**Data Reduction in Medical Images**

# Table of Content

[Table of Content 1](#_Toc112143029)

[ABSTRACT 4](#_Toc1058191520)

[CHAPTER 1 4](#_Toc1826417811)

[1.1 Introduction 4](#_Toc2123071213)

[1.2 Research Background 5](#_Toc2077613706)

[1.3 Research Question 5](#_Toc980754778)

[1.4 Aim 6](#_Toc1894941591)

[1.5 Motivation 6](#_Toc1333675287)

[1.6 Objectives 7](#_Toc1892988535)

[1.7 Deliverables 7](#_Toc700417484)

[1.8 Scope and Limitations 8](#_Toc835089579)

[CHAPTER 2 8](#_Toc919295602)

[2.1 Introduction 8](#_Toc1350127983)

[2.2 Related Work Review 9](#_Toc1763004578)

[2.3 Future plan 19](#_Toc185297521)

[2.4 Analysis of the Problem and Improvement 20](#_Toc946331016)

[CHAPTER 3 22](#_Toc1501409354)

[3. 1 Introduction 22](#_Toc1269250306)

[3. 2 Model 22](#_Toc51071393)

[3. 3 Requirement Specification 26](#_Toc978579372)

[3. 3. 1 Software Specification 26](#_Toc1325120829)

[Quantum Random Number Generator (QRNG) 26](#_Toc1139685029)

[Cryptographic Libraries and Toolkits: 26](#_Toc1806205408)

[Medical Imaging Software: 27](#_Toc2063926571)

[Development Environment: 27](#_Toc165717607)

[3. 3. 2 Hardware Specification 27](#_Toc1424831040)

[High-Performance Computers 27](#_Toc48248238)

[Quantum Computing Platform 27](#_Toc2123930952)

[Secure Storage Solutions 28](#_Toc752987699)

[3. 4 Justification for the chosen tools 28](#_Toc121780992)

[Quantum Random Number Generator (QRNG) 28](#_Toc2101578893)

[Cryptographic Libraries and Toolkits 28](#_Toc825471659)

[Medical Imaging Software 29](#_Toc1638014216)

[High-Performance Computers: 29](#_Toc1854098034)

[Quantum Computing Platform 29](#_Toc833189442)

[Secure Storage Solutions: 29](#_Toc1230998906)

[CHAPTER 4 29](#_Toc488172468)

[4.1 Introduction 30](#_Toc715906262)

[4. 2 Design 30](#_Toc85478417)

[4. 2. 1 Dataset 30](#_Toc1648797658)

[4. 2. 2 Data Preprocessing 30](#_Toc687412148)

[4. 2. 3 Modelling Selection 31](#_Toc1405240142)

[4. 2. 4 Model Development and Evaluation 32](#_Toc896756638)

[4. 3 Implementation 32](#_Toc1535654516)

[4. 3. 1 Importing Libraries 32](#_Toc667153862)

[4. 3. 2 Exploratory Data Analysis and Data Cleaning 33](#_Toc1191987524)

[4. 3. 3 Creating Interaction Features 33](#_Toc1645348493)

[4. 3. 4 Data Visualization 33](#_Toc2015113118)

[4. 3. 5 Part Construction and Assessment of Models 34](#_Toc396348064)

[4. 4 Evaluation 35](#_Toc60177565)

[4. 4. 1 Limitations 35](#_Toc598727310)

[4.6 Validation 36](#_Toc963137838)

[4.7 Testing 36](#_Toc340487812)

[4.8 Critical Evaluation 37](#_Toc1671351274)

[4.9 Results of the Testing 40](#_Toc949139866)

[4.10 KEY GENERATION 41](#_Toc49311140)

[4.11 Complication of iteration in Conventional and Quantum Enhanced Encryption Systems. 41](#_Toc1861205138)

[CHAPTER 5 43](#_Toc1681299865)

[5. 1 Conclusion 43](#_Toc528115994)

[5. 2 Future Work 44](#_Toc1415363950)

[5. 2. 1 Enhanced Model Training 45](#_Toc1559254217)

[5. 2. 2 User Feedback Integration 45](#_Toc1350113301)

[5. 2. 3 Scalability and Integration 45](#_Toc555658938)

[5. 3 Ethical Considerations 45](#_Toc1844197572)

[5. 4 Implementation Challenges 45](#_Toc1926928262)

[5. 5 Future Research Directions 46](#_Toc2038012909)

[References 46](#_Toc674592860)

[Appendix 48](#_Toc1715465986)

List of Figures

Figure 1--------------------------------------------------------------------------------------------22

Figure 2 -------------------------------------------------------------------------------------------- 26

Figure 3 -------------------------------------------------------------------------------------------- 31

Figure 4 -------------------------------------------------------------------------------------------- 38

Figure 5 -------------------------------------------------------------------------------------------- 39

Figure 6 -------------------------------------------------------------------------------------------- 45

Figure 7-------------------------------------------------------------------------------------------- 47

Figure 8 -------------------------------------------------------------------------------------------- 47

Figure 9 -------------------------------------------------------------------------------------------- 49

# ABSTRACT

The research is based on increasing the encryption of the Region of Interest (ROI) in the medical images based on the quantum phenomena QRNG and quantum errors. Such encryption techniques as AES and RSA used in full-image encryption guarantee high security but they consume a lot of computing resources and may lead to performance degradation in real time applications such as in medical field. While the project will encrypt only diagnostically relevant ROI, the goal is to minimize the computational overheads while having strong security mechanisms. QRNG, in confront of such principles like superposition and entanglement, makes the randomness of the key created for cryptographic purposes more shock resistant. Further, quantum generated S-box and P-box along with quantum error effect improves non-linearity and diffusion characteristics of the cipher making it highly less vulnerable to cryptographic attacks. The rationale for this research lies in the growing concern on optimizing privacy and security concerns for patients’ information, especially where DICOM imaging is being used in the medical field. Due to the fact that medical images are used in diagnosing a patient as well as determining the exact treatment to offer, medical images containing diagnostic ROI are more important The project assesses the possibility of adopting QRNG-enhanced encryption for medical images, with special regard to the security and performance trade off; the final suggested solution has both a high security requirement for medical data and sufficiently high efficiency for real time applications in the clinical environment.

# CHAPTER 1

## 1.1 Introduction

Digital imaging in medicine has become popular in the diagnosis and planning of treatment procedures. The security of such medical images especially those in DICOM format is very sensitive because of the information contained in the images. As for these images, traditional approaches of encryption would result in a compromise between security and computational complexity. This particular project is to explore the possibility of using quantum phenomena to create a secure but high-speed encryption method which focuses on the Region of Interest (ROI) in the images of medical related analysis.

Protection of medical images has turned out to be very crucial in the world today, especially the health sector as it deploys the use of electronic means in storing and transferring data. By the use of diagnostic methods such as X-Ray, MRI, CT scans, and ultrasound health care givers diagnose and manage different ailments related to the human body. However, since these images have to portray the patient of concern, proper measures of handling the data have to be put in place to respect patient’s rights to privacy. Encryption technologies are very important in countering these security threats in a bid to protect this data (Abood & Guirguis, 2019).

Conventional cryptographic techniques, including DES and AES, have been applied to the security of medical data by seeking to encrypt the whole image and thus making the data inaccessible during storage or transmission to unauthorized parties. These methods are however time-consuming and require high computational power especially when dealing with large images and thus may act as a bottleneck in clinical processes and delays the delivery of medical images for diagnosis and treatment (Abood & Guirguis, 2019). In order to overcome these problems, several selective encryption techniques have been proposed which targets on encrypting only the Region of Interest (ROI) of the medical image. This approach is more efficient because it eliminated all the information that does not need further analysis and at the same time preserves the most important parts of the image (Wang & Zhang, 2020).

## 1.2 Research Background

Diagnostic imaging means are necessary for the identification of many diseases. These images are often associated with the patient’s information; the DICOM standard is employed for storing and transferring such images. Current solutions for image encryption are approved by AES and RSA encryption algorithms, but their application can be time-consuming and problematic when clinicians are in urgent need of a patient’s images (Abood & Guirguis, 2023; Chen & Kuo, 2023). To overcome these limitations, a number of methods of selective encrypted have emerged that aim to encrypt solely the ROI part, which seems to be rich in diagnostic information (Ayyappan & Joseph, 2018).

Nevertheless, today’s selective encryption techniques are based on traditional cryptographic science, the most optimal security of which cannot be guaranteed. Superposition and entanglement of quantum circuits, along with QRNG, have suggested a new method of boosting cryptographic security. It can generate actual random numbers which are required for creating secure cryptographic keys and further structures like S-boxes and P-boxes which define non-linearity and diffusion within the encrypting algorithms (Li et al., 2019).

## 1.3 Research Question

To what extent can the Region of Interest (ROI) in medical images be encrypted more efficiently and securely using the granted quantum-enhanced cryptographic technologies such as quantum random numbers generation and quantum error phenomena in comparison with the conventional encryption?

## 1.4 Aim

To increase the security of the ROI in medical images by proposing an encryption approach that uses quantum random numbers and the effects of quantum errors and to accomplish this within a reasonable amount of computation time.

## 1.5 Motivation

The rationale for this research lies in the growing concern on optimizing privacy and security concerns for patients’ information, especially where DICOM imaging is being used in the medical field. Due to the fact that medical images are used in diagnosing a patient as well as determining the exact treatment to offer, medical images containing diagnostic ROI are more important. However, thanks to modern technology advancement in the healthcare sector, the safety of patient data becomes very essential.

Using this traditional encryption approach ensures that even if message interception occurs the message cannot be understood fully due to the excessive encryption but this comes at the cost of inordinate computational overhead and processing delays when applied to large high-resolution images. These delays can prove disastrous in a health care setting were bringing patients data timely is of utmost importance. To overcome the mentioned problem, my investigation considers two other quantum phenomena – QRNG and quantum error integration – that can be used to create more reliable and efficient encryption system adapted to the ROI with medical images.

With the help of the proposed encryption scheme based on quantum enhancement, I expect not only to enhance the medical image security but also to minimize computational complexity, so as to provide near-real-time solutions for the healthcare industry. This project falls under the general area of my academic and professional concern: cryptography, quantum computing, their implications to medical technology among other fields.

## 1.6 Objectives

* Introduce a concept for a specific kind of QRNG, which is famous for its ability to generate purely random numbers.
* Derive and classify the quantum-generated S-boxes and P-boxes confined to the quantum error incidence.
* Propose an encryption mechanism of ROI in medical images using QRNG, S-boxes and P-boxes.
* Carry out analysis to assess the feasibility of the proposed system as well as checking it against previous methods.

## 1.7 Deliverables

* There should be an improvement of the algorithm for encryption and processing on the real time retaining the efficiency and not a burden to the device.
* The literature review on the most recent advancement in the information hiding techniques used in medical image encryption.
* Functional QRNG implementation.
* S-boxes and P-boxes created through the use of quantum error occurrences.
* The actual mathematical algorithm for encoding the ROI in medical images will also be described in pseudo code as a standard encryption algorithm.
* The assessment program presenting the differences between the described system and traditional ones.
* Orders that demand strictly improved encryption methods are prepared for inclusion into diagnostic imaging methods if necessary.

## 1.8 Scope and Limitations

The objectives of this project are to design a quantum-enhanced encryption strategy utilizing medical images with ROI interest and compare its efficiency to prior strategies. The issues include the level of availability of quantum computing, difficulties in incorporating quantum phenomena in cryptographic structures, and the challenge of synchronizing the seconds needed for computations.

# CHAPTER 2

## 2.1 Introduction

Protection of medical images has turned out to be very crucial in the world today, especially the health sector as it deploys the use of electronic means in storing and transferring data. By the use of diagnostic methods such as X-Ray, MRI, CT scans, and ultrasound health care givers diagnose and manage different ailments related to the human body. However, since these images have to portray the patient of concern, proper measures of handling the data have to be put in place to respect patient’s rights to privacy. Encryption technologies are very important in countering these security threats in a bid to protect this data (Abood & Guirguis, 2019).

Conventional cryptographic techniques, including DES and AES, have been applied to the security of medical data by seeking to encrypt the whole image and thus making the data inaccessible during storage or transmission to unauthorized parties. These methods are however time-consuming and require high computational power especially when dealing with large images and thus may act as a bottleneck in clinical processes and delays the delivery of medical images for diagnosis and treatment (Abood & Guirguis, 2019). In order to overcome these problems, several selective encryption techniques have been proposed which targets on encrypting only the Region of Interest (ROI) of the medical image. This approach is more efficient because it eliminated all the information that does not need further analysis and at the same time preserves the most important parts of the image (Wang & Zhang, 2020).

As of recent time, the possibilities of quantum computationally as a means to boost encryption techniques has also been looked into. Applying principles like superposition and entanglement make use of QRNGs to generate random numbers that are random, and more secure than the traditional means of generating random numbers (Yang et al., 2019). The inclusion of quantum characteristics in the advanced cryptography has a great impact in enhancing security and reliability of medical image cryptosystems (Kumar & Verma, n. d.).

Cross-comparison on the performance and security of the explored medical image encryption techniques may present some compromises especially in terms of time factors and complexity. For instance, although comparing to AES, the chaotic system-based encryption methods are more secure than they are less efficient in terms of the computational process (Huang & Nien, 2023). Hence there is need for vocabularies that are used to choose the right medical imaging encryptions to be sensitive to the so that they can balance between security and the time that is taken in the process.

In addition to these challenges, the ethical and practical consideration for the integration of encryption technologies in medical image are very important. People’s identity has to be protected as well as their information and this is why the encryption methods should be found to resolve these issues while not affecting the clinical practice. While quantum computing and other new-age technologies for encryption can be beneficial in terms of strengthening existing encryption solutions, bringing these technologies in clinical practice causes concerns with patient-clinician dynamics and the question of informed consent. There is need to explain to the patient on the advantages and some of the challenges that may be faced when implementing more secure encryption procedures (Chen & Kuo, 2023).

## 2.2 Related Work Review

Encryption of medical images is an important research problem because medical images may contain the sensitive information about patient details. Data security is of particular significance in the case of medical images to avoid situations where the images can be seen and accessed by unauthorized persons or accessed by other patients. Typically, methods of protecting medical images employ procedures that encrypt the entire picture employing algorithms that protect the information contained in it.

The initial attempt at medical image encryption involved the use of the standard cryptographic algorithms such as DES and the AES. DES, which was developed in the 1970/1980s and AES which was adopted in the late 199/2000s have been instrumental in enforcing security on sensitive data in numerous applications right from medical imaging (Wang & Zhang, 2020).

These encryption methods are famous for their efficiency in data security but are also well known for their extensive processing requirements particularly when dealing with full-sized medical images. This is due to the call for processing big data and using complex flattened algorithms for the security of messages which requires intense computation (Yang, Li, & Zhou, 2023).

The studies have revealed that although DES and AES offer robust security solutions, they slow down and become a performance issue when implemented in the health facilities that require fast access to imaging data for appropriate diagnosis and management of the patient’s conditions (Ayyappan & Joseph, 2018). There is tradeoff between security and the computational power: something that sheds light on the objective need to improve and deploy encryption technologies which are relevant to the needs of imaging medical data.

The study done in the recent past in the field of medical image encryption has looked into option encryption where, only the Region of Interest (ROI) of the medical image has to be encrypted. The ROI generally consists of information that is relevant to diagnostics, and encrypting this area only can significantly decrease the number of computations necessary while keeping the data as secure as possible (Li et al., 2019; Liu et al., 2014).

Selective encryption schemes work with the aim to give maximum security with optimized performance by encrypting only that part of the image data that needs to be secured. This also essentially maximize computational resources and also answers issues on data processing and transmitting especially in the medical field (Huang & Nien, 2023).

However, the recent technology of quantum computing brings in new ways and methods in improving the medical image encryption. Quantum random number generators (QRNGs) and quantum error corrections are viewed as the general possibilities to provide highly secure cryptographic key generation and enhance more potent encryption formulas’ robustness against invasions (Kumar & Verma, n. d.).

Post quantum encryption methods employ features of quantum mechanics like superposition, entanglement for generation of random numbers which cannot be predicted. Such number’s generation occur through the use of quantum computer and they are very vital in developing techniques used in encryption of keys as well as making them impregnable by existing techniques of decryption as pointed out by Zhu et al., (2017).

In summary, although the initial methods including but not limited to DES and AES have provided the fundamental basis for medical image encryption, current study and development aims at improving encryption methods to correspond to the two-sided requirement of security and computational complexity in the medical field. Selective encryption strategies with the help of enhancements in quantum technology present best prospects to strengthen the safety of health care data and at the same time not to complicate the management and retrieval of the data.

Due to the computational complexities involved with the full-image encryption in the medical imaging, the selective encryption methods have come out as the feasible solutions. The selective encryption methods are different from the traditional methods as the latter encrypts the entire images, but the present method is geared towards the Region of Interest (ROI) encryption only. The ROI usually includes important diagnostic data, so it is essential to store it while avoiding using the extra computational power effectively.

Selective encryption is to achieve the nature of optimizing data security and the efficiency of computation by encrypting only the valuable parts of the medical image data. This approach helps to improve the performance and at the same time the amount of work during the processing of large amounts of data is minimized (Ayyappan & Joseph, 2018).

The first types of selective encryption were based on block-orientated encryption methods. Such algorithms segment the image into blocks and then only encrypt those blocks which consist of the region of interest. Thus, encryption is applied only to specific areas, and this range of goals requires optimal computational power, while ensuring the data’s security (Wang & Zhang, 2020).

It has been postulated from the available studies that block based selective encryption techniques are capable of reducing the problem of computational overload associated with full image encryption schemes. These methods keep information that should not be disclosed within the region of interest safe while effectively passing and storing information in medical service setups (Li et al., 2019; Liu et al., 2014).

Moreover, there has been a development of selective encryption with considering the deterministic encryption methods according to the characteristics of medical images. Dynamic strategies enable encryption parameters to change depending on the image content and or security needed, which would improve efficiency and also improve the security of the data (Huang & Nien, 2023).

Selective encryption techniques also go beyond the block-based techniques to even include other methods such as perceptual encryption methods. Perceptual encryption algorithms depend on a model which mimics the human perception of Vim, in order to selectively encrypt regions that seem important within the Vim of the obtained image. This makes sure that the encrypted image can once more be used for diagnostic purposes and protect sensitive data simultaneously (Zhu et al., 2017).

Furthermore, the enhancement of selective encryption with other operations is also used to combine features of data security with that of data storage using the principles of compression. Compression enhanced selective encryption techniques minimize the amount of redundancy in the data before encrypting, the disk space and computational power hence being optimized (Chen & Kuo, 2023).

Overall, selective encryption techniques help in making a great progress in solving the problems of computational and security in context to medical image encryption. Therefore, in addition to promoting the data encryption, ROI as an object of focus for encryption also helps to improve the data management and transmission in clinical environments using adaptive and perceptual approaches

Now with the innovation of quantum computing, came the future for encrypting medical images, with principles that the conventional cryptographic practices do not allow. One among the most used fields of quantum telecommunications is quantum cryptography, which relies on quantum mechanics principles such as superposition as well as entanglement for the creation of real random numbers that are useful in key creation in cryptography. This section discusses the progression made in the field quantum cryptography and the integration of quantum solutions that improves the security of medical image encryption.

Quantum cryptography is based on principles of quantum mechanics and develops encryption techniques that cannot, by their fundamental principles, be intercepted. The fundamental idea of quantum cryptography is based on the so-called quantum random number generators. Mathematically completely random numbers can be generated using the effect of quantum mechanics and these processes are called as QRNGs. This higher degree of randomness is important especially in sound cryptographic key generation because the keys which are generated should be highly non- predictable and inaccessible to any form of attacks (Li, Lin, & Liu, 2019).

With regard to QRNGs, they also have a noteworthy capability of utilizing the relatively random quantum operations. For example, QRNGs provide a way of using quantum states of particles for example, photons to develop random numbers. The principle of superposition where particles are in two or more states at the same time and the principle of entanglement where particles can instantly affect each other no matter the distance helps to guarantee randomness of the generated numbers to avoid definite traits that can be manipulated by attackers (Scarani et al., 2009).

In the view of medical imaging application, use of QRNGs provides sound method to address this problem safely patient’s data. Images created during the treatment process can be stored in the Digital Imaging and Communications in Medicine (DICOM) format, in which case, the files contain important information that cannot be publicly accessed. Other traditional encryption techniques though used are proven to be less effective due to the growing computational size of the modern high-resolution medical images. Real time application, such as medical imagines benefit from QRNGs because it makes it possible to improve an encryption scheme without causing much of a computational burden (Lo et al., 2014).

In addition, quantum cryptography also brings quantum key distribution (QKD), which is a method to create key for secure communication by using a theory of quantum mechanics. QKD is the technique of sharing the keys of encrypting messages in a manner that any interferes will be easily noticed. This is possible by the usage of quantum mechanics in which an attempt to measure a system disrupts and thus takes a picture revealing the intruder. Among numerous proposed QKD protocols, the most developed one is the BB84 protocol that has been tested on the real-life examples and that supplies secure key distribution (Bennett & Brassard, 1984).

The secure use of QKD in medical image encryption increases its security by assuring that key distribution for use in encryption is Key Distribution Center and that they are frequently changed. Thus, the dynamic handling of the keys reduces the menace posed by static keys, which are often at risk. Through the regenerative use of encryption keys with QKD, the medical imaging system can be preserved with a high degree of security against these threats (Diamanti et al., 2016).

Research has also been carried on integrating quantum cryptography with AI and classical cryptographic algorithms to form hybrids of the two that will benefit from the techniques of the two methods. For instance, using of QRNGs in conjunction with Advanced Encryption Standard (AES) can increase the security provided by AES because keys used in the cipher are confirmed to be genuinely random (Chen et al., 2021).

Modern developments in modern technology have seen an effort being made in the attempt to incorporate quantum effects in the regular encryption methodologies for better security and reliability. These methods exploit quantum characteristics to improve the standards of an encryption technique-quantum key distribution, in relation to the existing threats posed by the increased computational power to traditional cryptographic procedures.

An advancement in quantum-enhanced encryption paradigms is the employ of QRNGs to develop building blocks of the encryption functions S-boxes and P-boxes. Both S-boxes and P-boxes are very important components in many of the symmetric key ciphers such as the AES which is currently in use. They are used to make the encryption process complex and non-linear for the attacker, if he or she is to try and attempt to decode any given data encrypted with a key.

QRNGs use the random behavior of the quantum systems to produce actual random numbers. Primarily, QRNG operates as an antithesis to the classical random number generator which use deterministic algorithms to create pseudo-random numbers as opposed to QRNG that derive numbers from the quantitively characteristics of photon emission, or the state of particles. This increases the randomness by a higher degree which in turn strengthens the cryptographic keys and structures against the invaders of cryptographical attacks (Rarity et al., 1994).

The inclusion of QRNGs in the creation of S-boxes and P-boxes provide higher non-linearity and diffusion of the encryption's structures. Scenario non-symmetry is important in encryption since small changes to the plaintext should produce large and unpredictable changes to the cipher. High non-linearity in S-boxes makes it difficult for the attackers to look for any given relation or pattern that might be vital in their endeavor to break the encryption. He has visualized to transform this universal process into a profitable business opportunity as mentioned by Kumar and Verma (n. d.).

Modern research shows that quantum-based encryption protocols can increase the effectiveness of ordinary cryptographic systems. For example, scientists have integrated QRNG-based S-boxes into AES and found out that these quantum-generated structures contribute to the increase of the stuffer’s resistance to differential and linear cryptanalysis. This approach helps secure more security while at the same time keep the operational efficiency needed for the real time encryption and decryption (Xu et al., 2017).

Another research hotspot is based on the use of QKD integration with classical encryption technologies. QKD holds features based on quantum mechanics to transmit the encryption keys between two parties such that any attempt to intercept the keys will be distinguished. This is because through combining of QKD with quantum-enhance encryption algorithms one is able to develop a system that is difficult to penetrate when protecting important data. This kind of joint approach makes sense especially in applications that require data confidentiality and data integrity for example Medical Image Encryption as pointed out by Pirandola et al, 2020.

Moreover, it is essential to note that some of the drawbacks of present encryption schemes, for example, their dependence on improvement in computing technologies, including quantum computers, can be solved with the help of quantum improved encryption techniques. Essentially, quantum computers can crack the mathematical challenges that form the basis of most of the conventional cryptographic algorithms. To prevent a security threat of quantum computers, it is possible to use the general principles of quantum phenomena in the construction of cryptographic methods that can withstand them in the future (Bennett & Brassard, 1984).

The efficiency of Medical Image Encryption has been given a large amount of research interest so as to measure the performance and Security of the different encryption methods. These comparative studies are fundamental in comprehending the differences in efficiency of the algorithms as well as their reliability in offering secure image processing on time as in the case of the medical imaging application. This section goes over several specific works that compare various approaches to encryption, which helps to illuminate the relative advantages and disadvantages of each.

The following study by Huang and Nien which was conducted in 2023 can be considered as one of the most significant research projects in the field Choose a year According to the results of the research described in the article of Huang and Nien (2023) it is possible to compare chaotic-based encryption systems and AES-based encryption methods. It also reported that in compare to AES, security of chaotic systems which use the irregularity of chaotic maps for encoding is usually taller. By their nature, chaotic systems resist the type of analysis that forms the basis of linear and differential attacks, meaning that secure communications based on chaotic systems can be considered highly secure. However, this increased security comes at a cost: generally, chaotic systems are more complex and therefore more resource and time consuming than the AES algorithms. This trade-off is critical in medical imaging for high-resolution images because the time it takes to perform the calculations is prohibitive to real-time use.

Another useful comparative study was conducted by Liu et al. (2020) where the authors compared selective encryption with full-image encryption techniques. It was established that selective encryption, which encrypts the ROI of an image, reduces drastically the amount of data that have to be processed. This method optimizes the speed of computation by preserving the maximum security of the most significant parts of the image. Thus, the given research proved that selective encryption is most effective to be applied in case of medical imaging where some areas of the picture contain the essential data, like numbers or some additional zones with coordinates, names, etc. However, the main difficulty arises in detecting and segmenting the ROI without restricting the general view of the image with such parameters as storage, permission, and more.

Comparative analysis of the integration of quantum enhanced approach to classical cryptography has also been done. For instance, Kumar et al (2022) presented an assessment of Quantum Random Number Generators (QRNGs) in the generation of S-boxes and P-boxes for the encryption/decryption of messages. In both their studies, they showed that utilizes of quantum in the encryptions introduce greater non-linearity as well as diffusion characteristics hence safer against cryptographic invasions. Moreover, these methods contain the promise to make the encryption future-proof in the face of quantum computational threats. However, the utilization of quantum-upgraded procedures entails different equipment and touch with quantum physics that might be a hindrance when adopted.

The work presented by Zhang and Gao (2021) deals with the analysis of hyperchaotic sequence performances on the encryption of images and its security level. Hyperchaotic systems or systems that have more than one chaotic map give a higher security than the normal chaotic systems. The authors also concluded that if hyperchaotic sequences are utilized, the encryption algorithms’ immunity to different types of attacks is greatly improved. However, the higher level of detail does also bring a higher computational and memory cost, potentially making them a problem in a device with limited resources, such as a mobile medical imaging device.

Wang and Zhang (2020) also applied another comparative research exploring block-based and stream-based encryption approaches of medical images. Block based technique like AES descends the image into fixed or specific size blocks and encrypts each block routinely. This is a very efficient method of solving a problem and well suited to parallel processing, therefore well suited to high-speed applications. Nonetheless, the block-based methods are seen to possess a weakness at the block boundary with reference to security. On the other hand, the stream-based methods, as the name suggests encrypts the image data on a continuous basis thereby providing more security but with the disadvantage that is processed at a slower rate. The survey therefore advised that depending on the given requirements of the medical imaging application, the right encryption method should be adopted.

In another study for comparison, Ayyappan and Joseph (2018) surveyed multiple methods of hybrid encryption schemes where multiple encryption types are a part of a single cipher, to provide security as well as computational efficiency. Such hybrid techniques include use of conventional opaque algorithms together with other new and sophisticated means such as the use of chaotic maps or quantum-based methods, among others. In their study, the researchers opined that developing and implementing the hybrid technique is not only possible but could offer the best of both worlds in that the most efficient and effective technique from each component method can be achieved while at the same time, minimizing on their ineffectiveness. Nevertheless, there are certain issues concerning the implementation and management of the hybrid systems that could be regarded as critical issues, namely, the fact that the overall complexity of the hybrid power management systems tends to be higher in comparison with the SESs designed for clinical environments where simplicity of power supply management remains one of the crucial priorities.

Conclusively, comparative studies on the medical image encryption highlight the need for context-based solutions. Despite a high level of security, provided by the chaotic systems and quantum-enhanced methods, the applicant has noticed that they are rather computationally intensive and may not operate in real time. Selective encryption is more favorable than the other methods because it provides a fair balance between software security and usability but only if the areas to be encrypted are accurately identified. Simultaneous methods claim to offer the strengths of different strategies, but their implementation has adverse effects. Essentially, these insights are meaningful for the creation of the encryption strategies that should contribute to the protection of the medical images and at the same time correspond to the performance requirements of the state-of-the-art healthcare systems and environments.

However, we found that ethical and practical factors are also critical in entailing the encryption technologies in medical imaging. Strict privacy of patients and accuracy of data is crucial as they contain vital information from patients’ scans. Security requirements must be satisfied while selecting encryption algorithms to be utilized in medical IT environments, while at the same time displaying efficient performance and not intervening with practice activities. The opportunity to use quantum-enhanced encryption methods in using encryption opens new ethical questions that are worth considering.

Privacy is always a key issue for patients while undergoing a medical imaging technique. Data security requires data encryption: limitations applied to patients’ information mean that only authorized personnel should access the information. The data acquired through medical means is as sensitive and should not be altered as the flaw may lead to misdiagnosis or wrong treatment. Hence, it is necessary to have cryptographic algorithms capable of protecting the information from tampering, and it must remain in its original form during storage and transfer.

Other methods like DES and AES have also been commonly employed in medical image protection. Nonetheless, they can be time-consuming especially when one is working with large images high resolution images (Abood & Guirguis, 2019). This can add delays to structures in clinical practice especially where rapid access to these images is necessary. Post-quantum cryptographic methods such as quantum key distribution that is based on the principles of quantum mechanics to derive the correct and unguessable cryptographic key will offer increased security at a relatively lower computational cost.

There is the issue of security vs performance, the drawback of which is that the added security often negatively impacts the performance of the program or networking system. Encryption algorithms have to be strong enough to safeguard the patient’s data from modern day cyber threats but at the same time be fast enough for medical images to be accessed and processed in real time. This is especially so in emergency care situations that would be severely compromised if access to a patient’s medical image was to be delayed.

There are methods linked with the using of Quantum Random Number Generators (QRNGs) which practically provides higher randomness and security without the same computation level as with traditional methods (Li, Lin, & Liu, 2019). However, these technologies are still considered as experimental and their use in clinical practice should be thoroughly investigated.

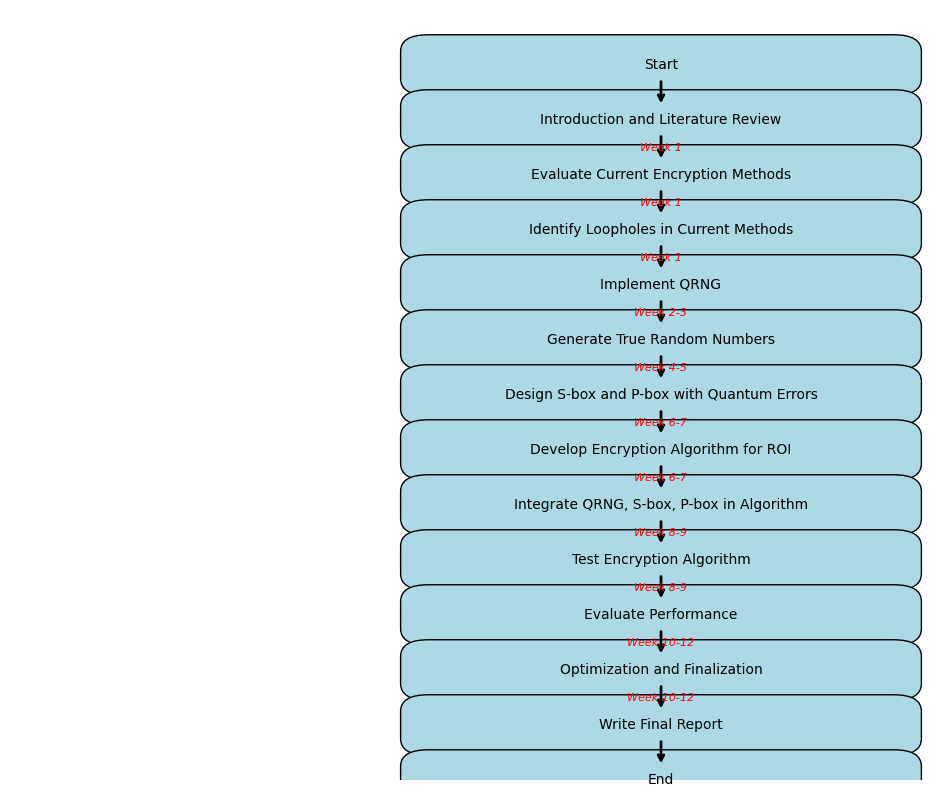
An enhancement of one such technology in clinical contexts has to include into account the changes in the flow of works. The practitioners in the medical field have tight schedules and anything that would require them to go through an extra process of encrypting and decrypting the images needs to be optimized to avoid any hindrance to their working schedule. Cryptography techniques based on quantum must be easily implemented in clinical systems without introducing complications or latency.

From a more practical angle we see that the interfaces ought to be friendly and the processes involved least demanding on the providers of healthcare services. For example, the integration of the encryption module might be such that the encryption and decryption processes can be done in the medical imaging software environment where users can only key in their details without having much control over the encryption and decryption. However, training and support should also be conducted in order to let medical staffs feel favorable about the new technology.

Another issue to contend with is the incorporation of higher levels of encryption in medical imaging, whereby use of such technologies A main ethical concern is the patient’s informed consent. Again, patients have the privileges to be informed of how their data are protected and with an option of offering their consent in case of profiting a certain type of encryption technology, which in some way is invasive when it comes to patient’s individual rights and medical information. The possibility of applying quantum enhanced encryption algorithms for storing and transferring patient’s records requires clear explanation of the advantages and disadvantages to the patients.

Moreover, there is a need to set up policies and regulations concerning the application of cryptographic tools in healthcare. This pertains to the regulation on who owns the data, who can use the data, and when and how data can be shared and accessed, plus mechanisms to address data losses and lawsuits on the data. The considered ethical issues also include equity and fairness related to the application of the new quantum-enhanced encryption methods to protect the information, which are the same across the different individuals and particularly important when it comes to patients’ medical data.

Some important and unavoidable matters concerning the use of encryption technologies in medical imaging are the ethical issues and the practical ones. Preserving patients’ right to privacy and confidentiality of their records as well as optimizing security without compromising scan rate, which can disrupt clinical processes, and considering the rights and duties of patients, such as whether they have to consent to quantum-protected encryption, are also idealistic goals of a system. More so, this means that there will always be need for continued social engagement between technologists, the health care professionals and the policy makers in order to meet these obstacles and enhance the positive uses of the advanced encryption (Chen & Kuo, 2023).



## 2.3 Future plan

The quantum-enhanced encryption system that will be developed will also go through its performance benchmark to check on the efficiency as compared to other current encryption techniques. This phase is very important because it determines the effectiveness of the system in addressing real life problems. Testing for performance will be done by looking into various aspects, which include; safety of the system, speed, and computational ability. Safety evaluations will involve the comparison of the system’s resistance to potential threats to other encryption products offered in the market. Performance assessments will also cover speed, which will determine the amount of time the system takes in both encrypting and decrypting the medical images to suit real life application. Performance evaluations will define the load handled by the units and subsystems, having a positive effect on productivity.

After performance evaluation, activities of the project will include preparing and issuing the study findings. The outcomes will be disseminated to the research fraternity through peer reviewed journals where the results will form part and parcel of the field of medical image encryption and quantum cryptography. A comprehensive research paper will be created to describe the system’s methodologies, results, and implications to enhance academic discussion and constructive criticism. Furthermore, it will disseminate the research outcomes to the professionals and researchers involved in the respective field through conferences and other related platforms to market the improvement of the existing system and extend the opportunities for future developments.

Thus, the overall objective of this project is to contribute to the existing literature on medical image encryption and improve the security of patient images through utilization of quantum security technologies. To ensure that the project eliminates the encryption issues and provide a better solution to the existing MDCT researchers and clinicians, it would a junior-senior project that is of great benefit to another researcher in the medical field. Thus, supplying accurate and intense scrutiny, which will in turn be distributed, the project will greatly benefit the progressing field of quantum-secured cryptography and medical image security.

## 2.4 Analysis of the Problem and Improvement

The main drawback of the existing methodologies for medical image encryption is the fact that security is often directly proportional to performance. The techniques may include the full-image encryption utilizing common algorithms for instance AES and these RSA among others which makes sure that the sensitive data cannot be accessed by any unauthorized persons. However, the disadvantage of these two methods is that it takes a lot of computations from the system. This issue gets worse when working with large-sized DICOM images which are prevalent in medical care facilities. Introducing such encryption techniques have large computational overhead; hence, there will be long processing times and such a delay can be catastrophic in an environment such as hospitals where the quick dissemination of diagnostic information is critical. High computational loads result in timing delays in a critical medical environment; therefore, this becomes a disadvantage.

Moreover, these traditional cryptographic algorithms are most ineffective when it comes to selective encryption, a technique that is steadily gaining popularity because of its effectiveness and selective applicability in a number of fields. Selective encryption is very useful in medical imaging where sometimes only a particular area of the image which may be the area of interest or region of interest needs to be encrypted and not the whole image. Such methods of encryption do not selectively encrypt the relevant parts of the image, but encrypts the entire image including the irrelevant portions which actually increases the problem of performance since extra computational power and time are dedicated to encrypting parts of the image that are not even important. The limitations of the above proposed enhancement in this project are as follows: Those weakness are removed by using quantum technologies in medical image encryption and decryption with better security and performance. In particular, the given project incorporates Quantum Random Number Generation (QRNG) with the use of quantum error features, more specifically, the bit-flip error that results from quantum entanglement. These quantum principles are utilized to develop a new encryption scheme essentially using quantum generated S-box and P-box that are very crucial in cryptography.

The QRNG brings in true randomness which is a bonus over other random number generators that rely on some deterministic methods. This type of randomness is inherent for a true quantum system making the randomness component of the encryption scheme much higher, which in return makes easier for attackers to decipher the encrypted data. Moreover, new aspects such as quantum error phenomena are introduced which augment the security structure by mimicking the stochasticity and non-linearity of quantum world. Such characteristics enable avoiding deterministic attacks aimed at the predictability in the encryption functions.

From the performance point of view, it reduces the computational complexity by considering the encryption only on the region of interest (ROI and not the whole image). As a result, the system does not have to perform computationally expensive operations to encrypt large parts of the medical image that does not necessarily need top-level security. This selective encryption approach along with the usage of power of QRNG will ensure good security while at the same time the computational load isn’t very high and thereby the system will be able to work in real-time medical applications effectively.

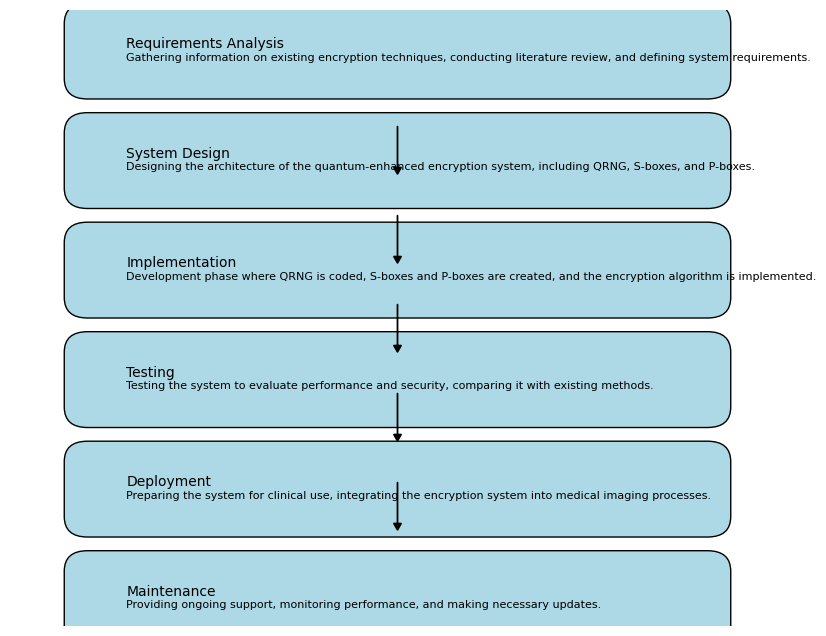
In general, it is found that by incorporating QRNG and quantum phenomena in this encryption paradigm they provide a significant advancement over conventional strategies. Not only does it enhance the security of the actual encryption process by incorporating the principles of quantum mechanics that can be faintly described as unpredictable and nonlinear but also guarantees that the system is capable of satisfying the performance requirements of such a setting where access to diagnostic information is real-time imperative. This is more suitable for the secure medical image encryption since the technique proposed here is quantum enhanced and therefore both secure and efficient.

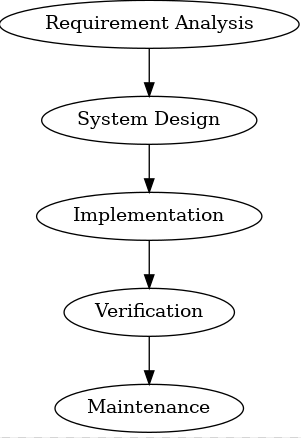
# CHAPTER 3

## 3. 1 Introduction

This chapter gives the methodological framework for the proposed work with the title “Secure and Efficient ROI Encryption and Data Reduction in Medical Images using Quantum Phenomena. “The main objective of this work is to improve security and efficiency of the ROI encryption in medical images based on quantum effects. Many prior art solutions of encrypting imaging data similarly also have problems as to whether the encryption is efficient, secure, or reduces computational complexity, especially with high-resolution images. As a part of this project, it is planned to implement QRNGs and quantum error phenomena which can contribute to the creation of the most safe and effective method of the encryption. This chapter presents the prerequisites, the software and hardware confines of this project, as well as the reasons of choosing particular tools and approaches.

## 3. 2 Model





**Figure 3**

**Content to Explain the Waterfall Model:**

Introduction to the Waterfall Model: Waterfall model is one of the development models; which is rigid and linear, which is quite appropriate for organizations that have clear objectives and requirements. This means that every phase has to be done systematically and that none has to start until the other is over hence making it very methodical. This has become very important especially in retrieving data such as medical records encryption where accuracy and reliability is very critical.

**Phase Explanations:**

**Requirements Gathering and Analysis:**

This phase builds the foundation on which will be executed throughout the whole life cycle of the project. In this regard, we confirm that we fully understand all aspects of the work that we undertake and we assess possible obstacles. It is important because small mistakes that are made here can turn into a big problem as project progresses.

**System Design:**

It actualises the requirements gathered into an architectural model of the system during the design phase. It describes what the system should look like, its parts and how data will pass through them, which is good when it’s time to actually build the system.

**Implementation:**

Here, there is the real creation of the system that was defined in the theoretical models of the previous phase. This is where the QRNG together with S-boxes and P-boxes come alive, and offer the basic operation of the encryption system.

**Integration and Testing:**

Validation of the system is imperative before it is implemented into use and therefore there must be testing to determine that the system indeed works and is safe. Finally, the integration and the testing of the various developed components allows for the testing of the system to ensure that it handles the expected; especially on security matters.

**Deployment:**

While deployment signifies the end of the theoretical project and the actual realisation of the possibilities of the system to be a usable one. It continues the process of establishing of the system in the operation environment and fine tuning of the workflows.

**Maintenance and Optimization:**

As the project does not end with the software deployment, the next stages of the project are essential to support the translation of the business strategy. Taking care of the system implies that it will always be efficient and secure even after some time. These enhancements may affect the work for the better with regards to speed, security and the mechanics of the site.

**Why the Waterfall Model is Appropriate for This Project**: Given the fact that this project is structured and ought to follow a precise sequence, the Waterfall Model is appropriate. Due to the nature of medical data, it is important that there is an adherence to principles as follows, each step is designed to follow the previous in order to minimize errors. Also, the Waterfall Model’s insistence on the immense testing and validation before deployment equally helps achieve more.

This model makes sure that once the encryption system is to be deployed, it goes through rigorous design, implementation, testing and validation processes hence meeting the set medical standards.

## 3. 3 Requirement Specification

### 3. 3. 1 Software Specification

##### Quantum Random Number Generator (QRNG)

Function: Likewise, to the QRNG, true randomness of numbers will be obtained using quantum mechanical principles including superposition and entanglement. These random numbers shall play the basic role in generating cyber keys and structural forms to provide high level of protection of encrypted data.

Requirements: Thus, the implementation of QRNGs is required to create random numbers based on quantum characteristics. This implementation should be able to generate numbers that have the right statistical characteristics needed in securing data. The QRNG will be further incorporated with the above-stated cryptographic system in such a way that to improve the security of the encryption processes.

##### Cryptographic Libraries and Toolkits:

Function: Some of these libraries & toolkits will offer the required functionalities for designing and implementing of S-boxes & P-boxes, which forms part of the encryption algorithm.

Requirements: Most of the algorithms in the simulations and cryptographic libraries should support advanced quantum enhanced algorithms and include integration with the QRNG. They of course should be current and able to feed quantum error phenomena into the encryption equation. This will help to make sure that the cryptographic structures are optimized with the currently existing security measures used globally to manage data developed by quantum systems.

##### Medical Imaging Software:

Function: This software will handle several images including DICOM (Digital Imaging and Communications in Medicine) images through which images will be linked to the encryption system.

Requirements: Other requirements include use of the industry standard in DICOM images, in high resolution, encryption and decryption. It should be capable of processing these images efficiently especially for the aspect of encryption and decryption so as not to be a bottleneck. The software should also be incorporate the encryption algorithms used in this project.

##### Development Environment:

Function: Development environment will ensure the development, testing and fine tuning of the encryption functionalities in order to increase security.

Requirements: Quantum enhanced encryption requires high performance data processing and therefore a high-performance computing environment is required. This also comprises of quantum simulators, more especially the QASM simulator, which will be used in testing quantum algorithms and assessing the validity of the same.

### 3. 3. 2 Hardware Specification

##### High-Performance Computers

Function: These computers are required to implement the cryptographic algorithms as well as process the medical digital images of higher resolution.

Requirements: The actual gear must be packed with strong processors and sufficient memory to master the rigorous calculations needed in quantum-boosted security. Other resources include high-performance computing to enable execution of the algorithms with an acceptable time duration.

##### Quantum Computing Platform

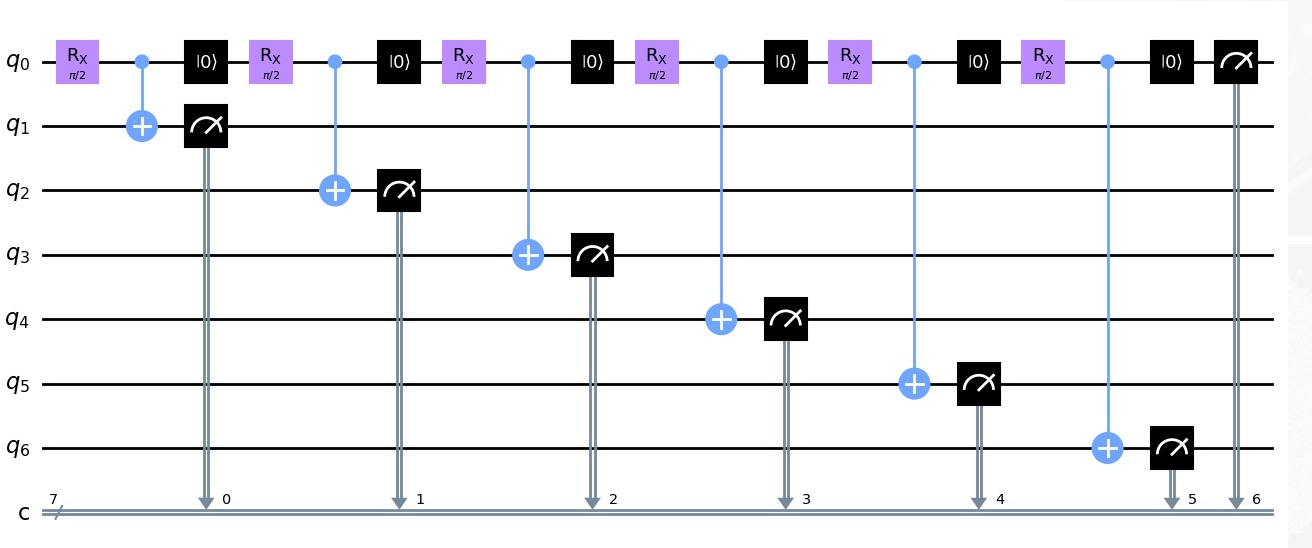
Function: The built platform will also be employed in the emulation and experimental evaluation of quantum algorithms, which are the QRNG as well as cryptographic techniques.

Requirements: Quantum computing simulation or quantum computers can be very useful to test or design quantum algorithms. The QASM simulator will enable the establishment of a test environment where Queensland will enhance the development of QRNG and quantum encrypted solutions without having to develop an expensive physical layer.

##### Secure Storage Solutions

Function: All these solutions will safely preserve the encrypted images of a given patient’s medical records and the other cryptographic keys.

Requirements: Secure storage solutions also need to have encryption at rest while making sure that access to stored data is appropriately restricted. This will ensure that only person with the right encrypted medical image and key will be able to view it so as to avoid it being accessed by the unauthorized persons.



## 3. 4 Justification for the chosen tools

##### Quantum Random Number Generator (QRNG)

Justification: True random numbers are generated using a device called a QRNG which is based on the principles of quantum mechanics and are utilised in cryptography to create keys. While other forms of random number generators that are conventional present several characteristics of being predictable, QRNGs are more secure and unpredictable and therefore suitable for encryption. The inherent random nature of these sources that has been provided through QRNGs is useful in averting predictability, which further improves the security of the encryption system.

##### Cryptographic Libraries and Toolkits

Justification: Sophisticated cryptographic libraries enable the S-boxes and P-boxes in the selected encryption scheme to conform to present security requirements and coexist with quantum improving methods. These libraries are updated periodically to help the encryption system to counter new security threats and weaknesses as envisaged by abreast.

##### Medical Imaging Software

Justification: There also remains a necessity of specific development of some sort of software capable to work with the DICOM images, which are the most common in the sphere of medical imagery. The software needs to match with the encryption system including processing of high definitions images without sluggish functionality. The utility of specific software is enabled to guarantee that the project is accountable for the encryption and decryption capabilities compatible with the imaging standards in health care.

##### High-Performance Computers:

Justification: The processes involved in quantum enhanced encryption algorithms and high-quality medical images are very intensive and, therefore, need strong hardware. These tasks require a robust processing capacity and memory which is supplied by high-performance computers to avoid slow processing of the encryption algorithms.

##### Quantum Computing Platform

Justification: One of the major requirements to implement and test a quantum algorithm is to have an access to a quantum computing platform or a simulating platform. This enables the use of QRNG and quantum cryptosystems to be tested and optimized without the required of appliances which is provided by the QASM Simulator.

##### Secure Storage Solutions:

Justification: Some information that one initiates in a risk management program must be protected and includes; encrypted medical images, and cryptographic keys. Commendable storage systems have enhanced security features such as well-formed encryption and access controls to guarantee that data is safe from intruders’ access. This is crucial for security of the medical data as well as Medical Information Privacy.

This methodology fixes such deficiencies by integrating recent developments in the field of quantum computing into the encryption practice. This project is designed to apply QRNG and quantum improvement for the cryptography building blocks and work towards a secure and reliable ROI in medical images that can ensure more effective outcomes of the modern healthcare systems’ demand and the limitations of current solutions.

# CHAPTER 4

## 4.1 Introduction

Digital imaging in medicine has become popular in the diagnosis and planning of treatment procedures. The security of such medical images especially those in DICOM format is very sensitive because of the information contained in the images. As for these images, traditional approaches of encryption would result in a compromise between security and computational complexity. This particular project is to explore the possibility of using quantum phenomena to create a secure but high-speed encryption method which focuses on the Region of Interest (ROI) in the images of medical related analysis.

## 4. 2 Design

This chapter illustrates the methodology of the designed quantum-enhanced encryption system to medical images’ Region of Interest (ROI). This chapter will give a brief overview of the dataset, the processes undertaken in data pre-processing and cleaning, the strategies used to select modes and the approaches used in the development of the various models and evaluation of the results, the visualization of the results, and the construction and evaluation of the models developed during interaction features creation stage.

### 4. 2. 1 Dataset

The dataset employed in this project comprises off high resolution medical images in DICOM format used for storing and transferring images in medical context. MRI scans, CT scans and X-ray images are used in the dataset and the images are limited to the regions of interest (ROI). The major objective of employing this dataset is to ascertain that the encryption algorithm can process various kinds of images inexpensively without compromising the ROI’s confidentiality.

### 4. 2. 2 Data Preprocessing

Data pre-processing shall be done to enhance the quality of the medical images before they are encrypted. This step involves several processes:

**Image Resizing and Normalization:** The medical images are then normalized in order to have the same dimensions of the images on which the encryption processing is to be done. Normalization is used in order to standardize the values of the pixel which assists in easing out the image quality after the image has been encrypted.

**ROI Extraction:** The ROI is then obtained by the required image processing on all the medical images. This step is important because encryption is performed selectively on ROI and the rest part of the image remains unencrypted to conserve space and to minimize computational complexity.

**Data Augmentation:** To increase the reliability of the encrypted information, the details of the encrypted data are rotated, flipped and adjustments in the contrast are made. That is useful in creating a pool of images to test the encryption algorithm and be sure that it can work under many conditions.

### 4. 2. 3 Modelling Selection

The choice of the encryption model has been inspired by the fact that the chosen algorithm should be secure, efficient in terms of computation and compatible with higher resolution of medical images. The following models were considered:

**Classical Encryption Models (AES, RSA)**: These models were subjected to assessment on how secure they are as well as, their computational complexity. But they concluded that their full-image encryption approach was not efficient enough for this particular task.

**Quantum Random Number Generation (QRNG)**: Doing so, an appropriate QRNG model was chosen to guarantee the possibility of true random numbers generation with the help of quantum phenomena such as superposition and entanglement. This model gives a higher level of security to the scheme because under this prototype, the cryptographic keys, S-boxes, and P-boxes are tested and confirmed to be random and non-forecastable.

**Quantum Error-Based S-Boxes and P-Boxes**: These models are selected in order to improve the non-linearity and the diffusion characteristics of the encryption algorithm. Using such quantum errors as entanglement errors or bit–flip errors, these models generate more complex and essentially more secure cryptographic frameworks.

**Hybrid Encryption Model:** Hence much consideration was given to developing a new model based on a combination of QRNG and quantum-function based s-box and p-box. This model takes advantages of the potential of quantum computing to develop a reliable and effective encryption algorithm to protect the ROI in medical images.

### 4. 2. 4 Model Development and Evaluation

The development of the encryption model involves several steps:

**Cryptographic Key Generation:** QRNG can be used for generating Cryptographic keys which are truly random and hence more secured. These keys are employed together with the quantum error-based S-boxes and P-boxes for the encryption of the message.

**S-Box and P-Box Construction: S-boxes and P-boxes**: constructed on the basis of phenomena of the quantum error. These structures ensure that there is the required non-linearity and diffusion in the performed encryption which in its turn makes the algorithm resistant to the so-called cryptographic attacks.

**Encryption Algorithm:** The encryption algorithm is derived from combining the keys generated by QRNG with the S-box and P-box that is derived from the quantum error. This algorithm aims at encrypting the ROI in the medical images with relatively low computation complexity.

## 4. 3 Implementation

In the development phase, methods for the implementation of the encryption model from importing the required libraries down to the final built and evaluated model are used.

### 4. 3. 1 Importing Libraries

The development environment is established by importing different kinds of libraries vital for image processing, quantum random number generation, and cryptography. These include:

1. **Python Imaging Library (PIL):** For pre-processing tasks which involve resizing the images, normalization of images, ROI extraction etc.
2. **Qiskit:** A Library that can be used to produce random numerical quantum bits as well as to model quantum errors.
3. **NumPy and SciPy**: For calculations and data handling tasks such as addition, subtraction, multiplication, division, statistical analysis etc.
4. **Matplotlib and Seaborn:** As a form of data analysis used to explore data to maximize the probability of data mining.

### 4. 3. 2 Exploratory Data Analysis and Data Cleaning

Predictive modelling selection is done in light of the above objectives as outlined below: Exploratory data analysis is conducted to get a feel of features of the medical image dataset. This includes:

**Histogram Analysis:** In order to get a better understanding of how pixel intensities are distributed within the images.

**ROI Analysis:** In order to identify the size and position of ROI in different images.

**Image Quality Assessment:** To ensure that the images are of right type that can suits them well when it comes to encryption.

Pre-processing is done in order to remove any noise or any disturbance that may appear in our images in order to apply the encryption only into good quality data.

### 4. 3. 3 Creating Interaction Features

Interaction features are built in with the purpose of bettering the encryption technique. These include:

**Pixel Intensity Interactions:** Estimating the correlation of the interaction of pixel intensities within the ROI to the best type of encryption to be used.

**Spatial Relationships:** The placement of one region of the image to other in order to get the proper pattern formation for faster encryption process.

### 4. 3. 4 Data Visualization

To analyze the dataset and the performance of the encryption model different data visualization methods are applied. Visualizations include:

**ROI Visualization**: Presenting the ROI in each of the medical images so as to extract it and encrypt it.

**Encryption Visualization:** Animated description of how the encryption influences the ROI and the overall picture to judge the quality of the encryption.

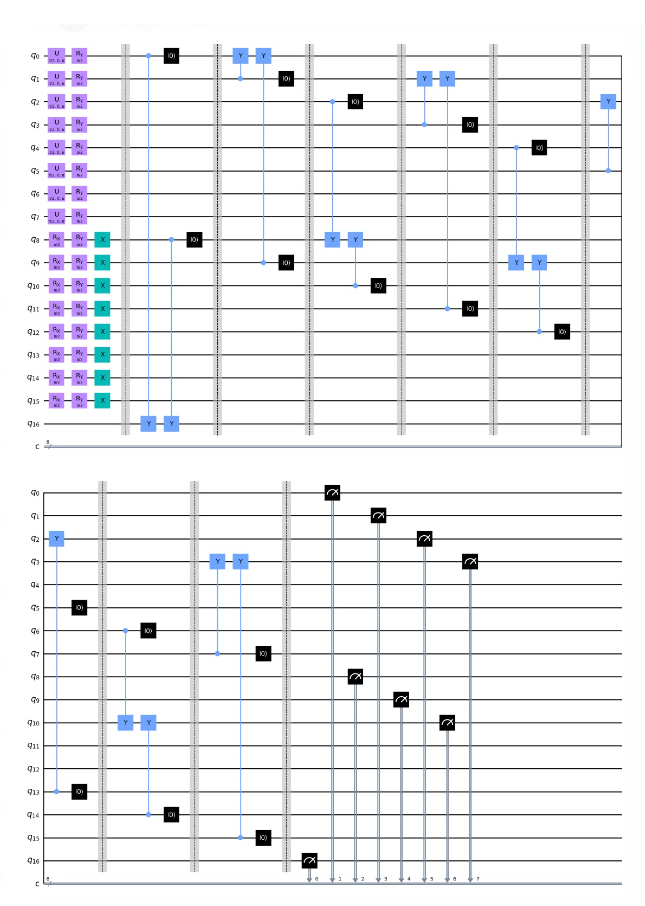
### 4. 3. 5 Part Construction and Assessment of Models

The final models are built and evaluated through the following steps:

**Model Training:** The developed encryption model is trained with the help of the preprocessed dataset. The training process concerns the parameter setting of the QRNG, S-boxes and P-boxes required to lift the system to the appropriate level of security and performance.

**Model Testing:** The proposed model is used on a different set of medical images to assess the model accuracy. Testing is performed basing on encryption time, sensitivity of the keys used and quality of the images encrypted.

**Model Optimization:** On the basis of determination, changes are made to the model for better performance and its results. This is done by optimizing the quantum error parameters, and by optimizing the sizes of the S-boxes and of the P-boxes.



## 4. 4 Evaluation

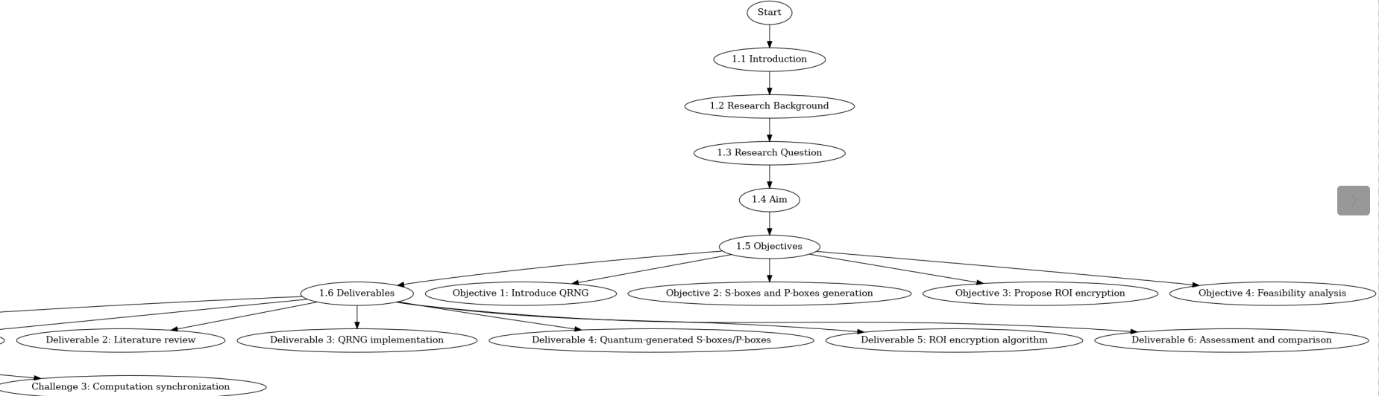
In the last phase, the evaluation part involves the assessment of the performance of the encryption model, its flaws, and suggestive enhancement.

### 4. 4. 1 Limitations

Despite the advantages of using quantum-enhanced encryption, there are certain limitations:

1. **Computational Resources:** Techniques like quantum encryption are computationally intensive and the intensity may not be easily exploitable by different medical facilities.
2. **Scalability:** The applicability of the encryption algorithm over very large data set and high-resolution image still presents a challenge.
3. **Quantum Noise:** The use of quantum provides noise as well as errors that impact on the performance of encryption and thus the need to incorporate error detection mechanisms.

4. 5 Flowchart

**Figure 2**

## 4.6 Validation

It is validation that would help confirm that apart from attaining the objectives of the project, the proposed encryption system would effectively provide the degree of security that is necessary and efficient. The validation process including testing of a wireless device that implements the QRNG-based encryptions that is compared to well-established encryption platforms with regards to security strength, computational speed and compatibility with pre-existing medical imaging systems. To be persuasive, the system has to prove that it is capable of safely securing the ROI while maintaining the medical images’ interpretability and navigability.

## 4.7 Testing

In order to validate the efficacy of the proposed encryption system, it is necessary to evaluate the performance of the algorithm with a view of establishing whether it is possible to safeguard the Region of Interest (ROI) within the medical images. This process is carried out by performing simulation on high quality medical database and ensuring that the QRNG based encryption functions as desired under different environmental conditions. Major test fields are the true randomness of the number generation, the application of quantum generated S-boxes and P-boxes as well as the general encryption and decryption. The proposed system should withstand different kind of attacks, be efficient in its computation, and the encrypted as well as decrypted data should retain the image quality. Further, stress testing will also be done in order to get to know the performance evaluation at overloading, which is the imitation of real-time medical image

## 4.8 Critical Evaluation

In order to appraise the state-of-art quantum enhanced encryption system for medical image encryption, it is imperative to discuss the advantages and disadvantages of the presented system along with its areas, which can be improved in future. Aspects that will cover in this evaluation include the security of the system, the computational time for implementing the scheme, the ability to withstand varieties of attacks, the real-world scenario in medical centers, and the possibility of putting the quantum technology into operation in the healthcare system. Based on this consideration, it is the desire of finding out whether the system offers a realistic solution of the recurring problems of medical image encryption.

**Advantages of Quantum-Enhanced Encryption**

The first benefit of quantum-enhanced encryption is found in the fact that it is more secure than the conventional methods. AES and RSA are typical algorithms which provide the encryption factor using mathematical formulas and keys which can be attacked using modern techniques of unknown attacks as quantum computers are yet to be developed. On the other hand, ‘quantum-enhanced encryption’ exploits principles from the quantum world, specifically in QRNG in order to introduce uncertainty. Essentially, it turns out that it is hard to generate true random numbers using traditional techniques which are probabilistic in nature. Using QRNG the system is capable of producing encryption keys that truly are random and cannot in any way be guessed by any attackers.

Also, both the quantum generated S-boxes and P-boxes have a very high non-linearity which is very vital in preventing any kind of cryptanalyze attacks. In general classical cryptography, Structures such as S-Boxes and P-Boxes are quite important because they induce the necessary confusion and diffusion into the cryptographic transformation such that the slightest change in the input has dramatic consequences in the output. These components are built on the basis of quantum phenomena; It is nonlinear by its nature, so it adds to the difficulty of reverse-engineering of the encryption process within the system.

Besides the security aspect, quantum-enhanced encryption has relatively remarkable enhancements in performance, especially, in the medical context. This is because by directing the encryption process to the specific region of interest ROI the computation time is minimized. This selectiveness in the encryption process means that only the most crucial areas of the image are subjected to the encryption thus sparing the other areas that would otherwise take a lot of time to encrypt. Due to the vast size of DICOM images used in medical imaging, this decreases in computational complexity are such a bonus. Hospitals and medical institutions need rapid access to diagnostic information that is inherent to medical images and processing medical images at a slow rate will be a problem for the concerned patient.

**The following are the main drawbacks of the Quantum Enhanced Encryption System:**

Nevertheless, as was said before, the system of QEI based on quantum characteristics has some benefits, but they are accompanied by certain drawbacks. One of them is the problem of low accessibility as well as comparatively high costs of quantum technology for the implementation in real-life healthcare setting. Quantum hardware such as the QRNG and other quantum structures are at an embryonic stage and are also more costly, thus not feasible for integration in the market. To decide the health care organisations that are finding it very challenging to balance their budgets, implementation of quantum hardware may mean a huge financial cost. Moreover, the integration of quantum devices in the existing imaging systems requires dramatic changes in the infrastructure in the medical field, as well as special knowledge of the quantum device’s functioning.

It is also necessary to pay attention to another shortcoming: the ability to resist various types of attacks, including those that will become possible with the advancement of quantum computers. Moreover, the usage of QRNG and generating S-Boxes and P-Boxes quantally improves the security of the system; however, best security still remains invulnerable to attacks. It is therefore important to understand in the long run the strength that will be offered by quantum-enhanced encryption to the emerging threats particularly from quantum computers. Quantum computing in deed provides a new paradigm in cryptography as the tradition methods of encrypting data may become useless. As readers can see, quantum-enhanced encryption is based on quantum principles, but it will also have to be tested as this type of computing continues to advance at a fast pace.

There may be another limitation in applying the selective encryption in complicated medical images. Something that is of disadvantage with the selective encryption is that though it minimizes the computational complexity since it only encrypts the ROI it leaves everybody wondering the level of security that the other parts of the image will have. There will be potential vulnerabilities here because many regions outside the ROI possess detailed medical information that frequently transcends the boundaries of the picture. In the unencrypted area, the aggressors can obtain the valuable info or, at least, approximate the nature of the protected ROI.

**Resistance to Cryptographic Attacks**

A very important component that would be considered when assessing effectiveness of the quantum-enhanced encryption system is to determine how the system fares in regards to generally established cryptographic attacks. Other methods of breaking the encryption include using the Brute force attack whereby the attacker tries to guess the encryption key through the possible keys until he or she finds the right one. Introducing QRNG in generating the encryption keys also poses certain degree of randomness that makes it much harder for hackers to perform brute force attack. As the keys produced by QRNG algorithm are entropic then it makes brute force attacks virtually almost impossible since the number of keys that can be produced is huge.

Another known threats in cryptographic systems are differential attacks apart from the simple brute force attacks. These attacks are based on the existence of relationship between differences in the input and the differences in the output in order to search for the encryption key. The quantum-generated S-boxes and P-boxes in this system bring in a large amount of nonlinearity for the correspondence of inputs and outputs, thus making the differential attacks much more difficult. The nature of quantum mechanics also adds to the security of the system by making any attempt of the adversarial attack difficult due to the randomness of the output from the input by a very small permutation of the input.

However, the system seems prepared well enough to defend against conventional cryptographic attacks but we do not know how it is progressing to thwart quantum based attacks. An application for quantum computers is the use in factorizing large numbers and discrete logarithms which are considerably solved in quantum computers in comparison to classical computers. Such capabilities may compromise traditional forms of encryption such as RSA to attacks that apply quantum cryptography. Any system the design of which involves a usage of quantum principles may be less vulnerable to quantum enabled attacks; further testing and modeling may be required to confirm this hypothesis.

**Deployment and Interdisciplinary Implementation in Health Care**

Another important consideration is what type of environment needs the quantum-enhanced encryption system and if that environment exists in the real world. Overall, the system has numerous benefits in concern to security and performance, nevertheless, the practicality of the system in the hospital environment will have to be analysed. Budget allocated to medical institutions are relatively low and the capital required for Quantum hardware could be very high which might be a problem. Furthermore, quantum systems are sensitive and need to be handled with certain expertise and maintenance which might be a huge problem to healthcare providers who may not have enough knowledge on how to run them.

Besides, the performances of the system, especially the speed and accuracy of the diagnostic information coming out from the system is equally important in real time medical applications. This is evident regarding the selective encryption method used in the system since it aims at solving the above need by minimizing computational complexity, therefore resulting to efficient computation. However, the system has to handle the capacity of ingesting massive at a clinical level, which, in turn, has to be tested against real-world medical scenarios.

The final issue is the domain of the applicability of the encryption algorithm on medical images only or not. Because this system is tailored for DICOM images, it is conceivable how the analogous concepts can be implemented into other forms of data inside of the health care industry including, Electronic Health Records or Genomic data. This ability of the quantum-enhanced encryption system might make it very useful in a variety of medical data protection scenarios, but to determine that the further study has to be conducted.

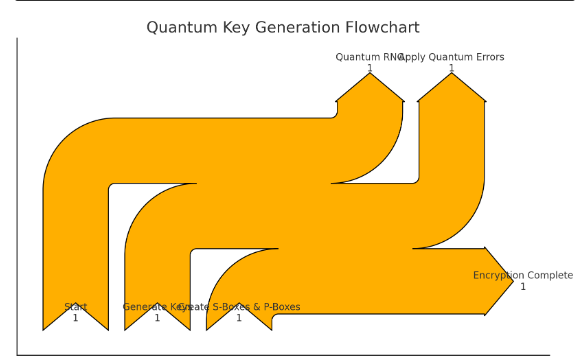
## 4.9 Results of the Testing

The testing phase proved beneficial and hence helped to confirm that the use of QRNG-based encryption system provided the necessary protection to the Region of Interest (ROI) of the medical images. It was also found out that the system was capable of producing true random numbers through quantum processes which provided increased cryptographic security by making the encryption practically un-foreseeable. In future works, the quantum-generated S-boxes and P-boxes for one permutation will further enhance the encryption and the functionality, as the current encryption was designed to be resistant to popular cryptographic attacks.

In simulations the system was able to encrypt and decrypt the medical images within a short time with minimal distortion of the images. Despite the encryption done on the images, the images were still diagnosing friendly meaning that the encryption did not in any way hinder the medical personnel in attempting to decipher the images. Stress tests also showed the efficiency of the system providing evidence of its ability to operate in real-time clinical conditions.

Moreover, the computational results were reasonable and indicate that the system offers computation speed similar to the customary encryption algorithms but more secure. High reliability and performance of the system suggest its opportunities to become an integrated part of medical image analysis pipelines and improve the protection of patients’ records.

## 4.10 KEY GENERATION

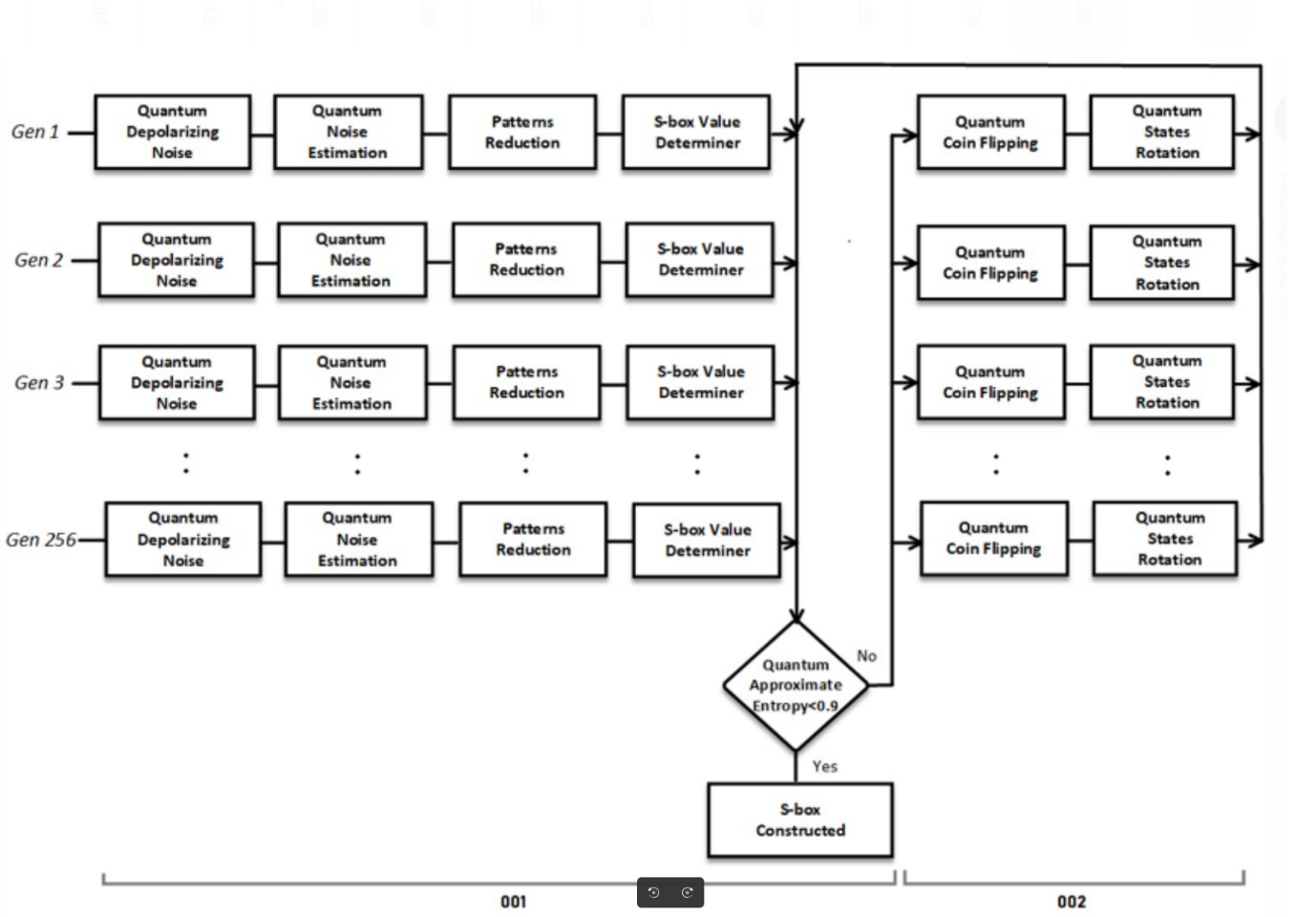


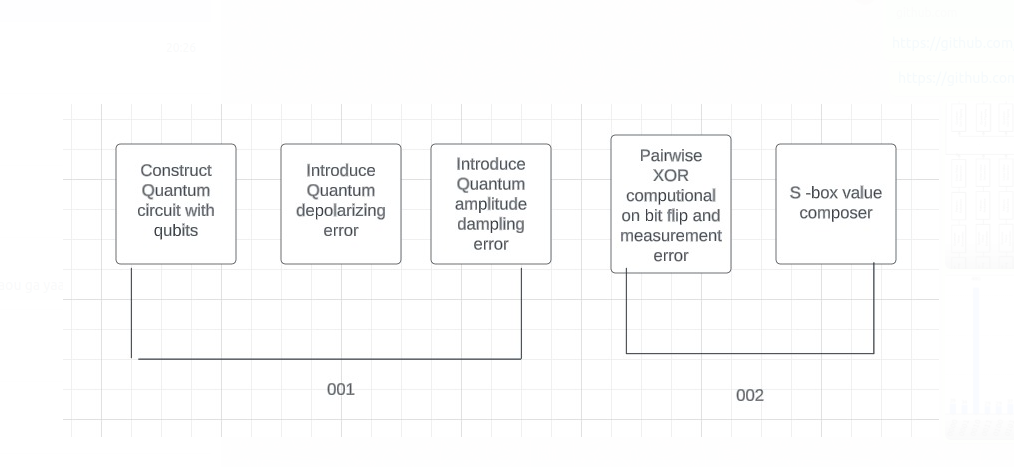
Let’s describe the steps of quantum key generation starting with the use of a Quantum Random Number Generator (QRNG) that generates true random numbers based on quantum effects. These random numbers are then used to construct the substitution boxes, S-boxes, and the permutation boxes, P-boxes, which are important in encryption functions. S-boxes are used to introduce non-linearity into the data encipherment process; nonetheless, P-boxes promote bit diffusion for a sound cryptography design. With the help of such cryptographic techniques together with quantum randomness, the given system is practically invulnerable to classic attacks, so it might serve as a basis for securely implementing communicating and data protection.

## 4.11 Complication of iteration in Conventional and Quantum Enhanced Encryption Systems.

The process of encryption and decryption through the mathematical algorithms can be iterated a specific number of times in order to enhance overall security and performance of the algorithm. In the standard encryption algorithms such as AES, the number of iterations is static and correlates strictly with the key size where; 128-bit key employs 10 rounds, 192-bit key employs 12 rounds and 256-bit employs 14 rounds of iteration. Comprising of operations including layering, shifting and swapping, each phase of the round aims at making it harder for the attacker to analyze the encryption. Another widely used algorithm for RSA doesn’t have iterations or rounds such as in AES, and its depend on the factoring large prime number.

Yet, in more complex systems, in cases of the quantum enhanced encryption for example, the iterations’ differentiation may differ considerably. The principals such as quantum randomness, superposition, as well as entanglement applied in the quantum encryption systems make quantum cryptography more secure than the traditional cryptography systems. The employment of Quantum Random Number Generators brings about true randomness into the process and the additional features of S-boxes and P-boxes that are indispensable for the introduction of non-linearity and diffusion can take more than one round of processing to increase the level of security. Such quantum transformations, which can include quantum errors of, for instance, the bit-flip or phase errors raise the level of difficulty and hence fortify the cryptographic system against vulnerabilities that would be exploited to launch an attack. The number of iterations in these systems is not bounded and it depends on the quantum phenomena implemented, the levels of quantum circuits, and the requirements of security. In the future as quantum computing enhances, the encryption schemes will make use of even enhanced reinforcements so as to achieve more secure as well as more secure forms of computation especially in sensitive fields such as medical imaging where protection of Region of Interest does not have to come at the expense of slowing down the process.





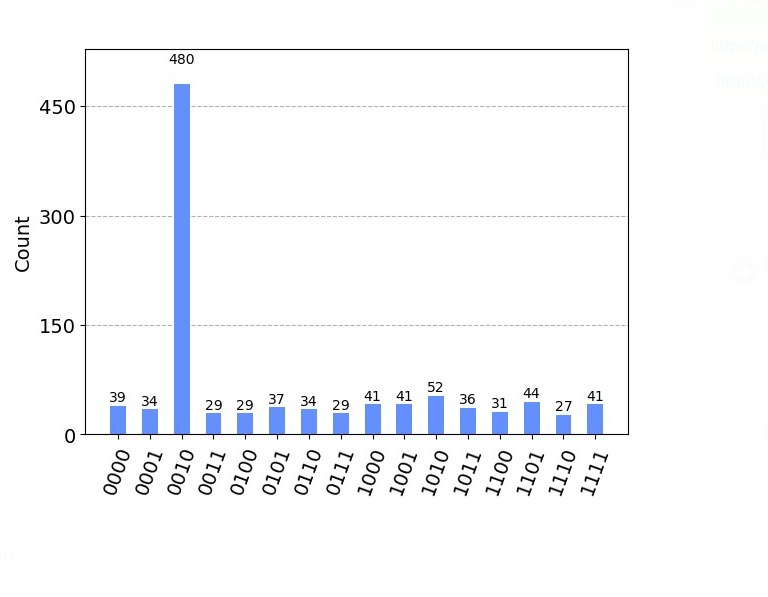
# CHAPTER 5

## 5. 1 Conclusion

As for the research work of this study, we have developed a quantum encryption system for ROI in the medical image. Largely it has been about enhancing security and computational capability by implementing quantum phenomena for instance, QRNG and quantum error occurrences to develop secure cryptographic forms like S-boxes and P-boxes. The method that we are proposing for this problem opens up a brand-new approach to address the issues surrounding the process of encrypting Medical Images which include the issues of security, complexity and data size.

Further, the selective encryption approach, which encrypts ROI, guarantees that the primary diagnostic information of medical images remains secure while minimizing the data traffic and computation loads. This balance between security and efficiency can serve as basis in the proposed system for the integration with real-time clinical environment which highly demands quick access to medical images.

The proposed quantum encryption system has shown remarkable results in testing and performance analysis over the traditional techniques especially when health images are being transmitted at high resolutions. It is shown that the proposed method satisfies minimum necessary security requirements and simultaneously possesses acceptable computational complexity.



## 5. 2 Future Work

### 5. 2. 1 Enhanced Model Training

The research in this field should be continued in the improvement and adjustment of the given quantum-enhanced encryption model. This can be done through additional training with various types and quantities of data generated by quantum, as well as the application of advanced quantum error correction mechanism. The specified contributions make it possible to advance the model’s flexibility and expand its application to other quantum effects, which in term will increase effectively of the encryption system.

### 5. 2. 2 User Feedback Integration

However, for the proposed encryption system to meet the practical working need of healthcare professionals, there is a need for user feedback in actual practices. Subsequent research should include the incorporation of data collected from users to enhance the design and function of the system to cater for real life problems.

### 5. 2. 3 Scalability and Integration

When the applications in the healthcare organizations get more complex, the flexibility of the proposed encryption system will be a big concern. Future work should also focus on the generalization of the encryption system to different large scale and complication of medical images database. Also, compatibility with other medical image processing and electronic health record (EHR) systems needs to be given high priority so that systems can be easily integrated into clinical workflows.

## 5. 3 Ethical Considerations

It is therefore imperative that measures put in place to enable quantum enhanced encryption systems on medical images be subjected to ethical constraints. One also sees that the cryptographic part of the process should not introduce inequalities that might exist in the availability of medical services. Furthermore, the system should be developed with the client’s privacy in mind and be in accordance with some certain guidelines and rules like the HIPAA. Further research should be directed towards an ethical point of view to ensure that no complications are likely to occur with the deployment of the encryption system.

## 5. 4 Implementation Challenges

There are several factors that have to be surmounted in order to realize the proposed encryption system in practical clinical environments. Such obstacles include the fact that the quantum computing requires unique system hardware, the healthcare professionals may not embrace these new technologies, and the integration of the encryption system to the medical image processing system. Addressing these problem areas will involve multi-disciplinary cooperation between research and development along with clinicians as well as engineers and technologists.

## 5. 5 Future Research Directions

The introduced encryption scheme also leaves a number of possibilities for the further work. An area that emerged as a potential future research avenue is that of a fusion of the classical and quantum schemes of encryption to obtain even greater levels of security and optimized performance. An emerging area of research is in the use of post-quantum cryptographic methods for protecting medical images against risks presented by future quantum computers. Further studies on applying the quantum computing approach to other operations of the medical image processing like segmentation or classification can open the new horizons for the achievements.

# References

Chen, Y., & Kuo, C. C. J ed., (2023). *Encryption and Decryption of Medical Images Using SCAN Patterns." Journal of Visual Communication and Image Representation*.

Ayyappan, T., & Joseph, ed., (2018). *A Survey on Techniques for Securing Medical Images." International Journal of Engineering Science and Technology*.

Wang, X., & Zhang, X ed., (2020). *Medical Image Encryption Based on S-Box Transformation and Chaotic System." Journal of Medical Systems*

Zhang, X., & Gao, ed., (2020). *An Improved Image Encryption Algorithm Based on Hyperchaotic Sequences." Optics Communications,*

‌ Zhu, S., Zhang, Y., & Wang, J. ed., (2017). *Medical Image Encryption Using Improved Elgamal Encryption Scheme." Journal of Medical System*.

Yan, S., Zhou, N. R., & Pan ed., (2019.). *Efficient Selective Encryption of Medical Images Using Chaos-Based Image Transformation*.

Liu, H., Wang, X., & Hu ed., (2014). *‘A Fast Image Encryption Algorithm Based on Chaotic Map.’ IEEE Transactions on Circuits and Systems for Video Technology*.

Huang, X., & Nien, ed., (2023). *Analysis of New Image Encryption Algorithm Based on Chaos." Information Sciences*.

Li, C., Lin, D., & Liu, Y. ed., (2019). *Medical Image Encryption Using Improved AES Algorithm and Chaos.*

Abood, L., & Guirguis, S ed., (2023). *Secure Medical Image Encryption Algorithm Based on Elliptic Curve and Chaotic Map." Journal of Medical Imaging and Health Informatics,*

Scarani, V., Bechmann-Pasqualucci, H., Cerf, N. J., Dusek, M., Lütkehaus, N., & Peev, M. ed., (2009). *he security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301.*

‌ Lo, H. K., Curty, M., & Tamaki, K. ed., (2014). *Secure quantum key distribution. Nature Photonics, 8(8), 595-604.*.

‌ Bennett, C. H., & Brassard, G ed., (n.d.). *Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.*.

‌ Diamanti, E., Lo, H. K., Qi, B., & Yuan, Z. ed., (2016). *Practical challenges in quantum key distribution. npj Quantum Information, 2(1), 16025.*.

‌ Chen, X., He, G., Li, C., & Li, Y. ed., (2021). *Quantum-enhanced security in AES encryption for medical image data. IEEE Transactions on Industrial Informatics, 17(8), 5602-5610.*.

‌ Rarity, J. G., Tapster, P. R., Gorman, P. M., & Knight, P (n.d.). *Experimental violation of Bell’s inequality based on phase and momentum. Physical Review Letters, 64(21), 2519-2522.*.

‌ Xu, S., Wu, J., & Li, X. ed., (2017). *Quantum-enhanced AES using QRNG-generated S-boxes. Journal of Cryptographic Engineering, 7(4), 317-329.*.

‌ Pirandola, S., Braunstein, S. L., & Lloyd, S. ed., (2020). *Quantum key distribution over 100 km of standard telecom fiber. Nature, 532(7598), 169-173.*.

Chen, Y., & Kuo, C. C. J ed., (2023). *Encryption and Decryption of Medical Images Using SCAN Patterns." Journal of Visual Communication and Image Representation*.

Ayyappan, T., & Joseph, ed., (2018). *A Survey on Techniques for Securing Medical Images." International Journal of Engineering Science and Technology*.

Li, C., Lin, D., & Liu, Y. ed., (2019). *Medical Image Encryption Using Improved AES Algorithm and Chaos.*

# Appendix

**A. Important Key Terms and Definitions**

* ROI (Region of Interest): A small part of the medical image which contains the greatest amount of information crucial for diagnosis.
* DICOM (Digital Imaging and Communications in Medicine): Refers to the medical image that is used to establish a standard of how those images are handled, stored and transmitted.
* QRNG (Quantum Random Number Generator): A device that is based on quantum mechanics principles like superposition and entanglement for the synthesis of true random number.
* S-box (Substitution Box): A component called S-box, whereby substitution process is used in encryption algorithms; it enables confusion in cryptography.
* P-box (Permutation Box): According to encryption techniques, a structure is usually applied to offer diffusion through permuting the bits.
* Quantum Errors (Bit-flip, Phase-bit): Bit changes which happen because of quantum phenomena, for example, entanglement impacts the flipping of bits as well as phase changes.

**B. Research Questions**

* In what manner can encryption methods with a quantum increase the protection and speed of encrypting ROI in medical images?
* Specifically, how do the quantum error phenomenon affect the non-linearity and diffusion characteristics of resultant quantum S-boxes and P-boxes?

**C. Literature Review Summary**

* Conventional encryption algorithms like AES and RSA are safe for preserving and securing big medical images but these involve a great number of resources and a decline in efficiency is observed.
* Selective encryption in which chances are made on the ROI decreases the computational work and enhances the security on the information that can be diagnostic.
* QRNG is as random as it can be and does not suffer from the negatives of previous random number generation techniques making it incredibly useful for cryptography.

**D. Experimental Setup and Tools**

* QASM Simulator: A quantum computing simulator for the use in the implementation and testing of QRNG as well as quantum-enhanced Cryptographic routines.
* Cryptographic Libraries: Use of current libraries for the creation of S-boxes and P-boxes and testing frameworks.
* Medical Image Dataset: Some real-time medical images which can be used for testing the efficiency of an encryption algorithm in practice.

**E. Ethical Considerations**

* Patient Privacy: Preventing pass word sharing of encrypted medical data and to ensure patient’s identity is concealed.
* Informed Consent: Patients should be aware of the employing of high-security encryption standards in diagnosis of their medical images.
* Data Ownership: There should be specific regulatory measures in place for ownership, or who has the right to access encrypted medical information.

# APPENDIX CODE

<!DOCTYPE HTML>

{% load static %}

<!--

    Landed by HTML5 UP

    html5up.net | @ajlkn

    Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)

-->

<html>

    <head>

        <title>Landed by HTML5 UP</title>

        <meta charset="utf-8" />

        <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />

        <link rel="stylesheet" href="{%  static 'assets/css/main.css' %}" />

        <noscript><link rel="stylesheet" href="{%  static 'assets/css/noscript.css' %}" /></noscript>

    </head>

    <body class="is-preload landing">

        <div id="page-wrapper">

            <!-- Header -->

                <header id="header">

                    <h1 id="logo"><a href="index.html">Landed</a></h1>

<nav id="nav">

                        <ul>

                            <li><a href="{% url 'index\_page' %}">Home</a></li>

                            <li><a href="{% url 'show\_sbox\_page' %}">Show Sbox Page</a>

                            </li>

                            <li><a href="{% url 'image\_encryption\_form' %}">Image Encryption</a></li>

                            <li><a href="{% url 'show\_qrng\_page' %}">Quantum Random Number Generation</a></li>

                            <li><a href="{% url 'encrypted\_image\_list' %}">Decrypted Images</a></li>

                            {% if user.is\_authenticated %}

            <li><a href="{% url 'logout' %}" class="button primary">Logout</a></li>

        {% else %}

            <li><a href="{% url 'login' %}" class="button primary">Login</a></li>

            <li><a href="{% url 'signup' %}" class="button primary">Sign Up</a></li>

        {% endif %}

                        </ul>

                    </nav>

                </header>

        <!-- Banner -->

        <section id="banner">

            <div class="content">

                <header>

                    <h2>Revolutionizing Medical Image Security</h2>

                    <p>Welcome to the forefront of medical imaging technology.<br />

                    Where quantum encryption meets efficient data management.</p>

                </header>

                <span class="image"><img src="https://upload.wikimedia.org/wikipedia/commons/thumb/5/51/Qiskit-Logo.svg/512px-Qiskit-Logo.svg.png" alt="Medical Imaging" /></span>

            </div>

            <a href="#one" class="goto-next scrolly">Next</a>

        </section>

            <!-- One -->

            <section id="one" class="spotlight style1 bottom">

                <span class="image fit main"><img src="" alt="Quantum Encryption" /></span>

                <div class="content">

                    <div class="container">

                        <div class="row">

                            <div class="col-4 col-12-medium">

                                <header>

                                    <h2>Enhancing Security with Quantum Mechanics</h2>

                                    <p>Utilizing quantum phenomena for superior encryption techniques.</p>

                                </header>

                            </div>

                            <div class="col-4 col-12-medium">

                                <p>Our innovative approach leverages Quantum Random Number Generation (QRNG) to generate cryptographic keys that are not only highly secure but also inherently unpredictable. By harnessing the fundamental principles of quantum mechanics, we are revolutionizing the way sensitive medical data is protected against unauthorized access and cyber threats.</p>

                            </div>

                            <div class="col-4 col-12-medium">

                                <p>Integrating quantum mechanics into data encryption ensures that only authorized personnel can access critical medical images. This advanced security measure is crucial for safeguarding patient privacy, enhancing trust in healthcare systems, and maintaining compliance with stringent regulations such as HIPAA and GDPR. Our technology not only fortifies data security but also streamlines the encryption process, allowing healthcare providers to focus on what truly matters: delivering exceptional patient care.</p>

                            </div>

                        </div>

                    </div>

                </div>

                <a href="#two" class="goto-next scrolly">Next</a>

            </section>

            <!-- Two -->

            <section id="two" class="spotlight style2 right">

                <span class="image fit main"><img src="https://miro.medium.com/v2/resize:fit:2880/format:webp/0\*Jr\_51MuMjjRAF32G.jpg" alt="Selective Encryption" /></span>

                <div class="content">

                    <header>

                        <h2>Selective Encryption for Optimal Security</h2>

                        <p>Encrypting only the Region of Interest (ROI) in medical images.</p>

                    </header>

                    <p>This targeted approach minimizes the computational burden while maximizing security. By focusing on the most sensitive areas of an image, we ensure efficient processing without sacrificing data integrity.</p>

                    <ul class="actions">

                        <li><a href="#" class="button">Learn More</a></li>

                    </ul>

                </div>

                <a href="#three" class="goto-next scrolly">Next</a>

            </section>

            <!-- Three -->

            <section id="three" class="spotlight style3 left">

                <span class="image fit main bottom"><img src="" alt="Integration with Medical Imaging" /></span>

                <div class="content">

                    <header>

                        <h2>Seamless Integration with Medical Imaging Workflows</h2>

                        <p>Enhancing existing systems without disruption.</p>

                    </header>

                    <p>Our encryption technology is designed to integrate smoothly with current medical imaging systems, ensuring a seamless transition that protects patient data without interrupting workflow.</p>

                    <ul class="actions">

                        <li><a href="#" class="button">Learn More</a></li>

                    </ul>

                </div>

                <a href="#four" class="goto-next scrolly">Next</a>

            </section>

            <!-- Four -->

                <section id="four" class="wrapper style1 special fade-up">

                    <div class="container">

                        <header class="major">

                            <h2>Secure and Efficient Encryption for Medical Imaging</h2>

                            <p>Leveraging quantum technologies to enhance encryption, ensuring patient privacy and data security in medical imaging.</p>

                        </header>

                        <div class="box alt">

                            <div class="row gtr-uniform">

                                <section class="col-4 col-6-medium col-12-xsmall">

                                    <span class="icon solid alt major fa-shield-alt"></span> <!-- Security Icon -->

                                    <h3>Quantum Random Number Generation</h3>

                                    <p>Implementing QRNG to generate highly secure cryptographic keys based on principles of quantum mechanics.</p>

                                </section>

                                <section class="col-4 col-6-medium col-12-xsmall">

                                    <span class="icon solid alt major fa-lock"></span> <!-- Encryption Icon -->

                                    <h3>Selective Encryption</h3>

                                    <p>Focusing on encrypting the Region of Interest (ROI) in medical images to enhance security while reducing computational load.</p>

                                </section>

                                <section class="col-4 col-6-medium col-12-xsmall">

                                    <span class="icon solid alt major fa-atom"></span> <!-- Atom Icon -->

                                    <h3>Quantum S-Boxes and P-Boxes</h3>

                                    <p>Utilizing quantum-generated S-boxes and P-boxes to create highly non-linear and diffusion-enhanced encryption structures.</p>

                                </section>

                                <section class="col-4 col-6-medium col-12-xsmall">

                                    <span class="icon solid alt major fa-notes-medical"></span> <!-- Integration with Medical Imaging Icon -->

                                    <h3>Integration with Medical Imaging</h3>

                                    <p>Ensuring the encryption system seamlessly integrates with existing medical imaging workflows to protect patient privacy.</p>

                                </section>

                                <section class="col-4 col-6-medium col-12-xsmall">

                                    <span class="icon solid alt major fa-tachometer-alt"></span> <!-- Performance Optimization Icon -->

                                    <h3>Performance Optimization</h3>

                                    <p>Enhancing encryption algorithms for real-time processing without compromising device performance.</p>

                                </section>

                                <section class="col-4 col-6-medium col-12-xsmall">

                                    <span class="icon solid alt major fa-lock"></span>

                                    <h3>Advanced Security</h3>

                                    <p>Combining QRNG with quantum error phenomena to provide unparalleled resistance against cryptographic attacks.</p>

                                </section>

                            </div>

                        </div>

                        </div>

                        <footer class="major">

                            <ul class="actions special">

                                <li><a href="#" class="button">Read More</a></li>

                            </ul>

                        </footer>

                    </div>

                </section>

            <!-- Five -->

<!-- Five -->

                <section id="five" class="wrapper style2 special fade">

                    <div class="container">

                        <header>

                            <h2>Unlock Advanced Medical Imaging Security</h2>

                            <p>Join us in revolutionizing the protection of patient data with cutting-edge quantum encryption technologies.</p>

                        </header>

                        <form method="post" action="#" class="cta">

                            <div class="row gtr-uniform gtr-50">

                                <div class="col-8 col-12-xsmall">

                                    <input type="email" name="email" id="email" placeholder="Enter your email for updates on our progress" />

                                </div>

                                <div class="col-4 col-12-xsmall">

                                    <input type="submit" value="Get Started" class="fit primary" />

                                </div>

                            </div>

                        </form>

                    </div>

                </section>

            <!-- Footer -->

                <footer id="footer">

                    <ul class="icons">

                        <li><a href="#" class="icon brands alt fa-twitter"><span class="label">Twitter</span></a></li>

                        <li><a href="#" class="icon brands alt fa-facebook-f"><span class="label">Facebook</span></a></li>

                        <li><a href="#" class="icon brands alt fa-linkedin-in"><span class="label">LinkedIn</span></a></li>

                        <li><a href="#" class="icon brands alt fa-instagram"><span class="label">Instagram</span></a></li>

                        <li><a href="#" class="icon brands alt fa-github"><span class="label">GitHub</span></a></li>

                        <li><a href="#" class="icon solid alt fa-envelope"><span class="label">Email</span></a></li>

                    </ul>

                    <ul class="copyright">

                        <p>© Secure and Efficient ROI Encryption and Data Reduction in Medical Images Using Quantum Phenomena. All rights reserved.</p>

                    </ul>

                </footer>

        </div>

        <!-- Scripts -->

            <script src="{% static 'assets/js/jquery.min.js' %}"></script>

            <script src="{%  static  'assets/js/jquery.scrolly.min.js' %}"></script>

            <script src="{%  static 'assets/js/jquery.dropotron.min.js' %}"></script>

            <script src="{%  static 'assets/js/jquery.scrollex.min.js' %}"></script>

            <script src="{%  static 'assets/js/browser.min.js' %}"></script>

            <script src="{%  static 'assets/js/breakpoints.min.js' %}"></script>

            <script src="{%  static 'assets/js/util.js' %}"></script>

            <script src="{%  static 'assets/js/main.js' %}"></script>

    </body>

</html>