Quantum Steganography Detector Using Qiskit

1. Introduction

Quantum computing is a rapidly growing field that uses the principles of quantum mechanics — such as superposition and entanglement — to process information in ways that classical computers cannot. Quantum systems can encode, transmit, and process information in a secure and powerful manner.

Steganography is the practice of hiding secret messages within other data, such as images, audio, or text. Quantum steganography extends this concept to quantum systems by hiding information in quantum states. Detecting such hidden information requires specialized methods that leverage quantum mechanics.

This project demonstrates a **Quantum Steganography Detector** using **Qiskit**, IBM's quantum computing framework. The detector simulates quantum data, introduces hidden tampering, and uses **quantum fidelity** to determine whether hidden data exists.

2. Topic About

The project focuses on **detecting hidden or tampered information in quantum systems** using simulation. It combines two key concepts:

1. **Quantum Teleportation / Quantum States** – representing data as qubits and quantum circuits.
2. **Quantum Steganography Detection** – comparing a clean quantum state with a tampered state using **fidelity** to detect hidden modifications.

3. Objective

The main objectives of this project are:

- To simulate a quantum communication system using Qiskit.
- To demonstrate how hidden data or tampering in a quantum channel can be detected.
- To compare clean and modified quantum states using **quantum fidelity**.

4. Methodology

The methodology follows these steps:

1. **File Reading** – A text file (sample.txt) is read. Its content is converted into a binary string.
2. **Quantum Encoding** – Each bit is encoded as a quantum bit (qubit):
    - Bit 0 → |0⟩
    - Bit 1 → |1⟩
3. **Circuit Creation** – Two quantum circuits are created:
    - **Normal circuit**: clean quantum data
    - **Tampered circuit**: simulates hidden data by applying a **Z gate** to one qubit
4. **Simulation** – Both circuits are simulated using **Qiskit Aer's statevector simulator**.
5. **Fidelity Comparison** – The statevectors of the normal and tampered circuits are compared using **quantum fidelity**.
6. **Detection** – If fidelity is significantly lower than 1, tampering (hidden data) is detected.

5. Code Snippets

Binary Conversion

```
def text_to_bits(text):
    return ''.join(format(ord(c), '08b') for c in text)
```

Circuit Creation

```
def make_quantum_circuit(bit_string, tampered=False):
    n = len(bit_string)
    qc = QuantumCircuit(n)
    for i, bit in enumerate(bit_string):
        if bit == '1':
            qc.x(i)
    if tampered and n > 0:
        tamper_index = random.randint(0, n-1)
        qc.z(tamper_index)
    qc.save_statevector()
```

```
    return qc
```

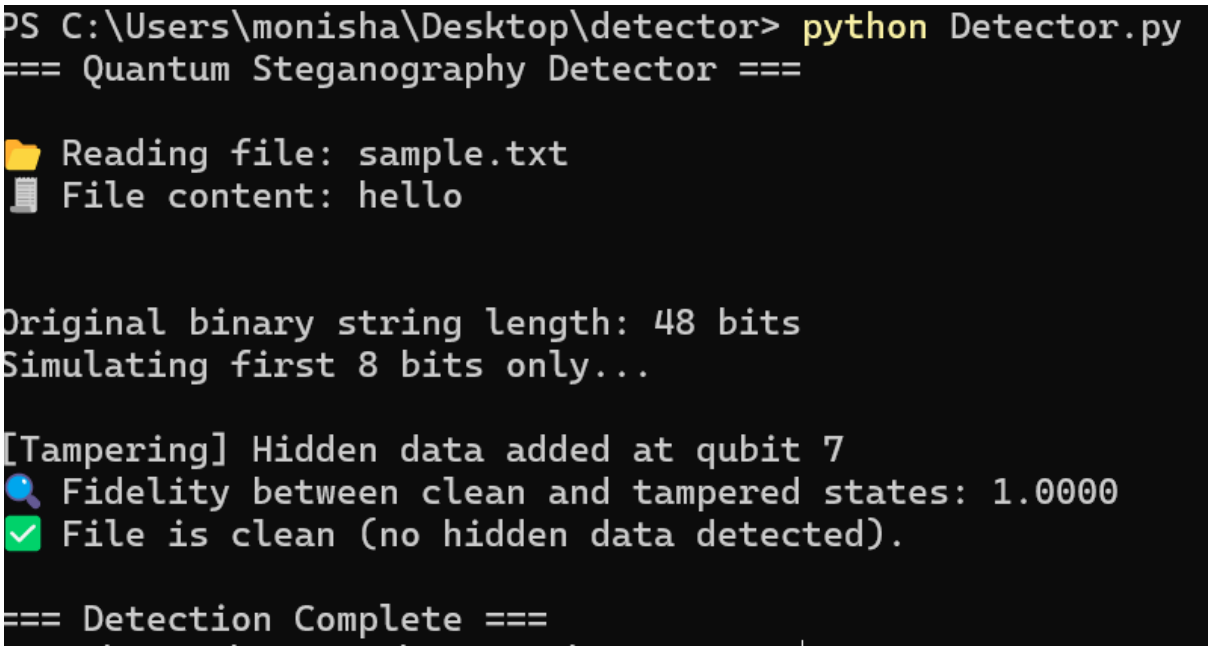
Fidelity and Detection

```
normal_state = simulator.run(normal_circuit).result().get_statevector()
tampered_state = simulator.run(tampered_circuit).result().get_statevector()
fidelity = state_fidelity(normal_state, tampered_state)


if fidelity < 0.95:
    print("Hidden data detected!")
else:
    print("File is clean")
```

6. Results

After running the simulation on sample.txt with content "hello", the following results were obtained:



- **Interpretation**: Since fidelity is 1, the detector concludes there is **no hidden/tampered data** in the simulated portion of the file.
- The detector successfully simulated **data detection**.

7. Future Scope

- Extend the detector to **simulate larger files** using optimized techniques (e.g., classical-quantum hybrid methods).
- Apply the methodology to **real quantum communication systems**.
- Develop **quantum key distribution security tools** to detect tampering or eavesdropping.
- Integrate **graphical visualization** of tampered qubits for educational demonstrations.

8. Conclusion

This project successfully demonstrates a **Quantum Steganography Detector** using Qiskit. By simulating a tampered quantum state and comparing it with a clean state via **quantum fidelity**, hidden information in a quantum system can be detected.

Although the current implementation works with small simulated file segments, it provides a **clear, educational framework** for understanding how quantum mechanics can enhance data security and steganography detection.

The project highlights the potential of quantum computing in **data integrity verification** and **secure communications**.