Chapter 2
Machine Learning in Digital Forensics

ABSTRACT

In the intricate landscape of digital forensics, the integration of machine learning has ushered in a transformative era. Digital forensics is a discipline concerned with the recovery, analysis, and presentation of digital evidence in a manner that is legally admissible. The field is increasingly important due to the growing dependence on digital technologies and the proliferation of cybercrimes. With the exponential growth of digital devices and the increasing complexity of cybercrimes, digital forensics has become more challenging. Machine learning (ML), a subset of artificial intelligence (AI), has emerged as a pivotal technology in context of cyber forensics, offering sophisticated methods for analyzing large volumes of data, detecting anomalies, and automating complex tasks (Suaib, Akbar, & Husain, 2020).

1. INTRODUCTION

In the intricate landscape of digital forensics, the integration of machine learning has ushered in a transformative era. Digital forensics is a discipline concerned with the recovery, analysis, and presentation of digital evidence in a manner that is legally admissible. The field is increasingly important due to the growing dependence on digital technologies and the proliferation of cybercrimes. With the exponential growth of digital devices and the increasing complexity of cybercrimes, digital forensics has become more challenging. Machine learning (ML), a subset of artificial intelligence (AI), has emerged as a pivotal technology in context of cyber forensics, offering

DOI: 10.4018/979-8-3693-2960-3.ch002

sophisticated methods for analyzing large volumes of data, detecting anomalies, and automating complex tasks (Suaib, Akbar, & Husain, 2020).

This chapter provides a comprehensive insight into the application of machine learning in cyber forensics. It explores foundational concepts, key applications, challenges, and future directions. The objective is to offer an in-depth understanding of how ML can be leveraged to enhance forensic investigations and address the evolving challenges in the digital landscape.

2. EMERGENCE AND IMPORTANCE OF MACHINE LEARNING

The emergence of machine learning as a powerful analytical tool for diverse applications forms the foundation for its integration into digital forensics. Machine learning is a branch of artificial intelligence (AI) that enables systems to learn from data and improve their performance over time without explicit programming.

2.1. Foundations of Machine Learning

Machine Learning (ML) is a subfield of artificial intelligence (AI) focused on developing algorithms and statistical models that enable computers to learn from and make predictions or decisions based on data. Unlike traditional programming, where explicit instructions are given to perform a task, machine learning systems use data to learn patterns and improve their performance over time without being explicitly programmed for specific tasks. The core of ML lies in its ability to recognize patterns and make decisions based on data inputs. Key concepts in ML includes:

2.1.1. Machine Learning Techniques

Machine Learning approaches are generally categorized into supervised learning, unsupervised learning, and reinforcement learning as shown in Figure 1.