Journal of Quantum Information Science, **2012, 2, 10-14**
http://dx.doi.org/10.4236/jqis.2012.21003 Published Online March 2012 (http://www.SciRP.org/journal/jqis)

Quantum Steganography Embedded Any Secret Text without Changing the Content of Cover Data

Takashi Mihara
Department of Information Sciences and Arts, Toyo University, Tokyo, Japan
Email: mihara@toyo.jp

Received December 6, 2011; revised January 30, 2012; accepted February 7, 2012

ABSTRACT

Steganography is a technique hiding secret information within innocent-looking information (e.g., text, audio, image, video, and so on). In this paper, we propose a quantum steganography protocol using plain text as innocent-looking information called cover data. Our steganograpy protocol has three features. First, we can use any plain text that is independent of any secret message sent between parties. When we make stego data, we do not need to change the content of plain text at all. Second, embedded messages are not included in opened information (innocent-looking messages), but are included as phases of the entangled states. Finally, in quantum states shared between parties in advance, *i.e.*, as quantum keys used when the parties recover secret messages from stego data, neither innocent-looking information nor the information of any secret message is included.

Keywords: Quantum Steganography; Hidden Data; Quantum Communication; Entangled State

1. Introduction

Both superposition states and entangled states have been effectively used in many fields of quantum information. For instance, Shor's quantum algorithms for prime factorization and discrete logarithms are typical examples [1]. However, it is also thought that his results will threaten partial security of information processing (the security of public key cryptosystems) in the future. In this situation, some quantum cryptosystems based on quantum physics have been also proposed [2-4], and have proved to be unconditionally secure [5-9].

As a result of typical quantum information security, Bennett and Brassard proposed a quantum cryptosystem called BB84 [2]. This system effectively uses superposetion states, and exchanges secret information between parties. Moreover, quantum secret sharing is proposed in order to store and manage information securely (e.g., see [10]). The subject of this problem is to share secret information among parties. Under cooperating among the parties, some parties can obtain some useful information. As being derived from the quantum secret sharing, quantum data hiding is also proposed [11-14]. The subject is to construct a protocol such that parties cannot recover secret information using only local operations supplemented by classical communication among them although this protocol also shares information among them.

Recently, quantum steganography has been also studied. *Steganography* is a technique hiding secret information within innocent-looking information (e.g., text, audio, image, video, and so on). Cryptography is to make information unreadable against any eavesdropper, whereas steganography is to hide information against any eavesdropper. Messages made by cryptography are obviously unnatural, and eavesdroppers can easily regard them as targets. On the other hand, messages made by steganography are natural. Therefore, eavesdroppers may pass them with high probability.

Early results of quantum steganography such as [15,16] (see also [17,18]) using superdense coding and [19] using quantum error-correcting codes are not sufficient because their results showed protocols sending secret information (embedded information, or embedded message) between parties securely, but did not show the technique embedding it within innocent-looking information (cover data). Martin also proposed a notion of quantum steganographic communication [20], *i.e.*, he proposed a quantum channel hidden within a quantum key distribution protocol such as BB84. In this situation, Shaw and Brun constructed a quantum steganography protocol using quantum error-correcting codes [21]. Their protocol showed a method embedding secret information (stego data) to cover data.

In this paper, we propose a quantum steganography protocol using plain text as cover data. First, we make a quantum entangled state representing a classical message. This quantum state means the cover data corresponding to the message. Next, we make quantum stego data includeing an embedded message by being included the cover data within the stego data.

The features of our steganograpy protocol are as follows. First, we can use any plain text that is independent of any secret message (*i.e.*, any embedded message). When we make stego data, we do not need to change the contents of innocent-looking messages at all. Namely, any eavesdropper cannot distinguish the cover data from the stego data. On the other hand, in Shaw and Brun's protocol, the cover data must be modified in order to embed secret messages as error-correcting codes [21]. Therefore, the stego data made by their protocol slightly differs from the original cover data. Second, roughly speaking, embedded messages are not included in opened information (innocent-looking messages) although they are included as partial information of the stego data within the quantum entangled states. They are included as phases of the states, and nobody can know the information except for legitimate parties. Finally, in quantum states shared between the parties in advance, *i.e.*, as quantum keys used when the parties recover secret messages from stego data, only the entangled state of a form of $\left(1/\sqrt{N}\right)\sum_{y=0}^{N-1}|y\rangle|y\rangle$ is shared between parties. In this quantum state, neither innocent-looking information nor the information of any secret message is included. Thus, any useful information does not leak in this procedure.

The remainder of this paper has the following organization. In Section 2, we show a quantum entangled state used as cover data. Although the form of this state seems to differ from the form of the stego data mentioned in Section 3, we show the relationship between the cover data and the corresponding stego data in Section 4. In Section 3, we construct a quantum steganography protocol. In Section 4, we evaluate secrecy and security of our protocol. Finally, in Section 5, we describe some concluding remarks.

2. Cover Data

We consider a situation such that a party Alice wants to send a classical message $a \in \{0,1, \quad ,N-1\}(N \geq 2)$ to another party Bob. This message may not be secret to anybody, *i.e.*, the information may be stolen by any eavesdropper or Alice may open it intentionally.

In this situation, we construct a protocol in the following way. First, Alice makes a quantum state

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-i2\pi ax/N}|x\rangle|x+r\rangle$$

corresponding to the classical message *a*, where $r \in \{0,1, \quad ,N-1\}$ is a random number chosen by her. Throughout this paper, the outcome of the addition is congruent modulo *N*, *i.e.*, $|x+r\rangle = |(x+r) \bmod N\rangle$, we call each state $|\bullet\rangle$ a register (although $|\bullet\rangle$ is only called a register when $N = 2^n$ for some positive integer *n* usually), and $i^2 = -1$. Next, she sends the state to Bob. Finally, Bob can recover the message *a* by applying a quantum Fourier Transform,

$$|x\rangle \to \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{i2\pi xy/N}|y\rangle,$$

to the two registers. Namely, by applying the quantum Fourier Transform, the state becomes

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-i2\pi ax/N}|x\rangle|x+r\rangle$$
$$\to \frac{1}{\sqrt{N^3}}\sum_{x=0}^{N-1}\sum_{x_1=0}^{N-1}\sum_{x_2=0}^{N-1} e^{-i2\pi ax/N}e^{i2\pi xx_1/N}e^{i2\pi(x+r)x_2/N}|x_1\rangle|x_2\rangle$$
$$= \frac{1}{\sqrt{N^3}}\sum_{x_1=0}^{N-1}\sum_{x_2=0}^{N-1} e^{i2\pi rx_2/N}\left(\sum_{x=0}^{N-1} e^{i2\pi(x_1+x_2-a)x/N}\right)|x_1\rangle|x_2\rangle$$
$$= \frac{1}{\sqrt{N}}\sum_{x_1+x_2\equiv a(\mathrm{mod} N)} e^{i2\pi rx_2/N}|x_1\rangle|x_2\rangle,$$

where we use the property such that $\sum_{x=0}^{N-1} e^{i2\pi yx/N} = N$ if $y \equiv 0(\bmod\ N)$, otherwise the sum is zero if $y \not\equiv 0(\bmod\ N)$. Then, Bob can recover the message *a* because he can obtain x_1 and x_2 satisfying $x_1 + x_2 \equiv a(\bmod\ N)$ by measuring the two registers.

In the next section, we use the form of this state made by Alice as a partial state of stego data, *i.e.*, as cover data.

3. Our Steganography Protocol

In this section, we show a quantum steganography protocol such that Alice sends a classical message $m \in \{0,1, \quad ,N-1\}$ to Bob secretly by embedding to the message *a* mentioned in Section 2.

In general, stego data is constructed by modifying cover data, *i.e.*, stego data is made by embedding a secret message to cover data. However, our stego data in our protocol is constructed by combining some quantum states with a secret message and a classical message corresponding to cover data. Although we showed cover data $\left(1/\sqrt{N}\right)\sum_{x=0}^{N-1} e^{-i2\pi ax/N}|x\rangle|x+r\rangle$ corresponding to the message *a* in Section 2, our stego data is not constructed by embedding a secret message *m* to the state but includes the quantum state of the cover data finally.

We construct a protocol in the following way.

Our Proposed Protocol

Step 1: Alice and Bob share an entangled state

$$\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|y\rangle|y\rangle$$

in advance, where Alice has the first register, and Bob has the second one. The state must be shared securely between the parties. Note that this step can be executed between them with being independent of both a secret message *m* and a cover message *a*, *i.e.*, they do not need to decide the messages in this step.

Step 2: After deciding a secret message *m* sending to Bob and a cover message *a*, Alice makes a state

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle$$

corresponding to the cover message *a*, and embeds the message *m* to the state in Step 1 as follows:

$$\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}e^{-\iota 2\pi my/N}\left|y\right\rangle\left|y\right\rangle.$$

Step 3: Alice combines the two states in Step 2, and makes an entangled state from them, *i.e.*, she adds the first register to the second register.

$$\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\right)\left(\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}e^{-i2\pi my/N}\left|y\right\rangle\left|y\right\rangle\right)$$
$$\to\frac{1}{\sqrt{N^2}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}e^{-i2\pi ax/N}e^{-i2\pi my/N}\left|x\right\rangle\left|x+y\right\rangle\left|y\right\rangle$$
$$=\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}e^{-i2\pi my/N}\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\left|x+y\right\rangle\right)\left|y\right\rangle$$

This state is the stego data corresponding to the message *m* embedded to the message *a*. Note that the message *m* is independent of the message *a*. Therefore, Alice can use any natural plain text as the classical message constructing cover data, and do not need to modify the message in constructing the corresponding stego data.

Step 4: Alice sends her two registers to Bob. The registers may be opened to anybody in public.

Step 5: Bob can recover the secret message *m* by applying the quantum Fourier transform to all the registers, *i.e.*,

$$\frac{1}{\sqrt{N^2}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}e^{-i2\pi ax/N}e^{-i2\pi my/N}\left|x\right\rangle\left|x+y\right\rangle\left|y\right\rangle$$
$$\to\frac{1}{\sqrt{N^5}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\sum_{x_1=0}^{N-1}\sum_{x_2=0}^{N-1}\sum_{y_1=0}^{N-1}e^{-i2\pi ax/N}e^{-i2\pi my/N}$$
$$\times e^{i2\pi xx_1/N}e^{i2\pi(x+y)x_2/N}e^{i2\pi yy_1/N}\left|x_1\right\rangle\left|x_2\right\rangle\left|y_1\right\rangle$$
$$=\frac{1}{\sqrt{N^5}}\sum_{x_1=0}^{N-1}\sum_{x_2=0}^{N-1}\sum_{y_1=0}^{N-1}\left(\sum_{x=0}^{N-1}e^{i2\pi(x_1+x_2-a)x/N}\right)$$
$$\times\left(\sum_{y=0}^{N-1}e^{i2\pi(y_1+x_2-m)y/N}\right)\left|x_1\right\rangle\left|x_2\right\rangle\left|y_1\right\rangle$$
$$=\frac{1}{\sqrt{N}}\sum_{\substack{x_1+x_2\equiv a(\mathrm{mod}\,N)\\ y_1+x_2\equiv m(\mathrm{mod}\,N)}}\left|x_1\right\rangle\left|x_2\right\rangle\left|y_1\right\rangle$$

Then, Bob can recover the message *m* because he can obtain y_1 and x_2 satisfying $y_1+x_2\equiv m(\mathrm{mod}\,N)$ by measuring the state (obviously, he can also recover the message *a*).

4. Secrecy and Security

First, we study a relationship between the stego data and the cover data. The stego data in Step 3 mentioned in the previous section is

$$\frac{1}{\sqrt{N^2}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}e^{-i2\pi ax/N}e^{-i2\pi my/N}\left|x\right\rangle\left|x+y\right\rangle\left|y\right\rangle$$
$$=\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}e^{-i2\pi my/N}\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\left|x+y\right\rangle\right)\left|y\right\rangle$$

On the other hand, the cover data mentioned in Section 2 is

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\left|x+r\right\rangle$$

Thus, the state of the cover data is the same form as a part of the stego data, $\left(1/\sqrt{N}\right)\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\left|x+y\right\rangle$. This means that we can also regard the stego data as the state made by the following way except for Bob's register. Although the state may not be constructed in order mentioned in the following procedure, we focus on a relationship between the stego data and the cover data.

First, Alice chooses a random number $r\in\{0,1,\quad,N-1\}$, and makes a state $\left(1/\sqrt{N}\right)\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\left|x+r\right\rangle$ corresponding to the message *a*. Next, the phase corresponding to the secret message *m*, $e^{-i2\pi mr/N}$, is applied, *i.e.*, $e^{-i2\pi mr/N}\left(1/\sqrt{N}\right)\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\left|x+r\right\rangle$. Finally, by computing all the sum from 0 to $N-1$ of any random number *r* for the state, the state becomes $\sum_{r=0}^{N-1}e^{-i2\pi mr/N}\left(1/\sqrt{N}\right)\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\left|x+r\right\rangle$. Note that the state is the same state as the stego data except for Bob's register.

By considering this process, we can conclude that our stego data can be made without changing the cover data. Therefore, the difference between Alice's registers revealed in Step 4 and the cover data cannot be found. Then, any eavesdropper cannot distinguish the cover data from the stego data even if Alice's registers in Step 4 is revealed, and the secrecy is held.

Next, Even if somebody applies the quantum Fourier transform to the partial state of the stego data (opened by Alice) $\left(1/\sqrt{N}\right)\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\left|x+y\right\rangle$ and measures the two registers, the message *m* can be recovered by Bob if he can know the outcome measured by the third party. Here, we observe the situation such that Bob executes his procedure after the cover data opened by Alice is operated and is measured.

First, by applying the quantum Fourier transform, the state of the stego data becomes as follows:

$$\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{-i2\pi my/N}\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} e^{-i2\pi ax/N}\left|x\right\rangle\left|x+y\right\rangle\right)\left|y\right\rangle$$

$$\to \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{i2\pi(x_2-m)y/N}\left(\frac{1}{\sqrt{N}}\sum_{x_1+x_2\equiv a \pmod N}\left|x_1\right\rangle\left|x_2\right\rangle\right)\left|y\right\rangle$$

Next, by measuring the first two registers, the third party can obtain only x_1 and x_2 satisfying $x_1+x_2\equiv a(\bmod N)$, and obtain the classical message *a* corresponding to the cover data. After the measurement, the state becomes $\left(1/\sqrt{N}\right)\sum_{y=0}^{N-1}e^{i2\pi(x_2-m)y/N}\left|y\right\rangle$. Therefore, by applying the quantum Fourier transform to his register and measuring it, Bob can obtain y_1 satisfying $y_1+x_2\equiv m(\bmod N)$.

In addition, even if any other operation is applied to the stego data, the third party can operate only the state $\sum_{x=0}^{N-1}e^{-i2\pi ax/N}\left|x\right\rangle\left|x+y\right\rangle$ corresponding to each state $\left|y\right\rangle$ of Bob's register since Bob has the last register entangled. Then, only Bob can recover the secret message *m* because it relates to Bob's register, and the security is held.

5. Conclusions

In this paper we proposed a quantum steganography protocol embedding secret messages to plain text. In general, steganography embedding secret messages to plain text is more difficult than that of other cover data such as image data or audio data since we feel the plain text strange even if the modification is slightly. On the other hand, we can use natural plain text as the cover data used in our steganography protocol. Therefore, any eavesdropper cannot decide whether the message is stego data or not. Moreover, although our protocol must share entangled states between parties in advance as quantum keys used when the parties recover secret messages from stego data, neither innocent-looking information nor the information of any secret message is included in the states.

By using the property that can use any natural plain text, a legitimate party is also able to have cover data made by a third party, *i.e.*, a third party creates a natural text *a*, and applies the phase $e^{-i2\pi ax/N}$ of Step 2 in Section 3.

REFERENCES

[1] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal of Computing*, Vol. 26, No. 5, 1997, pp. 1484-1509. doi:10.1137/S0097539795293172

[2] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 9-12 December 1984, pp. 175-179.

[3] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters*, Vol. 67, No. 6, 1991, pp. 661-663. doi:10.1103/PhysRevLett.67.661

[4] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States," *Physical Review Letters*, Vol. 68, No. 21, 1992, pp. 3121-3124. doi:10.1103/PhysRevLett.68.3121

[5] H.-K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances," *Science*, Vol. 283, No. 5410, 1999, pp. 2050-2056. doi:10.1126/science.283.5410.2050

[6] D. Mayers, "Unconditional Security in Quantum Cryptography," *Journal of the ACM*, Vol. 48, No. 3, 2001, pp. 351-406. doi:10.1145/382780.382781

[7] D. Mayers and A. Yao, "Quantum Cryptography with Imperfect Apparatus," *Proceedings of* 39th *Annual Symposium on Foundation of Computer Science*, Palo Alto, 8-11 November 1998, pp. 503-509.

[8] E. Biham, M. Boyer, P. O. Boykin, T. Mor and V. P. Roychowdhury, "A Proof of the Security of Quantum Key Distribution," *Proceedings of* 32*nd Annual ACM Symposium on Theory of Computing*, Portland, 21-23 May 2000, pp. 715-724.

[9] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters*, Vol. 85, No. 2, 2000, pp. 441-444. doi:10.1103/PhysRevLett.85.441

[10] R. Cleve, D. Gottesman and H. K. Lo, "How to Share a Quantum Secret," *Physical Review Letters*, Vol. 83, No. 3, 1999, pp. 648-651. doi:10.1103/PhysRevLett.83.648

[11] B. M. Terhal, D. P. DiVincenzo and D. W. Leung, "Hiding Bits in Bell States," *Physical Review Letters*, Vol. 86, No. 25, 2001, pp. 5807-5810. doi:10.1103/PhysRevLett.86.5807

[12] D. P. Di Vincenzo, D. W. Leung and B. M. Terhal, "Quantum Data Hiding," *IEEE Transactions on Information Theory*, Vol. 48, No. 3, 2002, pp. 580-598. doi:10.1109/18.985948

[13] D. P. DiVincenzo, P. Hayden and B. M. Terhal, "Hiding Quantum Data," *Foundations of Physics*, Vol. 33, No. 11, 2003, pp. 1629-1647. doi:10.1023/A:1026013201376

[14] T. Eggeling and R. F. Werner, "Hiding Classical Data in Multipartite Quantum States," *Physical Review Letters*, Vol. 89, No. 9, 2002, Article ID: 097905. doi:10.1103/PhysRevLett.89.097905

[15] M. Curty and D. J. Santos, "Quantum Steganography," 2*nd Bielefeld Workshop on Quantum Information and Complexity*, Bielefeld, 12-14 October 2000, pp. 12-14.

[16] S. Natori, "Why Quantum Steganography Can Be Stronger than Classical Steganography," *Quantum Computation and Information*, Vol. 102, 2006, pp. 235-240. doi:10.1007/3-540-33133-6_9

[17] Z.-G. Qu, X.-B. Chen, X.-J. Zhon, X.-X. Niu and Y.-X. Yang, "Novel Quantum Steganography with Large Payload," *Optics Communications*, Vol. 283, No. 23, 2010, pp. 4782-4786. doi:10.1016/j.optcom.2010.06.083

[18] Z.-G. Qu, X.-B. Chen, M.-X. Luo, X.-X. Niu and Y.-X. Yang, "Quantum Steganography with Large Payload

Based on Entanglement Swapping of χ-Type Entangled States," *Optics Communications*, Vol. 284, 2011, pp. 2075-2082. doi:10.1016/j.optcom.2010.12.031

[19] J. Gea-Banacloche, "Hiding Messages in Quantum Data," *Journal of Mathematical Physics*, Vol. 43, No. 9, 2002, pp. 4531-4536. doi:10.1063/1.1495073

[20] K. Martin, "Steganographic Communication with Quantum Information," *Lecture Notes in Computer Science*, Vol. 4567, 2007, pp. 32-49. doi:10.1007/978-3-540-77370-2_3

[21] B. A. Shaw and T. A. Brun, "Quantum Steganography with Noisy Quantum Channels," *Physical Review A*, Vol. 83, No. 2, 2011, Article ID: 022310. doi:10.1103/PhysRevA.83.022310