Computers and Electrical Engineering

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 al-gorithm 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 pro-posed 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

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

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

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:

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

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

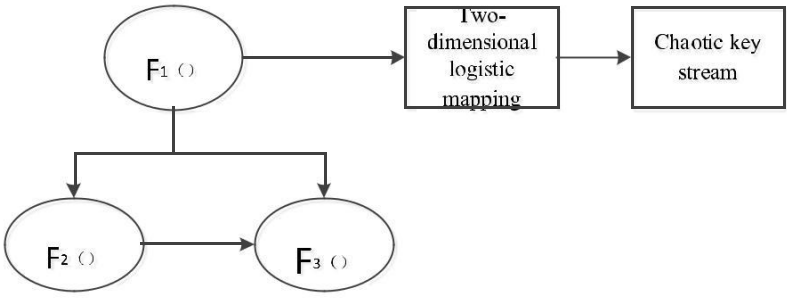


Fig. 1. Complex chaotic mapping.

few very narrow $\lambda < 0$, and the corresponding to chaotic region in the different periods of periodic windows, $\lambda = 0$ is bifurcation point. Discussed in the following based on two-dimensional logistic mapping in image encryption algorithm, we must ensure that the multimedia network is in a chaotic state. Therefore, according to the Lyapunov exponent to select appropriate parameters as a key to the effectiveness at multimedia network working in chaos state and keep the key.

2.1.2. Introduction of diffusion algorithm

Chaotic sequence is used to replace the general pseudo random sequence to realize the secure communication, the chaotic system is referred as a pseudo random sequence generator [11–14]. The chaotic system consists of a discrete chaotic system or a continuous chaotic system. The pseudo random sequence generated by the chaotic system is made XOR op-eration of the plaintext, and then the output will be the ciphertext. This is the original prototype of image pixel diffusion algorithm, but when it refers to realization in computer system, due to the limitation of computational accuracy, it is pe-riodic in essence, and some of the chaotic systems realized in this ways even have a very short period when using the ciphertext and selecting the express attack technology [15–19], this kind of encoding system is easy to be cracked.

Generally, a chaotic map is employed to generate a set of chaotic sequences in image pixel diffusion algorithm, and the diffusion of each pixel is simple using the value of each pixel and the corresponding value of the chaotic sequence to make some kind of operation, such as binary XOR etc. Every pixel value of the image is changed, so does the original image information. When it needs to restore the original image information, the same chaotic sequence to opposite operation is used.

Because Logistic chaotic map is employed to generate a set of chaotic sequences and diffuse the image pixels, the key space is relatively simple and it might be easy to be cracked. In this section, we take the following classical compound chaos mapping algorithm. The algorithm implementation process is shown in Fig. 1. It uses multiple Logistic chaotic maps to generate chaotic key stream by the periodic cycle of each Logistic chaotic map. This method takes advantage of the sensitivity on initial values and parameters of chaotic maps, increasing the complexity of the key stream, and providing a larger key space, which makes each bit of the original text related to multiple bits of the ciphertext and increases the difficulty of breaking the password.

The calculation procedure of chaotic sequence in this section is shown as follows:

Set $m \times n$ gray scale image in multimedia network is G. The two-dimensional matrix of the image is R, R is transformed into one-dimensional matrix, its length is $m \times n$. Settig $R_1 = \{r_1, r_2, , r_i, , r_{m \times n}\}$ and $p = \{p_1, p_2, , p_i, , p_{m \times n}\}$ are as encrypted one-dimensional matrix.

x and y created by two-dimensional logistic chaotic mapping are selected to diffuse pixels value. Firstly, $x = \{x_1, x_2, , x_i, , x_{m \times n}\}$ is used to diffuse.

Then the encryption process is: $p_i = (x_i \times 10 \wedge 5 - r_i) \bmod 256$.

The decryption process is: $r_i = (x_i \times 10 \wedge 5 - p_i) \bmod 256$.

The specific diffusion encryption algorithm is as follows:

(1) Making the original image is as G, the two-dimensional matrix of image data is R which size is $m \times n$, the two-dimensional logistic chaotic mapping will generate a chaotic sequence of x, y which length is $m \times n$, $x = \{x_1, x_2, , x_i, , x_{m \times n}\}$, $y = \{y_1, y_2, , y_i, , y_{m \times n}\}$.

(2) Let $t = \{t_1, t_2,, t_i,, t_{m \times n}\}$, among which, $t_i = x_i - y_i$, the matrix of image data R is transformed into one-dimensional matrix which length is $m \times n$, named as $R_1 = \{r_1, r_2, , r_i, , r_{m \times n}\}$.

(3) $p = \{p_1, p_2, , p_i, , p_{m \times n}\}$ is named as the encrypted one-dimensional matrix. When $t_i \geq 0$, $p_i = (x \times 10 \wedge 5 - r_i) \bmod 256$.

(4) p is transformed into two-dimensional matrix which size is $m \times n$, then to get the two-dimensional image data matrix R_2 corresponding to the encrypted image.

In the third step of the algorithm, there is a judgment condition t which is a $m \times n$-length chaotic sequence. When the diffusion operation is performed on each pixel, firstly it needs to judge whether t_i is greater than 0 or less than 0, then to pick one from the two chaotic sequences to perform the diffusion operation. The method is hard to be broken.

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

2.2. Image pixels scrambling in multimedia network

The basic idea of image scrambling and encryption in multimedia network is to realize the encryption by changing the position of the pixels in the image. When performing the pixel scrambling [20–23], usually the chaotic sequence generator is used to generate the real number sequence, and then perform quantization to generate scrambling address code and change the position of the image pixels [24].

In this section, scrambling encryption is performed on the basis of chaotic diffusion encryption, which will not only effectively expand the key space [25–27], but also have good statistical properties, further improving the anti-cracking ability of the encrypted image [28-30].

Image scrambling technology in multimedia network takes advantage of the digital image with the characteristics of digital matrix, scrambles the pixels position or color in the image, which will disorder the image, and finally to achieve the effect of confidentiality. Position transformation of image pixels is generally more complex, this study combines two algorithms to perform the image pixel scrambling.

The first scrambling algorithm is one-dimensional logistic chaotic mapping and the scrambling procedure is as follows:

(1) A set of chaotic sequences x is generated according to one-dimensional logistic chaotic mapping, $x = \{x_1, x_2, , x_i, , x_m \times n\}$, the chaotic value is sorted from small to large, to get the ordered sequence $x = \{x_1, x_k, , x_p\}$, and record the sequence number in ordered sequence of every x_i from the original sequence. Assuming the first element of original sequence is x_1, its position in ordered sequence is t, the position of the second element is n. Then a sequence of position $w_1 = \{t, n, , q\}$ is formed in which the elements‘ value is integers rang from 1 to $m \times n$.
(2) Assuming the matrix of image data in multimedia network is R which size is $m \times n$, R is transformed into one-dimensional matrix R_1. Making $R_1(i) = R_1(w_1(i))$, then the pixel value scrambling is finished.

In order to have sufficient security and improve the anti-cracking ability of encrypted image, the image needs to be scrambled in the same chaotic system after the first scrambling. Sometimes it takes many times of repeated scrambling to achieve satisfactory results.

The second method used in this section is two-dimensional Henon chaotic mapping, the model of Henon chaotic map-ping system is as follows:

$$\begin{aligned} x_{n+1} &= 1 - a x_n^2 + y_n \\ y_{n+1} &= b x_n \end{aligned} \tag{3}$$

When $0.8 \le a \le 1.4$ and $b = 3$, Henon mapping has chaotic attractor which trajectory is chaotic.

The procedure of scrambling by using the two-dimensional Henon chaotic mapping is as follows:

(1) Assuming the matrix of image data in multimedia network is R which size is $m \times n$. The m-length chaotic sequence $x = \{x_1, x_2, , x_i, , x_m\}$ and the n-length chaotic sequence $y = \{y_1, y_2, , y_i, , y_m\}$ are generated from the two-dimensional Henon chaotic mapping. Same as the first scrambling algorithm, the sequence of x and y is sorted and the position sequence w_2 and w_3 is generated.
(2) The pixel scrambling is performd as follows. Making w_2 and w_3 are as the row sequences and column sequences of the image data matrix R in multimedia network.

```
for i=1:m
for j=1: n
r(i,j)=R(w2(i),w3(j))
end
end
```

The above method generating two groups of chaotic sequences is used to construct scrambling matrix by a two-dimensional chaotic mapping, which will reduce the time of constructing scrambling matrix, and then, it can shorten the time of encryption processing.

Combined with the above two methods, the scrambling methods of this work are as follows: the order of the two kinds of scrambling methods is determined according to a certain decision condition. Assuming k_1 is as the average value of the logistic chaotic sequence x, k_2 is the average value of the Henon chaotic sequence x and y. The size of k_1 and k_2 is judged. If k_1 is larger, the first scrambling is performed by the first kind of scrambling method and the second scrambling by the second kind of scrambling method; if k_2 is larger, the first scrambling is performed by the second kind of scrambling method and the second scrambling by the first kind of scrambling method.

By using different chaotic sequences with different methods, the two times of scrambling are performed, which makes the scrambling effect more ideal than using same chaotic system to perform multiple times of scrambling, and the anti-cracking performance further is improved.

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

2.3. Image decryption in multimedia network

Image decryption algorithm in multimedia network is the inverse operation of image encryption. Firstly, the two-degree scrambling is performed, and then the diffusion operation is performed. In the process of image encryption and decryption, the initial values of the chaotic sequences and the system parameters are consistent.

3. The improved algorithm of image quantum encryption in multimedia network

Multimedia Networks image has the characteristics of high redundancy, large amount of data, and the correlation be-tween the pixels and so on. The current image encryption method which does not consider the characteristics of the image, the key cannot be reused, the cost of hardware resources are more and the encryption time are longer. This paper presents an improved algorithm of image quantum encryption. Quantum cryptography security was guaranteed by the principles of quantum mechanics. There are two types of the basic eavesdropper strategies: The first one is that by measuring the quan-tum state which carries the message, from the measurement results to obtain the required information.However, based on the basic principles of quantum mechanics, that is the Heisenberg uncertainty principle, it shows that the measurement of quantum states would interfere with the quantum state itself, so this is bound to leave a mark eavesdropping that can be discovered by legitimate users.The second one is to copy the quantum state of transmitted message directly, the eavesdrop-per sends original quantum state to the recipient, while leaving the copy of the quantum state is measured in order to steal information, so as not to leave any traces. However, the theorem of quantum no-cloning ensures that eavesdropper can't be successful. Any physical viable quantum copying machine can't clone a quantum state with input identical quantum state.

As the above properties of quantum physics, compared with typical encryption algorithm, quantum encryption algorithm has special advantages: the key can be reused. If a communication error is less than a certain threshold, it can reuses the key after a secret enlargement process, with fully used resources and less energy consumption.

3.1. The physical basis of the key generation and distribution in image quantum encryption

Quantum states in quantum mechanics are the most important concept that can fully describe quantum systems. There-fore, the image encryption process of a quantum system can be completely through the quantum states of the operation to complete. We can use the transferring process of the quantum state from A to B to describe the image transmission from A to B. The image acquisition may correspond to the measurements of quantum states at the same time. The quantum state has a linear superposition.

For the conveniences of analysis, we introduce the concept of quantum bit in quantum information theory. Quantum bit is the base unit in the quantum system describing the image. A quantum bit is the superposition state of two mutual orthogonal intrinsic quantum state, expressed as $a|0> + b|1>$, among them, a and b are coefficients, and $a^2 + b^2 = 1$; It is a two-dimensional Hilbert space vector. According to the characteristics of quantum state, a plurality of quantum bits can be expressed as the tensor product of each quantum bit. Thus, n quantum bits can be described as any quantum state in the

$$|\quad = \quad x{=}00\cdots0 \quad | \qquad x{=}00\cdots0 \; | \; | \; =$$

According to the quantum principle of superposition, blotters & Zurek proposed the theory that unknown quantum state couldn't be completely accurate copied of in 1982, which is the quantum non-cloning theorem. Despite the non-orthogonal quantum states cannot be cloned, Duan and Guo proposed the theory that non-orthogonal quantum states can clone in probability, and give the maximum probability of the non-orthogonal quantum states ($|\psi_0>$ and $|\psi_1>$) which could be cloned to be $\eta = 1/1 + \psi_0|\psi_1$.

When Quantum Systems consist of multiple parts, it will be entangled. If any state vectors of the two systems cannot be represented as the tensor product of $|n>$ and $|m>$, we call that the state vector is ten-entangled state. For example: $|\psi<_{AB} = a|0>_A|0>_B + b|1>_A|1>_B$ is an entangled state. When a state vector is entangled state, it is impossible that any composing observations can be measured accurately. However, when any observables of entangled state obtain the measured value, the measured value of other observables are obtained accurately.

3.2. The algorithm of the key distribution in image quantum encryption

There are two quantum key distribution protocols which depend on the quantum states of two different characteristics. The one is the single particle key distribution protocol which is based on the non-cloning theorem of non-orthogonal quan-tum state. The BB84 protocol based on four common quantum states and the B92 protocol based on two quantum states are common. The other key distribution protocol is relied on quantum entanglement properties, such as Ekert protocol.

In the ideal case, each protocol has provable security, the security of single particle key distribution protocol depends on the non-cloning theorem in the non-orthogonal quantum state. The security of two-particle entangled key distribution pro-tocol can be guaranteed only when the quantum bits are measured by the sender Alice and the receiver Bob; both of them provide an effective way to detect the presence or absence of an eavesdropper, which are classic encryption process cannot be achieved. The purpose is to make the communication between Alice and Bob via an unreliable channel to complete the key negotiation, in order to ensure absolute safety. Next, we will make an analysis of every key distribution algorithm.

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

3.2.1. The image encryption based on the algorithm of single particle key distribution

Single particle key distribution algorithm mainly includes BB84 protocol and the B92 protocol, we will analyze them separately.

BB84 protocol is the first key distribution protocol in Quantum cryptography, since Bennett and Brassard proposed in 1984, it is one of the quantum key distribution schemes that are used most frequently. BB84 protocol is based on the quantum complementarity, and the protocol is simple but has unconditional security. The protocol is coded by 4 kinds of polarization states of the photon: the linearly polarization state |↔ and | (horizontal and vertical polarization), the circularly polarization state $|\nearrow\rangle$. and $|\nwarrow\rangle$. (left handed and right-handed polarization). In these two states, the linearly polarized photon and the circular polarized photon are mutually orthogonal, but the state of the linearly polarized photon and circularly polarized photon are not orthogonal.

BB84 protocol implementation needs two channels: classical channel and quantum channel. The classical channel can effectively provide the send-receive of Alice and Bob to exchange some necessary multimedia image information. Quantum channel is used to transfer quantum state with randomness. The steps of the protocol implementation are as follows:

(1) four polarization directions of linear and circular polarization photons in multimedia network image are as the basis by Alice, a random quantum bit string $S = \{s_1, s_2, , s_n\}$ is generated, in which $s_i = \{|\leftrightarrow\rangle, |\updownarrow\rangle, |\nearrow\rangle, |\nwarrow\rangle\}$ ($i = 1, 2, , n$). At the same time, S is corresponding to a set of transmission basic sequence $M^a = \{m^a_1, m^a_2, \cdots, m^a_n\}$, $m^a_i \in \{+, \times\}$. The corresponding transmission basic sequence of state |↔ and | is +, and the one of state $|\nearrow\rangle$ and $|\nwarrow\rangle$ is ×;

(2) Alice transmits quantum bit string S to the Bob through the quantum channel. The time interval between any adjacent quantum bits is τ;

(3) Bob selects a random measurement basic sequence M^B to measure the received photons, among them, $M^B = \{m^b_1, m^b_2, \cdots, m^b_n\}, m^b_i \in \{+, \times\}$;

(4) By classic channel, Bob notifies the measurement basic sequence of M^B selected by Alice;

(5) the measurement basic sequence M^B of Bob is compared to the own reserved transmission basic sequence M^a of Alice, in addition, what measurement basic sequences used by Bob are the same and what are different should be informed to Bob;

(6) the measurement results of Alice and Bob with consistent measuring basis are saved, and the measurement results with inconsistent measuring basis are abandoned;

(7) according to the error rate of the selected measuring basis sequence, the attacks are to determine whether exist. ξ_0 is as the threshold value of error rate. If $\xi < \xi_0$, the following steps are continued; otherwise, the agreement is terminated;

(8) the quantum states are encode into binary bits by Alice and Bob in the following manner: $|\leftrightarrow\rangle = |\nearrow\rangle = 0$, $|\updownarrow\rangle = |\nwarrow\rangle = 1$, and the original key of the image can be obtained;

(9) the original secret key is made further processing by means of information consultation and security strengthening to improve the security of the key, and finally get the security key of the image.

In BB84 protocol, the linear and circular polarization are the conjugate state, which can meet the uncertainty principle. According to the uncertainty principle, the more accurate the measurement results of the linear polarized photons are, the less accurate the measurement results of the circularly polarized photons are. Therefore, the measurement of any attacker is bound to bring about the disturbance of the original quantum bits, while the legitimate communication can detect the disturbance according to the uncertainty principle, so as to detect whether the eavesdropping exists. In addition, the linear polarization state and the circular polarization state are non-orthogonal, so they are not distinguishable, and the attacker can not accurately measure every captured quantum state. The uncertainty principle and quantum no-cloning theorem ensure the unconditional security of BB84 protocol.

BB84 protocol is a four-state protocol. Each quantum bit transmitted in the channel is derived from the symbol set |↔ , | , $|\leftrightarrow\rangle, |\updownarrow\rangle, |\nearrow\rangle, |\nwarrow\rangle$ of quantum information source. The quantum bits in the subset |↔ , | and $|\nearrow\rangle, |\nwarrow\rangle$ of the symbol set of quantum information source are orthogonal. However, the orthogonality in the BB84 protocol does not have any substantial effect, so it can be removed. According to this idea, in 1992, Bennett proposed the B92 protocol. B92 protocol is a binary state protocol, and the implementation of the protocol is based on two non-orthogonal quantum bits.

If there are any two non-orthogonal quantum bits $|\psi$ and $|\phi$ in the multimedia network image, setting

$$|\langle\phi|\psi\rangle| = \cos 2\theta \tag{4}$$

In the formula, θ is the included angle between two non-orthogonal quantum bits, $0 < \theta < \frac{\pi}{4}$. $|\psi$ and $|\phi$ are used to construct the two projection operators:

$$P_\psi = 1 - |\phi\rangle\langle\phi|$$
$$P_\phi = 1 - |\psi\rangle\langle\psi| \tag{5}$$

If there are any two non-orthogonal quantum bits in the multimedia network image, the function of P_ψ and P_ϕ is to project the quantum bit $|\psi$ and $|\phi$ to the orthogonal subspace of $|\psi$ and $|\phi$ respectively. It is easy to verify as follow-

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

ing:

$$\begin{aligned} P_\psi|\psi\rangle &= |\psi\rangle - |\phi\rangle\langle\phi|\psi\rangle \\ P_\psi|\phi\rangle &= |\phi\rangle - |\phi\rangle\langle\phi|\phi\rangle = 0 \\ P_\phi|\phi\rangle &= |\phi\rangle - |\psi\rangle\langle\psi|\phi\rangle \\ P_\phi|\psi\rangle &= |\psi\rangle - |\psi\rangle\langle\psi|\psi\rangle = 0 \end{aligned} \tag{6}$$

The above expressions show the important properties as follows: P will eliminate the quantum bit $|\phi\rangle$ in the image, but make an effect on $|\psi\rangle$ to get a positive result, and the probability is:

$$P_\psi = |\langle\psi|P_\psi|\psi\rangle| = 1 - |\langle\phi|\psi\rangle|^2 \tag{7}$$

While, P_ϕ will eliminate the quantum bit $|\psi\rangle$ in the image, but make an effect on $|\phi\rangle$ to get a positive result, and the probability is,

$$P_\phi = |\langle\phi|P_\phi|\phi\rangle| = 1 - |\langle\psi|\phi\rangle|^2 = P_\psi \tag{8}$$

(1) In addition, because of the non-orthogonality of $|\psi\rangle$ and $|\phi\rangle$, they meet the quantum no-cloning theorem of the image. B92 protocol was designed according to the above characteristics by Bennett:
(2) Based on two arbitrary non-orthogonal quantum states of $|\psi\rangle$ and $|\phi\rangle$ in two-dimensional image space, Alice gener-ates a random quantum bit string;
(3) through the quantum channel, Alice sends this quantum bit string to Bob;
(4) the projection operator is randomly selected from the operator set $\{P_\psi, P_\phi\}$, and Bob makes it acting on the recieved quantum state;
(5) Bob tells Alice which operations can get positive results (but not publishs the specific way of the measurements);
(6) Detection of eavesdropping. The method is the same as the BB84 protocol;
(7) The processes of image data filtering, image data error correction, confidentiality enhancing and others are all same as the BB84 protocol.

In the multimedia network image space, any two non-orthogonal quantum bits and are indistinguishable, therefore, any measurement for the two non-orthogonal quantum bits will introduce a disturbance, thus in the final results errors are introduced, and the measurement is not possible to give accurate results. According to the correlation of Alice and Bob measurement results, they are able to detect the presence or not of the attack. So, as with the BB84 protocol, the B92 protocol is used to encrypt the multimedia image, and its security is guaranteed by the basic principle of quantum physics.

According to the correlation of Alice's and Bob's measurement results, we are able to detect the presence of an attack. As with the BB84 protocol, it is unconditional security to use B92 protocol to encrypt the multimedia image, and its security is guaranteed by the basic principle of quantum physics.

3.2.2. Image encryption based on the algorithm of two particles entangled state key distribution

EPR entanglement for quantum key distribution was first proposed by University of Oxford's Ekert A. in 1991, its main feature is the use of EPR entanglement effect, so people used to call it EPR protocol. The security of the protocol is guar-anteed by Bell theory. Assuming that the transmission particle of the multimedia network image in the channel is a spin 1/2 particle, the physical quantities needed to be measured are A and B, the corresponding values are α_i and β_j, and the corresponding vectors are a_i and b_j. In the case of an ideal channel with no eavesdropping, the EPR entanglement pair has the following relationship:

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{-+}(a_i, b_j) - P_{+-}(a_i, b_j) \tag{9}$$

Among them, $P_{\pm\pm}(a_i, b_j)$ is the probability of obtaining a result of ± 1 along the directions of a_i and b_j.
The correlation coefficient S of the entangled bits is defined as follows:

$$S = \sum_{i,j} a_i, b_j \tag{10}$$

The correlation coefficient is obtained without interference by the quantum mechanics:

$$S = -2\sqrt{2} \tag{11}$$

When there is interference in the multimedia network,

$$S = \int p(n_a, n_b)\, dn_a dn_b < 2\sqrt{n_a n_b} \tag{12}$$

In this formula, n_a and n_b are two unit vectors; $p(n_a, n_b)$ is the probability of capturing a spin component when it is measured in a particular direction. It can be proved that when there is a disturbance in the multimedia network image, S is satisfied: $-2\sqrt{2} \le S \le 2\sqrt{2}$.

According to the correlation coefficient, the legal users can detect the existence of the eavesdroppers. The agreement is summarized as follows:

The two particles of the PER particle pairs which are generated by the quantum source based on the multimedia network image are sent to Alice and Bob respectively. When it is in the ideal case with not considering the elimination, the two particles remain entangled. If the two sides (Alice and Bob) measure the spin of the two particles in the same direction, the results will be on opposite. Therefore, similar to the communication process of BB84, Alice and Bob can randomly select the measurement direction and have the measurement of the spin state of their own particles. When the measurements of both sides are over, Bob announces the measurement direction through public channel. After Alice comparing with its own situation, it will tell Bob the image data having the same measuring direction, and both sides will retain the image data of these bits, which is used as a shared key. If the error rate exceeds the standard value, the result of the communication will be given up. The rest is the same with the BB84 protocol.

3.3. Security analysis of the algorithm image quantum encryption

The non-cloning theory of non-orthogonal states of polarized photons can guarantee that Eve cannot get any useful information from the generation and distribution of the image quantum key in the multimedia network. This is because if the standard state of the measurement instrument prepared by Eve is $|m>$, it would like to identify $|0>$ and $|1>$ without destroying the quantum state, then the following positive transformation is needed:

$$|0>|m> \rightarrow |0>|m_0> \tag{13}$$

$$|1>|m> \rightarrow |1>|m_1> \tag{14}$$

Taking the inner product on both sides, $<0|1><m|m> = <0|1><m_0|m_1>$, it can deduce $<m_0|m_1> =1$. As a result, when the quantum state of the image is not destroyed, the final state of the instrument is the same in two cases, and the Eve can not get any information from the coded bits. Of course, the more commonly measurement process is to destroy the original quantum state, making it changes from $|0>$ to $|0>$, from $|1>$ to $|1>$. The measurement process
can be expressed as:

$$|0>|m> \rightarrow 0>|m_0> \tag{15}$$

$$|1>|m> \rightarrow 1>|m_1> \tag{16}$$

Taking the inner product on both sides, $<0|1>=<0|1><m_0|m_1>$, the minimum value of $<m_0|m_1>$ should cor-respond Eve and can distinguish the two state to get $<0|1>= 1$. That is to say, when Eve measures the transmission quantum states, $|0>$ and $|1>$ will became the same state. Therefore, the non-cloning theorem of non-orthogonal state guarantees that the image key generation and distribution of single particle polarized photon are absolutely safe.

Assuming that Eve uses the probability clone theory of the non-orthogonal state in the process of stealing image, and uses the maximum probability of cloning, to analyze the security in the key generation and distribution. From the theory of probability clone, the maximum probability of non-orthogonal states being able to be cloned is $\eta = 1/1 + \psi_0|\psi_1$. Assuming that Eve uses the base vector to measure in the process of stealing, and clones the quantum state based on in prob-ability, the probability of the quantum state is cloned, then the maximum probability of the quantum state which is based on that the Eve can clone is:

$$\eta = 1/1 + \psi_0|\psi_1 = 1/1 + \frac{1}{\sqrt{2}(\leftrightarrow +)|} = 2 - \sqrt{2} = 0.5858 \tag{17}$$

If we make a further assume that Eve steals the image in multimedia network in the way of truncation / retransmission, the effective image information that Eve can get in the process of Alice and Bob exchanging the basis vectors through a common channel can be 40% of total information of sender (bigger than 25% with no probabilistic cloning), but it is still less than the image information that the receiver can obtain (50% of total information). Through the encryption algorithm, we can still make the image key between Alice and Bob safe enough. Bob and Alice select a compression function G: $\{0, 1\}^n \rightarrow \{0, 1\}^r$ in public, r is the length of the compressed key. As much as possible the image information is to reduce that Eve obtains. When $s < n - t$, Alice and Bob can get the key $K = G(W)$ which the length is $r = n - t - s$ bit, G: $\{0, 1\}^n \rightarrow \{0, 1\}^{n-t-s}$. However, the image information obtained by Eve will be reduced with the exponential $s(V = f(e^{-\alpha_s}))$.

Thus, even in the case of the maximum clone probability, the generation and distribution of the image quantum key are still reliable.

The entangled particles are used to key distribution with absolute security, due to in network multimedia, any encryption information is inexistent in the image transmission process and key works only after a legitimate user measurement and makes the communication in the open channel. However, Eve may attempt to replace the EPR particle which generates the image quantum key with the prepared information to mislead the Alice and Bob. We assume that the channel disturbance is caused by the behavior of Eve. Considering a simple case: We assume that Eve is able to prepare for every particle of the EPR particle pair, and every particle in the EPR pair has a well-defined polarization direction. The polarization direction of every pair of particles is different, and assuming that the probability which the single particle quantum state obtained by Alice is $|\theta_a$ and the quantum state of Bob is $|\theta_b$, that is $p(\theta_a, \theta_b)$. θ_a and θ_b are the angles measured from the vertical axis

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

Fig. 2. The original image.

describing the polarization direction. This assumption makes Eve having the ability to control the state of every particle. In this case, Alice and Bob should discard the established image quantum key, as the calculated absolute value is always less than $\sqrt{2}$. This is because of the density operator:

$$\beta = \int_{-}^{\pi/2} p(\theta_a, \theta_b) \left| \theta_a \quad \theta_a \right| \left|_{\sigma_b} \quad {}^{\sigma}\right|_b d\theta_a d\theta_b \tag{18}$$

The correlation coefficient of the formula (12) is slightly modified, getting the following results:

$$S = \int_{-\pi/2}^{\pi/2} p(\theta_a, \theta_b) d\theta_a d\theta_b \{\cos[2(\varphi_1^a - \theta_a)] \cos 2\varphi_3^b - \theta_b + \cos[2(\varphi_1^a - \theta_a)] + \cos 2\varphi^{2b} - \theta_b$$
$$+ \cos[2(\varphi_2^a - \theta_a)] + \cos 2\varphi_3^b - \theta_b + \cos[2(\varphi_2^a - \theta_a)] + \cos 2\varphi^{2b} - \theta_b \tag{19}$$

We derive the formula and get the result:

$$S = \int_{-\pi/2}^{\pi/2} p(\theta_a, \theta_b) d\theta_a d\theta_b \sqrt{2} \cos[2(\theta_a - \theta_b)] \tag{20}$$

This is to say, for any probability distribution $p(\theta_a, \theta_b)$, $|S| \le \sqrt{2}$. So, Alice and Bob will be very easy to judge the full control of Eve, and do not hesitate to get the image quantum key to give up.

Of course, Eve can change the complete control of each single particle state in the particle pair, by using the form of partial control. But as long as Alice and Bob are using QPA, it is possible to establish a secure secret key by modifying the transmission scheme of the image quantum secret key. The status of Eve to aquire partial information ($\sqrt{2} \le |S| \le 2\sqrt{2}$) is considered. According to the characteristics of the quantum, any two particles in the pure state cannot entangle with any of the third particle. Therefore, the image transmission process of entangled pairs in the pure state must not be entangled with other entangled particles or the particles in other system in multimedia network.

Using a quantum iterative algorithm, from the beginning of the mixed state EPR particles, some particles are continued to drop concentrately, until the remaining particles converge to the pure state. At this time, the EPR particles and Eve are not entangled. From the previous proof, Alice and Bob can establish the absolute secure secret key. If iterative algorithm is not very good, the density operator of residual particles after each iteration will not converge and only trend nearly pure state density matrix. However, and the degree of entanglement with eavesdropper has continued to descend and down to any low degree. Therefore, Alice and Bob can still establish a sufficient security image quantum secret key in this case, to ensure the security of the image in the multimedia network.

4. Experimental results and analysis

In order to verify the effectiveness of the proposed method in this paper, it requires to make relevant experimental analysis. In this test, CPU is Intel. Core (TM) i3 M350@ 2. 27 Hz, the RAM is 2G, and the RSA is a comparative method.

4.1. Encryption result analysis with the method of this paper

In this paper, the Lena image is as the object of study. Taking the maximum value is $M = 256$, the maximum allowable encryption error is $_{max} = 0.5$. The original image in multimedia network is described in Figs. 2 and 3 is the image encryp-tion results by this method, the one depicted in Fig. 4 is the decrypted restoring image, depicted in Fig. 5 is the encrypted image by RSA method, and depicted in Fig. 6 is the decryption image by RSA method.

Analysis of the process shows that the decryption image obtained by this method is the same as the original image, which shows that the method has a high image encryption and decryption performance. While using the RSA algorithm to get encrypt image can still see the original image's information, and the decryption image and the original image are also a far cry, which shows that this proposed method for image has very high encryption performance.

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

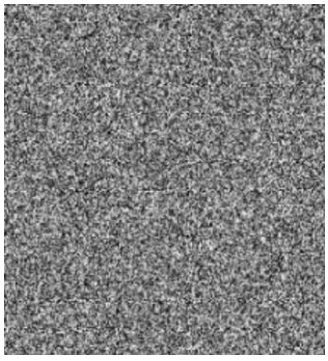


Fig. 3. Encrypted image of the method in this paper.

Fig. 4. The encrypted image of the method in this paper.

Fig. 5. The encrypted image of the RSA method.

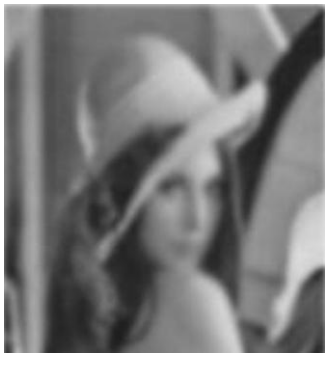
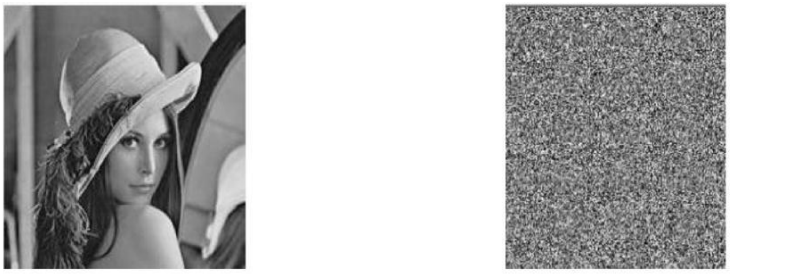


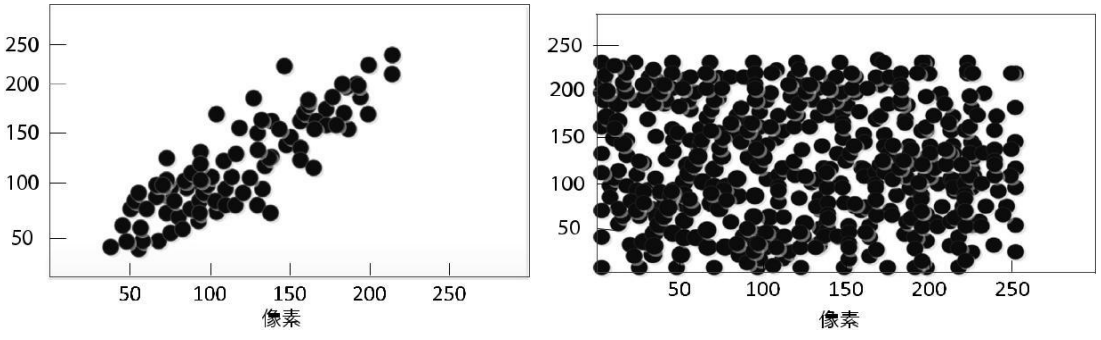
Fig. 6. The decryption image of the RSA method.

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



(a) The correct decryption image (b) The decryption image with the key of tiny perturbation

Fig. 7. Key sensitivity analysis.



（a）Correlation of original image （b）Correlation of encrypted image

Fig. 8. Correlation of adjacent pixels in horizontal direction.

4.2. Sensitivity analysis of key

Sensitivity of the key is the change degree of ciphertext when the initial key changes. First, the plaintext using the initial key is encrypted, and then on the initial value, an infinitesimal is added, respectively, which will be the key to encrypt the plaintext image. The obtained encrypted image and ciphertext images using the initial key are compared. The obtained results are described in Fig. 7.

Analysis of Fig. 7 can be seen that even if a small difference can also lead to the results of the decryption completely different, it shows that this method is extremely sensitive to the key.

4.3. Correlation analysis

Each pixel of the image in the multimedia network is not independent, and its correlation is very large, which shows that the gray value in the large area is quite different. And the smaller the correlation is, the better the effect of image encryption and the higher the security are. In this paper, the correlation coefficient is calculated from the horizontal, vertical and diagonal directions according to the 1000 pairs of pixels, which are randomly selected from the text and the cipher text:

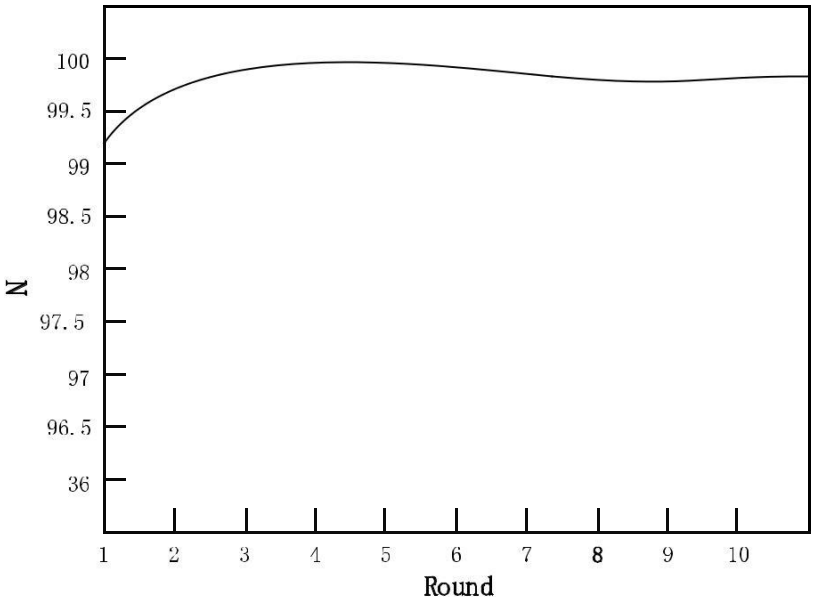
$$\rho_{xy} = \frac{Conv(x, y)}{D(x)\ D(y)} \tag{21}$$

Among them, $Conv(x, y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)]$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2$, $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, x and y are the pixel value of the two adjacent pixel

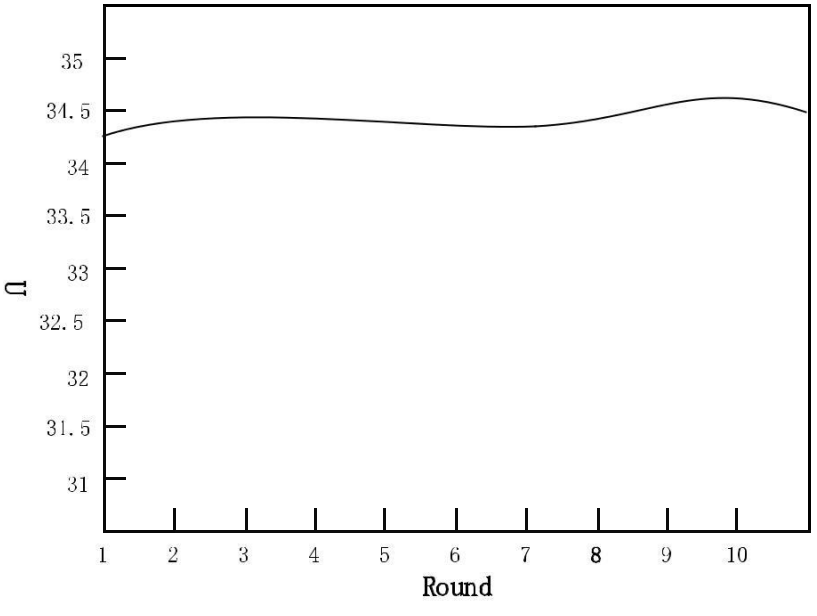
The results show that compare to the proposed method, RSA method has a comprehensive and significant improvement in the ability to hide the correlation of original image's adjacent pixels.

Fig. 8 shows the correlation between plaintext and ciphertext in the horizontal direction. Through the comparison of Fig. 8(a) and (b), it obviously can be seen that the correlation between the ciphertext image's adjacent pixels after encryption by the proposed method is random correspondence and the correlation between adjacent pixels is close to zero, which shows that this method has a good diffusion.

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



(a) NPCR



(b) UACI

Fig. 9. The changing trend of parameters in each round of encryption.

Table 1
Correlation between adjacent pixels of the original image and the encrypted image.

	Correlation coefficient		
Direction	Original image	Paper's method	RSA
Horizontal	0.9848	0.0041	0.0418
Vertical	0.9584	0.0021	0.0348
Diagonal	0.9341	0.0028	0.0522

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

4.4. Differential analysis

Number of Pixels Changing Rate (NPCR, N) and Unified Average Changing Intensity (UACI, U) are important indicators when measuring the ability of the image encryption algorithm to resist the differential attacks. N and U are represented after randomly changed a pixel value of the original image, the proportion and degree of the pixels are changed. The formulas are described as follows:

$$N = \frac{\sum_{i,j} D(i,j)}{256 \times 256} \times 100\% \tag{22}$$

$$U = \frac{1}{256 \times 256} \sum_{i,j} \frac{|v_1(i,j) - v_2(i,j)|}{255} \times 100\% \tag{23}$$

Assuming that two encrypted images v_1 and v_2 from multimedia network both have only one pixel different from the corresponding original images. The gray values of v_1 and v_2 at (i, j) are $v_1(i, j)$ and $v_2(i, j)$. If an array $D(i, j)$ which has the same size of v_1 and v_2 is selected, then $D(i, j)$ can be determined by $v_1(i, j)$ and $v_2(i, j)$. If $v_1(i, j) = v_2(i, j)$, then $D(i, j) = 0$; else, $D(i, j) = 1$, which means that $D(i, j)$ is the sum of $v_1(i, j)$ and $v_2(i, j)$ after the XOR opeation.

By the above two calculations: $N = 99.6292\%$, $U = 33.5608\%$. The result shows that, in the case of constant parameters, even two images have only one pixel different. As the number of encryption increasing, the encrypted image will also become completely different, and the diffusion rate is very fast. The result shows that, the method of this paper has a great ability to resist the known plain text attack and chosen plain text attack.

The changing trends of N and U in each round of encryption are shown in Fig. 9

The Figure [9] shows that, with the increase of the round of encryption, N and U doesn‘t change much, which shows that the times of encryption have little influences on the ability of this method to resist differential attack, instead, once encryption can get great results, this method can reduce the times of encryption, which means real-time stronger.

5. Conclusions

In this paper, an improved algorithm for image quantum encryption is proposed. The classical image encryption method is analyzed and aiming at the shortcomings of the classical encryption method, through the quantum encryption method, the classical encryption method is improved. the physical basis of the key production and distribution in the image quantum encryption is introduced, and single particle key distribution algorithm and 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. It can guarantee that the key is absolute safety, and ensure the safety of image. The security of the two kinds of key distribution algorithms is analyzed. The experimental results show that the proposed method has very high encryption performance, and the abilities of security and to resist differential attack are very high.

References

[1] http://learnrnd.com/detail.php?id=Biological_microsensor
[2] http://learnrnd.com/news.php?id=Ambient_Media:Present_Past_and_Future_Trends
[3] In QIEA. Quantum-inspired evolutionary algorithm for continuous space optimization based on multiple chains encoding method of quantum Bits. Math Probl Eng 2014;2014(3):166–83.
[4] Chen D, Chen J, Jiang H, Zou F, Liu T. An improved PSO algorithm based on particle exploration for function optimization and the modeling of chaotic systems. Soft Comput 2015;19(11):3071–81.
[5] Heng LU, Liu C, Nai-Wen LI, Guo JW. Segmentation of high spatial resolution remote sensing images of mountainous areas based on the improved mean shift algorithm. J Mt Sci 2015;12(3):671–81.
[6] Huang C, Zheng X. The Simulation study on image algorithm based on the reversible linear memory cellular automata integration with time delay. Sci Technol Eng 2014;14(3):86–92.
[7] Liu Q, Li P, Zhang M, Sui YX, Yang HJ. Image encryption algorithm based on chaos system having markov portion. J Electr Inf Technol 2014(6):1271–7.
[8] Fang D, Zhang J. Image encryption algorithm based on cat mapping and DNA Coding. Comput Eng 2014;40(12):89–93.
[9] Khan M, Shah T, Batool SI. Texture analysis of chaotic coupled map lattices based image encryption algorithm. 3D Res 2014;5(3):1–5.
[10] Lin L. A scrambling algorithm for color image digital watermarking based on the Arnold transform and the Lorenz chaotic system. Electr Des Eng 2014(18):165–8.
[11] Abowd GD, Mynatt ED. Charting past, present, and future research in ubiquitous computing. ACM Trans Comput-Hum Interact (TOCHI) 2015;7(1):29–58.
[12] Hu Z, Yuan S, Zhou C, Sha J, Zhao X, Jia L. Research progress on ultra-high-temperature Nb-silicide-based alloys. Hangkong Xuebao/acta Aeronautica Et Astronautica Sinica 2014;35(10):2756–66.
[13] Bo P, Lei L. An improved localization algorithm based on genetic algorithm in wireless sensor networks. Cognit Neurodyn 2015;9(2):249–56.
[14] Chen K, Zhou Y, Zhang Z, Dai M, Chao Y, Shi J. multilevel image segmentation based on an improved firefly algorithm. Math Probl Eng 2016;2016(285-296):1–12.
[15] Li L, Lv X, Xu W, Rong X, Wang H. A hybrid quantum genetic algorithm improved by quantum chromosomal coding and rotating gates. Basic Clin Pharmacol Toxicol 2015;117:15.
[16] Mousa AA, Elattar EE. Best compromise alternative to EELD problem using hybrid multiobjective quantum genetic algorithm. Appl Math Inf Sci 2014;8(6):2889–902.
[17] He Y, Deng Y, Luo MX. The improved evolution paths to speedup quantum evolution. Int J Theor Phys 2016;55(4):1977–87.

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

[18] Xu S, Wang Y, Lu P. Improved imperialist competitive algorithm with mutation operator for continuous optimization problems. Neural Comput Appl 2016;1:1–16.

[19] Ren-Fu LI, Myong-Chol D, Lin HU, Han CH. Mobile robot trajectory planning based on QPSO algorithm and experiment. Kongzhi Yu Juece/Control Decis 2014;29(12):2151–7.

[20] Nomura Y, Sakai S, Arita R. Multi-orbital cluster dynamical mean-field theory with an improved continuous-time quantum Monte Carlo algorithm. Phys Rev B 2014;89(19):4714–17.

[21] Wei XK, Shao W, Zhang C, Li JL. Improved self-adaptive genetic algorithm with quantum scheme for electromagnetic optimisation. Iet Microwaves Antennas Propag 2014;8(12):965–72.

[22] Hoye RLZ, Ehrler B, Böhm ML, Muñozrojas D, Altamimi RM, Alyamani AY, VaynzofY,SadhanalaA. Improved open- circuit voltage in ZnO-PbSe quantum dot solar cells by understanding and reducing losses arising from the ZnO conduction band tail. Adv Energy Mat 2014;4(8):105–10.

[23] Chen D, Chen J, Jiang H, et al. An improved PSO algorithm based on particle exploration for function optimization and the modeling of chaotic systems. Soft Comput 2015;19(11):3071–81.

[24] In QIEA Quantum-inspired evolutionary algorithm for continuous space optimization based on multiple chains encoding method of quantum bits. Math Probl Eng 2014;2014(3):166–83.

[25] Heng LU, Liu C, Nai-Wen LI, et al. Segmentation of high spatial resolution remote sensing images of mountainous areas based on the improved mean shift algorithm. J Mount Sci 2015;12(3):671–81.

[26] Sundani D, Mutiara AB, Juarna A, et al. Edge detection algorithm for color image based on quantum superposition principle. Social Work 2015;38(1):107–12.

[27] Hua T, Chen J, Pei D, et al. Quantum image encryption algorithm based on image correlation decomposition. Int J Theor Phys 2015;54(2):526–37.

[28] Chen CY, Zeng GJ, Lin FJ, et al. Quantum cryptography and its applications over the internet. IEEE Network 2015;29(5):64–9.

[29] Liu S, Fu W, He L, et al. Distribution of primary additional errors in fractal encoding method. Multimedia Tools Appl 2015. doi:10.1007/ s11042-014-2408-1.