1. Record Nr. UNINA9910842298403321

Titolo	Adversarial Multimedia Forensics / / edited by Ehsan Nowroozi, Kassem Kallas, Alireza Jolfaei
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-49803-8
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (298 pages)
Collana	Advances in Information Security, , 2512-2193 ; ; 104
Disciplina	005.8
Soggetti	Machine learning Image processing - Digital techniques Computer vision Computer crimes Signal processing Artificial intelligence Machine Learning Computer Imaging, Vision, Pattern Recognition and Graphics Computer Crime Signal, Speech and Image Processing Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Chapter. 1. Model Poisoning Attack against Federated Learning with Adaptive Aggregation -- Chapter. 2. Image Forgery Detection using Comprint: A Comprehensive Study -- Chapter. 3. Good or evil: Generative adversarial networks in digital forensics -- Chapter. 4. Refined GAN-Based Attack Against Image Splicing Detection and Localization Algorithms -- Chapter. 5. Generative Adversarial networks for Artificial Satellite Image Creation and Manipulation -- Chapter. 6. Domain Specific Information based learning for Facial Image Forensics -- Chapter. 7. Linguistic Steganography and Linguistic Steganalysis -- Chapter. 8. Random Deep Feature Selection’s Efficiency in Securing Image Manipulation Detectors Opposed by Adversarial Attacks -- Chapter. 9. Optimized Distribution for Robust Watermarking of Deep

neural Networks through Fixed Embedding Weights -- Chapter. 10. Anti Forensic Measures and Their Impact on Forensic Investigations -- Chapter. 11. Using Vocoder Artifacts for Audio Deepfakes Detection.

Sommario/riassunto

This book explores various aspects of digital forensics, security and machine learning, while offering valuable insights into the ever-evolving landscape of multimedia forensics and data security. This book's content can be summarized in two main areas. The first area of this book primarily addresses techniques and methodologies related to digital image forensics. It discusses advanced techniques for image manipulation detection, including the use of deep learning architectures to generate and manipulate synthetic satellite images. This book also explores methods for face recognition under adverse conditions and the importance of forensics in criminal investigations. Additionally, the book highlights anti-forensic measures applied to photos and videos, focusing on their effectiveness and trade-offs. The second area of this book focuses on the broader landscape of security, including the detection of synthetic human voices, secure deep neural networks (DNNs) and federated learning in the context of machine learning security. It investigates novel methods for detecting synthetic human voices using neural vocoder artifacts, and it explores the vulnerabilities and security challenges of federated learning in the face of adversarial attacks. Furthermore, this book delves into the realms of linguistic steganography and steganalysis, discussing the evolving techniques that utilize deep learning and natural language processing to enhance payload and detection accuracy. Overall, this book provides a comprehensive overview of the ever-evolving field of digital forensics and security, making it an invaluable resource for researchers and students interested in image forensics, machine learning security and information protection. It equips readers with the latest knowledge and tools to address the complex challenges posed by the digital landscape. Professionals working in this related field will also find this book to be a valuable resource.