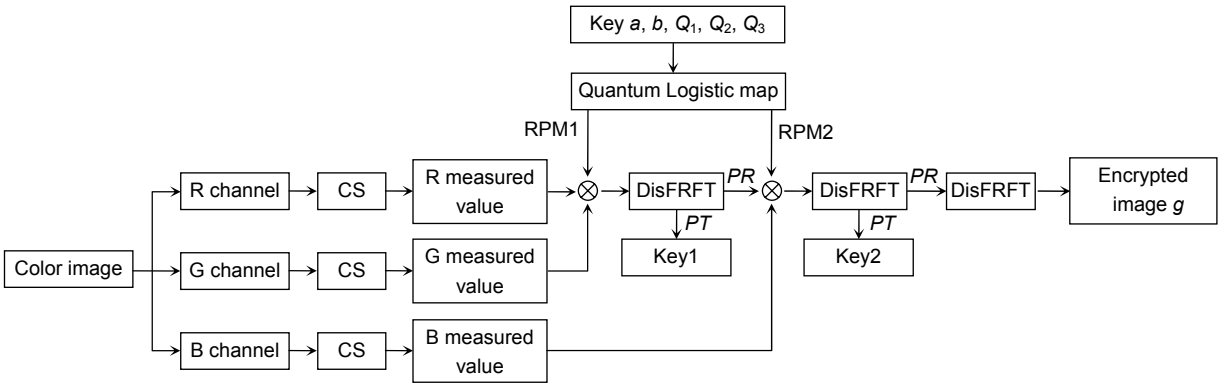
Optical color image asymmetric compressed encryption in fractional Fourier transform domain

Lang Jun*, Fu Xiangxue, Guo Pan

Computer Science and Engineering, Northeastern University, Shenyang, Liaoning 110004, China



The flow diagram of the system for image encryption and decryption

Overview: In recent years, with the development of multimedia technology, various kinds of information such as pictures, videos can be transmitted conveniently and quickly through the internet. People's work and study also increasingly depend on the network and information system. Therefore, the security of information has drawn more and more attention. Image security is especially important because image information can convey people's thoughts more clearly.

In this paper, we present a novel color image encrypted system based on compressed sensing and quantum logistic map. On the one hand, the system significantly decreases the number of transferred data in the cryptosystem; on the other hand, it increases the security of an encryption system. First, two steps are used to reduce the number of data. Step one, color image traditional encrypted process needs to deal with the data of three channels. In order to convert three-channel of color image to single-channel encrypted, we use some mathematical transformations to convert the green channel and the blue channel into two phase masks and add them into the optical cryptosystem. Single-channel can not only reduce the amount of data what it needs to process, it also simplifies the optical encryption system. Step two, this system significantly decreases the number of data processed in the cryptosystem by utilizing compressed sensing (CS). The most attractive characteristic of CS is that with far fewer samples or measurements than traditional Nyquist sampling methods, one can perfectly reconstruct certain signals. The CS also provides a mechanism for data security because the signal can only be reconstructed if the sensing matrix is known. Second, to enhance security, the proposed algorithm increases the robustness of the system used asymmetric optical encryption system based on the phase truncation fractional Fourier transform. This method can make the system resistant to plaintext attacks, and also make the encryption result a real value, which can save storage space and provide convenience in transmission. At the same time, the parameters of fractional Fourier transform are the keys of the cryptosystem, it adds the number of the keys to enhance security. Finally, to simplify the key exchange, we use quantum logistic chaotic to generate the random phase masks. Instead of transmitting the random phase masks which is hard and inconvenient to transmit and save, only five parameters of quantum logistic map are required. The encryption keys of the cryptosystem are the truncated phase, the fractional orders in the fractional Fourier transform and the parameters of quantum logistic map. The results show that this algorithm can obtain better image encryption and decryption results.

Citation: Lang J, Fu X X, Guo P. Optical color image asymmetric compressed encryption in fractional fourier transform domain[J]. *Opto-Electronic Engineering*, 2018, **45**(6): 170732

Supported by Fundamental Research Funds for the Central Universities (N150404004)

* E-mail: langjun@mail.neu.edu.cn