Application of Information Security in Image Encryption Processing Based on Big Data

Haicui Lv

Haojing College of Shaanxi University of Science & Technology, Shaanxi, China

*Corresponding author e-mail: zengrong@swufe.edu.cn

Abstract. With the widespread application of Internet technology, digital image encryption needs to be completed. But image is different from text, it has many inherent characteristics, such as large amount of image data, high redundancy, strong correlation between adjacent pixels. Therefore, the traditional symmetric encryption algorithm data encryption standard and advanced data addition standard will no longer be suitable for image encryption. Based on the concept of information security and image encryption, a new image processing method is proposed in this paper, which is based on the logistic tent sine composite algorithm model. The compression ratio is 75%. When the wrong key is input, the PSNR of the algorithm reconstruction result is only about 5dB, and the reconstruction error error is only 1, so the encryption effect of the model is better.

Keywords: Image Compression Encryption; Internet Technology; Image Information; Information Security

1. Introduction

The popularity and popularity of e-commerce is due to the rapid development of electronic technology and Internet. As the main part of e-commerce, e-commerce platform appears in front of people with unique trading mode, becoming the dominant trade mode and gradually occupying the leading position of people's life. The reason why e-commerce platform can be received and widely used in a short time. However, e-commerce platform is mixed. With the popularity of e-commerce platform, the problem of information security is also emerging. While Taobao, Jingdong and other large-scale e-commerce platforms provide users with more channels for trade negotiation, information security incidents emerge in an endless stream. Therefore, people from all walks of life hold a high degree of attention to the information security of e-commerce platforms [1]. Information security in e-commerce platform is not only related to the interests of businesses and consumers, but also affects the development of e-commerce platform to a certain extent. Therefore, the problem of information security in e-commerce platform needs to be solved.

With the rapid development of digital communication technology, multimedia data, especially image data, is growing and becoming an inseparable part of us. It also plays an important role in the fields of national defense, medical treatment, education and remote sensing, which puts forward higher requirements for the network bandwidth of image data transmission. However, mobile storage devices can not meet the requirements of such a large data storage. This phenomenon brings new challenges.
In the process of signal sampling, only when the sampling rate is greater than or equal to the Nyquist sampling rate (twice the bandwidth), can the reconstructed signal not lose the original information, so as to accurately recover the original signal [3]. The rapid development of information technology greatly affects our life. In this era of information explosion, people's demand for information is increasing, and the bandwidth of the signal is becoming wider and wider. If we continue to use Nyquist sampling theorem to process the signal, it will put forward higher requirements for hardware facilities and equipment. From the current point of view, the existing hardware facilities and equipment is difficult to meet the needs of applications, and the implementation cost of such hardware facilities and equipment is very high. At present, a better solution is to make full use of the huge storage space of cloud services, and there are also problems in this way. An important requirement for users is to use cloud storage services on the premise of ensuring the security of personal data [4].

With the advent of the 21st century, computer and network technology are not the same as before, and the business model has changed unprecedentedly. Most of the traditional markets are gradually replaced by e-commerce. People can realize the retrieval, collection, transmission and sharing of data and information through the Internet platform. However, the problem of information security is also slowly exposed. Based on the application of information security in image encryption processing under the background of big data, this paper analyzes and improves the new image encryption processing algorithm by elaborating the related concepts of information security and image encryption processing. Through the analysis of the actual test results, the algorithm can better process the information and achieve the desired effect.

2. Related Concepts of Information Security in Image Encryption Processing Under the Background of Big Data

2.1. Compressed Sensing and Image Encryption

The characteristic of compressed sensing is that it can process the signal with a new signal sampling method, and reconstruct the original signal through the corresponding algorithm. It includes three steps: sampling, transmission and reconstruction. This approach is very similar to the symmetric encryption model. Through analogy, it is very easy to find that if the compressed sensing measurement matrix can not only measure the matrix, but also give it security, it can achieve the purpose of encryption. Therefore, in terms of image encryption, the theoretical model of compressed sensing is very suitable and has inherent advantages. The current mainstream encryption method is based on the above analysis, through the data scrambling encryption and measurement matrix security processing, to achieve digital image encryption based on compressed sensing. However, only improving in this area can not achieve satisfactory encryption effect. In addition, the reconstruction quality of compressed sensing is also closely related to the measurement matrix. Therefore, it is necessary to improve and improve this kind of model [8].

2.2. Detailed Steps

Encryption process: the algorithm is divided into three steps

(1) Compression operation: the original image is compressed by two-dimensional sine logic modulation mapping.

(2) Diffusion operation: the pixel value of the compressed image is changed by XOR between the sequence generated by two-dimensional sinusoidal logic modulation mapping and the compressed image.

(3) Permutation operation: chaotic sequence generated by two-dimensional sinusoidal logic modulation map changes the pixel position of diffusion image.

Compression process: we define the original image as X (x ∈ RN × n), ψ (ψ ∈ RN × n) as the orthogonal matrix, and the transformation coefficient as α (α ∈ RN × n). The first step: the original image x is transformed into the ψ domain to obtain the transformation coefficient α, which can be completed by discrete cosine transform, Fourier transform and discrete wavelet transform. The second
step is to construct the measurement matrix by two-dimensional sinusoidal logic modulation mapping. Diffusion process: the diffusion process can greatly change the statistical characteristics of the original image, such as the histogram of the original signal and the correlation coefficient between pixels change.

Replacement process: in the algorithm proposed in this chapter, the purpose of replacing the output image is to achieve better encryption effect and make the algorithm achieve higher security level. Given the initial value, two sets of sequences with length of M × n are generated by two-dimensional sinusoidal logic modulation mapping. The index sequence s is obtained by taking the mean value of the two groups of chaotic sequences, and the final encrypted image C is obtained by changing the pixel position of the image.

Decryption process: decryption process is the reverse process of encryption process. The sender transmits the key to the receiver through the secure channel. The receiver obtains the Q 'through the reverse permutation process, and then obtains y' by the anti diffusion process. Finally, the reconstructed image X is obtained by sl0 reconstruction algorithm.

2.3. Information Security
The concept of information security has existed for a long time in history. In the 1990s, information security developed steadily. However, with the advent of the 21st century, with the development of information technology, information security issues become more and more important. Information security refers to the information system (including hardware, software, data, personnel, natural environment and infrastructure) damaged, modified or continuously operated due to accidental or malicious leakage. In the final analysis, it is the continuity of information activities [9].

2.4. Basic Requirements for Information Security
(1) Confidentiality. Confidentiality means that information is not allowed to be transmitted or disclosed to any entity or individual in any way. This is the most important requirement of information security. For example, investigations, transactions and e-commerce contracts involve many trade secrets and the private life of the public. If the account number and credit card user name are known, they may be stolen. Therefore, in order to ensure the security of e-commerce, we must prevent illegal access to information and theft of leaked information in the process of transmission.

(2) Reliability. Reliability is to ensure that the information system can continue to work with acceptable quality. The actor shall be responsible for his information action and shall not deny the action taken or the information received from the other party [10].

2.5. Information Security Mechanism
The means used to protect information security is also called information security mechanism. The establishment of information security mechanism is closely related to the development of network. At present, information security mainly includes encryption, security authentication, access control, integrity, inaccessibility, notarization and routing control mechanisms. The function of security mechanism is to protect the system from being monitored, to prevent the system from being attacked and to recover after being attacked. Therefore, the design of information security mechanism is to protect information from attack and prevent information security from being attacked. The establishment of mechanism depends on the legal system and system. In other words, only through the establishment of a corresponding mechanism can it play a role in practice. Information security mechanism is to protect the security of information through appropriate institutions and systems.

2.6. Correlation Formula Algorithm
(1) Logistic mapping

\[ x_{n+1} = \lambda x_n (1 - x_n) \]  

(2) Tent mapping
sparse reconstructed compare

4.1. Practice

4. Based on the Background of Big Data, Information Security in Image Encryption Processing Practice

The image is divided into a group of sensitive image data and a large group of insensitive image data by using sensitivity recognition method, which are stored in private cloud and public cloud respectively. The processing method is that the sensitive image data is encrypted in the counter mode, and the insensitive image data is processed by permutation diffusion sampling operation. Once the user requests the image data, the public cloud provides the reconstruction service to compress the insensitive image data, and the private cloud decrypts the sensitive image data and the anti diffusion and anti replacement operation of the insensitive image data. Finally, the decrypted sensitive image data and non sensitive image data are combined into a complete image.

We design an efficient security image service framework for users through hybrid cloud. Firstly, the private cloud divides the image into sensitive image data and non sensitive image data. This partitioning method can be chosen by the private cloud, which depends on the needs of users. In this chapter, we take the edge and contour of an image as an example. Digital display selective edge detector is used to distinguish sensitive image data from insensitive image data. Sensitive image data accounts for a small percentage of the image, while the rest of the image data is considered to be insensitive. Secondly, the insensitive image data is encrypted properly, and then the permutation diffusion encrypted image data is compressed by linear observation. The compressed measurements are transferred to the public cloud for storage. Sensitive image data is encrypted directly and stored in private cloud. Finally, once the user's request is received, the public cloud uses the reconstruction algorithm to transfer the decompressed image data to the private cloud. Private cloud decrypts the encrypted sensitive image data and non sensitive image data anti diffusion and anti replacement operations, and then the decrypted sensitive image data and non sensitive image data are assembled into the whole image.

4. Based on the Big Data Background, Information Security in Image Encryption Processing Practice Results Analysis

4.1. Model Reconstruction Results

| Picture    | PSNR | PSNR NS+randomization | ERROR | ERROR NS+randomization |
|------------|------|-----------------------|-------|------------------------|
| Barbara    | 32.3499 | 33.5584                   | 0.0486 | 0.0423                   |
| Camera     | 32.8472 | 33.3720                   | 0.0433 | 0.0408                   |
| Gold hill  | 32.1365 | 32.6578                   | 0.0515 | 0.0485                   |
| Lena       | 35.4059 | 36.4325                   | 0.0293 | 0.0297                   |
| Peppers    | 34.4008 | 35.2643                   | 0.0362 | 0.0328                   |
| Barbara    | 32.3499 | 33.5584                   | 0.0486 | 0.0423                   |

In order to quantitatively compare the experimental results, we choose to use PSNR and error to compare the quality of reconstructed images. As shown in Table 1, we give the reconstruction results corresponding to the test images. By comparison, it is not difficult to find that the PSNR of the reconstructed image is increased by 0.5db-1.2db when the model uses noise integer algorithm and sparse data randomization.
4.2. Comparison of Image Compression Models and Existing Algorithms Based on Compressed Sensing and DRPE

Table 2. Comparison of Image Compression Encryption Model and Existing Algorithms Based on Compressed Sensing and DRPE

| Algorithm | Ref. [61] | Ref. [62] | Ref. [63] | Ref. [64] | Ref. [65] |
|-----------|-----------|-----------|-----------|-----------|-----------|
| PSNR      | 25.99     | 26.00     | 32.50     | 33.53     | 36.43     |

Taking Lena image as an example, the algorithm is used to compress and encrypt the image, and the compression ratio is 75%. Table 2 shows the comparison results of the reconstruction effect between the proposed model and the existing algorithms. In this chapter, we found that the compression efficiency of the proposed algorithm is better.

4.3. Key Security and Key Space Analysis

Figure 1. Error Key Reconstruction Result

Figure 1 shows the PSNR, error, and NC corresponding to the error decryption image. As can be seen from Figure 1, when the wrong key is input, the PSNR of the reconstruction result is only about 5dB, and the reconstruction error error is only 1, and it is difficult to see any information of the original image by naked eyes, so the algorithm proposed in this paper has good security.

4.4. Security Analysis of Low Frequency Ciphertext Data
Future research, storage environment.

This paper proposes an image compression encryption algorithm based on compressed sensing and DRPE for different data transmission and storage environment and traditional network transmission environment. Aiming at cloud storage environment, an image compression encryption algorithm based on compressed sensing is proposed. The palmprint feature is embedded into the ciphertext data to realize the function of auxiliary identity authentication and further improve the data security. In the past decade, compressed sensing has had an impact in various fields. Its research on image compression and encryption has been relatively mature, but the one-dimensional chaotic system used is relatively simple, only considering the transmission of encrypted data in the traditional network environment. With the development of cloud computing, its powerful computing power and huge storage space are very consistent with compressed sensing theory. Due to the limited level of academic research, there are still many deficiencies in this paper, which will be improved and perfected in the future research and work.

References

[1] Abduljabbar W K, Abdul-Rahman S, Ramli R. A new processing of chaos-based fast image encryption algorithms[J]. Journal of Theoretical and Applied Information Technology, 2017, 95(11):2473-2479.

[2] Naeem H, Sang J, Abro W A, et al. Message Encryption by Processing Image Using Pseudo Random Key Streams Generation[J]. International Journal of Computer Trends and Technology, 2015, 20(2):78-82.

[3] Assad S E, Farajallah M. A New chaos-based image encryption system[J]. Signal Processing
Image Communication, 2016, 41(C):144-157.

[4] Wadi S M , Zainal N. Decomposition by binary codes-based speedy image encryption algorithm for multiple applications[J]. Image Processing Iet, 2015, 9(5):413-423.

[5] Liu L , Miao S , Hu H , et al. N-phase Logistic chaotic sequence and its application for image encryption[J]. Iet Signal Processing, 2017, 10(9):1096-1104.

[6] Chen J , Zhu Z , Zhang L , et al. Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption[J]. Signal Processing, 2017, 142(jan.):340-353.

[7] Chen, Junxin, Zhu, et al. Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption[J]. Signal Processing: The Official Publication of the European Association for Signal Processing (EURASIP), 2018, 142(1):340-353.

[8] Bao L , Yi S , Zhou Y . Combination of Sharing Matrix and Image Encryption for Lossless $S(k,n)$ -Secret Image Sharing[J]. IEEE Transactions on Image Processing, 2017, 26(12):5618-5631.

[9] Brahimi, Nini, Chahra, et al. Security analysis of a three-dimensional rotation-based image encryption[J]. IET Image Processing, 2015, 9(8):680-689.

[10] Li F , Wu H , Zhou G , et al. Robust real-time image encryption with aperiodic chaotic map and random-cycling bit shift[J]. 2019, 16(3):775-790.