Computers and Electrical Engineering 000 (2017) 1–15

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Research on the improved algorithm for image quantum encryption in multimedia networks☆

Bo Wang[a], Jing Xu[a], Houbing Song[b,*]

[a] Shaanxi Institute of Technology, Xi'an Shaanxi, 710302, China
[b] Department of Electrical and computer Engineering, West Virginia University Institute of Technology, WV 25136, USA

ARTICLE INFO

Article history:
Received 26 August 2016
Revised 18 January 2017
Accepted 18 January 2017
Available online xxx

Keywords:
Multimedia network
Image
Quantum cryptography
Improvement

ABSTRACT

The current image encryption methods do not take into account the characteristics of images, and these algorithms require higher hardware resources. Therefore, this paper presents an improved algorithm for image quantum encryption. Based on the analysis of the classic image encryption method, the physical basis of key generation and distribution of image quantum encryption are introduced, and the single particle key distribution algorithm and the two particles entangled state key distribution algorithm are analyzed. To Judge whether there is an effective way by using two key distribution algorithms, so that it can make the both communicating sides (Alice and Bob) to complete key negotiation and generation by using the unreliable channels, making sure that the absolutely safe of key, and ensuring the security of the image. The experimental results show that the proposed method has high encryption performance, and the security and the ability to resist differential attacks are also very high.

1. Introduction

With the development of computer technology and multimedia technology, the information that people deal with in their daily work tends to be more and more diverse [1]. Obviously, the main way for people to get information is through the eyes to see the image. Image information has many advantages such as vivid, intuition, information amount large and so on. Therefore, images are widely used in all aspects of people's life and work. Especially in the global background of Internet all over the world and the gradual maturity of digital processing technology, the processing and transmission of image in the multimedia network have made great progress in both theoretical research and practical application [2,3]. In some special industries, a lot of information need to be limited to a certain scope including image information. For example, in the military, remote medical, astronomy and geography and many other fields, it requires to do a good job of image security. Thus, it has great significance to make image encryption in the multimedia network and has become the focus of the studies, getting more and more extensive attentions [4,5].

At present, the methods for researching image encryption in multimedia network mainly include the chaos method, the standard method of data encryption and the method of elliptic curve cryptography. Among them, in literature [6], an image encryption algorithm based on chaos theory was proposed. The chaotic iteration function was designed through the tangent function and exponential function, and the chaos sequence was as the key to complete the encryption operations. However,

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. S. Liu.

* Corresponding author.
E-mail addresses: 275494108@qq.com, wb20160408@163.com (B. Wang), Houbing.Song@mail.wvu.edu (H. Song).

http://dx.doi.org/10.1016/j.compeleceng.2017.01.015
0045-7906/

the operation speed of encryption and decryption operation was very slow and inefficiency. Literature [7] proposed a kind of encryption method based on digital image, in which the parameters of the chaotic mapping using random sequence were improved. There was a delay time in the process of converting the chaotic sequence in each subspace, but the delay time had a great influence on the encryption efficiency. Literature [8] proposed an image encryption method based on parameter optimization, according to the sensitive dependence of the initial conditions and the ergodic property of the chaotic orbit, the number of key parameters was increased. However, this method prolonged the period of chaotic sequence, resulting the increase of the whole implementation process. Literature [9] proposed an image encryption method based on Logistic mapping, and the chaos forming sequence was made mapping into the pseudo-random sequence composed of integer, which was as the encryption key distributed in a certain interval, then by Logistic formula, encrypted ciphertext was obtained. But, this method could not reflect the scrambling of iterative chaotic, it was very difficult to achieve. In literature [10], an image encryption method based on Henon map was proposed. The domain and range were made decomposition, to determine the fixed length, and set up the mapping relation between domains of function and sub-rang. Several iterations of Henon mapping of standard text data were made, to complete the encryption process. The Henon inverse mapping of the encryption was performed for several times, to complete decryption. But the method was easy to be cracked, and the security was not enough.

In this paper, an improved algorithm for image quantum encryption is proposed. Aiming at the disadvantages of classical encryption methods, through quantum encryption method, the classical methods are improved. The physical basis of key generation and distribution in image quantum encryption is introduced, and the single particle key distribution algorithm and the two particles entangled state key distribution algorithm are analyzed. Two kinds of key distribution algorithms are used to determine whether the eavesdropper has effective ways to make both Alice and Bob communication using unreliable channel to complete the key consultation and generation. The security of the two kinds of key distribution algorithms is analyzed. The experimental results show that the proposed method has high very encryption performance, and the security and the ability to resist differential attacks are also very high.

2. Classical image encryption method in multimedia network

The classic multimedia network image encryption method is compound chaotic sequence method, and the basic ideas of the method is as follows: according to the principles of that diffusion is the first and scrambling is at last, The role of diffusion is to disperse the plaintext redundancy into ciphertext, which is easy to hide the statistical information of plaintext; the role of scrambling is to cover up the relationship among plaintext, ciphertext and secret key, to become more complex statistical relationship between ciphertext and key, so that the cryptanalyst cannot infer the ciphertext key from the plaintext; in the process of diffusion, there are two chaotic sequences can be to choose to make the image encryption in the network multimedia. A decision condition is set in advance, and when the pixel value of each pixel is diffused, a chaotic sequence is selected according to the establishment of the judgment condition, so that the two chaotic sequences can be taken in turn. To a certain extent, it can be said to encrypt the image randomly, replace the value of each pixel, and complete the diffusion of the image. Then, in the process of scrambling, two chaotic maps are selected to make twice scrambling for the images by different scrambling methods, in the two chaotic sequences, one is one-dimensional Logistic chaotic map, another is two-dimensional Henon chaotic map.

2.1. Diffusion of images in multimedia networks

2.1.1. Two-dimensional logistic chaotic mapping

According to the one-dimensional mapping, the two-dimensional mapping can be obtained

$$\begin{cases} x_{n+1} = 4\mu_1 x_n(1-x_n) + g_1(x_n, y_n) \\ y_{n+1} = 4\mu_2 y_n(1-y_n) + g_2(x_n, y_n) \end{cases} \tag{1}$$

Among them, g_1 and g_2 are as the coupling term, which is desirable in the following two cases: (1) A coupling term of $g_1 = \gamma \cdot y_n$, $g_2 = \gamma \cdot x_n$; (2) Symmetric two coupling terms in $g_1 = g_2 = \gamma \cdot x_n \cdot y_n$. This section uses a two-dimensional logistic mapping with a single coupling form:

$$\begin{cases} x_{n+1} = 4\mu_1 x_n(1-x_n) + \gamma y_n \\ y_{n+1} = 4\mu_2 y_n(1-y_n) + \gamma x_n \end{cases} \tag{2}$$

Its dynamic behavior is determined by the control parameters μ_1, μ_2 and γ, the range is

$$x_n \in (0, 1),\ y_n \in (0, 1).$$

According to the theory of chaos recognition, it is known that whether a system is chaotic or not, the most important one is to calculate the Lyapunov exponent. To this end, it is necessary to analyze the case of the Lyapunov exponent of the two-dimensional Logistic mapping with a coupling term. Take control parameters $\mu_1 = \mu_2 = \mu \in [0.6, 0.9]$, $\gamma = 0.1$, calculate the Lyapunov index, used λ to describe. When $\mu > 0.815$, $\lambda < 0$, then the system is not in a chaotic state; when $\mu > 0.815$, in most cases the $\lambda > 0$, then the system corresponding to the chaotic motion; but in this chaotic zone ($\mu > 0.815$),

Please cite this article as: B. Wang et al., Research on the improved algorithm for image quantum encryption in multimedia networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.01.015