Special Quantum Steganalysis Algorithm for Quantum Secure Communications Based on Quantum Discriminator

Xinzhu Liu[1,2], Zhiguo Qu[1,2,3,4,*], Xiubo Chen[4], and Xiaojun Wang[5]
[1] Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science and Technology, Nanjing, 210044 China
[2]School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, 210044 China
[e-mail: yzliubb@163.com]
[3]Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Nanjing University of Information Science and Technology, Nanjing, 210044 China
[4]Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876 China
[e-mail: qzghhh@126.com, flyover100@163.com]
5 School of Electronic Engineering, Dublin City University, Dublin 9, Ireland
[e-mail: xiaojun.wang@dcu.ie]
[*]Corresponding author: Zhiguo Qu

Received May 1, 2022; accepted June 13, 2023; published June 30, 2023

Abstract

The remarkable advancement of quantum steganography offers enhanced security for quantum communications. However, there is a significant concern regarding the potential misuse of this technology. Moreover, the current research on identifying malicious quantum steganography is insufficient. To address this gap in steganalysis research, this paper proposes a specialized quantum steganalysis algorithm. This algorithm utilizes quantum machine learning techniques to detect steganography in general quantum secure communication schemes that are based on pure states. The algorithm presented in this paper consists of two main steps: data preprocessing and automatic discrimination. The data preprocessing step involves extracting and amplifying abnormal signals, followed by the automatic detection of suspicious quantum carriers through training on steganographic and non-steganographic data. The numerical results demonstrate that a larger disparity between the probability distributions of steganographic and non-steganographic data leads to a higher steganographic detection indicator, making the presence of steganography easier to detect. By selecting an appropriate threshold value, the steganography detection rate can exceed 90%.

Keywords: Quantum computing, quantum discriminator, quantum machine learning, quantum steganalysis, quantum steganography.

1. Introduction

Steganography is a crucial technology for ensuring information security in communication. It effectively safeguards the confidentiality of digital communication by utilizing encryption, scrambling, and encoding techniques to embed secret information into the redundant parts of communication carriers. This makes it difficult for potential eavesdroppers to detect the presence of secret information, and even if they do, extracting the secret information becomes challenging. Quantum steganography, which can be seen as the quantum counterpart of classical steganography, has been widely employed in the field of quantum secure communication [1-2]. Compared to classical steganography, quantum steganography schemes are designed with the characteristics of quantum mechanics, making them less susceptible to eavesdropping.

However, steganography is a double-edged sword. While it provides secure and reliable methods for confidential communication, it can also be misused by criminals, posing a threat to public information security. In recent years, incidents of steganography being exploited in espionage, terrorist attacks, and criminal activities have emerged. Terrorists may use steganography to embed secret information into carriers such as text documents, pictures, and videos, spreading them worldwide through the internet. This poses a serious risk to national information security and personal privacy. Therefore, there is a pressing need to detect and analyze suspicious carriers for steganography, in order to supervise its use effectively and intercept the dissemination of malicious steganographic information.

The common approach for steganography detection is to analyze the statistical characteristics of steganographic carriers to identify abnormal statistical information. This enables detectors to determine the presence of malicious secret information hidden within the carriers, as well as estimate the amount and embedding position of the steganographic information. However, steganalysis is more challenging than steganography itself due to the diversity of steganography methods and the vast amount of information on the internet. This is why the development of steganalysis lags behind steganography. Given that steganalysis involves processing big data, machine learning methods hold great potential for addressing this problem.

In this paper, we focus on quantum steganalysis using a quantum discriminator. Firstly, due to the characteristics of steganography, the interference signal from steganographic information in the carriers is very weak. Therefore, we propose a data preprocessing method to amplify the characteristics of steganographic information. Secondly, we design a quantum discriminator based on a quantum neural network to analyze the statistical characteristics of steganographic and non-steganographic data. This enables the discrimination of whether quantum steganographic information is hidden within the detected carriers. We provide numerical results for this method through experiments on a simulation platform.

The structure of this paper is as follows. In the first chapter, we introduce the development of classical steganography and quantum steganography. The second chapter presents related works on quantum steganography and steganalysis, as well as quantum machine learning methods. The third chapter provides a detailed explanation of the proposed quantum steganalysis algorithm. The fourth chapter presents the numerical results. Finally, the fifth chapter summarizes the content of this paper and proposes future research prospects.

2. Related works

2.1 Quantum steganography

In recent years, the parallel processing capabilities of quantum computing have had a significant impact on classical cryptosystems that rely on computational complexity, such as the Shor algorithm and quantum Fourier transform. Additionally, the security of quantum communication based on quantum mechanical properties has been proven. As a result of the development of quantum secure communication, quantum steganography [3-5] has also received considerable attention. Quantum steganography typically hides secret information in various quantum carriers using coding, encryption, and other technologies. Examples include quantum covert communication protocols like quantum key distribution [6], quantum secret sharing [7], and quantum secure direct communication [8]. There are also quantum steganography protocols based on different multimedia formats [9-10].

2.2 Quantum steganalysis

Steganalysis research is primarily divided into three levels. The first level involves detecting the existence of steganographic communication. The second level focuses on estimating the amount of embedded steganographic information and identifying the type of steganography algorithm. The third level aims to decipher the content of steganographic information within the carrier. Due to the high difficulty of steganalysis, current research primarily focuses on the first stage, which is the detection of steganographic communication. Generally, advancements in steganalysis technology can also drive improvements in steganography.

Classical steganalysis methods include specific and general approaches. Specific steganalysis methods include the chi-square attack method, RS method, spa method [11], and WS method [12] for LSB replacement steganography. There is also an HCFCOM-based method for LSB matching steganography [13]. From a machine learning perspective, steganalysis can be viewed as a binary classification problem [14], particularly for general steganalysis methods. These methods employ machine learning techniques such as support vector machines [15], neural networks, and clustering to construct classifiers that distinguish steganographic carriers from non-steganographic carriers. To handle high-dimensional features, Kodovsky et al. proposed an integrated classifier based on Fisher linear discriminant [16].

Different from classical steganalysis, quantum steganalysis faces a significant challenge due to the irreversible damage caused by any observation to a quantum system, which is a result of the physical properties of quantum systems. In the study of quantum steganalysis, finding the most effective measurement method to accurately identify quantum states plays a crucial role. Qu et al. [17] proposed a quantum steganalysis protocol for the steganography algorithm based on the BB84 protocol. This protocol compares the difference in probability distribution of the quantum carrier before and after steganography. On the other hand, Luo et al. [18] developed a quantum steganalysis algorithm specifically for the quantum multimedia steganography protocol based on the least significant bit.

2.2 Quantum machine learning

The combination of machine learning and 5G has significantly advanced the development of the Internet of Things [19-24]. Moreover, it has opened up new possibilities for quantum steganalysis. Several popular q-machine learning methods have been recently proposed.

One advantage of quantum computing is its ability to accelerate classical linear algebra computations, which has led to the development of quantum support vector machines [25] that utilize matrix inversion [26]. Quantum optimization [27] has further contributed to the improvement of these methods. Additionally, these techniques can be applied to various types of quantum neural networks [28].

Deep learning is another emerging subdiscipline of machine learning, and quantum computers are being employed for deep learning applications that require significant time and storage. Examples of such applications include quantum generative adversarial networks [29], quantum Boltzmann machines, quantum variational autoencoders, and quantum convolutional neural networks [30]. Furthermore, reinforcement learning [31], a more sophisticated field within machine learning, focuses on learning over time with the assistance of the environment.

In the realm of quantum machine learning, the objective is to distinguish between the original carrier and the carrier embedded with steganography. The main challenge lies in detecting the hidden weak signal of the embedded steganography information amidst numerous strong signals.

Detecting steganography information poses a great challenge in the era of big data. Given that machine learning plays a crucial role in processing big data and identifying its statistical characteristics, we apply quantum machine learning methods [32-33] to quantum steganalysis to address the issue of destructive quantum steganography. In this paper, we propose a method for extracting statistical features from quantum steganography carriers using quantum machine learning techniques. Additionally, we design a quantum convolutional neural network to construct an automatic recognizer for quantum steganography analysis. The feasibility of the algorithm is demonstrated through simulation experiments.

3. Methodology

3.1 Overview

The general process of quantum steganography and steganalysis is illustrated in **Fig. 1**. The sender prepares the quantum carrier by encoding steganography information using a coding or embedding method. The carrier, along with the steganography information, is then transmitted to the receiver through noisy quantum channels. During transmission, a monitoring party may secretly detect steganography and retransmit the carrier to the receiver.

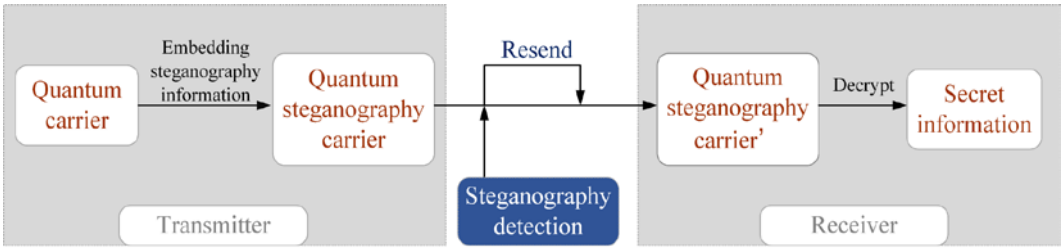

Fig. 1. General process of quantum steganography and steganalysis.

In pure-state-based quantum communication steganography protocols, the secret information is typically encoded onto a series of quantum bit strings based on the keys held by all communication parties. Since the steganography detector does not have access to these keys, intercepting the transmitted qubits does not reveal the secret information. In such protocols, the probability distribution of quantum channels often indicates the presence of

secret information to some extent. For instance, in certain protocols, the further the probability distribution deviates from high-frequency distributions like uniform or normal distributions, the more likely it is that the secret information is concealed within the quantum carrier.

Using the normal communication carrier and the steganographic carrier directly as input data for a quantum neural network poses significant challenges in training the model and achieving high accuracy. Therefore, a well-designed preprocessing process is necessary. The objective of this preprocessing process is to amplify the steganographic signal within the carrier and obtain more effective feature expression. Subsequently, the preprocessed labeled data are fed into the parametric quantum circuit for training, resulting in an automatic quantum steganalysis recognizer.

3.2 Preprocessing of quantum communication steganography protocol based on pure states

Let the probability distribution of quantum channel be (1).

$$\left\{\left|\varphi_i\right\rangle, \eta_i\right\}_{i=1}^{k} \tag{1}$$

It corresponds to pure state $\rho_i = \left|\varphi_i\right\rangle\left\langle\varphi_i\right|$. Construct feature expression matrix as (2).

$$\rho = \sum_{i,j=1}^{k} \sqrt{\eta_i \eta_j}\left\langle\varphi_i\middle|\varphi_j\right\rangle |i\rangle\langle j| = \begin{bmatrix} \eta_1 & \sqrt{\eta_1\eta_2}\left\langle\varphi_1\middle|\varphi_2\right\rangle & \cdots & \sqrt{\eta_1\eta_i}\left\langle\varphi_1\middle|\varphi_i\right\rangle \\ \sqrt{\eta_2\eta_1}\left\langle\varphi_2\middle|\varphi_1\right\rangle & \eta_2 & \cdots & \sqrt{\eta_2\eta_k}\left\langle\varphi_2\middle|\varphi_k\right\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \sqrt{\eta_k\eta_1}\left\langle\varphi_k\middle|\varphi_1\right\rangle & \sqrt{\eta_k\eta_2}\left\langle\varphi_k\middle|\varphi_2\right\rangle & \cdots & \eta_k \end{bmatrix} \tag{2}$$

The equivalent discrimination group is constructed according to its corresponding column, $\left\{\left|\phi_i\right\rangle, \eta_i\right\}_{i=1}^{k}$, where equivalent discrimination state is defined as (3).

$$\begin{aligned} \left|\phi_i\right\rangle &= \eta_i^{-\frac{1}{2}}\sqrt{\rho}\left|i\right\rangle = \begin{bmatrix} \sqrt{\eta_1\eta_i}\left\langle\varphi_1\middle|\varphi_i\right\rangle \\ \sqrt{\eta_2\eta_i}\left\langle\varphi_2\middle|\varphi_i\right\rangle \\ \vdots \\ \sqrt{\eta_k\eta_i}\left\langle\varphi_k\middle|\varphi_i\right\rangle \end{bmatrix} \\ &= \sqrt{\eta_1\eta_i}\left\langle\varphi_1\middle|\varphi_i\right\rangle\left|00\ldots0\right\rangle_k + \sqrt{\eta_2\eta_i}\left\langle\varphi_2\middle|\varphi_i\right\rangle\left|00\ldots1\right\rangle_k + \ldots + \sqrt{\eta_k\eta_i}\left\langle\varphi_k\middle|\varphi_i\right\rangle\left|11\ldots1\right\rangle_k \\ &= \sqrt{\eta_1\eta_i}\left\langle\varphi_1\middle|\varphi_i\right\rangle|1\rangle + \sqrt{\eta_2\eta_i}\left\langle\varphi_2\middle|\varphi_i\right\rangle|2\rangle + \ldots + \sqrt{\eta_k\eta_i}\left\langle\varphi_k\middle|\varphi_i\right\rangle|k\rangle \end{aligned} \tag{3}$$

The construction of equivalent discrimination groups aims to capture the correlation among equivalence discrimination states within the group and extract their characteristics to obtain statistical data. This statistical data is then input into quantum neural networks to effectively distinguish between steganographic and non-steganographic carriers.

In the quantum steganography communication protocol, set $\left|\varphi_0\right\rangle$ as ground state $\left|0\right\rangle$ in $\left\{\left|\varphi_i\right\rangle, \eta_i\right\}_{i=1}^{k}$, and other quantum states satisfy (4).

$$\begin{aligned} |\varphi_1\rangle &= R_{p1}(\theta_1)|\varphi_0\rangle, \\ |\varphi_2\rangle &= R_{p2}(\theta_2)|\varphi_0\rangle, \\ &\vdots \\ |\varphi_k\rangle &= R_{pk}(\theta_k)|\varphi_0\rangle. \end{aligned} \tag{4}$$

In (4), $p \in \{I, X, Y, Z\}$ and I, X, Y, Z are denoted as Pauli operations. This method can represent the carrier used in general quantum covert communication. Take the classical quantum key distribution protocol BB84 as an example in (5).

$$\begin{aligned} |\varphi_0\rangle &= |0\rangle, \\ |\varphi_1\rangle &= R_X(\pi)|0\rangle = |1\rangle, \\ |\varphi_2\rangle &= R_Y\left(\frac{\pi}{2}\right)|0\rangle = |+\rangle, \\ |\varphi_3\rangle &= R_Y\left(-\frac{\pi}{2}\right)|0\rangle = |-\rangle. \end{aligned} \tag{5}$$

The equivalent discrimination states are used for preprocessing. As shown in **Fig. 2**, the quantum information is transferred into the amplitude of quantum states by using the quantum inverse Fourier transform. Then the quantum information of the abnormal signal is amplified by using the amplitude amplification, which is input into the designed quantum neural network as training data.

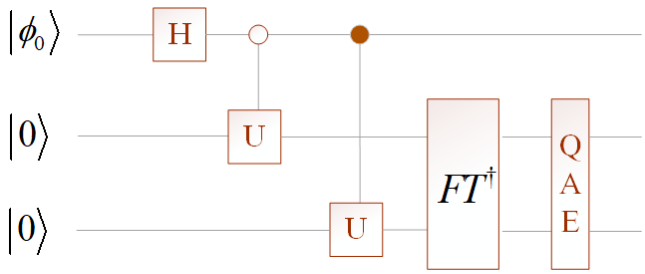

Fig. 2. Quantum data preprocessing.

The circuit of quantum amplitude estimation is shown in **Fig. 3**.

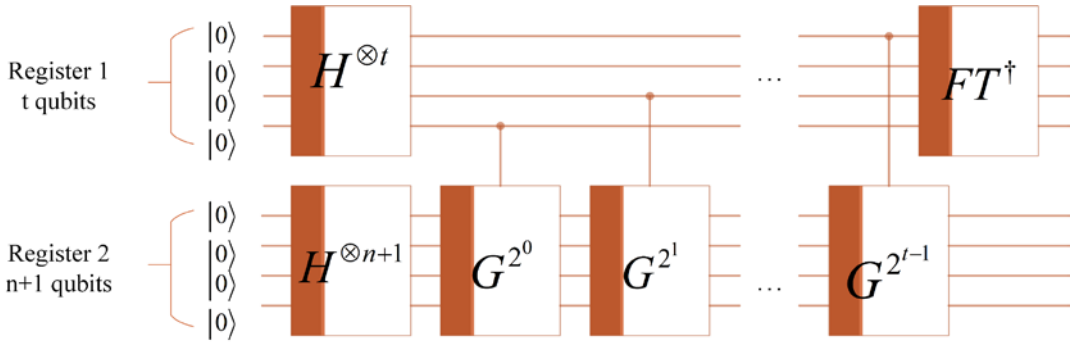

Fig. 3. The circuit of quantum amplitude estimation procedure.

3.3 Quantum discriminator

The basic module of the quantum discriminator is composed by unitary qubit rotation gates and controlled-not gates as is shown in **Fig. 4**. The inputs of each basic module are two qubits. The structure of the discriminator is changeable according to the number of input qubits as shown in **Fig. 5**.

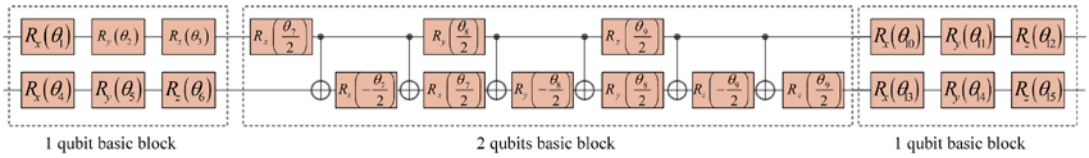

Fig. 4. The fundamental module of the quantum discriminator.

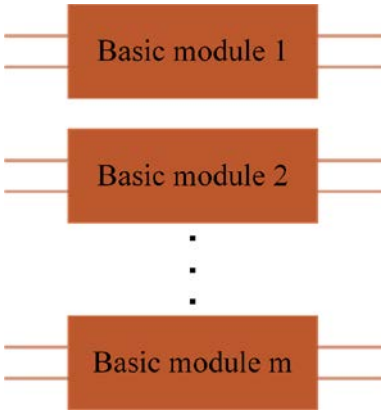

Fig. 5. Variable structure of the discriminator.

The operations by quantum gates on single qubit or two qubits in a basic module is shown in (6).

$$\begin{aligned} U(\vec{\theta}) = {} & R_x^1(\theta_1) R_y^1(\theta_2) R_z^1(\theta_3) R_x^2(\theta_4) R_y^2(\theta_5) R_z^2(\theta_6) R_x^1\left(\frac{\theta_7}{2}\right) U_{C-NOT}^{12} R_x^2\left(-\frac{\theta_7}{2}\right) \\ & U_{C-NOT}^{12} R_x^2\left(\frac{\theta_7}{2}\right) R_y^1\left(\frac{\theta_8}{2}\right) U_{C-NOT}^{12} R_y^2\left(-\frac{\theta_8}{2}\right) U_{C-NOT}^{12} R_y^2\left(\frac{\theta_8}{2}\right) R_z^1\left(\frac{\theta_9}{2}\right) U_{C-NOT}^{12} \\ & R_z^2\left(-\frac{\theta_9}{2}\right) U_{C-NOT}^{12} R_z^2\left(\frac{\theta_9}{2}\right) R_x^1(\theta_{10}) R_y^1(\theta_{11}) R_z^1(\theta_{12}) R_x^2(\theta_{13}) R_y^2(\theta_{14}) R_z^2(\theta_{15}) \end{aligned} \tag{6}$$

When it comes to a rotation gate with the parameter θ_j, the gradient of this parameter can be obtained by (7).

$$\frac{\partial}{\partial \theta_j} R_p(\theta_j) = \frac{\partial}{\partial \theta_j} e^{-i\theta_j P/2} = -\frac{i}{2} P R_p(\theta_j) \tag{7}$$

At the end of the quantum modules, the measurement operation W will be operated to the qubits as (8) shows. And the gradient corresponding to the measurement result is shown in (9).

$$\left\langle W(\vec{\theta}) \right\rangle = tr\left(\rho_0 U^{\dagger}(\vec{\theta}) W U(\vec{\theta})\right) \tag{8}$$

$$\frac{\partial}{\partial\theta_j}\langle W(\vec{\theta})\rangle = \begin{cases} -\frac{i}{2}tr\left(\rho_0 U_{1:j}^{\dagger}\left[U_{j+1:k}^{\dagger} W U_{k:j+1}, W\right] U_{j:1}\right), \text{ for } j = 1,\ldots,6 \text{ and } 10,\ldots,15 \\ -\frac{i}{4}tr\left(\rho_0 U_{1:j}^{\dagger}\left[U_{j+1:k}^{\dagger} W U_{k:j+1}, W\right] U_{j:1}\right), \text{ for } j = 7,8,9 \end{cases} \tag{9}$$

The cost function is defined as steganographic detection indicator (SDI) in (10).

$$f_{SDI} = f_C - \tilde{f}_C = \frac{1}{2N}\sum_{i=1}^{N}\left(\left(y^i - f_{\{\vec{\theta}_i\}}\left(\left|\phi^i\right\rangle\right)\right)_C^2 - \left(y^i - \tilde{f}_{\{\vec{\theta}_i\}}\left(\left|\phi^i\right\rangle\right)\right)_{\tilde{C}}^2\right) \tag{10}$$

The training process of the quantum neural network, composed of quantum circuits, is depicted in **Fig. 6**, utilizing the gradient descent method as the parameter update rule. Initially, the input data is randomly chosen using a coin flip. The tails and heads of the coin represent non-steganography data and steganography data, respectively. After multiple parameter updates, the optimal parameters are obtained. The detector then determines whether the input carriers are embedded with secret information or not. Throughout the training process, the rotation operators' parameters in the quantum discriminator circuits are initialized randomly. The loss function is then minimized to obtain the optimal parameters.

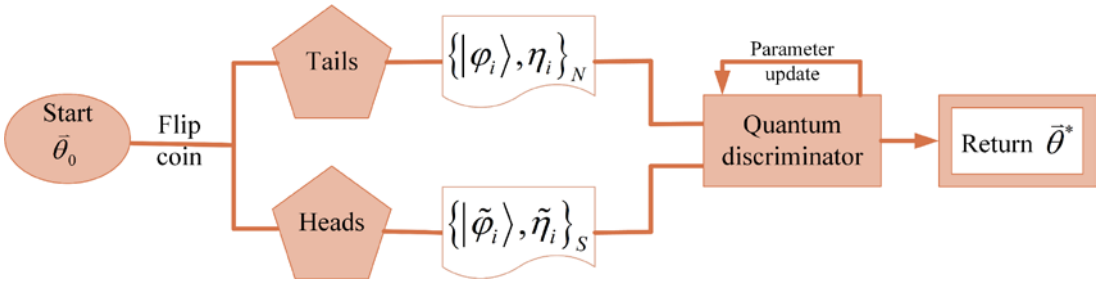

Fig. 6. Training flow of the discriminator.

The algorithm of the training process is shown in **Fig. 7**. The quantum carriers with or without encoded secret information $\{|\varphi_i\rangle, \eta_i\}_{i=1}^k$, $\{|\tilde{\varphi}_i\rangle, \tilde{\eta}_i\}_{i=1}^k$ are the input of our discriminator. And the detector will give the result on whether the input carriers are embedded with secret information or not. During the training process, first we randomly choose some values to initial all the parameters of rotation operators in the quantum discriminator circuits. Then minimize the loss function and get the optimal parameters.

Algorithm 1 Quantum discriminator.

Input: quantum carriers $\{|\varphi_i\rangle, \eta_i\}_{i=1}^{k}$, $\{|\tilde{\varphi}_i\rangle, \tilde{\eta}_i\}_{i=1}^{k}$
Output: Steganography detection results
$Q \leftarrow \emptyset$
// construct training quantum samples
for all $quantumcarriers$ **do**
put a quantum sample q_data in to Q
end for
// train the model
initialize all learnable parameters $\left\{\vec{\theta}_i\right\}$ in quantum discriminator
repeat
randomly select a batch of samples q_data from Q
find $\left\{\vec{\theta}_i\right\}$ by minimizing the objective $f_{SDI}\left\{\vec{\theta}_i\right\}$ with q_data
until stopping criteria is met
return $Steganography\_detection\_results$

Fig. 7. The algorithm of the quantum discriminator.

4. Numeral results

To conduct numerical experiments, a group of quantum states $\left\{\left|\varphi_i\right\rangle, \eta_i\right\}_{i=1}^{k}$ is prepared for quantum secure communication, adhering to a specific probability distribution (such as classical uniform distribution, normal distribution, etc.). Each group of quantum states can transmit a certain amount of classical information bits based on the corresponding communication protocols. We present the results of five experiments, evaluating the performance of the discriminator using the Steganography Detection Index (SDI). If the mean (or peak) of SDI in each epoch surpasses a certain threshold, it indicates the presence of steganography in the quantum communication.

The first experiment involves two normal distributions, N (0,0.01) and N (0,0.02). The curve depicting the SDI with respect to epochs is illustrated in **Fig. 8**.

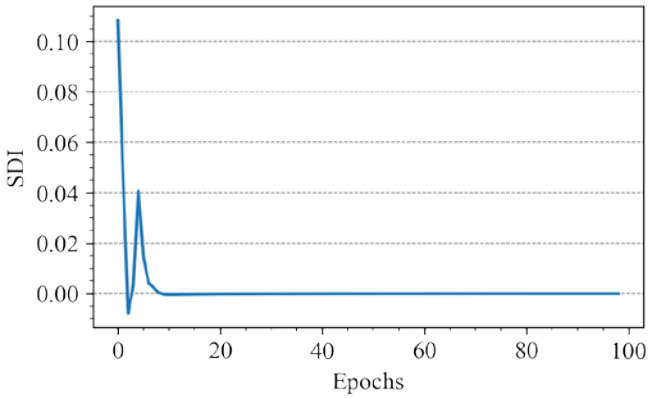

Fig. 8. The curve representing the SDI over epochs in the experiment using the distributions N (0,0.01) and N (0,0.02).

The second experiment involves two normal distributions, N (0,0.1) and N (0,0.2). In this experiment, the difference between the two distributions is larger than in the first experiment, indicating a higher amount of embedded secret information in the carriers. The curve illustrating the SDI over epochs is presented in **Fig. 9**.

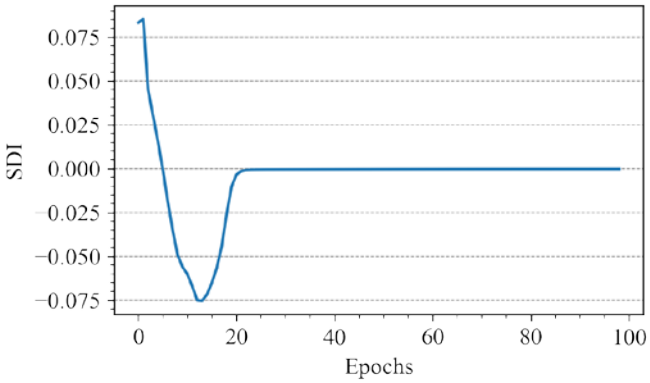

Fig. 9. The curve displaying the SDI over epochs in the experiment using the distributions N (0,0.1) and N (0,0.2).

The third experiment is conducted using a uniform distribution, U (0,1), and a normal distribution, N (0,0). In this experiment, the disparity between the two distributions is greater than in the second experiment due to the distinct types of distributions used. Consequently, there is an even higher amount of secret information embedded in the carriers compared to the second experiment. The curve depicting the SDI over epochs is displayed in **Fig. 10**.

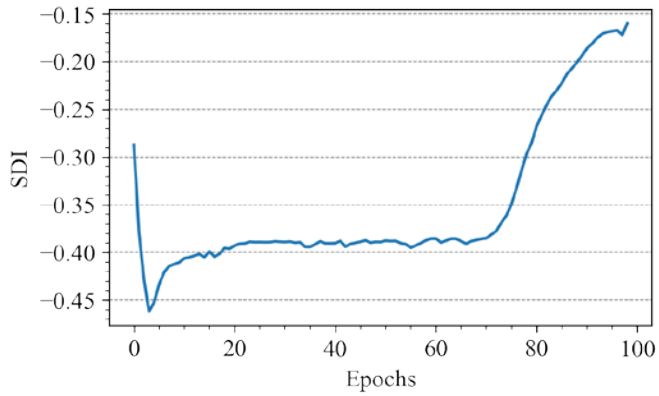

Fig. 10. The curve showing the SDI over epochs in the experiment using the distributions U(0,1) and N(0,0).

The fourth experiment is conducted using two uniform distributions, U (0,1) and U (0,0.99). The curve illustrating the SDI over epochs is presented in **Fig. 11**.

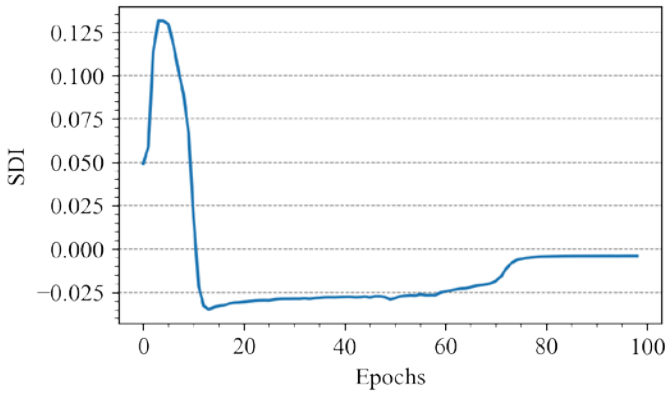

Fig. 11. The curve illustrating the SDI over epochs in the experiment using the two uniform distributions U (0,1) and U (0,0.99).

The fifth experiment involves two uniform distributions, U (0,1) and U (0,0.9). In this experiment, the disparity between the two distributions is larger than in the fourth experiment, indicating a higher amount of secret information embedded in the carriers. The curve depicting the SDI over epochs is displayed in **Fig. 12**.

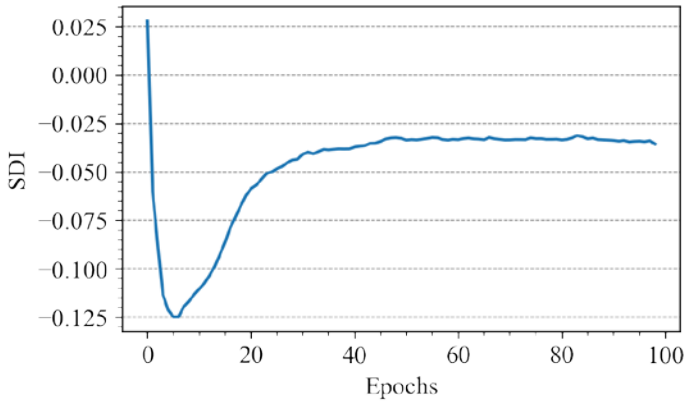

Fig. 12. The curve depicting the SDI over epochs in the experiment using the distributions U (0,1) and U (0,0.9).

Choosing a reasonable threshold, K_th, for the quantum discriminator is crucial as it directly impacts the steganography detection rate (SDR), as shown in **Table 1**. From **Table 1**, it can be observed that the greater the difference between the probability distributions of steganographic and non-steganographic data, the higher the SDI, making it easier to detect the presence of steganography.

The selection of K_th is another important aspect to consider. Based on our numerical experiments, when K_th is chosen within the range of -0.002 to 0.002, the performance of the quantum discriminator is satisfactory.

Table 1. Performance analysis of the quantum discritor.

Number	Probability distribution		SDI_AVG	K_th	SDR
1	N (0,0.01)	N (0,0.02)	0.002	±0.001	50%
				±0.002	0
2	N (0,0.1)	N (0,0.2)	-0.005	±0.001	80%
				±0.002	60%
3	U (0,1)	N (0,0)	-0.352	±0.001	99.7%
				±0.002	99.4%
4	U (0,1)	U (0,0.99)	0.008	±0.001	87.5%
				±0.002	75%
5	U (0,1)	U (0,0.9)	-0.047	±0.001	98.9%
				±0.002	95.7%

5. Conclusion

This paper introduces a novel quantum steganalysis algorithm to address the lack of research in the field of steganalysis. The algorithm utilizes a quantum discriminator based on quantum neural networks to detect the presence of steganography in general quantum secure communication schemes using pure state carriers. Simulation results demonstrate the feasibility of the proposed quantum steganalysis algorithm and confirm that a higher difference between the probability distributions of steganographic and non-steganographic data leads to a higher SDR value. The experimental results also highlight the significant influence of the threshold value, K_th, on the algorithm's performance.

However, there are certain limitations to this work. Firstly, in the simulation experiments, the probability distributions of quantum states before and after steganography are set as common distributions. In actual communications, the diversity of steganography methods makes it challenging to predict the probability distributions of quantum states in advance or describe them using specific probability distributions. Additionally, as the steganography embedding rate decreases, it becomes more difficult to detect the differences between quantum carriers before and after steganography. Lastly, the current special steganalysis algorithms are insufficient to handle the ever-evolving steganography technology. Therefore, there is an urgent need to develop universal steganography schemes.

In future work, we plan to focus on improving the performance of the quantum discriminator when steganography has minimal impact on the probability distribution of quantum pure state carriers. Additionally, we aim to design algorithms that can detect the content of steganography for common methods such as LSB steganography, as the current steganography detection primarily focuses on detecting the presence of steganography.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (No. 61373131, 61601358, 61501247, 61672290, 61303039, 61232016); Natural Science Foundation of Jiangsu Province (Grant No. BK20171458); Sichuan Youth Science and Technique Foundation (No.2017JQ0048); Open Foundation of State Key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) (SKLNST-2020-1-17), PAPD and CICAEET funds.

References

[1] G. Xu, K. Xiao, Z. Li, X. Niu and M. Ryan, “Controlled secure direct communication protocol via the three-qubit partially entangled set of states,” *Comput. Mater. Continua*, vol. 58, no. 3, pp. 809-827, Jan. 2019. Article (CrossRef Link)

[2] S. Y. Wu, W.J. Liu and Z.G. Qu, “A Novel Method to against Quantum Noises in Quantum Teleportation,” *J. Quantum Comput.*, vol. 2, no. 1, pp. 33-55, 2020. Article (CrossRef Link)

[3] G. F. Luo, R. G. Zhou and W. W. Hu, “Efficient quantum steganography scheme using inverted pattern approach,” *Quantum Inf. Process*, vol. 18, no. 7, pp. 1-24, may. 2019. Article (CrossRef Link)

[4] Z. G. Qu, S. Y. Wu and W. J. Liu, “Analysis and improvement of steganography protocol based on bell states in noise environment,” *CMC-Computers Materials & Continua*, vol. 59, no. 2, pp. 607-624, Jan. 2019. Article (CrossRef Link)

[5] Z. G. Qu, H. R. Sun and M. Zheng, “An efficient quantum image steganography protocol based on improved EMD algorithm,” *Quantum Inf. Process*, vol. 20, no. 53, pp. 1-29, Feb. 2021. Article (CrossRef Link)

[6] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado and M. Voznak, “Quantum key distribution: a networking perspective,” *ACM COMPUT SURV*, vol. 53, no. 5, pp.1-41, Oct. 2020. Article (CrossRef Link)

[7] X. Liao, Q. Y. Wen, Y. Sun et al, “Multi-party covert communication with steganography and quantum secret sharing,” *J. Syst. Softw.*, vol.83, no.10, pp.1801-1804, Apr. 2010. Article (CrossRef Link)

[8] Z. G. Qu, X. B. Chen, X. J. Zhou, et al, “Novel quantum steganography with large payload,” *Opt. Commun.*, vol. 283, no. 23, pp. 4782-4786, Dec. 2010. Article (CrossRef Link)

[9] A. A. El-latif, B. Abd-El-Atty and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol*, vol. 116, pp.92-102, Aug. 2019. Article (CrossRef Link)
[10] N. Jiang and L. Wang, "A novel strategy for quantum image steganography based on Moiré pattern," *Int. J. Theor. Phys.*, vol. 54, no. 3, pp. 1021-1032, Aug. 2015. Article (CrossRef Link)
[11] S. Dumitrescu, W. Xiaolin and W. Zhe, "Detection of LSB Steganography via Sample Pair Analysis," *IEEE Trans. Signal Process*, vol. 51, no. 7, pp. 1995-2007, July. 2003. Article (CrossRef Link)
[12] J. Fridrich, and M. Goljan, "On estimation of secret message length in LSB steganography in spatial domain," *Security, Steganography, and Watermarking of Multimedia Contents VI*, 2004. Article (CrossRef Link)
[13] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Process Lett.*, vol. 12, no. 6, pp. 441-444, June. 2005. Article (CrossRef Link)
[14] L. Sun, Y. L. Wang, Z. G. Qu and N. N. Xiong, "BeatClass : A Sustainable ECG Classification System in IoT-based eHealth," *IEEE Internet Things J.*, vol. 9, no. 10m pp. 7178-7195, 2022. Article (CrossRef Link)
[15] C. J. Burges, "A tutorial on support vector machines for pattern recognition," *Data Min Knowl. Discov.*, vol. 2, no. 2, pp. 121-167, 1998. Article (CrossRef Link)
[16] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble Classifiers for Steganalysis of Digital Media," *IEEE Trans. Inf. Forensics Secure*, vol. 7, no. 2, pp. 432-444, Apr. 2012. Article (CrossRef Link)
[17] Z. G. Qu, Y. M. Huang and M. Zheng, "A novel coherence-based quantum steganalysis protocol," *Quantum Inf. Process*, vol. 19, no. 10, pp.1-19, Sep. 2020. Article (CrossRef Link)
[18] J. Luo, R. G. Zhou, W. W. Hu, G. F. Luo and G. Liu, "Detection of steganography in quantum grayscale images," *Quantum Inf. Process*, vol. 19, no. 149, pp.1-10, Mar. 2020. Article (CrossRef Link)
[19] Y. Wei, F. Richard Yu, M. Song and Z. Han, "User Scheduling and Resource Allocation in HetNets with Hybrid Energy Supply: An Actor-Critic Reinforcement Learning Approach," *IEEE Trans. Wirel. Commun.*, vol. 17, no. 1, pp. 680-692, Jan. 2018. Article (CrossRef Link)
[20] Z. Xia, Q. Gu, W. Zhou, L. Xiong, J. Weng and N. Xiong, "STR: Secure computation on additive shares using the share-transform-reveal strategy," *IEEE Trans. Comput.*, Apr. 2021. Article (CrossRef Link)
[21] Z. Xia, L. Wang, J. Tang, N. Xiong and J. Weng, "A privacy-preserving Image Retrieval Scheme using Secure Local Binary Pattern in Cloud Computing," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 1, pp. 318-330, Jan. 2021. Article (CrossRef Link)
[22] Z. Xia, L. Jiang, D. Liu, L. Lu and B. Jeon, "BOEW: A Content-based Image Retrieval Scheme using Bag-of-Encrypted-Words in Cloud Computing," *IEEE Trans. Serv. Comput.*, vol. 15, no. 1, pp. 202-214. Jan.-Feb. 2022. Article (CrossRef Link)
[23] H. L. Chen, G. Xu, Y. L. Chen, X. B. Chen, Y. X. Yang et al., "Cipherchain: A Secure and Efficient Ciphertext Blockchain via mPECK," *J. Quantum Comput.*, vol. 2, no. 1, pp. 57-83, 2020. Article (CrossRef Link)
[24] W. Guo, N. Xiong, A. V. Vasilakos, G. Chen and H. Cheng, "Multi-source temporal data aggregation in wireless sensor networks," *Wirel. Pers. Commun*, vol. 56, no. 3, pp. 359-370, 2011. Article (CrossRef Link)
[25] P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum support vector machine for big feature and big data classification," *Phys. Rev. Lett.*, vol. 113, no. 13, pp. 130503, 2014. Article (CrossRef Link)
[26] A. W. Harrow, A. Hassidim and S. Lloyd, "Quantum algorithm for solving linear systems of equations," *Phys. Rev. Lett.*, vol. 103, no. 15, pp. 150502, 2012. Article (CrossRef Link)
[27] Y. Wei, Z. Wang, D. Guo and F. R. Yu, "Deep q-learning based computation offloading strategy for mobile edge computing," *Comput. Mater. Contin.*, vol. 59, no. 1, pp. 89-104, 2019. Article (CrossRef Link)
[28] M. H. Amin, E. Andriyash, J. Rolfe, B. Kulchytskyy and R. Melko, "Quantum Boltzmann machine," *Phys. Rev. X*, vol. 8, no. 2, pp. 021050, 2016. Article (CrossRef Link)

[29] S. Lloyd and C. Weedbrook, "Quantum generative adversarial learning," *Phys. Rev. Lett*, vol. 121, no. 4, pp. 040502, July, 2018. Article (CrossRef Link)
[30] I. Cong, S. Choi, M. D. Lukin, "Quantum Convolutional Neural Networks," *Nat. Phys.*, vol. 15, no. 1, pp. 1273-1278, 2019. Article (CrossRef Link)
[31] D. Dong, C. Chen, H. Li and T. J. Tarn, "Quantum reinforcement learning," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 38, no. 5, pp.1207-1220, 2008. Article (CrossRef Link)
[32] J. Liu, K. H. Lim, K. L. Wood, W. Huang, C. Guo and H. L. Huang, "Hybrid quantum-classical convolutional neural networks," *SCI CHINA Phys. Mech.*, vol. 64, no. 9, pp. 1-15, 2021. Article (CrossRef Link)
[33] Mitarai, Kosuke, N. Makoto, K. Masahiro and F. Keisuke, "Quantum circuit learning," *Phys. Rev. A.*, vol. 98, no. 3, pp. 032309, Jan. 2018. Article (CrossRef Link)

Xinzhu Liu, received the bachelor's degree in from Nanjing University of Information, Science and Technology, China, in 2020. She is currently studying for a master's degree at Nanjing University of Information, Science and Technology. Her research interests include quantum steganography, quantum secure communication, quantum computing, quantum machine learning.

Zhiguo Qu, received the Ph.D. degree in information security from Beijing University of Posts and Telecommunications, China, in 2011. From 2012 to 2014, he worked as a Post-doc Researcher Fellow at Dublin City University in Ireland. In July 2011, he joined Nanjing University of Information and Technology in China, where he is currently an Associate Professor in the School of Computer and Software. His research interests include quantum steganography, quantum secure communication, quantum computing, quantum machine learning.

Xiu-Bo Chen received the Ph.D. degree from Beijing University of Posts and Telecommunications in 2009. She is currently an associate professor in the school of cyber-space security at Beijing University of Posts and Tele-communications, Beijing, China. Her research interests include cryptography, blockchain and information security.

Prof. Xiaojun Wang received his MEng in computer applications in 1987 from BUPT. He received a PhD scholarship from the Sino-British Technical Co-operation Training Award in 1989, and did his PhD research in the School of Engineering in Staffordshire University (then Staffordshire Polytechnic), England, UK from 1989 to 1992. He joined the School of Electronic Engineering of Dublin City University as an assistant Lecturer in November 1992, permanent staff in 1995, and he is now an Associate Professor. He was Head of China Affairs in Dublin City University for five years between 2002 and 2007. His research interests include quantum secure communications.