Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

6

Cyber Forensic Security in Digital Multimedia Communication Using Deep Learning

Dipalee S. Hirde

Research Scholar,

P.G Department of Computer Science and Engineering, SGBAU, Amravati, India

Dr Swati S. Sherekar

Professor,

P.G Department of Computer Science and Engineering, SGBAU, Amravati, India

Abstract

In the computing world, Cyber forensic security for digital multimedia is an instigative and gruelling field. With the rapid-fire increase in the use of digital technology, crimes moment are committed using contemporary ways that don't involve physical contact. As a result, forensic specialists are unfit to examine and dissect the data at the crime scene. A change in the disquisition ways is necessary to achieve effective disquisition of crimes involving advanced technology. The forgery of digital images compromises the authenticity and integrity of the images. In recent times, the need for the forgery detection algorithm has increased because of the rapid-growth and availability of imaging processing software and the advancements made in digital cameras. With the growing frequency of digital communication, cybercrime similar to image forgery have surfaced as significant challenges. Traditional forensic methods struggle

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

to manage these advanced ways, challenging innovative results. To improve the detection and localization of manipulated areas in digital images, this study proposes a hybrid deep learning model that integrates Long Short-Term Memory (LSTM) networks with Convolutional Neural Networks (CNNs). Additionally, the Scale-Invariant Feature Transform (SIFT) algorithm is incorporated to enhance precision and robustness. The model effectively identifies forged regions, classifies tampering types (e.g., copy-move, image splicing), and delineates manipulated areas using bounding boxes. By generating double masks, it strengthens the accuracy of forensic analysis, contributing to advancements in digital forensic security. This exploration aims to use deep learning methods to produce a reliable frame for relating and examining these attacks, fulfilling an essential demand in the field of cyber forensics.

Index Terms: Cyber Forensic Security, Digital Multimedia, Digital Image Forgery, Image Splicing, Copy-Move Forgery, LSTM-based deep learning networks, CNN architectures for image forensics, SIFT-based feature extraction, Deep Learning, Tampered Region Localization, Forgery Detection Algorithm, Cybercrime, Digital Communication, Image Authenticity, Bounding Box Detection.

I. Introduction

The popularity of the internet has promoted an unequalled growth of multimedia content sharing. We live in a period where digital multimedia distribution over social spots has a wide impact on society. On-the-scene videos and pictures of disastrous pandemics, sports events, warfare, political mass meetings, and accidents, when published online, can reach millions of people presently. Still, the wide use of digital multimedia and technology has raised new enterprises. The rapid-fire relinquishment of digital technologies has converted communication, but it has also led to an increase in cybercrimes. Cyber forensic security, particularly for multimedia data, faces unknown challenges as culprits employ sophisticated ways similar to image forgery. Cyber forensic security, a branch of digital forensics, aims to combat similar crimes by probing, relating, and mollifying these manipulations. It's particularly pivotal in disciplines like journalism, law enforcement, healthcare, e-commerce, where the authenticity of digital multimedia plays a vital part. Despite progress in forensic techniques, conventional methods often prove inadequate when

dealing with the complexities of modern cybercrime. These approaches, which mainly rely on pixel-level and block-based analysis, struggle to detect advanced image manipulation techniques such as region duplication and composite image alterations. These manipulations are designed to bypass conventional discovery algorithms by altering the structural and contextual integrity of images. This study can help researchers understand the strengths and limitations of existing image forensic technologies, enabling them to develop more efficient algorithms for detecting image manipulations. Additionally, this comparative study examines various forgery detection techniques, including deep learning and complex neural networks, evaluating their advantages and limitations. In today's digital era, images serve as a primary source of information due to their ease of access and advanced capabilities [1]. Ensuring the authenticity of digital images and identifying signs of manipulation without relying on pre-extracted or pre-embedded data has emerged as a crucial and highly active research area in image processing [2]. Moreover, digital image forgery detection is widely applied across various domains, including media, publishing, law enforcement, healthcare, satellite imaging, and online platforms. Its significance arises from the ease with which digital images can be altered and manipulated [3]. As a result, various types of cameras and user-friendly software are utilized for creating and modifying digital images [4]. Such manipulations undermine the authenticity of digital content and erode trust in digital communications. Region duplication and composite image alterations are two prevalent forms of image forgery that require advanced detection techniques. This study leverages deep learning methodologies to establish a reliable framework for identifying and analyzing these threats, addressing a crucial need in the field of cyber forensics. With the rapid advancement of AI-generated synthetic media, these findings lay the groundwork for enhancing the security of digital platforms and ensuring the authenticity of information [5].

II. Literature Review

Being literature highlights the limitations of traditional forensic styles in combating multimedia-related cybercrimes. Classical approaches, similar to pixel-based and block-based detection, frequently fail to achieve high delicacy and robustness against complex forgery techniques. Recent studies demonstrate the potentiality of deep literacy models in image recognition and forgery detection. Convolutional-based neural models excel in feature

extraction, whereas LSTM-based neural networks are proficient in capturing temporal relationships. However, their combined application in cyber forensic investigations remains largely unexplored. The SIFT algorithm has been widely applied in feature matching and object recognition; however, its integration with deep learning for image forgery detection introduces a novel approach. This method examines how advancements in big data and machine learning enhance digital forensics by automating large-scale forensic processes, identifying potential cyber threats, and forecasting high-risk scenarios [6].

A. Enhanced Data Analysis

Yadav, R. T. (2024) [7] AI significantly improves data analysis in digital forensics by leveraging Algorithmic learning models and neural networks to process and interpret vast amounts of data. Traditional forensic approaches often face challenges in handling the immense scale and complexity of modern digital environments, where data is generated at an unprecedented rate. AI-driven algorithms can analyze this data more efficiently and accurately than human investigators, identifying patterns and extracting relevant information that might otherwise go unnoticed.

B. Digital Forensics and Investigations

Casey (2019) [8] offers an in-depth analysis of digital forensics, fastening on the interaction between people, processes, and technologies. This text offers a comprehensive overview of the methodologies and real-world applications in digital forensics. It lays the roots for the integration of AI technologies by detailing current practices and challenges within the field. The principles bandied in this textbook help frame how AI can round or transfigure traditional forensic styles, furnishing a literal environment that's pivotal for current advancements.

C. Blockchain Technology in Digital Forensics

Li and Qin (2022) [9] exploring the integration of blockchain technology with digital forensics, agitating both the challenges and openings presented by this decentralized technology. Blockchain's core attributes immutability and transparency, offer promising possibilities for enhancing the integrity and reliability of forensic substantiation. Their paper is precious for

understanding how blockchain can be used to overcome some of the limitations of traditional forensic methods, similar to issues related to tampering and data integrity.

D. Pattern Recognition and Classification

AI's ability to fete and classify patterns is a pivotal aspect of its part in digital forensics. Machine learning algorithms are trained on large datasets to identify specific features or anomalies that signify implicit substantiation. For example, in malware analysis, AI models can classify malware based on its behaviour, code structure, or other attributes, distinguishing between given and unknown threats. Pattern recognition extends beyond malware to include user action analysis and anomaly detection. AI-driven models can examine user activity records and network data to detect anomalies that may signal malicious or unauthorized behavior. This capability is particularly precious in detecting insider threats or sophisticated cyber-attacks that may not spark traditional security alerts [11].

III. Existing Methodology

A. Deep Neural Computation:

As a specialized field within machine learning, deep learning leverages multi-layered neural networks to process and extract insights from intricate data structures. It has proven highly effective in digital forensics, particularly in analyzing unstructured data like images, videos, and text.

B. Convolution-based neural models:

In the realm of digital forensics, CNNs serve as powerful tools for image and video examination, aiding in the detection of altered images, verification of visual evidence, and investigation of suspicious activities captured on video. These networks can identify image alterations and authenticate digital photos with precision.

C. Recurrence-driven deep learning models and Long-Term dependency learning frameworks:

Design for sequential data processing RNNs and LSTMs are highly effective in analyzing time-series information such as system logs and network activity. Their ability to capture temporal patterns and detect anomalies over time enables them identify trends and irregular system behaviour [7].

D. Generative-discriminative deep learning models:

Operate through the interaction of two neural networks, a generator that creates data and a discriminator that evaluates it, This adversarial process enables the generation of synthetic data for machine learning applications and aids in restructuring to generate synthetic data for training other models or to reconstruct damaged forensic evidence to enhance its quality [11].

Deep learning and feature extraction techniques for detecting and classifying multimedia forgeries. Key components include:

- *Preprocessing:* Input images undergo normalization and resizing to ensure consistency for model training and evaluation.
- *Feature Extraction:* CNNs are employed to extract spatial features from images, while LSTM networks analyze sequential patterns to capture contextual relationships.
- *Hybrid Model:* An LSTM-CNN hybrid model is designed to generate binary masks that highlight tampered regions in the image.
- *Enhanced SIFT Algorithm***:** The Scale-Invariant Feature Transform (SIFT) algorithm enhances detection accuracy by ensuring robustness and consistency in identifying forged areas. It strengthens the deep learning model by improving feature matching and refining localization, making forgery detection more precise.
- *Classification and Bounding Box Generation:* The system classifies tampering as either copy-move or image splicing and generates bounding boxes to delineate forged regions.

- *Analytical Metrics:* Performance assessment of the model is conducted using key metrics, including accuracy, precision, recall, and F1-score, applied to benchmark datasets containing manipulated images.

E. Natural Language Processing (NLP)

By bridging the gap between human communication and computational analysis, NLP helps in digital forensic investigations by processing textual data found in emails, social networks and chat platforms.

Text-based emotion analysis: Analyzing the emotional tone of textual data assists forensic experts in interpreting communication intent and detecting suspicious or harmful content. Named Entity Recognition (NER) systematically identifies and classifies the emotional tone of textual data. In forensic investigations, they help determine the intent behind communications and identify potentially suspicious or threatening content. Named Entity Recognition (NER) identifies and categorizes entities such as names, dates, and locations within textual data. It extracts critical information from forensic documents, social media, and communication logs, aiding in the identification of key individuals or events [11].

Text categorization: Categorizing textual content using NLP algorithms enhances the management of large scale text-based data. Approaches like Naive Bayes and SVM facilitate the differentiation of emails and messages, ensuring accurate classification into spam, phishing or authentic categories [11].

F. Blockchain Integration in Digital Forensics

Blockchain recognized, for its decentralized and tamper- resistant ledger has been incorporated with AI to strengthen digital forensic operations. The fusion of blockchain and AI enhances security and reliability in forensic data management.

Tamper-Proof Evidence Records: Blockchain safeguards the integrity of digital evidence by maintaining an unalterable and secure record. When paired with AI, it enables the verification and validation of forensic data, preventing manipulation and ensuring the accuracy of digital evidence.

Vidhyayana - ISSN 2454-8596
An International Multidisciplinary Peer-Reviewed E-Journal
www.vidhyayanaejournal.org
Indexed in: Crossref, ROAD & Google Scholar

Automated Forensic Processes with smart contracts: Blockchain-based smart contracts facilitate the automation of forensic procedures while ensuring compliance with established protocols. For instance, smart contracts can oversee the chain of custody for digital evidence, recording every interaction and allowing AI-driven systems to validate and authenticate these records.

IV. Study and analysis of various methods

A. Manipulation Detection Using Deep Learning

Manipulated multimedia content (e.g., doctored images or videos) is increasingly used in cybercrime. Detecting these alterations is crucial for maintaining data integrity.

Convolutional Neural Networks (CNNs): Extract spatial features from multimedia data, identifying patterns that deviate from genuine content. Anomalies such as noise inconsistencies, lighting issues, and pixel alignment are detected.

Autoencoders: Unsupervised learning models trained to reconstruct original media and detect manipulation by measuring reconstruction errors.

Advantages: High accuracy in detecting even subtle alterations.

Challenges: Computationally intensive for large-scale datasets.

B. DeepFake Detection

DeepFake technologies are misused for identity theft, misinformation, and impersonation attacks. Detecting such synthetic media is a core focus in cyber forensics.

Siamese Networks: Utilized to compare biometric features (e.g., facial landmarks or voice prints) of genuine and suspect content. These networks identify inconsistencies in identity-specific features.

Recurrent Neural Networks (RNNs): Analyze temporal data in videos to detect mismatches in facial expressions or body movements over time.

Advantages: Person-specific models reduce false positives in targeted applications.

Challenges: Requires extensive labelled datasets for training.

C. Ontology-based multimedia Forensic Frameworks

Understanding the context and semantics of multimedia communication can aid in cyber forensic analysis.

Ontology-Based Frameworks: Build a knowledge representation system to classify and interpret multimedia content. Combine this with machine learning models for automatic labelling and pattern recognition.

Hybrid Models: Use ontological reasoning to supplement ML-based forensic techniques.

Advantages: Enhances interpretability and reasoning in forensic investigations.

Challenges: Ontology creation is labour-intensive.

D. Recognition of Duplication-Based Image Forgery:

This type of forgery occurs when a portion of an image is replicated and repositioned to hide or alter details.

Graph-Based Learning: Adaptive graph representation learning models are used to detect texture and pattern similarities.

Patch-Based CNNs: The image is broken down into smaller sections, and similarity detection algorithms are applied to identify duplicated parts.

Advantages: Robust to transformations like rotation or scaling.

Challenges: Struggles with highly compressed or noisy images.

V. Analysis and Discussion

The paper provides a detailed framework for advancing cyber forensic security, particularly through a deep learning-based hybrid model. Traditional methods, which often rely on pixel-based or block-based analysis, are outperformed by the proposed solution, which excels in detecting advanced manipulations like copy-move forgery and image splicing. However, the system's computational demands and dependency on robust datasets could limit its adoption in resource-constrained environments.

Comparison of Methods

Method	Strengths	Weaknesses
Manipulation Detection	High accuracy for doctored media	Computationally expensive
Deepfake Detection	Effective for identity-related forensics	Requires large training datasets
Ontology-Based Frameworks	Enhances context understanding	Labor-intensive ontology creation
Copy-Move Forgery Detection	Robust to various transformations	Struggles with highly compressed data

Moreover, while the integration of blockchain technology and AI is briefly discussed, it opens avenues for future research, particularly in developing decentralized and immutable solutions for evidence validation. By focusing on deep learning techniques, this research enhances cyber forensics by addressing new and evolving security threats. Expanding this framework to encompass additional media types and integrating AI-driven evidence management systems could further enhance its utility in combating modern cybercrime challenges.

VI. Conclusion

Cyber forensic security for digital multimedia communication using advanced deep learning techniques. As digital communication increases, so does the complexity and prevalence of cybercrimes such as image forgery. Integrating CNNs with LSTM networks, this hybrid framework leverages the SHIFT algorithm to optimize image forgery identification and positioning. The system effectively addresses challenges like copy-move forgery and image splicing, offering precise tampering classification and localization via bounding boxes. This robust model sets a new standard for tackling the limitations of traditional forensic methods and adapting to sophisticated manipulation techniques.

References

[1] B. Pravallika, J. Sasikala, and S. Reddy, 'A Survey on Image Forgery Detection and Classification Using Machine Learning Forensic Approaches,' International Journal of Creative Research Thoughts (IJCRT), vol. 12, no. 6, June 2024.

[2] B. Mahdian and S. Saic, 'A bibliography on blind methods for identifying image forgery,' Signal Processing: Image Communication, vol. 25, pp. 389-399, 2010.

[3] J. Li, X. Li, B. Yang, and X. Sun, 'Segmentation-based image copy-move forgery detection scheme,' IEEE Transactions on Information Forensics and Security, vol. 10, no. X, pp. 507-518, 2015.

[4] H.-D. Yuan, 'Blind forensics of median filtering in digital images,' IEEE Transactions on Information Forensics and Security, vol. 6, no. X, pp. 1235-1245, 2011.

[5] R. P. Singh, N. H. Sree, K. L. S. P. Reddy, and K. Jashwanth, 'Convergence of deep learning and forensic methodologies using self-attention integrated EfficientNet model for deepfake detection,' SN Computer Science, vol. 5, article no. 1129, Dec. 2024.

[6] F. Ekundayo, 'Big data and machine learning in digital forensics: Predictive technology for proactive crime prevention,' Complexity, vol. 24, no. 2, pp. 2692-2709, Nov. 2024.

[7] R. T. Yadav, 'AI-driven digital forensics,' International Journal of Scientific Research & Engineering Trends (IJSRET), vol. 10, no. 4, July-Aug. 2024.

[8] E. Casey, Digital Forensics and Investigations: People, Process, and Technologies. Elsevier, 2019. Forensic Science International: Digital Investigation, vol. 32, no. X, 200888, Mar. 2020.

[9] X. Li and Z. Qin, 'Blockchain technology in digital forensics: Challenges and opportunities,' IEEE Access, vol. 10, pp. 1-14, 2022.

[10] T. T. Nguyen and X. Wang, 'AI in big data forensics: Techniques and applications,' Journal of Forensic Sciences, vol. 66, no. 1, pp. 23-35, 2021.

[11] R. T. Yadav, 'AI-driven digital forensics,' International Journal of Scientific Research & Engineering Trends (IJSRET), vol. 10, no. 4, July-Aug. 2024.