Int J Theor Phys (2015) 54:2505–2515
DOI 10.1007/s10773-014-2478-x

The Quantum Steganography Protocol via Quantum Noisy Channels

Zhan-Hong Wei · Xiu-Bo Chen · Xin-Xin Niu · Yi-Xian Yang

Received: 30 July 2014 / Accepted: 15 December 2014 / Published online: 13 January 2015

Abstract As a promising branch of quantum information hiding, Quantum steganography aims to transmit secret messages covertly in public quantum channels. But due to environment noise and decoherence, quantum states easily decay and change. Therefore, it is very meaningful to make a quantum information hiding protocol apply to quantum noisy channels. In this paper, we make the further research on a quantum steganography protocol for quantum noisy channels. The paper proved that the protocol can apply to transmit secret message covertly in quantum noisy channels, and explicity showed quantum steganography protocol. In the protocol, without publishing the cover data, legal receivers can extract the secret message with a certain probability, which make the protocol have a good secrecy. Moreover, our protocol owns the independent security, and can be used in general quantum communications. The communication, which happen in our protocol, do not need entangled states, so our protocol can be used without the limitation of entanglement resource. More importantly, the protocol apply to quantum noisy channels, and can be used widely in the future quantum communication.

Keywords Quantum steganography · Quantum measurements · Quantum noisy channels · Security

Z. H. Wei · X. B. Chen (✉) · X. X. Niu · Y. X. Yang
Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
e-mail: flyover100@163.com

Z. H. Wei · X. B. Chen · X. X. Niu · Y. X. Yang
State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

1 Introduction

As the major research of quantum information, quantum communication and quantum computation have attracted much attention of scholars over the past decades. With the ongoing development of quantum information theory and the advent of the relevant experiments [1–3], they have recently become important research topics, and some new research topic had been explained [4, 5]. As one kind of technique used to protect communication security, quantum information hiding can be known as the quantum counterpart of classical information hiding, and it utilizes the quantum mechanical effect to achieve the target of hiding information in process of quantum communication and quantum computation. Now, quantum information hiding has been a new research topic in quantum security communication.

As for quantum information hiding, the existing work mainly focus on two aspects: one is research about the quantum information hiding protocol based on characteristics of quantum mechanics; another is how to design novel quantum information hiding protocol with the aid of other quantum security communication. For the former, it was started with Therhal et al.'s [6] the work in 2001. They presented the first quantum data hiding protocol based on Bell states. In 2002, Eggeling and Werner [7] implemented LOCC (Local Operation and Classical Communication, LOCC) on multi-particle nonentangled states to extend Therhal et al.'s protocol. Later on, Guo et al. [8] used optical down converter to analyse the data hiding protocol based on Bell states, and presented an improved data hiding protocol. In 2005, Hayden et al. [9] proposed a quantum data hiding protocol with the aid of the threshold access structure, and their work laid the foundation for hiding the large capacity data. In 2007, Chattopadhyay et al. [10] presented a quantum multiparty data hiding protocol. The protocol utilized the characteristics that the reduced matrix of four orthogonal entangled states shared by even participants are the fully mixed states. In 2012, Fatahi and Naseri [11] proposed a quantum watermarking protocol. In the protocol, they used entanglement swapping to build up a hidden layer for secret messages. For the latter, researchers presented some quantum information hiding protocols based on other quantum security communication protocols. Worley [12] proposed the first quantum watermarking protocol in 2004. In the protocol, the secret message was embedded according to the error probability of measurement outcomes, and its idea is similar to Bennett and Brassard's quantum key distribution protocol(BB84 protocol) [13]. Based on BB84 protocol, Martin [14] also proposed a novel protocol for quantum steganographic communication. The protocol hid a steganographic channel in BB84 protocol. In 2010, Z. G. Qu et al. [15] proposed a quantum steganography protocol. In order to transmit secret messages covertly, they used entanglement swapping of Bell states to build up a hidden channel based on the improved ping-pong protocol. In 2013, Xu et al. [16] also proposed a high-efficiency quantum steganography protocol. In the paper, they firstly proposed a hidden rule among the secure message. Under the control of the hidden rule, they proposed the quantum steganography protocol based on the tensor product of Bell states. The protocol established a hidden channel to transmit the secret message within any quantum secure direct communication(QSDC) scheme. Besides the forgoing two types, there are other types of quantum information hiding protocols. In 2002, Julio Gea-Banacloche [17] explored the possibility that encode a quantum state using quantum error-correcting code(QECC) to hide messages as errors in an arbitrary quantum data file, and he thought that the embedded secret message can act as watermarks to ensure authenticity and integrity of the data. Bilal A. Shaw and Todd A. Brun [18] also proposed

two protocols for hiding quantum information based on QECC. Differ from the paper [17], this paper gave specific scheme for hiding information and a quantitative method for the secrecy of the protocol. G. Mogos [19] presented a novel quantum steganography protocol, which aimed to used qutrits (the three-orthogonal state system) to represent RGB(Red, Green, Blue) for hiding the secret message in digital color images. Moreover, the protocol expanded the field of applicability of the steganography from the classical informatics to the quantum one successfully. Takashi Mihara [20] proposed a new quantum steganography protocol. The protocol embedded the secret message into plain text without changing the content of the text, and had a good secrecy. In 2013, based on quantum Fourier transform, Zhang et al. [21] presented a quantum watermarking protocol. The protocol embedded the secret message in the coefficient of Fourier transform. However, the protocol did not consider the characteristics of quantum mechanics of quantum information, and used the classical computation in embedding procedure. In the same year, Yang et al. [22] showed the defect of Zhang's protocol, and improved the protocol.

We can see that quantum steganography is a promising branch of quantum information hiding. It can be used to transmit classical or quantum messages covertly via quantum channels. The foregoing mentioned quantum steganography protocols support the development of quantum information hiding. However, there are some limitations in these protocols. The limitations can be briefly described as below. Firstly, some protocols mainly used the physical characteristic of quantum states, such as quantum entangled states. But the resource of the quantum states which meet the characteristics is restricted. In addition, these protocols need a lot of auxiliary resources. Therefore, these protocols are limited in applications. Secondly, most of other quantum steganography protocols were proposed based on other quantum security communication protocols. The security of these protocols need to rely on other protocols. Therefore, these protocols hardly can be used in general quantum communication, and hardly can apply in the future society of quantum information and quantum communication. Thirdly, quantum superposition states and entangled states tend to be easily disrupted by noise and interactions with their environment and decoherence [23, 24]. Therefore, it is very significant for quantum steganography protocols to transmit secret messages reliably in quantum noisy channels. Considering the further research for quantum steganography from the above aspects, this paper proposes a quantum steganography protocol for quantum noisy channels.

The paper firstly proved the protocol can be used in quantum communication via quantum noisy channels. Then, the detailed protocol is given. Our protocol aims to transmit n-qubit secret messages covertly in quantum noisy channels. Senders can embed the secret message into the cover data with the aid of positive operator valued measure(POVM) operators. Receivers can extract the secret message with a certain probability by using a set of appropriate projective measurement operators. Therefore, the extracting procedure does not need to publish the cover data. Without the cover data, it is impossible for illegal receivers to obtain any useful information about the secret message. This make the secret communication be imperceptible. Therefore, the protocol has good a secrecy. In addition, the security of our protocol does not rely on any other protocol, and the protocol can be widely applied in general quantum communication.

The rest of this paper is organized as below. Section 2 shows our protocol can be used in quantum communication via quantum noisy channels. The protocol are depicted in detail in Section 3. Section 4 analyzes the performance of the protocol in detail. Finally, the paper ends up with a conclusion in Section 5.

2 The Idea of Our Protocol Applying in the Communication via Quantum Noisy Channels

Indeed, any real-life device, which is used to accomplish the quantum communication, unavoidably interacts with its environment. This means that quantum superposition states and entangled states can be easily interfered with their environment. Therefore, it is necessary to make quantum steganography protocols apply to communications in quantum noisy channels. Reference [25] presented a quantum steganography protocol based on probability measurements. This paper extends the protocol. We simplify the method and prove that the method can be applied to quantum noisy channels.

In quantum noisy channels, quantum states can be described by mix states using its density matrix. We suppose that mixed states of two qubits(2-level quantum system) are:

$$\rho_1 = p_0|\varphi_0\rangle\langle\varphi_0| + p_1|\varphi_1\rangle\langle\varphi_1| \tag{1}$$

$$\rho_2 = r_0|\varphi_0\rangle\langle\varphi_0| + r_1|\varphi_1\rangle\langle\varphi_1| \tag{2}$$

where $\{p_i, |\varphi_i\rangle\}, \{r_i, |\varphi_i\rangle\}, i = 0, 1$ are ensembles of pure states, and $\{|\varphi_i\rangle, i = 0, 1\}$ are mutually orthogonal. In order to meet $Tr(\rho_1) = Tr(\rho_2) = 1$, there are $p_0 + p_1 = 1, r_0 + r_1 = 1$.

In order to encode the state of two qubits in one qutrit, we need to do purifications for ρ_1 and ρ_2 at first. Given the reference system B, then we will obtain pure states:

$$|\phi_{1B}\rangle = \sqrt{p_0}|\varphi_0\rangle|\psi_0\rangle + \sqrt{p_1}|\varphi_1\rangle|\psi_1\rangle \tag{3}$$

$$|\phi_{2B}\rangle = \sqrt{r_0}|\varphi_0\rangle|\psi_0\rangle + \sqrt{r_1}|\varphi_1\rangle|\psi_1\rangle \tag{4}$$

Where $\{\psi_0, \psi_1\}$ is an orthogonal basis of B system. $|\phi_{1B}\rangle, |\phi_{2B}\rangle$ are pure states, and $\rho_1 = Tr(|\phi_{1B}\rangle\langle\phi_{1B}|), \rho_2 = Tr(|\phi_{2B}\rangle\langle\phi_{2B}|)$.

Constructing a set of POVM measurement operators. It is listed in (5):

$$\begin{aligned} M_{00} &= \tfrac{1}{3}(|\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| + |\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1| + |\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0|) \\ M_{01} &= \tfrac{1}{3}(|\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1| + |\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| + |\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1|) \\ M_{10} &= \tfrac{1}{3}(|\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0| + |\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| + |\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1|) \\ M_{11} &= \tfrac{1}{3}(|\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1| + |\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0| + |\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1|) \end{aligned} \tag{5}$$

Where $\sum_{i=00,01,10,11} M_i = I$.

We act the POVM measurement on $|\phi_{1B}\rangle \otimes |\phi_{2B}\rangle$ with the operator $\{M_{00} \otimes I \otimes I, M_{01} \otimes I \otimes I, M_{10} \otimes I \otimes I, M_{11} \otimes I \otimes I\}$:

Due to Heisenberg's uncertainty principle, the POVM measurement result is uncertainty. If the measurement result is 00, then the state $|\phi_{1B}\rangle \otimes |\phi_{2B}\rangle$ is projected onto a three-dimensional subspace. The state is changed to be:

$$|\phi_{00}\rangle = N_{00}(\sqrt{p_0r_0}|\varphi_0\varphi_0\rangle|\psi_0\psi_0\rangle + \sqrt{p_0r_1}|\varphi_0\varphi_1\rangle|\psi_0\psi_1\rangle + \sqrt{p_1r_0}|\varphi_1\varphi_0\rangle|\psi_1\psi_0\rangle)$$

where $N_{00} = 1/\sqrt{p_0r_0 + p_0r_1 + p_1r_0}$.

To recover the state of the first qubit, we perform the projective measurement on $|\phi_{00}\rangle$. The used projective measurement operators are given as follows:

$$P_{1,s} = |\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| + |\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0|;\ P_{1,f} = |\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1| \tag{6}$$

If the measurement result is $1s$, the state of the qutrit is projected onto a two-dimensional subspace. After the projective measurement, the state is changed to be (7):

$$|\phi_{00}^{'}\rangle = \sqrt{p_0}|\varphi_0\varphi_0\rangle|\psi_0\psi_0\rangle + \sqrt{p_1}|\varphi_1\varphi_0\rangle|\psi_1\psi_0\rangle \tag{7}$$

By taking the partial trace to the second particle and its reference system B, we obtain $|\phi_{1B}\rangle$. Computing $\rho_1 = Tr_B(|\phi_{1B}\rangle\langle\phi_{1B}|)$, we recover the state of the first qubit successfully. If the obtaining result is $1f$, the procedure of decoding fails. The probability of successful decoding the state of the first qubit is equal to $\frac{2}{3}$. The probability is given in the reference [25] in detail.

Similar to the above procedure of decoding, we can use a set of projective measurement operators to recover the state of the second qubit. This measurement operators are listed as below:

$$P_{2,s} = |\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| + |\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1|;\ P_{2,f} = |\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0| \tag{8}$$

The successful probability is also $\frac{2}{3}$.

Similarly, if the POVM measurements result are 01,10,11, there are the corresponding encoding procedure and the corresponding decoding procedure by using appropriate quantum measurement operators. Figure 1 clearly gives a description about the encoding procedure and the decoding procedure.

3 A Quantum Steganography Protocol for Quantum Noisy Channels

Based on the idea shown in the Section 2, this paper presents a quantum steganography protocol for quantum noisy channels. In our protocol, senders transmit $2n$-qubit (n-qubit are the secret message, and the rest n-qubit are the cover data) to receivers in public quantum channels. Moreover, receivers can correctly extract the secret message with the probability of $\frac{2}{3}$. Meanwhile, the cover data can normally be recovered with the same probability.

3.1 Embedding Procedure of the Secret Message

Suppose that Alice wants to covertly send n-qubit secret messages to Bob in public quantum channels. In order to make eavesdroppers be unaware of the existence of the secret message, Alice needs to use n-qubit cover data to conceal the secret message. The concrete embedding procedure is depicted as below:

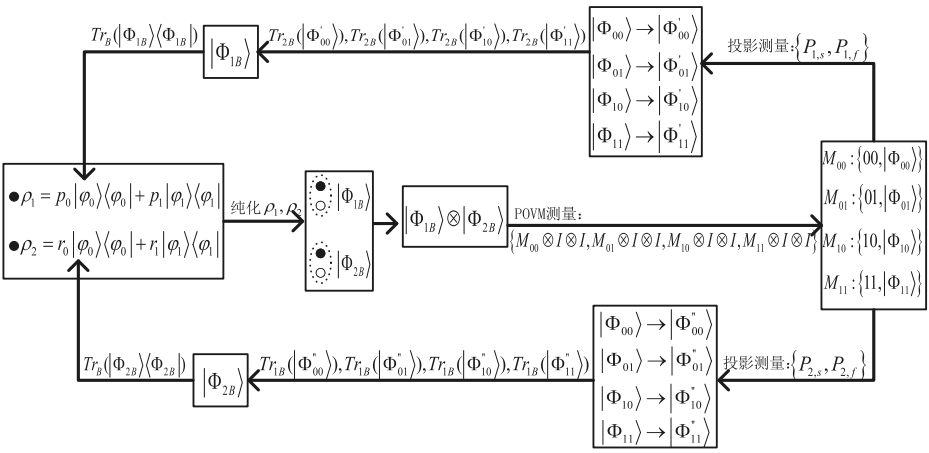

Fig. 1 The encoding and decoding workflow of mixed states of two qubits

(1) Prior to embedding the secret message, Alice and Bob firstly share some information before their communications. Later on, the shared information is listed in Table 1 in detail.

(2) Alice prepares two n-qubit systems. These two n-qubit systems are the cover data and the secret message respectively. They can be written as follows:

$$\rho_s = \rho_{s,0} \otimes \rho_{s,1} \otimes \cdots \otimes \rho_{s,n-1} \tag{9}$$

$$\rho_c = \rho_{c,0} \otimes \rho_{c,1} \otimes \cdots \otimes \rho_{c,n-1} \tag{10}$$

where $\rho_{s,i} = p_{0,i}|\varphi_0\rangle\langle\varphi_0| + p_{1,i}|\varphi_1\rangle\langle\varphi_1|$, $\rho_{c,i} = r_{0,i}|\varphi_0\rangle\langle\varphi_0| + r_{1,i}|\varphi_1\rangle\langle\varphi_1|$, $i = 0, 1, \cdots, n-1$, and $p_{0,i} + p_{1,i} = 1, r_{0,i} + r_{1,i} = 1$.

(3) Doing purifications for $\rho_{s,i}$ and $\rho_{c,i}, i = 0, 1, \cdots, n-1$: Given the reference system D, we obtain $|\phi_{sD,i}\rangle$ and $|\phi_{cD,i}\rangle, i = 0, 1, \cdots, n-1$. Then $|\phi_{sD,i}\rangle$ and $|\phi_{cD,i}\rangle, i = 0, 1, \cdots, n-1$ are pure states, and $\rho_{s,i} = Tr_D(|\phi_{sD,i}\rangle\langle\phi_{sD,i}|)$ and $\rho_{c,i} = Tr_D(|\phi_{cD,i}\rangle\langle\phi_{cD,i}|)$.

(4) Alice takes $|\phi_{sD,i}\rangle$ and $|\phi_{cD,i}\rangle (i = 0, 1, \cdots, n-1)$ to make tensor products respectively, and obtains the sequence $|\phi_{sD,0}\rangle \otimes |\phi_{cD,0}\rangle, |\phi_{sD,1}\rangle \otimes |\phi_{cD,1}\rangle, \cdots, |\phi_{sD,n-1}\rangle \otimes |\phi_{cD,n-1}\rangle$.

(5) Alice constructs n sets of POVM measurement operators, and each set of POVM measurement operators is given in (11).

$$\begin{aligned}
M_i^{00} &= \tfrac{1}{3}(|\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| + |\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1| + |\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0|) \\
M_i^{01} &= \tfrac{1}{3}(|\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1| + |\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| + |\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1|) \\
M_i^{10} &= \tfrac{1}{3}(|\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0| + |\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0| + |\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1|) \\
M_i^{11} &= \tfrac{1}{3}(|\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1| + |\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0| + |\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1|)
\end{aligned} \tag{11}$$

where $\sum_{j=00,01,10,11} M_i^j = I (i = 0, 1, \cdots, n-1)$, and each set of POVM measurement operators can be written as $M_i = \{M_i^{00}, M_i^{01}, M_i^{10}, M_i^{11}\}$. Then, Alice acts the POVM measurement on $|\phi_{sD,i}\rangle \otimes |\phi_{cD,i}\rangle$ $(i = 0, 1, \cdots, n-1)$ with the operators $M_i \otimes I \otimes I$ respectively.

(6) Alice does not publish the measurement result at once after acting the POVM measurements, but saves the measurement result. The result are written as $k_0k_1 \cdots k_{n-1}$. Meanwhile, $|\phi_{sD,i}\rangle \otimes |\phi_{cD,i}\rangle$ collapse to be $|\phi_i\rangle, i = 0, 1, \cdots, n-1$, and Alice obtains the new sequence $|\phi_0\rangle, |\phi_1\rangle, \cdots, |\phi_{n-1}\rangle$. The secret message and the cover data changed to be $|\phi_0\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{n-1}\rangle$.

(7) Finally, in order to prevent from being attacked, we need to do attack-detection in the communication. Therefore, Alice prepares decoy state particles and inserts the particle into $|\phi_0\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{n-1}\rangle$ for doing attack-detection. Then, Alice sends $|\phi_0\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{n-1}\rangle$ with the decoy state particle to Bob.

In this way, the secret message are embedded into the cover data successfully.

Table 1 The shared information between Alice and Bob

k_i	M_s	M_c
00	$P_{s,s} = \|\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0\| + \|\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0\|$	$P_{c,s} = \|\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0\| + \|\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1\|$
	$P_{s,f} = \|\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1\|$	$P_{c,f} = \|\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0\|$
01	$P_{s,s} = \|\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1\| + \|\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1\|$	$P_{c,s} = \|\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0\| + \|\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1\|$
	$P_{s,f} = \|\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0\|$	$P_{c,f} = \|\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1\|$
10	$P_{s,s} = \|\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0\| + \|\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0\|$	$P_{c,s} = \|\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0\| + \|\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1\|$
	$P_{s,f} = \|\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1\|$	$P_{c,f} = \|\varphi_0\varphi_0\rangle\langle\varphi_0\varphi_0\|$
11	$P_{s,s} = \|\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1\| + \|\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1\|$	$P_{c,s} = \|\varphi_1\varphi_1\rangle\langle\varphi_1\varphi_1\| + \|\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0\|$
	$P_{s,f} = \|\varphi_1\varphi_0\rangle\langle\varphi_1\varphi_0\|$	$P_{c,f} = \|\varphi_0\varphi_1\rangle\langle\varphi_0\varphi_1\|$

k_i is Alice's feasible POVM measurement results; M_s are the measurement operator used to extract the secret message; M_c are the measurement operator used to recover the cover data; $P_{s,s}$ and $P_{s,f}$ are a set of complete orthogonal basis of projective measurements, thereinto, $P_{s,s}$ is an operator used to extract the secret message successfully, while $P_{s,f}$ is an operator used to extract the secret message unsuccessfully; $P_{c,s}$ and $P_{c,f}$ similar to $P_{s,s}$ and $P_{s,f}$

3.2 Extracting Procedure of the Secret Message

After receiving the message from Alice, Bob wants to extract the secret message. Table 1 gives the shared information between Alice and Bob in detail. Without having influence on normally reading the cover data, Bob can extract the secret message with the probability of $\frac{2}{3}$ using the information in Table 1.

In Table 1, $k_i, i = 0, 1, \cdots, n-1$ is Alice's feasible POVM measurement results. M_s and M_c are projective measurement operators. Table 1 shows the corresponding relationship between M_s and k_i. It also gives the corresponding relationship between M_c and k_i. M_s and the corresponding relationship between M_s and k_i must be kept in secret and can be only known by Alice and Bob. While the corresponding relationship between M_c and k_i are public. Here, $P_{s,s}$, $P_{s,f}$ and $P_{c,s}$, $P_{c,f}$ are two sets of projective measurement basis, respectively.

To extract the secret message, Bob can perform the projective measurement on $|\phi_0\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{n-1}\rangle$ according to the shared information in Table 1. The extracting procedure can be depicted as below:

(1) When Bob receives the message with decoy state particles from Alice, he will detect if there are eavesdrops using decoy state particles at first. Then Bob tells Alice whether there are eavesdrops or not, and removes the decoy state particles.

(2) According to the result of attack-detection, Alice decide if she carry out the next step:

- If there is no eavesdrop, Alice publishes her POVM measurement results $k_0k_1\cdots k_{n-1}$, and Bob turns to the next step;
- Otherwise, Alice does not publish the measurement results $k_0k_1\cdots k_{n-1}$, and Bob does nothing. This communication is end.

(3) According to the measurement result $k_0k_1\cdots k_{n-1}$, Bob chooses a set of appropriate projective measurement operators $\{P_{s,s}, P_{s,f}\}$ of M_s in the Table 1. With the chosen operators $\{P_{s,s}, P_{s,f}\}$, Bob acts projective measurements on $|\phi_i\rangle, i = 0, 1, \cdots, n-1$,

respectively. Then, $|\phi_0\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{n-1}\rangle$ collapses to be $|\phi_0^{'}\rangle \otimes |\phi_1^{'}\rangle \otimes \cdots \otimes |\phi_{n-1}^{'}\rangle$.

(4) Bob takes the partial trace to the second particle and its reference system D of $|\phi_i^{'}\rangle, i = 0, 1, \cdots, n-1$ respectively, and obtains pure states $|\phi_{sD,i}\rangle, i = 0, 1, \cdots, n-1$.

(5) Computing $Tr_D(|\phi_{sD,i}\rangle\langle\phi_{sD,i}|)$ respectively, Bob can obtain the secret message $\rho_{s,i}, i = 0, 1, \cdots, n-1$ with the probability of $\frac{2}{3}$ successfully.

Likewise, we can read the cover data with the same probability by choosing an appropriate set of projective measurements operators $\{P_{c,s}, P_{c,f}\}$ of M_c according to Table 1 to perform projective measurements on $|\phi_0\rangle \otimes |\phi_1\rangle \otimes \cdots \otimes |\phi_{n-1}\rangle$ respectively.

4 Performance Analysis

Similar to the classical steganography, security, secrecy and capacity are three factors to be considered when we analyze the performance of quantum steganogranphy protocols. We need to consider two aspects about the security of quantum steganography protocols: one is that the protocol must ensure that eavesdroppers cannot be aware of the existence of the secret message; Another is that the protocol can resist all kinds of eavesdropping attacks and insure that eavesdroppers cannot obtain the secret message exactly even if they have suspicioned the existence of the secret message. The former can also be considered as the secrecy. The two aspects can ensure the security of quantum steganography protocols. It is known that the secrecy is an important measure to evaluate the performance of quantum steganogranphy protocols. It makes secret communications be imperceptible. This means that eavesdroppers can hardly be ware that the secret communication has happened so as to prevent eavesdroppers from damaging the secret message.

In general, most of quantum steganography protocols need the key and the cover data to extract the secret message. The key, which is used to embed the secret message and is used to extract the secret message, must be shared in secure channels and can be only known by senders and legal recipients(Alice and Bob) in the communication. As for the cover data, they must be published in order to exactly extract the secret message. However, our protocol embeds the secret message into the cover data by a set of POVM measurement operators. The POVM measurement results $k_0k_1 \cdots k_{n-1}$, which are used to extract the secret message, can be published after confirming that there is no eavesdrops in the communication. For illegal recipients, they can normally read the cover data by performing the projective measurement on the message according to Alice's POVM measurement results $k_0k_1 \cdots k_{n-1}$ and the public projective measurement operators M_c in Table 1. Therefore, the existence of the secret message does not influence the cover data. Similarly, Bob can also extract the embedded secret message from Alice by performing the projective measurement on the message according to Alice's POVM measurement results $k_0k_1 \cdots k_{n-1}$ and M_s in Table 1. But the M_s and the correspondence between $k_0k_1 \cdots k_{n-1}$ and M_s are secret. In our protocol, Bob can exactly extract the secret message without the cover data. Alice does not need to publish the cover data for extracting the secret message in the communication. This means that eavesdroppers cannot obtain useful information about the cover data. The information that eavesdroppers can only obtain is $|\Psi\rangle = |\Phi\rangle = |\phi_0\rangle \otimes |\phi_1\rangle, \cdots, |\phi_{n-1}\rangle$, so

$$D(\Psi, \Phi) = \frac{1}{2}|Tr(|\Psi\rangle\langle\Psi| - |\Phi\rangle\langle\Phi|)| = 0 \tag{12}$$

In this situation, any eavesdropper cannot distinguish the secret message from the cover data. Thus, it is impossible for eavesdroppers to be aware that there is the embedded secret message in the communication. In other words, the protocol can meet the secrecy requirement of quantum steganography protocols.

Once eavesdroppers start to suspect the existence of the secret message, it is very important for quantum steganography protocols to be able to resist all kinds of eavesdropping attacks. In order to obtain the secret message, eavesdroppers attempt to adopt all kinds of attacks: such as the intercept-resend attack and the auxiliary particle attack. But no matter which attack they adopt, it is inevitable to introduce errors. Therefore, the attack can eventually be detected by Alice and Bob using attack-detection. Once Alice have known that there are eavesdrops in the communication, she will not publish the POVM measurement results $k_0k_1\cdots k_{n-1}$. The POVM measurement results are completely random before being published by Alice. Therefore, eavesdroppers neither know $k_0k_1\cdots k_{n-1}$ nor the shared information, and they only randomly speculate the measurement results and the shared information. Eavesdroppers can guess the correct information for a qubit secret message with the probability of $\frac{1}{48}$. For n-qubit secret message, the probability is $\frac{1}{48^n}$. Then, when n is large enough, our protocol meets the requirement of a ϵ-security quantum steganography system. Moreover, all of the communication in our protocol except for the shared information can happen in the public quantum channel, and does not have special requests about the security of the quantum channel.

In general, our protocol can meet the secrecy and security requirement. In addition, we can see that the security of our protocol only relies on the uncertainty of quantum measurements, and does not rely on any other protocols. Therefore, our protocol can be used in general quantum communications. Using our protocol, we can utilize general quantum channels to covertly transmit the secret message. As for the physical implementation of our protocol, the problem faces two aspect: quantum purification and quantum state preparation. For common quantum states, purification and preparation of single-qubit states can be realized in cavity QED [26, 27]. The states, which are used in our protocol, are all common quantum states, and this make our protocol feasible in physical implementation.

For quantum steganography protocol, the capacity is an important measure. It is used to calculate that how many qubits(bits) secret message can be transmitted and how many qubits(bits) auxiliary information needs to be used in the communication for transmitting the secret message. Our protocol aims to transmit n-qubit secret message covertly. Our protocol needs not to expend a mass of the shared key and entangled states in the communication. With respect to the capacity, we give a calculation clearly about the consumption of our protocol: except for decoy state particles used in attack-detection, auxiliary resource used in our protocol includes n qubits and $2n$ bits message in order to transmit n-qubit secret message.

5 Conclusions

This paper presents a novel quantum steganography protocol for quantum noisy channels. The protocol is not affected by quantum noisy channels, and is able to transmit n qubits secret message covertly in public quantum channels. In our protocol, Bob can extract the secret message without publishing the cover data. The cover data can also be read normally by using the public projective measurement operator. Therefore, eavesdroppers can hardly be aware that the secret communication has taken place. Then, the protocol has a good

secrecy. In addition, the security of our protocol relies on the uncertainty of quantum measurements rather than any other protocols. Due to owing the kind of security, our protocol can widely be used in the general quantum communication. Moreover, Bob can extract the secret message according to Alice's POVM measurement results and the shared information in Table 1 in advance. The POVM measurement can be sent in public classical channels. This reduces the consumption of the communication. But because we used the POVM measurement operators in the embedding procedure and projective measurement operators in the extracting procedure respectively, the secret message can be only extracted with the probability of $\frac{2}{3}$. We hope that the imperfect can be improve in future work.

Acknowledgments We would like to thank editors and reviewers very much for careful work and helpful discussion. The work is supported by NSFC (Grant Nos. 61272514, 61170272, 61121061, 61411146001), NCET (Grant No. NCET-13-0681), the National Development Foundation for Cryptological Research (Grant No. MMJJ201401012) and the Fok Ying Tong Education Foundation (Grant No. 131067).

References

1. Bennentt, C.H., Bessette, F., Brassard, G., et al.: Experimental quantum cryptography. Cryptology **5**, 3–28 (1992)
2. Lo, H.K., Chau, H.F.: Unconditonal security of quantum key distribution over arbitrary long distance. Science **283**, 2050–2056 (1999)
3. Jin, X.M., Ren, J.G., Yang, B., Peng, C.Z., Pan, J.W.: Experimental free-space quantum teleportation. Nat. Photonics **4**, 376–381 (2010)
4. Le P.Q., Dong F., Hirota K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Inf. Process **10**, 63–84 (2011)
5. Hua, T., Chen, J., Pei, D., Zhang, W., Zhou, N.: Quantum image encryption algorithm based on image correlation decomposition. Int. J. Theor. Phys. (2014). doi:10.1007/s10773-014-2245-z
6. Terhal, B.M., DiVincenzo, D.P., Leung, D.W.: Hiding bits in bell states. Phys. Rev. Lett. **86**, 5807–5810 (2001)
7. Eggeling, T., Werner, R.F.: Hiding classical data in multipartite quantum states. Phys. Rev. Lett. **89**, 097905 (2002)
8. Guo, G.C., Guo, G.P.: Quantum data hiding with spontaneous parameter down- conversion. Phys. Rev. A. **68**, 044303 (2003)
9. Hayden, P., Leung, D., Smith, G.: Multiparty data hiding of quantum information. Phys. Rev. A. **71**, 062339 (2005)
10. Chattopadjyay, I., Sarkar, D.: Local indistinguishability and possibility of hiding cbits in activable bound entanglement states. Phys. Lett. A. **365**, 273–277 (2007)
11. Fatahi, N., Naseri, M.: Quantum watermarking using entanglement swapping. Int. J. Theor. Phys. **51**, 2094–2100 (2012)
12. Worley G.G. III: Quantum watermarking by frequency of error when observing qubits in dissimilar bases (2004). arXiv:quant-ph/0401041v2
13. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing, pp. 175–179. IEEE International Conference on Computers, Systems and Signal, New York (1984)
14. Martin, K.: Steganographic communication with quantum information, pp. 32–49. Proceedings of the 9th International Conference on Information Hiding, Heidelberg (2007)
15. Qu, Z.G., Chen, X.B., Zhou, X.J., Niu, X.X., Yang, Y.X.: Novel quantum steganography with large payload. Opt. Commun. **283**, 4782–4786 (2010)
16. Xu, S.J., Chen, X.B., Niu, X.X., Yang, Y.X.: High-efficiency quantum steganography based on the tensor product of Bell states. Sci. China Phys. Mech. Astron. **56**, 1747–1754 (2013)
17. Gea-Banacloche, J.: Hiding messages in quantum data. J. Math. Phys. **43**, 4531–4536 (2002)
18. Bilal, A.S., Todd, A.B.: Quantum steganography with quantum noisy channels. Phys. Rev. A. **83**, 022310 (2011)
19. Mogos, G.: Stego quantum algorithm, International Symposium on Computer Science and its Applications, Hobart Australia, (2008)

20. Mihara, T.: Quantum steganography embedded any secret text without changing the content of cover data. J. Quantum Inf. Sci. **2**, 10–14 (2012)
21. Zhang, W.W., Gao, F., Liu, B.: A watermarking strategy for quantum images based on quantum fourier transform. Quantum. Inf. Process. **12**, 793–804 (2013)
22. Yang, Y.G., Jia, X., Xu, P., Tian, J.: Analysis and improvement of the watermarking strategy for quantum images based on quantum Fourier transform. Quantum. Inf. Process (2013). doi:10.1007/s11128-013-0561-5
23. Lloyd, S.: Capacity of the noisy quantum channel. Physical. Rev. A. **55**, 1613–1622 (1997)
24. Zanardi, P., Rasetti, M.: Noiseless quantum codes. Phys. Rev. Lett. **79**, 3306–3309 (1997)
25. Wei, Z.H., Chen, X.B., Niu, X.X., Yang, Y.X.: A novel quantum steganography protocol based on probability measurements. Int. J. Quantum Inf. **11**, 1350068 (2013)
26. Yang, C.P., Chun, S., Han, S.Y.: Simiplified of two-qubit quantum phase gate with Our-level systems in cavity QED. Phys. Rev. A. **70**, 044303 (2004)
27. Biswas, A., Agarwal, G.S.: Quantum logic gates using Stark-shifted Raman transitions in a cavity. Phys. Rev. A. **69**, 062306 (2004)