# Past Research

Deval Deliwala

June 18, 2024

## 1 NEQRX: Efficient Quantum Image Encryption with Reduced Circuit Complexity

Reference

Various methods have emerged to compute and store digital image information on a quantum computer. The main two methods are

### 1.1 Flexible Representation of Quantum Images (FQRI)

Using FQRI, the positions $(x, y)$ of every pixel in an $n \times n$ image is encoded in a quantum register containining $2n$ qubits. The intensity of each pixel is encoded using the rotational angle of a separate qubit.

Therefore each of the $2n$ qubits contain their *own* qubit $|\psi\rangle$, where

$$|\psi\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle.$$

and $\theta$ is the angle representing the pixel's intensity. Therefore, an image with $N$ pixels (where $N = 2^n$) is represented as a quantum state:

$$|\psi\rangle = \frac{1}{N}\sum_{Y=0}^{N-1}\sum_{X=0}^{N-1}(\cos\theta_{YX}|0\rangle + \sin\theta_{YX}|1\rangle) \otimes |YX\rangle$$

Here $|YX\rangle$ represents the binary encoding of the pixel position, and $\theta_i$ represents the intensity angle for pixel at position $(X, Y)$.

#### Example

For a 2x2 image with grayscale values, the encoding process can be summarized as follows:

1. **Image Matrix**: Suppose the image matrix is

$$\begin{bmatrix} I_{00} & I_{01} \\ I_{10} & I_{11} \end{bmatrix}$$

where $I_{ij}$ represents the intensity of the pixel at position $(i, j)$.

2. Encode the positions using 2 qubits (for 2x2 image, 4 positions: 00, 01, 10, 11).
3. Encode the intensity values using rotation angles: $\theta_{00}, \theta_{01}, \theta_{10}, \theta_{11}$.

The quantum state representing the image $I$ will then be

$$|I\rangle = \frac{1}{2}\left(\cos\theta_{00}|0\rangle + \sin\theta_{00}|1\rangle\right)|00\rangle + \frac{1}{2}\left(\cos\theta_{01}|0\rangle + \sin\theta_{01}|1\rangle\right)|01\rangle + \cdots$$

Afterwards a bunch of quantum gates are applied to confuse and diffuse the quantum states. Then measurement gates are applied collapsing it to a classical state, from which the encoded pixel values and positions can be retrieved.

The time complexity of quantum image preparation for FRQI is too high. For a $2^n \times 2^n$ image, the procedure costs $O(2^{4n})$, quadratic in the image size. In addition because the gray-scale information of the image pixels is stored as the probability amplitude of a single qubit, accurate image retrieval is impossible for FRQI.

## 1.2 NEQR's Improvement

Reference

*Novel Enhanced Quantum Representation* (NEQR) is very similar to FRQI, except for its approach to encoding pixel values.

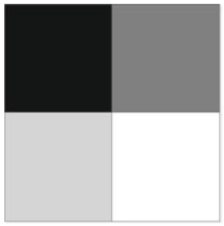
FRQI uses only a single qubit to store the gray-scale information for each pixel. NEQR uses two-entangled qubit sequences to store the gray-scale and position information, and stores the whole image in the superposition of the two qubit sequences.

Suppose the gray range of an image is $2^q$, then a binary sequence $C^0_{YX}C^1_{YX}\ldots C^{q-2}_{YX}C^{q-1}_{YX}$ encodes the gray scale value $f(Y, X)$ of the corresponding pixel $(X, Y)$. Mathematically,

$$f(Y, X) = C^0_{YX}C^1_{YX}\ldots C^{q-2}_{YX}C^{q-1}_{YX},\ C^k_{YX} \in [0, 1], \qquad f(Y, X) \in [0, 2^{q-1}]$$

Then the representative expression of a quantum image for a $2^n \times 2^n$ image can be written as

$$|I\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f(Y, X)\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\otimes_{i=1}^{q-1}|C^i_{YX}\rangle|YX\rangle$$



$$
\begin{aligned}
|I\rangle &= \frac{1}{2}(|0\rangle \otimes |00\rangle + |100\rangle \otimes |01\rangle + |200\rangle \otimes |10\rangle + |255\rangle \otimes |11\rangle) \\
&= \frac{1}{2}(|00000000\rangle \otimes |00\rangle + |01100100\rangle \otimes |01\rangle \\
&\quad + |11001000\rangle \otimes |10\rangle + |11111111\rangle \otimes |11\rangle)
\end{aligned}
$$

Figure 1: a $2 \times 2$ example image and its representative expression in NEQR

The paper in the second reference provides extensive detail on how to accomplish encoding a digital image in NEQR.

After quantum image preparation has been finished, you can manipulate everything reversibly or apply chaotic maps, logistic maps, to confuse and diffuse the image in a reversible manner.

The specific paper that implements *NEQRX*, just preforms NEQR but afterwards adds a generalized affine transformation and a logistic map. They also use an *Espresso* algorithm that apparently reduces computational cost by 50%.
Almost *every* quantum image encryption algorithm can be divided into two main types:

1. Transforming the image into a frequency domain with random operations
2. Encrypting the image using chaos theory

This paper goes into detail about the statistical tests you can employ to determine the effectiveness of an encryption algorithm – mainly *Differential Analysis* and a *Histogram Analysis*. It also performs a *Complexity Analysis* to assess the complexity of a quantum circuit.

It afterwards performs a *Noise Analysis*, where they use 6 known noisy backends and analyze the effectiveness of their algorithm and its dependence on noise.

# 2 Quantum Image Encryption Based on Quantum DNA Codec and Pixel-Level Scrambling

This encryption algorithm creates a quantum DNA codec that encodes and decodes the pixel color information of a quantum image using "its special biological properties". It afterwards employs *quantum Hilbert Scrambling* to muddle the position data in order to double the encryption effect. Then, the altered image was then employed as a key matrix in a quantum XOR operation with the original image.

## 2.1 NCQI Model

They use the NCQI model for encoding pixel information in quantum states. It is fairly similar to FIQR, where the NCQI model of a $2^n \times 2^n$ image $|I\rangle$ can be expressed as

$$|I\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C_{YX}\rangle \otimes |YX\rangle$$

where $|C_{YX}\rangle$ represents the color value of the pixel, which again is encoded by a binary sequence $R_{q-1} \dots R_0 G_{q-1} \dots G_0 B_{q-1} \dots B_0$.

## 2.2 DNA Coding Method & Operation

The ATCG binding rules for DNA state that A & T are complementary and C & G are complementary. Similarly, in binary, 0 and 1 are complementary, and they make certain binary sequences correspond to a DNA nucleoside. For example, for a $2 \times 2$ image, with 8 coding schemes in accordance with the rules of a biological model that encodes each nucleic acid with a 2-bit binary number, the DNA coding rules are as follows:

**Table 1.** DNA coding rules.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 00 | A | A | C | C | G | G | T | T |
| 01 | C | G | A | T | A | T | C | G |
| 10 | G | C | T | A | T | A | G | C |
| 11 | T | T | G | G | C | C | A | A |

Figure 2: DNA coding rules

Scheme 1 produces CACT is an image pixel's R-channel gray value is 71, which is represented by the binary sequence 01000111.

## 2.3 Quantum Hilbert Scrambling

Sounds fancy, but they just take the following matrix:

$$H_n = \begin{pmatrix} 1 & 2 & 3 & \dots & 2^n \\ 2^n+1 & 2^n+2 & 2^n+3 & \dots & 2^n+1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 2^{2n-1}+1 & 2^{2^n-1}+2 & 2^{2^n-1}+3 & \dots & 2^{2n} \end{pmatrix}$$

which employs the following transformation,

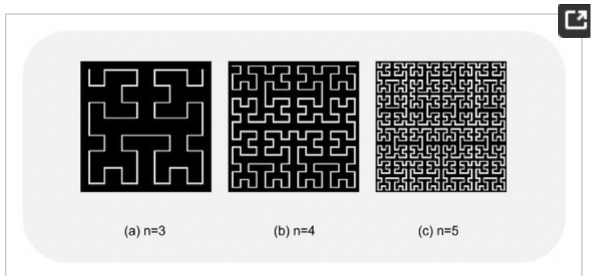



**Figure 2.** Hilbert curve.

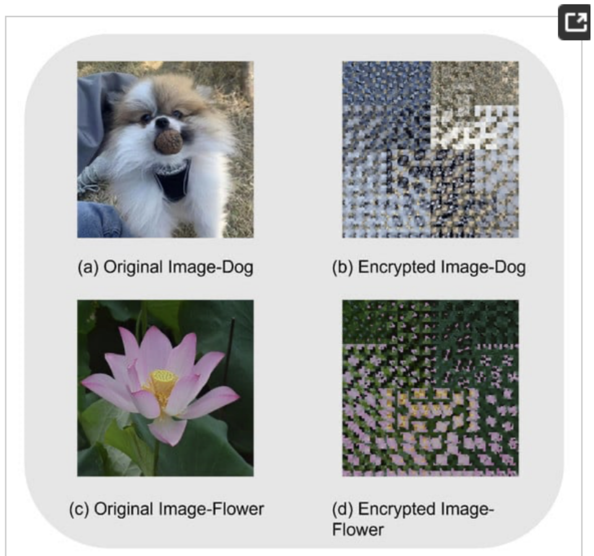



Figure 3: Results of performing a single Hilbert image scrambling

and then apply the following:

$$H_{n+1} = \begin{cases} \begin{pmatrix} H_n & (H_n + 4^n E_n)^T \\ (H_n + 3 \times 4^n E_n)^{\mathrm{pp}} & (H_n + 2 \times 4^n E_n)^T \end{pmatrix}, n \text{ is even} \\ \begin{pmatrix} H_n & (H_n + 3 \times 4^n E_n)^{\mathrm{pp}} \\ (H_n + 4^n E_n)^T & (H_n + 2 \times 4^n E_n)^T \end{pmatrix}, n \text{ is odd} \end{cases},$$

where $A^T$ represents a matrix $A$'s transpose, $A^{ud}$ its upper and lower direction reversed, $A^{ld}$ its left and right inversion, and $A^{pp}$ (haha pp) its center rotation matrix.

They then talk about how they encoded the DNA codec, and applied the quantum XOR operation, and afterwards go into the same statistical analysis as the previous paper.

# 3 Conclusion

Overall, these were the main two quantum image encryption algorithms that encapsulate all previous versions of quantum image encryption. There are many models like FIQR, NEQR, or NICQ that display a way to encode an image into a quantum state, but all of them are roughly the same apart from different time complexities to prepare the quantum state.

Our plan, which I think I have perfected, creates a completely new way to encode pixel color information, though it requires more qubits (unless we discretize an image into blocks of qubits, while somehow retaining the information of all pixels in a block, maybe by entangling the block-statevector with another qubit which holds all the RGB info for each pixel *in* the block?).
I'll start working on the paper that goes into the plan and have it ready soon.

## 3.1 References

### 3.1.1 Chaos Theory Papers

NEQR
FIQR
NEQRX
Four-Dimensional Chaos
Logistic Quantum Chaos

There are many others, but I do not have access to them and they are all roughly the same – apply a logistic map, or rounds of different logistic maps to scramble, then apply some color diffusing technique to gray-ify the image and so on. The other types of image encryption, that just perform scrambling by applying a bunch of other transformations are similar to the DNA codec paper or any other classical technique, while still applying NEQR or FIQR.

The good news is that our idea is very novel and has a different way of encoding information outside of FIQR or NEQR, and lowkey, is better than all of them ong.