INTERNATIONAL CONFERENCE ON RESEARCHES IN ENGINEERING, SCIENCE, TECHNOLOGY, MANAGEMENT AND HUMANITIES (ICRESTMH – 2024)

25TH AUGUST, 2024

CERTIFICATE NO : ICRESTMH /2024/C0824881

A Study of Digital Forensic Analysis for Digital Files by Using Deep Learning

Jillawar Roopali Jayprash

Research Scholar, Department of Electronics & Communication Engineering,
P.K University, Shivpuri, M.P., India.

ABSTRACT

Digital forensic analysis for digital files using deep learning has emerged as an advanced approach to investigate cybercrimes and secure digital evidence. With the rapid growth of digital data, traditional forensic techniques often struggle to handle large volumes of files efficiently and accurately. Deep learning methods, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), provide automated and intelligent solutions for analyzing diverse digital file formats such as images, documents, audio, and video. These models can detect hidden patterns, classify file types, identify malicious content, and uncover file tampering or forgery. For example, CNNs are highly effective in detecting image manipulation and deepfake content, while RNN-based models can analyze sequential log data for anomaly detection. Feature extraction is performed automatically, reducing dependence on manual rule-based systems. Additionally, deep learning techniques enhance malware detection by identifying suspicious code patterns within executable files. The integration of AI-driven analysis improves speed, accuracy, and scalability in forensic investigations. However, challenges such as data privacy, model interpretability, and computational requirements must be addressed.