International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Quantum Computing: Revolutionizing S-Box Creation for Enhanced Image Encryption

Sowmya M[a], Nidhin K V[b]

[a]MTech Scholar, Department of Electronics and Communication, NSS College of Engineering, India
[b]Assistant Professor, Department of Electronics and Communication, NSS College of Engineering, India

ABSTRACT :

The increased use of chat, Internet, and other wireless communications combined with high-quality video streaming provides protection and secure data transmission. Advanced Encryption Standard (AES) is the most effective method for image encryption and decryption. The AES algorithm includes several steps, among which the creation of the s-box is the most important. Highly variable bins (s-boxes) introduce a lot of confusion into the algorithm. In this paper, we propose an efficient method to create s-boxes based on quantum computing. Quantum computing is a developing technology that utilizes quantum mechanics to perform mathematical calculations faster, efficient and has low complexity. Also, the unique properties of quantum mechanics are being utilized to enhance the security of image data. Furthermore, the pa- per explores the role of Quantum Key Distribution (QKD) in securing image communication channels. QKD offers a quantum-safe alternative for generating shared secret keys, ensuring a level of security that remains resilient to quantum threats. The s-box which is created using quantum keying is used to XOR with the plain image that results in quantum encrypted image. Quantum encrypted images have high performance, complexity and large area. As quantum technology continues to evolve the proposed quantum image encryption method focuses on helping measure security in protecting visual information.

Keywords: Advanced encryption standard, Quantum computing, Quantum encrypted image, Quantum key distribution.

Introduction :

In the age of digital communication and information exchange, the security of sensitive information, especially in images, is extremely important. Image security and privacy includes security measures designed to protect images from unauthorized access, tampering, or misuse. Video security is a multifaceted construct that includes carefully designed strategies and techniques to improve the performance of visual devices[1]. At the same time, the privacy of the image is not only to protect the privacy of the visible material, but also to eliminate the threat associated with its size. As images travel through networks and storages, risks of interception and unauthorized access arise. Therefore, strong change procedures, security practices, as well as strict control and responsible data management are essential to protect the confidentiality of the information found. Photo encryption and decryption are responsible for seeing private information. In this case, privacy uses advanced methods and strategies to protect devices from unauthorized access.

Encryption is the art of converting simple, easy-to-understand images into hard, unreadable text and protecting them from prying eyes when transmitted or stored. Decryption, on the other hand, reverses the process, restoring the image to its original state for authorized users. Encryption methods often use advanced encryption methods such as AES (Advanced Encryption Standard) or RSA (Rivest–Shamir–Addleman) to manage image data[2]. These algorithms use complex mathematics to create unique passwords, effectively hiding images under a veil of complexity. Therefore, even if the encrypted image is compromised, it cannot be cracked without the decryption key. Encryption and decryption algorithms can be symmetric and asymmetric. Symmetric encryption uses a single key for encryption and decryption. This key should be stored securely and shared only among trusted individuals. It operates on blocks or streams of data by converting plaintext to ciphertext and ciphertext to plaintext. Asymmetric encryption involves a pair of keys for encryption and a private key for decryption[3]. The security of the system is based on the mathematical combination of certain mathematical problems makes it difficult to derive the private key from the public key. The choice between symmetric and asymmetric encryption depends on factors such as security requirements, computational efficiency, and key management considerations. The choice of this process often involves a trade-off between performance and management complexity. Symmetric algorithms are faster but require a secure exchange mechanism. Asymmetric algorithms provide distribution points but are more computationally intensive[4]. Many systems combine both, using the strengths of each to provide a balance between performance and security in various cryptographic applications.

Keying in image encryption refers to the use of cryptographic keys to secure the image data. Key is an important step in securing image data and uses a key to create a secure and unique key about the private image, using the accuracy of the properties of the chosen encryption algorithm secure key distribution and storage mechanism[5]. Keys are often created using encryption algorithms such as symmetric or asymmetric encryption techniques.

This article covers important techniques implemented as quantum computing. Additionally, the role of Quantum Key Distribution (QKD) in protecting video communications is also being investigated.

Classical Advanced Encryption Standard (AES) :

Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely used to protect sensitive data. It works on block data and supports file sizes of 128, 192 or 256 bits. AES has several implementations, including substitution (SubBytes), switching (ShiftRows), mixing (MixColumns), and adding keys (AddRoundKey). This process is repeated for several cycles depending on the size. Key expansion methods generate round keys from the primary encryption key, and these round keys are used for all transactions[6].

1.1. Substitute Byte Transformation (SubBytes)

SubBytes transformation is a one-step transformation in which each byte in the state matrix is replaced by another byte[7]. The S-box is an immutable table created by performing arithmetic operations to ensure that each byte value has a different variable. This nonlinear variation adds complexity and complexity, which increases the stability of the algorithm.

1.2. Shift Row Transformation (ShiftRows)

Bytes in each row of the state matrix are shifted left by different distances. The first line remains unchanged. The second line moves one position to the left. The third line moves two spaces to the left. The fourth column moves three spaces to the left . This function helps establish a relationship between input and output, making the encryption process resistant to attacks based on simple patterns.

1.3. Mix Column Transformation (MixColumns)

Each column of the state matrix is treated as a polynomial and multiplied by a constant polynomial. This equation is made in a special mathematical form (Galois space) using a predefined coefficient matrix. MixColumns ensures that each byte in a column belongs to all four bytes of that column, making the relationship between input and output difficult.

1.4. Adding Round Key (AddRoundKey)

In each round of encryption, the current state of the data (usually a 4*4 matrix) is XORed bitwise with the corresponding key. The current state matrix and round key matrix performs bitwise XOR operation to form new state matrix. This step helps include important information in encryption and is important for the overall security of the AES algorithm.

Substitution Boxes :

Substitution boxes (S-boxes) play an important role in many encryption algorithms such as block ciphers. The design of the S-box is crucial to ensure the security and strength of the cryptographic process[8]. Here are some standards and things often considered when designing S-boxes:

1.5. Nonlinearity

S-boxes must have a high level of nonlinearity to prevent linear cryptanal- ysis. Nonlinearity is a measure of how much the S-box field deviates from a linear function.

1.6. Differential Uniformity

S-boxes must have differential uniformity to prevent differential crypt- analysis. Differential uniformity measures how much the S-box output dis tribution changes as a result of different inputs.

1.7. Bijection

Ideally, an S-box should be bijective, meaning each unique entry points to a different object and vice versa. This property helps in preventing collisions and ensures reversibility.

1.8. Avalanche Effect

A small change in the input (even a single bit) should result in a signifi- cantly different output. This ensures that any change in the input propagates throughout the S-box, providing a high level of diffusion.

1.9. Strict Avalanche Criterion (SAC)

The SAC measures how much the output changes when a single input bit is complemented. A good S-box should satisfy the SAC to ensure that each output bit depends on each input bit.

1.10. Branch Number

This is a measure of the cryptographic strength of an S-box and is related to the number of active S-box output bits when a single input bit is complemented.

1.11. Resistance Against Algebraic Attacks

S-boxes should be designed to resist algebraic attacks, where an attacker models the cryptographic algorithm as a system of equations to derive the secret key.

1.12. Security Against Side-Channel Attacks

S-boxes should also be resistant to side-channel attacks, which exploit information leaked during the cryptographic computation, such as timing information or power consumption.

1.13. Statistical Properties

S-boxes should exhibit good statistical properties, including a balanced distribution of output values and resistance against bias.

1.14. Efficiency

S-boxes should be computationally efficient to ensure that the crypto- graphic algorithm remains practical for real-world applications.

These criteria help ensure that S-boxes provide a high level of confusion and diffusion, making it difficult for attackers to deduce information about the cryptographic key or plaintext from the ciphertext. S-box design is often a complex task that involves a balance between these various criteria. Re- searchers continually explore new methods and techniques to design secure and efficient S-boxes for cryptographic applications[9].

Quantum Key Distribution :

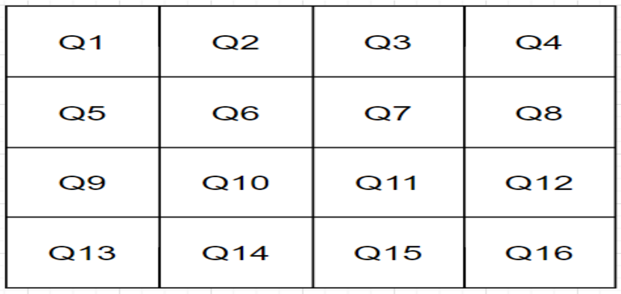
Quantum Key Distribution (QKD) is an encryption technology that uses the principles of quantum mechanics to create secure communications be- tween two parties. In QKD (commonly known as Alice and Bob), quantum particles (such as photons) are used to create a coherent system. The key consists of a quantum of these particles, and any attempt by an eavesdrop- per to tamper with the key can be detected due to the principles of quantum mechanics[10]. QKD provides data security by ensuring the confidentiality of keys and preventing computer attacks. Security keys obtained from QKD can be used to encrypt and decrypt messages, providing a secure means of communication that is resistant to traditional attacks.

Quantum Key Distribution (QKD) uses the principles of quantum mechanics to play a role-changing role in the creation of S-boxes for image encryption. Use special quantum properties such as superposition and entanglement to create eavesdropping-resistant keys based on the quantum uncertainty principle. The security key generated by the quantum channel can be used to create the S-box, which is the key in the image encryption algorithm. Quantum security S-box improves the overall security of the im- age encryption process and provides an effective way to improve the real-time confidentiality and adaptation of quantum computing of sensitive image data.

Proposed Method :

1.1. Generation of s-box using Quantum computing

Visuals are often used to represent most information because they contain more detailed information. Digital images can be protected using image encryption methods, where S-boxes are commonly used in image encryption systems. The proposed method was used to create s-boxes, which is an important step in the AES algorithm. The only non-linear part of the Advanced Encryption Standard (AES) is the s-box (Substitution Box), which makes the algorithm confusing. Therefore s-box should be as complex as possible. Here, quantum computing is used to create the s-box. Quantum computing is a technology that uses quantum mechanics to make calculations faster, more efficient and less complex. In addition, special properties of quantum mechanics are used to increase the stability of image data. The s-box created using the quantum key is used to XOR with the plaintext image to create the encrypted quantum image. Quantum encryption has high performance, low complexity and large key space.



Q1	Q2	Q3	Q4
Q5	Q6	Q7	Q8
Q9	Q10	Q11	Q12
Q13	Q14	Q15	Q16

Figure 1: Quantum based s-box

1.2. Key generation using Quantum computing

There are many important methods in quantum computing in which quantum key distribution (QKD) is quite successful. Quantum Key Distribution (QKD) is a method in quantum computing that allows two parties (usually called Alice and Bob) to generate a secure encryption key over an unsecured communication channel. Quantum Key Distribution (QKD) is an effective method for secure key exchange in the quantum domain. In image encryption using quantum keys, the QKD process involves the exchange of qubits or qubits. The quantum properties of these objects ensure that any at- tempt to eavesdrop on communications is detectable. When creating a secure quantum key, image encryption can be performed using classical encryption algorithms as a quantum-generated key. Keys generated by QKD are secure against any form of computing power, including quantum computers, and provide a way to detect eavesdropping.

Here, the plaintext image is XORed with the generated quantum key to create a quantum encrypted image.

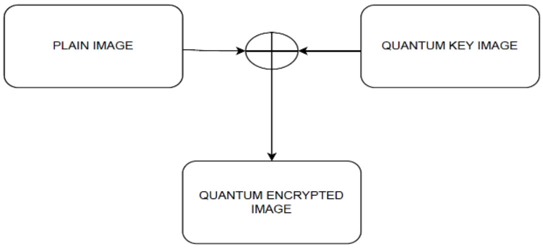


Figure 2: Quantum Encrypted image using Quantum Keying

Conclusion :

Quantum computing offers unprecedented potential for enhancing image encryption techniques. Its unique ability to process vast amounts of data simultaneously through quantum bits (qubits) presents a paradigm shift in cryptography. Leveraging quantum entanglement and superposition, quantum image encryption methods promise heightened security, surpassing classical algorithms. Quantum computing has the potential to revolutionize im- age encryption by using the principles of quantum mechanics to enhance both key generation and encryption processes. One significant advancement is the concept of quantum-encrypted images, where quantum states are utilized to encode image information securely. Using quantum key distribution to protect transactions against cryptographic threats. Although quantum image encryption is still in its infancy, research holds the promise of revolutionizing data protection. As quantum technology advances, it has become necessary to resolve the potential negative and create a strong quantum-resistant encryption method. The intersection of quantum computing and image encryption is an exciting way to protect data from obfuscation. The foundation of the quantum revolution in image encryption is quantum key distribution (QKD), a break- through technology for generating secure encryption keys. Unlike traditional key exchange methods, QKD uses quantum mechanical principles such as the non-cloning theorem and gate controllers to create a secure communication system. Secure distribution of quantum keys not only protects the confidentiality of images, also ensures the integrity of the communication channel and provides a great path for the future of quantum secure image encryption.

Quantum Key Distribution (QKD) looks set to replace image encryption and provides unparalleled security in the quantum domain. QKD enables secure transactions by leveraging the principles of quantum mechanics and is immune to eavesdropping attempts due to the principles of quantum superposition and entanglement. The integration of QKD into image encryption lays the foundation for the next level of data protection, especially in the face of the impending quantum threat to the experience of classical encryption methods With the continuous development of quantum technology, QKD not only improves the ability of image encryption to protect against today's risks, but also quantum It provides strong anti-quantum security, creating a new era in security communication protocol. Based on the principles of superposition and entanglement, quantum encrypted images should have enhanced security against both classical and quantum threats. Quantum key distribution has completely changed the basis of encryption key generation by providing an inherently secure channel for key exchange in image encryption. The integration of quantum S-box uses the symbolic computing power provided by quantum computing to increase the security of classical encryption algorithms. Although these advances are still in their infancy, they pave the way for a future in which quantum technologies will play an important role in protecting the privacy and integrity of devices found in the digital world.

REFERENCES :

1. Hadj Brahim, A. Ali Pacha, N. Hadj Said, An image encryption scheme based on a modified aes algorithm by using a variable s-box, Journal of Optics (2023) 1–16.
2. H. Susanto, A. Alamsyah, A. T. Putra, Security improvement of the 256-bit aes algorithm with dynamic s-box based on static parameter as the key for s-box formation, Journal of Advances in Information Systems and Technology 4 (1) (2022) 33–41.
3. M. S. M. Malik, M. A. Ali, M. A. Khan, M. Ehatisham-Ul-Haq, S. N. M. Shah, M. Rehman, W. Ahmad, Generation of highly nonlinear and dy- namic aes substitution-boxes (s-boxes) using chaos-based rotational ma- trices, IEEE Access 8 (2020) 35682–35695.
4. Singh, P. Agarwal, M. Chand, Analysis of development of dynamic s-box generation, Comput. Sci. Inf. Technol 5 (5) (2017) 154–163.
5. V. Nandan, R. Gowri Shankar Rao, Low-power and area-efficient design of aes s-box using enhanced transformation method for security appli- cation, International Journal of Communication Systems 35 (2) (2022) e4308.
6. P. Deshmukh, An image encryption and decryption using aes algorithm, International Journal of Scientific & Engineering Research 7 (2) (2016) 210–213.
7. R. S. Salman, A. K. Farhan, A. Shakir, Creation of s-box based one- dimensional chaotic logistic map: Colour image encryption approach, Int. J. Intell. Eng. Syst 15 (5) (2022) 2022.
8. P. Rajendran, D. K. Sadhasivam, Multi-level attack with dynamic s-box variable key pattern generation for key cohort using aes.
9. Singh, P. Agarwal, M. Chand, Image encryption and analysis using dynamic aes, in: 2019 5th international conference on optimization and applications (ICOA), IEEE, 2019, pp. 1–6.
10. R. Saini, B. K. Behera, H. Abulkasim, P. Tiwari, A. Farouk, Efficient quantum image encryption technique for securing multimedia applica- tions, arXiv preprint arXiv:2204.07996 (2022).