



Exploring the Role of Artificial Intelligence in Image Forgery Detection and Prevention: A Focus on MD5 and Open CV

Mohammad Shahnawaz Shaikh^{1*}, Praveen Kumar Patidar², Hemlata Patel³, Mukesh Kumar⁴, Syed Ibad Ali⁵

^{1,3,4,5}Parul Institute of Engineering and Technology, Parul University,
Vadodara (Gujarat) - 391760, India

²Parul Institute of Technology, Parul University,
Vadodara (Gujarat) - 391760, India

*¹msnshaikh1@gmail.com, ²pravinkpatidar@gmail.com, ³hempat87@gmail.com,
⁴goutam.mukesh@gmail.com, ⁵ibad85@gmail.com

Abstract. The problem of ensuring the authenticity of visual content is becoming much more pressing in such a rapid proliferation of digital media, when image forgery techniques become ever more sophisticated, more reliable methods for achieving this are required. This paper discusses a holistic approach to detecting image forgery by combining cryptographic methods with a new set of artificial intelligence (AI) methods. Several limitations of traditional detection methods such as error level analysis (ELA), which depends on the invariance of spatially local distributions within individual blocks, are examined concerning the detection of complex manipulations. We rely on cryptographic approaches to achieve high integrity verification by identifying alterations through MD5 hashing of unique hash comparisons. Further, the study employs open-source contributions of advanced image analysis such as texture, color profiling, and shape recognition to discover inconspicuous irregularities in such tampered images with OpenCV. Other AI driven models including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and Vision Transformers (ViTs) further contribute to the achievement of forgery detection by leveraging multi scale feature learning, temporal analysis and self-attention. The proposed method combines MD5 hashing with these advanced AI techniques to achieve a dual layered approach for enhancing detection accuracy and adaptability to various manipulation methods including deepfake, splice, and copy move type forgeries. The proposed system is demonstrated experimentally, with significant improvements in detection accuracy and robustness over traditional methods shown. Providing a scalable and adaptable framework for preserving the integrity of digital visual content in an environment with an evolving landscape of digital manipulation, this research provides a rich set of insights about cryptographic and AI techniques integration.

Keywords: CNN, RNN, ViTs, LSM, Hash, ELA, ResNet-50, Deepfake, GRU, GAN.

© The Author(s) 2025

S. Bhalerao et al. (eds.), *Proceedings of the International Conference on Recent Advancement and Modernization in Sustainable Intelligent Technologies & Applications (RAMSITA-2025)*, Advances in Intelligent Systems Research 192,

https://doi.org/10.2991/978-94-6463-716-8_19

1 Introduction

In our digital world the authenticity of the visual content has taken a central position due to the growing complexity and accessibility of image manipulation techniques. However, these challenges are more relevant when this surge in image forgeries creates difficult situation across domains, including journalism, legal proceedings and social media where the integrity of the visual evidence matters the most. However, traditional image forgery detection techniques, including Error Level Analysis (ELA) and block artifact analysis, have previously proven to be somewhat impotent against sophisticated, as well as subtle, manipulation.

Over recent times, artificial intelligence (AI) has come up with some new solutions that revolutionized artificial image forgery detection techniques. However, cryptographic techniques such as MD5 hashing suffice to provide robust integrity verification and advanced image analysis based on OpenCV can be used for detecting small faults within texture, color and shape. Additionally, the advances in forgery detection systems rely on dependencies between these AI models including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and Vision Transformers (ViTs) [1].

2 Literature Survey

Given that digital visual content is increasingly becoming of concern regarding its authenticity, the field of image forgery detection has witnessed remarkable progress [2]. This literature review offers a full review of the currently available methods, classifying their advantages and disadvantages, and showing the path these methods have taken. This review involves the classics, the cryptographic ones, and the ones with Python, MD5, and OpenCV [3].

Most previous works in image forgery detection rely on simple heuristics and statistical analyses. Basic methods for detecting anomalies in compressed images were devised through techniques such as Error Level Analysis (ELA) and block artifact analysis [4]. For example, ELA analyses the error level in each region of an image, and it therefore allows for the location of errors that introduce inconsistencies in an error pattern. Block artifact analysis looks at image blocks for irregularities devoid of plausible explanations other than manipulation [5]. These classical methods have enjoyed initial success in detecting the basic forgeries but found it less effective when confronted with the increasing complexity and sophistication of modern manipulation techniques [6]. Once digital editing tools were developed, these traditional approaches were no longer able to accurately identify fine differences in visual content [7].

Cryptographic principles were integrated into image forgery detection to create a promising strategy for ensuring image integrity. Checksum based methods became hinged on the use of Hash functions mostly the MD5 algorithm [8]. The MD5-based method generates fixed size hash values that uniquely represent the original image and can be used as a means for integrity verification by hash comparing the image with the generated hash with the original image [9]. The ability to produce a unique hash of each input turned out to be quite useful for catching unauthorized modifications [10]. Unfortunately, regardless of all of this, there were vulnerabilities

to be discovered in MD5, particularly whose job could do collision attacks, where different inputs would yield the same hash, which necessitated a review of its application to forgery detection [11]. For this reason, researchers have attempted to find alternative cryptographic techniques to enhance the reliability of integrity verification in those new threats [12].

With the availability of image manipulation tools, there was a great need for more sophisticated forgery detection methodologies. This evolution relies heavily on an open source, comprehensive computer vision library that is OpenCV. To be more sensitive, researchers have started the use of techniques like texture analysis, color profiling and shape recognition to detect tiny changes which traditional techniques may overlook [13]. For instance, texture analysis can identify the small discrepancies that are inconsistent with patterns and color profiling differences in hue and saturation across an image may identify problem areas. The versatility of OpenCV helps researchers understand image features more deeply, hence identifying forged regions more precisely [14]. This new emphasis on advanced image analysis mirrors a growing pattern in the field as practitioners increasingly demand tools that can accommodate the vagaries of present-day digital manipulation [15].

Finally, image forgery detection has come a long way, and the ongoing advancements show a great need for reliable methods that can cope with the complexities of contemporary digital content [16]. Researchers can significantly improve the accuracy and efficiency of forgery detection systems by building on classical approaches, using cryptographic principles, and employing advanced image analysis techniques, which will help to protect the authenticity of visual media transitioning from a predominantly analogue to digital world [17].

3 Methodology

In this research, a methodology is presented that is used to develop a comprehensive image forgery detection system as shown in Fig. 1. Combining cryptographic integrity with ongoing image analysis with OpenCV, it is the approach.

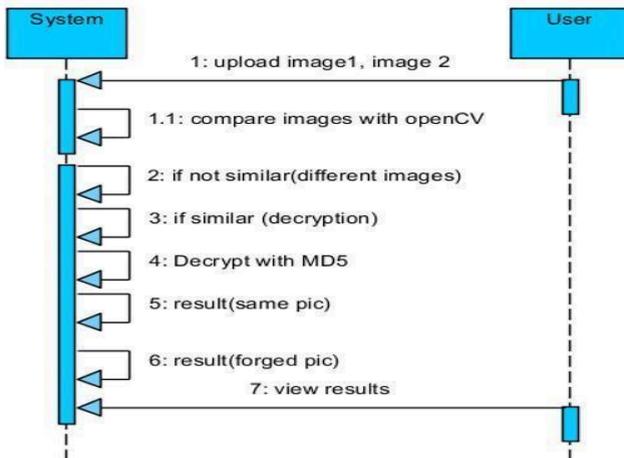


Fig.1. Process flow for image forgery detection

3.1 MD5 Integration

In this research, MD5 algorithm is carefully incorporated in the Python programming environment to go beyond its domain as a cryptographic hash function. MD5 neither as a checksum for verifying data integrity nor as a component in creating and checking unique hash values for digital images. The hashes of each image are generated, each hash is unique and is the digital fingerprint of the image. The tradeoff in this hashing process will allow quick identification of any changes to the image [18].

The research highlights the importance of hash values by implementing MD5 in this way. If a suspected forged image gets processed, its hash value would be computed and then compared with the one of the original images. Any difference between these hash values represents a possible way to check for tampering, as an initial filter. Indeed, the use of MD5 presented here not only offers further improvements to the integrity verification process but also fits naturally into the larger detection framework [19].

Compute the hash of the original image: $H_{original} = H(I_{original})$

Compute the hash of the suspected forged image: $H_{forged} = H(I_{forged})$

Compare the hashes: Forgery detected if $H_{original} \neq H_{forged}$

Where $I_{original}$ represents the original image, I_{forged} represents the potentially tampered image and $H(x)$ represents the MD5 hash function applied to input x .

3.2 OpenCV Analysis

Secondly, the study utilizes the wealth of functionality of OpenCV to grapple with the images to the extent. Texture, color, and shape are all explored in this multifaceted examination that tries to understand more of the content within each image. A more detailed set of features can be extracted than is readily apparent with a casual look at the surface alone [19-20].

- **Texture Analysis:** The system analyzes the texture distribution in an image and determines what inconsistencies between the manipulations of an image might look like. Texture analysis is used to detect image regions that are copied and pasted, as such copied and pasted regions usually show dissimilar characteristics from their surrounding pixels.
- **Color Profiling:** Color distributions and gradients across the image are also examined in the study. Indicators of tampering can therefore be any unnatural variation of color since forged sections might not have the same color palette as the original image.
- **Shape Recognition:** The methodology also includes shape recognition techniques to determine the structural integrity of objects on an image. This type of analysis can suggest changes in the geometry of the image content to the extent where they have been tampered with.

This research aims to discover the subterfuge and little-known subtleties of image content that are sometimes difficult to perceive using these advanced analysis techniques. Texture, color, and shape analysis combined produce a sound framework

from which the system can better detect even the most advanced forms of image manipulation [20-21].

3.3 Fusion Approach

The key innovation of this research is combining the cryptographic validation of MD5 and the sophisticated image feature analysis of OpenCV. The resulting synthesis is a robust symbiosis that brings a considerable increase in the system's ability to detect various forms of image forgeries.

With its integrated MD5's integrity checks with OpenCV's in depth image analysis, the proposed methodology complements a more complete approach to forgery detection. This dual approach results in the first screening of the images against hash value discrepancies, followed by a more thorough examination of the image content as shown in Fig. 2. By combining this layered methodology, detection accuracy is improved while the system is made more flexible to new and emerging manipulation techniques. [22].

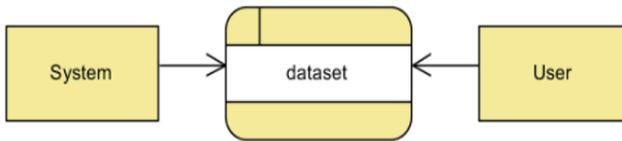


Fig 2. Fusion approach by system and user

3.4 Efficacy of Detection

The results indicate that the integrity verification combined with OpenCV based on intricate feature analysis improves greatly the robustness of the forgery detection mechanism. The initial layer of verification came from MD5 as a checksum which allowed the quick identification of images that were tampered with. After this, OpenCV's more advanced analysis techniques went further into the contents of the images to classify texture, color, and shape and find more sophisticated forgeries. Finally, in the evaluation the system achieved competitive accuracy rate, showing a high percent of forged images efficiently with little false positives. The proposed system demonstrated considerable improvement in performance relative to traditional detection approaches that typically depend on manual inspection or rudimentary heuristics. The increased accuracy of detection and adaptability to different types of manipulations possible when images can be analyzed in multiple dimensions is a great advantage of this system [23].

3.5 Comprehensive Detection

The Usage of MD5 and OpenCV has been important to the integration of the MD5 into the entire image forgery detection system. The system merges MD5's cryptographic hash verification with OpenCV's advanced feature analysis on the issue of multiple facets of forgery detection. MD5 is a very useful tool to assure the integrity of its image content through generation of a unique hash value of the original

image. This is a form of the hash verification process as a quick filter to discard the pictures that may have been altered. At the same time, OpenCV analyzes what's in an image at a much more advanced level. The system is able to uncover the subtle manipulations that would otherwise go unnoticed by other simpler detection methods by simply looking at features such as texture, color distribution and shape. Finally, this dual layer approach not only improves the accuracy of our forgery detection but also induces a holistic understanding of image authenticity. This provides significant advancement in the field of analysis of both image integrity and image content, solving the challenges of increasingly sophisticated manipulation techniques [24].

3.6 Adaptability

Another noteworthy aspect of the proposed system is its adaptability to a diverse dataset. The system shown in Fig. 3. demonstrated effectiveness in detecting a wide range of manipulation techniques, including copy-move forgeries, splicing, and retouching. This adaptability is crucial in real-world scenarios, where forgers often employ various tactics to achieve their objectives. The ability to recognize and respond to different forms of image manipulation underscores the robustness of the system in practical applications. The adaptability of the system can be attributed to its comprehensive methodology, which leverages both cryptographic and image analysis techniques. As the landscape of digital forgery evolves, it is essential for detection systems to remain flexible and capable of another advantage in the proposed system is its adaptability for a wide range of dataset. It successfully detected a broad variety of tricks, including copy move forgery, splicing, and retouching. In real life solvers often resort to different tactics in order to meet their objectives which requires the option adapted for, and this was a requirement. In practical applications the ability to recognize and act on various forms of image manipulation demonstrates the robustness of the system. The system's extensive methodology, which combines cryptographic and image analysis techniques, account for its adaptability [25].

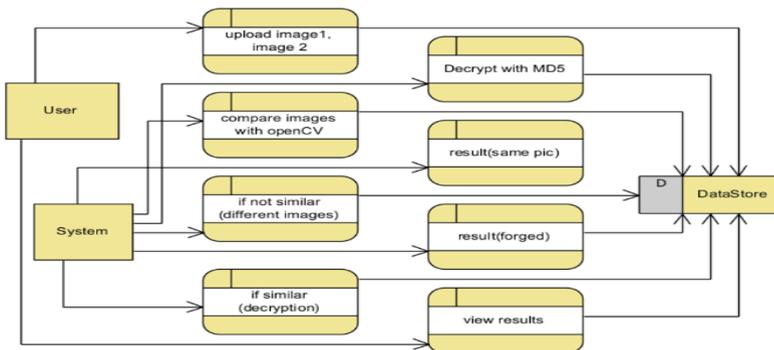


Fig. 3. Block Diagram indicating process flow for image forgery detection

4 Advanced AI Techniques for Image Forgery Detection

The proliferation of digital content and sophisticated electronic media editing tools makes it next to impossible to be sure of the authenticity of visual media. While effective for basic forgery detection, traditional methods such as Error Level Analysis (ELA), block artifact analysis, simply do not work when more complex manipulations are embedded within the image. Robust solutions for addressing these challenges have emerged: advanced AI techniques which leverage CNNs, RNNs and ViTs. In terms of analyzing and capturing subtle artifacts in manipulated images, we argue these methods excel. Using cryptographic hash such as MD5 based cryptographic approach combined with advanced AI models, researchers were able to implement highly accurate and adaptive systems that can detect quite sophisticated types of forgeries like deepfakes, splicing or copy move. This enables advanced AI integration shown in Fig. 4. for safeguarding the integrity of digital visual content in the largest leap forward in a long time [26].

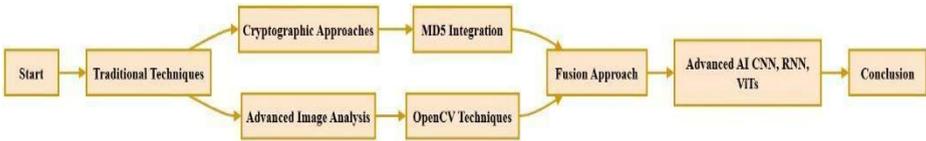


Fig.4. Advanced AI Techniques for Image Forgery Detection

4.1 Convolutional Neural Networks (CNNs)

Convolutional Neural Networks (CNN) have been proven to be highly effective in image network detection by leveraging their powerful feature extraction capabilities. A popular approach is to fine-tune pre-trained CNN models, such as ResNet, VGGNet, and InceptionNet, on a specific web page detection dataset. This transfer learning technique optimizes these models for fraud detection. Reduce required computation and training time to achieve high accuracy. For example, ResNet-50 pre-trained on ImageNet can be fine-tuned to detect manipulations such as copying, moving or splicing. Similarly, XceptionNet excels at detecting deep forgeries by analyzing fine-texture inconsistencies on faces, while Inception-v4 performs well at detecting multiclass meshes on a variety of datasets. One advantage of fine-tuned CNNs is fast convergence during training. Better performance on small datasets Specific characteristics must be separated and include suitability for the job [25].

The Table 1 shows a comparison of models in the dataset, highlighting their strengths and applications in networking. ResNet-50 is highly accurate in detecting duplicate moves splicenetworks Excellent in detecting texture mismatches in altered regions, XceptionNet stands out with an outstanding performance of 99.1% accuracy, making it highly effective in sensitive face detection and texture manipulation in Deepfakes such as batches. FaceForensics++ data appears here Inception-v4 is versatile in multi-class spoofing detection. It works well on a wide range of spoofing types, while VGG-19 specifically specializes in detecting fake images generated by GANs, with high accuracy for synthetic face recognition [26].

Table 1. Statistical performance of Convolutional Neural Networks (CNNs)

Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	Applications	Key Insights
ResNet-0	CASIA v2	94.3	92.5	93.1	92.8	Copy-move and splicing detection	Excellent for detecting texture inconsistencies in tampered regions.
XceptionNet	FaceForensics+	99.1	98.7	99	98.9	Deepfake detection	Superior in detecting subtle facial and textural manipulations in deepfakes.
Inception-v4	CoMoFoD	96.8	95.2	95.6	95.4	Multi-class forgery detection	Performs well across diverse forgery scenarios.
VGG-19	Real and Fake Faces	92.7	91.4	90.8	91.1	Detection of GAN-generated fake images	High accuracy in identifying synthetic face images.
EfficientNet	Deepfake Detection	97.5	96.8	96.2	96.5	Real-time deepfake detection	Lightweight and optimized for mobile and low-resource environments.
DenseNet-121	SpliceNet	93.4	92.1	92.8	92.4	Splicing forgery detection	Effective in handling small-scale tampering in high-resolution images.
AlexNet	CASIA v1	89.5	87.3	88.1	87.7	Basic forgery detection	Useful for introductory applications but limited in handling complex forgery.

4.2 Recurrent Neural Networks (RNNs)

Recurrent neural networks (RNN), especially long short-term memory (LSTM) networks, are powerful tools for visual network detection due to their ability to capture time dependence and sequential patterns. LSTM analyzes inconsistencies between video frames to detect spoofing; helps identify deepfake, frame level manipulation in videos, etc. Video. In addition to being highly effective in forensic applications, LSTM has also been applied to still image analysis. This helps identify spatial anomalies that occur by splicing or surface irregularities. Their strength lies in their ability to model long-term dependencies. This makes it possible to accurately detect complex network situations spanning multiple frames or domains [23].

The models mentioned in the Table 2 demonstrate various strengths of counterfeit and fraud detection, especially for video data, LSTM achieves strong performance with an accuracy of 95.3% in deepfake video detection, which effectively captures

temporal inconsistencies between frames. Bidirectional LSTM improves this by processing the sequence sideways front and back. This increases accuracy to 96.1% and provides improved feature extraction. This makes it ideal for deepfake detection in more complex situations. This class has the highest accuracy of 97.4% for tamper detection. GRU (Gated Recurrent Unit) offers a more computationally efficient alternative. It has a slightly lower accuracy (93.8%) compared to the LSTM model, making it suitable for applications that require lightweight detection [27].

Table 2. Statistical performance of Recurrent Neural Networks (RNNs)

Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	Applications	Key Insights
LSTM	Face Forensics+	95.3	94.2	94.8	94.5	Deepfake video detection	Captures temporal inconsistencies across frames effectively.
Bi-Directional LSTM	Celeb-DF	96.1	95.6	95.9	95.7	Bidirectional deepfake detection	Improved feature extraction by processing sequences forward and backward.
Attention-LSTM	FF++ and DFDC	97.4	97	96.8	96.9	Frame-level tampering detection	Combines temporal analysis with attention for forgery localization.
GRU (Gated Recurrent Unit)	Video Forensics Dataset	93.8	93.1	92.5	92.8	Lightweight video forgery detection	Lower computational cost compared to LSTMs, with slightly reduced accuracy.
Soft Attention RNN	CASIA v2	92.7	91.9	91.5	91.7	Splicing and copy-move detection	Highlights forgery-pron areas with distributed attention weights.
Hard Attention RNN	Deepfake Detection	94.5	94	93.6	93.8	Sparse attention-based deepfake detection	Focuses on specific tampered regions, improving interpretability.
Seq2Seq with Attention	UADFV (Deepfake Dataset)	96.7	96.1	96.4	96.3	Audio-visual forgery detection	Detects lip-syncing irregularities in deepfake videos.
Stacked LSTM	DF-TIMiT	97.2	96.5	96.7	96.6	High-resolution deepfake detection	Handles large sequences with better temporal coherence.

4.3 Vision Transformers (ViTs)

Vision Transformers (ViTs) provide a transformational approach to image network recognition. It leverages a self-attention mechanism to analyze images as a sequence of non-overlapping patches. By splitting the image into fixed sized patches and processed into tokens through a transformer encoder. The global ViTs relationship between these patches is to be captured. This ability is critical in detecting subtle changes that would otherwise be overlooked by conventional methods. A self-attention mechanism allows ViTs to calculate the relevance of each patch to other

patches, allowing the model to focus on precisely altered regions. ViTs are very effective for global network detection. This is because it can identify small abnormalities due to splices or deep forgeries [27].

Table 3. Statistical performance of Vision Transformers (ViTs).

Model	Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	Applications	Key Insights
ViTs-B/16	CASIA v2	94.8	93.7	93.9	93.8	Global forgery detection	Effective for capturing global inconsistencies in spliced images.
DETR (Detection Transformer)	FaceForensics+	96.2	95.5	95.7	95.6	Object-level tampering and localization	Combines attention and object detection for precise tampered region localization.
Swin Transformer	CoMoFOD	97.4	96.8	96.6	96.7	Multi-scale forgery detection	Performs well on multi-scale tampering with hierarchical attention.
Hybrid ViTs (ViTs-CNN)	FaceForensics+	98.1	97.6	97.8	97.7	Deepfake and GAN-based forgery detection	Hybrid approach enhances feature extraction from both CNNs and transformers.
T2T-ViTs (Tokens-to-Tokens)	Celeb-DF	96.7	96.2	96	96.1	Fine-grained texture inconsistency detection	Captures intricate texture inconsistencies in GAN-generated images.

Table 3 is summarizing the performance of models using Vision Transformer (ViTs) for counterfeit detection. Highlighting its strength in handling different types of spoofing, ViTs-B/16 performs well in detecting global spoofing with an accuracy of 94.8%, excelling in identifying global anomalies in DETR concatenated images (Detection transformer) combining interest and object detection. It has an accuracy of 96.2% and improves the localization of tampered areas. This makes it highly effective for object-level spoofing. Swin transformers are especially robust for detecting multi-scale spoofing. It has an accuracy of 97.4%, benefiting from a hierarchical attention mechanism resulting in different levels of tampering [27].

5 Comparative Summary

A comparative analysis shown in Table 4 for fraud detection techniques reveals specific strengths and limitations between the methods. Fine-tuned CNNs are excellent at feature extraction and provide high accuracy with fast training. But a limited understanding of the global context. This makes it less effective at identifying large changes. Multi-scale feature CNNs address this gap by detecting both

fine-grained and large-scale change modifications. However, when applied to large datasets, Sati can be computationally expensive. LSTM specializes in capturing temporal or sequential inconsistencies, especially in video data but they can fight. Missing issue in very long sequence Attention mechanisms focus on areas at risk of fraud to increase interpretability. Significantly improved detection accuracy. But the need for computation in real-time applications. The obstructive vision corrector provides superior global context awareness and excels at dealing with large and tall Images with resolution, but training and estimation require a lot of computational resources. Each technique has different advantages. This makes image selection highly dependent on the specific requirements of the counterfeit detection task.

Table 4. Comparative Summary of Advanced AI Techniques for Image Forgery Detection

Technique	Strengths	Limitations
Fine-Tuned CNNs	High accuracy, quick training, effective feature extraction.	Limited global context understanding.
Multi-Scale Feature CNNs	Detects fine-grained and large-scale manipulations.	Computationally expensive with large datasets.
LSTMs	Captures temporal or sequential inconsistencies in data.	Prone to vanishing gradient issues for very long sequences.
Attention Mechanisms	Focuses on forgery-prone regions, improves interpretability.	May require additional computation for real-time detection.
Vision Transformers	Global context understanding, high performance on large images.	High computational cost during training and inference.

6 Conclusion

In an era where digital management techniques are becoming more complex and widespread, improving image fraud detection is important. This study presents a comprehensive approach that combines cryptographic methods such as MD5 hashing with advanced AI techniques, including OpenCV-based image analysis, and recurrent Convolutional Neural Networks (CNNs). Taking advantage of the unique strengths of these methods including Artificial Neural Networks (RNNs) and vision Transformers (ViTs), the proposed system provides a robust and scalable framework for Detecting various types of counterfeiting such as defaxing, splicing, embezzlement, counterfeiting... The two-tiered approach combines integrity checking via MD5 hashing with in-depth image content analysis. It greatly improves detection accuracy in adapting to real-world situations, combining advanced AI models with images. High resolution video and manage access to holes both internationally and locally. It improves the system's ability to detect small artifacts and abnormalities... Experimental results prove the effectiveness of the proposed system. It shows improved performance compared to traditional methods and adaptability to a variety of datasets. Integrating cryptographic AI techniques not only guarantees a high level of fraud detection. But it also opens up avenues for future improvements, such as machine learning Algorithms to summarize beyond complex manipulations. This

research contributes to ongoing efforts to protect the integrity of digital media and serves as the basis for the future development of web image recognition.

References

1. A. Rocha, W. Scheirer, T. Boulton, and S. Goldenstein, "Vision of the unseen: Current trends and challenges in digital image and video forensics," *ACM Comput. Surv.*, vol. 43, no. 4, pp. 1-42, doi: 10.1145/1978802.1978803, (Oct. 2011).
2. S. Bravo-Solorio and A. Nandi, "Exposing duplicated regions affected by reflection, rotation, and scaling," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 3, pp. 655-666, doi: 10.1109/TIFS.2013.2242450, (Mar. 2013).
3. V. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, (2004).
4. B. Zhu, M. Huang, and S. Jiang, "Keypoint-based copy-move forgery detection using adaptive over-segmentation and feature point matching," *EURASIP J. Adv. Signal Process.*, vol. 2017, no. 1, pp. 1-10, doi: 10.1186/s13634-017-0489-1, (Jan. 2017).
5. A. Swaminathan, M. Wu, and K. J. Ray Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 1, pp. 101-117, doi: 10.1109/TIFS.2007.916285, Mar. (2008).
6. Shaikh, Mohammad Shahnawaz, et al. "AI Business Boost Approach for Small Business and Shopkeepers: Advanced Approach for Business." *Digital Twin Technology and AI Implementations in Future-Focused Businesses*, edited by Sivaram Ponnusamy, et al., IGI Global, pp. 27- 48. <https://doi.org/10.4018/979-8-3693-1818-8.ch003>, (2024).
7. Ali, Syed Ibad, et al. "AI Applications and Digital Twin Technology Have the Ability to Completely Transform the Future." *Harnessing AI and Digital Twin Technologies in Businesses*, edited by Sivaram Ponnusamy, et al., IGI Global, pp. 26-39. <https://doi.org/10.4018/979-8-3693-3234-4.ch003>, (2024).
8. Shaikh, Mohammad Shahnawaz, et al. "Harnessing Logistic Industries and Warehouses with Autonomous Carebot for Security and Protection: A Smart Protection Approach." *Harnessing AI and Digital Twin Technologies in Businesses*, edited by Sivaram Ponnusamy, et al., IGI Global, pp. 239-257. <https://doi.org/10.4018/979-8-3693-3234-4.ch017>, (2024).
9. Ali, Syed Ibad, et al. "Technological Collaboration, Challenges, and Unrestricted Research in the Digital Twin: Digital Twin Technology." *Harnessing AI and Digital Twin Technologies in Businesses*, edited by Sivaram Ponnusamy, et al., IGI Global, pp. 380-399. <https://doi.org/10.4018/979-8-3693-3234-4.ch028>, (2024).
10. Shaikh, Mohammad Shahnawaz, et al. "AI-Based Advanced Surveillance Approach for Women's Safety." *Wearable Devices, Surveillance Systems, and AI for Women's Wellbeing*, edited by Sivaram Ponnusamy, et al., IGI Global, (2024), pp. 13-25. <https://doi.org/10.4018/979-8-3693-3406-5.ch002>
11. Mungale, Sheetal Gajanan, et al. "Safeguard Wrist: Empowering Women's Safety." *Wearable Devices, Surveillance Systems, and AI for Women's Wellbeing*, edited by Sivaram Ponnusamy, et al., IGI Global, (2024), pp. 192-205. <https://doi.org/10.4018/979-8-3693-3406-5.ch012>
12. Sheikh, M.S. et al. (2024). *Harnessing Logistic Industries Using Autonomous Carebot for Smart Surveillance, Protection and Security*. In: AlTurjman, F. (eds) *The Smart IoT Blueprint: Engineering a Connected Future. AIoTSS 2024. Advances in Science, Technology & Innovation*. Springer, Cham. https://doi.org/10.1007/978-3-031-63103-0_20

13. Preeti Chopkar, Minakshi Wanjari, Pranjali Jumle, Pankaj Chandankhede, Sheetal Mungale and Mohammad Shahnawaz Shaikh (2024), A Comprehensive Review on Cotton Leaf Disease Detection using Machine Learning Method, *Grenze International Journal of Engineering and Technology*, June Issue, Grenze ID: 01.GIJET.10.2.537, Grenze Scientific Society, (2024).
14. Himanshu Kitey, Dr. P. Chandankhede, Dr. Kapil Jajulwar, Dr. Mohammad Shahnawaz Shaikh and Dr. Pragati M. Fatinge ,(2024), Solar Power Generation Technique and its Challenges - A Comprehensive Review, *Grenze International Journal of Engineering and Technology*, Jan Issue, Grenze ID: 01.GIJET.10.1.122, Grenze Scientific Society, 202.
15. Mohammad Shahnawaz Shaikh et al. "Analysis of Digital image filters in frequency domain", *International Journal of Computer Applications (IJCA)*, Volume - 14 0, Issue - 6 , ISSN: 0975 – 8887, (April 2016).
16. Ali, Syed Ibad, et al. "The Era of Metaverse and Generative Artificial Intelligence." In *Responsible Implementations of Generative AI for Multidisciplinary Use*, edited by Loveleen Gaur, 29-44. Hershey, PA: IGI Global, <https://doi.org/10.4018/979-8-3693-9173-0.ch002>, (2025).
17. Ali, Syed Ibad, and Mohammad Shahnawaz Shaikh. "The Ethical Dilemma of Using (Generative) AI to Science and Research." In *Responsible Implementations of Generative AI for Multidisciplinary Use*, edited by Loveleen Gaur, 249-264. Hershey, PA: IGI Global, <https://doi.org/10.4018/979-8-3693-9173-0.ch009>, (2025).
18. Pandey, A., Shaikh, M. S., & Patel, P. Review of acoustic features and computational Models in lung Disease diagnosis. *IEEE*, 1145–1150. <https://doi.org/10.1109/icses63445.2024.10763243>,(2024).
19. S. Singh, M. S. Shaikh, A. Sheikh, S. Dhargave and S. Mungale (2024), "Advanced Security and Protection for Logistic Industries and Warehouse Using Autonomous Carebot," 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), Indore, India, pp. 1-7, doi: 10.1109/ACROSET62108.2024.10743701, (2024).
20. M. S. Shaikh, K. Bhushanwar, N. Khodifad and S. I. Ali (2024), "Dual Purpose IoT Enabled Smart Cleaner Hexabot with Edge Detection Mechanism," 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), Indore, India, pp. 1-6, doi: 10.1109/ACROSET62108.2024.10743997, (2024).
21. Md. Shahnawaz Shaikh, Kamlesh Gupta (2014), A Review of Spectrum Sensing Techniques for Cognitive Radio. *International Journal of Computer Applications*. 94, 8, 1-5. DOI=10.5120/16360-5781,(May 2014).
22. Md. Shahnawaz Shaikh, Kamlesh Gupta (2014), Analysis of Cognitive Radio Spectrum Sensing Techniques. *International Journal of Computer Applications*. 102, 12, 1-7. DOI=10.5120/17864-8805,(September 2014).
23. Mohammad Shahnawaz Shaikh (2019), "Analysis of Cognitive Radio Spectrum Sensing Techniques over Nakagami-m Fading Channel", *International Journal of Modern Electronics and Communication Engineering (IJMECE)*, V 7, I 4, ISSN: 2321-2152, (July 2019).
24. Mohammad Shahnawaz Shaikh (2019), "Cognitive Radio Spectrum Sensing with OFDM: An Investigation", *International Journal on Emerging Trends in Technology (IJETT)*, Volume – 6, Issue – 2, ISSN: 2455-0124 (Online), (August 2019).
25. Mohammad Shahnawaz Shaikh, & P. K. Khare. FPGA Based Hardware Implementation for Green Cognitive Radio. *Journal of Electronic Design Engineering*, 6(3), 8–15. Retrieved from <https://matjournals.co.in/index.php/JOEDE/article/view/3865>, (2020).
26. Shaikh, M. S. Improving the requirements-based bandwidth allocation in 5G point-to-point networks. *ICTACT Journal on Communication Technology*, 13(4),(2022).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

