Chapter 8
Medical Data Are Safe:
An Encrypted Quantum Approach

Padmapriya Praveenkumar
Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India

Santhiyadevi R.
Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India

Amirtharajan R.
Shanmugha Arts, Science, Technology, and Research Academy (Deemed), India

ABSTRACT

In this internet era, transferring and preservation of medical diagnostic reports and images across the globe have become inevitable for the collaborative tele-diagnosis and tele-surgery. Consequently, it is of prime importance to protect it from unauthorized users and to confirm integrity and privacy of the user. Quantum image processing (QIP) paves a way by integrating security algorithms in protecting and safeguarding medical images. This chapter proposes a quantum-assisted encryption scheme by making use of quantum gates, chaotic maps, and hash function to provide reversibility, ergodicity, and integrity, respectively. The first step in any quantum-related image communication is the representation of the classical image into quantum. It has been carried out using novel enhanced quantum representation (NEQR) format, where it uses two entangled qubit sequences to hoard the location and its pixel values of an image. The second step is performing transformations like confusion, diffusion, and permutation to provide an uncorrelated encrypted image.

INTRODUCTION

The proliferation of telemedicine applications forces a massive requirement on the security and accurateness of the medical data transmission through communication channels. HealthInsurance Portability and Accountability Act (HIPAA) states that over 17 crores of medical data have been breached("Healthcare Data Breach Statistics"). IBM security and Ponemon Institute stated that the average cost of stolen record is increased to 4.8%(*Global Overview*, 2018). 20% of the victims received wrong diagnosis or delayed

DOI: 10.4018/978-1-5225-7952-6.ch008

treatment due to the illegal use of healthcare information("MIFA Shares Industry Wisdom on Medical Identity Theft and Fraud").The medical report includes personal details, health insurance policy number and healthcare history. Using this vast information, forged insurance can be claimed. The challenges in any medical system are that the number of images handled by the unit is substantial; also the size of the imagesis bulky. In contrast to the normal images, medical images have more redundant data. As a result, it is essential to devise encryption methods to process these medical images, so as to reduce the computational complexity. To manage this situation in classical image processing; the concept of quantum-based computation has been integrated with image encryption algorithms to achieve high computation speed and to provide parallelism and minimal storage requirements.

BACKGROUND

A good encryption scheme should possess Confidentiality, Integrity and Authentication (CIA). The first one indicates that the data is kept private from unauthorised disclosure. Integrity is offered by constructing the data that has not been transformed or tampered. Finally, authentication is the method of data recognition by the sender and receiver.

Undeniably, a well-devised healthcare security system should fulfil two conditions: confusion and diffusion to accomplish CIA in any security system. The chaotic equations are induced for achieving the above-said conditions, due to its aperiodic nature and susceptible to the primary condition. The first chaotic system-based encryption was proposed by Fridrich J(Fridrich, 1998). Since then, a variety of chaotic system-based encryption algorithms were framed. Further to prevail over the weakness like small key space and to eliminate the discontinuous range of chaotic behaviour, Zhou *et al.*(Zhou, Bao, & Chen, 2014) proposed a new chaotic system, by integrating the existing chaotic maps.

For the bulky medical data, conventional encryption algorithms like Advanced Encryption Standard (AES), Data Encryption Standard (DES)and s-box permutation matrix are incapable of surviving against various brute force, statistical and differential attacks. Therefore, a number of encryption algorithms have been developed based on DeoxyriboNucleic Acid (DNA), watermarking and hash algorithms to provide privacy and to ensure the integrity of the medical images used across the globe. Transmitting the entire bulky medical data tends to overload the traffic across communication channels. To evade this scenario, partial encryption and integrity check algorithms were proposed recently by many researchers (Ravichandran *et al*, 2017).

Classical image encryption algorithms are naturally extended to the quantum scenario due to the breakthrough of quantum information and quantum computation. Quantum computation has become an innovative tool for meeting with the real-time computational requirements. In an information storage and parallel computing, it has numerous exclusive computational qualities such as superposition of quantum state, quantum coherence and entanglement which makes quantum computing greater to its classical counterpart. In (Feynman, 1982), Feynman framed the initiative for the quantum computer, which comprises a physical machine which accepts input states as a superposition of many inputs (Deutsch, 1985).

In a quantum-enabled computer, the quantum image is an edition of the classical image. A variety of methods have been projected to signify the importance of quantum images and quantum image processing algorithms. Various quantum representation schemes were evolved to store the quantum image; few of them were Novel Enhanced Quantum Representation (NEQR), Entangled, Real ket, Multi-Channel Representation of Quantum Image (MCRQI), Flexible Representation of Quantum Images (FRQI) and