


Chapter 3


AI–Powered Secure Bio– Medical Image Analysis

Shaik Balkhis Banu

 <https://orcid.org/0000-0001-8014-0342>

*Department of Physiotherapy, Fatima
College of Health Sciences, Al Ain,
UAE*

T. Keerthika


 <https://orcid.org/0000-0002-1911-1785>

*School of Artificial Intelligence, Amrita
Vishwa Vidyapeetham, Coimbatore,
India*

Geetha Kathirvelu


Independent Researcher, Oman

S. Meena

 <https://orcid.org/0000-0001-9979-8689>

*Department of Chemistry,
Dayanandasagar College of
Engineering, Bangalore, India*

Anantha Murthy


 <https://orcid.org/0000-0002-9009-7541>

*NMAM, Institute of Technology, Nitte
University, India*

A. S. Hovan George

*Tbilisi State Medical University,
Georgia*

Devanga Dharani Lakshmi

 <https://orcid.org/0009-0008-3812-8663>

*Department of Computer Science
and AI, Central University of Andhra
Pradesh, Ananthapuramu, India*

ABSTRACT

Artificial intelligence (AI) is revolutionizing the field of medical image analysis, highlighting the vital need of strong security protocols to safeguard private patient information. The use of cutting-edge analytical tools improves the precision and effectiveness of medical imaging, enabling earlier diagnoses and better treatment outcomes as healthcare increasingly uses AI-driven technologies. But using a lot of patient data creates serious privacy issues, so data protection needs to be prioritized.

DOI: 10.4018/979-8-3693-9821-0.ch003

Differential privacy, federated learning, and secure multi-party computation are three important approaches that are covered. These techniques enable collaborative analysis without disclosing raw data.

INTRODUCTION

Healthcare is changing as a result of faster and more accurate medical imaging made possible by AI-powered biomedical image analysis (Pandey, B. K., & Pandey, D., 2025). Modern machine learning algorithms are able to identify subtle patterns in images, such as MRIs and X-rays, and can frequently spot abnormalities earlier than more conventional techniques. For illnesses like cancer, heart disease, and neurological disorders, this has resulted in better diagnosis and more individualized treatment regimens. But there are issues with data security and privacy as digital image processing becomes more and more common (Satheesh, N. et al., 2025). Sensitive information is frequently contained in medical images, making it susceptible to cyberattacks during storage, transmission, and analysis. Advanced encryption techniques are employed to protect this data at every stage of its lifecycle, guaranteeing that even in the event of access, the data cannot be read by unauthorized parties. When data is transferred between imaging systems and healthcare providers, secure transmission protocols like VPNs further safeguard it (Sheela, M. S. et al., 2025). Apart from encryption, real-time monitoring systems assist in identifying questionable activities related to the access or usage of data. These systems are able to identify possible breaches before they have a major negative impact. Collaborative analysis of medical data is made possible by privacy-preserving techniques that prevent external systems from seeing the actual images (Kumar, M. S. et al., 2025). This keeps privacy violations less likely while allowing for thorough analysis.

Landscape of Biomedical Imaging

The field of biomedical imaging is currently characterized by rapid technological advancements that have significantly improved the accuracy, speed, and resolution of medical images. These advancements have had a significant impact on the field. In clinical settings (Khadka, M. et al., 2025), diagnostic procedures such as magnetic resonance imaging (MRI), computed tomography (CT) scans, X-rays, and ultrasound are frequently utilized for the purpose of diagnosing, monitoring, and treating a wide variety of medical conditions. Clinicians are able to visualize the internal structures of the body through the use of these imaging modalities (Konapure, C. G. et al., 2025), which assists in the diagnosis of diseases such as cancer, cardiovascular disorders, and neurological issues. In recent years, the incorporation of digital technology has

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/ai-powered-secure-bio-medical-image-analysis/382848

Related Content

Artificial Intelligence Based Intrusion Detection System to Detect Flooding Attack in VANETs

Mannat Jot Singh Aneja, Tarunpreet Bhatia, Gaurav Sharma and Gulshan Shrivastava (2018). *Handbook of Research on Network Forensics and Analysis Techniques* (pp. 87-100).

www.irma-international.org/chapter/artificial-intelligence-based-intrusion-detection-system-to-detect-flooding-attack-in-vanets/201606

Authentication Through Elliptic Curve Cryptography (ECC) Technique in WMN

Geetanjali Rathee and Hemraj Saini (2018). *International Journal of Information Security and Privacy* (pp. 42-52).

www.irma-international.org/article/authentication-through-elliptic-curve-cryptography-ecc-technique-in-wmn/190855

Improved Feature-Level Fusion-Based Biometric System for Genuine and Imposter Identification

Bharath M. R. and Radhakrishna Rao K. A. (2022). *International Journal of Information Security and Privacy* (pp. 1-44).

www.irma-international.org/article/improved-feature-level-fusion-based-biometric-system-for-genuine-and-imposter-identification/307068

Using Hybrid Gamification to Build Community and Self-Efficacy Among Diverse University STEM Students

Karen J. Cotter (2023). *Handbook of Research on Current Trends in Cybersecurity and Educational Technology* (pp. 182-200).

www.irma-international.org/chapter/using-hybrid-gamification-to-build-community-and-self-efficacy-among-diverse-university-stem-students/318728

Enhancing Cryptography of Grayscale Images via Resilience Randomization Flexibility

Adnan Gutub (2022). *International Journal of Information Security and Privacy* (pp. 1-28).

www.irma-international.org/article/enhancing-cryptography-of-grayscale-images-via-resilience-randomization-flexibility/307071