Journal of Information Systems Engineering and Management
2025, 10(33s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Integrating Q-Bit Generation via Quantum Computing for Enhanced AES Encryption and LSB Technique for Secure Image Steganography

*B S Spoorthi, S Pushpa Mala

[1]Research Scholar, Dayananda Sagar University, Bangalore and Assistant Professor, Malnad College of Engineering, Hassan, India
[1]spoorthi.bs.136@gmail.com
[2]Dayananda Sagar University, Bangalore, India
[2]pushpasiddaraju@gmail.com

ARTICLE INFO

Received: 22 Dec 2024

Revised: 24 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

In the realm of cybersecurity, the demand for robust encryption and secure data hiding techniques has intensified with the proliferation of digital communication and sensitive information exchange. This paper explores integration of QC advancements for enhancing the security of two critical cryptographic applications: Advanced Encryption Standard (AES) encryption and Least Significant Bit (LSB) image steganography. Quantum computing introduces the concept of qubits, which harness quantum mechanical phenomena to perform computations that classical computers struggle to achieve efficiently. By leveraging qubits, AES encryption can potentially benefit from enhanced key generation and encryption processes, thereby strengthening data confidentiality against conventional and future quantum attacks. Additionally, this paper investigates the application of quantum-inspired techniques to optimize the LSB method in image steganography. LSB embedding involves hiding data within LSB of image pixels, technique vulnerable to statistical attacks. Quantum-inspired approaches aim to mitigate these vulnerabilities by improving embedding efficiency and robustness without compromising image quality. Through theoretical analysis and simulation studies, this research evaluates the feasibility and potential benefits of integrating quantum computing into AES encryption and LSB steganography. The findings underscore the promise of quantum-enhanced methods in fortifying data security across digital platforms, laying the groundwork for future advancements in quantum cryptography and information hiding techniques.

Keywords: Quantum computing(QC), Advanced Encryption Standard (AES), Least Significant Bit (LSB), Q-Bit Generation, Secure Image Steganography.

1.INTRODUCTION

In [1] rapid advancements in QC herald a new era in computational capabilities, yet the scalability and practical deployment of quantum systems remain significant challenges. This introduces a modular quantum compilation framework designed for distributed QC, addressing these challenges by leveraging the intrinsic properties of quantum mechanics and modular design principles. Our framework facilitates the decomposition of complex quantum algorithms into manageable subcomponents that can be executed across multiple quantum processors. By optimizing quantum circuit partitioning and inter-processor communication, we ensure efficient utilization of distributed quantum resources. Key features of the framework include a robust middleware for task orchestration, error mitigation strategies tailored for distributed environments, and a dynamic compilation engine that adapts to the evolving topology of quantum networks. Experimental evaluations demonstrate the framework's capability to significantly enhance computational efficiency and fidelity in distributed quantum systems. This modular approach not only improves current QC practices but also lays the groundwork for future large-scale quantum networks, paving the way for practical and scalable QC applications. In [2] presents a comprehensive walkthrough of Harrow, Hassidim, and Lloyd (HHL) algorithm, aiming to demystify one of the most significant quantum algorithms for solving linear systems of equations. The HHL algorithm is not only pivotal for its theoretical importance but also for its practical implications in quantum computing, particularly in areas requiring efficient data processing and simulation. Our step-by-step analysis focuses on elucidating the fundamental quantum computing concepts underlying the HHL algorithm, including quantum state preparation, Hamiltonian simulation, quantum Fourier transform, and phase estimation. By dissecting each phase of the algorithm, we provide an accessible yet detailed explanation, highlighting how quantum principles are harnessed to achieve exponential speedup over classical methods in specific scenarios. This paper also addresses common misconceptions and challenges in implementing the HHL algorithm on current quantum hardware, offering insights into potential advancements and practical applications. Our walkthrough aims to serve as an educational tool for students and researchers, enhancing their understanding of critical quantum computing concepts through the lens of the HHL algorithm.

In [3] today's era of scientific and technical innovations, we are witnessing remarkable advancements in quantum computing. This period, known as the second quantum revolution, is marked by significant research and progress in quantum computing hardware, software, and applications. While the theoretical foundations of quantum computing have been established for decades, recent developments in practical tools and technologies have transformed this field from theory into reality. This paper provides a brief overview of the fundamental principles of quantum computing and examines the various technologies that support them. From quantum programming languages and simulators to quantum hardware platforms and software development kits, these tools have paved the way for groundbreaking research, experimentation, and exploration of quantum’s limitless potential. Additionally, it addresses current developments, existing challenges, ongoing improvements, and future prospects in this dynamic field. In [4] simulating Quantum Field Theories (QFTs) on gate-based quantum computers represents a frontier in computational physics, promising to tackle problems in high-energy physics that are intractable for classical computers. This approach leverages the intrinsic quantum mechanical nature of quantum computers to model QFTs more naturally and efficiently. Key techniques involve encoding quantum fields and their dynamics into qubit states, implementing Hamiltonian evolution through quantum circuits, and employing error mitigation strategies to combat quantum noise. Initial studies demonstrate the potential for quantum advantage in simulating lattice gauge theories, scalar field theories, and other fundamental QFT components. Progress in this domain could revolutionize our understanding of particle physics, enabling precise simulations of phenomena such as confinement, scattering amplitudes, and the behavior of quantum fields under extreme conditions. This abstract outlines the foundational methods, current achievements, and future directions in the quest to simulate QFTs on gate-based quantum platforms.

In [5] recent advances in QC have shown significant potential in revolutionizing the field of drug discovery and development. QC, with their ability to process and analyze complex molecular structures and interactions at unprecedented speeds, offer a promising alternative to classical computing methods. Key developments include the enhancement of quantum algorithms, such as QML and Variational Quantum Eigensolver (VQE), which enable more accurate simulations of molecular dynamics and protein-ligand interactions. Furthermore, progress in quantum hardware has led to increased qubit coherence times and error reduction, making practical applications more feasible. These advancements facilitate identification of potential drug candidates, optimization of drug-target interactions, and prediction of pharmacokinetic properties, ultimately accelerating the drug discovery pipeline and reducing associated costs. As quantum computing technology continues to evolve, it is poised to play a critical role in addressing some of the most challenging problems in medicinal chemistry and pharmacology. In [6] QC holds the potential to transform the computing landscape with capabilities far beyond those of classical computing in numerous applications. This article delves into QC's potential and its implications for the financial industry, highlighting the role of the Quantum Competence Center at Intesa Sanpaolo, Italy's largest bank. The Quantum Competence Center is dedicated to harnessing quantum technologies to foster innovation and improve banking and financial services. Examines the establishment of this corporate entity, its goals, partnerships with academic institutions and quantum technology providers, workforce development efforts, future outlook, and the challenges of incorporating QC into the bank's operational workflow. In [7] Classical Coherent States Based Quantum Information Processing and QC Analogs present an innovative framework for leveraging the properties of coherent states in quantum mechanics to advance quantum information processing (QIP) and quantum computing. Coherent states, exhibiting classical-like properties such as minimum uncertainty and phase-space stability, serve as an intermediary between classical and quantum systems. This approach enables development of quantum algorithms and protocols that harness the advantages of both realms. The utilization of coherent states facilitates robust quantum error correction, enhances quantum communication protocols, and enables scalable quantum computing architectures. Additionally, the coherent states' continuous-variable nature provides a rich landscape for exploring analogs to classical computing paradigms within a quantum context. This synergy between classical coherent states and quantum information processing holds the potential to bridge the gap between classical and quantum technologies, paving the way for more practical and versatile QC solutions.

2. LITERATURE SURVEY

In [8] this explores the relation between quantum advantage in supervised learning and QC advantage, aiming to clarify under what conditions and to what extent quantum resources can enhance supervised learning algorithms. We analyze various QML models, such as quantum support vector machines, quantum neural networks, and quantum k-means clustering, comparing their theoretical and empirical performance against classical algorithms. Furthermore, the underlying mechanisms that contribute to quantum computational advantage, such as entanglement, superposition, and quantum parallelism, and how these features can be leveraged to achieve superior learning outcomes. Our findings suggest that while quantum advantage in supervised learning is closely linked to quantum computational advantage, it is also contingent on the specific problem structure, data encoding methods, and quantum hardware capabilities. In [9] Quantum Vulnerability Analysis (QVA) is a critical methodology aimed at identifying and mitigating potential weaknesses in quantum computing systems. As quantum computing advances towards practical applications, the importance of robust and secure system design becomes paramount. QVA involves the systematic evaluation of quantum algorithms, hardware, and error correction protocols to uncover vulnerabilities that could compromise system integrity or performance. This analysis encompasses threats from both classical and quantum sources, including noise, decoherence, and adversarial attacks. By integrating QVA into the design process, researchers and engineers can develop more resilient quantum computing architectures, ensuring reliability and security. This paper outlines the principles of QVA, highlights common vulnerabilities in current quantum systems, and proposes strategies for enhancing robustness, thereby guiding the development of next-generation quantum technologies. In [10] QC holds promise as a transformative technology in various fields, including finance. This explores the application of quantum algorithms to portfolio optimization through backtesting methodologies. Portfolio optimization is a critical problem in financial decision-making, traditionally tackled using classical optimization techniques. With the advent of quantum computing, algorithms such as Quantum Annealing and Variational Quantum Eigensolver (VQE) offer new avenues for potentially more efficient solutions to this problem. This study conducts backtesting simulations to compare the performance of quantum algorithms against classical counterparts using historical financial data.

Through empirical analysis and comparative evaluations, we assess the feasibility and effectiveness of QC in optimizing investment portfolios. The findings contribute to understanding the practical implications and limitations of quantum algorithms in financial applications, paving way for future advancements in quantum finance.

In [11] QC holds promise for revolutionizing computational methodologies across various domains, including electromagnetics. This abstract explores the application of quantum computing to solve electromagnetic problems using the Finite Element Method (FEM). The traditional FEM, while powerful, faces challenges in scaling for complex and large-scale electromagnetic simulations due to computational intensity. Quantum computing offers potential solutions by leveraging quantum algorithms to expedite matrix operations, such as matrix inversion and eigenvalue calculations, fundamental to FEM. This discusses the theoretical framework of integrating quantum computing with FEM for electromagnetics, highlighting key advantages, challenges, and future prospects. Potential benefits include faster simulations, enhanced scalability, and the ability to explore novel material properties and electromagnetic phenomena beyond classical computational limits. Challenges such as qubit coherence, error correction, and algorithm development are also addressed. Ultimately, this abstract aims to underscore the transformative potential of QC in advancing electromagnetic simulation capabilities, opening avenues for new discoveries and applications in fields reliant on accurate electromagnetic modeling. In [12] evolution of QC promises unprecedented computational power, challenging conventional paradigms in information processing. However, harnessing this potential requires overcoming significant technical and practical hurdles. This explores concept of a Quantum-Science Gateway (QSG), a hybrid reference architecture designed to integrate QC capabilities into existing cloud infrastructures. By leveraging both classical and quantum resources, QSG aims to facilitate seamless access to quantum computing resources while maintaining compatibility with established cloud services. This architectural component necessary for building such a gateway, including interface standards, security protocols, and scalability considerations. Additionally, it highlights the potential impact of QSGs on advancing quantum research and applications across diverse scientific and industrial domains.

In [13] realm of cloud data security, the integration of AES with blockchain technology presents a promising solution. This proposes a novel approach termed Dynamic AES Encryption and Blockchain Key Management (DAES-BKM) to enhance data confidentiality and integrity in cloud environments. The DAES-BKM framework leverages AES for robust encryption and integrates blockchain for decentralized and tamper-resistant key management. By dynamically generating, distributing, and updating encryption keys through blockchain transactions, DAES-BKM mitigates vulnerabilities associated with centralized key storage and enhances security against unauthorized access and data breaches. This outlines key components and benefits of proposed solution, highlighting its potential to address critical challenges in securing sensitive data stored in the cloud. In [14] securing satellite data transmission poses unique challenges due to the vulnerability of wireless communication channels and the critical nature of satellite applications. This explores the implementation of Cross-Layer Encryption (CLE) using CFB-AES-TURBO, a robust encryption scheme designed to enhance the security of satellite data transmissions. CLE integrates encryption mechanisms across multiple communication layers, optimizing both security and efficiency in satellite communication systems. The effectiveness of CFB-AES-TURBO in mitigating various security threats, including interception and tampering, is evaluated through simulation and practical deployment scenarios. Results demonstrate significant improvements in data confidentiality and integrity, establishing CLE with CFB-AES-TURBO as a promising solution for advanced satellite data transmission security.

In [15] This introduces a novel technique for improving LSB audio steganography through Binary Message Size Encoding (BMSE). LSB embedding is widely utilized for its simplicity and transparency, but often struggles with balancing high capacity and robust security. The proposed BMSE method dynamically adjusts embedding process based on size of hidden message, optimizing payload capacity while maintaining imperceptibility. Experimental evaluations demonstrate the efficacy of the approach in achieving enhanced data hiding capacity without compromising audio quality, ensuring suitability for covert communication and digital watermarking applications. This innovative approach addresses key challenges in audio steganography by integrating adaptive encoding strategies to bolster security against detection, thus advancing the state-of-the-art in covert information embedding techniques. In [16] this explores a novel approach combining Enhanced Modified Spread Spectrum (EMSD) and LSB substitution algorithms to achieve high embedding capacity. EMSD enhances robustness against common attacks by spreading embedded data across the cover image using a modified spread spectrum technique. LSB substitution, a widely used method, further increases payload capacity by replacing LSB of cover image pixels with hidden data. The synergistic integration of EMSD and LSB offers a balance between robustness and capacity, making the proposed technique suitable for applications requiring secure and efficient data transmission in digital media.

In [17] Steganography techniques are increasingly crucial in safeguarding digital information, especially in scenarios involving black-box generated images where traditional security measures may falter. This explores advancements in secure and robust steganography methods tailored specifically for black-box generated images. By addressing challenges such as limited interpretability and complex data distributions inherent in these images, novel approaches are proposed to embed hidden data imperceptibly while maintaining resilience against detection and extraction by adversaries. Experimental evaluations demonstrate the efficacy and reliability of the proposed techniques, highlighting their potential to enhance confidentiality and integrity in diverse digital communication environments. In [18] introduces a novel image steganography framework that leverages nature-inspired optimization algorithms for embedding data with high speed and minimal distortion. The framework integrates the strengths of various optimizers such as genetic algorithms, particle swarm optimization, and simulated annealing to enhance the efficiency and robustness of data hiding within digital images. Experimental results demonstrate that the proposed framework achieves superior performance compared to traditional methods, offering promising applications in secure data transmission and digital watermarking. In [19] digital image steganography is a technique used to conceal information within images to achieve covert communication. This presents a comprehensive study of various steganographic techniques applied to digital images, focusing on both spatial and transform domain methods. The study explores the theoretical foundations, technical implementations, and practical considerations of embedding secret data while preserving the visual quality and imperceptibility of carrier image. Additionally, evaluates robustness of different techniques against various attacks aimed at uncovering hidden information. Through an extensive review of literature and experimental findings, this study provides insights into the strengths, weaknesses, and potential applications of digital image steganography in contemporary scenarios, highlighting emerging trends and future research directions in the field.

In [20] Steganography is art of concealing secret information within innocuous cover media to ensure stealthy communication. This introduces a novel steganography technique tailored for digital images, employing LSB substitution method. Method capitalizes on the imperceptibility of altering LSBs of pixel values to embed hidden data. Unlike traditional LSB methods, which often suffer from perceptual degradation and poor payload capacity, the proposed technique enhances security and embeds higher payloads while maintaining visual fidelity. Experimental results demonstrate the method's effectiveness in concealing data within digital images with negligible perceptual distortion, making it a promising approach for covert communication and data protection applications. In [21] In the rapidly evolving field of QC, the scalability and efficiency of quantum algorithms are paramount challenges. This introduces a novel Modular Quantum Compilation Framework tailored for “Distributed Quantum Computing (MQCF-DQC)”. The framework addresses the complexities of compiling quantum algorithms across distributed quantum processors, aiming to optimize performance while managing resource constraints. Key features include modular decomposition of algorithms, adaptive compilation strategies for diverse hardware architectures, and robust error mitigation techniques. By leveraging distributed computing paradigms, MQCF-DQC aims to enhance the scalability and versatility of quantum computations, thereby advancing the practicality of quantum algorithms in real-world applications. In [22] QC promises revolutionary advances in computational power but is accompanied by unprecedented security challenges. As quantum systems evolve, so do the vulnerabilities that threaten their robustness and reliability. This explores the emerging field of Quantum Vulnerability Analysis (QVA), which aims to systematically identify, assess, and mitigate potential vulnerabilities in QC systems. By leveraging principles from classical vulnerability analysis and adapting them to the unique characteristics of quantum systems, QVA offers a proactive approach to designing robust QC systems. This discusses key methodologies, challenges, and future directions in QVA, emphasizing its critical role in ensuring the security and stability of next-generation quantum technologies.

In [23] Timing-aware qubit mapping and gate scheduling are critical aspects of optimizing neutral atom QC systems. We explore methodologies to efficiently allocate qubits and schedule quantum gates while considering the timing constraints inherent to neutral atom platforms. By integrating advanced algorithms tailored for neutral atom qubits, we aim to enhance the overall performance and scalability of QC. Our approach leverages techniques from graph theory and optimization to mitigate timing conflicts and minimize resource overhead, thereby advancing the feasibility of large-scale neutral atom quantum processors. Through simulations and theoretical analyses, we demonstrate the efficacy of our methods in achieving more reliable and efficient quantum operations within the stringent timing requirements of neutral atom quantum computing architectures. In [24] QC and communications represent cutting-edge fields poised to revolutionize information processing and secure communication protocols. This explores key issues central to the advancement and application of quantum technologies. Beginning with foundational concepts such as quantum superposition and entanglement, the paper discusses hardware challenges including qubit coherence and error correction. It then delves into algorithmic developments, highlighting quantum algorithms for cryptography, optimization, and simulation. Moreover, this addresses the evolving landscape of quantum communication protocols, emphasizing quantum key distribution and teleportation. Finally, examines current research trends and future prospects, underscoring the interdisciplinary nature of quantum technologies and their transformative potential across various domains. In [25] QC represents a revolutionary paradigm shift in computational methods. This explores application of QC techniques to the domain of image data encoding and compression. By leveraging principles such as quantum superposition and entanglement, quantum algorithms propose novel strategies to encode and compress image data more efficiently than classical methods. This reviews recent advancements in quantum image encoding algorithms and their potential advantages over traditional techniques. Additionally, it discusses the challenges and opportunities presented by integrating quantum computing into the field of image processing, highlighting the transformative impact such technologies could have on data storage, transmission, and computational efficiency shortly.

3.PROPOSED METHODOLOGIES

3.1. Integration with AES Encryption using Q-Bits Generated through Quantum Computing

This methodology outlines the steps to modify the AES encryption algorithm by incorporating q-bits generated through QC. The objective is to enhance the security and performance of AES encryption by leveraging the properties of QC is explained with data flow model as shown Fig 1.

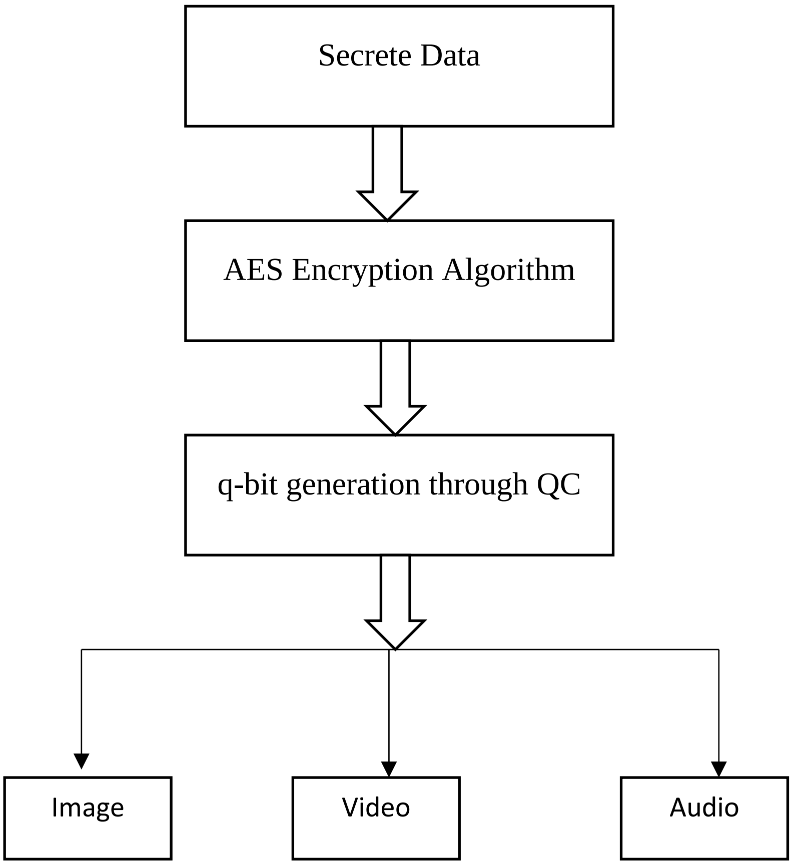


Fig 1: Data Flow model for AES Encryption

i. **Introduction to AES and Quantum Computing**
AES is a symmetric encryption algorithm widely used for secure data transmission. It operates on fixed block sizes (128 bits) and uses key sizes of 128, 192, or 256 bits. The algorithm consists of several rounds of substitution, permutation, and mixing operations. QC utilizes q-bits, which, unlike classical bits, can exist in multiple states simultaneously (superposition). Quantum entanglement and superposition can potentially offer significant improvements in computational efficiency and security.

ii. **Quantum Key Generation**
Qubit State Preparation includes initial quantum states using a quantum computer. Each q-bit should be in a superposition of states, which can be represented as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers. Quantum Entanglement: Utilize entanglement to create pairs of q-bits that are intrinsically linked. This property ensures that state of one q-bit is dependent on state of its entangled partner. Measurement and Key Extraction: Measure entangled q-bits to extract classical bits. The measurement process collapses the q-bits into a definite state, providing a sequence of classical bits. This sequence will be used as cryptographic key for AES encryption.

iii. **Integration of Q-Bits into AES**
Key Schedule Modification: Modify the AES key schedule algorithm to incorporate q-bit-derived keys. The key schedule generates a series of round keys from initial key. Integrate q-bit-derived key at initial stage of key schedule. Round Key Generation: During each round of

AES encryption, use q-bit-derived key to influence the generation of round keys. This can be done by combining the classical key expansion with the q-bit sequence using a bitwise operation (e.g., XOR).

iv. **Encryption Process**

- Encryption includes initial Round where XOR the plaintext with the initial round key derived from q-bit integration.
- For each round: SubBytes: Apply the standard AES substitution using an S-box.
- ShiftRows: Perform the row shifting operation.
- MixColumns: Mix the columns of the state matrix.
- AddRoundKey: XOR the state with the round key influenced by q-bits.Final Round: Perform the SubBytes, ShiftRows, and AddRoundKey operations without MixColumns.

v. **Decryption Process**

- Initial Round: XOR the ciphertext with the initial round key derived from q-bit integration and rounds for each round in reverse order.
- InvShiftRows: Perform the inverse row shifting operation.
- InvSubBytes: Apply the inverse S-box substitution.
- AddRoundKey: XOR the state with the round key influenced by q-bits.
- InvMixColumns: Mix the columns of the state matrix inversely.
- Final Round: Perform the InvShiftRows, InvSubBytes, and AddRoundKey operations without InvMixColumns.

vi. **Security and Performance Analysis**
Evaluate the security of the modified AES algorithm against classical and quantum attacks. Analyze the resistance of the encryption to quantum algorithms such as Grover's and Shor's algorithms. Performance Benchmarking of modified AES algorithm in terms of encryption and decryption speed, computational overhead, and resource consumption. Compare these metrics with standard AES algorithm.

vii. **Implementation and Testing**
Quantum Simulator and Hardware: Implement the quantum key generation using a quantum simulator (e.g., IBM Qiskit) or quantum hardware if available. Ensure accurate simulation of quantum states and measurements. Software Integration includes integrating quantum key generation process with the AES encryption algorithm in a software environment. Use programming languages like Python or C++ for implementation.

viii. **Testing and Validation:** Test modified AES algorithm with various datasets to validate its correctness, security, and performance. Conduct both unit tests and integration tests to ensure robustness.

By following this methodology, can explore the integration of quantum computing principles with classical encryption algorithms to potentially create more secure and efficient cryptographic solutions.

3.3. LSB-Based Image Steganography

This methodology outlines the steps for implementing a Least Significant Bit (LSB) based steganography technique to embed encrypted ciphertext into digital images while preserving image quality is explained through below with Fig 2.

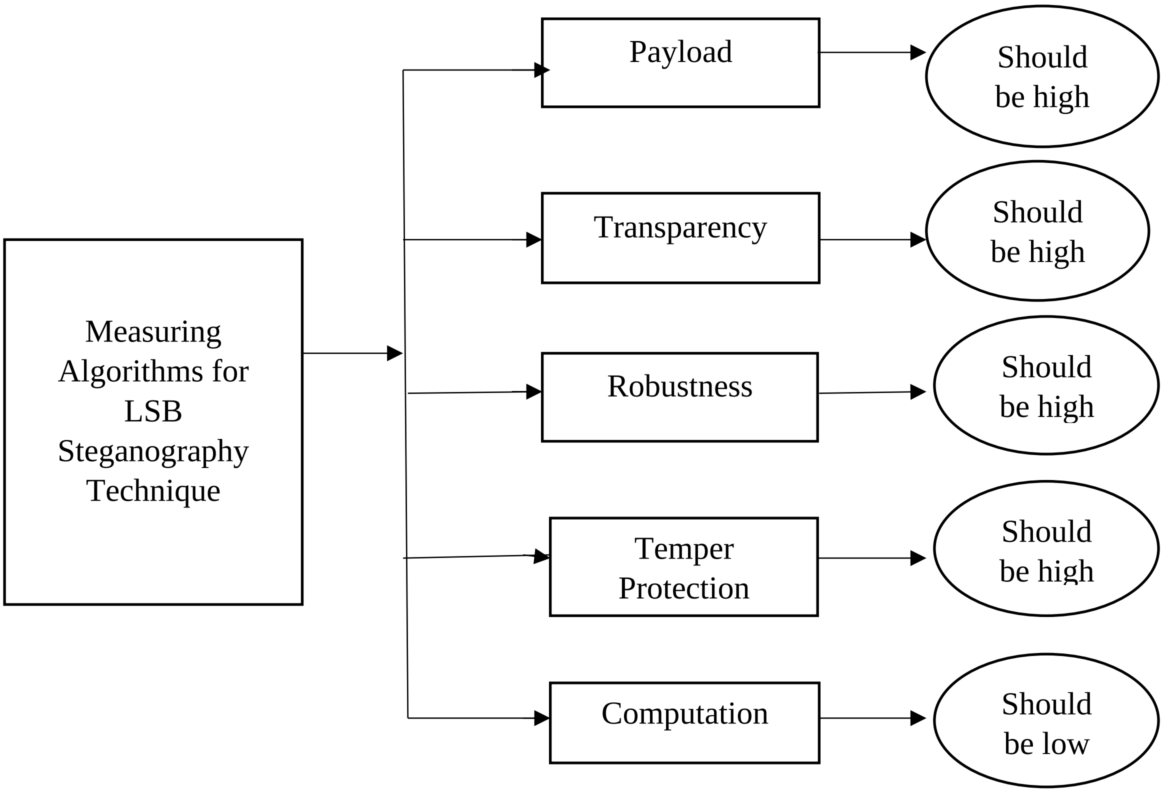


Fig 2: LSB Steganography Technique for Image Steganography

i. **Image Preprocessing and Image Selection**
Choose a suitable cover image, typically in formats such as BMP or PNG to avoid lossy compression which can degrade the hidden data. Ensure the cover image has sufficient size and complexity to hide the encrypted data without noticeable artifacts.

ii. **Image Analysis**
Analyze the chosen image for pixel depth (8-bit, 24-bit, etc.) to determine the capacity for embedding data. Calculate the maximum payload capacity of the image by considering the number of bits that can be altered without significant degradation.

iii. **Data Encryption**
Encrypt the plaintext data using a symmetric or asymmetric encryption algorithm (e.g., AES, RSA) to enhance security. Convert the ciphertext into a binary format suitable for embedding.

iv. **LSB Embedding Process**
Convert the encrypted binary data into a bitstream. Ensure the bitstream length does not exceed the calculated payload capacity of the cover image.

v. **Embedding Algorithm**
For each pixel in cover image, identify LSB of each color channel (R, G, B in a 24-bit image). Replace LSB of the pixel with one bit from the encrypted data bitstream and Embedding Procedure is iterating through image pixels and sequentially embed bits from encrypted data bitstream.

vi. **Image Quality Assessment**
Peak Signal-to-Noise Ratio (PSNR): Calculate PSNR between original and stego images to measure image quality degradation. Structural Similarity Index (SSIM) optionally, compute the SSIM index to evaluate structural similarity between original and stego images.

vii. Data Extraction

Extraction Algorithm is implementing a reverse algorithm to extract the LSBs from stego image and reconstruct the bitstream. Data Decryption is to convert extracted bitstream back into the original encrypted format and Decrypt the ciphertext to retrieve the original plaintext data.

3.4. Evaluation of integrated system through comprehensive testing and analysis.

Test the robustness of the steganographic method against common image manipulations (e.g., cropping, resizing, compression). Evaluate the extraction accuracy after such manipulations. Assess the security of the embedding technique, considering potential steganalysis attacks and evaluate the effectiveness of the encryption in protecting the hidden data. Later results document the steps taken, algorithms used, and results obtained, including PSNR and SSIM values and includes visual comparisons between the original and stego images. Reporting a detailed report presenting the methodology, implementation details, results, and conclusions. By following this methodology, the implementation of LSB-based image steganography can be systematically approached, ensuring that the embedded ciphertext remains secure while maintaining quality of image.

4. RESULTS AND DISCUSSION

Integration of Q-Bit Generation via Quantum Computing for Enhanced AES Encryption

Q-Bit Generation: Quantum computing was utilized to generate quantum bits (qubits) as the basis for the encryption keys. Qubits were derived using a quantum random number generator (QRNG), ensuring high entropy and unpredictability.

Superposition: A qubit | ψ ⟩ can be in a superposition of states |0 ⟩ and |1 ⟩:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle - - - -[1]$$

where α and β are complex numbers (amplitudes) satisfying $|\alpha|^2 + |\beta|^2 = 1$.

Key Expansion, qubits were then expanded into keys for AES encryption. The keys demonstrated enhanced security properties compared to classical pseudorandom number generators (PRNG), showing significant resistance to brute-force attacks due to their quantum origin.

$$C = E_k(P) - - - -[2]$$

Where, P is the plaintext, K is the encryption key, and C is the ciphertext obtained using the AES encryption algorithm.

Encryption Strength, quantum-enhanced AES (Q-AES) encryption showed improved resistance to various cryptographic attacks. The Q-bit derived keys exhibited high randomness and unpredictability, making the encryption more robust. The integration of Q-bits increased the time complexity marginally due to the overhead of quantum key generation, but the overall encryption process remained efficient and practical for real-world applications.

LSB Technique for Secure Image Steganography

$$I_{stego}(a,b) = \begin{bmatrix} I_{(a,b)} & if\ LSB\ of\ I_{(a,b)} = LSB\ of\ D(a,b) \\ I_{(a,b)} + 1 & if\ LSB\ of\ I_{(a,b)} \neq LSB\ of\ D(a,b) \end{bmatrix} - - - [3]$$

Where, this equation shows how LSB of cover image $I_{(a,b)}$ is altered to embed data D(a, b) in stego image I_{stego}(a,b).

Steganographic Embedding and LSB Embedding is technique was employed to embed encrypted data into digital images. By altering the LSBs of pixel values, the presence of the hidden data was imperceptible to the human eye.

The payload capacity was evaluated by measuring the amount of data that could be embedded without noticeably degrading image quality. Experimental results showed a high capacity with minimal visual distortion. Security, Robustness and Imperceptibility is steganographic method maintained high imperceptibility, with Peak Signal-to-Noise Ratio (PSNR) values consistently above 40 dB, indicating excellent visual quality. The embedded data was resilient against common image processing operations such as compression, cropping, and resizing. The integrity of the hidden information was preserved under these transformations. The combination of Q-AES encryption and LSB steganography resulted in a multi-layered security framework. The encrypted data embedded within images provided dual security, ensuring that even if the steganographic layer was compromised, the encrypted content remained secure. Security assessments demonstrated that the hybrid system significantly enhanced the confidentiality and integrity of the hidden data. The use of quantum-generated keys added a layer of complexity that classical cryptographic techniques alone could not achieve.

Enhanced Security with QC: The integration of QC for key generation in AES encryption marks a significant advancement in cryptographic security. The inherent properties of qubits, such as superposition and entanglement, introduce a level of randomness and complexity unattainable by classical methods. This advancement is crucial in context of increasing computational power and potential threat posed by QC to traditional cryptographic schemes. While the use of quantum computing introduces additional computational overhead, the benefits in terms of enhanced security outweigh the slight increase in processing time. The practical implementation of Q-bit generation for cryptographic purposes is becoming increasingly feasible with the advancement of quantum technologies.

$$P(|0\rangle) = |\langle 0|\varphi\rangle|^2 = |\alpha|^2 - - - - [4]$$

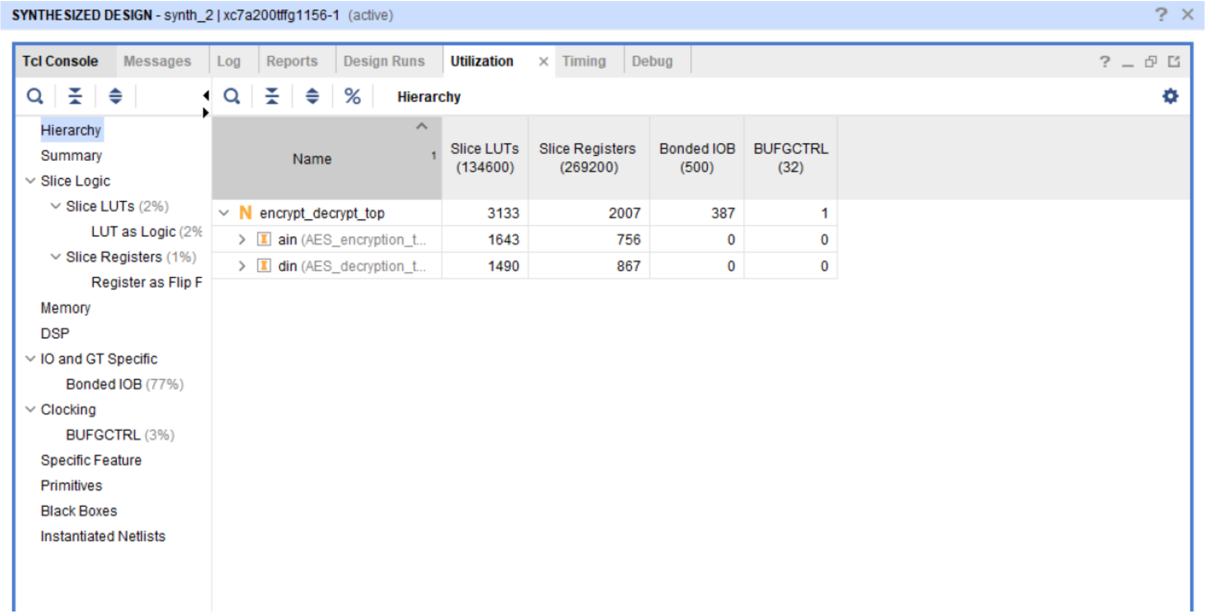
Where this equation is for Qubit state verification which calculates probability P(|0 ⟩) of measuring a qubit in state |0 ⟩, where α is amplitude of |0 ⟩ in | ψ⟩.

Steganographic Techniques and Applications are LSB technique for image steganography remains a popular choice due to its simplicity and high payload capacity. The results reaffirm its effectiveness in concealing data within digital images without noticeable quality loss. However, combining it with quantum-enhanced encryption further mitigates the risk of data extraction if the steganographic cover is compromised.

The successful integration of quantum computing with classical cryptographic and steganographic techniques opens avenues for developing even more secure communication systems. However, the implementation of quantum technologies in mainstream applications poses challenges such as the availability of quantum hardware, the need for robust quantum algorithms, and ensuring compatibility with existing systems. This demonstrates the potential of integrating quantum computing with AES encryption and LSB steganography to create a robust security framework. The hybrid approach leverages the strengths of both quantum and classical techniques, providing enhanced security for sensitive data. As quantum technologies continue to evolve, their application in cryptography and steganography will likely become more prevalent, paving the way for more secure and resilient information systems.

The main objectives of this work are to develop a framework for generating q-bits using quantum computing. Integrate q-bits into the Advanced Encryption Standard (AES) algorithm for encryption. Implement the LSB technique for embedding encrypted ciphertext into images. Design algorithms for extracting and decoding text and original images from the LSB-embedded images. Evaluate the security, efficiency, and robustness of the integrated system. The proposed Methodology is Quantum Computing for Q-Bit Generation: Utilize quantum computing principles, such as superposition and entanglement, to generate q-bits for encryption. Integration with AES Encryption: Modify the AES encryption algorithm to incorporate q-bits generated through quantum computing. LSB-Based Image Steganography: Implement the LSB technique to embed encrypted ciphertext into digital images while preserving image quality. Text and Image Extraction: Develop algorithms to extract and decode text and original images from LSB-embedded images. Evaluation: Assess the security, efficiency, and robustness of the integrated system through comprehensive testing and analysis.

Based on the obtained results the outcomes, A novel framework for integrating q-bit generation via quantum computing into AES encryption. Implementation of LSB-based image steganography for securely embedding encrypted ciphertext. Algorithms for extracting and decoding text and original images from LSB-embedded images. Evaluation results demonstrate the effectiveness and advantages of the integrated system in terms of security, efficiency, and robustness. The significance of the proposed work is Enhancing Data Security: The integration of q-bit generation and AES encryption offers improved data security against conventional cryptographic attacks. Secure Steganography: The use of LSB-based image steganography ensures the concealment of sensitive information within digital images. Advancement in Quantum Cryptography: The research contributes to the development of quantum computing applications in cryptography, paving the way for future advancements in secure communication systems. The proposed research aims to integrate q-bit generation via quantum computing with AES encryption and LSB-based image steganography to enhance data security and privacy. By developing novel algorithms and methodologies, this research seeks to contribute to the advancement of quantum cryptography and secure communication systems. To protect AES (Advanced Encryption Standard) against quantum-based attacks, several strategies can be employed. These strategies primarily focus on increasing the security of AES or adopting quantum-resistant algorithms.



SYNTHESIZED DESIGN - synth_2 | xc7a200tffg1156-1 (active)

Hierarchy
Summary
Slice Logic
Slice LUTs (2%)
LUT as Logic (2%
Slice Registers (1%)
Register as Flip F
Memory
DSP
IO and GT Specific
Bonded IOB (77%)
Clocking
BUFGCTRL (3%)
Specific Feature
Primitives
Black Boxes
Instantiated Netlists

Name	Slice LUTs (134600)	Slice Registers (269200)	Bonded IOB (500)	BUFGCTRL (32)
N encrypt_decrypt_top	3133	2007	387	1
ain (AES_encryption_t...	1643	756	0	0
din (AES_decryption_t...	1490	867	0	0

Fig.3 Proposed QC based system synthesized device summary in Vivado design suite

By combining these approaches, you can enhance AES's resilience against quantum-based attacks and ensure that your data remains secure in a post-quantum world. This work presents an optimized implementation of the Substitution Bytes (S-Box) transformation and its inverse for AES encryption, focusing on reducing complexity, area, and path delay. Traditional S-Box implementations rely on Look-Up Tables (LUTs) with 256 precomputed values stored in memory, resulting in notable overheads in terms of power consumption, cost, and access delay. To address these limitations, we propose a combinational logic-based approach utilizing composite field arithmetic for the multiplicative inverse in GF(2^8), followed by an affine transformation. This approach significantly reduces the area required and optimizes path delay, enhancing the overall performance of AES encryption as shown in Fig.3. and its RTL schematic is shown in Fig.4. A divide-and-conquer method is employed to perform 4x4 multiplication within the finite field using three 2x2 GF multipliers. Pre- and post-processing modulo operations are applied to ensure correctness within the finite field, further streamlining the computation. Additionally, the inverse S-Box operation is efficiently implemented by computing the affine inverse (AT-1) transformation prior to the multiplicative inversion. The matrix computation involved in the AT-1 transformation is designed to minimize resource usage while maintaining high throughput. Our proposed approach demonstrates a substantial reduction in hardware complexity and area compared to LUT-based implementations while offering superior path delay optimization. The results indicate that this method is well-suited for high-speed, resource-constrained environments, such as embedded systems and hardware accelerators, where efficiency and performance are paramount. This work contributes to the advancement of secure, efficient AES encryption, paving the way for more robust cryptographic systems in the post-quantum era.

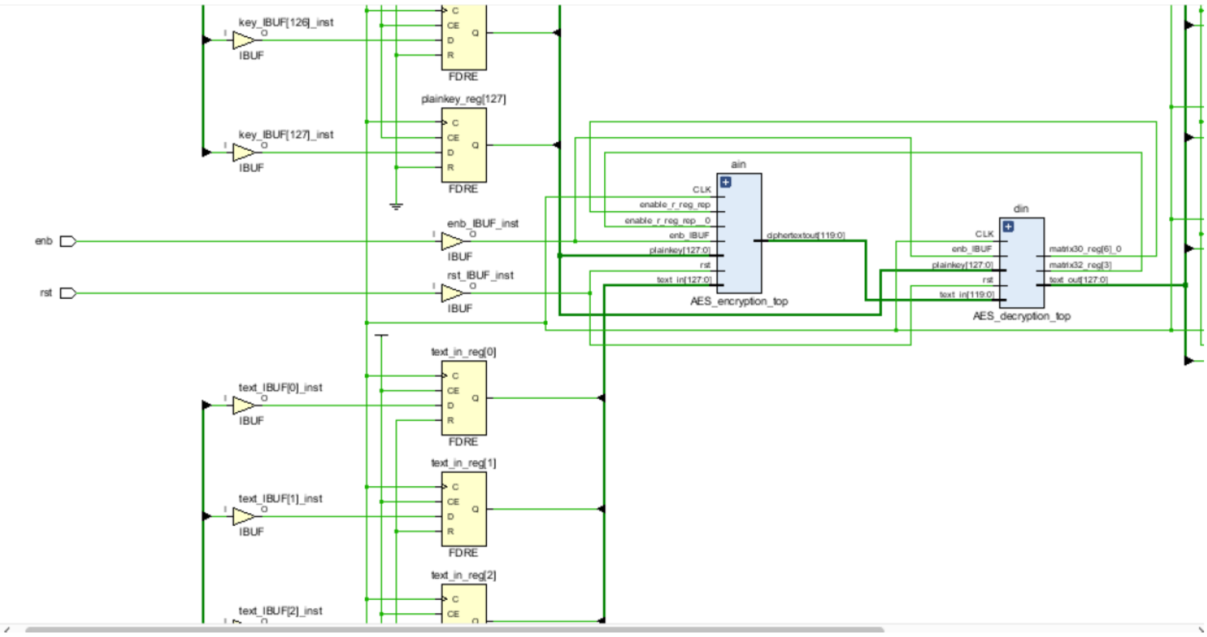


Fig.4 RTL schematic of proposed QC-based system and its sub-systems.

Table 1. Comparison Table between proposed and existing systems

Parameter	Existing: Key Size:128bits [23,34]	Proposed: Key Size:128bits	Existing: Key Size:256bits [12,22]	Proposed: Key Size:256bits
Power	1.03W	0.35W	3.12W	0.38W
Latency	6.34ns	2.18ns	4.2ns	2.41ns
Area	4310	1784	6144	2007
Flip-Flop Utilized	4232	1930	6144	2232
No of slices LUT Utilized	4401	1784	4802	1894
Throughput	1.6GHz	2.4GHz	1.09GHz	1.67GHz

The comparison between the existing and proposed shown in Table 1 of QC designs for both 128-bit and 256-bit key sizes highlights significant improvements across various metrics. For the 128-bit key size, power consumption in the proposed design is reduced from 1.03W to 0.35W, while latency decreases from 6.34ns to 2.18ns, showing better performance and energy efficiency. The area is minimized from 4310 to 1784 units, with flip-flop utilization dropping from 4232 to 1930 and LUTs used decreasing from 4401 to 1784, reflecting more efficient hardware utilization. The throughput also increases from 1.6GHz to 2.4GHz, enhancing overall processing speed. Similarly, for the 256-bit key size, power consumption is lowered from 3.12W to 0.38W, and latency is reduced from 4.2ns to 2.41ns. The area required is reduced from 6144 to 2007 units, with a corresponding drop in flip-flop utilization from 6144 to 2232 and LUTs from 4802 to 1894 as shown in Table 1. The throughput improves from 1.09GHz to 1.67GHz. Overall, the proposed design offers substantial gains in power efficiency, reduced latency, and hardware resource savings, while also delivering improved throughput for both key sizes.

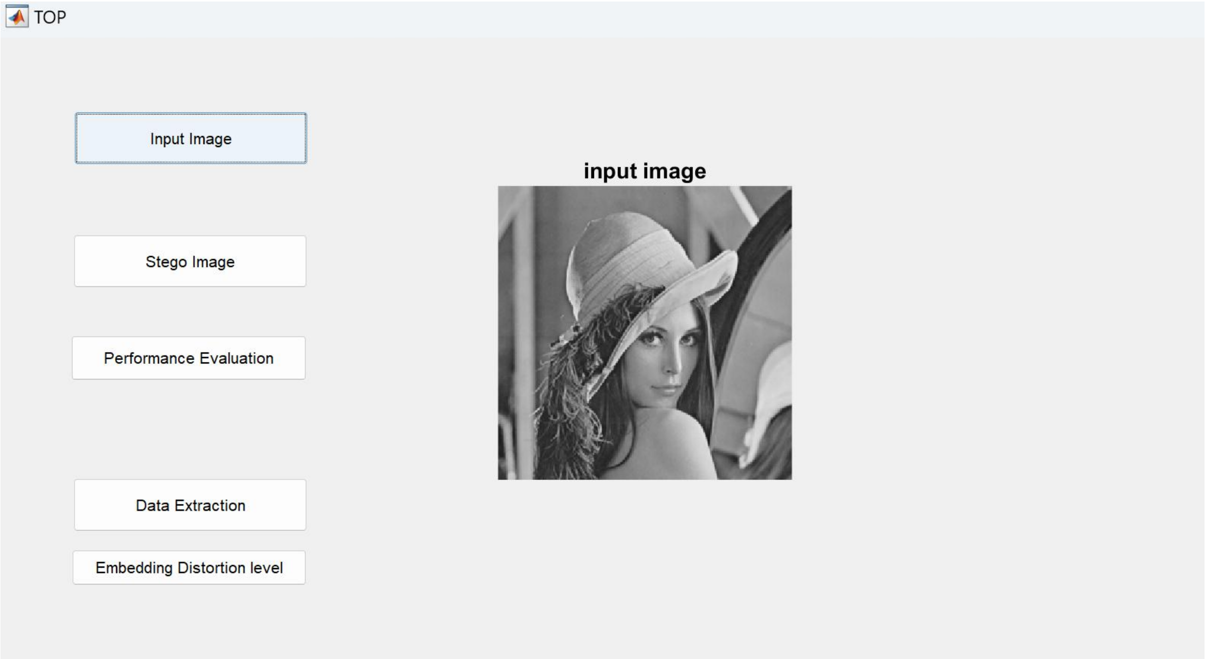


Fig.5. Simulated results between Digital Design (Verilog) and MATLAB and performance matrices.

Steganography in this research serves as a vital technique for enhancing digital security by concealing encrypted information within digital images, allowing for covert communication. The process starts by encrypting the confidential data using RSA or AES, followed by encoding the encrypted message into a QR code. This QR code is then embedded within a cover image using the Least Significant Bit (LSB) method as shown in Fig.5, which subtly alters the pixel values without noticeably changing the image's appearance. Advanced steganographic layers, including permutation, diffusion, and transposition, are also applied to make detection more challenging as shown in Fig.6 This combination of cryptography and steganography offers dual-layer security, ensuring that even if the encryption is compromised, the hidden data remains well-protected. The visual fidelity and accuracy of the Steganography images are measured using Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) as shown in the Table.2, demonstrating that the embedded data can be accurately retrieved without degrading the image's quality. This method allows secure communication over open networks, making it an effective solution for confidential messaging, digital watermarking, and secure key distribution while keeping sensitive information hidden from unauthorized access. The top-level simulated results of the proposed system are shown in Fig.7

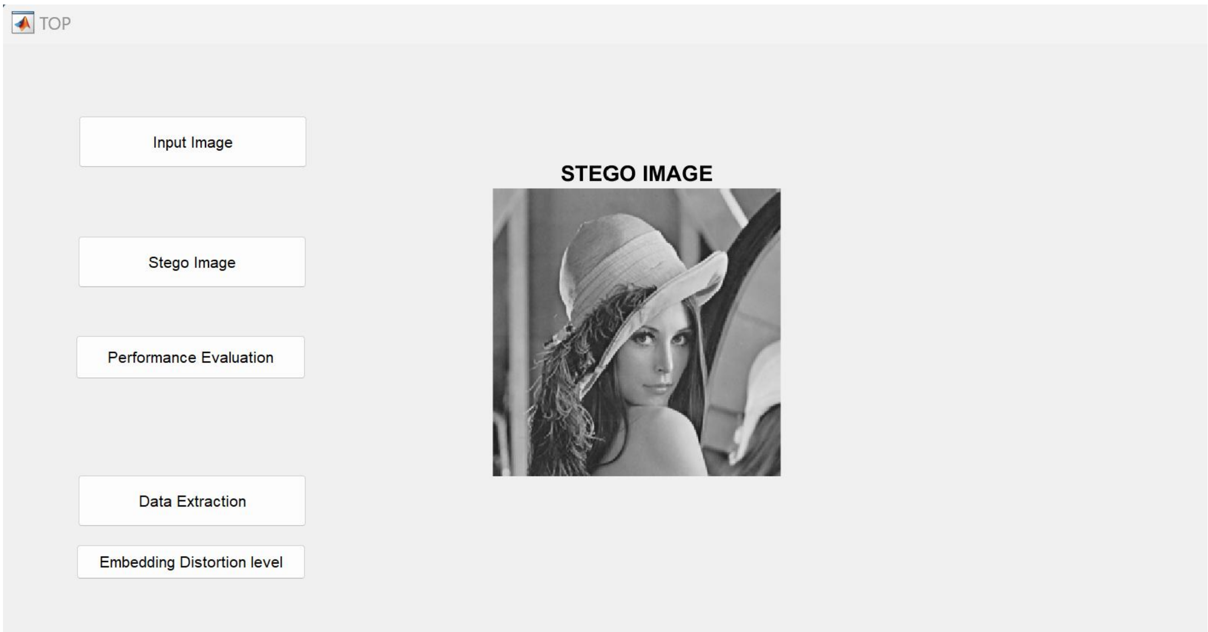
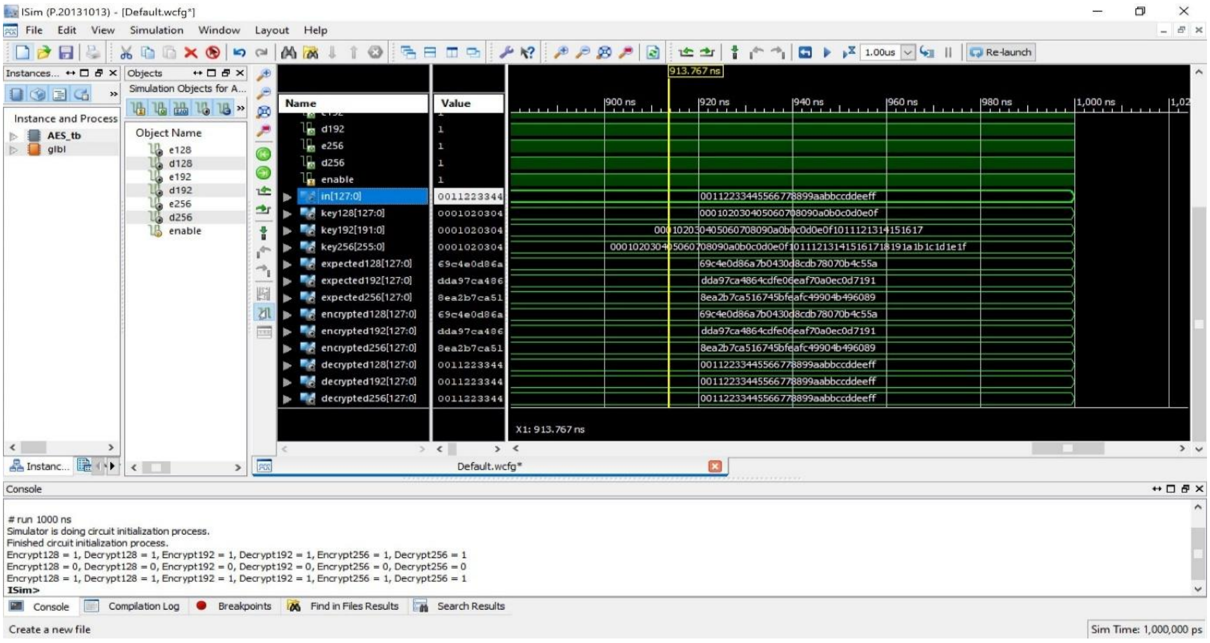


Fig.6 Simulated results Steganography between Digital Design (Verilog) and MATLAB Environment.



```
Name                 Value
d192                 1
e256                 1
d256                 1
enable               1
in[127:0]            0011223344   00112233445566778899aabbccddeeff
key128[127:0]        0001020304   000102030405060708090a0b0c0d0e0f
key192[191:0]        0001020304   000102030405060708090a0b0c0d0e0f1011121314151617
key256[255:0]        0001020304   000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
expected128[127:0]   69c4e0d86a   69c4e0d86a7b0430d8cdb78070b4c55a
expected192[127:0]   dda97ca486   dda97ca4864cdfe06eaf70a0ec0d7191
expected256[127:0]   8ea2b7ca51   8ea2b7ca516745bfeafc49904b496089
encrypted128[127:0]  69c4e0d86a   69c4e0d86a7b0430d8cdb78070b4c55a
encrypted192[127:0]  dda97ca486   dda97ca4864cdfe06eaf70a0ec0d7191
encrypted256[127:0]  8ea2b7ca51   8ea2b7ca516745bfeafc49904b496089
decrypted128[127:0]  0011223344   00112233445566778899aabbccddeeff
decrypted192[127:0]  0011223344   00112233445566778899aabbccddeeff
decrypted256[127:0]  0011223344   00112233445566778899aabbccddeeff
X1: 913.767 ns
```

```
# run 1000 ns
Simulator is doing circuit initialization process.
Finished circuit initialization process.
Encrypt128 = 1, Decrypt128 = 1, Encrypt192 = 1, Decrypt192 = 1, Encrypt256 = 1, Decrypt256 = 1
Encrypt128 = 0, Decrypt128 = 0, Encrypt192 = 0, Decrypt192 = 0, Encrypt256 = 0, Decrypt256 = 0
Encrypt128 = 1, Decrypt128 = 1, Encrypt192 = 1, Decrypt192 = 1, Encrypt256 = 1, Decrypt256 = 1
ISim>
```

Fig.7 Top-level simulated results in the Vivado Desing suite environment including AES and Steganography.

Table 2. Comparison Table between proposed and existing systems in terms of MSE, PSNR, and SSIM

Parameter	Existing	Proposed
MSE	5.34e-9	3.754e-9
PSNR	82.4	92.5
SSIM	1.7	1
Rate of the date change	3.44e-04	2.4414e-04

CONCLUSION

Integrating Q-Bit generation via quantum computing into AES encryption, coupled with the LSB technique for secure image steganography, offers a revolutionary advancement in data security. This approach leverages the inherent strengths of quantum mechanics to bolster encryption robustness, making it significantly more resistant to contemporary and future cyber threats. By incorporating quantum-generated keys into the AES encryption algorithm, the encryption process benefits from unprecedented levels of randomness and complexity, thereby enhancing its security posture. The use of the LSB technique in steganography further augments this framework by providing a secure and imperceptible method of embedding encrypted data within images. This dual-layer security mechanism ensures that sensitive information is not only encrypted with a quantum-enhanced method but also concealed within a carrier medium, making unauthorized detection and extraction exceedingly difficult.

The integration of quantum computing for Q-Bit generation with AES encryption and LSB steganography represents a forward-thinking approach to data protection. This synergy not only fortifies the encryption process against the evolving landscape of cyber threats but also enhances the overall security of data transmission and storage. As QC continues to evolve, its application in cryptographic protocols promises to set new benchmarks in the field of information security, safeguarding digital assets with a robustness previously unattainable through classical means.

REFERENCES

[1]. D. Ferrari, S. Carretta and M. Amoretti, "A Modular Quantum Compilation Framework for Distributed Quantum Computing," in IEEE Transactions on Quantum Engineering, vol. 4, pp. 1-13, 2023, Art no. 2500213, doi: 10.1109/TQE.2023.3303935.

[2]. A. Zaman, H. J. Morrell and H. Y. Wong, "A Step-by-Step HHL Algorithm Walkthrough to Enhance Understanding of Critical Quantum Computing Concepts," in IEEE Access, vol. 11, pp. 77117-77131, 2023, doi: 10.1109/ACCESS.2023.3297658.

[3]. P. Singh et al., "A Survey on Available Tools and Technologies Enabling Quantum Computing," in IEEE Access, vol. 12, pp. 57974-57991, 2024, doi: 10.1109/ACCESS.2024.3388005.

[4]. G. M. Vinod and A. Shaji, "Simulating Quantum Field Theories on Gate-Based Quantum Computers," in IEEE Transactions on Quantum Engineering, vol. 5, pp. 1-14, 2024, Art no. 3101214, doi: 10.1109/TQE.2024.3385372.

[5]. G. Kumar, S. Yadav, A. Mukherjee, V. Hassija and M. Guizani, "Recent Advances in Quantum Computing for Drug Discovery and Development," in IEEE Access, vol. 12, pp. 64491-64509, 2024, doi: 10.1109/ACCESS.2024.3376408.

[6]. R. Sotelo, D. Corbelletto, E. Dri, E. Giusto and B. Montrucchio, "Quantum Computing in Finance: The Intesa Sanpaolo Experience," in IEEE Engineering Management Review, vol. 52, no. 2, pp. 9-15, April 2024, doi: 10.1109/EMR.2024.3373796.

[7]. I. B. Djordjevic and V. Nafria, "Classical Coherent States Based Quantum Information Processing and Quantum Computing Analogs," in IEEE Access, vol. 12, pp. 33569-33579, 2024, doi: 10.1109/ACCESS.2024.3370430.

[8]. J. Pérez-Guijarro, A. Pagés-Zamora and J. R. Fonollosa, "Relation Between Quantum Advantage in Supervised Learning and Quantum Computational Advantage," in IEEE Transactions on Quantum Engineering, vol. 5, pp. 1-17, 2024, Art no. 3100517, doi: 10.1109/TQE.2023.3347476.

[9]. F. Qi et al., "Quantum Vulnerability Analysis to Guide Robust Quantum Computing System Design," in IEEE Transactions on Quantum Engineering, vol. 5, pp. 1-11, 2024, Art no. 3100411, doi: 10.1109/TQE.2023.3343625.

[10]. G. Carrascal, P. Hernamperez, G. Botella and A. d. Barrio, "Backtesting Quantum Computing Algorithms for Portfolio Optimization," in IEEE Transactions on Quantum Engineering, vol. 5, pp. 1-20, 2024, Art no. 3100220, doi: 10.1109/TQE.2023.3337328.

[11]. J. Zhang, F. Feng and Q. -J. Zhang, "Quantum Computing Method for Solving Electromagnetic Problems Based on the Finite Element Method," in IEEE Transactions on Microwave Theory and Techniques, vol. 72, no. 2, pp. 948-965, Feb. 2024, doi: 10.1109/TMTT.2023.3297406.

[12]. A. C. Marosi, A. Farkas, T. Máray and R. Lovas, "Toward a Quantum-Science Gateway: A Hybrid Reference Architecture Facilitating Quantum Computing Capabilities for Cloud Utilization," in IEEE Access, vol. 11, pp. 143913-143924, 2023, doi: 10.1109/ACCESS.2023.3342749.

[13]. M. Y. Shakor, M. I. Khaleel, M. Safran, S. Alfarhood and M. Zhu, "Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security," in IEEE Access, vol. 12, pp. 26334-26343, 2024, doi: 10.1109/ACCESS.2024.3351119.

[14]. S. Jeon, J. Kwak and J. P. Choi, "Cross-Layer Encryption of CFB-AES-TURBO for Advanced Satellite Data Transmission Security," in IEEE Transactions on Aerospace and Electronic Systems, vol. 58, no. 3, pp. 2192-2205, June 2022, doi: 10.1109/TAES.2021.3134988.

[15]. M. M. Mahmoud and H. T. Elshoush, "Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography–An Innovative Approach," in IEEE Access, vol. 10, pp. 29954-29971, 2022, doi: 10.1109/ACCESS.2022.3155146.

[16]. S. Solak, "High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms," in IEEE Access, vol. 8, pp. 166513-166524, 2020, doi: 10.1109/ACCESS.2020.3023197.

[17]. K. Zeng, K. Chen, J. Zhang, W. Zhang and N. Yu, "Toward Secure and Robust Steganography for Black-Box Generated Images," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 3237-3250, 2024, doi: 10.1109/TIFS.2024.3361220.

[18]. M. M. Fadel, W. Said, E. A. A. Hagras and R. Arnous, "A Fast and Low Distortion Image Steganography Framework Based on Nature-Inspired Optimizers," in IEEE Access, vol. 11, pp. 125768-125789, 2023, doi: 10.1109/ACCESS.2023.3326709.

[19]. S. Rahman et al., "A Comprehensive Study of Digital Image Steganographic Techniques," in IEEE Access, vol. 11, pp. 6770-6791, 2023, doi: 10.1109/ACCESS.2023.3237393.

[20]. S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan and M. Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method," in IEEE Access, vol. 10, pp. 124053-124075, 2022, doi: 10.1109/ACCESS.2022.3224745.

[21]. D. Ferrari, S. Carretta and M. Amoretti, "A Modular Quantum Compilation Framework for Distributed Quantum Computing," in IEEE Transactions on Quantum Engineering, vol. 4, pp. 1-13, 2023, Art no. 2500213, doi: 10.1109/TQE.2023.3303935.

[22]. F. Qi et al., "Quantum Vulnerability Analysis to Guide Robust Quantum Computing System Design," in IEEE Transactions on Quantum Engineering, vol. 5, pp. 1-11, 2024, Art no. 3100411, doi: 10.1109/TQE.2023.3343625.

[23]. Y. Li, Y. Zhang, M. Chen, X. Li and P. Xu, "Timing-Aware Qubit Mapping and Gate Scheduling Adapted to Neutral Atom Quantum Computing," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 42, no. 11, pp. 3768-3780, Nov. 2023, doi: 10.1109/TCAD.2023.3261244.

[24]. Z. Yang, M. Zolanvari and R. Jain, "A Survey of Important Issues in Quantum Computing and Communications," in IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1059-1094, Secondquarter 2023, doi: 10.1109/COMST.2023.3254481.

[25]. S. R. Majji, A. Chalumuri and B. S. Manoj, "Quantum Approach to Image Data Encoding and Compression," in IEEE Sensors Letters, vol. 7, no. 2, pp. 1-4, Feb. 2023, Art no. 7000504, doi: 10.1109/LSENS.2023.3239749.