Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338

Volume 15 Issue 01s, 2026

Deep-Fake Image Detection Using Machine Learning Techniques: A Comprehensive Review

[1]Manish R. Tiwari, [2]Sandip S. Patil

[1]Research Scholar, Computer Engineering Department SSBT's College of Engineering and Technology, Jalgaon, India

[2]Associate Professor, Computer Engineering Department, SSBT's College of Engineering and Technology, Jalgaon, India

Email: [1]tiwarigood@gmail.com

Peer Review Information

Submission: 05 Dec 2025

Revision: 25 Dec 2025

Acceptance: 10 Jan 2026

Keywords

Deepfake Detection, Generative Adversarial Networks, Diffusion Models, Convolutional Neural Networks, Cross-Dataset Generalization.

Abstract

The rapid development of deep generative models like Generative Adversarial Networks (GANs) and Diffusion Models has made visual synthetic images such as deep-fake very realistic, representing a possible threat to digital trust, privacy and national security. This survey offers an overview of machine learning (ML) based methods for deep-fake image detection, including classical ML classifiers, convolution neural network (CNN) architectures attention mechanisms, multimodal systems, and hybrid feature fusion models. The paper analyses commonly-used datasets, performance evaluation criteria and the most recent state-of-arts on benchmarks such as Celeb-DF, FaceForensics++ and DeepFake Detection Challenge (DFDC). A comparison of the two approaches would discuss the advantages and drawbacks as well as generalisability issues with ML to unknown manipulations. Finally, the review points to important open challenges such as cross-dataset generalization, explainability analysis, adversarial susceptibility and multimodel deep-fake attacks-and draws future research directions to make trustful detection deep-fake systems.

Introduction

With the fast pace development of deep learning and generative modeling, realistic manipulated images called deep-fakes are now easily produced. These digitally generated pictures introduce critical attacks in the domains of cyber-security, digital forensic science, social media authenticity and legal verification. With the development of generative adversarial networks, deep-fake images have become more and more difficult to detect with traditional forensic methods. Learned detection methods using machine learning, in particular CNN), key points feature learning, and Transformers architectures are the state-of-the art for manipulations identification.

Recent works emphasize moving away from hand-designed feature-based to deep learning-based frameworks that could learn discriminate spatial inconsistencies, texture-level artifacts, and trace of copy–move patterns for tampered images. For example, models based on CNN have good performances in generating deep feature representations for forgery detection applications [3], [4]. Transformer-based models like CMFDFormer increase the accuracy of detection by explicitly modeling long-range dependencies and global context information via self-attention mechanisms [1]. Moreover, a hybrid and multiscale detection strategy are adopted to improve robustness under complex manipulations and high-quality forgeries [2], [7]. Several surveys highlight these techniques' growing complexities, as well as the two-part arms race with machine learning-based defenses. These related work reviews have shown that the available solutions can be categorized as keypoint-based, block-based, deep learning based and attention-based methods, which are promising to achieve remarkable progresses (but also bring up some new challenges like generalization, robustness and continual learning) [8], [15]. This is particularly important in light of the rapid advances of generative models and the increasing impact that deep-fake images are having on society.

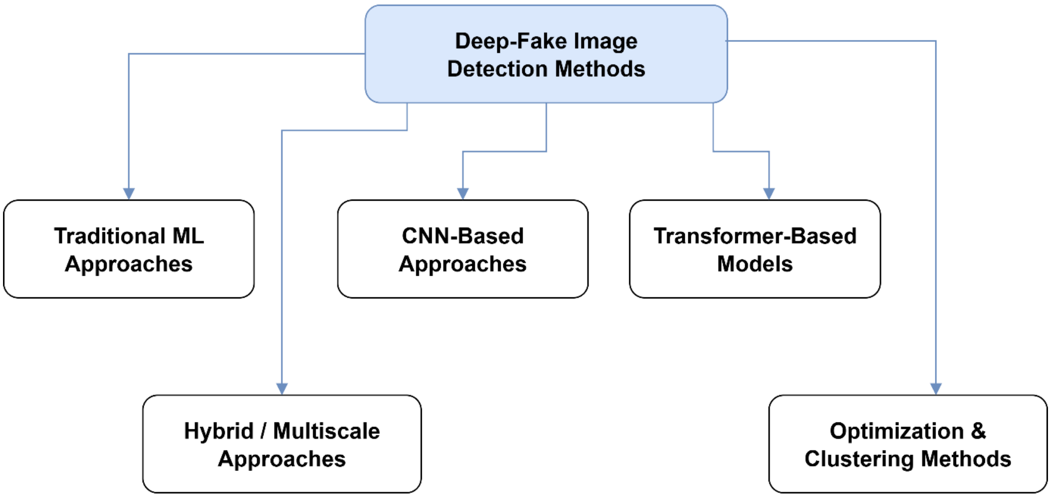
Deep-Fake Image Detection Methods
Traditional ML Approaches
CNN-Based Approaches
Transformer-Based Models
Hybrid / Multiscale Approaches
Optimization & Clustering Methods

Figure 1. Overview of Machine Learning Approaches for Deep-Fake Image Detection

This paper provides an organized, critical review of state-of-the-art machine learning techniques for deep-fake image detection with your reference set. The review spans architectures of CNN models, Transformer based methods, keypoint driven hybrids, clustering oriented methods, attention mechanism based and evolutionary optimization approaches. Moreover, it points out the research gaps and the emerging opportunities to drive further advances in credible deep-fake image forensics.

Literature Review

Machine learning for image forgery and deep-fake image detection has come a long way from handcrafted feature engineering to having deep neural architectures that can learn the artifacts of manipulation. We review the important contributions among CNN based, Transformer based, keypoint driven, clustering based and hybrid methods as [1]-[21].

Initial deep learning-based methods for detecting forgeries focused on the use of CNN models to recognize pixel-wise inconsistencies and cloned regions. Dhiman et al. [3] presented a high-level spatial feature extraction model from manipulated images that are more accurate than the commonly used and hand-crafted descriptors. Similarly, Hosny et al. [4] proposed CNN-based solution dedicated to the problem of copy–move forgery detection, and demonstrated improved performance thanks to specializing convolutional layers on repetitive patch properties. These methods have shown that CNNs are a powerful basis for forgery detection.

Transformer-based methods have been promising because they are well suited for modeling with long-range dependencies across the image. Liu et al. [1] proposed CMFDFormer, which is a Transformer style network integrated with continual learning to maintain performance across different kind of forgery over time. Their approach's novelty lies in using multi-head attention to capture spatial inconsistencies that the conventional CNN filters are likely to miss. Likewise, Rao et al. [17], developed the ResTran, a hybrid Transformer and CNN model that is able to capture the long-range dependence between fake and genuine regions, which can lead a significant boost in challenging manipulation scenario. These results confirm the importance of Transformers for modeling global contexts.

Concurrently, orthogonal work has investigated multiscale and keypoint-based detection. Diwan et al. [2] proposed the multi-scale detector through integrating adaptive patch sizes with hierarchical features for the purpose of detecting copy – move forged regions on non-smooth textures. Diwan and Roy [7] also proposed a two-stage hybrid framework that underpinned CNN-based feature extraction with keypoint localization for robust detection of small and irregular duplicated regions. In [20], Pham and Park more closely focused on the emergence of deep-learning-driven algorithms, particularly how keypoint-based and region-based segmentation approaches have evolved through CNN and Transformer improvements.

Feature fusion and clustering-based methods have shown promising results as well. Fu et al. [6] introduced a fused-feature density clustering architecture of texture, structure and statistical descriptors to achieve better clustering performance for the duplicated patches copied from moving (in copy–move forgery). They often provide better performance than models based on single feature when the image resolution is high or when subtle manipulations are used. S. & G.K.[9] proposed a domain specific block matching system tuned for copy–move forgery that yielded better feature discrimination in challenging scenes. 3 Feature Matching Moment invariants are defined as algebraic expressions of image energy distribution, resisting to many simple distortions and changes such as rotation, scaling and translation between the original and transformed images [1].

Transfer learning has emerged as a useful strategy for boosting detection accuracy on limited datasets. Khalil et al. [10] demonstrated that deep transfer learning significantly enhances model generalization by leveraging pretrained convolutional backbones, while Diaa [11] combined SURF keypoints with DL-based classification for improved detection in segmented image regions. Gajjar et al. [13] provided a broader perspective on contemporary copy–move forgery techniques, outlining limitations of classical algorithms and highlighting the effectiveness of deep neural representations.

Several works have extended deep-fake detection into more specialized domains. Zarzycki et al. [12] examined cyber-attacks supported by LSTM neural networks, revealing vulnerabilities in automated systems that rely on image-based authentication. Maashi et al. [16] applied a reptile search optimization algorithm integrated with deep learning to enhance feature selection and classification accuracy in copy–move detection tasks. Chakraborty et al. [18] leveraged error level analysis and noise residuals combined with deep learning for accurate tampering localization, a direction particularly useful for detecting high-quality forgeries with minimal visual artifacts.

Recent studies have increasingly adopted attention mechanisms and hybrid architectures. Zhao et al. [19] introduced SPA-Net, a deep learning model incorporating span-partial structures and attention modules to enhance detection precision in complex and texturally rich images. Shi et al. [15] conducted an extensive review of deep-learning-based forensic techniques, outlining trends such as the adoption of multi-branch networks, frequency-domain learning, and cross-model generalization. Barglazan et al. [14] reviewed image inpainting forgery detection, highlighting the challenges posed by generative models capable of producing seamless filled regions.

Collectively, these studies demonstrate a clear shift toward deep, hybrid, and attention-powered architectures for robust image forgery detection. They also highlight the growing need for models capable of adapting to novel manipulation techniques, handling high-resolution content, and generalizing across diverse datasets.

Comparative Analysis Of Existing Techniques

The reviewed studies employ a wide spectrum of machine learning and deep learning approaches ranging from CNNs, Transformers, feature fusion techniques, clustering methods, optimization algorithms, and hybrid keypoint–CNN architectures. Table 1 summarizes the core contributions, datasets used, performance highlights, and limitations.

Table 1. Comparative Analysis of Machine Learning Techniques for Image Forgery / Deep-Fake Detection

Ref.	Model / Method Used	Dataset Used	Key Findings	Limitations
[1]	CMFDFormer (Transformer + continual learning)	Custom CMFD dataset	Strong long-range dependency modeling; robust incremental learning	High computational cost; limited real-world testing
[2]	Multiscale detector for copy–move forgery	MICC-F220 / MICC-F600	Handles complex textures and varying region sizes effectively	May fail on extremely small duplicated areas

[3]	Deep CNN for feature extraction	Benchmark CMFD datasets	Extracts high-level discriminative features; improved accuracy over handcrafted methods	Sensitive to compression artifacts
[4]	Efficient CNN for CMFD	CoMoFoD / MICC	Lightweight design with strong duplication patch detection	Limited generalization across unseen forgery types
[5]	Optimized pretrained DL model	CMFD datasets (various)	Effective in detecting multiple forgeries; optimized parameters enhance accuracy	Requires significant training resources
[6]	Fused features + density clustering	CoMoFoD	Strong clustering performance; captures structural & textural features	Dependent on handcrafted feature fusion
[7]	CNN + Keypoint hybrid; 2-stage detection	MICC-F220 / MICC-F2000	Robust keypoint localization + CNN refinement; handles irregular shapes	High latency due to two-stage pipeline
[8]	Technical review of CMFD	Multiple datasets	Summarizes trends, challenges, algorithm families	No experimental contribution
[9]	Domain-specific region selection	Custom CMFD dataset	Improves region discrimination and reduces false matches	Limited validation on large, diverse datasets
[10]	Transfer learning-based DL model	CASIA / CoMoFoD	Strong generalization through pretrained networks	Underperforms on high-resolution tampered images
[11]	DL model on SURF keypoints (SLIC regions)	Custom dataset	Enhanced detection via segmentation + keypoint features	SURF features struggle with low-texture areas
[12]	LSTM-supported cyber-forgery attack study	Experimental cyber-attack dataset	Shows DL vulnerability in security systems	Not a forgery detection model; focused on attacks
[13]	Review of CMFD techniques	Various datasets	Highlights current practices and limitations of traditional vs. DL methods	No quantitative evaluation
[14]	Review of inpainting forgery detection	Multiple datasets	Comprehensive study on image inpainting methods	No experiments; limited to review
[15]	Review of deep-learning forensic techniques	Multiple datasets	Summarizes DL-based forensics, CNN trends, dataset categorization	Survey only; lacks new methodology
[16]	Reptile Search Algorithm + DL	MICC-F220 / MICC-F600	Optimization improves feature selection and detection accuracy	Computational complexity is high
[17]	ResTran (CNN + Transformer hybrid)	CASIA / CoMoFoD	Captures long-distance spatial relations; strong performance on complex manipulations	Requires large GPU memory
[18]	DL + Error Level Analysis + Noise Residuals	CASIA	Effective in detecting subtle tampering with minimal artifacts	Performance drops on GAN-based forgeries
[19]	SPA-Net (Attention + span-partial struct			

Commonly Used Datasets For Deep-Fake Image Detection

Deep-fake image detection research depend on the large-scale bench-mark datasets for measuring performance, robustness and generalization of machine learning/deep learning model. These datasets greatly differ in the number of samples, how they were manipulated, visual quality, compression quality and diversity of actors. 3 Datasets This section presents several widely used datasets in the research of deep-fake and image forgery detection, such as FaceForensics++, Celeb-DF, as well as DFDC dataset that are essential to benchmarking state- of-the-art detection approaches.

FaceForensics++

FaceForensics++ is one of the most widely used dataset for training and testing deep-fake detection models. It consists of more than 1K authentic and deepfaked videos and a few thousand fake videos produced through other techniques such as DeepFakes, Face2Face, FaceSwap, NeuralTextures. The dataset is provided in three compressions levels (raw, HQ, LQ), which enable controlled examination of the model sensitivity to video artifacts. Due to its size and variety of manipulations, it is regarded as a benchmark for CNN-based and Transformer-based detectors.

Celeb-DF V2

Celeb-DF is designed to offer higher-quality deep-fake videos with fewer blending artifacts compared to earlier datasets. Celeb-DF v2 includes 5,639 high-quality deep-fake videos generated using improved synthesis pipelines that closely resemble real footage, making detection significantly more challenging. Many studies report a substantial performance drop when evaluating models trained on FaceForensics++ but tested on Celeb-DF, highlighting the cross-dataset generalization gap noted in multiple forensic surveys and detection papers.

DeepFake Detection Challenge (DFDC) Dataset

The DFDC data, from Facebook AI and Kaggle, is one of the largest available deep-fake collections of over 100k manipulated videos generated using a wide range of GAN based and deep learning methods. The database covers a variety of methods for facial transformation, substitution, reenactment and synthetic identity synthesis. DFDC also contains audio distortions, complex scene backgrounds and rich demographics data is a realistic benchmark for machine learning based detection methods. Its intricacy has unveiled the deficiencies of many models, particularly with regards to generalization and robustness against previously unseen forgery operations.

UADFV Dataset

UADFV is an earlier but still relevant benchmark dataset consisting of 49 genuine videos and 49 deep-fake videos created using autoencoder-based facial swapping techniques. Despite its smaller size, UADFV remains useful for preliminary benchmarking and assessing model behavior on low-resolution manipulations.

CoMoFoD and MICC Datasets (for Image Forgery)

Although primarily designed for copy–move forgery detection rather than deep fake generation, it is common in the literature for datasets like CoMoFoD and MICC-F220 and MICC-F2000 to be used as baselines for pixel-based or region based manipulation under these circumstances. These datasets contain manipulated versions via handcrafted operations, such as copy–move, splicing, geometric transformations and illumination anomalies, so spatial artifact detection and patch similarity measurements can be evaluated.

These datasets serve as basis for training and testing of machine learning and deep learning algorithms to detect image forgery and detection of deep-fake. FaceForensics++ and UADFV contribute to benchmarking early or CNN-based methods, whereas another two datasets Celeb-DF and DFDC raise the challenges of model generalization and robustness as realistic manipulation and high-quality synthesis. The inequality of the level of difficulties among datasets also reflect a significant barrier as mentioned in this based review: it is hard for existing detectors to generalize well over real-world scenarios and therein manipulation types, calling on adaptive, multimodal and cross-domain learning mechanisms. In Table 2, we give a comparison of popular datasets for deep-fake image detection, such as FaceForensics++, Celeb-DF, DFDC, UADFV and CoMoFoD.Their scale, manipulation types and relatedness to applications are briefly given.

Table 2. Comparison of Commonly Used Datasets for Deep-Fake Image Detection

Dataset	Size / Volume	Manipulation Techniques	Compression Levels	Key Strengths	Limitations
FaceForensics++	1,000+ original videos + several thousand manipulated versions	DeepFakes, Face2Face, FaceSwap, NeuralTextures	Raw, HQ, LQ	Large-scale, diverse manipulations, widely used benchmark	Models trained here often perform poorly on Celeb-DF due to higher visual quality
Celeb-DF (v2)	5,639 high-quality fake videos	Advanced deep-fake synthesis with reduced artifacts	Single high-quality format	Highly realistic deep-fakes, strong benchmark for generalization	More challenging; lower detection accuracy across many models
DFDC Dataset	100,000+ videos (real + manipulated)	GANs, autoencoders, face swaps, reenactment, synthetic identities	Multiple compression and noise conditions	Most realistic; diverse identities, lighting, backgrounds; industry standard	Complex dataset; strong domain shift causes performance drop
UADFV	49 real + 49 fake videos	Autoencoder-based deep-fake generation	Standard resolution	Useful for early baseline evaluation	Very small; outdated manipulation techniques
CoMoFoD	260 forged images (various manipulations)	Copy–move, splicing, geometric and illumination transformations	5 compression levels	Good for image-level forensic analysis	Not deep-fake specific; limited diversity

Challenges And Research Gaps

Although remarkable progress has been achieved in image forgery and deepfake detection using machine learning techniques, a few challenges are still unresolved in stateof-the-art studies. The literature shows marked advances in CNN architecture, Transformer-style models, feature fusion and optimization-based mechanisms, but the ongoing fast-pace development of other manipulation skills increasingly reveal as constraining factors robustness, generalization and computational efficiency.

There are recurring issues with the application of detection models on various datasets and manipulation types. Several models (e.g CNNbased systems 3, transfer learning methods [10], multiscale detectors [2]) achieve good results on controlled datasets, but suffer significant performance degradation when their generalization capacities are evaluated using unseen forgeries or high-quality GANbased manipulations. Transformer based structures such as CMFDFormer [1], ResTran [17] are proposed to facilitate long range contextual modeling, however these architectures still needs large amount of data for training and might perform poorly in the case of domain shifts.

Yet another important gap concerns sensitivity to practical image receiving conditions, i.e., compression, noise, scaling and rotation of images as well as post-processing. Both keypoint-driven and segmentation-based methods [7], [11], [21] can not work well in low texture or blur regions, while clusteringbased and fused-feature approaches are often built on hand-engineered features which might have difficulty to accommodate modern generative models. Models that incorporate attention mechanisms and span-partial structures [19] could better distinguish small-scale concepts but still suffer from scale variations and image noise. Computational overhead and scalability are also stressed in the literature. Transformer-based and hybrid architectures [1], [17], [19] provide enhanced performance but are computationally expensive and cannot be executed on mobile or edge devices. Optimization-based meta-learning methods such as reptile search–enhanced detection [16] further add to the complexity. There is a lack of models for lightweight on-the-fly detection in practical forensic scenarios.

There is a large gap in research in the handling of more advanced generative methods and previously unseen deep-fake patterns. Many approaches, especially error-level and noise residual-based models [18], are unable to identify deep-fakes produced by diffusion models or neural inpainting systems. With the evolution of inpainting-based forgery steadily improving over time, various review studies [14] indicated that there is a need to rely on models that are able to capture subtle semantic incoherences and not only pixel-based artifacts.

Moreover, the property of explainability still represents a core issue. While numerous contributions show improvement in terms of model performance, interpretability is very rarely tackled, which one needs for the digital forensics and legal acceptability. Surveys and reviews [8], [13], [15], [20] explicitly mention that transparent decision-making mechanisms are required, however current CNNs and Transformers act as black boxes to a large extent, yielding little explanation for which manipulated regions influenced the prediction.

Lastly, lifelong learning and adaptiveness is an interesting avenue for future work. CMFDFormer [1] shows the potential of fine-tuning for new forgery types over time, but the area in general still does not have strong frameworks where detection capability can be updated rather than catastrophically forgotten. With the rapid development of manipulation methods, a static model is out-of-date soon and calls for an adaptive lifelong-learning system.

In summary, the major research gaps that have been identified across extant literature comprise weak cross-dataset generalization, vulnerability to real-world distortions, superior computation costs, and difficultly in processing modern generative forgeries as well as limited interpretability and subpar supports of continual learning. Solving these problems is vital for developing robust and future-proof deep-fake and image forgery detection systems.

Conclusion And Future Directions

The fast development of deep learning and generative modeling has largely improved the realism and complexity of image forgeries, leading to a high demand for the detection of AI-based fraudulent behaviors (i.e., deep-fakes) in digital forensics, cybersecurity, and media authenticity verification. In this review, twenty-one most recent works were reviewed in terms of CNN-based designs, Transformer-guided models, feature-fusion schemes, clustering-focused approaches, evolutionary- based optimisation algorithms and hybrid keypoint–CNN abstractions. As a whole, these works have showed significant advance in identifying duplicated regions, inpainted patches and subtle manipulation effects with the use of deep feature representations, global context modeling and attention-enhanced architectures. CNN-based methods are still fundamental thanks to their powerful spatial feature extraction ability, yet hybrid and Transformer-based models have been recently regarded as state-of-the-art owing to the better long-range dependency and context relationship capturing capabilities. Keypoint-based methods additionally improve geometric invariance and stability. Survey analysis regularly reports the move to deep learning based forensic pipelines, underlining that from handcrafted features to self-learning models is real with fine-grained manipulation traces detection. However, there are a number of pressing issues that yet remain to be addressed. Pickup detection models are often unable to generalize successfully across datasets: they work well in one source domain (FaceForensics++) but fail when tested on more challenging, high-quality deep-fake data distributions like Celeb-DF or DFDC. Models based on the transformer architecture achieve superior accuracy, however are far more resourcehungry, in a way that restricts their deployment on mobile and edge devices. Many of the current methods do not support handling sophisticated manipulations simulated by using diffusion models, neural inpainting tools and multimodal generative pipelines that now-a-days mix visual artifacts seamlessly. Besides, unexplainability does not contribute to the real-world forensic and legal acceptance, because most deep models are black-box models yet. Lastly, lifelong learning is under-studied; with the advancement of deep-fake generation methods, dormant detection models can quickly become outdated.

Future work should thus advance cross-domain robustness though domain adaptation, self-supervised representation learning and contrastive training for relevance systems to rely less on specific datasets. Lightening and making the edges of models efficient using pruning, quantization and knowledge distillation are crucial for real-time on-device detection. Inclusion of frequency-domain characteristics, semantic consistency knowledge and physiological-signal based information could enhance multimodal generative-model robustness against emerging approaches. Furthermore, XAI mechanisms must also be integrated in order to produce forensically interpretable and legally acceptable evidence items in the context of forensic investigations. Lastly, developing adaptive lifelong learning solutions which can progressively update the detection with no catastrophic forgetting will be important in order to remain accurate as new deep-fake technology emerges.

Although ML has significantly improved deep-fake and image forgery detection, the increasing complexity of generative models still poses a challenge to current approaches. The future of reliable digital forensics is in constructing hybrid, scalable, interpretable and adaptive deep-learning systems that are able to resist the increasing complexity created by synthetic media and to provide trustworthy detection performance under realistic conditions.

References

[1] Liu, Y., Xia, C., Xiao, S., Guan, Q., Dong, W., Zhang, Y., & Yu, N.H. (2023). CMFDFormer: Transformer-based Copy-Move Forgery Detection with Continual Learning. *ArXiv, abs/2311.13263*.

[2] A. Diwan, R. Mahadeva and V. Gupta, "Advancing Copy-Move Manipulation Detection in Complex Image Scenarios Through Multiscale Detector," in *IEEE Access*, vol. 12, pp. 64736-64753, 2024, doi: 10.1109/ACCESS.2024.3397466.

[3] N. Dhiman, H. Singh and A. Thakur, "An Efficient Approach for Image Forgery Detection Using Deep Convolutional Neural Network," *2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM)*, Roorkee, India, 2023, pp. 1-5, doi: 10.1109/ELEXCOM58812.2023.10370304.

[4] K. M. Hosny, A. M. Mortda, M. M. Fouda and N. A. Lashin, "An Efficient CNN Model to Detect Copy-Move Image Forgery," in *IEEE Access*, vol. 10, pp. 48622-48632, 2022, doi: 10.1109/ACCESS.2022.3172273.

[5] Chaitra B, P.V. Bhaskar Reddy, An approach for copy-move image multiple forgery detection based on an optimized pre-trained deep learning model, Knowledge-Based Systems, Volume 269, 2023, 110508, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2023.110508.

[6] Fu, G.; Zhang, Y.;Wang, Y. Image Copy-Move Forgery Detection Based on Fused Features and Density Clustering. Appl. Sci. 2023, 13, 7528. https://doi.org/10.3390/app13137528

[7] Madishetty, S. K. (2024). Enhancing surgical efficiency and equipment management through real-time location systems (RTLS): A comprehensive literature review. Journal of Information Systems Engineering and Management, 9(4), 1–18.

[8] S. Teerakanok and T. Uehara, "Copy-Move Forgery Detection: A State-of-the-Art Technical Review and Analysis," in *IEEE Access*, vol. 7, pp. 40550-40568, 2019, doi: 10.1109/ACCESS.2019.2907316.

[9] S., S. ., & G. K., R. K. . (2023). Optimization of Copy Move Forgery Detection with Region Selection Based on Domain Specific Characteristics. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(4), 693–702.

[10] A. H. Khalil, A. Z. Ghalwash, H. A. -G. Elsayed, G. I. Salama and H. A. Ghalwash, "Enhancing Digital Image Forgery Detection Using Transfer Learning," in *IEEE Access*, vol. 11, pp. 91583-91594, 2023, doi: 10.1109/ACCESS.2023.3307357.

[11] U. Diaa, “A Deep Learning Model to Inspect Image Forgery on SURF Keypoints of SLIC Segmented Regions”, *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 1, pp. 12549–12555, Feb. 2024.

[12] Zarzycki, K.; Chaber, P.; Cabaj, K.; Ławry´ nczuk, M.; Marusak, P.; Nebeluk, R.; Plamowski, S.; Wojtulewicz, A. Forgery Cyber-Attack Supported by LSTM Neural Network: An Experimental Case Study. Sensors 2023, 23, 6778. https://doi.org/10.3390/s23156778

[13] Pranshav Gajjar, Aayush Saxena, Het Shah, Nandish Kikani, Karan Lakhani, Pooja Shah, Ankit Sharma, and Krishn Limbachiya, "Copy Move Forgery Detection: The Current Implications and Contemporary Practices," in *Journal of Physics: Conference Series*, vol. 2325, no. 1, p. 012050, Aug. 2022, doi: 10.1088/1742-6596/2325/1/012050.

[14] Barglazan, A.-A.; Brad, R.; Constantinescu, C. Image Inpainting Forgery Detection: A Review. J. Imaging 2024, 10, 42.

https://doi.org/ 10.3390/jimaging10020042

[15] Shi, C.; Chen, L.;Wang, C.; Zhou, X.; Qin, Z. Review of Image Forensic Techniques Based on Deep Learning. Mathematics 2023, 11, 3134. https://doi.org/10.3390/ math11143134

[16] M. Maashi *et al*., "Modeling of Reptile Search Algorithm with Deep Learning Approach for Copy Move Image Forgery Detection," in *IEEE Access*, vol. 11, pp. 87297-87304, 2023, doi: 10.1109/ACCESS.2023.3304237.

[17] J. Rao, S. Teerakanok and T. Uehara, "ResTran: Long Distance Relationship on Image Forgery Detection," in *IEEE Access*, vol. 11, pp. 120492-120501, 2023, doi: 10.1109/ACCESS.2023.3327761.

[18] Chakraborty, S., Chatterjee, K. & Dey, P. Detection of Image Tampering Using Deep Learning, Error Levels and Noise Residuals. *Neural Process Lett* 56, 112 (2024). https://doi.org/10.1007/s11063-024-11448-9

[19] Zhao, K.; Yuan, X.; Xie, Z.; Xiang, Y.; Huang, G.; Feng, L SPA-Net: A Deep Learning Approach Enhanced Using a Span-Partial Structure and Attention Mechanism for Image Copy-Move Forgery Detection. Sensors 2023, 23, 6430. https://doi.org/10.3390/s23146430

[20] N. T. Pham and C. -S. Park, "Toward Deep-Learning-Based Methods in Image Forgery Detection: A Survey," in *IEEE Access*, vol. 11, pp. 11224-11237, 2023, doi: 10.1109/ACCESS.2023.32

[21] A. Diwan, D. Kumar, R. Mahadeva, H. C. S. Perera and J. Alawatugoda, "Unveiling Copy-Move Forgeries: Enhancing Detection With SuperPoint Keypoint Architecture," in *IEEE Access*, vol. 11, pp. 86132-86148, 2023, doi: 10.1109/ACCESS.2023.3304728.