ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

**Research Paper**

# Hybrid Deep Learning and Forensic Approach for Satellite Image Forgery Detection

Pendem Pavan Kumar,
PG Scholar,
Department of Computer Science and Engineering,
Jawaharlal Nehru Technological University Hyderabad University College of Engineering Jagtial (Autonomous),
Nachupally (Kondagattu),
Telangana, India – 505501.
pavankumarpendem0072@gmail.com

Dr. B. Sateesh Kumar,
Professor,
Department of Computer Science and Engineering,
Jawaharlal Nehru Technological University Hyderabad University College of Engineering Jagtial (Autonomous),
Nachupally (kondagattu),
Telangana, India – 505501.
sateeshbkumar@jntuh.ac.in

## ABSTRACT

The rapid growth of remote sensing technologies and the increasing availability of high-resolution satellite imagery have significantly expanded their applications in environmental monitoring, urban planning, disaster management, military surveillance, and geospatial intelligence. However, the widespread accessibility of advanced image editing tools has also increased the risk of satellite image manipulation, raising serious concerns regarding data authenticity, reliability, and forensic integrity. Conventional image forensic techniques often rely on handcrafted features and statistical analysis, which exhibit limited robustness against sophisticated manipulations such as copy-move, splicing, object insertion, object removal, and region replacement. To address these challenges, recent research has increasingly adopted deep learning-based approaches that automatically learn discriminative representations for forgery detection and localization. Furthermore, hybrid frameworks integrating digital image forensic techniques with convolutional neural networks have demonstrated improved capability in identifying both semantic inconsistencies and low-level manipulation traces. This survey presents a comprehensive review of existing literature on hybrid deep learning and forensic approaches for satellite image forgery detection. The surveyed studies are systematically categorized based on forensic methodologies, deep learning architectures, hybrid feature extraction strategies, and manipulation localization techniques. The survey further analyzes commonly used datasets, evaluation metrics, existing challenges, and emerging research trends while identifying critical research gaps related to cross-domain generalization, multi-task learning, explainable artificial intelligence, and real-time deployment. This survey provides a structured reference for researchers and practitioners seeking to advance robust, scalable, and reliable satellite image forgery detection systems.

***Index Terms:*** *Satellite image forgery detection, digital image forensics, deep learning, remote sensing, manipulation localization, convolutional neural networks, hybrid forensic approaches.*

## INTRODUCTION

Satellite imagery has become an indispensable resource for numerous applications, including environmental monitoring, precision agriculture, urban planning, disaster management, military surveillance, and geospatial intelligence [1]. The continuous advancement of remote sensing technologies and the availability of high-resolution satellite sensors have enabled the acquisition of detailed Earth observation data with unprecedented spatial and temporal resolution [2]. These images support critical decision-making processes in both civilian and defense sectors, where the authenticity and reliability of visual information are of paramount importance. However, the rapid evolution of sophisticated image editing software and artificial intelligence-based manipulation techniques has significantly increased the possibility of generating forged satellite images that are visually convincing yet intentionally misleading [3].

Satellite image forgery involves unauthorized modifications such as copy-move manipulation, image splicing, object insertion, object removal, region replacement, and other composite editing operations that alter the original scene while concealing evidence of tampering [4]. Such manipulations can lead to incorrect geographic interpretations, inaccurate environmental assessments, compromised military intelligence, and unreliable disaster response planning. Consequently, ensuring the integrity and authenticity of satellite imagery has emerged as a critical research problem within the fields of remote sensing, computer vision, and digital image forensics [5].

Traditional satellite image forgery detection techniques primarily rely on handcrafted features, statistical analysis, and signal-processing methods to identify inconsistencies introduced during image manipulation [6]. Although these approaches provide satisfactory performance for certain manipulation types, they often struggle to detect complex and carefully crafted forgeries due to variations in sensor characteristics, image compression, illumination, spatial resolution, and post-processing operations. Recent advances in deep learning have significantly transformed this research area by enabling automatic feature learning through convolutional neural networks, transformer-based architectures, attention mechanisms, and multi-task learning frameworks capable of jointly performing forgery classification and pixel-level localization [7].

More recently, hybrid approaches that combine deep learning with digital image forensic techniques have demonstrated promising performance by integrating semantic scene understanding with low-level forensic evidence [8]. These frameworks exploit both visual content and manipulation artifacts to improve detection accuracy, robustness, and localization precision across diverse forgery scenarios. Despite substantial progress, the existing literature remains fragmented, with studies focusing on individual algorithms, datasets, or specific manipulation categories without providing a unified perspective on hybrid forensic methodologies [9].

This survey presents a comprehensive review of hybrid deep learning and forensic approaches for satellite image forgery detection. The survey systematically categorizes existing techniques, compares their methodologies, discusses commonly used datasets and evaluation metrics, analyzes current research challenges, and identifies emerging directions for future investigation. By synthesizing recent developments, this survey aims to provide researchers and practitioners with a structured understanding of the current state of the art while highlighting opportunities for developing more accurate, interpretable, and scalable satellite image forgery detection systems [10].

## SURVEY METHODOLOGY

This survey adopts a systematic literature review methodology to provide a comprehensive and unbiased analysis of existing research on satellite image forgery detection using hybrid deep learning and digital image forensic approaches. The review process was designed to identify, evaluate, and synthesize recent contributions in the fields of remote sensing, computer vision, image forensics, and artificial intelligence. A structured methodology was followed to ensure the inclusion of high-quality studies while minimizing selection bias and maintaining consistency throughout the literature analysis [11].

### Data Sources

The literature was collected from internationally recognized digital libraries and academic databases, including **IEEE Xplore**, **ScienceDirect**, **SpringerLink**, **Scopus**, **ACM Digital Library**, and **Google Scholar [12]**. These repositories provide extensive collections of peer-reviewed journal articles, conference proceedings, and review papers related to remote sensing, digital image forensics, deep learning, and satellite image analysis.

### Search Strategy

A keyword-based search strategy was employed using combinations of relevant terms such as *satellite image forgery detection*, *digital image forensics*, *remote sensing image manipulation*, *deep learning*, *convolutional neural networks*, *copy-move forgery detection*, *image splicing detection*, *forgery localization*, *hybrid forensic methods*, and *image authentication*. Boolean operators (AND, OR, and NOT) were used to refine search queries and retrieve the most relevant publications. Additional studies were identified through citation analysis of highly referenced research articles.

### Inclusion and Exclusion Criteria

The inclusion criteria for this survey were defined as follows:

- Peer-reviewed journal articles and conference papers.
- Publications written in English.
- Studies published between **2016 and 2025**.
- Research focusing on satellite image forgery detection, digital image forensics, deep learning, hybrid forensic frameworks, or manipulation localization.

The exclusion criteria included:

- Non-peer-reviewed articles, editorials, tutorials, and opinion papers.
- Studies unrelated to satellite imagery or image forgery detection.
- Duplicate publications and incomplete research reports.

- Articles lacking sufficient technical or experimental details.

### Study Selection and Analysis

The collected publications were initially screened based on their titles and abstracts to determine their relevance to the survey topic. Subsequently, full-text analysis was conducted on the shortlisted papers to examine their methodologies, datasets, deep learning architectures, forensic techniques, evaluation metrics, and reported limitations. The selected studies were systematically categorized according to their primary research focus, including traditional forensic methods, deep learning-based approaches, hybrid deep learning and forensic frameworks, and forgery localization techniques. A qualitative comparative analysis was then performed to identify prevailing research trends, strengths, limitations, and open research challenges, thereby providing a structured overview of the current state of satellite image forgery detection research.

## TAXONOMY AND CLASSIFICATION OF EXISTING APPROACHES

To systematically analyze the existing literature on satellite image forgery detection, this survey categorizes prior research based on the underlying detection methodology and the type of features utilized for identifying image manipulations. The proposed taxonomy classifies the surveyed studies into four major categories: traditional digital image forensic approaches, deep learning-based detection methods, hybrid deep learning and forensic approaches, and forgery localization techniques [13]. This classification facilitates a comprehensive comparison of existing methods while highlighting the evolution of satellite image forgery detection from conventional handcrafted feature extraction to advanced multi-task deep learning frameworks.

### Traditional Digital Image Forensic Approaches

Traditional digital image forensic approaches focus on detecting image manipulation through handcrafted features, statistical inconsistencies, and signal-processing techniques. These methods analyze artifacts introduced during image acquisition or editing, including sensor noise, compression signatures, color inconsistencies, resampling traces, and frequency-domain characteristics. Techniques such as copy-move forgery detection using keypoint descriptors, block-matching algorithms, discrete cosine transform (DCT), discrete wavelet transform (DWT), principal component analysis (PCA), and error level analysis (ELA) have been widely investigated. Although these approaches are computationally efficient and interpretable, their performance is often limited when confronting sophisticated image manipulations, multiple editing operations, or complex satellite scenes with varying spatial resolutions and environmental conditions [14].

**Deep Learning-Based Detection Approaches**

Recent research has increasingly adopted deep learning techniques to automatically learn discriminative representations directly from satellite imagery. Convolutional neural networks (CNNs), residual networks (ResNet), DenseNet, EfficientNet, Vision Transformers (ViT), and attention-based architectures have demonstrated remarkable performance in detecting forged satellite images. Unlike conventional methods, these models eliminate the need for handcrafted feature engineering by learning hierarchical semantic features from large-scale datasets. Several studies further incorporate transfer learning, feature pyramid networks, and transformer-based attention mechanisms to improve detection accuracy and robustness across different manipulation categories. However, deep learning models generally require extensive annotated datasets, significant computational resources, and careful optimization to achieve reliable generalization across diverse remote sensing environments.

**Hybrid Deep Learning and Forensic Approaches**

Hybrid approaches combine the complementary strengths of digital image forensics and deep learning to improve both forgery detection and manipulation analysis. These methods integrate low-level forensic evidence, such as noise residuals, high-pass filtering, sensor artifacts, or Spatial Rich Model (SRM) residual features, with high-level semantic representations extracted by deep neural networks [15]. Multi-stream architectures, feature fusion strategies, attention mechanisms, and multi-task learning frameworks have become increasingly popular for simultaneously learning semantic context and forensic traces. Such hybrid models demonstrate improved robustness against complex manipulations, cross-dataset variations, and post-processing operations while providing more reliable detection performance than either forensic or deep learning techniques used independently.

**Forgery Localization and Multi-Task Learning Approaches**

Beyond binary forgery detection, recent studies increasingly focus on accurately localizing manipulated regions within satellite images. Pixel-level forgery localization enables forensic analysts to identify the precise boundaries of tampered areas, thereby improving the interpretability and practical usefulness of detection systems. Encoder-decoder architectures such as U-Net, U-Net++, DeepLab, HRNet, and other segmentation networks are widely employed to generate manipulation masks. More advanced multi-task learning frameworks jointly perform authenticity classification, manipulation category recognition, and pixel-level localization within a unified architecture. These integrated approaches provide comprehensive forensic evidence by simultaneously determining whether an image has been manipulated, identifying the manipulation type, and highlighting the affected regions, making them particularly suitable for practical remote sensing forensic applications.

## COMPARATIVE ANALYSIS OF SURVEYED STUDIES

This section presents a comparative analysis of the existing literature on satellite image forgery detection, focusing on the evolution of traditional forensic methods, deep learning models, hybrid detection frameworks, and forgery localization techniques. The comparison is based on the primary objectives, underlying methodologies, application domains, strengths, and reported limitations of the surveyed studies. Analyzing these approaches collectively provides valuable insights into current research trends and identifies areas requiring further investigation [16].

### Comparison of Traditional Digital Image Forensic Techniques

Traditional digital image forensic techniques primarily rely on handcrafted features and statistical analysis to identify inconsistencies introduced during image manipulation. Common approaches include copy-move detection using feature matching algorithms, frequency-domain analysis based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), Error Level Analysis (ELA), sensor pattern noise analysis, and resampling artifact detection. These methods are computationally efficient and provide interpretable forensic evidence; however, their effectiveness decreases when images undergo multiple editing operations, geometric transformations, compression, or sophisticated post-processing. Furthermore, handcrafted feature extraction often lacks the adaptability required to detect emerging manipulation techniques in high-resolution satellite imagery.

### Comparison of Deep Learning-Based Detection Methods

Deep learning-based approaches have significantly improved the performance of satellite image forgery detection by automatically learning hierarchical feature representations from large-scale datasets. Convolutional Neural Networks (CNNs), ResNet, DenseNet, EfficientNet, Vision Transformers (ViT), and attention-based models have demonstrated superior capability in identifying complex manipulation patterns compared to conventional forensic techniques. Transfer learning and multi-scale feature extraction further enhance model generalization across different satellite datasets [17]. Nevertheless, these methods require extensive labeled training data, high computational resources, and careful hyperparameter optimization. In addition, many deep learning models function as black-box systems, limiting their interpretability and reducing user confidence in forensic investigations.

**Comparison of Hybrid Deep Learning and Forensic Approaches**

Recent studies increasingly adopt hybrid frameworks that integrate digital image forensic techniques with deep learning architectures to exploit both low-level manipulation artifacts and high-level semantic information. These approaches combine forensic residual extraction, high-pass filtering, noise analysis, or Spatial Rich Model (SRM) features with convolutional neural networks or transformer-based architectures. Feature fusion mechanisms, attention modules, and multi-task learning strategies enable these systems to achieve higher robustness against complex image manipulations while improving forgery classification and localization accuracy. Although hybrid frameworks generally outperform standalone forensic or deep learning approaches, they introduce increased architectural complexity, higher computational cost, and greater dependence on balanced and well-annotated datasets [18].

**Comparison of Forgery Localization Techniques**

Forgery localization has emerged as a critical component of modern satellite image forensic systems because identifying manipulated regions provides stronger forensic evidence than simple binary classification. Encoder-decoder segmentation networks, including U-Net, U-Net++, DeepLab, HRNet, and related architectures, are widely employed to generate pixel-level manipulation masks. More advanced multi-task frameworks simultaneously perform authenticity verification, manipulation category classification, and localization within a unified model, thereby improving overall forensic analysis. Despite these advancements, localization accuracy often deteriorates for very small tampered regions, blurred boundaries, compressed images, or images containing multiple manipulation types, highlighting the need for more robust and fine-grained localization strategies.

**Comparative Summary**

Table I presents a concise comparison of the major categories of satellite image forgery detection approaches discussed in the surveyed literature.

**Table I. Comparative Summary of Surveyed Studies**

| Approach Category | Techniques Used | Application Focus | Reported Limitations |
|---|---|---|---|
| Traditional Digital Image Forensics | DCT, DWT, ELA, PCA, Feature Matching, Sensor Noise Analysis | Detection of copy-move, splicing, resampling, and compression artifacts | Limited robustness against complex manipulations, geometric transformations, and post-processing operations |
| Deep Learning-Based Methods | CNN, ResNet, DenseNet, EfficientNet, Vision Transformer, Attention Networks | Automatic forgery detection and manipulation classification | Large annotated datasets required, high computational cost, limited model interpretability |
| Hybrid Deep Learning and Forensic Methods | SRM Filtering, High-Pass Residual Learning, Feature Fusion, Multi-Task Learning, CNN-Forensic Integration | Joint semantic and forensic feature extraction for robust forgery detection | Increased model complexity, longer training time, dependence on balanced datasets |
| Forgery Localization Approaches | U-Net, U-Net++, DeepLab, HRNet, Encoder-Decoder Networks, Pixel-Level Segmentation | Pixel-level localization of manipulated regions and forensic evidence generation | Reduced accuracy for small manipulated regions, blurred boundaries, and multiple simultaneous manipulations |

## DATASETS AND EVALUATION METRICS

The performance and reliability of satellite image forgery detection techniques largely depend on the availability of benchmark datasets and standardized evaluation metrics. Publicly available datasets enable researchers to train, validate, and compare different forensic algorithms under diverse manipulation scenarios, while evaluation metrics provide objective measures for assessing detection accuracy, localization performance, and model robustness. Although this survey does not introduce new datasets or experimental results, it summarizes the datasets and evaluation criteria that are most frequently adopted in the existing literature.

### Commonly Used Datasets

#### Satellite Image Forgery Datasets

- **DeepGlobe Satellite Dataset:** One of the widely used remote sensing datasets containing high-resolution satellite imagery. Several studies utilize this dataset to generate authentic and manipulated image samples for evaluating forgery detection and localization algorithms.
- **WHU-RS19 Dataset:** A publicly available remote sensing image dataset frequently employed for image analysis and forensic research. Researchers often create manipulated versions of these images to evaluate copy-move, splicing, and object manipulation detection methods.
- **UC Merced Land Use Dataset:** This dataset contains aerial and satellite scene images representing diverse land-use categories. It is commonly adopted for evaluating deep learning models under various manipulation scenarios and environmental conditions.
- **AID (Aerial Image Dataset):** A large-scale aerial image dataset comprising multiple scene categories with varying spatial resolutions. The dataset is widely used for transfer learning, feature extraction, and performance evaluation of satellite image forgery detection frameworks.

#### Digital Image Forensics Datasets

- **CASIA Image Tampering Dataset:** One of the most extensively used benchmark datasets for image forgery detection, containing authentic and manipulated images generated through splicing and copy-move operations. It is frequently employed for pretraining and validating deep learning-based forensic models.

- **Coverage Dataset:** Designed specifically for evaluating copy-move forgery detection algorithms, this dataset includes realistic manipulations with various geometric transformations and challenging background textures.
- **CoMoFoD (Copy-Move Forgery Detection Dataset):** A benchmark dataset containing copy-move manipulated images subjected to multiple post-processing operations such as rotation, scaling, noise addition, and compression, enabling comprehensive robustness evaluation.

**Evaluation Metrics**

The effectiveness of satellite image forgery detection methods is commonly assessed using classification, localization, and computational performance metrics reported throughout the literature.

**Classification Performance Metrics**

- Accuracy
- Precision
- Recall (Sensitivity)
- F1-Score
- Receiver Operating Characteristic (ROC) Curve
- Area Under the ROC Curve (AUC)

These metrics evaluate the capability of a model to correctly distinguish authentic satellite images from manipulated images while minimizing false detections.

**Forgery Localization Metrics**

- Intersection over Union (IoU)
- Dice Similarity Coefficient (DSC)
- Pixel Accuracy
- Mean Intersection over Union (mIoU)
- Boundary F1-Score

These measures assess the quality of pixel-level segmentation by comparing the predicted manipulation mask with the corresponding ground-truth localization mask.

**Computational Performance Metrics**

- Inference Time
- Model Size
- Computational Complexity
- Floating Point Operations (FLOPs)
- Memory Consumption

These metrics evaluate the practical feasibility of deploying forgery detection models in real-time remote sensing applications where computational efficiency and scalability are critical.

The adoption of standardized datasets and comprehensive evaluation metrics enables consistent benchmarking of satellite image forgery detection techniques. However, the surveyed literature indicates considerable variation in dataset selection, manipulation generation strategies, and performance evaluation protocols, making direct comparison among different approaches challenging. The development of unified benchmark datasets and standardized evaluation frameworks remains an important research direction for advancing robust and reproducible satellite image forensic systems.

## CHALLENGES AND OPEN RESEARCH ISSUES

Despite substantial advancements in digital image forensics and deep learning, satellite image forgery detection remains a highly challenging research problem. The surveyed literature reveals several technical limitations that affect the reliability, scalability, interpretability, and practical deployment of existing approaches. These challenges arise from the unique characteristics of remote sensing imagery, the increasing sophistication of image manipulation techniques, and the lack of standardized forensic benchmarks [19].

**Limited Availability of Large-Scale Annotated Datasets**

Deep learning models require extensive labeled datasets containing both authentic and manipulated images to achieve robust generalization. However, publicly available satellite image forgery datasets remain limited in size, diversity, and manipulation complexity. Many studies generate synthetic manipulations using custom procedures, resulting in datasets that differ significantly in editing strategies, image resolutions, and annotation quality. The absence of large-scale, standardized benchmark datasets restricts fair comparison among methods and reduces the ability of trained models to generalize across unseen satellite imagery.

**Cross-Dataset Generalization and Domain Adaptation**

Satellite images are acquired using different sensors, spatial resolutions, spectral bands, and environmental conditions. Models trained on one dataset often experience significant performance degradation when evaluated on images captured from different satellites or geographical regions [20]. Variations in illumination, atmospheric conditions, seasonal changes, and compression settings further complicate the detection process. Developing domain-adaptive and cross-dataset generalizable forgery detection models therefore remains an important open research issue.

**Detection of Sophisticated and Multi-Step Manipulations**

Modern image editing tools and AI-based content generation techniques can create highly realistic satellite image manipulations that preserve visual consistency while removing obvious forensic traces. Existing methods often perform well on single manipulation types such as copy-move or splicing but struggle when confronted with multiple simultaneous manipulations, object insertion combined with post-processing, or adversarially modified images. Detecting such sophisticated manipulations while maintaining high localization accuracy continues to be a major challenge.

**Explainability and Interpretability**

Many deep learning-based forgery detection systems operate as black-box models, providing predictions without clearly explaining the underlying forensic evidence. In critical applications such as military intelligence, disaster response, and geospatial decision-making, analysts require interpretable outputs that justify why an image is considered forged. Although localization masks improve transparency, there is still a need for explainable artificial intelligence techniques that provide reliable and understandable forensic reasoning.

**Computational Complexity and Real-Time Deployment**

Advanced deep learning and hybrid forensic models often contain multiple processing branches, attention mechanisms, and segmentation modules that increase computational cost and memory requirements. High-resolution satellite imagery further intensifies this challenge because large images frequently require patch-based processing and reconstruction. Achieving real-time detection while maintaining high accuracy and localization performance remains difficult, particularly for resource-constrained environments and operational remote sensing systems.

**Lack of Standardized Evaluation Frameworks**

The surveyed studies employ diverse datasets, manipulation generation procedures, evaluation protocols, and performance metrics, making direct comparison between approaches difficult. Some studies emphasize classification accuracy, whereas others prioritize localization metrics such as IoU or Dice coefficient. The absence of universally accepted benchmark datasets and standardized evaluation frameworks hinders reproducibility and slows the systematic advancement of satellite image forgery detection research.

**Privacy, Security, and Adversarial Threats**

As forgery detection systems become increasingly dependent on deep learning, they also become vulnerable to adversarial attacks designed to deceive or bypass forensic models. Carefully crafted perturbations can significantly alter model predictions while remaining visually imperceptible. Furthermore, concerns related to secure data sharing, model robustness, and the integrity of forensic evidence introduce additional challenges for deploying forgery detection systems in real-world environments. Robust and attack-resistant forensic frameworks therefore represent an important direction for future research.

## FUTURE RESEARCH DIRECTIONS

The rapid advancement of deep learning, remote sensing technologies, and digital image forensics presents significant opportunities for improving satellite image forgery detection systems. Based on the challenges identified in the surveyed literature, several promising research directions have emerged that can enhance the accuracy, robustness, scalability, and practical applicability of future forensic frameworks.

**Explainable and Trustworthy Artificial Intelligence**

Although deep learning models have achieved remarkable detection performance, their decision-making processes often remain difficult to interpret. Future research should focus on developing explainable artificial intelligence (XAI) techniques that provide transparent reasoning for forgery predictions and clearly identify the forensic evidence supporting model decisions. Interpretable models can improve analyst confidence, facilitate forensic investigations, and support the adoption of satellite image forgery detection systems in high-stakes applications such as defense, disaster management, and national security.

**Advanced Hybrid Forensic Frameworks**

The integration of semantic feature learning with traditional forensic analysis has demonstrated considerable potential for improving forgery detection. Future studies should investigate more sophisticated hybrid architectures that combine spatial residual analysis, transformer-based attention mechanisms, frequency-domain representations, and multi-scale feature fusion. Such frameworks can better exploit both low-level manipulation traces and high-level contextual information, resulting in more robust detection across diverse manipulation scenarios.

**Domain Adaptation and Cross-Dataset Generalization**

A major limitation of existing approaches is their reduced performance when applied to satellite images captured by different sensors or geographical regions. Future research should explore domain adaptation, self-supervised learning, transfer learning, and few-shot learning techniques to improve cross-dataset generalization. Developing models capable of adapting to unseen imaging conditions without extensive retraining will significantly enhance their applicability in real-world remote sensing environments.

**Multi-Task Learning and Fine-Grained Localization**

Emerging forensic systems should extend beyond binary forgery detection by simultaneously performing manipulation classification, pixel-level localization, confidence estimation, and forensic evidence generation within a unified architecture. Future research can investigate advanced multi-task learning strategies that improve the accuracy of both classification and segmentation while reducing computational redundancy. More precise localization of small manipulated regions and complex editing operations will further strengthen forensic analysis.

**Robustness Against AI-Generated and Adversarial Manipulations**

The rapid evolution of generative artificial intelligence has introduced new forms of image manipulation that are increasingly difficult to detect using conventional forensic techniques.

Future studies should focus on developing robust detection models capable of identifying AI-generated content, diffusion-based image synthesis, and adversarial attacks designed to deceive deep learning models. Improving resilience against these emerging threats will be essential for maintaining the reliability and integrity of satellite image authentication systems.

**Standardized Benchmarking and Real-Time Deployment**

Future research should prioritize the development of standardized benchmark datasets, unified evaluation protocols, and reproducible experimental frameworks to enable fair comparison among competing approaches. In addition, lightweight deep learning architectures, model compression techniques, edge computing, and hardware-efficient implementations should be explored to support real-time satellite image forgery detection in operational remote sensing systems. Such advancements will facilitate the deployment of reliable forensic solutions for large-scale Earth observation and time-sensitive geospatial applications.

## DISCUSSION AND CONCLUSION

The surveyed literature demonstrates that satellite image forgery detection has evolved significantly from traditional digital image forensic techniques to advanced deep learning and hybrid forensic frameworks. Conventional methods based on handcrafted features, statistical analysis, and signal-processing techniques remain valuable for identifying specific manipulation artifacts; however, their performance is often limited when confronted with complex editing operations and diverse remote sensing conditions. Recent deep learning models have substantially improved forgery detection by automatically learning hierarchical feature representations, while hybrid approaches have further enhanced performance by integrating semantic information with low-level forensic evidence. This combination has enabled more accurate authenticity verification, manipulation classification, and pixel-level localization, making hybrid frameworks increasingly attractive for practical satellite image forensic applications.

**Trends and Key Insights**

The current research trend emphasizes the integration of digital image forensics with deep learning to develop robust, multi-task satellite image forgery detection systems. Attention mechanisms, transformer-based architectures, feature fusion strategies, and encoder-decoder segmentation networks have become prominent components of modern forensic frameworks.

Simultaneously, there is growing interest in explainable artificial intelligence, cross-domain generalization, and lightweight models suitable for real-time deployment. Despite these advancements, the surveyed studies continue to face challenges related to limited benchmark datasets, inconsistent evaluation protocols, computational complexity, and the increasing sophistication of AI-generated image manipulations. These observations indicate that future research should focus on developing standardized datasets, interpretable detection models, and generalized forensic frameworks capable of operating reliably across diverse satellite imaging environments.

**Summary**

This survey systematically reviewed existing research on hybrid deep learning and forensic approaches for satellite image forgery detection by categorizing and comparing traditional forensic methods, deep learning-based techniques, hybrid architectures, and forgery localization frameworks. The survey also summarized commonly used datasets, evaluation metrics, current research challenges, and emerging directions for future investigation. The comprehensive analysis indicates that hybrid approaches combining semantic feature learning with forensic evidence extraction provide a promising foundation for developing accurate, robust, and scalable satellite image authentication systems. As remote sensing applications continue to expand across environmental monitoring, defense, disaster management, and geospatial intelligence, the development of reliable and interpretable forgery detection techniques will remain a critical research priority for ensuring the authenticity, integrity, and trustworthiness of satellite imagery.

## REFERENCES

[1] I. Demir et al., “DeepGlobe 2018: A Challenge to Parse the Earth through Satellite Images,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, 2018.

[2] S. K. Yarlagadda, D. Güera, P. Bestagini, F. M. Zhu, S. Tubaro, and E. J. Delp, “Satellite Image Forgery Detection and Localization Using GAN and One-Class Classifier,” Electron. Imaging, pp. 214-1–214-9, 2018, doi: 10.2352/ISSN.2470-1173.2018.07.MWSF-214.

[3] J. Horvath, H. Hao, D. Mas Montserrat, and E. J. Delp, “Anomaly-Based Manipulation Detection in Satellite Images,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, pp. 62–71, 2019.

[4] J. Horvath, D. Mas Montserrat, H. Hao, and E. J. Delp, “Manipulation Detection in Satellite Images Using Deep Belief Networks,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, pp. 2832–2840, 2020.

[5] J. Horvath, S. Baireddy, H. Hao, D. Mas Montserrat, and E. J. Delp, “Manipulation Detection in Satellite Images Using Vision Transformer,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, pp. 1032–1041, 2021, doi: 10.1109/CVPRW53098.2021.00114.

[6] B. Zhao, S. Zhang, C. Xu, Y. Sun, and C. Deng, “Deep Fake Geography? When Geospatial Data Encounter Artificial Intelligence,” Cartogr. Geogr. Inf. Sci., vol. 48, no. 4, pp. 338–352, 2021, doi: 10.1080/15230406.2021.1910075.

[7] C. Gudavalli, E. Rosten, L. Nataraj, S. Chandrasekaran, and B. S. Manjunath, “SeeTheSeams: Localized Detection of Seam Carving Based Image Forgery in Satellite Imagery,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, pp. 1–11, 2022.

[8] F. F. Niloy, K. K. Bhaumik, and S. S. Woo, “HRFNet: High-Resolution Forgery Network for Localizing Satellite Image Manipulation,” in Proc. IEEE Int. Conf. Image Process., pp. 3165–3169, 2023, doi: 10.1109/ICIP49359.2023.10221974.

[9] X. Ding, Y. Nie, J. Yao, and Y. Lang, “Forensic Research of Satellite Images Forgery: A Comprehensive Survey,” Artif. Intell. Rev., 2024, doi: 10.1007/s10462-024-10909-w.

[10] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, “Learning Rich Features for Image Manipulation Detection,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., pp. 1053–1061, 2018.

[11] J. H. Bappy, A. K. Roy-Chowdhury, J. Bunk, L. Nataraj, and B. S. Manjunath, “Exploiting Spatial Structure for Localizing Manipulated Image Regions,” in Proc. IEEE Int. Conf. Comput. Vis., pp. 4970–4979, 2017.

[12] Y. Wu, W. AbdAlmageed, and P. Natarajan, "ManTra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries with Anomalous Features," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., pp. 9543–9552, 2019.

[13] X. Bi, Y. Wei, B. Xiao, and W. Li, "RRU-Net: The Ringed Residual U-Net for Image Splicing Forgery Detection," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, 2019.

[14] M.-J. Kwon, I.-J. Yu, S.-H. Nam, and H.-K. Lee, "CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing," in Proc. IEEE Winter Conf. Appl. Comput. Vis., pp. 375–384, 2021.

[15] X. Chen, C. Dong, J. Ji, J. Cao, and X. Li, "Image Manipulation Detection by Multi-View Multi-Scale Supervision," in Proc. IEEE/CVF Int. Conf. Comput. Vis., pp. 14185–14193, 2021.

[16] J. Wang et al., "ObjectFormer for Image Manipulation Detection and Localization," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., pp. 2364–2373, 2022.

[17] S. Das, M. S. Islam, and M. R. Amin, "GCA-Net: Utilizing Gated Context Attention for Improving Image Forgery Localization and Detection," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, pp. 81–90, 2022.

[18] S. Agrawal et al., "SISL: Self-Supervised Image Signature Learning for Splicing Detection and Localization," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops, pp. 22–32, 2022.

[19] F. Guillaro, D. Cozzolino, A. Sud, N. Dufour, and L. Verdoliva, "TruFor: Leveraging All-Round Clues for Trustworthy Image Forgery Detection and Localization," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., pp. 20606–20615, 2023.

[20] X. Guo, X. Liu, Z. Ren, S. Grosz, I. Masi, and X. Liu, "Hierarchical Fine-Grained Image Forgery Detection and Localization," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., pp. 3155–3165, 2023.