DESIGNING CYBER SECURITY TOOLS IN QUANTUM COMPUTING ERA

Our project focuses on secure communication using quantum steganography, combining the invisibility of hidden messages with the advanced protection of quantum mechanics for tamper-proof data transfer.

INTRODUCTION

This project explores the development of cyber security tools using quantum steganography, an advanced technique that hides messages within quantum states. Unlike traditional methods, it ensures both the secrecy of the message and the invisibility of the communication itself. By leveraging quantum principles like superposition, entanglement, and the BB84 protocol, the system detects any eavesdropping attempts.

OBJECTIVE

The objective of our project is to achieve secure data transmission by embedding information within text or images using quantum steganography.

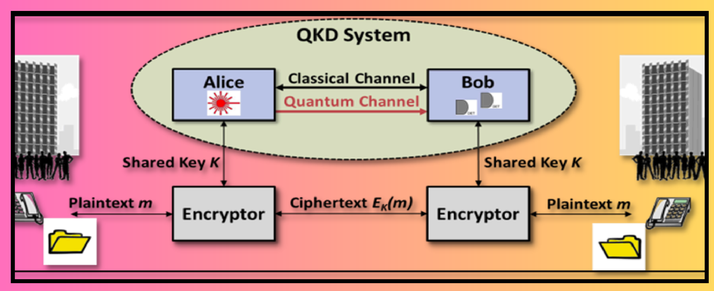
METHODOLOGY

Text Steganography

- Simulated BB84 protocol using Qiskit for secure key exchange.
- Applied XOR encryption on the message using the shared quantum key.
- Embedded encrypted bits into a cover text using case sensitivity (uppercase = 1, lowercase = 0).

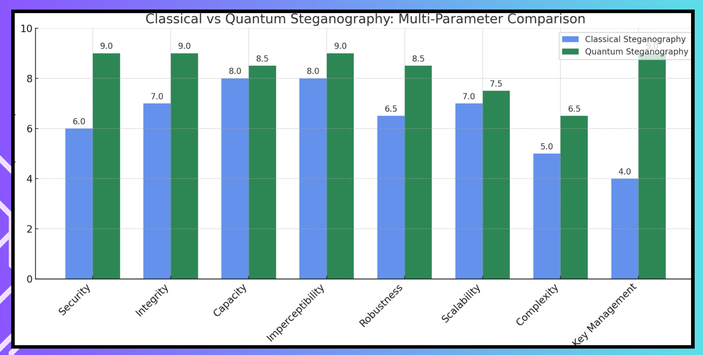
Image Steganography

- Converted message to binary and embedded it in the LSB of the red channel of an image.
- Used Cirq to apply quantum phase modulation (e.g., ZPowGate) on corresponding qubits.
- Reconstructed the message by extracting LSBs and decoding the binary back to text.



RESULTS/FINDINGS

- Integrates BB84 Quantum Key Distribution with classical steganography.
- Hides text using case variations; images via LSB embedding.
- Achieves high image quality (PSNR ~58.6 dB).
- Ensures strong security and high imperceptibility.
- Demonstrates robustness and practical feasibility in quantum cybersecurity.

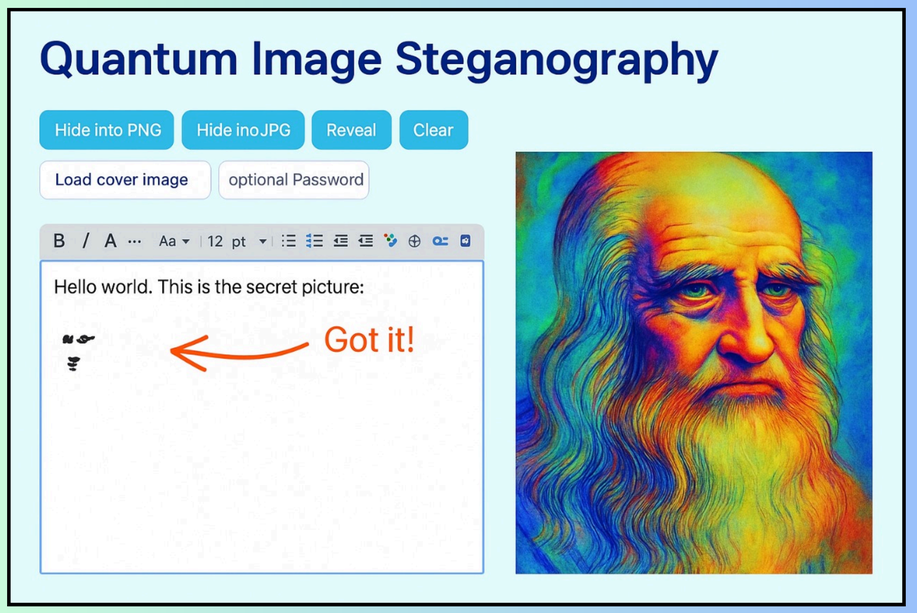


ANALYSIS

The project successfully combined quantum key distribution with steganography for secure text and image communication. Text messages were accurately encrypted and hidden using letter casing, while image steganography maintained high visual quality with an average PSNR of 58.6 dB. Overall, the system proved to be secure, reliable, and highly imperceptible.

QUANTUM TEXT STEGANOGRAPHY PORTAL

QUANTUM IMAGE STEGANOGRAPHY PORTAL



CONCLUSION

This project showcases a novel approach to secure communication by integrating quantum principles with classical steganography. Using Quantum Key Distribution (BB84) and data embedding techniques, it ensures both secrecy and undetectability. The results confirm high security, minimal distortion, and strong resistance to attacks. While currently simulated, the framework provides a solid foundation for real-world quantum-secure systems in the near future.

UNDER THE GUIDANCE
OF: DR. BISWAJITA DATTA
COMPUTER SCIENCE & ENGINEERING
BISHAL GHOSH (12200121012)
MOUSUMI DEY (12200121039)
SOUMYAJIT CHAKRABORTY (12200121053)
AINDRILA CHAKRABORTY (12230621006)