International Journal of Multimedia and Ubiquitous Engineering
Vol. 4, No. 2, April, 2009

A quantum way to data hiding

Gabriela Mogos
Al.I.Cuza University
Computer Science Department, Iasi, Romania
gabi.mogos@gmail.com

Abstract

Though security is nothing new, the way that security has become a part of our daily lives today is unprecedented. Today, steganography is most often associated with the high-tech variety, where data is hidden within other data in an electronic file. Steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in an audio or video file. This work has as purpose to expand the field of applicability of the steganography from the classical informatics to the quantum one.

1. Introduction

Cryptography provides the means for secure communications; steganography provides the means for secret communication. Steganography is the art and science of hiding the fact that communication is taking place. Steganographic systems can hide messages inside of images or other digital objects. To a casual observer inspecting these images, the messages are invisible. The security of a classical steganographic system relies on the secrecy of the encoding system. Once the encoding system is known, the steganographic system is defeated. However, modern steganography should be detectable only if secret information is known, namely, a secret key. Because of their invasive nature, steganographic systems leave detectable traces within a medium's characteristics. This allows an eavesdropper to detect modified media, revealing that secret communication is taking place. Although the secret content is not exposed, its existence is revealed, which defeats the main purpose of steganography. Algorithmic steganography often uses as support audio or video files, speculating the imperfections of the human sense organs. The files hiding information will continue to perform their mission: the image will be able to be seen normally, the music will be listened normally and the documents will be read normally. Somebody who does not know in advance that these files dissimulate supplementary information will not realize it even after using these files. The advantage of steganography as compared to cryptography is that the hidden message does not draw attention towards itself. Taking into account the advantages of steganography in classical informatics, and starting from the premise that a classical color image can be seen as a register of "colored" qutrits in quantum informatics, this work has as purpose to expand the field of applicability of the steganography from the classical informatics to the quantum one.

2. Image as a matrix of colored qutrits

We might say that the concept of information represents a notion of maximum generality signifying a piece of news, a message, a signal, etc., about events, facts, states, objects, etc., in general about forms of manifestation of the reality which surrounds us. Using the holographic principle according to which the information emitted in the Universe by an object

is proportional with the entropy and with the area of the closed field including the object, we can look at the object as if it were painted on a closed surface limiting it, i.e. similar to a hologram. Shannon defines entropy as a function measuring the quantity of information. In the theory of sending the information, the informational entropy is defined as the quantity of information reported to an element of the sent message.

The pixel is the smallest particle of an image, the digital image being made of a finite number of pixels. Thus, according to the holographic principle, the pixel can be seen as an object limited by a closed surface, being a carrier of information. The pixel appears under the shape of a dot, and it has different colors. In classical informatics, the value of a color is usually 32 bits, in RGB format (R=Red, G=Green, B=Blue), any color being obtained by mixing different quantities of these three 3 colors.

A quantum analog to natural colors occurs with qubits [1]. As is well-known, the pure states of qubits (i.e. quantum systems with a two-dimensional Hilbert space) can be represented in a natural manner as points which form the surface of a sphere: *Bloch's sphere*. The impure states (which form the interior of Bloch's sphere) could be chosen to correspond to natural colors.

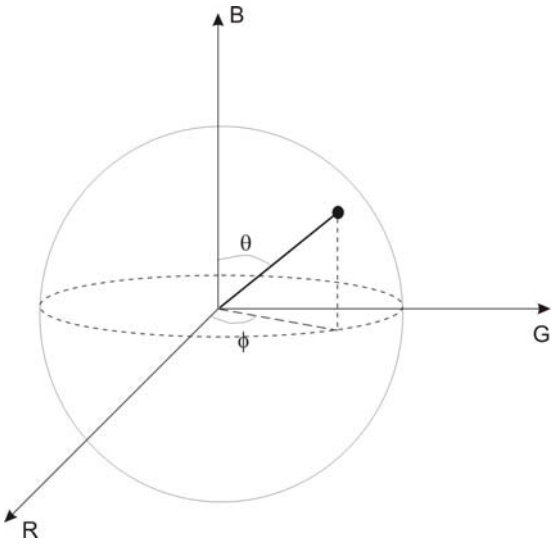

Figure 1. Bloch sphere

A quantum analogy of natural colors could be realized using three-dimensional systems called qutrits.

The three coordinate axes in which the qutrit is represented are labeled $\{|1\rangle, |2\rangle, |3\rangle\}$. Replacing the three-dimensional system $\{|1\rangle, |2\rangle, |3\rangle\}$ with $\{|R\rangle, |G\rangle, |B\rangle\}$, we can write the state of such a qutrit as a linear combination of the projections on the three coordinate axes:

$$|\Psi\rangle = r|R\rangle + g|G\rangle + b|B\rangle$$

There are three basic colors, red, green and blue, corresponding to:

$$|R\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad |G\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \quad |B\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

Starting from this representation of the qutrit ("color" representation), the work presents a steganographic algorithm in which the image file used as a support is in fact a register of qutrits.

The basic principles of the steganography in the case of common digital information are the following:

- The basic message is first encrypted with a certain algorithm;

- The choice of a support for this message;

- The modification of the support in a subtle way, so as to contain encrypted messages, but without losing its functionality and basic characteristics.

3. Quantum Steganographic Algorithm

The proposed algorithm follows the basic principle of the classical steganography, the chosen support being an image made of a register of qutrits, and the encrypting key being obtained with the protocol Bechmann-Pasquinucci and Peres [2]. Conventionally, we call Alice (the sender), and Bob (the receiver) the two entities who exchange information through a quantum channel.

3.1. Obtaining the secret key

In 1984, Bennett and Brassard developed a protocol in order to obtain the secret key using qubits. In the year 2000, Bechmann-Pasquinucci and Peres expanded this protocol for the case of the three-level systems (qutrits). For the three-dimensional spaces, four mutually unbiased bases (MUB) [3] [4] were used, corresponding to 12 vectors. The first two bases are:

$$\{|R\rangle, |G\rangle, |B\rangle\};$$

$$\left\{ \frac{1}{\sqrt{3}}(|R\rangle + |G\rangle + |B\rangle),\ \frac{1}{\sqrt{3}}(|R\rangle + e^{2\pi i/3}|G\rangle + e^{-2\pi i/3}|B\rangle),\ \frac{1}{\sqrt{3}}(|R\rangle + e^{-2\pi i/3}|G\rangle + e^{2\pi i/3}|B\rangle) \right\}$$

and the second two bases use:

$$\left\{ \frac{1}{\sqrt{3}}(e^{\pm 2\pi i/3}|R\rangle + |G\rangle + |B\rangle) \right\}$$

and theirs cyclic permutations.

The protocol is identical to the one already known: Alice will send a qutrit to Bob (using a quantum channel), which will measure its state by projecting it randomly on one of the four possible bases. He will make public (using a classical channel) only the chosen base, and not the obtained result. If the choice was good, then Alice and Bob will share the same qutrit, thus they will eliminate it completely. Alice and Bob will realize a number of iterations until they

will obtain a key with a corresponding length. After that, they will apply the error correction and the privacy amplification [5].

3.2. Encrypting and hiding the message

The encrypting of the message which will be afterwards hidden in the image is realized using the key obtained with the protocol presented above. The encrypting is realized by entangling the states of the qutrits contained in the message with the ones of the key. It is easy to see that Bob will easily decrypt the message, because he knows the decrypting key, this being identical with the encrypting one. This cryptosystem is one with a secret key.

We assume that Alice is sending a message made of a qutrit with the generic state**:**

$$\left|\Psi\right\rangle_1 = \alpha\left|R\right\rangle_1 + \beta\left|G\right\rangle_1 + \gamma\left|B\right\rangle_1$$

Where α, β, γ satisfies the relation: $\left|\alpha\right|^2 + \left|\beta\right|^2 + \left|\gamma\right|^2 = 1$

We assume that the encrypting/decrypting key is made of two qutrits. The qutrits are maximally entangled with the message, with the following result:

$$\left|\Psi\right\rangle_{123} = \alpha\left|RRR\right\rangle_{123} + \beta\left|GGG\right\rangle_{231} + \gamma\left|BBB\right\rangle_{123}$$

The entanglement resulted is "hidden" by the combination of the state $\left|\Psi\right\rangle_{123}$ with the one of a qutrit $\left|\Psi\right\rangle_4$ from the image. After their combination, we get the state:

$$\left|\Psi\right\rangle_{1234} = \left|\Psi\right\rangle_{123} \otimes \left|\Psi\right\rangle_4$$

This equation can be written:

$$\left|\Psi\right\rangle_{1234} = (\alpha\left|RRR\right\rangle_{123} + \beta\left|GGG\right\rangle_{231} + \gamma\left|BBB\right\rangle_{123}) \otimes (\left|R\right\rangle_4 + \left|G\right\rangle_4 + \left|B\right\rangle_4)$$

3.3. Decrypting and extracting the message

The sending of the image file is realized through an ideal quantum channel (with no noises). After this one arrives to the receiver, the message must be extracted. Using the decryption key qutrits, which he already has as a result of the protocol previously established, Bob will realize their entanglement and then he will measure them. Bob will realize a Bell projective measurement for pair (2, 3). There are obtained $3^2 = 9$ possible states and the general Bell-basis states [6] can be written as:

$$\left|\Psi_{nm}\right\rangle = \sum_j e^{2\pi ijn/3}\left|j\right\rangle \otimes \left|j+m \bmod 3\right\rangle / \sqrt{3}$$

where $n \in \{0,1,2\}$, $m \in \{0,1,2\}$ and $j \in \{0,1,2\}$ are the three dimensions (R,G,B) numbered {0,1,2} to simplify the calculus. After the measurement, the system will evolve in one of the states:

$$\frac{1}{3}\left|\Psi_{RR}\right\rangle_{23}(\alpha\left|RR\right\rangle_{14}+\beta\left|GG\right\rangle_{14}+\gamma\left|BB\right\rangle_{14})$$

$$\frac{1}{3}\left|\Psi_{RG}\right\rangle_{23}(\alpha\left|GG\right\rangle_{14}+\beta\left|BB\right\rangle_{14}+\gamma\left|RR\right\rangle_{14})$$

$$\frac{1}{3}\left|\Psi_{RB}\right\rangle_{23}(\alpha\left|GG\right\rangle_{14}+\beta\left|RR\right\rangle_{14}+\gamma\left|GG\right\rangle_{14})$$

$$\frac{1}{3}\left|\Psi_{GR}\right\rangle_{23}(\alpha\left|RR\right\rangle_{14}+e^{-2\pi i/3}\beta\left|GG\right\rangle_{14}+e^{2\pi i/3}\gamma\left|BB\right\rangle_{14})$$

$$\frac{1}{3}\left|\Psi_{BR}\right\rangle_{23}(\alpha\left|RR\right\rangle_{14}+e^{2\pi i/3}\beta\left|GG\right\rangle_{14}+e^{-8\pi i/3}\gamma\left|BB\right\rangle_{14})$$

$$\frac{1}{3}\left|\Psi_{GG}\right\rangle_{23}(\alpha\left|GG\right\rangle_{14}+e^{-4\pi i/3}\beta\left|BB\right\rangle_{14}+e^{-4\pi i/3}\gamma\left|RR\right\rangle_{14})$$

$$\frac{1}{3}\left|\Psi_{BG}\right\rangle_{23}(\alpha\left|GG\right\rangle_{14}+e^{-4\pi i/3}\beta\left|BB\right\rangle_{14}+e^{-8\pi i/3}\gamma\left|RR\right\rangle_{14})$$

$$\frac{1}{3}\left|\Psi_{GB}\right\rangle_{23}(\alpha\left|BB\right\rangle_{14}+e^{-2\pi i/3}\beta\left|RR\right\rangle_{14}+e^{-4\pi i/3}\gamma\left|GG\right\rangle_{14})$$

$$\frac{1}{3}\left|\Psi_{BB}\right\rangle_{23}(\alpha\left|BB\right\rangle_{14}+e^{-4\pi i/3}\beta\left|RR\right\rangle_{14}+e^{-8\pi i/3}\gamma\left|GG\right\rangle_{14})$$

Checking the message is similar for each of the results. If we consider that Bob is measuring the pair (2, 3) and he will get as a result $\left|\Psi_{RR}\right\rangle_{23}$. In this case, the state of the pair (1, 4) will collapse in:

$$\alpha\left|RR\right\rangle_{14}+\beta\left|GG\right\rangle_{14}+\gamma\left|BB\right\rangle_{14}=\frac{1}{3}[(\left|R\right\rangle_1+\left|B\right\rangle_1+\left|G\right\rangle_1)(\alpha\left|R\right\rangle_4+\beta\left|G\right\rangle_4+\gamma\left|B\right\rangle_4)+$$

$$+(\left|R\right\rangle_1+e^{2\pi i/3}\left|G\right\rangle_1+e^{4\pi i/3}\left|B\right\rangle_1)(\alpha\left|R\right\rangle_4+e^{-2\pi i/3}\beta\left|G\right\rangle_4+e^{-4\pi i/3}\gamma\left|B\right\rangle_4)+$$

$$+(\left|R\right\rangle_1+e^{4\pi i/3}\left|G\right\rangle_1+e^{2\pi i/3}\left|B\right\rangle_1)(\alpha\left|R\right\rangle_4+e^{-4\pi i/3}\beta\left|G\right\rangle_4+e^{-2\pi i/3}\gamma\left|B\right\rangle_4)]$$

If Bob will measure the state of the qutrit:

$$\left|R\right\rangle_1+\left|B\right\rangle_1+\left|G\right\rangle_1$$

He will determine the collapsing of the qutrit in the state:

$$(\alpha\left|R\right\rangle_{14}+\beta\left|G\right\rangle_{14}+\gamma\left|B\right\rangle_{14})$$

this is in fact the message. If Bob will measure the state of the qutrit:

$$(\left|R\right\rangle_1+e^{2\pi i/3}\left|G\right\rangle_1+e^{4\pi i/3}\left|B\right\rangle_1)$$

Bob can reconstruct the message by applying the unitary operator:

$$O_1=\sum_{k=R,G,B}e^{2\pi ij/3}\left|k\right\rangle\left\langle k\right|$$

over the state of the qutrit:

$$\alpha\left|R\right\rangle_4 + e^{-2\pi i/3}\beta\left|G\right\rangle_4 + e^{-4\pi i/3}\gamma\left|B\right\rangle_4$$

If Bob will measure the state of the qutrit:

$$\left|R\right\rangle_1 + e^{4\pi i/3}\left|G\right\rangle_1 + e^{2\pi i/3}\gamma\left|B\right\rangle_1$$

He will reconstruct the state of message's qutrit by applying the unitary operator:

$$O_2 = \sum_{k=R,G,B} e^{4\pi ij/3}\left|k\right\rangle\left\langle k\right|$$

4. Analysis

Steganalysis is the process of analyzing various media such as digital photos, video, audio and other file formats in order to find the existence of a secret message or watermark and respond appropriately to the find. The ethical nature of the "appropriate" response may be debated but we are concerned with the technology. A steganalysis "attack" represents the technique with which the steganalyst attempts to recover, modify or remove a stego message. In classical cryptography, there exist 5 steganalysis attacks which are incidentally derived from 4 cryptanalysis techniques: *stego-only*, *known-cover, known message, chosen stego* and *chosen message*. In the stego-only method the steganalyst only has available the stego medium or the finished stego product. This is by far the most difficult attack approach since there is no starting point from which to start extracting the hidden message. So typically the steganalyst will scan by steganalysis algorithm type first. The "known message attack" assumes either a part of or the entire hidden message is available to the steganalyst. An efficient approach is to begin in parallel an effort to decrypt the message and an effort to detect other hidden messages based on the signature of the known message. The "chosen stego attack" asserts the steganography algorithm and the cover data are known. In this case the key, if the message is encrypted and the hidden message are unknown. "Chosen message attack" refers to the steganalyst's knowledge of the hidden message with the goal of effectively detecting stego messages. This attack assumes the hidden message is known but a community has no knowledge of which container is hiding it. In this effort the steganalyst will generate various stego messages using various stego algorithms in an attempt to find consistent patterns and improve detection of the hidden message.

In the case of the quantum cryptography, the steganalysis "attack" also implies the use by the steganalyst of some techniques by which a stego message can be recovered, modified or removed, but the ways to realize this are different from the classical case.

On one hand, in order to be able to interfere in any of the ways (recover or modify) over the hidden message, it is necessary to know the encrypting key. An eavesdropper (Eve) can try to rebuild the encrypting key obtained as a result of the protocol Quantum Key Distribution (QKD). Eve can wiretap the public channel, but that won't do her any good. She gets information on the bases and not on the outcome of the measurement. In case Eve attempts to measure part of the Quantum Channel she betrays herself by a high Quantum Bit Error Rate (QBER) and Alice and Bob are warned. The Quantum Bit Error Rate (QBER) is the ratio of an error rate to the key rate and contains information on the existence of an eavesdropper and how much he knows.

On the other hand, trying to remove the message from the image file involves a series of steps. Then, considering that the message suffered a series of "transformations" (the state entanglement between the qutrits of the message and those of the encrypting key,

and then again the combination of the resulted state with the qutrits belonging to the image support) the qutrits which compose the message will be difficult to extract, and the message will be difficult to recover completely, without knowing the encrypting key, and, of course, the state of the support qutrit.

5. Conclusions

Quantum steganography is a fascinating illustration of the dialog between classical and quantum informatics and it is based on a beautiful combination of concepts from quantum physics and information theory. Its security principle relies on deep theorems in classical information theory and on a profound understanding of Heisenberg's uncertainty principle and entanglement theory.

Data hiding in multimedia can help in providing proof of the origin and distribution of content. Multimedia content providers can communicate with the *compliant multimedia players* through the *subliminal*, steganographic channel. This communication modality might control or restrict access of multimedia content and carry out e-commerce functions for pay-per-use implementations. The concept of compliant multimedia players may extend to computer operating systems that would recognize protected multimedia files, meaning one may not be able to print a document or make additional copies unless authorized by the hidden data in the document. Note that all material available on paper may eventually be in electronic form. Downloading or distributing the documents could be controlled by the hidden data in the documents.

References

[1] U. Mutze, "Quantum Image Dynamics — an entertainment application of separated quantum dynamics", www.ma.utexas.edu/mp arc/c/08/08-199.pdf, 2008.

[2] H. Bechmann-Pasquinucci and A. Peres, "Quantum Cryptography with 3-state systems", Phys. Rev. Lett., 85, 3313, 2000.

[3] I.D. Ivanovic, J. Phys. A: Math. Gen., 14, 3241, 1981.

[4] W.K. Wootters, Found. Phys., 16, 391, 1986.

[5] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J.Cryptol., 5, 3, 1992.

[6] X.S. Liu, G.L. Long, D.M. Tong, and F. Li, Phys. Rev. A., 65, 022304, 2002.

[7] S. Katzenbeisser, F.A.P. Petitcolas, Information hiding techniques for steganography and digital watermarking, Artech House Inc., ISBN 1-58053-035-4, 2000.

Authors

She received B.S. degree in Physics and M.S. degree in Informatics from Al.I.Cuza University of Iasi, Romania. She is currently pursuing her Ph.D. in Informatics at Al.I.Cuza University of Iasi. Her research interests are quantum computing, quantum algorithm and quantum cryptography.