Simulation of Quantum Selective Encryption for Medical Images

Brian Cornet[1,3,4], Honggang Wang[2]
[1]*Computer and Information Science,* [2]*Electrical and Computer Engineering,* [3]*Mathematics*
University of Massachusetts Dartmouth
Dartmouth, MA 02747, USA
[4]*Population and Quantitative Health Sciences*
University of Massachusetts Medical School
Worcester, MA 01655, USA
bcornet@umassd.edu, hwang1@umassd.edu

***Abstract*—Selective image encryption allows for a faster encryption process without compromising solid-color space ideal for compression. Quantum computing is expected to dramatically improve the time complexity of encryption algorithms even further, well beyond what classical computers could achieve. This paper replicates one such method used for selective imaging and describes its implementation and challenges.**

I. Introduction

Image encryption is an essential part of securely transferring and storing digital images, particularly for images containing sensitive information [1] [2]. By transforming an image into something visually unrecognizable and indecipherable, encryption prevents unauthorized users from accessing it. Authorized users privy to the original encryption process can then restore the image to its original form as needed. Effective encryption may be a lengthy process for large images. In such cases, selective encryption may be used. With selective encryption, the encryption process is only performed on certain regions of interest (ROI).

Medical images are notable for containing highly sensitive personal information. In addition, many medical images such as x-rays and ultrasounds often have large empty spaces represented as a solid black background (e.g. off-body space) [3]. Such regions are useful for compression methods such as run-length encoding, but would become indistinguishable from ROI when fully encrypted. As a result, selective encryption is highly compatible with medical images for the purposes of improving encryption, transmission, and decryption times.

It is expected that quantum-based technologies will be a core component of 6G communications introduced by 2030 [4]. Quantum computers have been shown to dramatically reduce the time complexity of large data operations as seen in Arute et al.[5], and quantum communications are used in provably secure communications as seen in Liao et al. [6]. Though quantum technologies are still in their relative infancy, the translation of classical methods into quantum-based environments is an ongoing area of research.

This paper simulates a quantum selective encryption method intended for 8-bit grayscale images as described in Heidari et al. [1]. The original method utilizes a method for translating classical image data into a quantum format known as a Bitplane Representation of Quantum Images (BRQI) from Li et al. [2]. Section II of this paper describes the differences between classical and quantum computing. Section III details the process of creating and measuring quantum images with Python's Qiskit library. Section IV discusses the results of this simulation.

II. Classical vs. Quantum Computing

Classical computing – as seen in almost every modern device – operates with data as a discrete permutation of binary values or ”bits” (0 or 1) [7]. A bit string of 10001010 may corresponds to the number 138 as an unsigned integer, for example. It can be said that a bit string of length n has 2^n distinct possible values, though it may only represent one of those values at a single time. Barring the use of compression methods to simplify this data, operations to transform an entire set of these values must operate on each value individually. For an image of $M \times N$ size, this would require MN total operations. An uncompressed representation of an image with a P color palette would require $M \cdot N \cdot C$ bits, where $C = \lceil \log_2 P \rceil$ is the bit length of the color palette.

Quantum computing instead relies on the concept of the quantum state [8] [9]. Quantum particles such as photons and electrons can exist in a quantum state where they do not have definite measured values for various properties. Instead, they are represented as probability vectors for any possible outcome prior to measurement. The principle of superposition states that the combination of any number of quantum states results in another quantum state, meaning any quantum state can be represented as a sum of independent states. For this reason, a particle in a quantum state is often described as being all of its results simultaneously.

A qubit (”KYOO-bit”) is a quantum state with two possible outcomes [8]. Much like a classical bit, these outcomes can be described as 0 or 1. While the qubit is in its quantum state however, the probabilities of these outcomes are represented as a linear combination of probability amplitudes α and β, where $\left|\alpha^2\right|$ is the probability of a value of 0, $\left|\beta^2\right|$ is the probability of a value of 1, $\left|\alpha^2\right| + \left|\beta^2\right| = 1$, and both α and β are complex numbers. Upon being measured, a qubit will ”collapse” into a basis state of either 0 or 1 depending on the values of α and β. Qubits can be ”created” from any two-level quantum-mechanical system where 0 and 1 can be represented by binary states, such as the polarization of light in a photon or the spin of an electron. Qubits are typically represented geometrically through a Bloch sphere. Assuming a qubit in a ”pure” quantum state, each point on the surface of the Bloch sphere represents a possible value of the vector $|\Psi\rangle$. The definition can be expanded using the spherical coordinates $\alpha = \cos\frac{\theta}{2}$ and $\beta = e^{i\varphi}\sin\frac{\theta}{2}$.

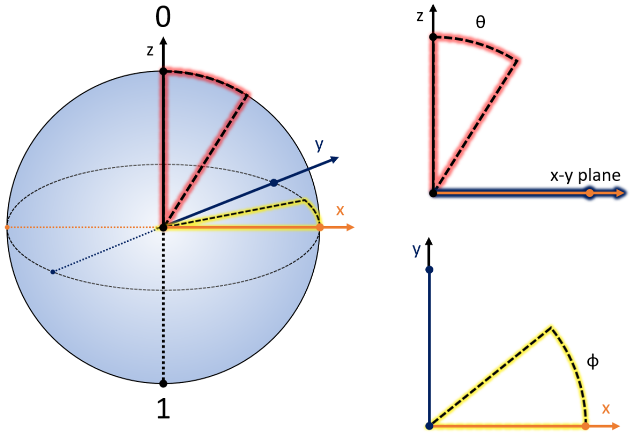

Fig. 1. A Bloch sphere.

One of the key differences between quantum and classical physics is the concept of quantum entanglement [8]. Two or more particles are said to be ”entangled” when the quantum state of one particle is dependent on the state of the others, even at a large distance. This creates not only a linear dependency between sets of entangled qubits, but allows measurements to be performed at any distance so long as the entanglement remains. Note that the entanglement ends as soon as either qubit is measured as the quantum state is lost for that qubit. In addition, the correlation between a set of entangled qubits cannot be determined without comparing the results of these measurements through a classical channel. And since no changes can be observed on qubits in a quantum state, the change itself cannot be used as a means of instantaneous communication [10].

Since a qubit can represent both 0 and 1 simultaneously, a quantum computer can describe an image of $M \times N$ size with a C color bit length to be represented with the BRQI protocol with as few as $\lceil \log_2(MNC) \rceil + 1$ qubits [7] [2]. For example, a 512×1024 image with about 16 million colors (24 bit) might require 12,582,912 classical bits (1.5 MB) to store uncompressed. A BRQI version of that image would instead require 25 entangled qubits: 9 for M, 10 for N, 5 for C, and an additional qubit to represent value. Operations can also be performed over an entire set of qubits in one step rather than iteratively as with classical systems. This allows quantum computers to achieve a significantly faster time complexity for large data sets. In 2019 [5], a 53-qubit quantum computer (approx. 9 quadrillion possible states) completed a given task in 200 seconds that a classical supercomputer was estimated to complete in about 10,000 years. This was considered the first instance of quantum supremacy: proof of a task that a classical supercomputer could not complete – or could not complete within a reasonable amount of time – that a quantum computer could.

Owing to an inability to measure or reproduce a quantum state without compromising it [11], communication through entangled qubits is provably secure [8]. Quantum communication relies on the concept of quantum teleportation, which takes advantage of the irrelevance of distance between entangled qubits [12]. Transmitting an entire set of quantum data would be ideal as the whole set would be completely secure, but this is fairly difficult due to the sensitivity of entangled states [13]. Fortunately, an entangled qubit set can instead serve as an encryption key for a classical set of encrypted data – this forms the basis of the highly-effective quantum key distribution (QKD) method. Developments for a global quantum network (or quantum internet) are expected to be realized by 2030 alongside 6G wireless communication networks [4]. Experiments from Liao et al. [6] demonstrate the practicality of such networks.

Quantum encryption methods such as the method described by Heidari et al. [1] will depend on the availability of quantum computing services to perform the encryption process. Particularly, professional medical organizations such as hospitals will either require a quantum computer on location or rely on third-parties to manage the encryption, communication, and decryption processes remotely. Decryption can be performed on the same device so long as the quantum encryption key can be stored. Alternatively, communicating an encrypted image and allowing the receiver to decrypt the image securely is also possible through QKD [12].

III. Quantum Selective Encryption Method

The basis of the encryption method from Heidari et al. [1] utilizes the BRQI protocol described by [2]. Any classical image can be represented as a collection of bitplanes, or binary images that indicate the color value at each pixel coordinate $(i,\ j)$ in $M \times N$ for a particular color bit. Note that while BRQI supports any color palette size, the original algorithm specifies 256 color (8-bit) grayscale images as the input given the purpose of encrypting medical images:

$$\begin{gathered}
|\Psi\rangle = \frac{1}{\sqrt{MNC}} \sum_{l=0}^{C-1} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} |g(x,y)\rangle\,|x\rangle\,|y\rangle\,|l\rangle \\
|\Psi_B^8\rangle = \frac{1}{\sqrt{2^{m+n+3}}} \sum_{l=0}^{2^3-1} \sum_{x=0}^{2^m-1} \sum_{y=0}^{2^n-1} |g(x,y)\rangle\,|x\rangle\,|y\rangle\,|l\rangle \\
m = log_2 M, \quad n = log_2 N, \quad m+n \text{ is an integer}
\end{gathered} \tag{1}$$

Equation 1 describes the vector $|\Psi\rangle$ as the BRQI for an image of C color bits and $|\Psi_B^8\rangle$ for an image of $P = 256$

colors respectively. Here, M and N are the image height and width respectively (in pixels), C is the bit length (or number of color bits), m and n are the number of qubits needed to represent all pixel locations, x and y are coordinates for a particular position, l is a bitplane within the range of 0 to $\lceil \log_2 C \rceil$, and $g\left(x,y\right)$ is the binary value at a particular location for that bitplane (also known as the target value). The bottom equation assumes $C = 8$ and will be used in this simulation.

A. Creating Quantum Images

In order to apply the encryption methods, the classical image needs to be replicated in a quantum state. Note that these are two physically different things: classical bits are electric voltages, whereas qubits are particles. And unlike with classical data, quantum information cannot be arbitrarily assigned to any particular value [11]. Fortunately, particular states can be approximated through quantum circuits, where various quantum logic gates act as physical transformations often described through unitary matrices.

The final qubit set state under BRQI can be described as a vector of length $M + N + C + 1$ [2], where $M + N + C$ variables are free (representing all positions and bitplanes) and the extra variable (the target value) is determined by any particular permutation of measurements from those free variables. For these free variables, the Hadamard gate (H gate) is used to map each qubit to an initial superposition state with an equal probability of being measured to 0 or 1. The target value however requires being initially mapped to the ground state $|0\rangle$, or to a state where 100% of measurements will be 0. The methods for doing so with a real quantum computer are described in Nielsen et al. [9], with improvements being the subject of research as of 2020. In the Qiskit simulated environment, the $reset()$ function achieves this result. At this point, measuring the initialized image set would produce a solid black image since the target value would always measure to 0.

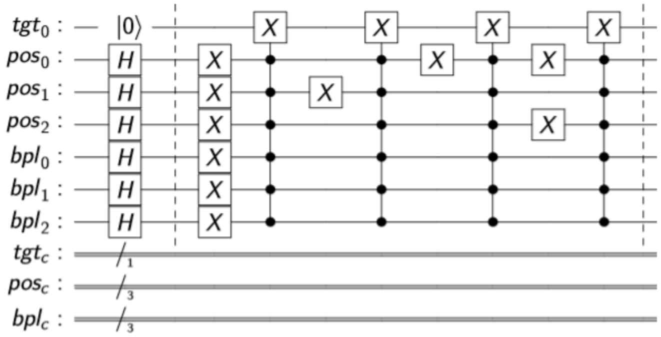

Fig. 2. Initial steps in an example circuit for an 8 pixel image. Bitplane 0 has target values of 1 at positions 0, 2, 3, and 5.

After initializing the qubit set, each position and bitplane must be associated with its corresponding target value from the original classical image. To do this, a series of conditional NOT (CNOT) gates are used to flip the target value's initial state of 0 to a value of 1 based on particular position and bitplane values. A series of Toffoli (CCNOT) gates can replicate this effect on the condition of two values being 1 affecting the target qubit. Qiskit conveniently provides the $mcx()$ function for a multiple CNOT (MCNOT) operation. Treating each initial H state as a 1, a series of Pauli-X (NOT) gates must be applied to positional and bitplane qubits to change target values associated with them. For example, a 4×2 8-bit image with a value of 32 in the position $(2, 0)$ would require applying NOT gates to figuratively transform 0 11 1 111 into 0 10 0 101, then apply the MCNOT gate to change the target to 1 to create the dependency 1 10 0 101. This must be done for all target values of 1 across all positions and bitplanes. The final circuit must ensure that an even number of NOT gates has been applied to each positional and bitplane qubit to avoid repositioning pixels or interchanging bitplanes. In other words, if H states are treated as 1s, the example image must end as t 11 1 111 (where t is whatever target value was assigned to the last pixel's most significant bitplane).

B. Adding Encryption and Decryption

From Li et al. [2], there are four methods of image processing used in scrambling an image for encryption purposes. Between these methods described, there are 16! or about 2.09×10^{13} possible transformations of an image. For selective encryption, this number is reduced to $8! \cdot 8!$ or about 1.63×10^{9}. The encryption method from Heidari et al. uses several of these conditionally based on the values of an arbitrary length qubit string K [1]. The algorithm then applies one of two transformations based on the value of each qubit in the string.

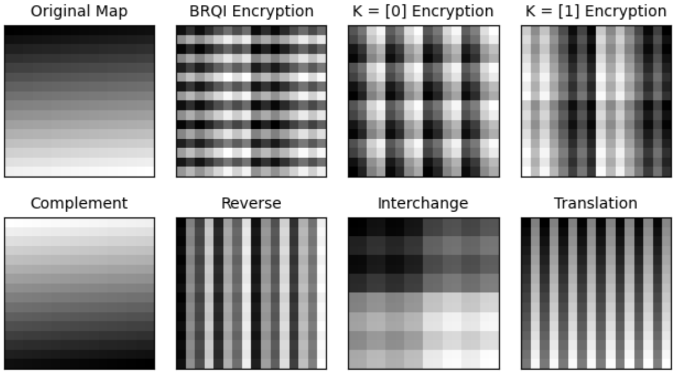

Fig. 3. A 16×16 color map of all possible grayscale values (top-left) with different encryption methods applied (remaining top row). Individual operations illustrate sequential changes in the color palette (bottom row).

1) Complement: Also known as inversion, this operation simply applies a NOT gate over the target value qubit. It can be replicated classically through the same NOT operation, flipping all color bits from 0 to 1 or 1 to 0. By itself over an entire image, this operation has little value since an inverted image will resemble the original and is easily restored. Note that this operation – and only this operation – can cause a solid black area (such as the empty space in medical images) to become a different color. As a result, it should be avoided in selective encryption. However, the method used in Heidari et al. [1] introduces a conditional complement for any key qubit K_i that differs from the third bitplane qubit l_3.

2) Reverse: This operation rearranges the order of bitplanes by applying NOT gates to all of the bitplane qubits. A classical replication would involve reversing the order of bits for each pixel location (e.g. an 8-bit value of 10110111 or 182 would become 11101101 or 109). Bitplanes of lesser significance are typically noisy, whereas bitplanes of increasingly greater significance more and more closely resemble the original image. By reversing the bitplane order, an image will generally appear indecipherable.

3) Interchange: This operation mixes bitplanes by applying two CSWAP gates to the bitplane qubits based on the target value. For target values of 0, l_0 and l_1 are swapped, and for target values of 1, l_0 and l_2 are swapped. This allows for a different form of encryption beyond simply rearranging the bitplanes, though the first and last bitplanes are ignored. Note that while this operation is the only one to introduce a condition based on the target value, any operation other than

4) Translation: This operation right shifts the bitplanes though a NOT, CNOT, and CCNOT gate sequence, or left shifts through a reversed order. A classical replication can be performed with the bitwise circular shift operations for right and left shifts such that 10110111 would become 01011111 (right shift) or 01101111 (left shift). This can have less of a dramatic change on the visibility of an image compared to the reverse operation but allows for more bitplane permutations for scrambling.

5) Decryption: Since all quantum computing operations are Hermitian matrices, the decryption process is the inverse of the encryption process [9]. Applying each gate from the original operation in reverse order is sufficient for replicating the inverse of the original transform. Any operation matrix U_i will be multiplied by its inverse U_i^{-1} sequentially leading to $U_iU_i^{-1} = I$, where I is the identity matrix and corresponds to the original image state. For example, an encryption algorithm described as $U_1U_2U_3$ would carry the decryption algorithm $U_3^{-1}U_2^{-1}U_1^{-1}$, and the final result after applying both processes would be $U_1U_2U_3U_3^{-1}U_2^{-1}U_1^{-1} = I$. As long as the original encryption process is known, decryption is trivial.

C. Measuring Quantum Images

Qubits exist as probabilities of possible measurements rather than discrete values as with classical bits [9]. Measuring these qubits results in each qubit ”collapsing” into a classical bit value of 0 or 1. The quantum circuit will have established dependencies on the target values based on the outcomes of a measurement for every positional and bitplane qubit. However, a single measurement will only return one target value from one position on one bitplane. 2^{m+n+3} possible outcomes exist at an equal probability of $\frac{1}{m+n+3}$ for $m + n + 3$ qubits initialized with an H-gate – note that the target value qubit is entirely determined by every other qubit as it was initialized with the ground state $|0\rangle$. To account for every value possible, thousands or even millions of measurements may be necessary depending on the size of the image. The results will then produce a series of bit strings that can be interpreted into an image through various bit operations.

With a real quantum computer, the results will see some error caused by the imperfections of the physical circuit implementation. Quantum error correction is necessary for resolving these errors and is typically implemented through increasing the number of measurements as needed. Alternatively, additional qubits can be used to simulate the error correction methods used in classical computers. Examples of this include the Shor code (requires 8 error qubits per regular qubit) and the CSS or Calderbank-Shor-Steane code (requires 4) [14]. This is not necessary in a simulation, however. The Qiskit $measure()$ function will specifically return a dictionary of string as keys with integer counts for how many times that particular result was measured. A conversion into a numeric format is necessary for the keys of this dictionary.

It is expected that simulations run on personal devices will not replicate the speed of a real quantum computer or a simulation run on a supercomputer. Memory limits may also prevent the simulation of a sufficiently large image entirely. To solve these issues, it is recommended that images are broken into a block of 16×16 pixels, generated through quantum circuits, encrypted or decrypted, then measured. The resulting blocks may then be reshaped into the original image size to complete the process.

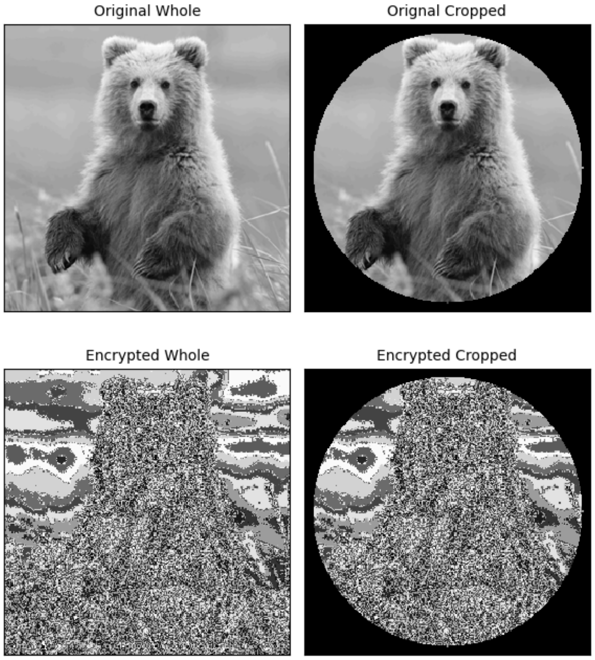

Fig. 4. An example image with the selective encryption algorithm with and without a cropping border applied.

IV. Simulation Results

Several aspects of this simulation were successful. Classical images of sizes up to 512×512 were used to generate a quantum circuit that could be extended with the encryption or decryption circuits as needed. 11 distinct 8-bit grayscale images were used, including a 16×16 bit colormap of all possible values. To replicate the empty space seen in medical images, solid black borders of variable shape and thickness were added over the perimeters of these images (marked as ”cropped”) to allow 21 different test images to evaluate the effectiveness of the encryption process.

According to Heidari et al. [1], the encryption key $|K\rangle$ is to have an arbitrary length m. However, it was observed that upon seven iterations of U_b (which occurs when $K_i = 0$), the transformations reproduce the original image entirely. In other words, $U_b^7 = I$. Seven iterations of U_a (when $K_i = 1$) produces the complement of the original image which is identical to applying a NOT gate to the target value qubit. Another seven iterations of U_a reproduces the original image entirely such that $U_a^1 4 = I$. Since an unconditional complement operation offers a minuscule improvement to security, every seven applications of U_a can be treated as a loop similar to seven applications of U_b. Therefore, $|K\rangle$ may be restricted to having an effective length interval of 1 to 12, with no more than 6 qubits assigned to 0 or 1 each. This produces 48 possible key combinations when excluding the original value, or 96 when including complements. Of all 96 key combinations, 6 produced a result that left the empty space unchanged. It is expected that one of these 6 was consistently used in the original experiment.

An analysis of adjacent pixel correlation coefficients as seen in Heidari et al. is replicated here [1]. This is used to evaluate the effectiveness of the encryption method: normal images generally have a high correlation between adjacent pixels, whereas encrypted images should ideally have a low correlation. The original paper reported coefficients for fully encrypted images to be lower than 2% in all examples, whereas the simulation varied between nearly 50% in the worst cases and 1% in the best cases. It should be noted that without any operations on the positional qubits, any image with a solid color section will have a higher limit on its potential minimum correlation coefficients. This includes the empty space seen in medical images and is representative of the reduced security of selective encryption.

Curiously, Heidari et al. suggest a higher entropy from using Shannon’s Entropy formula [1], where $p(n)$ is the probability of a particular color value across the entire image:

$$\text{Entropy} = -\sum_{n=0}^{255} p(n) \log_2 (p(n)) \tag{2}$$

However, this conflicts with results of the operations described previously since every transformation equates to a $1 : 1$ function for each individual color value. In other words, no two distinct input values will produce the same output, and the distribution of probabilities will remain unchanged. Predictably, the entropy analysis over every image produced the same result regardless of encryption.

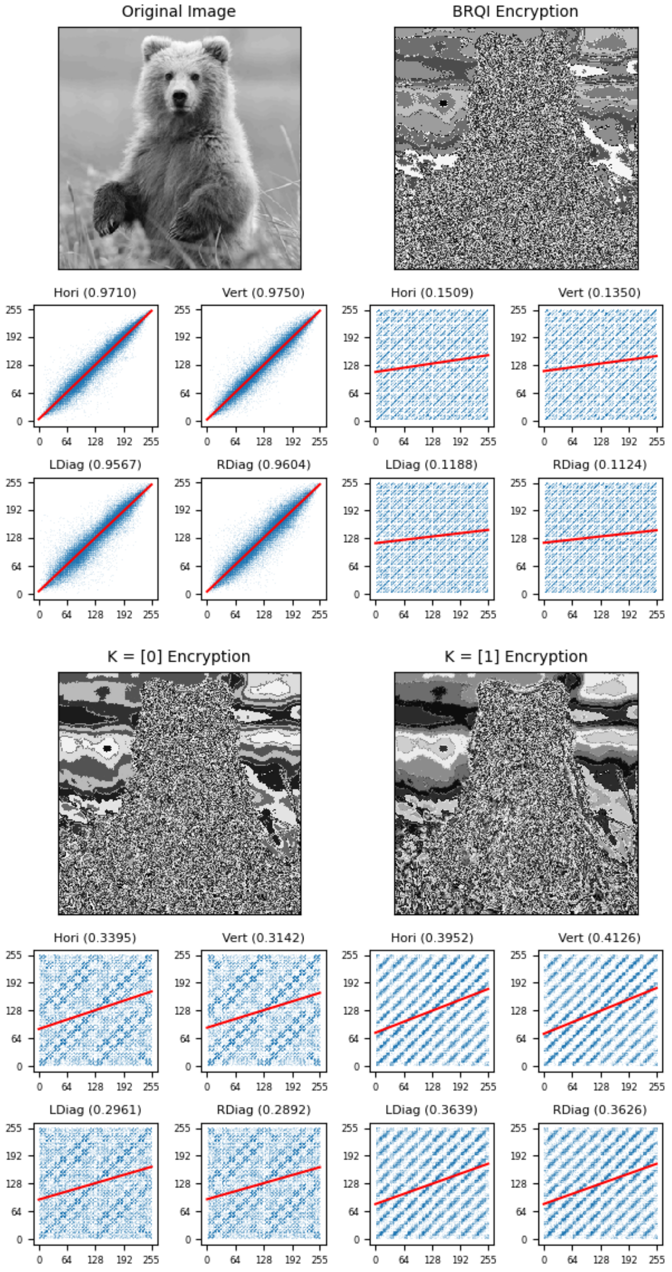

Fig. 5. A correlation coefficient analysis for an image with various full encryption methods applied. Note the solid color areas on the sides.

V. Conclusion

Medical images are well-suited to selective encryption methods to reduce encryption, decryption, and transmission time by taking advantage of empty space. Quantum computers allow for the implementation of selective encryption methods with a considerably smaller time complexity over classical computers. Simulations of quantum methods are possible on personal devices through platforms such as Qiskit and are capable of evaluating the effectiveness of theorized encryption methods. For selective encryption to avoid changing empty space, the algorithm should avoid or negate any complement operations through the proposed encryption circuit. Variable applications of encryption operations must also be carefully managed to avoid negation through repetition.

References

[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. [Online]. Available: https://doi.org/10.1007/s10773-019-04258-6.

[2] H. Li, X. Chen, H. Xia, Y. Liang, and Z. Zhou, "A quantum image representation based on bitplanes," *IEEE Access*, vol. 6, pp. 62 396–62 404, 2018. DOI: 10.1109/ACCESS.2018.2871691.

[3] D. Solenov, J. Brieler, and J. F. Scherrer, "The potential of quantum computing and machine learning to advance clinical research and change the practice of medicine," eng, *Missouri medicine*, vol. 115, no. 5, pp. 463–467, 2018, PMC6205278[pmcid], ISSN: 0026-6620. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/30385997.

[4] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6g wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, pp. 28–41, 2019. DOI: 10.1109/MVT.2019.2921208.

[5] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019, ISSN: 1476-4687. DOI: 10.1038/s41586-019-1666-5. [Online]. Available: https://doi.org/10.1038/s41586-019-1666-5.

[6] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Sep. 2017, ISSN: 1476-4687. DOI: 10.1038/nature23655. [Online]. Available: https://doi.org/10.1038/nature23655.

[7] S. Jain, "Quantum computer architectures: A survey," in *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2015, pp. 2165–2169.

[8] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 881–919, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8439931.

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th. USA: Cambridge University Press, 2011, ISBN: 1107002176.

[10] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional quantum teleportation," *Science*, vol. 282, no. 5389, pp. 706–709, 1998. [Online]. Available: https://science.sciencemag.org/content/282/5389/706.

[11] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[12] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2014.05.025. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0304397514004241.

[13] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, 26 Dec. 1998. DOI: 10.1103/PhysRevLett.81.5932. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.81.5932.

[14] A. R. Calderbank, E. M. Rains, P. M. Shor, and N. J. A. Sloane, "Quantum error correction via codes over gf(4)," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1369–1387, Jul. 1998, ISSN: 1557-9654. DOI: 10.1109/18.681315. [Online]. Available: https://arxiv.org/pdf/quant-ph/9608006.pdf.