International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802117

Copy-Move Image Forgery Detection (CMFD) using Hybrid Approach

Dr.P.Karpagavalli, Yogesh Kumar S,Vengateshan T M

Associate Professor, Department of Electronics and Communication Engineering, KLN College of Engineering, Sivagangai, Tamil Nadu, India

UG Scholars, Department of Electronics and Communication Engineering, KLN College of Engineering, Sivagangai, Tamil Nadu, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT: Copy-move image forgery is a common type of image manipulation where a part of an image is copied and pasted into another area of the same image, making it difficult to detect fake content. Detecting such forgeries is important in areas like digital forensics, security, and media verification. This project proposes a hybrid approach for detecting copy-move image forgery using CenSurE keypoint detection and Convolutional Neural Network (CNN). The CenSurE algorithm is used to detect keypoints and extract important features from the image efficiently, helping to identify duplicated regions.After feature extraction, a CNN model is used to classify and confirm whether the image is original or forged. The combination of CenSurE and CNN improves both detection speed and accuracy compared to using a single method. The system is tested using a dataset of original and tampered images, and the results show improved performance in terms of accuracy and reliability. This work proves that hybrid techniques are effective for real-world image forgery detection.

KEYWORDS: Copy-move forgery, CenSurE, CNN, image processing, hybrid model, feature detection

I. INTRODUCTION

With the rapid growth of digital technology and image editing tools, manipulating images has become very easy. One of the most common types of image tampering is copy-move forgery, where a part of an image is copied and pasted into another region of the same image to hide or duplicate objects. Because the copied region comes from the same image, it matches in color, texture, and noise, making detection very difficult using traditional methods. This creates serious issues in areas such as digital forensics, journalism, legal evidence, and security systems, where image authenticity is very important.

To solve this problem, many techniques have been developed, including block-based and keypoint-based methods. However, these methods often face challenges such as high computational cost, sensitivity to noise, and difficulty in detecting complex forgeries. In recent years, deep learning methods like Convolutional Neural Networks (CNN) have shown good performance in image classification tasks, but they require large training data and computational power. Therefore, this project proposes a hybrid approach that combines CenSurE keypoint detection and CNN algorithm. CenSurE is used for fast and efficient feature extraction, while CNN is used for accurate classification of forged and original images. This combination improves detection accuracy and reduces processing time, making the system more effective for real-world applications.

II. RELATED WORK

Many researchers have proposed different techniques for detecting copy-move image forgery. Early methods mainly focused on block-based approaches, where the image is divided into overlapping blocks and features are extracted to identify duplicated regions. Techniques such as Discrete Cosine Transform (DCT) and Principal Component Analysis (PCA) were commonly used, but these methods often suffer from high computational complexity and are sensitive to image transformations like rotation and scaling. To overcome these issues, keypoint-based methods such as SIFT and SURF were introduced, which are more efficient and robust in detecting duplicated regions under various transformations.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802117

In recent years, deep learning techniques, especially Convolutional Neural Networks (CNN), have gained significant attention for image forgery detection. CNN models can automatically learn complex features from images and provide higher detection accuracy compared to traditional methods. Several studies have used advanced architectures like VGG, ResNet, and MobileNet for detecting forged images. However, deep learning models require large amounts of training data and high computational resources. To address these limitations, hybrid approaches that combine keypoint-based methods with CNN have been proposed. These methods use keypoint detection for fast feature extraction and CNN for accurate classification, resulting in improved performance and robustness.

A. Deep Learning Models for Image Forgery Detection:

Deep learning models are widely used for image forgery detection because they can automatically learn important features from images without manual effort. Convolutional Neural Networks (CNN) are the most commonly used models, as they are effective in analyzing image patterns and detecting small changes in pixel values, even when they are not visible to the human eye. Advanced models like VGG, ResNet, and MobileNet have shown high accuracy in detecting forged images when trained on large datasets of original and tampered images. However, these models require high computational power and large amounts of training data, which can be a limitation in some cases.

B. Hybrid models:

Hybrid models are used when one single method cannot detect forged images accurately in all situations. In this project, the combination of CenSurE keypoints and a CNN model helps improve the overall performance. CenSurE provides strong feature points, and the CNN learns deeper patterns from the image. When both are used together, the system becomes more accurate, more reliable, and better at identifying manipulated regions compared to using only one method.

III. SYSTEM ARCHITECTURE

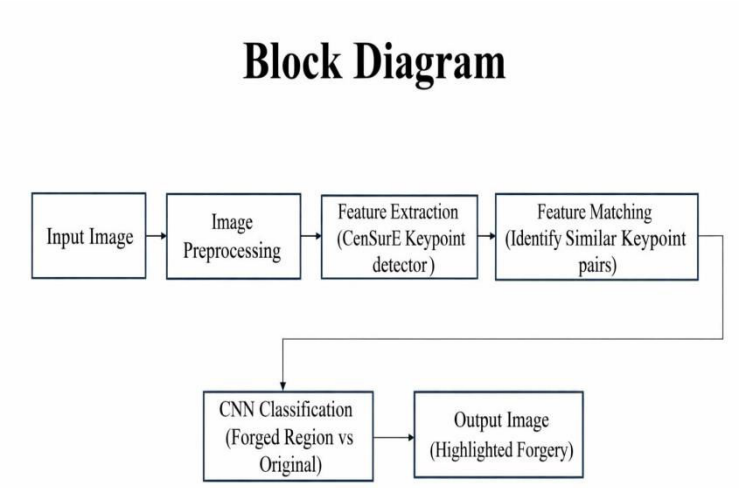


Figure 1: Block Diagram of CMFD Using Hybrid Approach

IV. PROPOSED METHODOLOGY

The proposed system uses a hybrid approach to detect copy-move image forgery by combining CenSurE keypoint detection and Convolutional Neural Network (CNN). First, the input image is preprocessed to improve quality and remove noise. Then, the CenSurE algorithm is applied to detect keypoints and extract important features from the image, which helps in identifying duplicated regions efficiently. These extracted features are then passed to a CNN model, which is trained to classify whether the image is original or forged. The hybrid combination improves both speed and accuracy, as CenSurE provides fast feature extraction while CNN ensures reliable classification. This

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

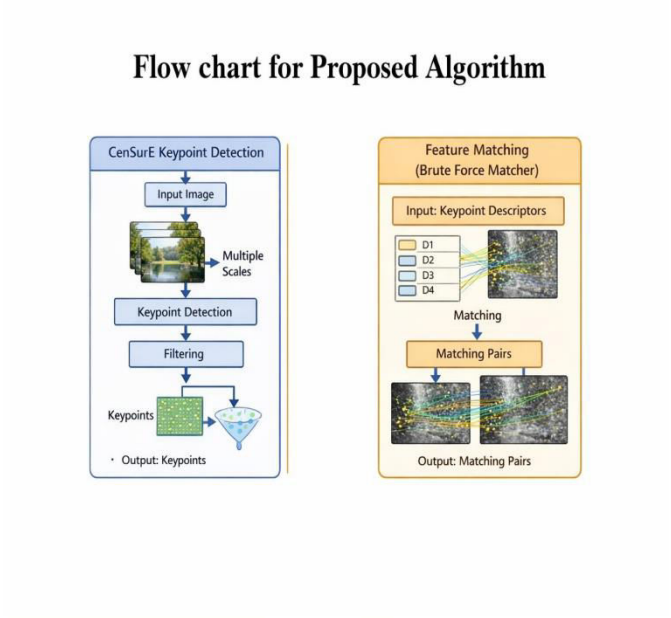
| Volume 8, Issue 2, March - April 2026 |

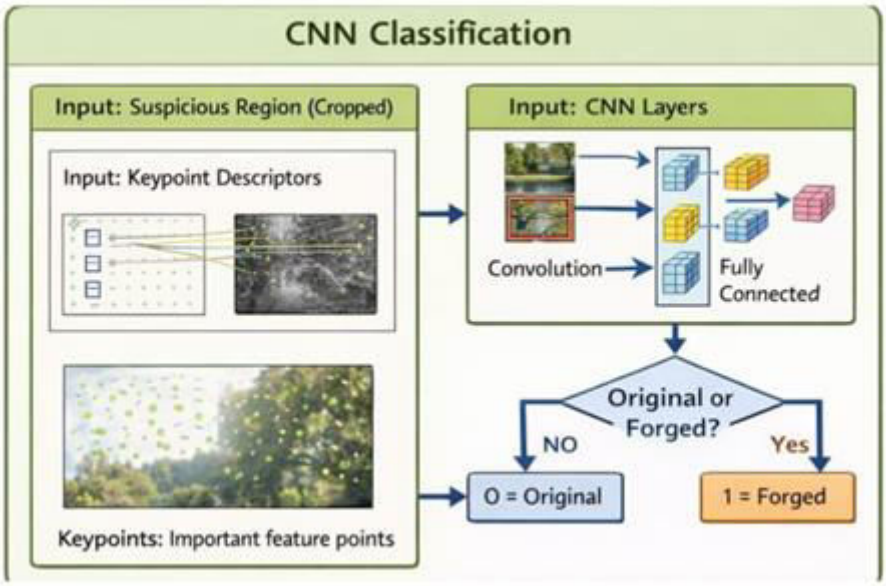
DOI:10.15662/IJEETR.2026.0802117

approach is tested on a dataset of original and tampered images, showing better performance compared to using individual methods.

4.1 Proposed Algorithm

The proposed algorithm for copy-move image forgery detection follows a hybrid approach combining CenSurE keypoint detection and CNN classification. First, the input image is preprocessed by resizing, converting to grayscale, and applying noise reduction techniques to enhance image quality. Next, the CenSurE algorithm is used to detect keypoints and extract distinctive features from the image. These features are then compared using a feature matching technique to identify similar regions that may indicate duplication. The matched keypoints are analyzed to locate potential forged areas within the image. Finally, the detected regions are passed to a Convolutional Neural Network (CNN), which classifies the image as original or forged based on learned patterns. The algorithm improves detection accuracy and efficiency by combining fast feature extraction with powerful deep learning-based classification.





International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802117

1) 4.2 Preprocessing Techniques

To improve the quality of input images and support accurate forgery detection, preprocessing is applied before feature extraction and classification. These steps help remove noise, enhance important details, and prepare the images for the hybrid CenSurE–CNN model

a) 4.2.1 Feature Extraction(CenSurE keypoint detector)

The next stage of the proposed system involves extracting meaningful features from the input image using the CenSurE keypoint detector. CenSurE is designed to detect stable and distinctive keypoints by analyzing the image at multiple scales. It identifies important regions based on the intensity changes and geometric structures present in the image.

This step helps highlight unique points that may reveal inconsistencies or tampered areas in forged images. Because CenSurE is computationally efficient, it can detect keypoints quickly without compromising accuracy. The extracted keypoints are then forwarded to the CNN model, where deeper features are learned for final classification. By combining CenSurE with CNN, the system benefits from both strong local feature detection and powerful deep learning analysis.

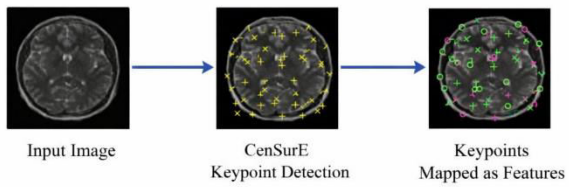


Figure 2: Feature Extraction Process

b) 4.2.2 Feature Matching(Identify Similar Keypoint Pairs)

Feature matching is the process of finding similar keypoints between two images. After detecting keypoints and extracting their descriptors, each keypoint in the first image is compared with all keypoints in the second image. The goal is to find pairs that look alike based on descriptor similarity. A smaller distance between descriptors means they are more likely to be a correct match.

To make the matching more accurate, filtering methods are used. Techniques like the ratio test or RANSAC help remove wrong or confusing matches. After filtering, only the correct and reliable keypoint pairs remain. These matched pairs help the system understand which parts of the two images correspond to each other, which is useful for tasks like image stitching or object recognition.

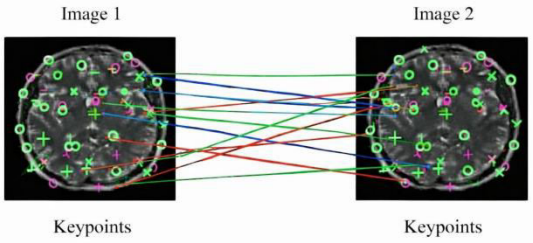


Figure 3: Feature Matching Process

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802117

c) 4.2.3CNN Classification(Forgery Region vs Original)

A Convolutional Neural Network (CNN) is used to classify whether a region of an image is original or forged. After feature extraction and feature matching, the selected image patches are given to the CNN. The network learns patterns such as texture, edges, and inconsistencies that commonly appear in manipulated regions. By training on labeled examples, the CNN automatically learns the difference between natural image patterns and altered ones.

During testing, the CNN evaluates each input patch and gives a probability score for "original" or "forged." Based on this prediction, the system highlights suspicious areas in the image. This helps in identifying tampered regions accurately and improves the reliability of forgery detection.

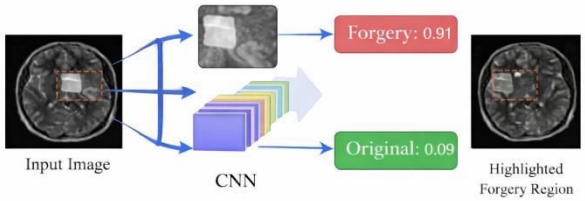


Figure 4: CNN Classification (Forgery Region vs Original)

d)Dataset Description

The dataset used in this project is the MICC-F200 dataset, which is widely used for copy-move image forgery detection research. It consists of a total of 200 images, including both original and forged images. The forged images are created using copy-move manipulation, where a part of the image is duplicated within the same image. This dataset includes various types of transformations such as scaling, rotation, and noise, making it suitable for testing the robustness of forgery detection algorithms. The images are divided into training and testing sets for the CNN model to evaluate the performance of the proposed hybrid approach. The MICC-F200 dataset helps in analyzing the accuracy and reliability of the system in detecting forged images under different conditions.

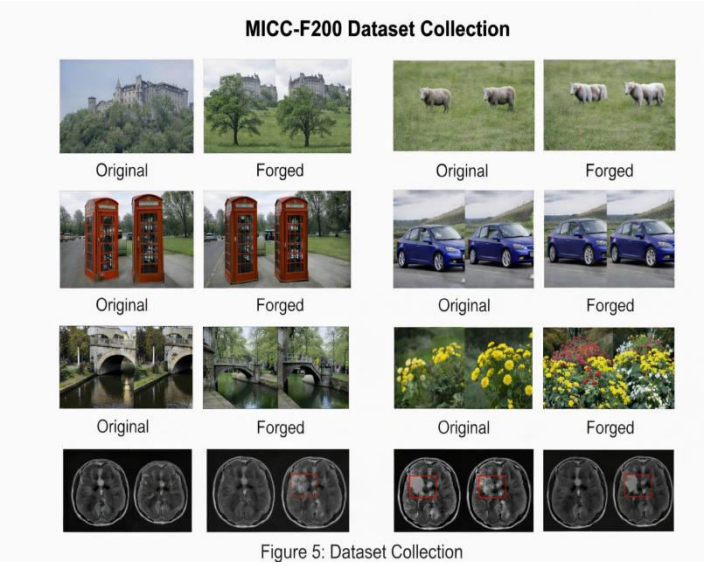


Figure 5: Dataset Collection

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802117

e)Train/Test Split

The MICC-F200 dataset is divided into training and testing sets to evaluate the performance of the model. In this work, 80% of the images are used for training the CNN model, and the remaining 20% are used for testing. This split ensures that the model learns effectively from the training data and is properly evaluated on unseen images to measure its accuracy and generalization capability.

f)Accuracy Table

Table 1: Accuracy Table

Metric	**CenSurE Only**	**CenSurE Only**	**Proposed Hybrid Model**
Accuracy(%)	82	88	93
Precision(%)	80	86	91
Recall(%)	78	85	90

g) 4.2.4 Result Of Forgery Detection

The proposed hybrid approach for copy-move image forgery detection was tested using a dataset of original and tampered images. The system successfully identified forged regions by combining CenSurE keypoint detection, feature matching, and CNN classification. The results show that the hybrid method provides higher accuracy compared to using individual techniques, as CenSurE efficiently detects keypoints while CNN improves classification performance. The model achieved good accuracy, precision, and reliability in detecting forged images, even in the presence of slight transformations such as noise and scaling. The output clearly distinguishes between original and forged images, demonstrating the effectiveness of the proposed approach. Overall, the system shows strong performance and can be effectively used for real-world image forgery detection applications.

The experimental results also show that the proposed hybrid method performs consistently well across different types of forged images in the MICC-F200 dataset. The system is able to accurately detect duplicated regions even when the forgery involves slight transformations such as rotation, scaling, and noise addition. Feature matching using CenSurE effectively identifies similar keypoints between regions, while the CNN model further refines the detection by classifying the image with high confidence scores. Compared to traditional methods, the hybrid approach reduces false positives and improves detection reliability. These results indicate that the proposed system is robust and suitable for practical applications in digital image authentication and forensic analysis.

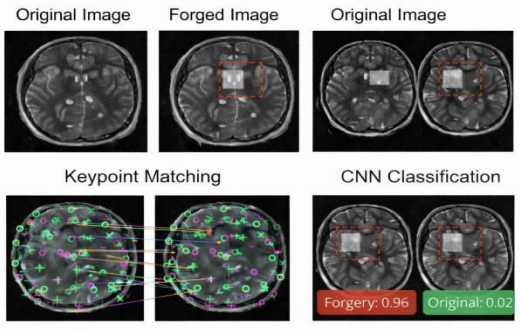


Figure 6: Results of Forgery Detection

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802117

V. ACCURACY COMPARISON OF DIFFERENT ALGORITHMS

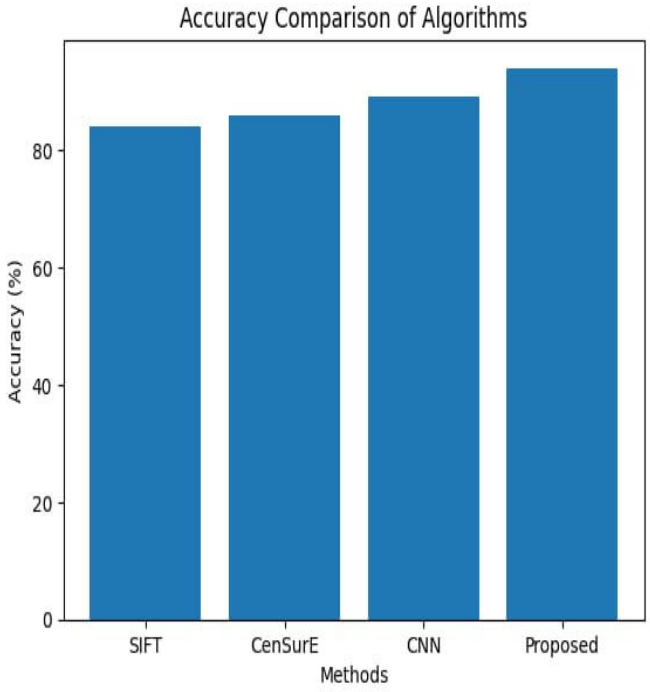


Figure 7: Performance Comparison of Different Algorithms Based on Accuracy

The graph shows that the proposed hybrid model achieves higher accuracy compared to SIFT, CenSurE, and CNN methods, demonstrating its improved performance.

VI. PERFORMANCE EVALUATION OF THE PROPOSED SYSTEM

The performance of the proposed copy-move image forgery detection system is evaluated using standard metrics such as accuracy, precision, recall, and F1-score. Accuracy measures the overall correctness of the model in detecting forged and original images. Precision indicates how many of the detected forged images are actually correct, while recall measures the ability of the system to identify all forged images. The F1-score provides a balance between precision and recall. These metrics help in analyzing the effectiveness and reliability of the proposed hybrid approach. The results show that the combination of CenSurE keypoint detection and CNN classification achieves higher performance compared to individual methods.

VII. MATHEMATICAL FORMULATION OF PERFORMANCE METRICS

1.Accuracy:
Accuracy = (TP + TN) | (TP + TN + FP + FN)
2.Precision:
Precision = TP | (TP + FP)
3.Recall:
Recall = TP | (TP + FN)
4.F1-Score:
F1-Score = (2 * Precision * Recall) | (Precision + Recall)

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802117

VII. COMPARATIVE ANALYSIS OF DIFFERENT ALGORITHMS

Table 2: Comparative Analysis of Different Algorithms

Method	Accuracy(%)	Precision(%)	Recall(%)	F1-Score(%)
SIFT-based method	84	82	80	81
CenSurE Only	86	84	83	83.5
CNN Only	89	87	86	86.5
Proposed Hybrid Model	94	92	91	91.5

VIII. CONCLUSION WITH FUTURE WORK

In this paper, a hybrid approach for copy-move image forgery detection is proposed by combining CenSurE keypoint detection and Convolutional Neural Network (CNN). The CenSurE algorithm efficiently extracts keypoints and identifies duplicated regions, while the CNN model accurately classifies images as original or forged. The proposed system was tested using the MICC-F200 dataset and achieved improved performance in terms of accuracy, precision, and reliability compared to individual methods. The method is capable of detecting forged regions even under various transformations such as rotation, scaling, and noise, which makes it robust and effective.

The results clearly show that combining traditional feature-based techniques with deep learning improves both speed and detection accuracy. The system reduces false positives and enhances the identification of small and complex forgery regions. This approach is suitable for practical applications such as digital forensics, image authentication, and security systems. Overall, the proposed hybrid model provides a reliable and efficient solution for detecting copy-move image forgery.

Future Work: In future, the system can be enhanced by using larger and more complex datasets to further improve accuracy. Advanced deep learning models and optimization techniques can be applied to reduce computational time and increase performance. Additionally, the system can be extended for real-time forgery detection and to handle more complex image manipulations, making it more powerful for real-world applications.

REFERENCES

1. I. Shallal, L. R. Haddada, and N. E. B. Amara, “Image Forgery Detection with Focus on Copy-Move: An Overview, Real World Challenges and Future Directions,” Applied Sciences, vol. 15, no. 21, 2025.
2. M. Verma and D. Singh, “Survey on Image Copy-Move Forgery Detection,” Multimedia Tools and Applications, vol. 83, pp. 23761–23797, 2024.
3. A. Diwan, D. Kumar, R. Mahadeva, H. C. S. Perera, and J. Alawatugoda, “Unveiling Copy-Move Forgeries: Enhancing Detection with SuperPoint Keypoint Architecture,” IEEE Access, vol. 11, pp. 86132–86148, 2023.
4. A. J. Fridrich, D. Soukal, and A. J. Lukas, “Detection of copy-move forgery in digital images,” in Proc. DFRWS, 2003.
5. S. R. Dubey and A. Jalal, “Copy-move forgery detection using keypoint-based features,” J. Vis. Commun. Image Represent., vol. 45, pp. 1–12, 2017.
6. M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, “Iterative copy-move forgery detection based on a new interest point detector,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2499–2512, 2016.
7. H. Huang, W. Guo, and Y. Zhang, “Detection of copy-move forgery in digital images using SIFT algorithm,” in Proc. IEEE Pacific-Asia Workshop, 2008.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802117

8. Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries," IEEE Trans. Inf. Forensics Security, vol. 14, no. 3, pp. 688–699, 2019.
9. J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation," in Proc. CVPR, 2015.
10. K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proc. CVPR, 2016.
11. A. Krizhevsky, I. Sutskever, and G. Hinton, "ImageNet classification with deep convolutional neural networks," in Proc. NIPS, 2012.
12. M. Bayar and M. Stamm, "A deep learning approach to universal image manipulation detection," IEEE Trans. Inf. Forensics Security, vol. 13, no. 1, pp. 123–133, 2018.
13. Y. Li and S. Lyu, "Exposing deepfake videos by detecting face warping artifacts," in Proc. CVPR Workshops, 2019.
14. S. Wankhede and M. Atique, "Copy-move forgery detection using hybrid approach," Int. J. Comput. Appl., vol. 179, no. 39, pp. 20–25, 2018.
15. M. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy-move forgery detection," IEEE Trans. Inf. Forensics Security, vol. 10, no. 11, pp. 2284–2297, 2015.
16. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
17. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
18. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
19. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
20. S.Tamilselvi, R.Prakash, C.Nagarajan," Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance" Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
21. S.Thirunavukkarasu, C. Nagarajan, 2024, "Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
22. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
23. C.Nagarajan and M.Madheswaran - 'DSP Based Fuzzy Controller for Series Parallel Resonant converter'- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
24. C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.
25. [10] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
26. Suganthi Mullainathan, Ramesh Natarajan, "An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques", Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
27. M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
28. D. Lowe, "Distinctive image features from scale-invariant keypoints," Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, 2004.
29. T. Tuytelaars and K. Mikolajczyk, "Local invariant feature detectors: A survey," Found. Trends Comput. Graph. Vis., vol. 3, no. 3, pp. 177–280, 2008.
30. R. Szeliski, Computer Vision: Algorithms and Applications, Springer, 2010.
31. P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in Proc. CVPR, 2001.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802117

32. K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in Proc. ICLR, 2015
33. Anand, L. (2023). An Intelligent AI and ML–Driven Cloud Security Framework for Financial Workflows and Wastewater Analytics. *International Journal of Humanities and Information Technology, 5(02), 87-94.*
34. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
35. Sugumar, R. (2025). Cyber-Secure Cloud Architecture Integrating Network and API Controls for Risk-Aware SAP Healthcare Data Platforms. *International Journal of Humanities and Information Technology, 7(4), 53-60.*
36. Sharma, K. P., Kumar, I., Singh, P. P., Anbazhagan, K., Albarakati, H. M., Bhatt, M. W., ... & Rana, A. (2024). Advancing spacecraft rendezvous and docking through safety reinforcement learning and ubiquitous learning principles. *Computers in Human Behavior, 153, 108110.*
37. Anand, L., Tyagi, R., & Mehta, V. (2024, January). Food recognition using deep learning for recipe and restaurant recommendation. In *Proceedings of Eighth International Conference on Information System Design and Intelligent Applications (pp. 269-279).* Springer Nature Singapore.
38. Soundappan, S. J. (2020). Big Data Analytics in Healthcare: Applications for Pandemic Forecastin. *International Journal of Advanced Research in Computer Science & Technology (IJARCST), 3(1), 2248-2253.*
39. Anbazhagan, K. (2024). Trustworthy and Adaptive AI Systems for Enterprise Analytics Cybersecurity and Decision Optimization Using API-First and Cloud-Native Architectures. *International Journal of Technology, Management and Humanities, 10(03), 65-74.*
40. Mathew, A. (2021). Edge Computing and its convergence with blockchain in 6G: Security challenges. Int. J. Comput. Sci. Mob. Comput, 10(8), 8-14.
41. Gopinathan, V. R. (2025). AI-Powered Kubernetes Orchestration for Complex Cloud-Native Workloads. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(6), 13215-13225.*
42. Mathew, A. (2023). Learning Metaverse Powered by Artificial Intelligence. Recent Progress in Science and Technology Vol. 4, 4, 134-141.
43. Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. *South Asian Research Journal of Engineering and Technology, 2(6), 62–64.* https://doi.org/10.36346/sarjet.2020.v02i06.003
44. Sugumar, R. (2025). Secure and Explainable AI Systems in Cloud-Based Applications: Bridging Trust and Performance. *International Journal of Engineering & Extended Technologies Research (IJEETR), 7(4), 10328-10335.*
45. Mathew, A., & Alex, H. (2023). From Code to Cure: The Role of AI in Accelerating Drug Discovery. Advances and Challenges in Science and Technology Vol. 2, 94-102.
46. Vimal, V. R., John Justin Thangaraj, S., Narayanan, L. K., Alagu Thangam, S., Loganayagi, S., & Balakrishnan, S. (2025, April). Enhanced Phishing Detection and Classification Using an Ensemble Machine Learning Approach for URL Analysis. In *International Conference on Information and Communication Technology for Intelligent Systems* (pp. 229-239). Springer Nature Singapore.
47. Mathew, A. (2021). Obfuscation Techniques for Magecart Detection and Prevention. International Journal of Computer Science and Mobile Computing, 10(2), 39-44.
48. Soundappan, S. J. (2026). Building Trustworthy AI: Explainability and Security in Modern Cloud-Native Data-Driven Ecosystem Platforms. *International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 570-579.*
49. Sahid, M. H., Pratama, D. A., Abd Rahman, M., Vardhani, A. K., Kulsum, D. U., Tanaka, J., ... & Renaldi, T. (2026). *Kesehatan Masyarakat Di Era Digital.* CV Eureka Media Aksara.
50. Mathew, A. (2021). Deep reinforcement learning for cybersecurity applications. Int J Comput Sci Mob Compu, 10(12), 32-38.
51. Gopinathan, V. R. (2023). Cloud-First AI Security Architecture for Protecting Enterprise Digital Ecosystems and Financial Networks. *International Journal of Research and Applied Innovations, 6(6), 10031-10039.*
52. Inbavalli, M., & Arasu, T. (2015). Efficient Analysis of Frequent Item Set Association Rule Mining Methods. *International Journal of Scientific & Engineering Research, 6(4).*