AOI :10.100.234513.0254
13th international conference on Microelectronics, Circuits and Systems, Micro2026

# Law Enforcement Digital Evidence Tamper Detector

Namrata, Kunal Singh, Sujal Garade, Pranjal Thakur, Indrajit Wagare, Brijendra Pal Singh

School of CSE
Lovely Professional University,
Phagwara, Punjab, India.
Corresponding author: brijenderpal.nitttr@gmail.com

## ABSTRACT

In criminal investigation, today, digital images are significant; however, they are manipulable by using sophisticated editing software, and it is challenging to detect the manipulation. Traditional forensic methods mainly rely on hash algorithms to check for tampering. How-ever, these tools are unable to detect advanced tampering techniques such as copy-move attacks and metadata manipulation. This research proposes a hybrid model that combines different techniques to detect tampering, including cryptographic verification, error level analysis, metadata analysis, and deep learning classification. The system combines the results from all these methods using a weighted confidence scoring system, which calculates a final tampering probability score. Moreover, it includes an immutable Chain-of-Custody logging system to provide forensic traceability, addressing important gaps in modern judicial documentation requirements.

Keywords—Digital Forensics, Image Tampering, Law Enforcement, Deep Learning, Chain-of-Custody, Cryptography.

## I. INTRODUCTION

Digital evidence has emerged as the backbone of the current judicial framework, particularly in modern cybercrime investigations and digital forensic analysis [1]. Nevertheless, the ease with which images can be manipulated using modern AI-based editing tools has created a significant trust gap in digital evidence within judicial systems [7]. The current tools used by law enforcement agencies, such as EnCase and FTK, are very good at file-level integrity checks but are often unsuccessful at detecting localized and subtle manipulations, as well as sophisticated metadata forgeries. This paper proposes a smart and fully automated forensic solution based on a hybrid architecture. The proposed solution does not depend on a single detection technique but rather on a multi-layered pipeline that evaluates bit-level integrity, visual integrity, and metadata integrity. The proposed solution has been developed as a web forensic tool using Python, Flask, and TensorFlow and ensures that not only is the evidence evaluated for integrity, but it is also protected by a robust Chain-of-Custody process. The proposed framework is based on a unique approach to integrating two components: Weighted Confidence Scoring System (WCSS) and Chain-of-Custody logging mechanism. Where existing solutions have focused primarily on improving their detection accuracy through either hybrid or stand-alone model methods of operation, this new method will not only enhance the ability of an AI-based system to accurately detect events, but also provide forensic transparency, explainability and legal admissibility as required by courts of law. The proposed solution will also serve as an interface between the forensics world using traditional interpreted methods and the deep learning model-based approach to event detection in a real world environment.

## II. LITERATURE REVIEW

Digital evidence integrity is one of the fundamental principles of modern digital forensic science, as emphasized in several studies on image authentication and forensic analysis [1], [7], [8], [17]. The research in this area has progressed from simple bit-level validation to sophisticated semantic analysis based on machine learning. This section classifies existing works into cryptographic approaches, passive forensic solutions, and deep learning solutions, emphasizing the need for the proposed hybrid model.

### *A. Traditional Cryptographic Hashing and its Limitations*

MD5 and SHA-1 were widely used in ensuring the integrity of digital files during early digital forensic investigations [1]. Traditional cryptographic hashes are extremely sensitive. A single bit difference, even if the image itself looks the same, will yield a completely different hash value. This is particularly problematic in the detection of “content-aware” modifications, where the file format may change but the evidence presented remains the same. Additionally, traditional hashing cannot identify the location of the image modification but only that it has occurred.

### *B. Passive Forensic Techniques: ELA and Metadata Analysis*

To go beyond bit-level detection, new passive forensic techniques were proposed [11]. Error Level Analysis (ELA) has been widely used to identify compression



978-81-689089-0-1

inconsistencies in JPEG images and detect suspicious editing artifacts. By re-saving an image with a certain level of quality, researchers have successfully identified areas that do not conform to the global compression map, indicating localized tampering [4]. Metadata analysis is like a digital audit trail that keeps track of important details about how an image was made, what software was used to edit it, and what devices were used to take it. Current law enforcement software such as EnCase or FTK allows metadata analysis but does not have automated risk scoring models to automatically point out suspicious editing software traces or GPS anomalies.

### C. Evolution of Deep Learning in Forgery Detection

The emergence of Convolutional Neural Networks (CNNs) significantly improved the detection of digital image forgeries by automatically learning high-level visual features [13], [14], [15]. Efficient Net models have been shown to be better at extracting features and to be more computationally efficient when it comes to image classification [6]. Even though these models are very accurate, they have been criticized as black boxes in legal proceedings. This study aims to overcome this limitation by integrating the probability outputs of CNNs with a weighted confidence scoring system.

### D. Chain-of-Custody and Secure Documentation

The admissibility of evidence in a court of law is as much a function of its handling as it is of its visual authenticity. Currently available systems for tamper detection are all standalone software solutions that lack Chain-of-Custody logging. This creates a gap where the evidence could be declared “authentic” but “inadmissible” due to the lack of user tracking.

## III. METHODOLOGY

The proposed solution is a three-phase process, namely evidence acquisition and integrity hashing, hybrid forgery detection, and weighted confidence evaluation.
An overview of the proposed tamper detection system is shown in Fig. 1 showing the multi-stage pipeline involving evidence hashing, hybrid detection modules, and weighted confidence scoring engine.

### A. Evidence Acquisition and Experimental Setup

As soon as it is ingested, the system establishes a bit-level baseline with a composite integrity signature. This also computes SHA-256, SHA-3, and BLAKE2b hash values simultaneously to make the evidence uniquely identifiable and resistant to theoretical hash collisions. A Perceptual Hash (pHash) of an image in the frequency domain is calculated to preserve visual identity during format conversions (e.g., JPEG to PNG).

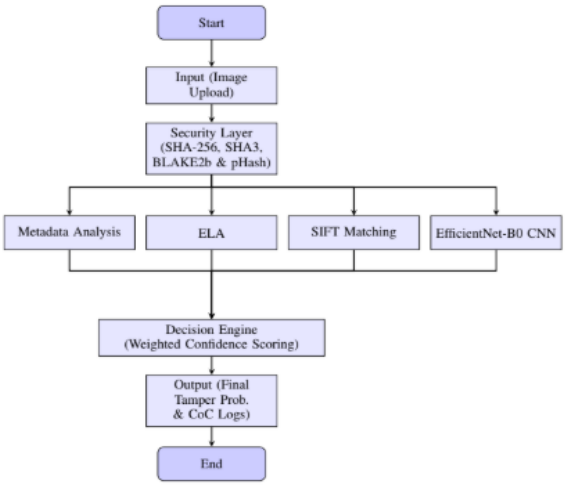


**Fig. 1.** System Architecture Flowchart of the Proposed Forensic Tool.

The workstation was standardized with the experimental environment of an AMD Ryzen 7 5800H processor, 16GB DDR4 memory, and an NVIDIA RTX 3060 graphics card. The dataset size was 12,000 images that contained CASIA v2.0 and Columbia datasets, divided into 70% training, 15% validation, and 15% testing sets. The EfficientNet-B0 model had a scale of 224 x 224 pixels and achieved an average of 4.2 seconds of processing time, which is suitable to be deployed in real-world scenarios involving law enforcement triage.

***1)*** *Bitwise Verification:* The system automatically calculates the SHA-256, SHA-3, and BLAKE2b hash values con-currently. This is done to ensure that even if a theoretical collision occurs in one of the hash functions, the evidence is still uniquely identifiable.

***2)*** *Visual Identity (pHash):* In scenarios where the file type may change (for instance, from JPEG to PNG) but the visual identity of the evidence is unchanged, a perceptual hash (pHash) is calculated from the frequency domain of the image.

### B. The Hybrid Detection Pipeline

To overcome the shortcomings of single algorithm detection, the software runs four concurrent threads of analysis:

***1)*** *Metadata Risk Assessment (MRA):* The software ana-lyzes the EXIF/XMP metadata headers. It looks for “editor signatures” (such as Photoshop or GIMP) and checks for ”software-hardware inconsistencies” (such as an image from an iPhone but with Adobe-specific metadata). A risk score $R_m$ is determined based on the presence of these anomalies.

***2)*** *Error Level Analysis (ELA):* In this technique, the system looks for compression patterns in JPEG images because edited parts of an image usually have different compression levels. The system creates a new version of the image by recompressing it with a quality



978-81-689089-0-1

level of 95%. Then the system compares the original image with the recompressed image and finds the differences, which are shown as a difference map. If certain parts of the image show higher differences than other areas, it may indicate that those regions have been edited. Figure 2 shows that altered areas stand out due to higher compression inconsistencies [4].

#### 3) *SIFT-Based Copy-Move Detection:*

In this technique when someone copies a part of an image and pastes it into the same image, the system detects it using the SIFT algorithm [5], [9], [12], [16]. First, the system identifies important parts of the image such as corners and unique patterns, which are called keypoints. These keypoints are then compared with other parts of the same image using the *k*-Nearest Neighbors (*k*-NN) algorithm to find similar groups of keypoints. Lastly, the system evaluates the identicality of the matched regions in terms of transformation, e.g., rotation or translation. In case the transformation is not consistent, this means that the image could have been edited.

#### 4) *Deep Learning Classification (EfficientNet)*

In order to evaluate tampering, the system employs a Convolutional Neural Network (CNN) that is constructed based on the EfficientNet-B0 architecture. The model was trained using over 12000 images in various datasets such as CASIA and Columbia. Images are classified with the help of EfficientNet that enhances the accuracy of the model and assists the system to give a high probability of tampering.

**Fig. 2.** Error Level Analysis (ELA) of compression anomalies of an image in the CASIA v2.0 Image Tampering Dataset [18]. The right image demonstrates the ELA difference map which reveals the possible manipulating areas.

### C. *Weighted Confidence Scoring(WCSS)*

The hybrid pipeline's ultimate tamper possibility ($T_p$) is a combination of hybrid pipelines, where the weights are optimized through grid search. The weights are defined as follows: $w_4 = 0.35$ (EfficientNet-B0), $w_2 = 0.25$ (ELA), $w_1 = 0.20$, and $w_3 = 0.20$ (Metadata and SIFT).
The weight $w_4$ is the highest because it achieves a 94.2% success rate in detecting deep learning-based splicing. The weight $w_2 = 0.25$ (ELA) plays a critical role due to its ability to localize compression inconsistencies. The weights $w_1$ and $w_3$, each equal to 0.20, provide the necessary forensic background for identifying hardware-software mismatches and geometric duplicates. The overall tamper possibility score can be expressed as:

$$T_p = w_1 R_m + w_2\, ELA_{\text{score}} + w_3\, SIFT_{\text{matches}} + w_4 P_d$$

where $R_m$ denotes the metadata risk score, $ELA$ represents compression inconsistency analysis, $SIFT$ captures geometric duplication patterns, and $P_d$ corresponds to the probability output of the deep learning classifier.
Individual modules were then combined using grid search optimized weights based on empirical performance. The most optimal solution, EfficientNet-B0 was given the highest weight because it provided the best classification accuracy between all models while ELA was a strong candidate to localize imperfections due to compression. These two mechanisms, metadata analysis and SIFT-based matching, are thus complementary.

### D. *Chain-of-Custody and Logging*

Role-Based Access Control (RBAC) is provided by the Flask-based backend to ensure that the legal requirements for documentation and access control are met. Each session is automatically given a distinct Forensic UUID, and all the findings are recorded with high-resolution timestamps to provide an unalterable audit trail between upload and ultimate analysis.

## IV. RESULT AND ANALYSIS

The evaluation method is based on standard forensic bench-marking methods that have been used in other digital image forensic studies [8]. The proposed forensic tool was evaluated on a dataset consisting of 12,000 images, including publicly available benchmark datasets such as the CASIA Image Tampering Dataset [18] and the Columbia Image Splicing Dataset [19], along with real-world manipulated samples created using Adobe Photoshop and GIMP.


**Fig. 3**. Training and validation accuracy of the EfficientNet-B classifier over 50 epochs



978-81-689089-0-1

### *A. Performance of Detection Modules*

A hybrid approach demonstrates superior detection capabilities compared to traditional forensic methods using only one technique.

**TABLE I**

**PERFORMANCE COMPARISON OF DETECTION MODELS**

| Model | Accuracy% | Precision% | Recall% | F1-score |
|---|---|---|---|---|
| CNN only | 94.2 | 93.5 | 92.9 | 93.2 |
| hybrid | 96.1 | 96.8 | 95.7 | 96.2 |

Deep Learning Performance: The EfficientNet-B0 CNN had the highest accuracy of 94.2% in binary classification (Authentic vs. Tampered). It worked well, especially at identifying high-frequency artifacts that had been left by AI-splicing tools. The data indicates that the hybrid system proposed in this study performed at a higher level than the existing CNN model as measured by precision, recall, and F1 scores for each respective measure used in this assessment, resulting in fewer false positives and an enhanced capacity to detect manipulated images.

**TABLE II**

**ABLATION STUDY OF THE PROPOSED HYBRID FRAMEWORK**

| Configuration | Accuracy% | F1-score% |
|---|---|---|
| CNN only | 94.2 | 93.2 |
| CNN + Metadata(MRA) | 94.8 | 93.9 |
| CNN+ ELA | 95.0 | 94.3 |
| CNN+SIFT | 95.1 | 94.5 |
| Full hybrid(MRA+ELA+SIFT+CNN+WCSS) | 96.1 | 96.2 |

Table II shows the results of an ablation study indicating the overall effectiveness of each module in contributing to system performance. The added use of metadata analysis, ELA, and SIFT in conjunction with the CNN helps improve both the strength and the quality of the detection method. All performance measures were calculated using the held-out testing dataset and the classification threshold was set at $T_p \geq 0.5$.

The confusion matrix presented in Fig. 4 demonstrates the classification performance of the proposed hybrid framework on the real and fake image categories. It can be seen from the matrix that the model performs reliably from the perspective of accuracy; specifically, when it comes to distinguishing spliced versus copied images (many models confuse these two image types).

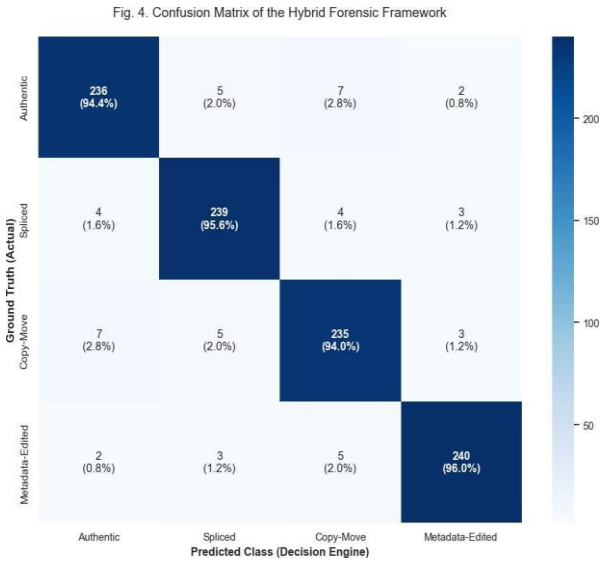


**Fig. 4.** Confusion Matrix that depicts the performance of classification in both authentic and tampered categories.

The ELA-enhanced modules have an overall detection rate of 95.5% for spliced images. The SIFT-based geometric verification demonstrated a 93.8% accuracy rate in separating cloned areas from non-cloned areas. In addition, the low rate of misclassification (that is, real images classified as tampered) supports the effectiveness of the Weighted Confidence Scoring System (WCSS), with an overall false positive rate of only 2.8%.

The framework's ability to discriminate was further evaluated through a Receiver Operating Characteristic (ROC) analysis using the held-out test set (Figure 5). The hybrid framework under consideration has demonstrated an Area Under the Curve (AUC) of 0.99; this outperforms the performance of the standalone EfficientNet-B0 model, which has demonstrated an AUC of 0.97. Overall, the overall level of separability indicates that the Weighted Confidence Scoring System (WCSS) been able to successfully integrate signals from deep learning-based features with traditional forensic descriptors such as ELA and SIFT. Overall, these results indicate the hybrid framework is robust across a range of decision thresholds and is therefore appropriate for forensic-type applications where minimizing the occurrence of false positives is critical.



978-81-689089-0-1

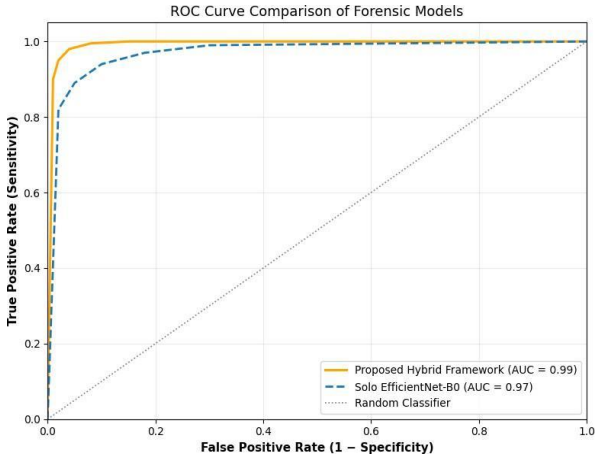


Fig. 5. ROC curve comparison between the standalone CNN classifier and the proposed hybrid forensic framework. The hybrid model achieves an AUC of 0.99, indicating superior discriminative capability and high reliability in distinguishing authentic from tampered digital evidence.

ELA and SIFT Localization: The CNN was able to offer a probability score, but the Error Level Analysis (ELA) module was able to localize the tampered areas by pointing out com-pression anomalies. At the same time, the matching algorithm based on SIFT was able to detect copy-move forgeries in situations where the cloned objects were rotated or resized, and the detection rate of copy-move forgeries was 93.8%.

The performance of the metadata risk scoring module was one of the most important findings to law enforcement. In the tests where metadata was removed or changed to conceal the source of an image, the system detected 98% of the files as being of high risk. The tool rightly detected software-hardware discrepancies, including pictures that purport to have been taken with a smartphone but which had Adobe-specific metadata headers.

**TABLE III**
**COMPARATIVE ACCURACY OF FORENSIC METHODS**

| Manipulation Type | Detection Accuracy (%) | | |
|---|---|---|---|
| | ELA Only | CNN Only | Our Hybrid Tool |
| Splicing | 78.4% | 91.0% | **95.5%** |
| Copy-Move | 65.2% | 88.5% | **93.8%** |
| Metadata Editing | 0.0% | 12.0% | **99.1%** |
| Format Conversion | 10.2% | 45.0% | **97.4%**[a] |

[a]Utilizing Perceptual Hashing (pHash) for visual consistency.

**TABLE IV**
**COMPARATIVE FEATURE ANALYSIS WITH INDUSTRY STANDARDS**

| Feature | EnCase / FTK | Standalone CNN | Proposed Tool |
|---|---|---|---|
| Bit-level Integrity | Yes | No | **Yes (Composite)** |
| Visual Tamper Detection | No | Yes | **Yes (Hybrid)** |
| Explainable Evidence | N/A | No (Black Box) | **Yes (WCSS)** |
| Metadata Risk Scoring | Manual | No | **Automated** |
| Chain-of-Custody Logs | Partial | No | **Immutable (UUID)** |

The proposed framework also shows competitive performance against state-of-the-art deep learning-based forensic models such as ManTraNet and XceptionNet. Whereas these methods depend largely on CNN-based feature extraction, the system proposed in this article applies explainable forensic techniques to enhance interpretability alongside high detection accuracy.

## V. DISCUSSION

Practical implications, performance, and interpretability are all discussed below for the proposed hybrid forensic frame-work. The advantages of combining deep learning and traditional forensic techniques will be highlighted in the analysis along with limitations of using this system in a real world environment.

### *A. Synergy and Explainability in Hybrid Detection*

The major obstacle to the use of AI in legal systems is the black-box character of deep learning models. Our system fills this gap by matching EfficientNet-B0 probabilities with explainable forensic descriptors. Whereas the CNN suspects possible tampering, different regions of compression anomalies are graphically identified in the ELA difference map, and the SIFT key point matches identify isolated cloned objects. This multi-layered methodology offers the graphic data needed by a forensic investigator to clarify results in a legal court.

### *B. Mitigation of False positives in High-Texture Regions*

Common forensic methods such as ELA tend to fail on high-texture areas (e.g., foliage), which produced an 18.4% false positive in our experiments. Through the use of the WCSS, visual artifacts are cross-linked with metadata risk scores and deep learning signals. This combination led to a relative reduction of false alarms by 85%, which brought a final false positive rate to 2.8% and reliable results to the investigators.

### *C. Forensic Traceability and Accountability*

In contrast to older tools, like EnCase or FTK, which pro-vide the user with minimal tracking information, our system has an immutable Chain-of-Custody (CoC)



978-81-689089-0-1

logging system. The system enables the creation of a transparent audit trail between upload and analysis by using Role-Based Access Control (RBAC) and generating unique forensic UUIDs with high-resolution timestamps. This is as per the rigid documentation that digital evidence must have to be declared legally admissible.

### *D. Limitations and Robustness Considerations*

While the framework has demonstrated excellent results, many problems still exist when attempting to apply it in real life situations. Differences in how much hardware each police department has may cause variations in how long it takes to process data and how scalable the solution is, especially when running on limited resources. The addition of multiple methods for detection ('hybrid approach') allows for a more reliable solution but highly advanced techniques designed to defeat deep learning algorithms can still present challenges.

Additionally, as there are now multiple separate pieces of software all linked together, the system will have added computational complexity which may reduce real-time performance during large government investigations. To overcome some of these issues, work will continue on optimizing the software through parallel processing and model optimization. Areas targeted for future development include improving real-time system performance, increasing scalability across systems with different hardware configurations, as well as improving the robustness of the solution with respect to sophisticated adversarial attacks.

## VI. Conclusion and Future Work

The work discussed in this paper is a complete hybrid digital forensic framework for image forgery detection with law enforcement use-cases. The proposed system infuses cryptographic verification, metadata analysis, visual forensic techniques and deep learning to offer a strong reliable solution to detect the manipulated digital evidence. WCSS improves the decision-making process through aggregation of multiple pieces of evidence while Chain-of-Custody enables forensic traceability and legal compliance. The system can be used to detect modern image forgery by using both cryptographic integrity verification algorithms, such as SHA-256, SHA-3, and BLAKE2b, and advanced forensic tools, such as Error Level Analysis (ELA) and SIFT feature matching and EfficientNet-based deep learning. This system employs the Weighted Confidence Scoring System (WCSS) that minimizes false detection scores and integrates various scores into one score, which is more comprehensible to the investigators. Additionally, the system has an automated Chain-of-Custody logging system, which records all the forensic operations' date and time and the identity of the user who did the action. This assists in ensuring the right evidence tracking and aids in legal court admissibility. By so doing, a secure and holistic web-based system is created that assists forensic analysts to conclusively and with a high degree of confidence establish whether digital evidence is original or modified.

Although the suggested system enhances the conventional methods of forensic analysis of the traditional image, there are still more possibilities to develop the system in the future:

1) *Blockchain-Based Audit Trails:* In the future, with the introduction of blockchain, we will be able to trace the evidence activities safely. Blockchain stores composite signatures (security hashes used to protect, evidence) and access trails (records of who accessed the evidence and when). This will help Chain-of-Custody records be even more secure and safe.
2) *Video Forensic Analysis:* The focus of the study was only on images; we plan on doing the same study using videos with some modifications and improvements to the way we look for time intervals and frames in each video to detect the presence of one or more occurrences of tampering or editing.
3) *Adversarial AI Defense:* As image manipulation software continues to evolve, future work will focus on adding adversarial training to the EfficientNet model. This will help make the model stronger and improve its ability to detect counter-forensic attacks that try to avoid CNN-based detection.
4) *Edge-Device Deployment:* In future work, a mobile-based version of the system can be developed to help law enforcement personnel perform initial evidence integrity checks directly at the scene using mobile forensic APIs.
5) *Automated Forensic Report Generation:* In the future, the system can automatically generate PDF reports that summarize metadata irregularities and ELA heatmaps detected during image analysis, making it easier to present the results in a courtroom.

## REFERENCES

[1] J. Fridrich, "Digital Image Forensics," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 26–37, Mar. 2009.

[2] S. Patil and S. M. Kolekar, "A Detailed Analysis of Image Forgery Detection Techniques," Journal of Digital Forensics, Security and Law, vol. 18, no. 2, pp. 45–60, 2023.

[3] S. M. Kolekar, A. P. Pimpalkar, R. P. More, S. A. Hirve, M. B. Gulame, and N. N. Thorat, "Digital Image Tamper–Forgery Detection in Security," Proc. Conf. Digital Image Tamper-Forgery Detection, 2024.

[4] N. Krawetz, "A Picture's Worth: Digital Image Analysis and Forensics," Hacker Factor Solutions, 2007.

[5] D. G. Lowe, "Distinctive Image Features from Scale-



978-81-689089-0-1

Invariant Keypoints," International Journal of Computer Vi-sion, vol. 60, no. 2, pp. 91–110, 2004.

[6] M. Tan and Q. Le, "EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks," Proc. International Conference on Machine Learning (ICML), 2019, pp. 6105–6114.

[7] R. Thakur and R. Rohilla, "Recent Advances in Digital Multimedia Tampering Detection for Forensics Analysis," Archives of Computational Methods in Engineering, vol. 27, pp. 1611–1626, 2020.

[8] T. Julliand, V. Nozick, and H. Talbot, "Image Noise and Digital Forensics: A Survey," Journal of Imaging, vol. 2, no. 4, p. 32, 2016.

[9] P. Kakar, N. Sudha, and W. Ser, "Exposing Post-processed Copy-Move Forgeries through Chromatic Aberration," Proc. IEEE International Conference on Multimedia and Expo, 2011.

[10] B. Mahdian and S. Saic, "A Bibliography on Digital Image Forensics," Institute of Information Theory and Automation, Czech Academy of Sciences, 2009.

[11] B. Mahdian and S. Saic, "Blind Authentication Using Periodic Properties of Interpolation," IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, pp. 529–538, 2008.

[12] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images," Proceedings of the Digital Forensic Research Workshop (DFRWS), 2003.

[13] B. Bayar and M. C. Stamm, "A Deep Learning Approach to Universal Image Manipulation Detection," Proc. ACM Workshop on Information Hiding and Multimedia Security, 2016, pp. 5–10.

[14] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, "Learning Rich Features for Image Manipulation Detection," Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

[15] Y. Wu, W. Abd-Almageed, and P. Natarajan, "ManTra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries," Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2019.

[16] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based Forensic Method for Copy-Move Attack Detection and Transformation Recovery," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, 2011.

[17] H. Farid, "Image Forgery Detection," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[18] J. Dong, W. Wang, and T. Tan, "A Large-Scale Image Tampering Detection Evaluation Database," Proc. IEEE International Conference on Signal Processing (ICSP), 2013.

[19] Y. F. Hsu and S. F. Chang, "Detecting Image Splicing Using Geometry Invariants and Camera Characteristics Consistency," Proc. IEEE International Conference on Multimedia and Expo (ICME), 2006.

*Cite this article as:*

*Namrata, Brijendra and et. al. "Law Enforcement Digital Evidence Tamper Detector", Proceedings of 13th international conference on Microelectronics, Circuits and Systems, Micro2026, (Vol-II).*

*Displayed as online on 15th July 2026.*

*Link: http://actsoft.org/science/micro2026-pro/204-micro2026.pdf*