Pune Institute of Computer Technology
Dhankawadi, Pune

A SEMINAR REPORT
ON

Quantum Steganography for Hiding Secret Text

SUBMITTED BY

Name : Mitesh Adake
Roll No. : 31401
Class: TE-4

Under the guidance of
Prof. Parag Jambhulkar

DEPARTMENT OF COMPUTER ENGINEERING
Academic Year 2021-22

DEPARTMENT OF COMPUTER ENGINEERING

Pune Institute of Computer Technology

Dhankawadi, Pune-43

CERTIFICATE

This is to certify that the Seminar report entitled

"Quantum Steganography for Hiding Secret Text"

Submitted by

Mitesh Adake Roll No. : 31401

has satisfactorily completed a seminar report under the guidance of Prof. Parag Jambhulkar towards the partial fulfillment of third year Computer Engineering Semester I, Academic Year 2021-22 of Savitribai Phule Pune University.

Prof. Parag Jambhulkar
Internal Guide

Dr. M.S.Takalikar
Head
Department of Computer Engineering

Place:Pune
Date: 09/11/2021

ACKNOWLEDGEMENT

It is my pleasure to present report on "Quantum Steganography for Hiding Secret Text". First of all, I would like to thank our Seminar Coordinator Prof. D.D. Kadam, Head of Department Dr. M.S.Takalikar and Principal Dr. R.Sreemathy for their encouragement and support.

I would also genuinely express my gratitude to my guide Prof. Parag Jambhulkar, Department of Computer Engineering for his constant guidance and help. He has constantly supported me and has played crucial role in completion of this report. His motivation and encouragement from beginning till end to make this seminar a success.

Last but not the least I would thank all the faculty, my parents and friends who have helped me.

Contents

1 INTRODUCTION **1**

2 MOTIVATION **2**

3 LITERATURE SURVEY **3**

4 A SURVEY ON PAPERS **4**
4.1 Why Quantum Steganography Can Be Stronger Than Classical Steganography 4
4.2 Steganography Protocols for Quantum Channels 4
4.3 Quantum Steganography Embedded Any Secret Text without Changing the Content of Cover Data 4
4.4 An Information-Theoretic Model for Steganography 4

5 PROBLEM DEFINITION AND SCOPE **5**
5.1 Problem Definition 5
5.2 Scope 5

6 PROTOCOL USED FOR QUANTUM KEY DISTRIBUTION **6**
6.1 BB84 Protocol 6

7 METHODOLOGY **7**
7.1 Workflow 7
7.2 Calculations 8
7.3 Key Terms 8
7.4 Algorithm 8

8 RESULTS **10**

9 CONCLUSION **12**

References **13**

List of Tables

1 Literature survey 3
2 Encoding 6

List of Figures

1 Overall Quantum Steganography model: Workflow [6] 7
2 Validation and Generation of Shared Key 10
3 Embedding the Secret Text in the Cover Message and Decrypting the Cover Message 10
4 Implementing the Complete Protocol at once 10
5 Using the BB84 Key to embed the Message in Cover Message . . . 11

Abstract

Steganography is a technique of hiding secret data within an information like text, audio, image, video, and so on. With the rise of threats to classical computer's ways of communication, a quantum approach for data hiding can be used for secure communication between two parties. Early results of secure communication with superdense coding and quantum error-correction codes are not sufficient as these methods only showed technique to communicate securely between two parties, but did not show the technique to embed the data in a cover data. In this seminar, implementation of quantum steganography to hide the data as cover data will be done. Usage of Qiskit module will be done for creating the quantum states and quantum circuits. Further, results from IBM Quantum Hardware/ Qasm Simulator will be analyzed.

Keywords

Quantum Mechanics, Quantum Communication, Quantum Key Distribution, Cryptography, Hidden Data, Qubit.

1 INTRODUCTION

Quantum Computing has been studied for an extended time in the field of research and many researchers have come up with variety of applications. One of the applications in this field deals with cryptography. Securely sharing information among people has been an issue in the times of internet being accessible to most of the people. There have been many protocols that help us communicate securely, despite there are chances of eavesdropping. To develop a secure communication between two parties, a shared key is used to encrypt data/ message using the standard one-time-pad encryption scheme. Thus, generating a secure shared key between the parties is essential. But, all classical methods for distribution of a shared key are insecure because there is no way of preventing an eavesdropper from eavesdropping during the transit from Alice to Bob. Such methods will also be vulnerable to large scale quantum computers. In future, as a large scale quantum computers have potential to crack RSA encryption and prime factorization of huge numbers can be computed faster on a large scale quantum computer. An alternative method of secure communication can benefit the field of cybersecurity. This is where quantum comupters can be used to generate secure shared key with the properties of superpostion and entanglement.

With the rise of quantum technology and it's applications in cryptography can be extended to secure communication. Quantum Key Distribution(QKD) promises unconditional security based on laws of quantum physics. Unlike classical key distribution, It is not possible for eavesdropper to interrupt the quantum signals in the process of key distribution.

To generate a secure communication between two parties(Alice and Bob) requires a quantum cryptography protocol. BB84 protocol, developed by Charles Bennett and Gilles Brassard, is the first quantum cryptography protocol, which can be used to generate a shared key between two parties. Further, this key is used to encode. Steganography is method of hiding secret data;text can be hid by encoding the encrypted message generated from shared key. With an additional steganographic encoder for the cover data, which can be used to encode the message.

2 MOTIVATION

Recently the rise of privacy and data security has gained massive attention. Peer-to-peer communication can be vulnerable to various attacks. Using quantum mechanical properties in computer can help enhance the security. As quantum properties of qubit do not allow eavesdropper to keep transcript of quantum signals in the process of quantum key distribution. With potential of qubits to exhibit superposition and entanglement, which reduces the vulnerability of the key distribution. Quantum Computers have the ability to ehnance the privacy of data with it's properties of superposition, entanglement and no-cloning theorem.

3 LITERATURE SURVEY

The Following table shows the literature survey:

Table 1: Literature survey

No.	Paper Title	Summary	Limitations
1	Why Quantum Steganography Can Be Stronger Than Classical Steganography	Extended the model of classical steganography and showed quantum steganography model can be secure than classical model	Building a quantum steganography model while Noisy Intermediate-Scale Quantum era is difficult
2	Steganography Protocols for Quantum Channels	Showed that quantum channels are more diverse than classical channels	Practical implementation with current number of qubits
3	Quantum Steganography Embedded Any Secret Text without Changing the Content of Cover Data	Proposed a quantum steganography protocol embedding a secret message in plain text	Requires in advance sharing of quantum keys

4 A SURVEY ON PAPERS

4.1 Why Quantum Steganography Can Be Stronger Than Classical Steganography

This paper describes about a general model that can be created to hide the secret message into a cover data using quantum properties by extending the classical model. Later it also introduces to a quantum steganography system which can not be simulated or imitated on classical system. Comparison of the classical and quantum steganography is done by the author, with a block diagram for each system to be demonstrated. Although the system shown in the paper is hypothetical one. Last but not the least the author conclude with no clear answer of which system being stronger and claims it's practical use to be an open question.

4.2 Steganography Protocols for Quantum Channels

This paper is based on various steganography protocols that can be used for quantum channels. This paper also elaborates about the cover protocols and it's various ways to use for steganography. Finally, three main results are obtained describing the cover protocols in both classical and quantum systems. Another result obtained, when the channel is noiseless there is no requirement of a shared key to run the steganography protocol.

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

This paper focuses on embedding a secret text in a cover data without changing it. The attempt in this paper is to extend the BB84 protocol such that parties can not recover information using only local operations by classical communication among them. Describes about various steps to implement the proposed protocol. Further, the authors conclude that embedding a secret message in a plain text is more difficult than embedding in a video or audio file. AS it is easy to identify any change in a text as compared to identifying change in video or audio file by the eavesdropper.

4.4 An Information-Theoretic Model for Steganography

This information-theoretic model for steganography considers a situation as Simmons' "Prisoners' Problem". Based on this, a model of secret-key stegosystem is developed. A probabilistic model approach is used to encode the text message in cover text. The security of the steganography system is measured by the relative entropy between the distributions of covertext and stegotext. Later to test the performance of the system, a hypothesis testing is done by introducing eavesdropping

5 PROBLEM DEFINITION AND SCOPE

5.1 Problem Definition

To implement quantum steganography protocol to hide secret text in cover data.

5.2 Scope

The consistency of the protocol depends on the quantum hardware. Using a simulation will give perfect results, which might not be the case with actual quantum hardware. At present there is no practical implementation of a quantum steganography and implementing huge models mentioned in the paper are hypothetical and unstable with the current technology.

Current limitations of quantum technology makes it difficult for implementing a complete quantum based steganography. Thus, classical computers help in simulating and recording the messages. Although, Qiskit(Quantum Software Development Kit) is used for this instance, the results may vary depending on the software kit and the source code settings for measurement of the qubits from a quantum system.

6 PROTOCOL USED FOR QUANTUM KEY DISTRIBUTION

6.1 BB84 Protocol

In this protocol, two parties(Alice and Bob) want to develop a secure communication between them. To do this they need to generate a shared key, which can be used to encode their messages. Alice transmits a random secret key to Bob by sending the quantum states(usually string of polarized photons). Any interruption by Eve can lead to measuring of qubits, resulting into collapse of the quantum state into classical binary state. Eve also does not have the privilege to copy the qubits according to no-cloning theorem. This property will help Alice and Bob to figure out there is an interruption and can resend the bitstring to generate the shared key.
The following table shows the Alice's encoding of the qubits with all combination of bases with bitstring.

Table 2: Encoding

Bit in Alice's Bitstring	Corresponding bit in Alice's Bases	Encoding Bases	Qubit State
0	0	$\|0\rangle, \|1\rangle$	$\|0\rangle$
0	1	$\|+\rangle, \|-\rangle$	$\|+\rangle$
1	0	$\|0\rangle, \|1\rangle$	$\|1\rangle$
1	1	$\|+\rangle, \|-\rangle$	$\|-\rangle$

7 METHODOLOGY

7.1 Workflow

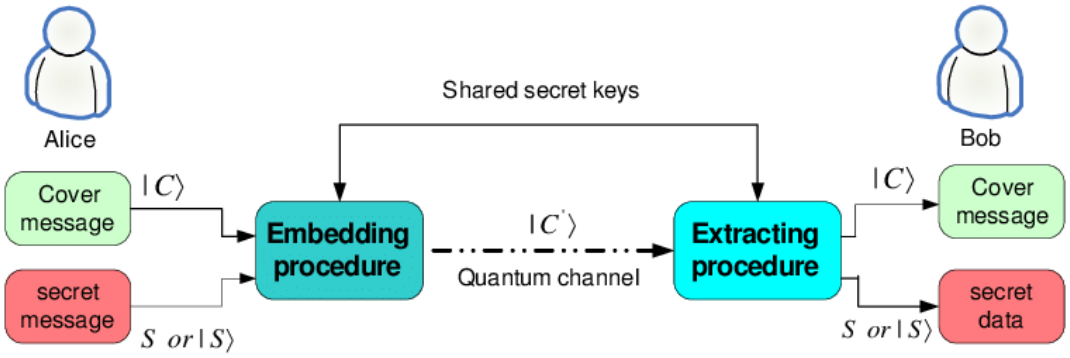

Figure 1: Overall Quantum Steganography model: Workflow [6]

7.2 Calculations

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \quad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}, \quad X = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}, \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$$

Qubit State representation in Computational basis:$|a\rangle = v_0|0\rangle + v_1|1\rangle$

$X|0\rangle = |1\rangle$

$X|1\rangle = |0\rangle$

$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$

$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$

Z-Basis: $|0\rangle, |1\rangle$

X-Basis: $|+\rangle, |-\rangle$

7.3 Key Terms

$\langle|, |\rangle : Bra - ketNotation$

X: Pauli-X Gate

H: Hadamard Gate

7.4 Algorithm

Consider two parties, Alice and Bob.

SELECT ENCODING: Alice randomly selects a basis (× or +) to encode each bit.

SELECT MEASUREMENT: Bob randomly selects a basis (× or +) to measure each

ENCODING: Alice creates the quantum states encoded in the selected bases.

SENDING: Alice sends Bob the encoded states via the quantum channel.

MEASUREMENT: Bob measures the quantum states in his pre-selected measurement bases.

SEND BASES: Alice send which basis were used to encode each bit via the classical channel.

FIND SYMMETRIC KEY: Alice and Bob discard bits in their key that used a different encoding and decoding basis.

ENCODER and DECODER: Build a encoder and decoder for the secret message using the shared key with the cover message.

8 RESULTS

```
In [18]:
alice_key = key_from_indices(alice_bitstring, CLASSICAL_CHANNEL)
bob_key = key_from_indices(bob_bitstring, agreeing_bases)

print("alice_key: ", alice_key[:20])
print("bob_key: ", bob_key[:20])
print("Alice's key is equal to Bob's key: ", alice_key == bob_key)

alice_key:  10010011010010010110
bob_key:  10010011010010010110
Alice's key is equal to Bob's key:  True
```

Finally after Alice and Bob discard every bit that was encoded using a basis that they didn't agree on, they will have a shared key at the end.

```
In [19]:
BB84_key = alice_key
BB84_key

Out[19]: '10010011010010010110110100100100110001101011001001000111100011111001100011010101011111101011001101100110101111011000100011101000000000010001101111000100100101001110011101010101100011101111000010000111110001111101001111101011101001110110001010001111011101100111'
```

Figure 2: Validation and Generation of Shared Key

```
In [23]:
message = "Quantum Steganography!"
print("Original Messge:", message,'\n')
encrypted_message = encrypt_message(message, alice_key)
carrier_msg=''.join([choice("abcdefghijklmnopqrstuvwxyz") for _ in range(len(encrypted_message))])
carrier_msg = encrypt_cover_msg(encrypted_message, carrier_msg)
print("Cover message:", carrier_msg,'\n')
decrypt_msg = decrypt_cover_msg(carrier_msg)
decrypted_message = decrypt_message(decrypt_msg, bob_key)
print("Decrypted message:", decrypted_message)

Original Messge: Quantum Steganography!

Cover message: DBiepjObteBQLKbbwjsqUQvphFruKbXeRuJMurBgFPojxMTDvlGqEyFrFsJiKAMLGDrrEaTTEqJgesaCohjEMvHFCDjSmYbwqbASCdmeIQxpx
qngYwbiKRpKjRaHMQaQcMBMxzFizqCgcHSYXrnycagFzPzwqnNkouuaThGaMBOIaCqj

Decrypted message: Quantum Steganography!
```

Figure 3: Embedding the Secret Text in the Cover Message and Decrypting the Cover Message

```
In [25]:
# Step 1
alice_bitstring, alice_bases = select_encoding(key_length)
# Step 2
bob_bases = select_measurement(key_length)
# Step 3
encoded_qubits = encode(alice_bitstring, alice_bases)
# Step 4
QUANTUM_CHANNEL = encoded_qubits
# Step 5
bob_bitstring = measure(bob_bases, QUANTUM_CHANNEL, Aer.get_backend('qasm_simulator'))
# Step 6
CLASSICAL_CHANNEL = alice_bases
agreeing_bases = bob_compare_bases(CLASSICAL_CHANNEL, bob_bases)
# Step 7
CLASSICAL_CHANNEL = agreeing_bases
alice_key = key_from_indices(alice_bitstring, agreeing_bases)
bob_key = key_from_indices(bob_bitstring, agreeing_bases)

print("alice_key: ", alice_key[:20])
print("bob_key: ", bob_key[:20])
print("Alice's key is equal to Bob's key: ", alice_key == bob_key)

alice_key:  10111101001010001111
bob_key:  10111101001010001111
Alice's key is equal to Bob's key:  True
```

Figure 4: Implementing the Complete Protocol at once

In [26]:

```
message = "Quantum Steganography!"
print("Original Messge:", message,'\n')
encrypted_message = encrypt_message(message, alice_key)
carrier_msg=''.join([choice("abcdefghijklmnopqrstuvwxyz") for _ in range(len(encrypted_message))])
carrier_msg = encrypt_cover_msg(encrypted_message, carrier_msg)
print("Cover message:", carrier_msg,'\n')
decrypt_msg = decrypt_cover_msg(carrier_msg)
decrypted_message = decrypt_message(decrypt_msg, bob_key)
print("Decrypted message:", decrypted_message)
```

```
Original Messge: Quantum Steganography!

Cover message: KFWsBVdkfPbAFBqQCwyWAqoOwOkcfkUfrmpzvxRHUOTYDZSigexFUlZMzaEfUDJEBlQnSnoiSoRBjHBALyhUHVPkeGbBtoccjuFEMBBWxNdnL
qUtXKkwsbmKAojvCYFFNLuyUqAtBywAJDdOrmFFGjjUuLEhIWyBaNqXtFCUbwBVqOvi

Decrypted message: Quantum Steganography!
```

Figure 5: Using the BB84 Key to embed the Message in Cover Message

9 CONCLUSION

A quantum steganography model was successfully implemented to hide the secret text with the cover message. The model was able to generate different shared keys between the two parties and could embed the secret message into the cover message.

The quantum steganography protocol was implemented on a simulator, without any error in the qubits' states. Thus, the protocol works for noiseless quantum computer.

References

[1] M. Tahmasbi and M. R. Bloch, "Steganography Protocols for Quantum Channels," 2019 IEEE International Symposium on Information Theory (ISIT), 2019, pp. 2179-2183, doi: 10.1109/ISIT.2019.8849593

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", Theor. Comput. Sci., vol. 560, pp. 7-11, 2014.

[3] Takashi Mihara, "Quantum Steganography Embedded Any Secret Text without Changing the Content of Cover Data", Journal of Quantum Information Science Vol.2 N0.1, 2012.

[4] S. Natori, "Why Quantum Steganography Can Be Stronger than Classical Steganography," Quantum Computation and Information, Vol. 102, 2006, pp. 235-240, 2006.

[5] Christian Cachin, "An information-theoretic model for steganography", Information and Computation, Volume 192, Issue 1, 2004.

[6] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, S. Elmougy and A. Ghoneim, "Secure Quantum Steganography Protocol for Fog Cloud Internet of Things," in IEEE Access, vol. 6, pp. 10332-10340, 2018, doi: 10.1109/ACCESS.2018.2799879.