplus I_g(R). 
\] (7)

In equation (7), \( \text{Chebyshev}'[2] \) is the result of the third
iteration in step 6.

\[ I_g(R) = I_g(B) \oplus I_{g-1}(R), \quad (8) \]

\[ I_g(G) = I_g(R) \oplus I_{g-1}(G), \quad (9) \]

\[ I_g(B) = I_g(G) \oplus I_{g-1}(B), \quad (10) \]

In equations (8) and (10), \( G \) represents green and \( B \) represents blue.

The decryption algorithm is completed on the basis of the encryption algorithm. The decryption process is the inverse process of encryption. The space complexity and time complexity of the decryption algorithm are the same as those of the encryption algorithm. Therefore, the steps of the decryption algorithm based on double chaotic diffusion are also the steps of the encryption algorithm. It is not repeated here.

Since most of the images of public big data involve privacy and are difficult to obtain, and these images are mostly color images, the image form has little effect on the experiment. Therefore, the color image of open-source data is used to replace the images of public big data to conduct experiments. The encryption effect verification of the designed algorithm adopts the flower pattern in the open source digital image dataset “102 Category Flower Dataset” to display the encryption effect and decryption effect. There are two images showing the encryption and decryption effects.

3.4. Design and Reliability Research of Evaluation System of Image Encryption Algorithm. To test the performance indicators of different algorithms, an image encryption algorithm evaluation system is designed. The system includes a valuation platform and realization platform of an encryption algorithm. The image encryption algorithm mainly completes the effect preview and performance parameter calculation of different image encryption algorithms. The encryption algorithm comparison evaluation platform mainly compares the parameters and the two algorithms.

The reliability analysis and security analysis of the algorithm will be carried out on three platforms, including Windows platform, mobile platform, and TOSSIM platform based on WSN. The experimental environment of the three platforms is shown in Table 1.

The correlation of adjacent pixels is an important evaluation index for the security of image encryption algorithms. The calculation of pixel correlation analysis is shown in equations (11)–(15).

\[ f_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)} \sqrt{D(y)}}, \quad (11) \]

In equation (11), \( x \) and \( y \) are two adjacent pixel pairs, \( f \) is the correlation coefficient, \( D \) is the variance, and \( \text{cov}(x, y) \) is
In equation (12), $U$ is the mean value, $N$ is the number of adjacent pixel pairs, and $i$ is the serial number.

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - U(x))^2.$$  \hfill (12)

In equation (12), $U$ is the mean value, $N$ is the number of adjacent pixel pairs, and $i$ is the serial number.

$$\sqrt{D(x)} \neq 0 \text{ and } \sqrt{D(y)} \neq 0,$$  \hfill (13)

$$U(x) = \frac{1}{N} \sum_{i=1}^{N} x_i,$$  \hfill (14)

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - U(x))(y_i - U(y)).$$  \hfill (15)

2,000 pairs of adjacent pixels are selected from the "102 Category Flower Dataset" flower dataset, and their correlations in the diagonal, vertical, and horizontal directions are calculated. In the flower dataset, 3,000 pairs of adjacent pixels are randomly selected. Combined with equations (12)–(15), the pixel correlations in three directions are calculated and compared with the algorithm results in the literature.

The information entropy can be used to evaluate the randomness of the image, and the calculation of the covariance.
Information entropy is shown in equation (16).

\[ E(X) = -\sum_{i=1}^{n} p(x_i) \log_2 p(x_i). \]  

(16)

In equation (16), \( x_i \) represents the gray value of the image pixel. \( i \) is the serial number of the image pixel. \( p \) stands for the ratio. \( E \) is the information entropy, \( 0 \leq E \leq 8 \), and \( n \) is the number of image pixels. The greater the information entropy, the better the randomness of the image and the better the performance of the encryption algorithm.

In the evaluation of information entropy, on the basis of the flower dataset, the “Dogs vs. Cats” dataset is also added for experimental comparison. The information entropy before and after encryption of the algorithm on the cat and dog image dataset is compared with the literature algorithm.

Differential attack is mainly used to change the context of ciphertext. It contains two indicators, Unified Average Changing Intensity (UACI) and Number of Pixels Change Rate (NPCR). The calculation of UACI is shown in equation (17).

\[ UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%. \]  

(17)

In equation (17), \( M \times N \) indicates the image size. \( Q_1 \) is the ciphertext image matrix before the image is changed, and \( Q_2 \) is the ciphertext image matrix after the image is changed. The ideal value for UACI is 33.33%.

The calculation of NPCR is shown in equations (18) and (19).

\[ NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%, \]  

(18)

\[ D(i, j) = \begin{cases} 1, C_1(i, j) \neq C_2(i, j) \\ 0, C_1(i, j) = C_2(i, j) \end{cases}. \]  

(19)

In equations (18) and (19), \( D(i, j) \) is a secondary matrix, and the ideal value of this indicator is 100%. \( C \) refers to the pixel value.

One image from each of the two datasets is selected. Pixel points are randomly selected, changing the pixel value. The same key is used to encrypt the plaintext images before and after the change, and then, the index values of UACI and NPCR are calculated.

The Labelme dataset is also selected to evaluate the sensitivity of encryption algorithms. All images in the dataset are evaluated, and one pixel of the original image is randomly changed to encrypt, and the differential attack index between the corresponding two password images is calculated. Based on the mobile platform, the algorithm execution efficiency is evaluated. The experimental pictures are randomly selected from the three datasets, a total of three pictures.
4. Result Analysis of Image Encryption Algorithm Based on Double Chaos Cross-Diffusion

4.1. Effect Verification of Image Encryption Algorithm and Encryption Platform. The performance verification of the encryption and decryption algorithm is based on the Android platform. Thus, the experimental environment is the CPU HiSilicon Kirin 960 with 8 cores, the operating system is Android 7.0 or above, the main frequency is 2.5 GHz, and the RAM is 4GB. To evaluate the encryption and decryption effect of the designed algorithm and exclude the influence of more variables, the same image is used as the function evaluation of the encryption and decryption algorithm. The effect of the designed image encryption and decryption algorithm based on double chaotic cross-diffusion is shown in Figures 5 and 6.

It can be obtained from Figures 5 and 6 that the encryption effect and decryption effect of the designed algorithm are good. The encryption effect of Figure 5(b) is good, and the image information is well protected. In Figure 6(b), the decrypted image completely restores the original image information. It is preliminarily demonstrated that the designed image encryption algorithm based on double chaotic cross-diffusion has a good effect.

The calculation results of the correlation coefficient before and after the encryption of the image encryption algorithm in realization platform are shown in Figure 7.

Figure 7 manifests that in the designed image encryption platform, encryption is performed in different directions for the three color channels, and the encryption effect is good. The correlation coefficient before encryption is around 0.96, and the correlation coefficient after encryption is about 0.01. Since the correlation coefficient is an important evaluation index for the security of the image encryption algorithm, the smaller the correlation coefficient, the higher the security of the image encryption algorithm, so the designed image encryption algorithm is more secure.

The result comparison and the information entropy comparison of the encryption algorithm comparison evaluation platform of the correlation coefficient of the adjacent pixels are shown in Figures 8 and 9.

In Figures 8 and 9, the results of the encryption algorithm comparison evaluation platform AES algorithm encryption and the designed algorithm encryption are well reflected, indicating that the algorithm comparison platform has good practicality. The following subsections will conduct specific performance evaluation of the designed algorithm.

4.2. Reliability Results of Image Encryption Algorithms. The comparison of the correlation coefficients of adjacent pixels before and after each channel encryption of the constructed image encryption algorithm is shown in Figure 10.

Figure 10 illustrates that after the image is encrypted, the correlation of adjacent pixels is significantly reduced. No matter from the horizontal, vertical, or diagonal direction of the color channel, the law that the correlation of adjacent pixels decreases is established. The correlation coefficients of adjacent pixels in the three directions of the original image are between 0.77 and 0.94. After encryption, the correlation coefficients of adjacent pixels in the three directions of the encrypted image are between 0.001 and 0.02. It can be seen that the correlation coefficient has dropped significantly, indicating that the encryption algorithm is more secure.

The algorithm compares the correlation of pixels in the horizontal, vertical, and diagonal directions with the literature algorithm, and the results are shown in Figure 11.

Figure 11 indicates that the correlation of adjacent pixel pairs in three directions in the first three channels of the image is highly correlated. After the designed algorithm is encrypted, the correlation coefficient value of adjacent pixel pairs is greatly reduced, and the maximum reduction is 0.97. The results of the literature algorithm and the designed algorithm are relatively close, but the designed algorithm is still better than the literature algorithm, and the difference is about 0.1. It shows that the designed algorithm has a good statistical characteristic diffusion on the original image and further enhances the invisibility of the plaintext. The algorithm has a great resistance to statistical analysis.

The comparison of the information entropy between the designed algorithm and the literature algorithm is shown in Figure 12.

The data with asterisks in Figure 12 is the data of dataset 2. It can be seen from the content in Figure 12 that the
information entropy of the red, green, and blue channels before encryption is lower than the information entropy of the three-color channel after encryption. The information entropy value of the designed algorithm is not much different from the literature value. However, the information entropy of the designed algorithm is higher than the literature value, and this algorithm is closer to 8, which is the optimal value of the information entropy, indicating that the designed encryption algorithm has a better random sequence of pixels.

The results of UACI and NPCR for the three channels of the two types of images are shown in Figure 13. The data with asterisks in Figure 12 is the data of dataset 2. Figure 13 demonstrates that for the UACI index value and the NPCR index value, the values of the designed algorithm are higher than those of the literature algorithm. The average UACI of the designed algorithm is 99.62%, while the average UACI of the literature algorithm is 98.33%. The NPCR value of the designed algorithm is 33.52%, and the NPCR value of the literature algorithm is 31.23%. It shows that the designed algorithm can effectively resist differential attack analysis.

The average efficiency of encryption and decryption of the image encryption algorithm on the three platforms is shown in Figure 14.

Figure 14 means that the time of encryption and decryption of the designed algorithm is shorter than that of the literature algorithm. For image 1, the time of encryption and decryption of the designed algorithm is 0.05 s, while the time of encryption and decryption of the literature algorithm takes 0.26 s and 0.27 s, respectively. For image 2, the designed algorithm takes 0.03 s, and the literature algorithm takes 0.05 s. For image 3, the literature time takes 0.3 s, while the designed algorithm takes 0.25 s. It can be seen from the overall point of view that the encryption and decryption time of the designed algorithm is better than that of the literature algorithm, and the encryption and decryption time is less than 1 second, indicating that the designed algorithm will be widely used in the three platforms.

A number of research results are analyzed, and the conclusion is drawn that the designed image encryption algorithm based on double chaotic cross-diffusion has good performance from the content in Figures 5 and 6. From Figures 7–9, it is concluded that the image encryption algorithm based on double chaotic cross-diffusion has good security and the encryption platform has strong practicability. From Figures 10–14, it demonstrates that the designed algorithm has great resistance to statistical analysis, good randomness of the pixel sequence of the encryption algorithm, strong resistance to differential attacks, and can be well applied in Windows platform, mobile platform, and TOSSIM platform. Therefore, it is concluded that the designed image encryption algorithm based on double chaotic cross-diffusion has good performance.

5. Conclusion

Based on the weak security of data encryption in current WSN, a chaotic system is introduced to analyze the security of public big data of widely used images from the perspective of smart devices. By the introduction of current image encryption algorithms, their shortcomings are compared, and the idea of applying a chaotic map to image encryption is proposed. According to this, an image encryption algorithm of double chaotic cross-diffusion is designed, and an algorithm comparison platform is constructed. The designed algorithm and the performance of the algorithm comparison platform are analyzed. Finally, the superiority of the designed algorithm is shown. The encryption and decryption of the designed algorithm are within 1 second, and the encryption and decryption efficiency are high. The research provides a reference for the security processing of image data in WSN and provides a development direction for the application of chaotic systems in image encryption algorithms. It provides favorable thinking for the security of public data and also provides reasonable suggestions for the development of image encryption in the era of smartphones. The practical significance is that it can be applied to the security field of public images to better protect people’s privacy. There are still some shortcomings, for example, the image data of different pixels is not subdivided, and the performance verification of the designed algorithm is not specific enough. The tight integration of content and WSN still needs to be improved. Therefore, in the follow-up research, image data with different pixel sizes will be classified, processed, and evaluated, and more algorithm performance evaluations will be added. The combination of content and wireless sensor network is also added, so that the content can better serve the comprehensive development of the wireless sensor network. And the constructed algorithm can be widely used in practical fields, such as medical image, big data processing, and other public fields.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References


