Chapter 13
Quantum Cryptography for Biomedical Image Security in Next-Generation Telemedicine Networks

L. B. Muralidhar
https://orcid.org/0000-0003-3453-613X
Jain University, India

Varanasi Rahul
https://orcid.org/0000-0003-2407-7654
Jain University, India

H. R. Swapna
https://orcid.org/0000-0003-0362-409X
Jain University, India

Digvijay Pandey
https://orcid.org/0000-0003-0353-174X
Department of Technical Education, Government of Uttar Pradesh, India

N. Sathyanarayana
https://orcid.org/0000-0002-4185-7751
Jain University, India

Pankaj Dadheech
https://orcid.org/0000-0001-5783-1989
Swami Keshvanand Institute of Technology, Management, and Gramothan, India

K. Nethravathi
https://orcid.org/0000-0003-4138-0276
Jain University, India

ABSTRACT

Next-generation telemedicine networks transform healthcare delivery by enabling real-time diagnostics, monitoring, and treatment. However, they face significant cybersecurity challenges, especially in safeguarding sensitive biomedical images. Traditional cryptographic techniques are vulnerable to emerging quantum computing threats, necessitating advanced solutions. Quantum cryptography, leveraging prin-

DOI: 10.4018/979-8-3693-9821-0.ch013

ciples like Quantum Key Distribution (QKD), offers unparalleled security through physical law-based encryption. This chapter explores the integration of quantum cryptography in telemedicine, addressing implementation challenges such as cost, scalability, and infrastructure compatibility. It highlights emerging protocols, like MDI-QKD, and their role in securing biomedical data in applications such as remote surgeries and teleradiology.

INTRODUCTION

Next-generation telemedicine networks epitomise technological innovation in the quest for improved healthcare delivery through enhanced communication systems. These networks are part of the digitisation of healthcare, enabling real-time remote diagnostics, monitoring, and treatment delivery, especially in resource-constrained areas (Sun et al., 2023). An essential aspect of such systems is biomedical image security since the data of patients transmitted over telemedicine networks contains sensitive and confidential information(Kshetri, 2021; Madaan, G., Swapna, H. R., Kumar, A., Singh, A., & David, A., 2021). Considering that these data transmissions have increased in the face of rising cyber threats against health systems worldwide, this chapter reviews the multidimensional dimensions of telemedicine networks, focusing on biomedical image security using theoretical frameworks, comparative perspectives, and the emerging role of quantum cryptography in secure communications.

PROBLEM STATEMENT

In the pace of rapid digital transformation concerning healthcare, telemedicine network architectures have become crucial in both diagnosis and treatment conducted distantly, patient data management, etc.; however, these networks are vulnerable to biomedical image security and protected patient information against rising concerns of cybersecurity threats due to ever-evolving data breaches, ransomware, unauthorised assess, among others. Additionally, conventional cryptographic methods do not have much power to confront the new quantum computers' powers(Pandey, B. K., & Pandey, D., 2025). Quantum cryptography provided some revolutionary solutions to these, including QKD and a variety of other higher-order protocols. On a more macro level, costs, scalability, and possible integrations with existing infrastructure provide barriers to widespread adoption. Resolving these issues is important in ensuring patient privacy and regulatory compliance and opening up global innovation within this sector. The study is conducted to determine how far