An Improvement Steganography System Based on Quantum One Time Pad Encryption

Alharith A. Abdullah 1∗, Zaid A. Abod 2, and Mustafa S. Abbas 3

1) College of Information Technology, University of Babylon, Babil, Iraq
2) College of Food Science, Al-Qasim Green University, Babil, Iraq
3) College of Information Technology, University of Babylon, Babil, Iraq

Abstract

The goal of this work is to increase the confidentiality and security of the steganography system by combining the steganography system with the quantum cryptography. In this proposed system, the easiest and popular steganography method is the least significant bit (LSB) substitution is used to hide a secret message into a cover image and encrypt the output by using one of the quantum cryptography mechanisms, which is a quantum one-time pad. A model will be more secured due to combining two-security mechanisms, which are least significant bit and a quantum one time pad. The security analysis and how the model works are presented in this study. An overview of the complete process from the steganography system to the quantum encryption algorithm is illustrated explicitly.

Keywords: Steganography, Image Steganography, Least Significant Bit, Quantum Cryptography, Quantum Encryption Algorithm, Quantum One Time Pad.
I. Introduction

Cryptography is a wide science and always sophisticated by looking for new ideas that help in the evolution of this science. The idea of combining cryptography and steganography are emerging and the goal of these techniques is to provide confidentiality, authenticity, non-repudiation, integrity and data security. Cryptography and steganography are a closely related method where the steganography is considered the art of invisible communication, is achieved by hiding secret data inside a carrier file such as an image. After hiding the secret data, the carrier file should appear unsuspicious so that the very existence of the embedded data is concealed. On the other hand, cryptography is the art of secure communication, is achieved by encryption data. The encrypted Data is unreadable but if given enough time, once alerted, someone could potentially decrypt the data so it is a drawback. So the solution for this problem is the combining the cryptography with steganography where the encrypted data will be hiding and unreadable, therefore, cryptography and steganography are a closely related method.

There are many aspects proposed related to the combination of cryptography and steganography some of them close to our proposed idea.

According to [1], the researchers combine cryptography and steganography in their works they introduced classical One-Time Pad encryption and steganography system, including all software necessary to complete practical communication. Another similar approach but using different cryptography algorithm has been proposed by [2]. They used transposition cipher method for the encryption process. This encryption process has been combined with random LSB technique to make the model more secure. The researchers in [3] proposed a method for integrating cryptography and steganography for secure communication using an image file. The AES algorithm is used in encryption, which is then hidden into the cover image using the steganography concept. The authors in [4] presented a rapid combine method based on DES encryption and LSB steganography. Another proposed a method for integrating cryptography and steganography for secure communication using an image file. The RSA algorithm is used in encryption and LSB
technique for steganography [5]. Recently, two models are presented by combining cryptography and steganography. One of them employed a quick response codes for encoding the encrypted message before hiding it in the image. And the other model used classical hybrid algorithms, which is RSA and Diffie-Hellman before hiding it in the image [6] [7].

In this paper, we developed the idea of combining the cryptography and steganography by using quantum cryptography, which relies on quantum laws. We combine a complete steganography system with the quantum cryptography based on Quantum One-Time Pad (QOTP) encryption and least significant bit (LSB) substitution adaptive steganography technology. The hybrid system is tested and shown to be resistant to many common security analysis attacks. The rest of this paper is organized as follows: Section 2 reviews the (LSB) steganography. Section 3 produces the main concepts of the Quantum One-Time Pad (QOTP) and the related with the existing model. Section 4 presents the proposed model to produce a secure steganography. Section 5 discusses the experimental results and section 6 provides the concluding remarks.

II. LSB Steganography

The least significant bit (LSB) substitution is a simplest and a popular image steganography method [8]. This method replaces the least significant bits directly through embeds messages into the cover image. To increase the capacity of hiding it can be used up to four least significant bits (one each for Red, Green, Blue, and Alpha color channels, respectively) in each pixel. It has a common weak point i.e. the sample value changes asymmetrically. When the LSB of cover medium sample value is equal to the message bit, no change is made. Otherwise, the value 2n is changed to 2n+1 or 2n+1 is changed to 2n [9]. There are many improvements and modifications that have been proposed to strengthen this technique, such as adaptive techniques that alter payload distribution based on image characteristics. If the message is first encrypted and then embedded, the security is enhanced.
III. Quantum One-Time Pad

The "One-Time Pad" encryption algorithm was invented early and has since been proven as unbreakable. The ciphertext is proved to be unbreakable when the "One-Time Pad" condition is satisfied where the "one-time pad" is typically implemented by using exclusive-or (XOR) addition to combine plaintext elements with key elements, the key is completely random and the key cannot be used more than once and this is the conditions of the "one-time pad" to be unbreakable [10].

The central problem in "One-Time Pad" is distributed key where the key should be the same length with the plaintext among N number of users. Classical key distribution protocols are unable to detect an adversary between two legitimate parties. Quantum key distribution (QKD) protocol solves this problem. The most commonly used (QKD) protocol is BB84 [11]. The security of (QKD) is guaranteed by the laws of quantum. The quantum uncertainty principle explained in [12] allows to securely sharing a secret key among two legitimate parties.

The idea of a "Quantum One-Time Pad" (QOTP) is presented in [13]. The protocol works by transmitting the quantum particles from receiver to sender, where the sender embeds his information and then from sender to the receiver where "Quantum One-Time Pad" is an encryption scheme for qubits.

IV. PROPOSED MODEL

In this paper, we introduced a new model for two stages secure mechanism that uses quantum cryptography and steganography to secure and hide the secret message, prior to sending it via quantum communication channel.

A proposed model has five main processes; divided, embedding, encryption, decryption and extracting. For the divided and embedding processes we get the message and divide it to groups where each group has 8 character and then get the image and divide it to
blocks where each block has “9*9” cells and calculate the variance for each block and then will choose the blocks that have the highest value of variance depending on the numbers of groups of the characters, where this blocks will be using in hiding step as shown in figure (1). To make those blocks that are selected specific we will make the LSB of the center of the block “1”, and other unselected blocks to “0”. And after these operations we will hide the groups of message in blocks of image.

![Diagram](image-url)

**Figure (1):** hiding one group “eight character” of message in one Block “9*9” of image

**Algorithm of Sender side**  
**Input:** Message, Image  
**Output:** Qubits  
**Begin**  
1- Save the image in array  
2- Calculate the length of the message.
3- Divide the array of image to non-overlaying blocks, when each block has 9*9 cell
4- Calculate the variance of each block
5- Divide the message to groups when each group have eight character from the message, and store the number of groups in variable no_group.
6- Calculate the number of block and number of character in the last block:
   No of block = Length of message/8
   flag = false
   if Length of message mod 8 > 0 then
      flag = true
      no of block = no of block + 1
      no of char in last block = Length of message mod 8
   end if
7- Select the same number of blocks that have higher value of variance.
8- Make the least significant bit of the center of each selected block to "1".
9- Make the least significant bit of the center of each unselected block to "0".
10- By using least significant bit, we will be hiding group i in selected block i.
    For i = 1 to no of blocks or no of groups
    Begin
    If i = no of block AND flag = true then
       No of char = no of char in last block
    Else
       No of char = 8
    End if
    For j = 1 to no of char
    Begin
       Get the character j from group i and convert it to binary and save the result to binary array
       This will produce eight bit saved in array of eight cells
       If j=1 then
          Begin if
             If i = no of groups and flag = true then make least significant bit of indicator cell to 1.
          End if
          hide the eight bit of the binary array in the least significant bit cells of the vertical diameter cells of the block i.
       end if
       If j=2 then
          Begin if
             If i = no of groups and flag = true then make least significant bit of indicator cell to 1.
          End if
          hide the eight bit of the binary array in the least significant bit cells of the horizontal diameter of the block i.
       End if
       If j=3 then
          Begin if
       End if
If \( i = \text{no of groups} \) and flag = true then make least significant bit of indicator cell to 1.

hide the eight bit of the binary array in the least significant bit cells of the diagonal at an angle of 45 of the block \( i \)

End if

If \( j = 4 \) then

Begin if

If \( i = \text{no of groups} \) and flag = true then make least significant bit of indicator cell to 1.

hide the eight bit of the binary array in the least significant bit cells of the diagonal at an angle of 135 of the block \( i \)

End if

If \( j = 5 \) then

Begin if

If \( i = \text{no of groups} \) and flag = true then make least significant bit of indicator cell to 1.

hide the eight bit of the binary array in the least significant bit cells of the first quarter of the block \( i \) in circular form.

End if

If \( j = 6 \) then

Begin if

If \( i = \text{no of groups} \) and flag = true then make least significant bit of indicator cell to 1.

hide the eight bit of the binary array in the least significant bit cells of the second quarter of the block \( i \) in circular form.

End if

If \( j = 7 \) then

Begin if

If \( i = \text{no of groups} \) and flag = true then make least significant bit of indicator cell to 1.

hide the eight bit of the binary array in the least significant bit cells of the third quarter of the block \( i \) in circular form.

End if

If \( j = 8 \) then

Begin if

If \( i = \text{no of groups} \) and flag = true then make least significant bit of indicator cell to 1.

hide the eight bit of the binary array in the least significant bit cells of the fourth quarter of the block \( i \) in circular form.

End if

11- Convert all the data of image to Binary

12- Convert all the data produced from above step to Vector

13- Apply QOTP by applying a bit flips with the vector and quantum key, where
key is choosing by using BB84 protocol between sender and receiver.

14- The output of the algorithm sends via quantum channel.

15-End

**Figure (2): Algorithm of Sender Stage**

For the encryption process, "Quantum One-Time Pad" algorithm has been used to encrypt the data of the image that already convert it to quantum bits (Qubits) as shown in figure (2).

Figure (3) shows the block diagram of our proposed model, which included divided, hiding and encryption processes.

For decryption process, after the sender and receiver exchange the quantum key by using BB84 protocol the "Quantum One-Time Pad" algorithm has been used to decrypt the quantum bits (Qubits) that the receiver receive it and then convert to data of the image as shown in figure (4).

Figure (5) shows the block diagram of our proposed model, which included decryption processes, extracting information and final message.
Figure (3): Block Diagram of the Proposed System for Sender Stage

- **Image**
  - Divide Image to non-overlapping blocks, each block has 9*9 cell
  - Calculate the variance of each block
  - According to the number of groups, select the blocks that have the higher value of variance
  - Make the LSB of the center of each selected block to "1" and "0" for each unselected block
- **Message**
  - Calculate the length of the message
  - Calculate the length of the Message and divide the Message to groups, when each group has 8 characters

- **hide group \( i \) in selected block \( i \)**
- Convert the data of the image to Binary, and then Convert it to vector
- **Key**
- **QOTP**
- **Stream**
**Algorithm of receiver side**

**Input:** Qubits

**Output:** message

**Begin**

1. Received data (qubits) via quantum channel.
2. Apply QOTP by applying a bit flips with the vector and quantum key, where key is choosing by using BB84 protocol between sender and receiver.
3. Convert all the vectors to the Binary.
4. Convert all Binary to the data of Image.
5. Divide the array of Image to non-overlaying blocks, when each block has 9*9 cell.
6. Searching about the blocks that have the least significant bit of the cells in center’s blocks and select them.
7. Extracting the hidden message from selected blocks:
   - for i = 1 to number of selected blocks
     - if (i < number of selected blocks) OR (i = number of selected blocks and the least significant bit of the indicator cell equal to “1”) then:
       - get the least significant bit from the cells in the vertical diameter of the block i, and convert
       - the series of bits that extracted character.
     - if (i < number of selected blocks) OR (i = number of selected blocks and the least significant bit of the indicator cell equal to “1”) then:
       - get the least significant bit from the cells in the horizontal diameter of the block i, and convert
       - the series of bits that extracted character.
     - if (i < number of selected blocks) OR (i = number of selected blocks and the least significant bit of the indicator cell equal to “1”) then:
       - get the least significant bit from the cells in the diagonal at an angle of 45 of the block i, and convert
       - the series of bits that extracted character.
     - if (i < number of selected blocks) OR (i = number of selected blocks and the least significant bit of the indicator cell equal to “1”) then:
       - get the least significant bit from the cells in the diagonal at an angle of 135 of the block i, and convert
       - the series of bits that extracted character.
     - if (i < number of selected blocks) OR (i = number of selected blocks and the least significant bit of the indicator cell equal to “1”) then:
       - get the least significant bit from the cells in the of the first quarter of the block i, and convert
       - the series of bits that extracted character.
if (i < number of selected blocks) OR (i = number of selected blocks and the least significant bit of the indicator cell equal to “1”) then:
get the least significant bit from the cells in the of the second quarter of the block i, and
convert the series of bits that extracted character.
if (i < number of selected blocks) OR (i = number of selected blocks and the least significant bit of the indicator cell equal to “1”) then:
get the least significant bit from the cells in the of the third quarter of the block i, and
convert the series of bits that extracted character.
if (i < number of selected blocks) OR (i = number of selected blocks and the least significant bit of the indicator cell equal to “1”) then:
get the least significant bit from the cells in the of the fourth quarter of the block i, and
convert the series of bits that extracted character.
8- Collect the character and save them.
End

Figure (4): Algorithm of Receiver Stage
V. EXPERIMENTAL RESULT

The application involved two main modules; sender and receiver respectively. Figure (3) shows the sender interface. On the sender side, the user to browse an image, also access secret quantum key that shared by both parties by the BB84 protocol.

Principally, capacity is used as one of the evaluation criteria. Capacity can be defined as the amount of information that can be hidden within the cover image. By using the proposed algorithm, capacity can be expressed as a number of 8 bits, which indicates the maximum message size that might be inserted into an image. The histograms of cover and stego-images have been used to indicate that the proposed algorithm is very much statistically strong. The histograms are the common method to discover the effect of hiding data inside the cover image.

For testing purpose, several different images have been used with different width and height. In order to ensure the quality of the stego-image, Peak Signal-to-noise Ratio (PSNR). According to [14], PSNR is the ratio between the maximum values of signal measured by the amount of noise that affects the signal. The formula of PSNR calculation is defined as equation (1).

\[
PSNR = 20 \log_{10} \frac{C_{\text{max}}^2}{\text{MSE}} \quad (1)
\]

Where MSE is referring to Mean Square Error which has given in formula in equation (2).

\[
\text{MSE} = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2 \quad (2)
\]

\(C_{\text{max}}\) holds the maximum value in the original image. \(S_{xy}\) is the pixel of the cover image in which coordinate \((x, y)\) and \(C_{xy}\) is the pixel of the stego-image in the coordinate \((x, y)\). \(M\) and \(N\) is the size of the cover image and the stego-image.
In the experimental process, three images have been used as in Figure (6).

![Figure (6): Pictures Used in Experimental.](image)

The dimensions of the pictures are different. The secret message is different characters length. Table (1) shows the PSNR value for each stego-image. For comparison, the calculated PSNR values varied from (75.09 dB to 59.81 dB).

This result shows that the proposed algorithm produced a high capacity of secret message. In practice, it becomes very difficult to see the differences between the cover image and the stego-image especially in the high PSNR values. Where as long as the value of the PSNR is high the distortion of image will be low. In other words, the high value of PSNR will make the recognition of the image is difficult and the possibility of a variety of visual attacks by human eyes is low.

**Table (1): The PSNR Value for Stego-Image**

<table>
<thead>
<tr>
<th>Times of Sentences</th>
<th>Number of Characters</th>
<th>PSNR Value</th>
<th>Average PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Lena</td>
<td>Baboon</td>
</tr>
<tr>
<td>1</td>
<td>60</td>
<td>72.50</td>
<td>80.97</td>
</tr>
<tr>
<td>2</td>
<td>158</td>
<td>69.85</td>
<td>76.82</td>
</tr>
<tr>
<td>3</td>
<td>238</td>
<td>68.63</td>
<td>74.99</td>
</tr>
<tr>
<td>4</td>
<td>400</td>
<td>66.72</td>
<td>72.79</td>
</tr>
<tr>
<td>5</td>
<td>518</td>
<td>65.84</td>
<td>71.53</td>
</tr>
<tr>
<td>6</td>
<td>972</td>
<td>63.32</td>
<td>69.03</td>
</tr>
<tr>
<td>7</td>
<td>1500</td>
<td>61.56</td>
<td>67.17</td>
</tr>
</tbody>
</table>
Figure (7) shows the histogram for the originals images (a). Histogram images in (b) are for the cover images while images in (c) are the histogram for the stego-images. The histogram for the stego-images is similar to their respective original images if observed using naked eyes. This emphasizes on the result that the distortion between the cover image and the stego-image is minimum.
VI. CONCLUSION

In this paper, we have presented a complete "Quantum One-Time Pad" (QOTP) encryption and steganography system, including all software necessary to complete practical communication. This is first time combine between steganography system and quantum encryption where in this model, the least significant bit (LSB) responsible for embedding the secret message while "Quantum One-Time Pad" (QOTP) is responsible for encrypting and decrypting the stego-image.

This model is robust because extracting data without knowing the architecture of the proposed technique and extracting data is difficult because all the classical data convert it to quantum bits (Qubits). Where the eavesdropper cannot get the information from the cover image; he still could not read the secret message because it is in the form of quantum ciphertext. From the experimental result, it has proved that the model will produce a good quality image after inserting the high capacity of a secret message for instance 3000 characters with the average PSNR value of 59.81 dB. When the embedding capacity of the secret message increases, it will result in a slight decline of PSNR value.
References


