mathematics

MDPI

Article

Quantum Steganography Based on the B92 Quantum Protocol

Alexandru-Gabriel Tudorache *, Vasile Manta and Simona Caraiman

Department of Computer Science and Engineering, Gh. Asachi Technical University of Iasi, D. Mangeron 27A, 700050 Iasi, Romania

* Correspondence: alexandru-gabriel.tudorache@academic.tuiasi.ro

Abstract: This paper presents a communication algorithm in which a grayscale image, shared between two parties, can be used to transmit a secret message, by applying the idea introduced in the B92 quantum protocol. The least significant qubits of the pixels' representation in certain regions of the image are used. With the help of a server, the algorithm generates a random message, which can further act as a secret key for cryptographic algorithms in order to secure the data that two parties might want to exchange later on. The chosen representation of the image is NEQR (novel enhanced quantum representation) and the platform used for testing the described idea is IBM Quantum Experience, along with the open-source Python framework called Qiskit. This solution allows users to design, implement quantum circuits (containing various quantum gates), and simulate them using real devices and local simulators. An implementation using this platform for a sample image and the corresponding results are also presented in this paper.

Keywords: cryptography; quantum steganography; quantum image representation; least significant bit; quantum key distribution; quantum circuit

MSC: 81P68

check for updates

Citation: Tudorache, A.-G.; Manta, V.; Caraiman, S. Quantum Steganography Based on the B92 Quantum Protocol. *Mathematics* **2022**, *10*, 2870. https://doi.org/10.3390/math10162870

Academic Editors: Theodore Andronikos and Georgios I. Goumas

Received: 15 July 2022
Accepted: 9 August 2022
Published: 11 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Cryptography and its applications present the utmost importance in the classical information processing research areas. The theory and analysis for different cryptographic algorithms used in encrypting day-to-day communication to and from commonplace computers, ranging from social media private chats to internet banking applications, is exactly the part that guarantees that the operations carried out by the average user on the internet can be conducted safely and without much privacy concerns. Now, with the rise of the Internet of Things (IoT) universe, we also have to mention the specially designed algorithms and hardware platforms for the embedded devices, which require new operating conditions, such as low power, a longer life span, and so on—see paper [1] for the challenges met when proposing the architecture of these devices.

Quantum information processing is one of the most promising fields in computer science and engineering, with huge speed-up potential, but also represents a real threat to the security protocols in place in today's world. Since its beginnings, the emergence of this field has raised the problem of how the classical security protocols would be able to resist the attacks launched using this new technology, as well as how the new quantum algorithms would have to be designed in order to keep the same level of security, without compromising the power usage (and other physical factors). This requires another way of thinking, by also processing the data in a new environment, and by also using the quantum properties, such as entanglement and superposition, to be able to fully utilize the quantum processing power.

Section 2 presents some related papers in the field of quantum cryptographic protocols. Section 3 goes over some of the quantum representation techniques developed by different researchers, briefly presents the core concepts behind the chosen platform (IBM Quantum

Experience and Qiskit) used to simulate the algorithm, and then describes the proposed protocol. Section 4 presents the implementation details using a sample grayscale image, the circuits, and the obtained simulation results; it also shows the mathematical formulas on which the illustrated algorithm relies. The final section is the conclusion of the paper and it highlights the main points achieved in this article.

2. Related Work

Multiple quantum algorithms have been proposed over the years, and the following paragraphs present some of the most relevant quantum cryptographic protocols. A comprehensive review of multiple techniques used in quantum cryptography along with their analyses are presented in the paper [2].

One of the best-known quantum key distribution (QKD) protocols is the BB84 protocol (see article [3]). This protocol uses two bases and four states, with two states from each basis; the classical choice is the pair of $|0\rangle$ and $|1\rangle$ states for the Z basis, and $|+\rangle$ and $|-\rangle$ states for the X basis. A key point is that that an eavesdropper cannot clone any states (this would break the no-cloning theorem), nor interfere in any other way without Alice and Bob (the two entities used in describing cryptographical protocols) being aware of this fact. For each qubit, Alice encodes her value and sends it to Bob, who measures it using a random basis. The combination between the $|0\rangle$ and $|+\rangle$ states is translated to a value of 0, while the $|1\rangle$ and $|-\rangle$ states indicate a value of 1. This combination ensures the non-orthogonality condition and guarantees that the condition cannot be cloned or measured accurately. After transmitting the qubits, Bob also sends Alice the measurement basis he used for each qubit and Alice responds with her measurement basis, at which point, both parties have a common key; after this step, they decide to only keep a random number of these qubits, which will represent the secret key.

Another QKD protocol was proposed in 1992 by Charles Bennett, also known as B92 (see paper [4]). Unlike BB84, this protocol requires only two states for the transmission of a key; Alice encodes each bit by making the following association—for 0, she uses a state of $|0\rangle$, from the computation basis $(|0\rangle, |1\rangle)$ and for 1, she uses $|+\rangle$, from the non-orthogonal basis $(|+\rangle, |-\rangle)$. Bob also randomly measures using one of the two bases, and then the key is generated from the states where the measurement results yield $|1\rangle$ or $|+\rangle$. After this step, in a similar manner to BB84, Bob sends Alice the position of the qubits that he decides to keep in order for both parties to share the secret key.

The authors of paper [5] introduce a new type of quantum key distribution protocol, where the proposed scheme is not only secure in the previously analyzed eavesdropper scenario, but also the case of a theoretical post-quantum eavesdropper. In the beginning, Alice and Bob share a quantum channel, which contains a source that generates pairs of qubits in the maximally entangled state. Alice can pick one of three measurements with basis $x = \{0,\ 1,\ 2\}$ for $\left|0\rangle \pm e^{i\phi(x)}|1\right\rangle$, with $\phi(0) = \pi/4$, $\phi(1) = 0$, and $\phi(2) = \pi/2$, while Bob can measure using $y = \{0,\ 1\}$ for the measurement described by $\left|0\rangle \pm e^{-i\phi(y)}|1\right\rangle$, with $\phi(0) = \pi/4$ and $\phi(1) = -\pi/4$. In order to maximize the CHSH inequality (see paper [6]), Alice has to measure using the 0 and $\pi/2$ bases. A combination of measurements using $\pi/4$ by Alice and $-\pi/4$ by Bob gives uncorrelated results; the only case for a strongly correlated outcome is if both parties measure using the $\pi/4$ basis, which leads to creating the secret key.

Quantum image steganography is the art of hiding various types of information inside an image, using the quantum properties of qubits, such as superposition and entanglement. Some of the most recent innovations in this field are mentioned in the following paragraphs.

The authors of paper [7] present a novel watermarking protocol, which combines the NEQR transformation with the Gray transform and the least significant bit (LSB) technique, for the edges of the image. In another watermarking protocol, after the initial expansion of the watermark image, the Arnold transform is used and the LSB method is applied for the embedding step (see [8]). The bit-plane scrambling operation is used, along with

utilizing the LSB, in paper [9]. This operation is followed by the Arnold scrambling and the embedding procedure; two keys are used for hiding and recovering the secret message.

Different ideas are also presented regarding an exploiting modification direction (EMD) algorithm (see papers [10,11]); two out of three color channels (R, G, B) are selected in the process of obtaining the key. Paper [11] also shows how EMD and dynamically sharing between subgroups, together with the usage of bit-plane embedding, help achieve a better embedding rate; the quantum circuits and their implementations are also presented. Paper [12] illustrates a method based on the inverted pattern approach; the idea here is that depending on the value (state) of the quantum key, every pixel from the secret image is either inverted or left unchanged in embedding the message. A configurable number of LSBs are used to store the desired key.

Another idea for quantum steganography is presented in paper [13], where the novel enhanced quantum representation (NEQR, see [14]) is used alongside the LSB steganographic technique, this time for illustrating a detection method. The quantum image is broken into multiple blocks, classified into three groups, and their processing may reveal a potential secret message. The probability of the correct transmission of data is described in paper [15], where metrics, such as geometric coherence and $\frac{1}{2}$-affinity coherence, are taken into account, together with an analysis of the BB84 quantum protocol. In paper [16], the authors present a way of implementing the least significant bit-based quantum steganography (LSBq) for multi-wavelength quantum images; the main concept refers to replacing the least significant qubits in the cover image with the qubits corresponding to the secret string. The techniques used for hiding the secret message are the modulo method and the Hilbert scrambling, with good results in attack scenarios on the stego-image.

3. Materials and Methods

3.1. Quantum Image Representation Techniques

In order to implement an algorithm in the field of quantum steganography, an image representation technique has to be used. Some of the ideas proposed over the last years to represent an image with the help of quantum computing include:

1. FRQI, flexible representation for quantum images (see [17])—its definition combines information about the pixel colors and positions;
2. NEQR, novel enhanced quantum representation (see [14])—the information on the pixel color is saved in the multi-qubit computational basis of the superposition state;
3. NCQI, novel quantum representation of color digital images (see [18]), a technique built on NEQR for color (RGB) images;
4. QRCI, a new quantum representation model of color digital images (see [19]), takes the idea from NCQI but also combines the bit-plane concept, applied to each color component, to create the quantum state that can define the image.

The NEQR representation has been chosen for this paper, as it has good control of the information for the color component and also gives the user the ability to recover the image in a finite number of quantum measurements. Its implementation and integration in the chosen platform (IBM) can also be conducted more easily.

3.2. IBM's Quantum Solutions

There are two ways of interacting with IBM's quantum services, by using IBM Quantum Experience (see [20]) and Qiskit (see [21]), which have been selected to implement and simulate the circuits in this paper. IBM Quantum Experience allows its users to drag-and-drop quantum gates in order to create their circuits, as well as simulate them and analyze the results, either on a simulator or on a real quantum device. This can also be done directly, using the open-source Qiskit framework, written in Python, which gives programmers and researchers the possibility to code directly in their desired IDEs. The main parts of Qiskit are Terra, Aer, Aqua, and Ignis. Qiskit Terra is the collection of tools required for the design at the circuit level. Qiskit Aer is the simulator part of Qiskit; optimized backends, written in

C++, can be found here. Various quantum algorithms can be accessed through Qiskit Aqua, while Qiskit Ignis can be used to analyze various metrics for the noise in quantum systems.

3.3. Algorithm Details

This section presents the proposed procedure of using the idea behind the B92 protocol with the help of a grayscale image, considering the classical Alice and Bob—sender and receiver entities, as well as an auxiliary service, which can act as the server. We assume the fact that the random message that Alice would like to send is 8 bits long, so the encoding for this protocol would require 8 pixels of the image.

The first step is represented by a selection phase in which both parties decide what common image to use (from a set of any given images, stored on a server) or allow the server to pick one randomly before any processing takes place. After an image is selected, in order to keep the idea from B92, the server sets to 0 the LSB of all the pixels from the original image (the target ones are the relevant ones). Alice and Bob receive a copy of this image in order to process it locally (and independently from each other). Alice decides what kind of encoding she wants for her pixels and which of them should be used (this part can be extended with various ideas, for processing individual pixels or groups of pixels); for example, Alice's choices can be grouped into two categories, each of them with two main options:

1. Group 1—encoding type: she can decide to select, and then set to a certain value the least significant bit (LSB) of certain pixels, or modify the image to use the number of bits of "1" in the binary representation of the gray value of that pixel;
2. Group 2—pixel selection: she can use the first 8 pixels in the first row of the image or the first 8 pixels in the first column; other simple algorithms can be used to indicate the position of the target pixels.

The option from the first group can also be correlated in various ways with the encoding base of the B92 algorithm; assuming Alice chooses the LSB value of the first 8 pixels on the first row in the grayscale representation, we can propose the following association: a bit of "0" (LSB of the current pixel being processed) means that she would like to select the usual computational basis, while "1" means that she would like to use a different one (the non-orthogonal basis, commonly referred to as $(|+\rangle, |-\rangle)$, which requires applying a Hadamard gate to her qubit). Once the image is ready (the required bits are processed as needed), Alice sends her image to the server, as well as her options from the two groups. Bob modifies whatever pixel values in his image he desires (he can also use a local program to randomly modify some or all of them), unbeknownst to Alice's changes, and once finished, he can send the image to the server. Quite obviously, when one of the two parties finishes the processing on his/her part and uploads the image to the server, it must then wait for the other one to finish; at this point, neither Alice nor Bob know what the other party changed in the image. Table 1 shows the correlation between the LSB value of each gray level and the quantum gate applied by the server on the matching qubit.

Table 1. The correspondence between the LSB value of the gray intensity for the selected pixels in the images sent by Alice and Bob to the server, measurement basis, and applied quantum gate in the circuit created by the server.

LSB Value	Measurement Basis	Applied Quantum Gate
0	$(\|0\rangle, \|1\rangle)$	No quantum gate
1	$(\|+\rangle, \|-\rangle)$	A Hadamard gate

Once the server receives both images, it first creates the NEQR circuit for each pixel that belongs to the part of the image that was selected by Alice. The server then compares the images by evaluating the parameters indicated by Alice's options as well as Bob's changes, and applies the required transformations by both parties; the circuit that is presented in the

following section can be seen as extending one implementation of the B92 protocol (see paper [22]). After the measurements, the results are sent to Alice and Bob.

In other words, in the proposed scheme, the server and the data transmission between it and the two parties play the role of the classical system that intermediates the communication. We assume that all data transmitted between these entities are encrypted using a classical cryptographic algorithm. The ideas described above can be summarized in Figure 1.

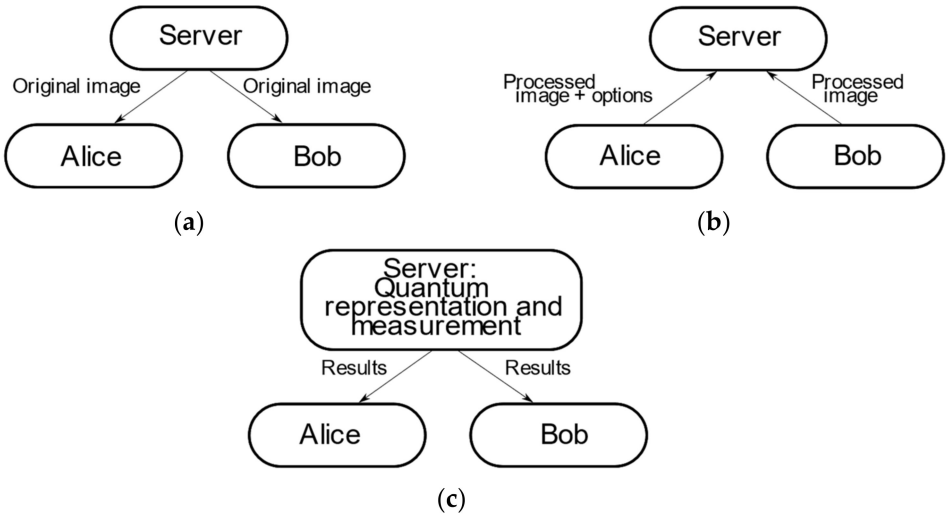


Figure 1. The proposed algorithm scheme can be summarized in 3 steps. (**a**) Step 1. The server sends an image to both parties. (**b**) Step 2. The parties process the image locally and send it back to the server (and Alice also sends some additional options, informing the server of the selected pixels and how they should be processed). (**c**) Step 3. The server processes the received images in a quantum manner, by taking into account the LSB of the indicated pixels (NEQR representation and measurement); the LSB values are used to create the quantum circuits and to apply the idea behind the B92 protocol to the qubit that corresponds to the LSB of the gray level for each pixel. After this, the server sends the results to both parties.

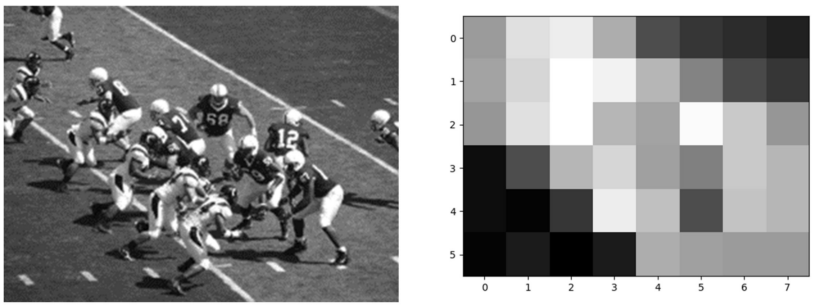
The server would represent a secure environment for the classical part of the proposed scheme. Moreover, an important idea, just theoretically described and perhaps showing a more interesting variation to the system illustrated above, necessary to preserve the key concept of the B92 protocol (and, therefore, to protect against eavesdropping attacks), would be the future concept of a quantum server—it should somehow be able to give users access to pairs of shared qubits, required for various quantum algorithms that need entanglement and correlated states. That means that both parties would be aware of the fact that the data stored there is a valid image (without measuring the qubits), while at the same time giving them the possibility of handling it in a low-level manner using quantum gates as well. A fine control such as the one presented allows for measurements on different bases and the successful implementation of various quantum communication protocols. This concept would mostly come down to the internal quantum design of the physical systems that would make the described algorithm, as well as the original B92 protocol, feasible over larger distances and wide quantum computer networks.

4. Results

4.1. Details of the Quantum Implementation for a Specific Image

In this section of the paper, we present the design of the quantum circuit and its simulation results, for the part of the image that involves the pixels from Alice's selection, using Qiksit (the code being written in Python). The following grayscale image was chosen, with the original color photo available at FreeImages (see [23])—this would be the image

that both Alice and Bob would agree to process (or receive randomly from the server), as can be seen in Figure 2.



(**a**) (**b**)

Figure 2. (**a**) The sample image (256 × 192 pixels). (**b**) A downscaled version of the sample image (8 × 6 pixels).

In order to indicate the position of a pixel inside a grayscale image (with 8 bits per pixel), the NEQR representation uses a number of qubits equal to the bits required to represent the dimensions of the image. Since the image above would require 256 × 192 pixels, which would translate to 16 position qubits (without the auxiliary ones). For demonstration purposes, the image in the figure above has been rescaled to 8 × 6 pixels, so that the number of position qubits would be much lower; as far as the algorithm goes, this operation can be an automatic part of what the server is sending to both parties, depending on the quantum computing power (the downscale does not have to be so radical as in this example). Here, we also need to take into account the fact that ancilla qubits are also required.

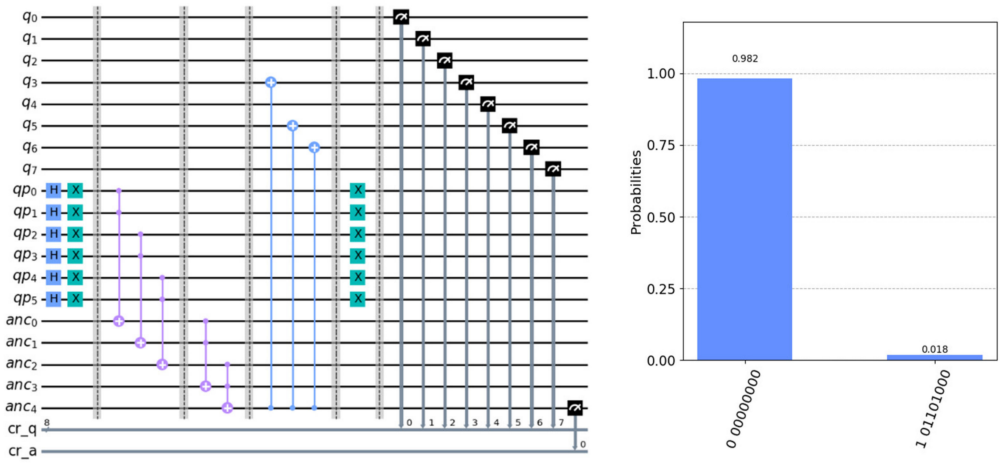
Therefore, for this simulation, the following 19 qubits are required:

1. Eight qubits for the grayscale value representation;
2. Six qubits for the pixels' positions;
3. Five qubits for auxiliary calculus, used to control the gray level qubits (depending on the states of the position ones).

The NEQR representation for the first pixel, with gray level 104, is presented in Figure 3 below; the position qubits (qp_0–qp_2 for the row and qp_3–qp_5 for the column component) are first set in superposition using Hadamard gates, and then NOT gates are used, as we look for states of $|1\rangle$ for all position qubits at this point. For the first pixel, we are searching for the situation where they are all in state $|0\rangle$ immediately after the Hadamard gates, so they all require NOT gates. A couple of controlled-controlled-NOT (CCNOT) gates are required to set the values of the ancilla qubits, such that the final one, anc_4, is set to $|1\rangle$ only when all position qubits are in the desired states. This qubit is then used to set the corresponding states for the actual gray value qubits, q_0–q_7. Another set of NOT gates is used, where necessary, to mirror the initial NOT gates and return the position qubits to their initial superposition states. At this point, the gray value qubits can be measured, along with the final ancilla qubit, as illustrated in Figure 3.

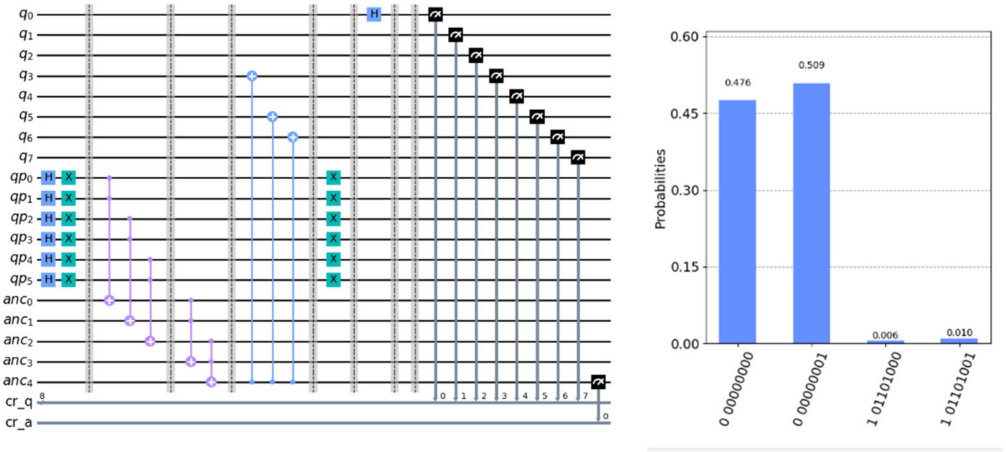
By following the procedure described in the previous section, we analyze the following situation: Alice uses the LSB as the encoding type and selects the first 8 pixels on the first row; she decides to alternate between setting her LSB for her pixels as in the following vector: [1, 0, 1, 0, 1, 0, 1, 0]; Bob performs multiple changes to his image, but for the first line he sets the LSB of the first four pixels to 0 and the LSB of the following four to 1.

The server creates the circuit by first setting to 0 the LSB of some of the pixels selected by Alice and then by comparing the received images, where the LSB of the chosen pixels is the one that must be taken into account for the different measurement bases; for the first pixel, Alice chooses the value of 1 for the LSB, while Bob selects 0 (see Figure 4). The quantum gates between the last three barriers indicate Alice's and Bob's measurement bases as follows: a Hadamard gate corresponds to $(|+\rangle, |-\rangle)$, while the lack of any gate is used to indicate the $(|0\rangle, |1\rangle)$ basis.



(**a**) (**b**)

Figure 3. (**a**) NEQR representation for gray level 104 and (**b**) results on the local simulator. The probability difference is due to the fact that there is only one combination out of a maximum of 64, for the position qubits, where all 6 qubits are in state $|1\rangle$ (immediately after the Hadamard and NOT gates).

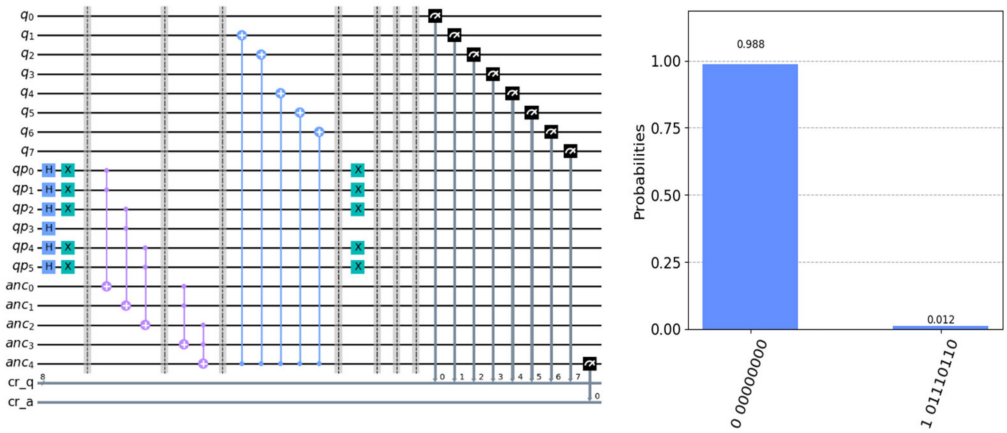


(**a**) (**b**)

Figure 4. (**a**) The NEQR representation for the first pixel (gray level 104, LSB set to 0) is presented, along with the quantum gates, required for the measurement basis, added by the server, depending on the LSB from the images sent by Alice and Bob. For her first pixel, Alice encodes her qubit using the $(|+\rangle, |-\rangle)$ basis, while Bob uses the computational basis $(|0\rangle, |1\rangle)$. (**b**) The probability for the states is presented; the results are obtained by running the circuit on the local simulator, with 1024 shots—the same applies to all of the following circuits.

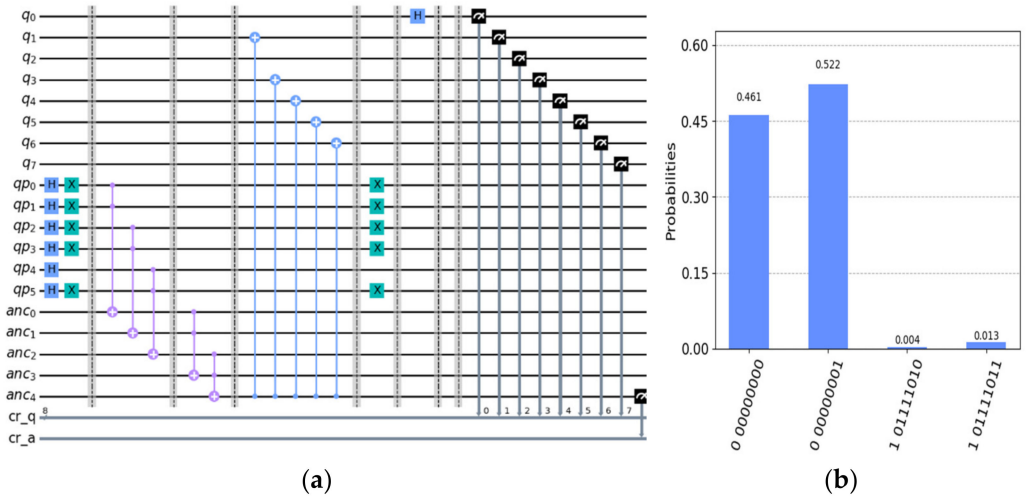
Figures 4–11 show the resulting circuits, where the described process is repeated for the first 8 pixels (starting in the left upper corner).

Table 2 presents the values for the LSBs of these pixels for Alice with her encoding basis, Bob's LSBs, and his encoding basis, all together with the expected result.



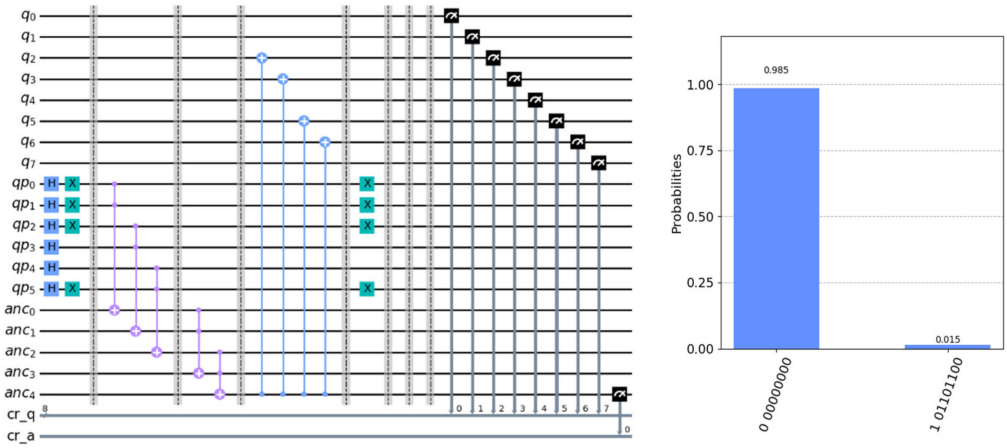
(**a**) (**b**)

Figure 5. (**a**) The NEQR representation for the second pixel (gray level 118, LSB set to 0) and (**b**) the measurement results.



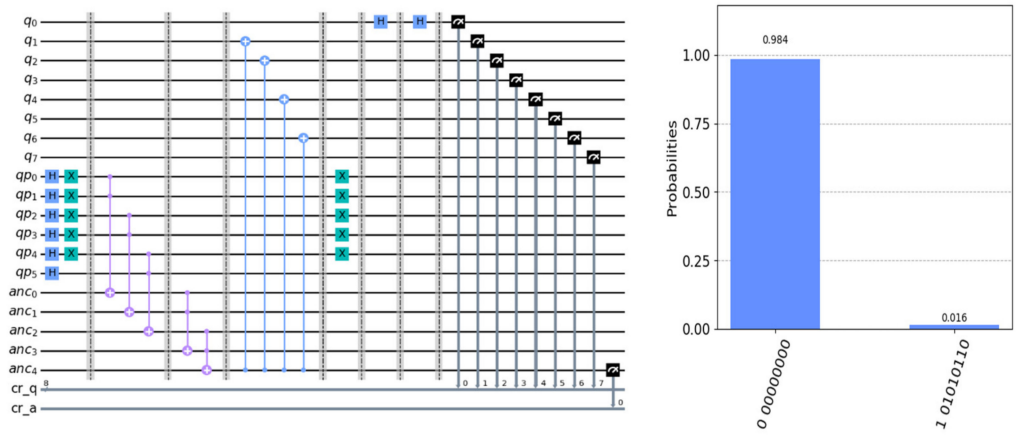
(**a**) (**b**)

Figure 6. (**a**) The NEQR representation for the third pixel (gray level 122, LSB set to 0) and (**b**) the measurement results.



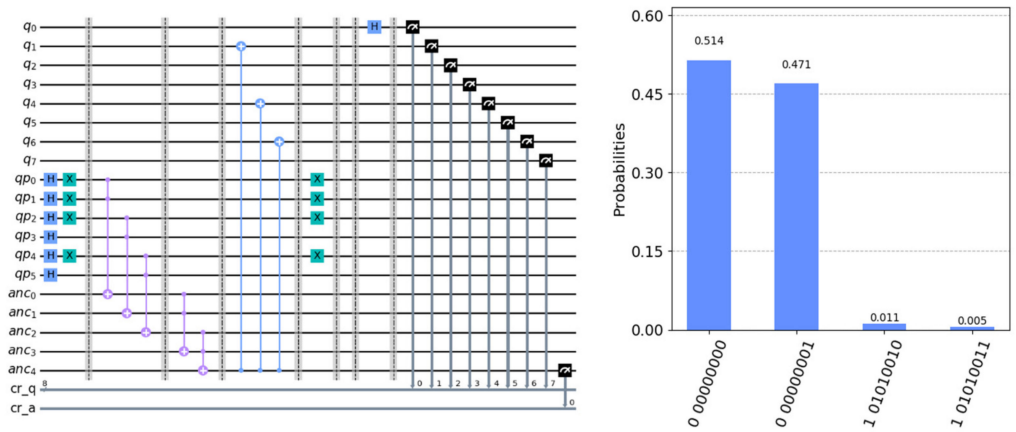
(**a**) (**b**)

Figure 7. (**a**) The NEQR representation for the fourth pixel (gray level 108, LSB set to 0) and (**b**) the measurement results.



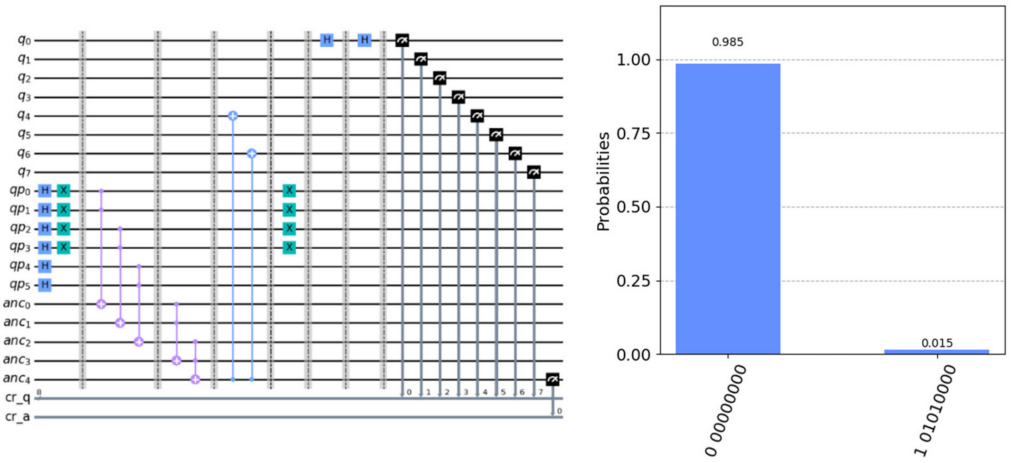
(**a**) (**b**)

Figure 8. (**a**) The NEQR representation for the fifth pixel (gray level 86, LSB set to 0) and (**b**) the measurement results.



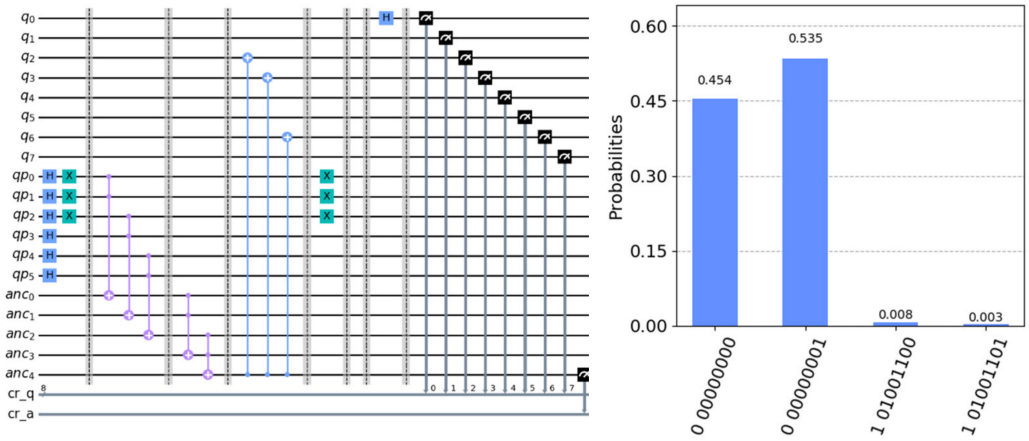
(**a**) (**b**)

Figure 9. (**a**) The NEQR representation for the sixth pixel (gray level 82, LSB set to 0) and (**b**) the measurement results.



(**a**) (**b**)

Figure 10. (**a**) The NEQR representation for the seventh pixel (gray level 80, LSB set to 0) and (**b**) the measurement results.



(**a**) (**b**)

Figure 11. (**a**) The NEQR representation for the eighth pixel (gray level 76, LSB set to 0) and (**b**) the measurement results.

Table 2. The selected basis for the LSB by Alice and Bob, their measurement basis, and the expected results.

Qubit nr.	Alice's LSBs	Alice's Encoding Basis	Bob's LSBs	Bob's Encoding Basis	Result
q[0]	1	$(\|+\rangle, \|-\rangle)$	0	$(\|0\rangle, \|1\rangle)$	$\|1\rangle$
q[1]	0	$(\|0\rangle, \|1\rangle)$	0	$(\|0\rangle, \|1\rangle)$	$\|0\rangle$
q[2]	1	$(\|+\rangle, \|-\rangle)$	0	$(\|0\rangle, \|1\rangle)$	$\|1\rangle$
q[3]	0	$(\|0\rangle, \|1\rangle)$	0	$(\|0\rangle, \|1\rangle)$	$\|0\rangle$
q[4]	1	$(\|+\rangle, \|-\rangle)$	1	$(\|+\rangle, \|-\rangle)$	$\|0\rangle$
q[5]	0	$(\|0\rangle, \|1\rangle)$	1	$(\|+\rangle, \|-\rangle)$	$\|+\rangle$
q[6]	1	$(\|+\rangle, \|-\rangle)$	1	$(\|+\rangle, \|-\rangle)$	$\|0\rangle$
q[7]	0	$(\|0\rangle, \|1\rangle)$	1	$(\|+\rangle, \|-\rangle)$	$\|+\rangle$

Once the circuit has been created, the server measures the states, analyzes the results, and then sends Alice and Bob the positions of the qubits where the result is different from $|0\rangle$—in the presented example, this would mean qubits with indexes 0, 2, 5, and 7 (see the final column in Table 2). Moreover, another way of interpreting the simulation results from the presented circuits is to notice the fact that whenever the last qubit is always in the $|0\rangle$ state (that means that both Alice and Bob are measured on the same basis), then that qubit is not selected by the server. The generated key, $|1\rangle$ $|1\rangle$ $|+\rangle$ $|+\rangle$, can be further used by both parties as needed; more pixels from the image can be processed as described above and, for example, this key can be used to further encode communication using a symmetrical cryptographical algorithm.

4.2. Mathematical Interpretation

We now describe the core operations performed by the server in creating the quantum circuits from a mathematical perspective. For the circuits in Figures 4–11, all qubits are initially set in the $|0\rangle$ state. This is followed by setting all the position qubits in superposition, and at this point, we can write:

$$H(qp_i) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \text{ for } i = \overline{0,5}.$$

This is followed by a layer of NOT gates, in order to match the desired position of the pixel in the image, which will be applied again, at the end of the representation for the current pixel (specific to the NEQR representation). The auxiliary qubits (anc_i, for $i = \overline{0.4}$) are used, in order to create the link between the desired position and a qubit (the final

ancilla qubit, anc_4) that will be then set to the $|1\rangle$ state. The state of this qubit (which is also initially $|0\rangle$) should be interpreted as follows:

$$\begin{aligned}|anc_4\rangle &= |anc_0\rangle \wedge |anc_1\rangle \wedge |anc_2\rangle \\ &= |qp_5\rangle \wedge |qp_4\rangle \wedge |qp_3\rangle \wedge |qp_2\rangle \wedge |qp_1\rangle \wedge |qp_0\rangle.\end{aligned}$$

The CNOT gates set the corresponding position qubits to the $|1\rangle$ state, using this last ancilla qubit. This can be written as follows, for the qubits that match the bits of 1 in the binary representation of the gray level:

$$|q_i\rangle = |q_i\rangle \oplus |anc_4\rangle.$$

The steganography component that is combined with the B92 protocol can be seen for the q_0 qubit (equivalent to the LSB in the classical representation). We will refer to f as the function that is performed by the server on this qubit. Here, we can group the possible choices into two main categories:

1. The first scenario is when both Alice and Bob choose the same value for their LSB. If both of them set their LSB to 0, the server adds no gate and then the state of the qubit can be expressed as applying an identity gate:

$$f(q_0) = I(q_0) = q_0 = |0\rangle;$$

If both Alice and Bob set their LSB to 1, we will arrive at the same result; the server adds two Hadamard gates (one for each party), and the state of the qubit can be expressed as follows:

$$\begin{aligned}f(q_0) = H(H(q_0)) &= H\left(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \\ &= \tfrac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle;\end{aligned}$$

2. The second scenario is when only a single entity sets the LSB value to 1, and the other one sets it to 0. In this case, the state of the q_0 qubit can be written as follows, with the action of a single Hadamard gate:

$$f(q_0) = H(q_0) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle.$$

The measurement results clearly indicate that, for the first scenario, we obtain the $|0\rangle$ state for the q_0 qubit; the results where the anc_4 qubit is in the $|1\rangle$ state are the ones of interest (see the probability histograms from Figures 5, 7, 8 and 10). In the second case, we obtain equal probabilities for the state of the q_0 qubit, which is interpreted by the server as the $|+\rangle$ state (see the probability histograms from Figures 4, 6, 9 and 11).

5. Discussion and Conclusions

The proposed paper describes the manner in which a shared grayscale image can be used to deliver a secret message, using the encoding idea from the B92 protocol. The algorithm that presents the method of obtaining the visually hidden string is parameterized—there is a group of options regarding encoding and position, which can be extended for different scenarios; the scheme also requires a server, used for the safe communication between the two parties. The concept unifies one of the quantum image representation techniques with steganography and a secure quantum communication protocol, thus presenting a bridge between various fields, suggesting a way that could perhaps change the perspective of quantum communication used alongside image processing.

The key points of the paper are:

- A new quantum steganography method is presented, combining some of the ideas from various subfields of quantum information processing;

- An implementation of the circuit representing the pixel values of the sender and receiver is described, along with their chosen bases for encoding information;
- The server is introduced as a third entity that can assist in the communication between the two parties, using the already established classically secured protocols. In the presented article, the server helps to convert the classical images to their quantum measurement basis in the quantum representation, but as a future concept, it could act directly as a qubit sharing entity.

Author Contributions: Conceptualization, A.-G.T. and V.M.; methodology, S.C.; software, A.-G.T.; validation, A.-G.T., V.M. and S.C.; formal analysis, A.-G.T.; investigation, A.-G.T.; writing—original draft preparation, A.-G.T.; writing—review and editing, A.-G.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the "Gheorghe Asachi" Technical University of Iasi.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Vai, M.; Whelihan, D.; Nahill, B.; Utin, D.; O'Melia, S.; Khazan, R. Secure Embedded Systems. *LLabJ* **2016**, *22*, 110–122.
2. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
3. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *arXiv* **2020**, arXiv:2003.06557. [CrossRef]
4. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121–3124. [CrossRef] [PubMed]
5. Acin, A.; Massar, S.; Pirono, S. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New J. Phys.* **2006**, *8*, 126. [CrossRef]
6. Clauser, J.F.; Horne, M.A.; Shimony, A.; Holt, R.A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **1969**, *23*, 880–884. [CrossRef]
7. Hu, W.; Zhou, R.G.; Luo, J.; Liu, B. LSBs-based quantum color images watermarking algorithm in edge region. *Quantum Inf. Process.* **2019**, *18*, 16. [CrossRef]
8. Zhou, R.G.; Hu, W.; Fan, P. Quantum watermarking scheme through Arnold scrambling and LSB steganography. *Quantum Inf. Process.* **2017**, *16*, 212. [CrossRef]
9. Zhou, R.G.; Luo, J.; Liu, X.; Zhu, C.; Wei, L.; Zhang, X. A Novel Quantum Image Steganography Scheme Based on LSB. *Int. J. Theor. Phys.* **2018**, *57*, 1848–1863. [CrossRef]
10. Hu, W.W.; Zhou, R.G.; Liu, X.A.; Luo, J.; Luo, G.F. Quantum image steganography algorithm based on modified exploiting modification direction embedding. *Quantum. Inf. Process.* **2020**, *19*, 137. [CrossRef]
11. Qu, Z.; Sun, H.; Zheng, M. An efficient quantum image steganography protocol based on improved EMD algorithm. *Quantum Inf. Process.* **2021**, *20*, 53. [CrossRef]
12. Luo, G.; Zhou, R.G.; Hu, W. Efficient quantum steganography scheme using inverted pattern approach. *Quantum Inf. Process.* **2019**, *18*, 222. [CrossRef]
13. Luo, J.; Zhou, R.G.; Hu, W.W.; Luo, G.F.; Liu, G.Z. Detection of steganography in quantum grayscale images. *Quantum Inf. Process.* **2020**, *19*, 149. [CrossRef]
14. Zhang, Y.; Lu, K.; Gao, Y.; Wang, M. NEQR: A novel enhanced quantum representation of digital images. *Quantum Inf. Process.* **2013**, *12*, 2833–2860. [CrossRef]
15. Qu, Z.; Huang, Y.; Zheng, M. A novel coherence-based quantum steganalysis protocol. *Quantum Inf. Process.* **2020**, *19*, 362. [CrossRef]
16. Şahin, E.; Yilmaz, İ. A novel quantum steganography algorithm based on LSBq for multi-wavelength quantum images. *Quantum Inf. Process.* **2018**, *17*, 319. [CrossRef]
17. Le, P.Q.; Dong, F.; Hirota, K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. *Quantum Inf. Process.* **2011**, *10*, 63–84. [CrossRef]
18. Sang, J.; Wang, S.; Li, Q. A novel quantum representation of color digital images. *Quantum Inf. Process.* **2017**, *16*, 42. [CrossRef]
19. Wang, L.; Ran, Q.; Ma, J.Y.; Yu, S.; Tan, L. QRCI: A new quantum representation model of color digital images. *Opt. Commun.* **2019**, *438*, 147–158. [CrossRef]
20. IBM Quantum Experience. Available online: https://quantum-computing.ibm.com/ (accessed on 14 July 2022).

21. Qiskit–Open-Source Quantum Development. Available online: https://qiskit.org/ (accessed on 14 July 2022).
22. Warke, A.; Behera, B.K.; Panigrahi, P.K. Experimental realization of three quantum key distribution protocols. *Quantum Inf. Process.* **2020**, *19*, 407. [CrossRef]
23. Free Football Stock Photo. Freeimages. Available online: https://www.freeimages.com/photo/football-1437517 (accessed on 14 July 2022).