UNIVERSITI TEKNOLOGI MARA

# CYBERSECURITY, BIG DATA, AND ARTIFICIAL INTELLIGENCE:

## FROM WATERMARKING TO FEDERATED LEARNING






UiTM Professorial Lecture

JASNI MOHAMAD ZAIN

# TABLE OF CONTENTS

*List of Figures* ix
*List of Tables* xi
*Preface* xiii
*Acknowledgements* xv
*List of Abbreviations* xvii

**CHAPTER 1** **1**

**PRINCIPLES AND PARADIGMS OF MEDICAL IMAGE WATERMARKING**

- Introduction to Teleradiology and Security Threats 1
- Mathematical Foundations of Reversible Watermarking (LSB and Difference Expansion) 2
- Region of Interest (ROI) and Region of Non-Interest (RONI) Segmentation Strategies 4
- Tamper Localisation and Multilevel Authentication (TALLOR-RSMA Framework) 8
- Lossless Watermark Compression (LZW) in Ultrasound Imagery 9
- Frequency Domain Embedding: DWT-SVD and PSO 10

# ACKNOWLEDGEMENTS

The research conducted for this publication is an example of a great collaborative effort; it represents an institutional commitment to the pursuit of knowledge through academic research. I wish to express my sincere appreciation to the institutions and colleagues who provided the foundation upon which these academic pursuits were built. I wish to thank Universiti Teknologi MARA (UiTM), and particularly FSKM, for creating such a dynamic and state-of-the-art research environment at the Institute for Big Data Analytics and Artificial Intelligence (IBDAAI). I would also like to extend my warmest congratulations to FSKM on its 60th-year celebration. The academic freedom and resources that UiTM has provided have been fundamental to advancing our Artificial Intelligence and Big Data research to meet international standards. I also wish to recognise the Faculty of Computer Systems & Software Engineering at Universiti Malaysia Pahang Al-Sultan Abdullah (UMPSA), where I had the unique opportunity to serve as Dean for eight formative years.

Additionally, I wish to acknowledge the contribution of Brunel University London, my alma mater, whose support during my early doctoral studies under the excellent and patient supervision of Professor Malcolm Clarke and the late Professor Ray J Paul helped lay the groundwork for what would become my research footprint today. Without the dedication, brilliance and perseverance of my

# CHAPTER 1

# PRINCIPLES AND PARADIGMS OF MEDICAL IMAGE WATERMARKING

## INTRODUCTION TO TELERADIOLOGY AND SECURITY THREATS

The modernisation of medical diagnostics has become inextricably linked with digital transmission and remote assessment of patient scans. This paradigm, known as teleradiology, enables specialists in urban centres to instantly evaluate diagnostic imaging (such as MRIs, CT scans, and ultrasounds) from remote or rural clinics. Digital Imaging and Communications in Medicine (DICOM) has emerged as the universal standard for these transmissions. However, as these files traverse heterogeneous healthcare information systems, Picture Archiving and Communication Systems (PACS), and public networks, they expose highly sensitive clinical telemetry to significant security, integrity, and authenticity risks.

Malicious actors, network transmission errors, or accidental administrative overwrites can corrupt clinical metadata or alter diagnostic-grade imaging. A single altered pixel block in an ultrasound or MRI scan could obscure a lesion or create an artefact, leading to a catastrophic misdiagnosis. While traditional cryptographic mechanisms such as Advanced Encryption Standard (AES) or Rivest-Shamir-Adleman (RSA) secure data robustly during transit, they suffer from a fundamental flaw in this context: they

In this concise book, I synthesise my foundational research at the critical nexus of cybersecurity, big data, and artificial intelligence to provide both a historical overview and a forward-looking blueprint for secure, intelligent systems. By tracing the evolution of my work, from autonomous Intrusion Response Systems (IRS) and reversible cryptographic watermarking in healthcare to the pioneering Single-Round, Privacy-Preserving Federated Learning (PraFL) Paradigm, and advanced spatiotemporal predictive modelling for marine environments, this publication demonstrates how the exponential scale of massive datasets can be securely harnessed to train powerful AI models without compromising user privacy. Ultimately, this compilation serves as a concentrated, high-impact guide for researchers, practitioners, and policymakers, illustrating that the future of resilient technological infrastructure relies on the inseparable integration of advanced machine learning capabilities with uncompromising, mathematically sound cryptographic safeguards.



**Professor Dr. Jasni Mohamad Zain** received her bachelor's degree in computer science from the University of Liverpool, England, UK in 1989 and PhD from Brunel University, West London, UK in 2005. She started her career as a tutor at Universiti Teknologi Malaysia (UTM) in 1997. She currently serves as the Director of Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), UiTM Shah Alam. She previously served as the Deputy Director (Cybertechnology) Research Nexus UiTM and the Head of Advanced Analytics and Engineering Centre (AAEC). She was also the Dean of the Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang (now known as UMPSA) for eight years.

PENERBIT PRESS
UNIVERSITI TEKNOLOGI MARA

ISBN 978-629-496-212-5
Harga / Price : RM62.00
9 786294 962125