# Storing, Processing and Retrieving an Image using Quantum Mechanics

S.E. Venegas-Andraca(a) and S. Bose(b)

[a]Centre for Quantum Computation, Department of Physics, University of Oxford Parks Road, Oxford OX1 3PU, U.K. svenegas@qubit.org

[b]Centre for Quantum Computation, Department of Physics, University of Oxford Parks Road, Oxford OX1 3PU, U.K. s.bose@qubit.org

## ABSTRACT

*We investigate the storage and retrieval of an image in a multi-particle quantum mechanical system. Several models are studied and compared with corresponding classical digital methods. We consider a situation in which qubits replace classical bits in an array of pixels and show several advantages.*

*For example, we consider the situation in which 4 different values are randomly stored in a single qubit and show that quantum mechanical properties allow better reproduction of original stored values compared with classical (even stochastic) methods. The retrieval process is uniquely quantum (involves measurement in more than one bases). The independence and the finiteness of the stored copies of the image play an important role in the quantum protocol being better that the classical one.*

*Other advantages of quantum storage of an image are found in its security.*

**Keywords:** Quantum Image Processing, Quantum Computation, QUantum Information, Artificial Intelligence

## 1. INTRODUCTION

The purpose of this paper is to provide an initial step towards the definition of a new field where Quantum Physics, Computer Science and Engineering join: Quantum Image Processing.

In areas like Pattern Recognition and Computer Vision, both being fields of Artificial Intelligence (AI), Image Processing (IP) is widely used due to the need of extracting essential information from our 3D world. However, it is known that the very nature of visual information (highly redundant and content-related), algorithm complexity and the representation of 3D scenes in 2D spaces are all open research areas.

For example, the vast amount of available information and the difficulty of defining search criteria that meets an optimal performance of current computer hardware model[1] as well as the role image-related noise plays, are two examples of state of the art problems in such areas.

We consider that the analysis of previously mentioned problems under the light of Quantum Computation (QC) and Quantum Information (QI), may result in new ways of understanding the nature of visual information.

Back in 1985, Deutsch showed in[2] that a quantum computer, that is, a *physical* system capable of performing computations according to the rules of quantum mechanics, can perform certain tasks faster than its classical counterpart. Deutsch and Jozsa[3] and Shor[4] showed concrete problems where such speed-up is possible.

Among quantum computer properties, we find:

Further author information: (Send correspondence to S.E. Venegas-Andraca: E-mail: svenegas@qubit.org, Telephone: 0044-1865-282399

- Superposition of states. Classical computers measure bit values using only one basis, {0,1} and the only two possible states are those that correspond to the measurement outcomes, 0 or 1. On the other hand, qubits (quantum computers elementary components), due to its quantum nature, can be seen as rays in a complex Hilbert space $\mathcal{H}^2$[5] (see figure 1.a). The fact that vector spaces such as $\mathcal{H}^2$ have an infinite number of bases is fundamental to understand the nature of a qubit (see figure 1.b).

- Entanglement, a special correlation among quantum systems that has no paragon in classical systems. Entanglement is seen to be at the heart of QI processing unique properties, and an example of it is its role in Quantum Teleportation.[5]

QC can thus be regarded as the study and development of methods that, by using quantum mechanical properties, solve problems in finite time. Correspondingly, QI is the field devoted to understanding how information is represented and communicated using quantum states.

Encouraged by the quantum mechanical analysis of Computer Science problems and the properties of quantum computers mentioned above, it is our belief that QC and QI may have important implications in Image Processing and AI both on theoretical (e.g. faster algorithms, secure tranmissions and the physical nature of information) and technological spheres (current technology is now being built taking into account quantum effects due to component size).

The rest of the paper is divided as follows: Section 2 contains a review of state of the art IP Fundamentals, particularly what colour models are and what they are used for. In section 3 we explain why colour models are not required as well as how to store colour in a qubit and an image in a qubit lattice. Section 4 is devoted to explain a probabilistic process to retrieve an image from a qubit lattice with minimum uncertainty. Finally, section 5 compares a novel method for storing information in a quantum system with a classical probabilistic method.

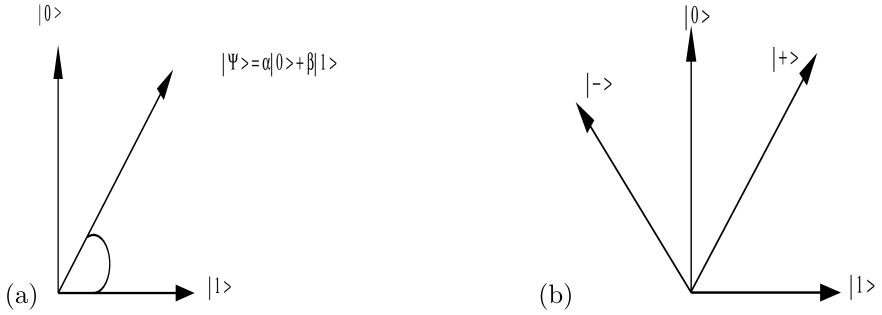


**Figure 1.** Mathematical Representation for a qubit

a) The canonical counterpart of classical bits $\{0,1\}$ in QIP is $\{|0\rangle, |1\rangle\}$. An arbitrary qubit can be written as $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$.

b) Note that $|\Psi\rangle$ can be written as a linear combination of an infinite number of bases, in particular as a combination of either $B_1 = \{|0\rangle, |1\rangle\}$ or $B_2 = \{|+\rangle, |-\rangle\}$, where $|+\rangle = [|0\rangle + |1\rangle]/\sqrt{2}$ and $|-\rangle = [|0\rangle - |1\rangle]/\sqrt{2}$.

## 2. PREVIOUS WORK

IP is a branch of Computer Science and Engineering where information coming from the perception of electromagnetic waves is captured, stored and manipulated. IP has raised interest in the scientific community for two main reasons: improvement and availability of visual information for human interpretation, and processing of scene data for autonomous machine perception and AI processes.

Methods used for storing visual information in a computer have important consequences in fields like Computer Vision and Pattern Recognition, as such methods are hardware and human oriented, that is, it is assumed that

- Machines used for IP are built according to the so-called Von Neumann architecture, and

- Generally speaking, humans will be the ultimate costumer for digital visual information.

The raw material for IP and related fields is gray scale and/or colour images (video can ultimately be converted into sets of frames). In particular, the use of colour is motivated by two principal factors:

- Colour is a powerful descriptor that simplifies object recognition, identification and delimitation. Thus, colour is an essential element for AI purposes
- The Human Vision System is excellent at detecting thousands of colour shades and intensities, compared to about only two-dozens shades of gray.

Human colour perception is a physiopsychological phenomenon that has its origin in the fact that the human eye can detect electromagnetic waves of certain frequency (roughly speaking, frequencies in the range of 400 to 700 nm). Actually, due to the structure of the human eye, all colours are seen as variable combinations of the three so-called primary colours Red, Green and Blue (RGB). It must be noted that, given that no single colour (i.e. no single electromagnetic wave of specific wavelenght) can be called Red, Blue or Green, then the previous statement holds as long as wavelenghts for RGB are allowed to vary in the corresponding subsets of the visible spectrum.[6]

In order to specify colours in a standard way, several colour models have been developed, having specific purposes in mind (some models are hardware oriented, while others are manipulation and hardcopy printing oriented).

The colour models used for image processing are the RGB and HSI models.

### The RGB Model

In the RGB model, each image consists of three independent image planes, one for each primary colour.

### The HSI model

The acronym HSI stands for *Hue*, *Saturation* and *Intensity.*

- **Hue** is a descriptor that measures the quantity of pure colour (pure yellow, orange or red) contained in a specific colour
- **Saturation** is a parameter that provides a measure of how much a pure colour is diluted by white light
- **Intensity**. In this context, intensity can be defined as the brightness or darkness of a colour.

# 3. STORING AN IMAGE IN A QUANTUM SYSTEM

## 3.1. No Colour Models

Colour models are used to specify colours in a standard way that makes sense under the theoretical and technological assumptions of classical computers and/or printing systems.

In the case of quantum computers, the continuous nature of the parameters of a qubit allows us to store information without having to pre-process it.

This approach has a clear advantage over colour models: every colour can be studied and analysed using the actual values of its physical parameter (frequency), rather than a representation of it (e.g. a linear combination of RGB).

The rest of this section is devoted to explain how to use qubits to store colour and consequently images, without using any pre-processing steps but rather only the physical nature of colour.

### 3.2. Storing Colour in a qubit

Let us define a machine $A$ such that $A$ is capable of detecting electromagnetic waves and, depending on the frequency of the detected wave, it outputs an initialised qubit (see figure 2). $A$ acts like an injective function $A : F \rightarrow \Psi$, where $F$ is the set of monochromatic electromagnetic waves whose frequencies can be detected by $A$ and $\Psi$ is the set of quantum states of the form

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\gamma}\sin\frac{\theta}{2}|1\rangle \qquad (1)$$

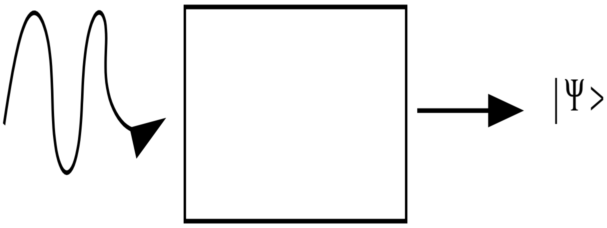


**Figure 2.** Frequency to quantum state apparatus
Schematics of an apparatus $A$ capable of detecting electromagnetic frequencies and producing a quantum state as output (note that a neccesary property of $A$ is to initialise qubits in different quantum states for different detected frequencies).

Indeed, regardless the frequency value of a particular monochromatic electromagnetic wave, it is always possible to find a value for the real parameter $\theta$ in eq. (1) such that $A$ can initialise qubits in different states when different waves are detected. Parameter $\gamma$ is left uninitialised for the moment as the purpose of this paper is to focus on how to store, process and retrieve information using a single quantum parameter.

Let us give an example of a realization of machine $A$: First, build an apparatus for frequency detection and recording; furthermore, apply a magnetic field proportional to the stored frequency to a spin-half particle originally prepared in either the spin up or the spin down state. That way, it is possible to produce a quantum state whose real parameter $\theta$ is proportional to the recorded frequency (see[7]).

Note that this storage protocol allows us to store frequencies from all the spectrum, not only from the visible spectrum. Thus, *a quantum system used for image processing purposes could be used for AI processes with non-visible waves as input.* In particular, due to the continuous nature of $\theta$, it is easy to accommodate the prospect of recording a new colour with frequency lying anywhere in a given domain without readjusting our storage protocol as opposed to digital storage protocols, where an adjustment on the number of bits required to record colour is needed once the storage capacity limit is reached.

### 3.3. Storing an Image in a Qubit Lattice

Let us define $Q$ as a lattice of qubits, that is,

$$Q = \{|q\rangle_{i,j}\}, i \in \{1, 2, \ldots, n_1\}, j \in \{1, 2, \ldots, n_2\}$$

A set of qubit lattices $Z$ is defined as

$$Z = \{Q_k\}, k \in \{1, 2, \ldots, n_3\} \qquad (2)$$

Thus, $Z = \{|q\rangle_{i,j,k}\}$ is a set of $n_1 \times n_2 \times n_3$ qubits.

Our goal is to store visual information in $Z$. Each lattice $Q_k \in Z$ will be used to store a copy of the image so that, by the end of the recording procedure, $Z$ will be a set of $n_3$ lattices all of which have been prepared identically. In the following section it will become clear why it is necessary to have several copies of the same image.

The procedure to store an image in a set of qubit lattices $Z$ is explained in algorithm 1. In this algorithm it is assumed that a lattice $L$ made out of machines $A$ is available. We will refer to the element of lattice $L$ as $A_{i,j}$, $i \in \{1, 2, \ldots, n_1\}$ and $j \in \{1, 2, \ldots, n_2\}$

**Algorithm 1**. Storing an Image in a Qubit Lattice $Q_k$

1. **Indices initialisation**. Set $i = 0$ and $j = 0$
2. **Prepare qubits as a frequency is detected**. For a given frequency $\nu_{i,j}$ use machine $A_{i,j}$ from lattice $L$ in order to prepare qubits $|q\rangle_{i,j,k}$, $k \in \{1, 2, \ldots, n_3\}$, in the same quantum state corresponding to frequency $\nu_{i,j}$
3. **Update indices**. Update $i, j$ values according to the way visual information is made available and go back to step 2, until no more qubits or frequencies are available.

Note that we have assumed in algorithm 1 that visual information is made available to us in a 'serial' method. Of course, modifying such algorithm for parallel detection of monochromatic electromagnetic waves (as in a digital camera) is a trivial exercise.

So, after having completed algorithm 1, the whole set $Z$ is initialised; $n_3$ identically prepared qubit lattices, each containing a copy of the same image.

## 4. RETRIEVING AN IMAGE FROM A QUANTUM SYSTEM

One of the most shocking properties of Quantum Mechanics is the probabilistic nature of quantum measurement. In this section we show a method for minimising the uncertainty in the retrieval process of a quantum parameter.

This section is divided as follows: first, we show a procedure for retrieving a single colour from a set of qubits. Secondly, it is explained how to retrieve a full image.

### 4.1. Retrieving a single frequency

Reading (that is, measuring) a general quantum state is a probabilistic process. Thus, if only one basis is used to measure all states in $Z$, information retrieval will not be accurate. In addition, the postulates of quantum mechanics state that the post-measurement quantum state is, in general, different from the pre-measurement quantum state (they are equal if and only if the pre-measurement quantum state is equal to one of the orthogonal vectors of the measurement basis).

So, given that the protocol we defined in the previous section does produce general quantum states, we have defined a statistical protocol to retrieve visual information as accurately as possible.

First, let us define the observable

$$\hat{\mathbf{P}} = \alpha_1 \hat{\mathbf{P_1}} + \alpha_2 \hat{\mathbf{P_2}} \tag{3}$$

where

$$\hat{\mathbf{P_1}} = |0\rangle\langle 0|, \hat{\mathbf{P_2}} = |1\rangle\langle 1| \tag{4}$$

Using eqs. (1) and (4), it is clear that

$$p(\alpha_1) = \langle\psi| \hat{P}_1 |\psi\rangle = cos^2 \frac{\theta}{2}$$

$$p(\alpha_2) = \langle\psi| \hat{P}_2 |\psi\rangle = sin^2\frac{\theta}{2}$$

Since the angle $\theta$ is the quantum parameter used to store colour information in every qubit in $Z$, our goal in the statistical procedure shown in the rest of this section is to minimise the uncertainty in the retrieved value of such parameter for every single recorded frequency. We shall assume we can perform a finite number of experiments, $M$ (note that $M \leq n_3$, where $n_3$ is the number of identically prepared lattices $Q_k$).

The procedure is divided into two steps explained in algorithm 2.

**Algorithm 2**. Estimating $\hat{\theta}$ for a single frequency
For each set of identically prepared qubits $|q\rangle_{i,j,k}$, $k \in \{1, 2, \ldots, n_3\}$ and $i, j$ fixed (i.e. for each set of identically prepared set of qubits representing the same frequency at the same spatial location):

1. **Estimate** $\hat{\theta}_l$. Divide the set of $M$ measurements into $r$ subsets $M_l$, and compute for each subset $M_l$ an estimate of $\hat{\theta}_l$
2. **Estimating** $\hat{\theta}$. Using the set of estimates $\{\hat{\theta}_1, \hat{\theta}_2, \ldots \hat{\theta}_r\}$, compute a final estimate $\hat{\theta}$. $\hat{\theta}$ will be taken as the closest estimate to the actual value of $\theta$.

The outcome of algorithm 2 is an estimate of $\hat{\theta}$ for one stored frequency. To put it in classical terms, algorithm 2 produces the value of one pixel.

### Estimating $\hat{\theta}_l$

For each set of qubits $M_l = \{|q\rangle_{i,j,k}, k \in \{1, 2, \ldots, n_3\}\}$ we shall perform $M$ measurements using the observable $\hat{\mathbf{P}}$ defined in eq. (3). As outcomes, we can only have $\alpha_1$ or $\alpha_2$. Let us say that in $m_{1l}$ experiments get $\alpha_1$ as outcome and in $m_{2l}$ experiments get $\alpha_2$. Thus, the following statement holds:

$$cos^2\frac{\theta_l}{2} = p(\alpha_1) \approx \frac{m_{1l}}{m_{1l} + m_{2l}}$$

And, in order to make

$$cos^2\frac{\theta_l}{2} \cong \frac{m_{1l}}{m_{1l} + m_{2l}}$$

we must find out how many experiments have to be performed.

So, let us define

$$p_l = \frac{m_{1l}}{m_{1l} + m_{2l}}$$

for a certain number of experiments, and $P_l$ as the true proportion of experiments with outcome $\alpha_1$ when the number of experiments approaches infinity (that is, $P_l = cos^2\frac{\theta_l}{2}$. It is assumed that $p_l$ would distribute normally).

We also define $d_l$ as the error between the estimate proportion $p_l$ and the true proportion $P_l$ and $\epsilon_l$ as the probability of such an error ($\epsilon_l$ can be understood as the risk we are willing to take).

So, the following equation:

$$Pr(|p_l - P_l| \geq d_l) = \epsilon_l$$

expresses the fact that, for the estimation of $\theta_l$, we are prepared to take a risk equal to $\epsilon_l$ that the difference between the estimate $\alpha_l$ and the true value $\alpha$ is bigger than $d_l$.

Sampling theory[8] shows that the number of experiments $M_l$ that have to be performed in order to fulfill the above assumptions is equal to

$$M_l = \frac{t_l^2}{4d_l^2} \tag{5}$$

where $t_l$ is the value of the abscissa axis for which $\epsilon_l$ of the area under the normal curve lies to the right of $t_l$.

Thus, it is clear that having an increasing number of experiments always provides better estimates. It must only be decided what the error we are prepared to accept is, in order to define the number of necessary experiments.

In addition, this approach allows us to suit the technological restrictions (the number of total experiments that can actually be performed under a certain technology) that may be faced in any realistic implementation.

So, a total number of $r$ estimates $\{\theta_1, \theta_2, \ldots, \theta_r\}$ have to be computed for each recorded frequency (again, using classical terms, a total number of $r$ estimates per 'pixel' have to be computed).

### Estimating $\hat{\theta}$

The purpose of the following algorithm is to compute the best estimate $\hat{\theta}$ out of the $r$ estimates $G = \{\theta_1, \theta_2, \ldots, \theta_r\}$.

The steps contained in algorithm 3, will lead us to the number of measurements required to estimate a value for $\theta$:

**Algorithm 3**. Estimating $\hat{\theta}$ from a set of estimates $G = \{\theta_1, \theta_2, \ldots, \theta_r\}$

1. **Using the Central Limit Theorem**. Let $G$ be a random sample from a population having mean $\mu$ and standard deviation $\sigma$. Provided $r$ is sufficiently large, then the sampling distribution of the mean has approximately a normal distribution.

   Thus, $\mu_{\theta_r}$ is distributed according to:

   $$f = \frac{1}{\sqrt{2\pi\sigma^2/r}} \exp \frac{-(\mu_{\theta_r} - \mu)^2}{2\sigma^2/r} \tag{6}$$

   If we take $S$, the standard deviation of $G$, as a good approximation of $\sigma$, then eq. (6) becomes:

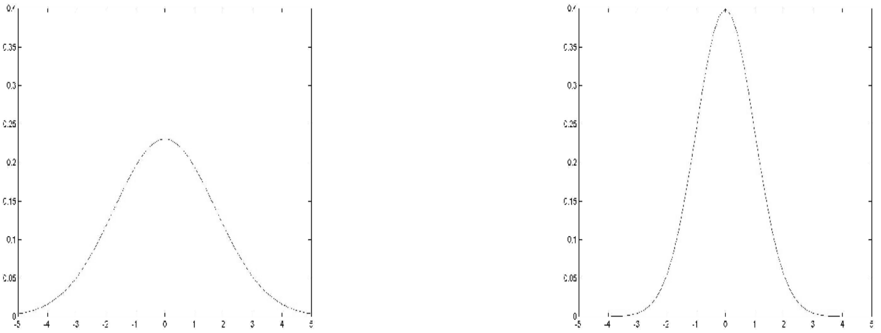
   $$g = \frac{1}{\sqrt{2\pi S^2/r}} \exp \frac{-(\mu_{\theta_r} - \mu)^2}{2S^2/r} \tag{7}$$

   So, after performing this step, we have achieved to shape $G$ into a normal distribution. In the following two steps we will take advantage of some properties of the normal distribution in order to accurately retrieve $\hat{\theta}$.

2. **Minimise dispersion**. Dispersion can be minimised by decreasing the variance. Thus, since the variance of distribution $g$ is $\sigma'^2 = \frac{2S^2}{r}$ then we must choose a suitable value for $r$ in order to narrow the normal distribution as much as it is required (see figure 3)

3. **Create a confidence interval for $\theta$.** Finally, once distribution $g$ has been narrowed (that is, dispersion has been minimised), we create a confidence interval to ensure that the estimate $\hat{\theta}$ is within the confidence interval in almost every retrieval process.
   In order to create a confidence interval, the number of samples $r$ and the normal distribution parameters are related by means of the equation
   $$r = \frac{Z^2_{\alpha/2}}{L^2}$$
   (see figure 3). As an example, a 95% confidence interval requires a $Z_{\alpha/2} = 0.05$ (that is, the probability of not finding estimate $\hat{\theta}$ within the confidence interval for a certain experiment) and $L = 0.1038$. (the values of L can be found in standard normal distribution look-up tables).

Finally, we must choose the largest number of steps from those steps required in eq. (5) and algorithm 3. Let us call such number $T$. Note that $T$ depends on the level of desired accuracy. Actually, this property can be seen as an additional advantage of IP in a Quantum Computer: the level of accuracy is not determined by the computer architecture but rather by the level of accuracy we aim at. Indeed, it is a property that would allow a 'standard' quantum computer to be used in different levels of precision depending on the application.



(a) (b)

**Figure 3**. Normal Distributions, Variances and Confidence Intervals

a) Normal distribution with high variance. In order to decrease variability in estimates, it is necessary to reduce the variance of the distribution. According to equation (5), variance is inversely proportional to the number of samples.

b) Normal distribution with small variance. Having reduced the variability of data, it is mandatory to define a confidence interval. The definition of a confidence interval is also related to the number of samples.

## 4.2. Retrieving a full Image

It must be noted that in the process of storing an image, we have assumed that adjacent frequencies are independent of each other. Even though it is not necessarily the case (colours are not randomly located in the human body), it is true that in many cases this condition suffices for analysis purposes.

Algorithm 4 provides a straightforward explanation of how to retrieve a full image.

**Algorithm 4**. Retrieving a full Image from a set of Qubit Lattices $Z$

1. Initialize ordered pair $(i, j)$
2. Compute algorithm 3 for $(i, j)$
3. Update $i, j$ and go back to step 2 until halting conditions are satisfied (for example, $i = n_1$ and $j = n_2$)

So, after having computed algorithm 4 a maximum number of $n_1 \times n_2$ times, the image stored in $Z$ is retrieved.

## 5. QUANTUM VS CLASSICAL STORAGE AND RETRIEVAL OF INFORMATION

The purpose of this section is to show how to use quantum mechanical properties in order to store, hide and retrieve sensible information. The quantum procedure is compared with a corresponding classical probabilistic method and it is shown that quantum mechanical unique properties (measurement using several bases) provide better results.

### 5.1. 4 colours

Let us assume we are allowed to work with only four colours: $C = \{C_1, C_2, C_3, C_4\}$. The purpose of this analysis is to show how quantum mechanical effects can help to represent and hide information, as well as to contrast such results with classical ones.

We first define the computational representation of colours in classical and quantum cases. Secondly, a procedure for storing classical and quantum values is shown and finally, a retrieval procedure for classical and quantum values is presented.

- In the classical case, let us represent the colours from $C$ by:
  $C_1 : 0$,
  $C_2 : 1$,
  $C_3 : \{0 \text{ with probability } p \text{ and } 1 \text{ with probability } 1-p\}$,
  $C_4 : \{0 \text{ with probability } 1-p \text{ and } 1 \text{ with probability } p\}$

- In the quantum mechanical case, we represent colours from $C$ by:
  $C_1 : |0\rangle$,
  $C_2 : |1\rangle$,u
  $C_3 : \sqrt{p}\,|0\rangle + \sqrt{1-p}\,|1\rangle$,
  $C_4 : \sqrt{1-p}\,|0\rangle - \sqrt{p}\,|1\rangle$

Note that in the classical case, colours $C_1, C_2, C_3, C_4$ are expressed as probability distributions while in the quantum mechanical case they are represented by quantum states. Therefore, in both cases identifying colours $C_1, C_2, C_3, C_4$ makes sense if and only if a certain number of measurements are performed.

We now randomly pick up colours from $C$ and store them in classical and quantum lattices. Let us suppose that $n$ 4-classical bit lattices $A_\alpha = (a_{i,j})_\alpha$ are available as well as $n$ 4-qubit lattices $B_\beta = (b_{i,j})_\beta$.

- For the classical case, take lattice $A_1$. Randomly and without replacement, choose colours from $C$ and initialize $a_{1,1}$, $a_{1,2}$, $a_{2,1}$ and $a_{2,2}$.

  Furthermore, all $n-1$ $A_2, A_3, \ldots, A_n$ lattices are initialized using the same spatial distribution as of $A_1$.

- The case for quantum mechanically storing colour information is quite similar to the previous one. Randomly and without replacement, choose colours from $C$ and use machine $A$ defined in section 1 to initialize qubits $b_{1,1}$, $b_{1,2}$, $b_{2,1}$ and $b_{2,2}$ from lattice $B_1$ with corresponding quantum states.

  Finally, all $n-1$ $B_2, B_3, \ldots, B_n$ lattices are initialized using the same spatial distribution as of $B_1$

Now, let us point at a very interesting situation. Let $p = 0.5$. In that case, colours $C_3$ and $C_4$ are *NOT* distinguishable in the classical case (the distributions for $C_3$ and $C_4$ are exactly the same for $n$ copies). In contrast, the quantum mechanical case allows us to distinguish between colours $C_3$ and $C_4$ as it will be shown in the following paragraphs.

A retrieval process is presented in the following lines for both classical and quantum mechanical cases. We include a discussion about retrieval and distinguishability for the case $p = 0.5$. Note that the fact that it is possible to use an infinite number of bases to measure a quantum mechanical system, plays a major role in our analysis.

- Information retrieval in the classical case is performed by measuring (that is, reading) bit values from 4 sets: $\{a_{1,1,i}\}$, $\{a_{1,2,i}\}$, $\{a_{2,1,i}\}$ and $\{a_{2,2,i}\}$ with $i \in \{1,2,3,4\}$.

  The above distributions are examples of Bernoulli distributions. Then, the expectation value of each distribution $\{a_{i,j,k}\}$, $k \in \{1,2,3,4\}$ is the average of all values in each set.

  Thus, it is possible to know for sure where colours $C_1$ and $C_2$ were stored (expectation values of the sets were $C_1$ and $C_2$ were stored are 1 and 0, respectively). However, it is not possible to determine the spatial location of neither $C_3$ nor $C_4$ as in both cases, the expectation value is equal or nearly equal to 0.5.

- In the quantum case, let us define the observables

  $$\hat{A}_1 = \alpha_1 |0\rangle \langle 0| + \alpha_2 |1\rangle \langle 1|$$

  and

  $$\hat{A}_2 = \beta_1 |+\rangle \langle +| + \beta_2 |-\rangle \langle -|$$

  And let us suppose that observable $\hat{A}_1$ is used to measure all qubits from a number of lattices $B_\beta$. It is clear that by means of this method, the experimenter can get to know where $C_1$ and $C_2$ are located, while $C_3$ and $C_4$ locations remain unknown.

  In addition, we can use observable $\hat{A}_2$ to measure at the locations of another set of lattices $B_\beta$. It can be seen that this procedure will allow the experimenter to know where colours $C_3$ and $C_4$ are located.

  Therefore, we can conclude that it is possible to store information (that has been randomly selected *a priori*) in qubits and, in spite of such random selection, to retrieve such information by using the unique measurement properties of quantum mechanics.

Let us finish this section with a comment on entanglement and its applications on IP: Our quantum protocol can benefit from the aplicability of dense coding (that is, the capability of transmitting 2 bits per qubit using prior shared entanglement between two particles. see[5]). Therefore, in case it is needed to transmit an image, using our storage method leads to a compression technique that has no paragon in the classical world.

### 5.2. Quantum secrecy vs Eavesdropping

It is relevant to point out the fact that having no *a priori* knowledge of what measurement bases are available to read information from qubit lattices $B_\beta$ introduces two very convenient properties: secrecy and eavesdropping detection.

Indeed, if an eavesdropper tries to read the information contained in an arbitrary set of qubits $|q\rangle \in B_\beta$ without knowing what bases are available for measurement, two main advantages with no counterpart in classical computers are found:

- The eavesdropper has only a certain chance to read accurate information (if he/she fails to choose the right measurement basis, he/she will get only a random outcome).

  For example, in the case stated at the beginning of this section, if only observable $\hat{A}_1$ were used to retrieve information, it would be impossible to determine where $C_3$ and $C_4$ were stored as the outcome distribution would actually be a Bernoulli distribution for those colours.

- The post-measurement state of a measurement performed with a wrong basis allows us to detect eavesdropping.[9]

## Acknowledgments

S.E. Venegas-Andraca gratefully acknowledges the receipt of grant 148528 from the people of México through the Mexican National Council of Science and Technology (CONACyT).

The authors want to thank N. Paunković for his very stimulating and wise comments about this work.

## REFERENCES

1. C. Trugenberger, "Probabilistic quantum memories," *Phys. Rev. Lett.* **87**, p. 067901, 2001.
2. D. Deutsch, "Quantum theory, the church-turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* **400**, pp. 97–117, 1985.
3. D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* **439**, pp. 553–558, 1992.
4. P. Shor, "Polynomial-time algorithms for prime factorization and discrete algorithms on a quantum computer," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, I. C. Society, ed., *Foundations of Computer Science*, pp. 124–134, 1994.
5. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, CUP, Cambridge, UK, 2000.
6. R. Gonzalez and R. Woods, *Digital Image Processing*, Addison-Wesley CO., USA, 1993.
7. E. F. G. ao and L. Hardy, "Substituting a qubit for an arbitrarily large amount of classical communication," *Preprint quant-ph/0110166* , 2001.
8. W. G. Cochran, *Sampling Techniques*, John Wiley and Sons, USA, 1978.
9. A. E. Dirk Bouwmeester and e. Anton Zeilinger, *The Physics of QUantum Information*, Springer-Verlag, Berlin, 2001.