The Application of Quantum Cryptography in Military GIS Security

Li Guoming
The Sixth Landforms Surveying Team of SBSM, Chengdu, China
Email: li-guoming@foxmail.com

Li Sheng and Ying Guowei
The Sixth Landforms Surveying Team of SBSM, Chengdu, China
Email: 331293996@qq.com, 250970390@qq.com

***Abstract*—Because the security of the algorithm depends on the security of the key, the security of the key is especially important in the transmission process. This paper discusses the key of digital watermarking algorithm using quantum cryptography protocol. According to the Heisenberg uncertainty principle in quantum mechanics, Any eavesdropper would not be able to eavesdrop on information in quantum cryptography without being detected that once the eavesdropper interception of certain information, you will change the state of photons, and then the communication will realize information stolen and change quantum key, this is to ensure the information security in the transmission process. This effectively guarantees the security of digital watermarking embedded in military geographic information systems.**

***Index Terms*—military geographic information system, security, quantum, watermark**

I. Introduction

At present, the geographic information system involving almost all walks of life, has become an important data system for the decision-making process of environmental analysis, route design, urban development planning and target point selection[1-2]. Compared with the traditional paper maps, geographic information system spatial data is more easy to share, in the ease of use and at the same time it brings great hidden danger to the security and confidentiality of data. There are many ways to steal, copy and intercept data, especially in the field of military, where security involves the national security, digital watermarking technology has been widely used in recent years to solve military geospatial data security.

With the production of quantum computers, the so-called complex keys cannot be protected, which requires us to improve the security of the keys [3]. The biggest difference between a quantum password and a classic password is that it can withstand any attack from a technical or computational tool, the reason is that its safety is guaranteed by the laws of physics rather than by some highly complicated operation. In this paper, we discuss the transmission of quantum keys by quantum cryptography in digital watermarking of military GIS.

II. Quantum Cryptography

A. The Concept of Quantum Cryptography

Quantum cryptography is a new science of quantum physics and cryptography, It has successfully solved the disadvantages of the security system built up in the traditional cryptography, which cannot be solved by solving mathematical problems, which has attracted international attention [4].

The idea of quantum cryptography was put forward by American Wiesner in a manuscript in the late 1960s.Then two scientists Charles.H.Bennett and Gilles Brassard proposed the first quantum cryptographic protocol, now known as the BB84 protocol, which marks the birth of quantum cryptography. They produced the first prototype quantum key distribution in 1989.The properties of tiny particles such as electrons and photons are very different from those that people can see and touch[5-6]. Quantum effects occur when particle particles are small to a certain extent, and an important characteristic of quantum effects is the Heisenberg uncertainty principle. Heisenberg's uncertainty principle refers to when two sets of physical quantities that are complementary to quantum mechanics were observed, the precise measurement of the quantity of one group of inevitably leads to another set of completely not sure. The velocity and position of an object can be measured at the same time in daily life, however, In the range of quantum effects, the velocity and position of objects cannot be determined at the same time. If you want to measure the position of the object, you can't measure the velocity of the object, and if you want to measure the velocity of the object, you can't measure the position of the object. This is because a measurement of one quantity can destroy another quantity of data. The principle of quantum cryptography is If the attacker wants to eavesdrop on the information that is represented by the quantum of the transmission, the quantum state must be affected, so that the sender and the receiver will know the quantum in the process of transmission is under attack, so as to give up this a quantum information.

The quantum cryptography has developed into a systematic system, which ins quantum key distribution,

quantum cryptography, quantum authentication, quantum cryptography, quantum cryptography, information security agreement theory, analysis of quantum cryptography. The "quantum cryptography" in this article essentially refers to the allocation of quantum keys, rather than directly transmitting the information itself.

B. Basic Principles of Quantum Key Distribution

Quantum key distribution (QKD) is a part of the field of quantum cryptography, whose main purpose is to build a Shared security key for remote communication by relying on unreliable channels. It is characterized by the ability to achieve key distribution in real time, which can be used to produce the key, which does not require long storage of keys. The key information is carried by photons, and according to the Heisenberg uncertainty principle, the attacker cannot obtain the full information of the carrier photon; And because of the existence of the measurement collapse principle, as long as the attacker has carried out the measurement of the carrier photon, the partial information will be destroyed, which will eventually be discovered by the two parties. The non-cloning principle guarantees that quantum signals in the channel will not be copied by the listener. The security of quantum key distribution is guaranteed by the basic theory of quantum mechanics .Bennett and Brassard proposed and implemented the quantum key distribution protocol, which called as the BB84 protocol.

C. Quantum Cryptographic Protocol (BB84 Protocol)

The BB84 protocol uses polarized light as a quantum carrier. Photon 0 ° and 90 ° polarization respectively were used as |0〉and|1〉, and 45 ° and 135 ° polarization respectively corresponding to |+〉 and |-〉. If with the level to the right direction to measure the Angle of the starting point, and in a counterclockwise direction Angle of the positive direction, the |0〉, |+〉, |1〉, |-〉 can image the surface for the "-", "/", "|" "\".So "┼" customarily represent by measuring base {|0〉,|1〉}, known as the baseline base;"╳" for measuring base {|+〉,|-〉}, is called a diagonal matrix.

In practice, the transmission of photons in the channel is inevitably influenced by the environment, resulting in loss or error. However, in order to facilitate the theoretical study, we only consider that the channel is ideal for perfect, without loss and error. At this time, the implementation of the BB84 agreement is as follows:

(1) Alice sends a series of photons to Bob, independently of the state of each photon randomly selected as |0〉, |+〉, |1〉, |-〉.

(2) Bob randomly selects a straight base or diagonal basis for each photon received, and it has a 50 percent chance of selecting the correct measurement basis for testing.

(3) Bob announces to Alice the measurements he uses each time, but does not release the measurements results..

(4) Alice tells Bob which measurements are correct and remained, and the rest is discarded

(5) Alice and Bob reserved only the corresponding data for those photons with respect to the base.

(6) they uses the |0〉 and Alice and Bob |+〉 as a classic of number "0", the |1〉 and |-〉 as a classic number "1".

(7) safety inspection: Alice and Bob randomly select a portion of the data that is retained in step (5), and to reveal the numbers obtained by this part in step (6), and check whether the number on both sides are the same. If there are different results, it means that there are eavesdroppers and the two parties end this communication process; If they are all the same, then they can go on.

(8) Alice and Bob have the remaining undetected Numbers as confidential information obtained by both parties.

After this process, Alice and Bob end up with a classic binary bit string. The content is not selected by either party, but is subject to the randomness made by the two parties in step (1), (2) and (7).But it can be used as a secret "key" to deliver meaningful content and not random information, so the process is called quantum key distribution.

Ⅲ. QUANTUM RYPTOGRAPHIC DIGITAL WATERMARKING SCHEME

Alice wrote a digital message. Alice wants to send a message to her friend Bob. Alice trusts Bob, which enough to send the message to Bob. She wanted to make sure he didn't try to ask for his identity. To complete this process, Alice will add watermarks to her message, which should have the following characteristics:

- Not perceptual — — The change caused by watermark embedding should be lower than the perceived threshold. It's not visible here. Bob will not notice the presence of watermarks.
- Robustness — — the ability to resist distortion or malicious processes the data. This is unbroken unless the message is destroyed during use.
- Security — — If watermark embedding and extraction algorithm makes it impossible for unauthorised users to detect and remove watermark, watermark is safe. It is only verifiable secret for Bob.

First Alice has some quantum message M, and she wants to change it to M 'by watermark. To put all the bits $|\psi i\rangle \in M$ prior to the original keys J. Then use different key K to all bits $|\psi i\rangle$ add watermark bits (which $i \in L$, L is the phase of M collection), the resulting watermark M '.Now M 'contains the original bit of write key J and when $i \in L$ $|\psi'_i\rangle \in M'$ watermark bits, which add the key K, K is not equal to J.When can be found M on the basis of J'(we said for M' ◦ J) watermarking was established. When both L and K are secret, only the key K can find that the generated watermark has a certain probability of error.

ⅣCONCLUSION

Quantum digital watermarking scheme is a quantum algorithm to observe the relative error frequency of quantum bits on different bases. Alice has a quantum bit information that is transformed by quantum information or by classical algorithms. After inserting the watermark, she could immediately send a message in the form of a quantum bit by observing the information so that Bob could discover the quantum bit. Note that the watermark is not generated until Bob finds it, so it may be the best for Alice to avoid being attacked.

With Quantum cryptography has been developing rapidly in recent decades, reliability, transmission distance, communications equipment and other technical difficulties were successively conquer, at present, quantum secret communication on metropolitan area network has been basically mature, the use of "quantum science experimental satellite" of our country also launched in July 2016, the first star to achieve transmission, and plans to be completed in 2030, the globalization of quantum communication satellite network. Predictably, in the near future, wide-area perhaps will replace the existing traditional quantum communication network data transmission system, quantum cryptography technology as a reliable means of secrecy is expected to military geographic space information provides the basis in the field of security services and the most reliable security.

ACKNOWLEDGEMENT

Thanks are due to colleagues for assistance with soft science research project support of sichuan province, China (NO. 2017ZR0123, 2017ZR0122).

REFERENCES

[1] F. Yan, A. M. Iliyasu, B. Sun, “A duple watermarking strategy for multi-channel quantum images,” Quantum Information Processing, vol.14, pp. 1675-1692, 2015.
[2] J. Mo, Z.F. Ma, Y.X. Yang, X.X. Niu, “A Quantum Watermarking Protocol Based on Bell Dual Basis,” International Journal of Theoretical Physics, vol. 52, pp. 3813－3819, 2013.
[3] W.W. Zhang, F. Gao, B. Liu, “A Quantum Watermark Protocol,” International Journal of Theoretical Physics, vol. 52, pp. 504-513, 2013.
[4] Y.G. Yang, P. Xu, J. Tian, “Analysis and improvement of the dynamic watermarking scheme for quantum images using quantum wavelet transform,” Quantum Information Processing, vol.13, pp.1931-1936, 2014.
[5] X.Y. Qu, “The system of mobilization ability construction lead defense mobilization innovation and development,” National Defense, vol. 10, pp. 19-22, 2014.
[6] K. Xu, “Practice and Exploration in the Building of National Defense Mobilization System of New China,” Contemporary China History Studies, vol. 13, pp.29-36, 2016.