Quantum Selective Encryption for Medical Images

Heidari, S., Naseri, M. & Nagata, K.
International Journal of Theoretical Physics **58,** 3908–3926 (2019).
https://doi.org/10.1007/s10773-019-04258-6

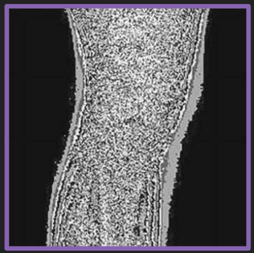
Brian Cornet
ECE 621 – Multimedia Communications
Dr. Honggang Wang
November 24, 2020

Selective Encryption for Medical Images

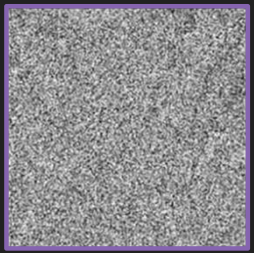
- Image encryption for only the relevant parts of an image, aka region of interest (ROI)
  - Improves encryption/decryption time over full encryption by skipping irrelevant parts
  - Less secure than full encryption of the entire image
- Medical grayscale images from ultrasounds, x-rays, etc. have large black (0x00) space
  - Ideal for entropy encoding to reduce file size and improve transmission time
  - Selective encryption retains black space; full encryption makes it noisy

Original Image

Selectively Encrypted

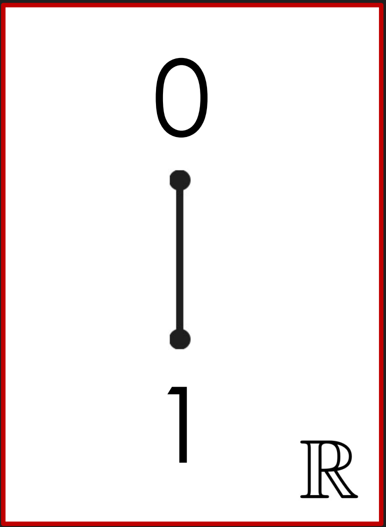


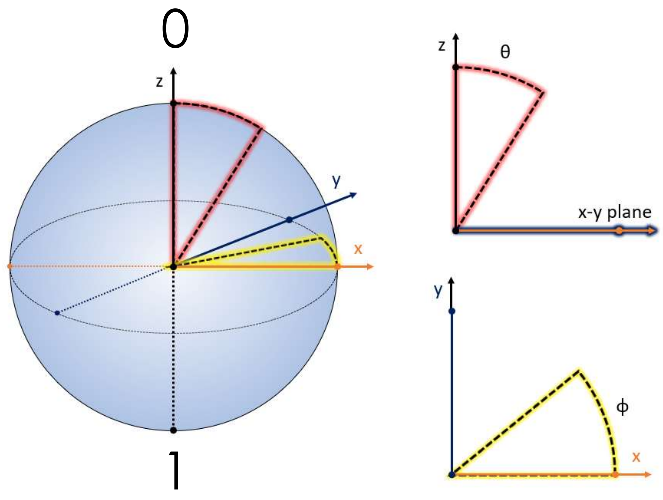
Fully Encrypted



Classical vs. Quantum: Bit Representation

- **Classical bits** are <u>discrete</u> values of **0** or **1** <u>exclusively</u>
- **Quantum bits (qubits)** are <u>continuous</u> probability vectors of **0** or **1** <u>inclusively</u>



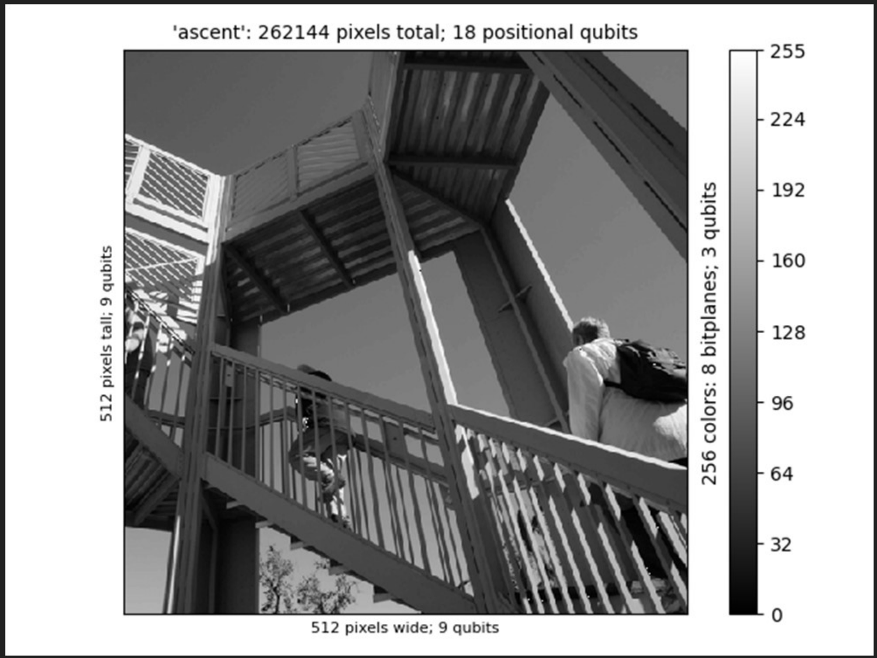


$$
\begin{aligned}
|\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\
&= \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\
&= \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} \end{bmatrix}
\end{aligned}
$$

Classical vs. Quantum: Bit String Lengths

- In a classical bitmap, an $\boldsymbol{M}\times\boldsymbol{N}$ image with $\boldsymbol{C}$ colors needs $\boldsymbol{M}\times\boldsymbol{N}\times log_2(\boldsymbol{C})$ bits
- The Bitplane Representation of Quantum Images (BRQI) method needs $log_2(\boldsymbol{M}\times\boldsymbol{N}\times log_2(\boldsymbol{C})) + 1$ qubits

Bit Type	Classical	Quantum
Position	262144	18
Color	8	3
Value	1	1
Total Bits	2097152	22



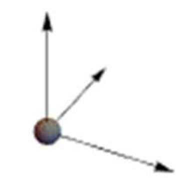
Classical vs. Quantum: Algorithms

- **Classical algorithms** must operate over sets of bits iteratively
  - Very easy to manipulate, less prone to error
  - Improved with more efficient algorithms, better processors, and multiple threads

$$\begin{bmatrix} 2 & 5 & 2 \\ 1 & 0 & -2 \\ 3 & 1 & 1 \end{bmatrix} \begin{bmatrix} -2 & 1 & 0 \\ -2 & 2 & 1 \\ 0 & 0 & 3 \end{bmatrix} = \begin{bmatrix} \quad & \quad & \quad \end{bmatrix}$$

- **Quantum algorithms** can operate over sets of entangled qubits simultaneously
  - Significantly improved time complexity for large sets, completely secure while in quantum state
  - Improved with better particles/environments for manipulation, better error correction

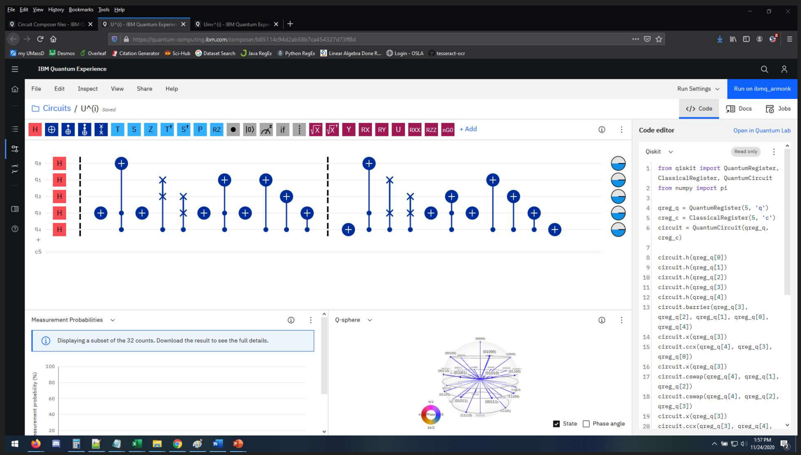
$$\begin{pmatrix} -5.20 & -2.28 & 7.06 \\ -2.28 & 6.22 & -3.51 \\ 7.06 & -3.51 & -0.09 \end{pmatrix}$$



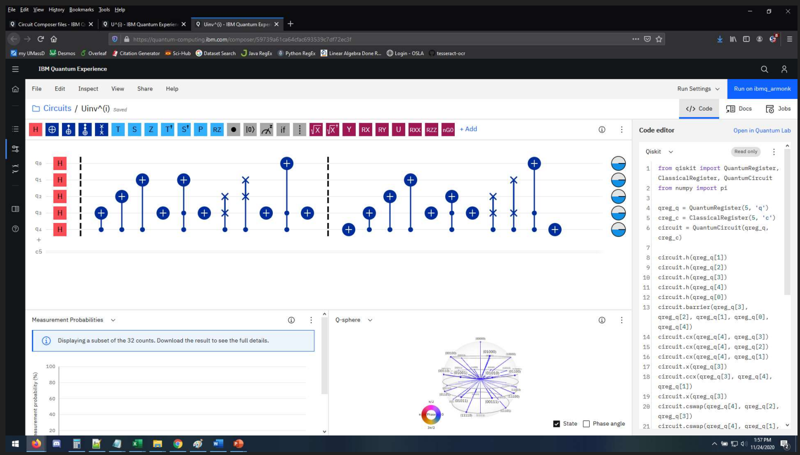
Recreating the Encryption Method

The base paper from Heidari et al.[1] describes the encryption and decryption methods for an image already represented in quantum data. Recreating these methods was done in IBM's Quantum Computing Circuit Composer. This provided initial code for Qiskit (Python).

Encryption Method

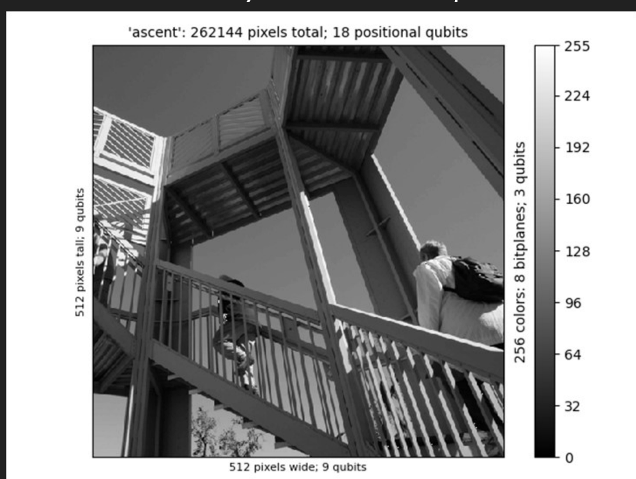


Decryption Method

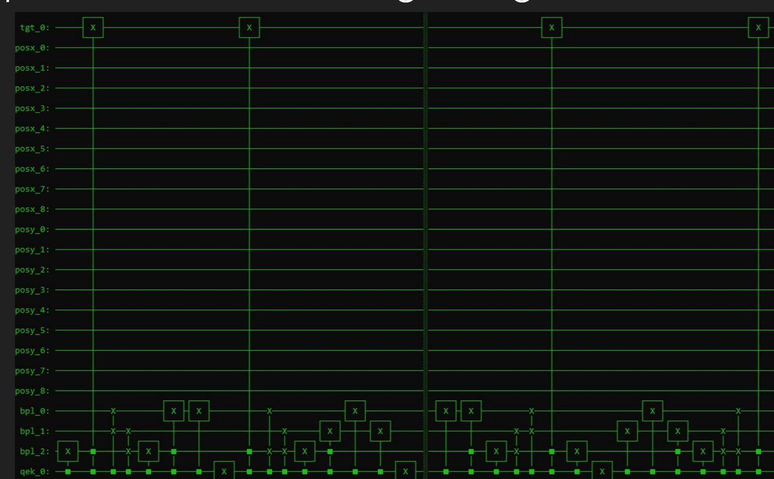


Converting Classical Data to Quantum

- **Problem:** need to recreate images in qubits
- **No-cloning theorem:**
  - *An arbitrary unknown qubit cannot be copied or amplified without disturbing its original state.*



?



Using Quantum Circuits to Initialize Data

- Solution in "A Quantum Image Representation Based on Bitplanes" by Li et al[3].
- Initial states are created through a quantum circuit specific to that image
  - CNOT (conditional-NOT) gates are used to create dependencies between specific outcomes

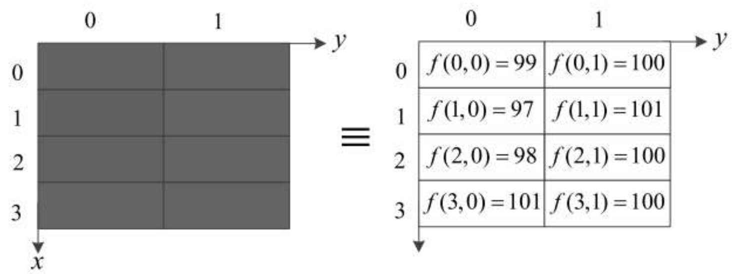


FIGURE 3. A 4 × 2 grayscale image.

For instance, we can store the image in Fig.3 in quantum systems using the circuit in Fig.7.

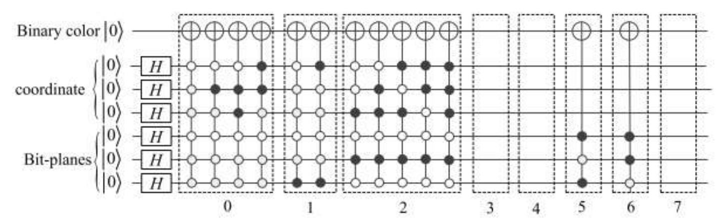
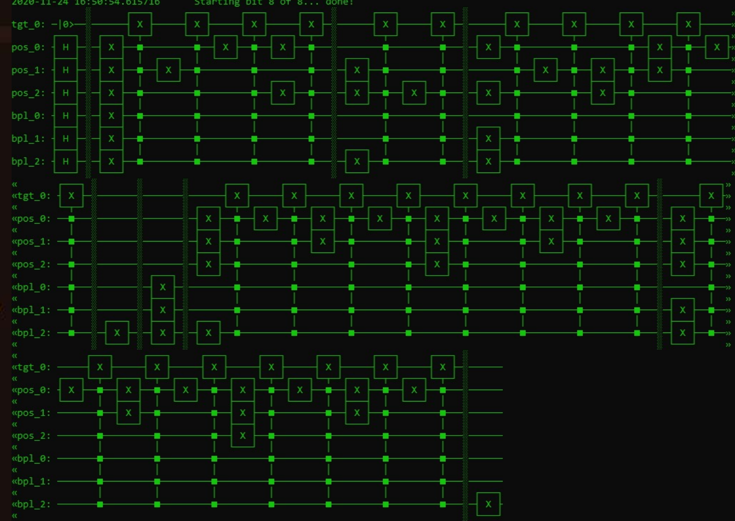


FIGURE 7. The implementation circuit of BRQI for grayscale images.

Qiskit Circuit Generation

```python
from qiskit import QuantumRegister, QuantumCircuit
from qiskit.tools.visualization import circuit_drawer
from datetime import datetime
import numpy as np
try:
    from PIL import Image, ImageDraw, ImageColor
except ImportError:
    import Image

def c2q(img): # takes about 3 minutes 20 seconds for lena.bmp
    x,y = img.size
    j,k = np.ceil(np.log2(x)),np.ceil(np.log2(y))
    n = j+k
    p = np.array(img).flatten()
    L = 2**np.arange(8).astype(int)
    N = 2**np.arange(n).astype(int)
    init = int(2**n - 1)
    prev = init
    Lset = [0,2,1,2,0,2,1,2]
    bpl = QuantumRegister(3, 'bpl')
    tgt = QuantumRegister(1, 'tgt')
    pos = QuantumRegister(n, 'pos')
    circ = QuantumCircuit(tgt,pos,bpl)
    circ.h(pos[:]+bpl[:])
    circ.reset(tgt)
    for i in range(8):
        print('%s\tStarting bit %d of 8... '%(datetime.now(),i+1),end='')
        circ.barrier()
        circ.x(bpl[Lset[i]:])
        iter = np.where(p.flatten() & L[i] > 0)[0]
        for a in iter: # values that require a circuit adjustment
            B = np.where(N & (a^prev) > 0)[0]
            for b in B:
                circ.x(pos[b])
            circ.mcx(pos[:]+bpl[:],tgt)
            prev = a
        print('done!')
    if n < 5:
        print(circuit_drawer(circ))
    return circ
```

```
In [84]: brqi_array = np.array([[99,100],[97,101],[98,100],[101,100]]).astype('uint8')^M
    ...: brqi_image = Image.fromarray(brqi_array)^M
    ...: brqi_circ = c2q(brqi_image)
2020-11-24 16:50:54.599510      Starting bit 1 of 8... done!
2020-11-24 16:50:54.600507      Starting bit 2 of 8... done!
2020-11-24 16:50:54.601504      Starting bit 3 of 8... done!
2020-11-24 16:50:54.603499      Starting bit 4 of 8... done!
2020-11-24 16:50:54.609513      Starting bit 5 of 8... done!
2020-11-24 16:50:54.610482      Starting bit 6 of 8... done!
2020-11-24 16:50:54.613479      Starting bit 7 of 8... done!
2020-11-24 16:50:54.615716      Starting bit 8 of 8... done!
```



This code demonstrates a basic implementation of the method for creating a circuit that generates a specific image as quantum data.

The example here is the same as the image from the previous slide.

Image Retrieval through Measurements

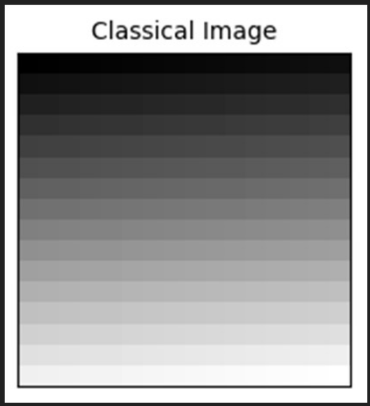
- Quantum states need to be measured to "collapse" onto a classical 0 or 1
  - One measurement only gives one out of 2^{n+3} results at random, so we need lots of measurements
- With all 2^{n+3} results returned as bit strings, the image can eventually be reconstructed

```
                 Count
Result
000 00000000 0       6
000 00001000 0       9
000 10000000 0       7
000 10000001 1      11
000 10000010 0       9
000 10000011 1      10
000 10000100 0      15
000 10000101 1       6
000 10000110 0       8
000 10000111 1      12
...                ...
111 11110111 1      11
000 01111111 1       9
111 11111000 1      12
111 11111001 1      11
111 11111010 1       7
111 11111011 1       6
111 11111100 1       7
111 11111101 1       6
111 11111110 1       6
111 11111111 1       8

[2048 rows x 1 columns]
```

```
        b         p  t
0     000  00000000  0
1     000  00000001  1
2     000  00000010  0
3     000  00000011  1
4     000  00000100  0
5     000  00000101  1
6     000  00000110  0
7     000  00000111  1
8     000  00001000  0
9     000  00001001  1
...   ...       ... ..
2038  111  11110110  1
2039  111  11110111  1
2040  111  11111000  1
2041  111  11111001  1
2042  111  11111010  1
2043  111  11111011  1
2044  111  11111100  1
2045  111  11111101  1
2046  111  11111110  1
2047  111  11111111  1

[2048 rows x 3 columns]
```

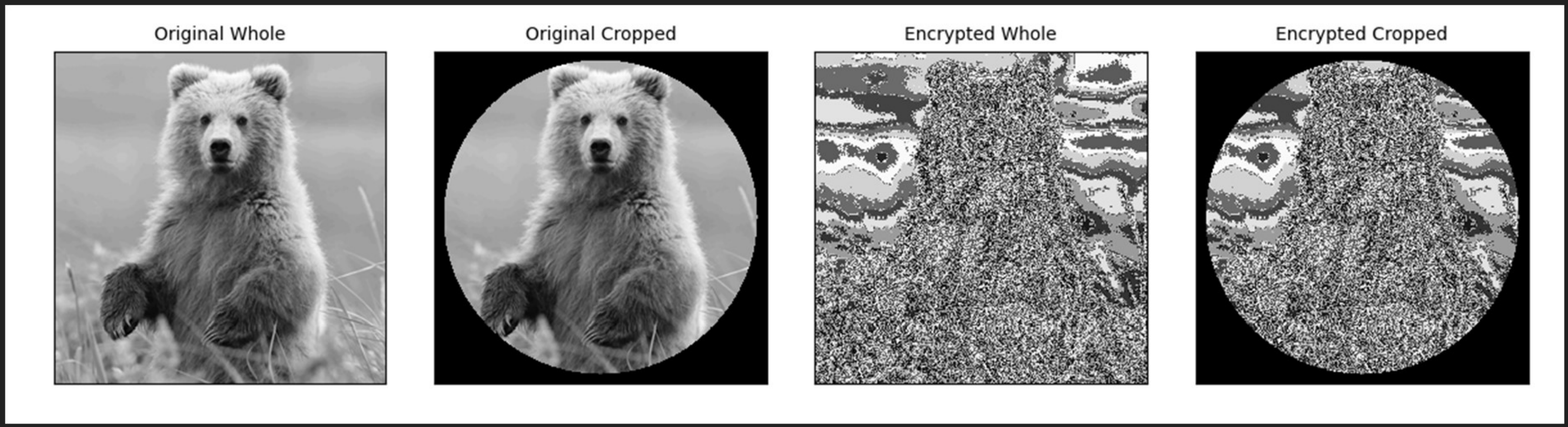
```
      b    p  t  VAL
0     0    0  0    0
1     0    1  1    1
2     0    2  0    0
3     0    3  1    1
4     0    4  0    0
5     0    5  1    1
6     0    6  0    0
7     0    7  1    1
8     0    8  0    0
9     0    9  1    1
...  ..  ... ..  ...
2038  7  246  1  128
2039  7  247  1  128
2040  7  248  1  128
2041  7  249  1  128
2042  7  250  1  128
2043  7  251  1  128
2044  7  252  1  128
2045  7  253  1  128
2046  7  254  1  128
2047  7  255  1  128

[2048 rows x 4 columns]
```

```
array([[  0,   1,   2,   3,   4,   5,   6,   7,   8,   9,  10,  11,  12,  13,  14,  15],
       [ 16,  17,  18,  19,  20,  21,  22,  23,  24,  25,  26,  27,  28,  29,  30,  31],
       [ 32,  33,  34,  35,  36,  37,  38,  39,  40,  41,  42,  43,  44,  45,  46,  47],
       [ 48,  49,  50,  51,  52,  53,  54,  55,  56,  57,  58,  59,  60,  61,  62,  63],
       [ 64,  65,  66,  67,  68,  69,  70,  71,  72,  73,  74,  75,  76,  77,  78,  79],
       [ 80,  81,  82,  83,  84,  85,  86,  87,  88,  89,  90,  91,  92,  93,  94,  95],
       [ 96,  97,  98,  99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111],
       [112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127],
       [128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143],
       [144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159],
       [160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175],
       [176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191],
       [192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207],
       [208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223],
       [224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239],
       [240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255]],
      dtype=uint8)
```



Encrypting Large Images

- Quantum simulations on a common classical device can still take a while
- Images over 16x16 (6 positional qubits) exceed memory limits
- Solution is to break images into 16x16 blocks, encrypt, then reassemble

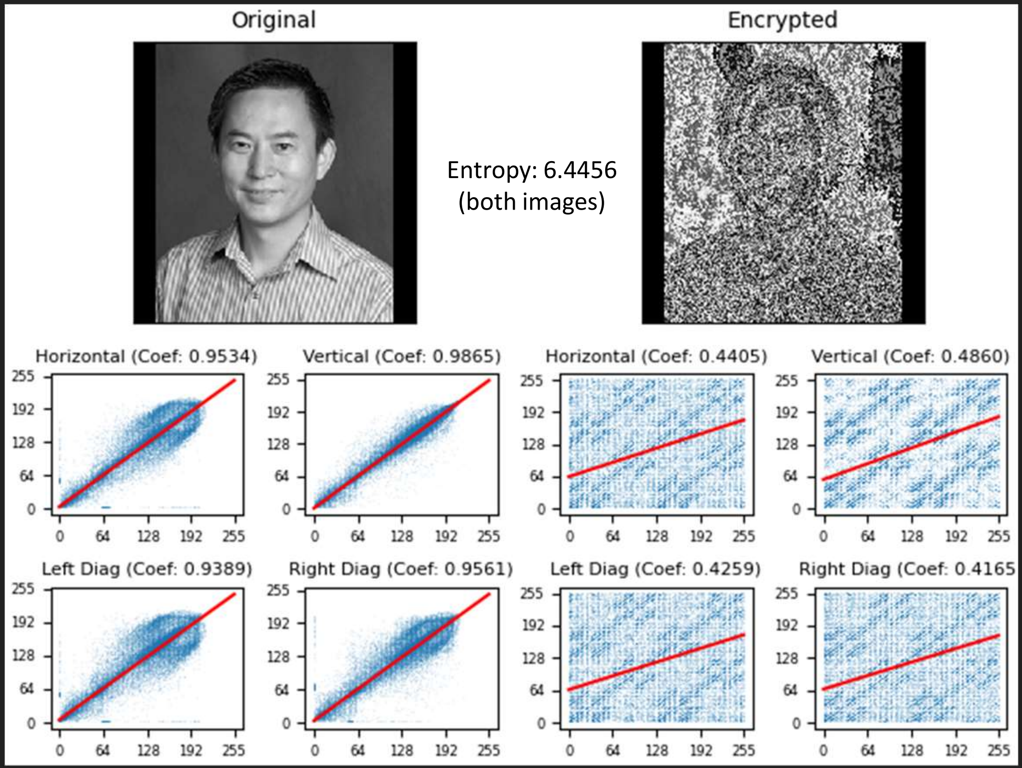


Correlation and Entropy Testing

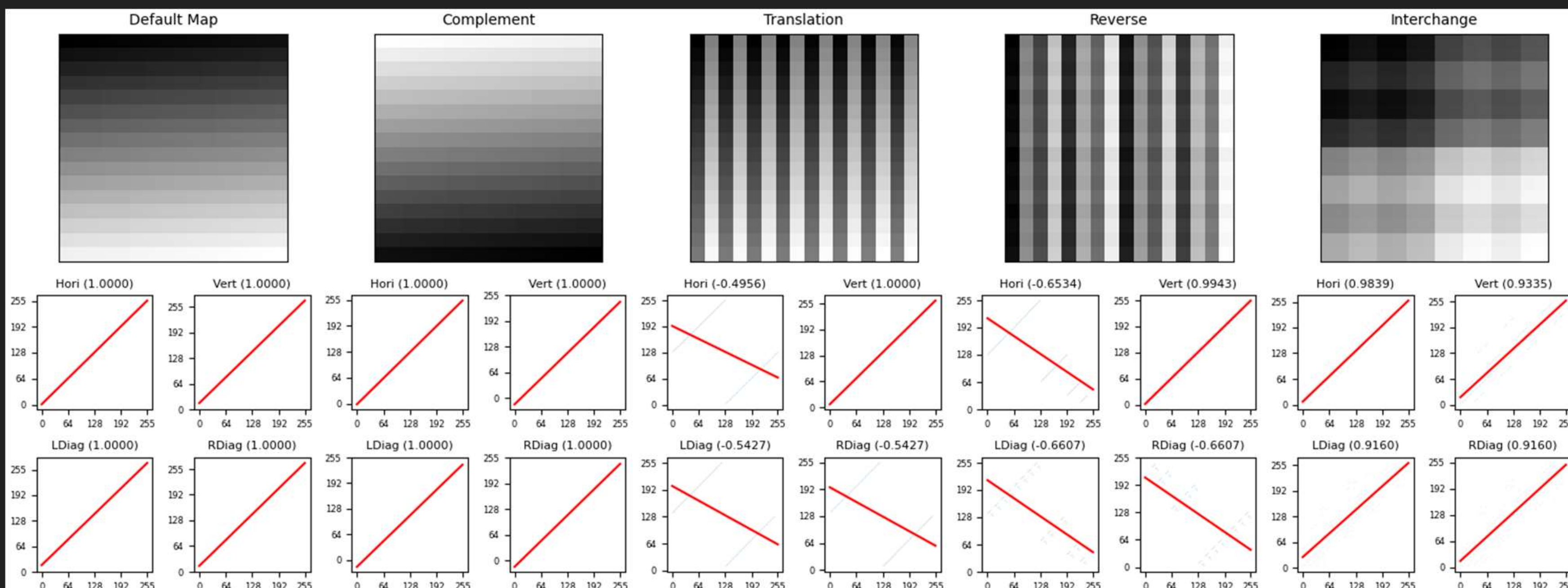
- Normally, adjacent pixels have a high correlation
- Encrypted images should have lower correlation and a Shannon entropy near 8

$$Entropy = -\sum_{i=1}^{2^L-1} p(u_i) log_2 \left(p(u_i)\right)$$

Heidari et al. reported correlation coefficients < 2% and entropy > 7.95 for fully encrypted 256 x 256 images



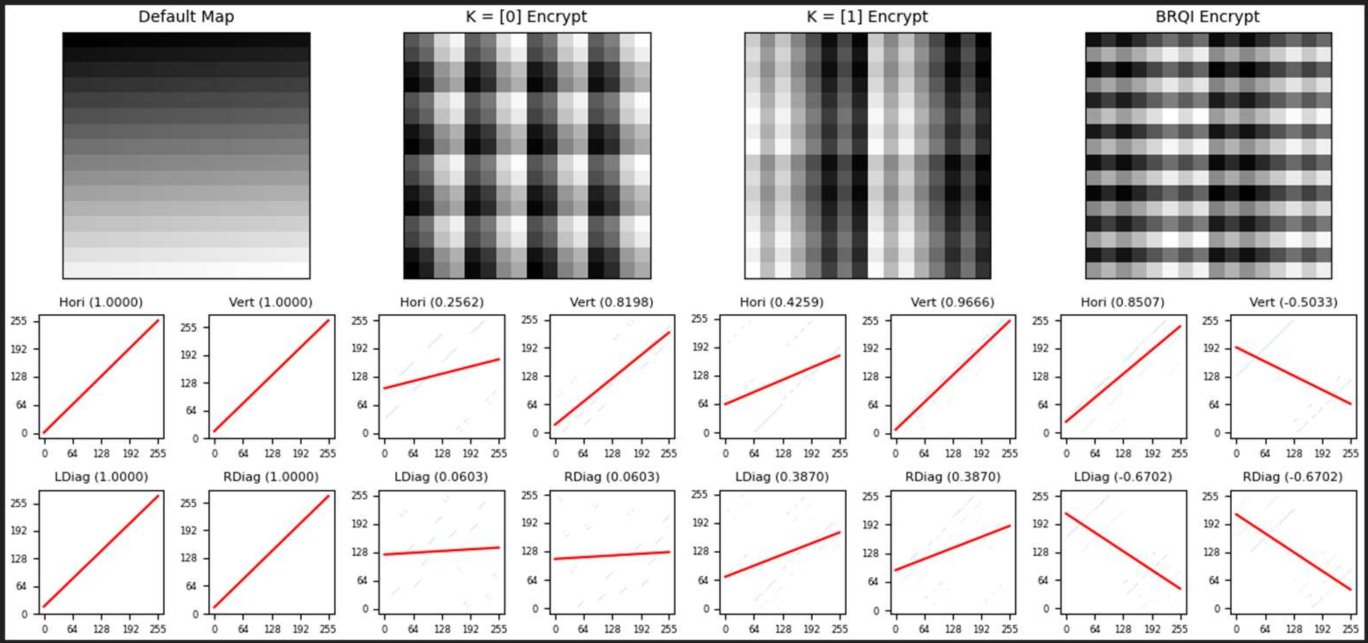
Encryption Transformations



Encryption Methods on Sample Palette

Ignoring complement methods which are incompatible with selective encryption, the BRQI transform has a better immediate result than either encryption operation.

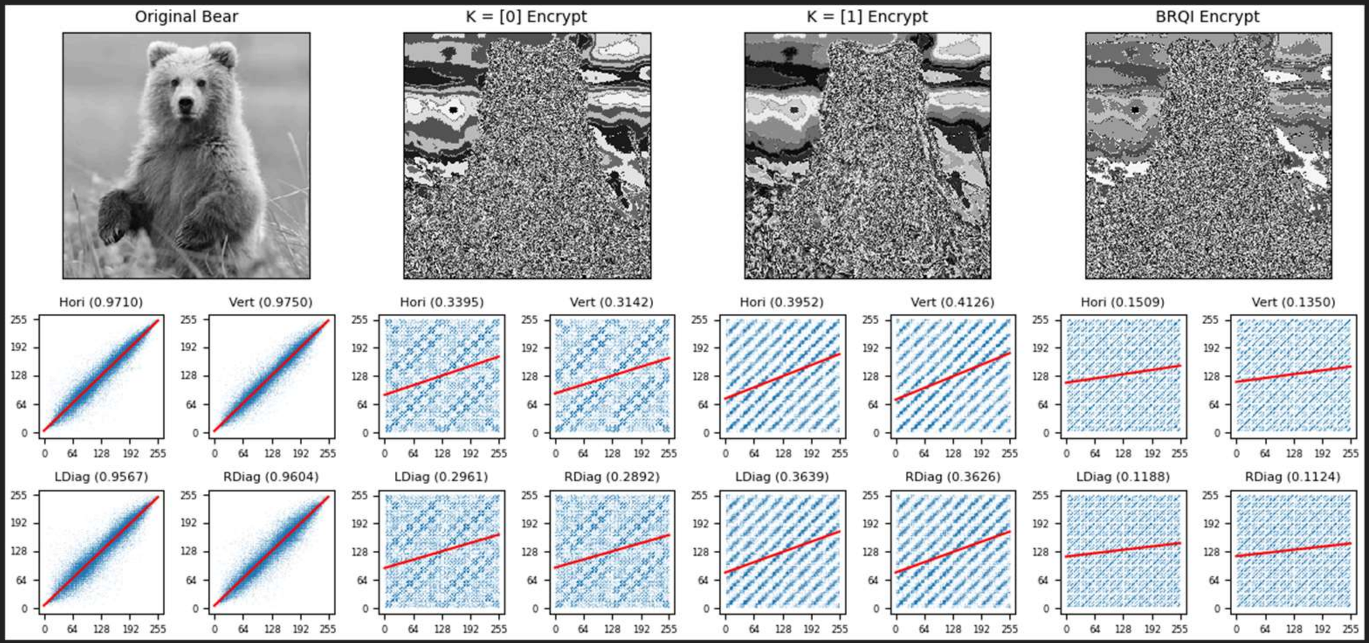
Note that entropy is still fixed and minimum correlations will be limited when some areas have solid colors.



Encryption Methods on Bear Image

Ignoring complement methods which are incompatible with selective encryption, the BRQI transform has a better immediate result than either encryption operation.

Note that entropy is still fixed and minimum correlations will be limited when some areas have solid colors.



Simulation Results

- ☑ Correctly created quantum circuits and generated quantum images
- ☑ Successfully implemented encryption/decryption process with measurements
- ☒ Simulation did not see similar results in correlation and entropy analysis

- First attempt at quantum computing!
- The original algorithm uses **complements** to flip the value bits from 0 to 1 or 1 to 0
  - This causes black pixels (0x00) to become another color unless specific keys are used
  - Security is better improved through other methods (reverse, interchange, translation)
- **Solution:** develop a new algorithm that avoids complement operations
  - Black or white pixels will be left alone, all others change conditionally

References in Draft Report

1. S. Heidari, M. Naseri, and K. Nagata, "Quantum Selective Encryption for Medical Images," *International Journal of Theoretical Physics,* vol. 58, no. 11, pp. 3908–3926, Nov. 2019, ISSN:1572-9575, doi: 10.1007/s10773-019-04258-6.
2. W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot Be Cloned," *Nature*, vol. 299, no. 5886, pp. 802-803, 1982.
3. H. Li, X. Chen, H. Xia, Y. Liang, and Z. Zhou, "A Quantum Image Representation Based on Bitplanes," in *IEEE Access*, vol. 6, pp. 62396-62404, 2018, doi: 10.1109/ACCESS.2018.2871691.

Additional References for Final Draft

4. C. H. Bennett and G. Brassard. “Quantum Cryptography: Public Key Distribution and Coin Tossing,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 1, pp. 175-179, 1984.
5. N. Hosseinidehaj, et al, “Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook,” in *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 881-919, 2019.
6. J.-W. Pan, et al, “Satellite-to-Ground Quantum Key Distribution,” *Nature*, vol. 549, no. 7670, pp. 43-47, 2017.
7. A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum Error Correction Via Codes Over GF(4)," *Proceedings of IEEE International Symposium on Information Theory*, Ulm, Germany, 1997, pp. 292-337.
8. Z. Zhang et al., "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," in *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28-41, Sept. 2019.