International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Image Cloning and Forgery Detection Techniques

Goldi Soni
Assistant professor
Amity University
Chhattisgarh, Raipur

Siddheshwari Sahu
B.Tech (CSE)
Amity University
Chhattisgarh, Raipur

Riya Thakur
B.Tech(IT)
Amity University
Chhattisgarh, Raipur

Abstract - Digital images are widely used as reliable sources of information in media, legal evidence, and social communication. However, the availability of advanced image editing tools has made image manipulation easy and common. Image cloning, also known as copy–move forgery, is one of the most frequently used techniques where a part of an image is copied and pasted within the same image to hide or duplicate objects. Detecting such forgeries is challenging because the copied region shares similar color, texture, and noise properties with the original image. This review paper presents a comprehensive study of various image cloning and forgery detection techniques proposed in recent years. The paper analyzes both block-based **and** keypoint-based **methods used for identifying duplicated regions. It also discusses the role of feature extraction techniques such as DCT, PCA, SIFT, SURF, and deep learning approaches. The performance of these methods is compared based on accuracy, robustness, and computational complexity. In addition, the study highlights challenges such as rotation, scaling, noise addition, and compression. The paper also reviews available benchmark datasets and evaluation metrics used in forgery detection research. Furthermore, recent advancements using machine learning and convolutional neural networks are examined. The objective of this review is to provide a clear understanding of existing techniques and their limitations. This study will help researchers identify research gaps and develop more robust and efficient image forgery detection methods in the future.**

Keywords Copy–Move Forgery, Digital Image Forensics, Image Authentication, Feature Extraction, Forgery Detection.

1.INTRODUCTION

With the rapid growth of digital technology and the widespread use of smartphones and social media, digital images have become a primary source of communication and information sharing. Images are commonly used in journalism, legal investigations, medical records, surveillance systems, and scientific documentation. Because of their importance, digital images are often considered reliable evidence. However, the availability of powerful and user-friendly image editing software has made it easy to manipulate images without leaving visible traces, raising serious concerns about their authenticity and credibility.Digital image forgery refers to the process of altering the content of an image to misrepresent information. Among various types of image manipulation, image cloning, also known as copy–move forgery, is one of the most common techniques. In this method, a portion of an image is copied and pasted within the same image to hide unwanted objects or to duplicate certain elements. Since the copied region originates from the same image, it shares similar color, texture, and noise characteristics, making detection a challenging task. To address this issue, researchers have developed various techniques for detecting image cloning and other forms of forgery. These methods are broadly categorized into block-based approaches and keypoint-based approaches, which rely on different feature extraction and matching strategies. In recent years, advanced techniques based on machine learning and deep learning have also been introduced to improve detection accuracy and robustness.

This review paper presents a comprehensive overview of existing image cloning and forgery detection techniques. It analyzes different methodologies, compares their performance, and discusses their advantages, limitations, and challenges. The objective of this study is to provide a clear understanding of the current research trends and to identify potential areas for future improvements in digital image forgery detection.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

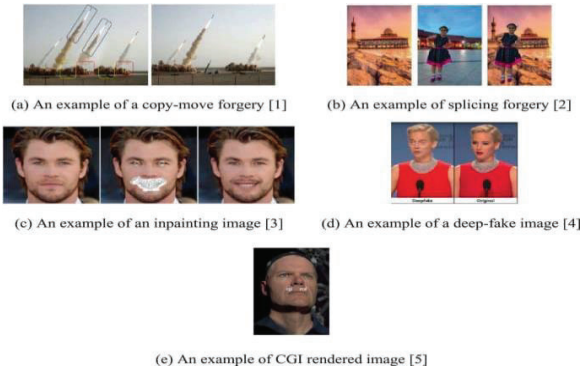

Fig 1. A Pictures of Different Forgery Techniques.

2 .LITERATURE REVIEW

This review paper discusses a study that focuses on the increasing use of deepfake technology as a powerful instrument of deception and disinformation in contemporary conflict scenarios. The main objective of the study is to analyze how deepfakes are employed to manipulate public opinion, destabilize political systems, and undermine trust in digital media and information sources. The paper aims to highlight the serious social, political, and security risks posed by the rapid advancement of artificial intelligence–generated audio and visual content. The methodology of the study is based on an extensive qualitative review of existing academic literature, policy reports, media investigations, and real-world case studies related to deepfake usage in political campaigns, military conflicts, and social unrest. The authors systematically examine the techniques used to create deepfakes, the platforms through which they are disseminated, and the psychological impact they have on audiences. The study also evaluates current detection technologies, legal responses, and regulatory challenges associated with combating deepfake-driven disinformation. In conclusion, the paper emphasizes that deepfakes represent a significant threat to information integrity, national security, and democratic processes, especially during times of conflict. It concludes that effective mitigation requires a multidisciplinary approach involving advanced detection tools, strong legal frameworks, media literacy education, and international cooperation to counter the harmful effects of deepfake deception and disinformation.[1]

This review paper presents an analysis of a study that addresses the growing challenge of detecting and localizing forged images shared on social networking platforms. The main objective of the study is to design a robust and accurate system capable of identifying manipulated images and precisely highlighting tampered regions under real-world conditions such as compression, resizing, and noise. The methodology adopted in the study is based on a dual-branch deep learning architecture that combines an image-level classification branch with a pixel-level segmentation branch. An ensemble of segmentation models is employed to capture diverse forgery features, improving generalization across different manipulation types. Additionally, a reinforcement learning-based refinement module is integrated to iteratively enhance the accuracy of the predicted forgery masks by reducing false positives and improving boundary localization. The proposed approach is evaluated using standard benchmark datasets and socially degraded images to simulate realistic online environments. Experimental results show that the method achieves very high detection accuracy and significantly improved localization performance compared to existing state-of-the-art techniques. In conclusion, the study demonstrates that the integration of ensemble learning and reinforcement learning offers a highly effective solution for image forgery detection and localization. It highlights the importance of such advanced forensic systems in maintaining the authenticity and credibility of digital images circulated on social media platforms.[2]

The primary objective of the reviewed paper is to study and analyze automated techniques for detecting digital image forgery with the help of deep learning approaches. The work focuses on maintaining image authenticity and integrity by identifying manipulated

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

images created using advanced image editing tools. It aims to examine common image forgery techniques such as copy-move, splicing, and resampling, and to evaluate the effectiveness of active and passive forgery detection methods. Another objective is to explore the use of deep learningmodels to improve accuracy and robustness in detecting forged digital images. The methodology discussed in the paper involves both traditional image forensic techniques and modern deep learning-based approaches. The existing system utilizes the MobileNetV2 architecture, which is optimized for lightweight and efficient image analysis. The proposed system enhances this approach by employing Convolutional Neural Networks (CNNs) to automatically extract discriminative features from images. Adaptive over-segmentation is used to divide images into irregular regions, followed by the application of the Scale-Invariant Feature Transform (SIFT) algorithm to extract robust feature points. These feature points are matched to detect suspicious regions that indicate forgery. The study also integrates transfer learning to improve detection performance and validates robustness using comparative accuracy analysis and confusion matrices on benchmark datasets such as MICC-F220. The review concludes that deep learning-based image forgery detection techniques significantly improve the accuracy and reliability of identifying manipulated images. The combination of CNN models with feature-based methods like SIFT proves effective in detecting various forgery types, including copy-move and splicing attacks. The study highlights that JPEG images are particularly vulnerable to manipulation, making automated detection essential. Although current methods show strong performance, challenges remain due to evolving image manipulation techniques and dataset limitations.[3]

This review paper examines a study that addresses the growing challenge of copy-move forgery detection (CMFD) in digital images. The primary objective of the work is to improve the accuracy, robustness, and computational efficiency of passive image forgery detection, particularly under geometric transformations and post-processing attacks. To achieve this, the authors propose a novel methodology that integrates a Division-based SIFT (DivSIFT) descriptor with a modified Kirsch (mKirsch) edge detector and blob detection techniques. The methodology involves preprocessing RGB images into grayscale, extracting robust keypoints using DivSIFT, enhancing edge sensitivity by selectively removing diagonal Kirsch masks, and identifying duplicated regions through blob-based matching. Extensive experiments were conducted on standard benchmark datasets under various attack conditions such as rotation, scaling, JPEG compression, and multiple cloning. The results demonstrate that the proposed approach achieves high true positive rates, zero or minimal false positive rates, and faster execution times compared to several state-of-the-art methods. In conclusion, the study effectively shows that combining optimized edge detection with an efficient feature descriptor significantly enhances CMFD performance, making the approach suitable for practical image forensic and authentication applications, although further improvements are needed for complex multiple-clone scenarios.[4]

The primary objective of this review paper is to analyze and summarize recent advancements in deep learning–based techniques for Copy-Move Image Forgery Detection (CMFD). With the rapid growth of digital image manipulation tools, detecting forged images has become a major challenge in digital forensics. This study aims to: Provide an updated overview of deep learning approaches used for copy-move image forgery detection. Classify existing CMFD techniques, including traditional and deep learning–based methods. • Compare the performance of various deep learning models and highlight their advantages over traditional approaches. • Review commonly used datasets and evaluation metrics in CMFD research. • Identify research gaps, limitations, and future directions for improving forgery detection systems. The methodology followed in this review paper is analytical and comparative in nature. The author systematically examines a wide range of previously published research works related to copy-move image forgery detection, with a strong focus on deep learning techniques. Initially, image forgery detection methods are classified into active and passive approaches, where the passive (blind) approach is emphasized due to its practical applicability. The paper further categorizes CMFD techniques into traditional methods (block-based, keypoint-based, and object-based) and deep learning methods. For deep learning–based CMFD, the review

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

discusses key principles such as training and testing phases, feature extraction, classification, and decision-making processes. Various deep learning architectures including CNNs, RNNs, transfer learning models (VGG16, ResNet, AlexNet, EfficientNet) and hybrid models are analyzed. A comparative analysis is carried out using performance metrics such as accuracy, precision, recall, F1-score, and AUC. The paper also reviews popular datasets like CASIA, CoMoFoD, MICC-F220, MICC-F2000, NIST Nimble, and GRIP, highlighting their role in evaluating CMFD models. Finally, results from multiple studies are summarized in comparative tables to clearly show the strengths and limitations of different deep learning approaches.[5]

The primary objective of the reviewed research is to enhance the accuracy and reliability of digital image forgery detection using machine learning techniques. The study focuses on identifying manipulated regions in images, addressing challenges posed by copy-move forgery, splicing, and retouching. It aims to develop an automated, scalable, and high-performance system capable of detecting forged images with minimal human intervention, particularly in applications such as digital forensics, media verification, and security systems . The reviewed paper employs a deep learning–based approach using Convolutional Neural Networks (CNNs), with particular emphasis on the VGG16 and ResNet50 architectures. The methodology involves preprocessing digital images through resizing, filtering, and normalization, followed by patch-based feature extraction. The dataset is split into training and testing sets in an 80:20 ratio. The CNN models are trained to classify image patches as authentic or forged. Performance evaluation is carried out using standard metrics such as accuracy, precision, and recall. Fine-tuning of pretrained networks is applied to improve generalization and detection performance. The review highlights that machine learning, particularly deep learning models like VGG16 and ResNet50, significantly outperforms traditional image forgery detection techniques. The fine-tuned VGG16 model achieves a maximum accuracy of 99.15%, along with high precision and recall, demonstrating strong robustness against various image manipulations. Despite challenges such as computational complexity and vulnerability to adversarial attacks, the study confirms that CNN-based approaches provide an effective and reliable solution for modern image forgery detection tasks. The reviewed work establishes deep learning as a key technology for ensuring visual content integrity in the digital era .[6]

The paper aims to survey blind digital image forgery detection methods by analyzing common manipulation techniques and comparing traditional signal-processing approaches with modern machine and deep learning methods, highlighting their strengths and limitations in image forensics. The authors adopt a systematic literature review methodology to analyze existing research work in the field of digital image forensics. The study categorizes image forgery detection techniques into active and passive (blind) approaches, with major emphasis on blind methods due to their practical applicability when prior image information is unavailable. The methodology discusses the general pipeline of blind forgery detection, which includes input image acquisition, preprocessing, feature extraction, feature matching, filtering, post-processing, and final classification of images as forged or genuine. Various feature extraction techniques such as DWT, DCT, FMT, SIFT, SURF, LBP, PCA, SVD, and deep learning models like CNNs, GANs, Autoencoders, and ConvLSTM are reviewed in detail. The paper further classifies blind forgery detection into three major areas: imaging device identification, copy-move forgery detection, and splicing detection. For each category, multiple research works are analyzed and compared using performance metrics such as accuracy, precision, recall, F1-score, false positive rate, and false negative rate. The authors also provide an extensive comparison of publicly available datasets like CASIA, CoMoFoD, MICC-F series, COLUMBIA, GRIP, CIFAR-10, and Dresden Image Database, which are widely used for training and validatin vo bc bc 7. G forgery detection models. The review concludes that blind forgery detection is essential in digital image forensics, with deep learning methods outperforming traditional techniques in accuracy and robustness. Despite challenges like high complexity and limited generalization, the study emphasizes hybrid models and improved datasets as key directions for future research.[7]

The primary objective of this research is to develop an efficient and accurate deep learning-basedapproach for

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

detecting copy-move image forgery, which is one of the most common types of digital image manipulation. The study aims to overcome the limitations of traditional and moment-based forgery detection methods by proposing a lightweight Convolutional Neural Network (CNN) model. Another key objective is to achieve high detection accuracy while maintaining low computational complexity and reduced testing time. The model is also intended to perform robustly across multiple benchmark datasets. The methodology proposed in this research is based on a deep learning framework using a Convolutional Neural Network (CNN) to detect copy-move image forgery effectively. Unlike traditional block-based techniques that rely on handcrafted feature extraction, the proposed method analyzes the entire image automatically to learn discriminative features related to forgery patterns. The proposed system consists of three main stages: preprocessing, feature extraction, and classification. In the preprocessing stage, the input images are resized to a fixed dimension to ensure uniformity and compatibility with the CNN architecture. This resizing is performed without cropping any part of the image so that no important visual information is lost. The preprocessing step helps in reducing computational complexity while maintaining image integrity. The feature extraction stage forms the core of the proposed approach. It uses three convolutional layers, each followed by a max-pooling layer. The convolutional layers apply multiple filters to the input image to extract low-level and high-level features such as edges, textures, and duplicated regions. The Rectified Linear Unit (ReLU) activation function is employed to introduce non-linearity and accelerate the training process. Max-pooling layers are used to reduce the spatial dimensions of the feature maps, which helps in minimizing overfitting and improving computational efficiency. After feature extraction, the obtained feature maps are flattened into a one-dimensional vector and passed to the fully connected layer.[8]

The main objective of this research paper is to provide a comprehensive and systematic review of digital image forgery techniques and their corresponding detection methods in the domain of multimedia forensics. With the widespread availability of powerful image editing tools, forged images have become increasingly difficult to detect using human visual inspection alone. This has raised serious concerns in critical areas such as forensic investigations, medical imaging, journalism, surveillance systems, and courts of law. The authors aim to: • Present a clear taxonomy of digital image forgery techniques, distinguishing between content-preserving and content-altering manipulations. • Analyze and compare passive image forgery detection techniques, including copy–move forgery, image splicing, retouching, and resampling. • Review commonly used datasets, software tools, and performance metrics employed in evaluating forgery detection methods. • Identify existing challenges, limitations, and research gaps to guide future research in digital image forensics. The methodology adopted in this paper is based on an extensive literature survey and comparative analysis of existing research works in digital image forgery and forensics. The authors systematically classify image forgery techniques into two major categories: forgery-independent (content-preserving) and forgery-dependent (content-altering) methods. Further classification is performed based on the type of manipulation, such as copy–move forgery, image splicing, retouching, and resampling. The paper reviews active and passive forgery detection approaches, with a primary focus on passive (blind) techniques, as they do not require prior embedded information like watermarks or digital signatures. Passive techniques are further categorized into pixel-based, format-based, camera-based, physical environment-based, and geometric-based methods. A detailed comparison of block-based, keypoint-based, and hybrid detection techniques is presented, highlighting their working principles, feature extraction methods, classifiers used, datasets, and performance metrics.[9]

The paper aims to compare major copy-move forgery detection (CMFD) methods used in digital image forensics. It analyzes the effectiveness, robustness, and efficiency of DCT-based, adaptive over-segmentation, and PatchMatch-based techniques under challenges such as rotation, scaling, and compression, to identify the most reliable approach for practical forensic use. The methodology adopted in the paper involves a comparative experimental evaluation of three widely used CMFD algorithms. First, the DCT-based CMFD approach divides the image into overlapping blocks and extracts DCT coefficients from each block. These

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

coefficients are quantized and lexicographically sorted to identify similar blocks. Matching block pairs are analyzed using shift vectors, and regions with frequent identical shifts are marked as forged. While this method is effective for detecting simple copy-move forgeries without geometric transformations, it is computationally expensive and less robust against rotation and scaling . Second, the adaptive over-segmentation and feature point matching method combines block-based and keypoint-based techniques. The image is segmented into irregular superpixels using the SLIC algorithm. Scale Invariant Feature Transform (SIFT) features are extracted from each segment, and matching blocks are identified using feature similarity thresholds. Morphological operations are then applied to localize forged regions. This method significantly improves robustness against geometric transformations and reduces computational cost compared to traditional block-based techniques. Finally, the PatchMatch-based CMFD scheme employs a dense nearest-neighbour field approach to efficiently match image patches. A modified PatchMatch algorithm is used to handle translation, rotation, and scaling by extending the search space and using invariant feature descriptors. This approach achieves high accuracy with significantly lower processing time, even for large images. The methods are evaluated on standard datasets using precision, recall, F1-score, and execution time. The review finds that no single CMFD approach handles all forgery types: DCT-based methods lack robustness, adaptive over-segmentation improves accuracy, while PatchMatch-based methods achieve the best accuracy with low computation time.[10]

The primary objective of the reviewed research paper is to develop an effective and robust copy–move forgery detection (CMFD) technique that can accurately detect and localize forged regions in digital images. The method aims to overcome limitations of existing block-based and keypoint-based approaches, particularly in cases where the forged regions are smooth, small, or subjected to post-processing attacks such as scaling, rotation, JPEG compression, and blurring. Another important objective is to avoid the use of fixed thresholds and instead introduce a dynamic thresholding mechanism to improve localization accuracy across different image characteristics. The proposed copy–move forgery detection approach follows a hybrid methodology that combines the strengths of both keypoint-based and block-based techniques. The methodology is divided into two main phases: Rough Forgery Region Determination and Exact Localization. In the first phase, the input image is processed using both RGB and L*a*b* color spaces. Specifically, the gray channel from RGB and the a* and b* channels from L*a*b* space are used to extract richer texture information. To enhance contrast in low-contrast and smooth regions, Contrast Limited Adaptive Histogram Equalization (CLAHE) is applied. Scale Invariant Feature Transform (SIFT) keypoints are then extracted independently from each channel due to their robustness against scale and rotation attacks. Keypoint matching is performed using the generalized two nearest neighbor (g2NN) strategy, followed by false match elimination based on spatial distance and shift vector consistency. The valid matches from all channels are fused, and RANSAC-based homography estimation is applied to obtain a roughly marked forged region. In the second phase, the roughly marked image and its transformed version are divided into overlapping blocks. Discrete Cosine Transform (DCT) is applied to these blocks to extract frequency-domain features. The similarity between corresponding blocks is calculated using Euclidean distance, and a similarity matrix is constructed. Unlike traditional methods that use a fixed threshold, the proposed technique dynamically determines an optimal threshold by analyzing minimum-distance patterns in the similarity matrix.[11]

The primary objective of the reviewed research paper is to present a comprehensive survey of copy–move forgery detection (CMFD) techniques used in digital image forensics. Copy–move forgery is one of the most common and challenging image manipulation techniques, where a region of an image is copied and pasted within the same image to conceal or duplicate objects. The paper aims to: Classify CMFD techniques based on detection methodology, detection paradigm, and detection capability. Analyze conventional CMFD methods, particularly block-based and keypoint-based approaches, and highlight their strengths and limitations. Explore deep learning-based CMFD techniques and explain how they address challenges faced by traditional methods. Identify key challenges such as geometric transformations, post-processing

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

operations, computational complexity, and dataset dependency. Provide future research directions to improve robustness, accuracy, and generalization of CMFD systems. Overall, the objective is to help researchers understand the current state, limitations, and future potential of copy–move forgery detection techniques. The methodology adopted in the reviewed paper follows a systematic survey-based approach. The authors organize and analyze existing CMFD techniques by dividing them into multiple logical categories. Firstly, the paper explains passive (blind) image forensics, which does not require prior information such as digital watermarks or signatures. Since copy–move forgery uses content from the same image, it is particularly difficult to detect using simple statistical inconsistencies. The CMFD techniques are categorized according to detection methodology as: Visual similarity-based techniques, which detect similar regions within an image. Tampering artifact-based techniques, which rely on inconsistencies introduced during manipulation. Hybrid techniques, which combine both approaches for better accuracy. Secondly, based on the detection paradigm, techniques are classified into: Conventional methods, including block-based and keypoint-based techniques. Deep learning-based methods, which automatically learn discriminative features.[12]

The primary objective of the reviewed research is to evaluate the effectiveness of integrating Error Level Analysis (ELA) with Convolutional Neural Networks (CNNs) for digital image forgery detection. The study aims to determine whether ELA feature extraction improves detection accuracy compared to using CNN alone. Additionally, the research investigates the impact of different ELA compression levels (10%, 50%, and 90%) on classification performance and computational time. The authors employ a deep learning–based passive image forgery detection approach using CNN architecture. A dataset comprising 646 images (323 original and 323 forged) was collected from publicly available sources, including the CASIA ITDE dataset and images from high-resolution digital cameras. The forged images included copy-move, splicing, and resampling manipulations. Prior to CNN processing, ELA feature extraction was applied by recompressing images at different quality levels (10%, 50%, and 90%) and computing the error differences. The CNN architecture consisted of three convolutional layers, pooling layers, and a fully connected layer with sigmoid activation. The model was trained using K-fold cross-validation, and performance was evaluated using accuracy, validation accuracy, loss values, and processing time. Experimental results with and without ELA were compared to assess effectiveness. The review highlights that incorporating ELA features with CNN significantly improves image forgery detection accuracy compared to using CNN alone. The highest training accuracy (approximately 86%) was achieved using ELA at 90% compression, while the best test accuracy was observed at 50% ELA compression. Statistical analysis confirmed that the improvement in validation accuracy using ELA is significant. However, the addition of ELA slightly increases computational time by about 5.6%. Overall, the reviewed study demonstrates that ELA is a valuable preprocessing technique for enhancing deep learning–based image forgery detection, with future scope for precise localization of forged regions.[13]

The primary objective of the reviewed paper is to evaluate the effectiveness of convolutional neural network (CNN)–based deep learning models for digital image forgery detection. The study aims to determine whether CNN architectures can accurately distinguish authentic images from forged ones and to identify the most suitable CNN model for this task. Additionally, the research seeks to compare the performance of different CNN architectures using standard evaluation metrics such as accuracy, precision, recall, specificity, and F1-score. The paper adopts a deep learning–based approach for image forgery detection using transfer learning. A balanced dataset consisting of 13,000 images (6,500 authentic and 6,500 forged) sourced from Kaggle is used. The dataset is divided into training (80%), validation (10%), and testing (10%) subsets. Pre-trained CNN models including VGG-16, VGG-19, ResNet-50, ResNet-101, ResNet-152, and Wide ResNet-50 are fine-tuned using ImageNet weights. The top 70% layers are frozen, and the remaining layers are trained on the forgery dataset. Models are trained using the Adam optimizer, binary cross-entropy loss function, and early stopping with learning rate scheduling. Performance is evaluated using accuracy, precision, recall, specificity, and F1-score to ensure balanced assessment across both authentic and forged image

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

classes. The review concludes that convolutional neural networks are highly effective for image forgery detection tasks. Among all evaluated models, ResNet-101 achieved the best overall performance, recording the highest accuracy (93.46%), recall (92.10%), and F1-score (93.57%). The results demonstrate that deeper CNN architectures with residual connections outperform traditional CNN models such as VGG. In contrast, VGG-19 showed poor performance and failed to reliably detect forged images. Overall, the study confirms that CNN-based deep learning models, particularly ResNet variants, provide a robust and efficient solution for image forgery detection in digital forensics applications, while also highlighting the potential for future improvements using additional datasets and advanced deep learning architectures.[14]

The primary objective of the reviewed research is to develop an efficient and robust method for Copy-Move Forgery Detection (CMFD) in digital images. The study aims to overcome the limitations of traditional block-based and keypoint-based CMFD techniques, such as high computational cost, sensitivity to geometric transformations, and reliance on filtering algorithms. Specifically, the objectives include: Reducing the number of keypoints required for matching. Improving robustness against geometric transformations like rotation and scaling. Minimizing false positives without using additional filtering methods such as RANSAC. Enhancing detection accuracy under post-processing operations including noise addition, blurring, and JPEG compression. The proposed method integrates image blob detection with Binary Robust Invariant Scalable Keypoints (BRISK) features. Initially, preprocessing is performed where large images are resized and edge detection is applied to enhance foreground structures. Blob detection is then carried out using the Difference of Gaussian (DoG) approach, which identifies meaningful regions at multiple scales while effectively separating foreground objects from background areas. After blob detection, BRISK keypoints and their binary descriptors are extracted. A key methodological innovation is that BRISK keypoints are grouped according to the blobs in which they lie. Keypoints within the same blob are not matched, as copy-move forgeries are expected to occur across different blobs. Feature matching is performed using Hamming distance and a nearest-neighbor ratio test to identify similar keypoints across different blobs. The method is evaluated on standard datasets such as MICC-F220, MICC-F8multi, and CoMoFoD, using performance metrics including precision, recall, F1-score, true positive rate, and false positive rate. Comparative analysis with existing CMFD techniques is also conducted to validate effectiveness. The reviewed paper concludes that combining image blobs with BRISK features significantly enhances copy-move forgery detection performance. The proposed approach successfully reduces the number of keypoints to be matched by nearly 50%, thereby lowering computational complexity.[15]

The primary objective of the reviewed research paper is to address the growing problem of copy-move image forgery, which threatens the authenticity and reliability of digital images in fields such as digital forensics, media, and legal investigations. The study aims to develop a robust and efficient forgery detection approach capable of identifying duplicated regions within the same image, even under post-processing operations like scaling, rotation, noise addition, and JPEG compression. Another important goal is to combine the strengths of block-based and keypoint-based techniques to overcome the individual limitations of each method and improve detection accuracy, precision, and recall. The reviewed paper proposes a hybrid copy-move forgery detection (CMFD) framework that integrates Discrete Wavelet Transform (DWT) and Scale Invariant Feature Transform (SIFT). Initially, the input image is preprocessed using a Gaussian filter to reduce noise and computational complexity. A fourth-level DWT decomposition is then applied to analyze the frequency components of the image and estimate low- and high-frequency energy distributions. This helps in determining the size of super-pixels used for segmentation. Next, the image is segmented into non-overlapping irregular blocks using the SLIC (Simple Linear Iterative Clustering) algorithm. For feature extraction, the SIFT algorithm is employed due to its invariance to scale, rotation, and illumination changes. SIFT extracts distinctive keypoints and generates feature descriptors from irregular blocks. Feature matching is performed using dot product-based matching, where similarities between feature vectors are evaluated to detect duplicated regions, referred to as “tentacles.” To eliminate false matches caused by

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

naturally similar regions in high-resolution images, the RANSAC (Random Sample Consensus) algorithm is applied. Finally, performance evaluation is conducted using metrics such as accuracy, precision, recall, false positive rate (FPR), and false negative rate (FNR). The experiments are carried out on images of varying resolutions using MATLAB.[16]

The objective of this study is to present a concise and systematic review of recent copy–move forgery detection (CMFD) techniques used in digital image forensics. Copy–move forgery is widely used because it copies regions from the same image, making detection difficult due to consistent color, texture, and illumination. The authors aim to analyze modern CMFD methods with respect to detection accuracy, robustness against geometric transformations and post-processing operations, and computational efficiency. Another important goal is to introduce a structured CMFD process pipeline to clearly explain each stage involved in forgery detection and to assist future research in this domain. This paper adopts a literature-based review methodology, focusing on CMFD techniques published between 2015 and 2018 in IEEE and ScienceDirect journals. The authors propose a new CMFD process pipeline consisting of preprocessing, feature extraction, feature matching, localization, and optimization stages. Various feature extraction techniques are reviewed, including block-based and keypoint-based methods using DCT, DWT, PCA, SIFT, SURF, and moment-based descriptors. Feature matching strategies such as lexicographical sorting, nearest-neighbor search, hashing, and hierarchical structures are analyzed. Post-processing techniques, including morphological operations like erosion and dilation, are also discussed to improve detection accuracy and reduce false positives. Comparative tables are provided to summarize and contrast recent methods based on performance and robustness. The review concludes that copy–move forgery detection remains a challenging task due to the trade-off between accuracy, robustness, and computational complexity. Block-based methods achieve high accuracy but require high computational cost, while keypoint-based methods are faster and more robust to transformations but may fail in smooth regions. The proposed CMFD pipeline provides a clear framework for understanding and developing detection techniques. The study highlights the need for hybrid and advanced approaches to improve reliability and efficiency in future CMFD systems.[17]

To study and analyze different types of digital image forgeries, including copy-move, splicing, retouching, morphing, and enhancement. • To classify image forgery detection techniques into active and passive (blind) approaches. • To review and compare recent research methods and algorithms proposed for digital image forgery detection. • To highlight the strengths and limitations of existing forgery detection techniques. • To provide insights into future research directions for improving the accuracy and reliability of image forgery detection systems. This review paper follows a survey-based methodology. The authors systematically analyze previously published research work related to digital image forgery detection. The methodology includes: Classification of forgery detection techniques into active approaches (watermarking and digital signatures) and passive approaches, which do not require prior embedded information. Detailed discussion of passive forgery detection techniques, further categorized into: • Pixel-based techniques • Format-based techniques • Camera-based techniques • Physical environment-based techniques • Geometry-based techniques • Examination of related work from 2011 to 2017, covering traditional methods, machine learning approaches, and emerging deep learning-based techniques such as CNNs. • Comparative analysis of various algorithms based on features used, classifiers applied (e.g., SVM), and detection accuracy reported in prior studies. The paper concludes that digital image forgery has become increasingly common due to the availability of powerful image editing tools. Among different forgery types, copy-move forgery is identified as the most frequently occurring manipulation. Existing detection techniques, including block-based and keypoint-based methods, each have their own advantages and limitations. The authors emphasize that no single method is sufficient for all scenarios. Hence, hybrid approaches combining multiple techniques are suggested as a promising direction to improve detection accuracy and robustness.[18]

In recent years, the widespread use of digital images and powerful image editing tools has increased the risk of image manipulation. Copy–move forgery is one of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

the most common image tampering techniques, where a portion of an image is copied and pasted within the same image to conceal or duplicate objects. The main objective of this review paper is to study and analyze various copy–move image forgery detection techniques used in the field of computer graphics and digital image processing. This paper aims to understand different detection approaches, their effectiveness, and their limitations in identifying forged regions in digital images. This review paper is based on an in-depth analysis of existing research articles published in journals and conferences related to computer graphics, image processing, and multimedia security. The studied techniques are broadly categorized into block-based and keypoint-based approaches. Block-based methods divide the image into overlapping blocks and extract features using techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Principal Component Analysis (PCA), and Singular Value Decomposition (SVD). These methods are effective in detecting duplicated regions but require high computational time. Keypoint-based methods use feature extraction algorithms such as Scale-Invariant Feature Transform (SIFT) and Speeded-Up Robust Features (SURF). These methods are faster and more robust against geometric transformations like rotation and scaling. Recent studies also focus on hybrid methods and deep learning-based techniques, which improve detection accuracy by automatically learning complex features from images. Copy–move image forgery detection is an important research area in computer graphics and digital forensics. This review shows that traditional block-based methods provide high accuracy, while keypoint-based methods offer better computational efficiency. Deep learning approaches have shown promising results but require large datasets and high processing power. No single technique is suitable for all types of forgeries.[19]

The objective of this review paper is to examine digital image forgery detection techniques, with particular emphasis on copy–move forgery detection (CMFD). Due to the widespread use of image editing tools, digital images can no longer be considered fully reliable. This paper aims to analyze existing forgery detection approaches, understand their working principles, and identify the limitations that affect their performance. The review also highlights the importance of developing robust methods to ensure image authenticity in applications such as forensics, media, and security. This review is based on an extensive analysis of research work in the field of digital image forensics. The forgery detection techniques discussed in the literature are broadly classified into traditional image processing methods and advanced learning-based approaches. Traditional techniques rely on handcrafted features and similarity matching, whereas recent methods employ machine learning and hybrid strategies to improve detection accuracy. The study compares different techniques based on their ability to detect forged regions, robustness against post-processing operations such as rotation, scaling, and compression, and computational efficiency. Commonly used benchmark datasets and evaluation metrics are also reviewed to assess the performance of CMFD methods. This review concludes that digital image forgery detection remains a challenging research area due to the increasing complexity of manipulation techniques. While traditional CMFD methods have shown effectiveness in controlled environments, they often fail under complex transformations and real-world conditions. Advanced approaches have demonstrated improved performance but still face challenges related to generalization and computational cost. Future research should focus on designing more robust, efficient, and scalable forgery detection techniques. This review provides a concise overview of current methods and serves as a helpful reference for researchers in digital image forensics.[20]

The main objective of video copy–move forgery detection research is to ensure the authenticity of digital videos against advanced editing tools that enable seamless manipulation. Early works, such as Wang and Farid (2007), focused on identifying temporal inconsistencies caused by duplicated frames, while later studies like Liu and Huang (2017) improved detection accuracy using texture and chromatic features. Recent research aims to achieve high accuracy, robustness to post-processing attacks, and low computational complexity, with approaches such as Jia et al. (2018) balancing efficiency and reliability across different video formats and camera motions. Various methodologies have been proposed in the literature to achieve the objectives of video copy–move forgery detection. These approaches can

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

be broadly classified into image feature–based methods and video feature–based methods. Image feature–based techniques analyze individual video frames using features such as pixel gray values, texture descriptors, color histograms, and sensor noise patterns. Wang and Farid (2007) utilized temporal and spatial correlation matrices of grayscale values to detect duplicated frames. Liao and Huang (2013) employed Tamura texture features like contrast and directionality, while Hsu et al. (2008) leveraged sensor pattern noise for forgery detection. Although effective under controlled conditions, these methods are highly sensitive to compression, noise, and filtering, which limits their robustness. Video feature–based methods exploit characteristics unique to video data, such as motion information, optical flow, and compression artifacts. Chao et al. (2014) introduced optical flow consistency analysis to detect inter-frame forgery, demonstrating improved robustness compared to image-based methods. Kingra et al. (2017) combined optical flow and prediction residuals to detect frame-level manipulation in compressed videos. A significant methodological advancement was proposed by Shan Jia et al. (2018) through a coarse-to-fine detection strategy based on optical flow. Their method first performs coarse detection using optical flow sum consistency to identify suspicious regions, followed by fine detection using optical flow correlation to accurately match duplicated frame pairs.[21]

The main objective of this study is to examine the growing problem of digital image forgery and its impact on image authenticity. The paper aims to classify different types of image forgery and review existing forgery detection techniques. It also seeks to highlight the challenges involved in detecting forged images and the need for reliable detection approaches in digital image forensics. The methodology adopted in this study is primarily a systematic literature-based analysis of existing image forgery detection techniques rather than experimental implementation. The authors analyze and synthesize findings from previously published research to develop a structured understanding of forgery types and detection approaches. Initially, the study examines the fundamental problems associated with image forgery detection, such as identifying the original source of an image and the absence of standardized datasets for performance evaluation. Following this, the authors categorize image forgery techniques based on how images are manipulated, supported by visual examples to illustrate real-world forgery scenarios. The detection methodologies are broadly classified into active approaches and passive approaches. Active approaches include techniques like digital watermarking and digital signatures, where additional information is embedded into the image at the time of capture to verify authenticity later. These methods require prior knowledge or pre-processing of the image In contrast, passive (or blind) approaches do not rely on any embedded information. Instead, they analyze intrinsic image characteristics such as pixel correlations, compression artifacts, camera sensor noise, shadows, and reflections. The study further categorizes passive techniques into pixel-based, format-based, camera-based, shadow-based, and reflection-based methods. Each category is discussed in terms of its working principles and relevance in detecting specific types of forgery. The paper also presents a general framework for image forgery detection, outlining key stages such as image preprocessing, feature extraction, classification, and authentication decision-making.[22]

With the rapid growth of digital imaging devices and powerful image editing software, image forgery has become increasingly common and difficult to detect. Among various types of image manipulation, copy-move forgery is one of the most frequently used techniques, where a part of an image is copied and pasted within the same image to hide or duplicate objects. Traditional detection methods often suffer from high computational complexity, poor robustness against post-processing operations, and dependence on experimentally defined thresholds. The main objective of the reviewed research is to design a robust, accurate, and computationally efficient method for detecting copy-move forgery in digital images. The study specifically aims to eliminate threshold dependency during feature matching, improve detection accuracy under different post-processing conditions, and achieve precise localization of forged regions. By integrating binary discriminant features with superpixel-based region localization, the proposed method seeks to enhance the overall performance of copy-move forgery detection systems in the field of image forensics. The methodology presented in the reviewed paper adopts an integrated approach by

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

combining the strengths of both keypoint-based and block-based forgery detection techniques. Initially, keypoints are extracted from the entire image using the FAST keypoint detector due to its computational efficiency and high repeatability. To ensure robustness against scale variations, keypoints are detected at multiple scales, and rotational invariance is achieved by assigning a dominant orientation to each keypoint. For feature description, the method employs Binary Discriminative Features (BDF), which utilize local gradient information to generate compact binary descriptors. Unlike traditional floating-point descriptors such as SIFT and SURF, BDF significantly reduces memory usage and computational cost. Feature matching is carried out using Hamming distance, and only keypoints with identical binary descriptors are considered matches. This approach removes the need for experimentally determined threshold values, thereby increasing robustness and reducing false matches.[23]

The primary objective of the reviewed research is to develop an efficient and robust technique for detecting copy-move forgery in digital images. Copy-move forgery is one of the most common image tampering techniques where a region of an image is copied and pasted within the same image to conceal or duplicate content. The paper aims to overcome limitations of traditional block-based methods by introducing an object-based approach that improves detection accuracy, reduces false positives, and enhances robustness against geometric transformations such as rotation, scaling, and translation. The proposed method introduces a two-stage copy-move forgery detection (CMFD) algorithm based on object recognition and feature matching. In the first stage (matching stage), the input image undergoes preprocessing using morphological operations and edge detection. Connected Component Labeling (CCL) is then applied to segment the image into distinct objects. For each detected object, Speeded-Up Robust Features (SURF) descriptors are extracted to build an object catalog. Objects are compared using feature matching, and similar objects indicate potential copy-move forgery. If matching objects remain after removing intersecting regions, the image is classified as forged. The second stage (refinement stage) is applied to images initially classified as original. This stage uses both opening and closing morphological operations to enhance object boundaries and detect subtle forgeries missed in the first stage. SURF features are again extracted, and object matching is repeated to confirm the originality or detect hidden forged regions. The algorithm is evaluated on four benchmark datasets: MICC-F220, MICC-F2000, MICC-F600, and SATS-130, using performance metrics such as accuracy, true positive rate, false positive rate, and computational time. The reviewed study demonstrates that the proposed two-stage CMFD algorithm significantly improves forgery detection performance compared to single-stage and traditional methods. Experimental results show high detection accuracy, reaching 99.09% on MICC-F220 and maintaining strong performance across other datasets.[24]

The primary objective of this research is to develop an effective and accurate method for video copy-move forgery detection, particularly focusing on cloned object movement within a single video. The study aims to overcome the limitations of existing video forgery detection techniques that fail when objects are added or removed from video scenes. Specifically, the objectives include: Detecting duplicated or cloned moving objects in tampered videos Utilizing optical flow inconsistencies to analyze object motion Representing object movement through displacement paths Improving detection accuracy compared to existing state-of-the-art methods. The proposed methodology is based on optical flow analysis combined with Dynamic Time Warping (DTW) for similarity measurement. First, optical flow is computed between successive video frames to estimate motion vectors of moving objects. The video frames are divided into non-overlapping blocks, and displacement vectors are calculated to track motion accurately. To separate real moving objects from background changes, an adaptive thresholding technique is applied to the optical flow values. Blocks with displacement values greater than the threshold are identified as moving objects. These moving blocks are then grouped using 8-connectivity labeling, ensuring accurate extraction of object regions. Each detected moving object is represented by its centroid point, and centroid positions across frames are connected to form a displacement path, representing the trajectory of object movement over time. To identify cloned objects, the displacement paths of all moving objects

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

are compared using Dynamic Time Warping, which effectively handles temporal misalignment and non-linear motion variations. If two displacement paths show high similarity, the video is identified as forged. Digital image forgery detection remains challenging due to complex post-processing and realistic manipulations. While learning-based passive forensic methods improve accuracy, challenges such as high complexity and limited robustness persist, highlighting the need for hybrid models, better datasets, and improved real-world forensic systems.[25]

The primary objective of the reviewed research is to develop a robust and automated mechanism for detecting copy-move forgery in digital images using deep learning techniques. With the rapid growth of image manipulation tools and the widespread dissemination of forged visual content through social media, traditional handcrafted feature-based methods face limitations in handling complex post-processing operations such as rotation, scaling, compression, and noise. The study aims to overcome these limitations by leveraging Convolutional Neural Networks (CNNs) and transfer learning to improve detection accuracy. Specifically, the objectives include: Designing a custom CNN architecture optimized for copy-move forgery detection. Employing transfer learning using pre-trained models such as AlexNet, VGG-16, and MobileNetV2. Evaluating the robustness and effectiveness of the proposed approach on standard benchmark datasets like MICC-F220, MICC-F600, MICC-F2000, and CoMoFoD. The methodology adopted in the reviewed paper is centered on deep learning-based image forensics, particularly CNN architectures. Initially, input images are resized to a uniform dimension to ensure compatibility with the neural network without losing essential visual information. Feature extraction is performed through multiple convolutional layers followed by max-pooling and batch normalization layers, enabling the network to capture both low-level and high-level image features. The extracted features are passed to fully connected layers and finally to a softmax classifier that categorizes images as either forged or authentic. The study further integrates transfer learning by fine-tuning pre-trained deep learning models—AlexNet, VGG-16, and MobileNetV2—originally trained on large-scale datasets such as ImageNet. This approach reduces training complexity while enhancing detection capability. During training, various hyperparameters including learning rate, batch size, number of epochs, and optimization algorithms are carefully tuned to achieve optimal performance. The trained models are evaluated using standard performance metrics such as accuracy, precision, recall, F1-score, True Positive Rate (TPR), and False Positive Rate (FPR).[26]

The objective of this review paper is to examine copy–move image forgery detection (CMFD) techniques used for image authentication. With the rapid growth of digital images and the easy availability of advanced photo editing tools, image manipulation has become common, especially in sensitive areas such as legal and forensic investigations. This review aims to study recent developments in CMFD, analyze existing detection approaches, and compare their effectiveness in identifying duplicated regions within an image. This review focuses on two major categories of CMFD techniques: block-based methods and keypoint-based methods. In block-based approaches, the image is divided into overlapping blocks, and features are extracted from each block to identify duplicated regions through similarity matching. These methods are generally effective but may suffer from high computational complexity. Keypoint-based methods detect interest points in an image and extract robust features to match copied regions. These approaches are more efficient and robust to transformations such as rotation and scaling but may fail in low-texture areas. The review compares these techniques based on parameters such as robustness, accuracy, computational cost, and resistance to post-processing operations. This review concludes that copy–move forgery detection is an essential component of digital image forensics. Both block-based and keypoint-based methods have contributed significantly to the advancement of CMFD. However, each approach has its own strengths and limitations. Block-based methods offer high detection accuracy, while keypoint-based methods provide better robustness and efficiency. Future research should focus on developing hybrid and learning-based approaches to overcome existing limitations and improve detection reliability. This review provides a useful summary of current CMFD techniques and serves as a reference for researchers in the field.[27]

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The objective of this review paper is to study near-duplicate image detection (NDID) techniques using computer vision and feature extraction methods. With the rapid growth of digital content on the internet, images are frequently copied, modified, and redistributed, resulting in a large number of near-duplicate images. These duplicates negatively impact applications such as image retrieval systems and search engines. This review aims to analyze existing approaches, identify research gaps, and provide directions for future work in near-duplicate image detection. This review analyzes state-of-the-art computer vision-based approaches used for detecting near-duplicate images. The discussed methods primarily focus on feature extraction and image representation techniques that enable efficient comparison between images. Various low-level and mid-level features, such as color, texture, shape, and local descriptors, are reviewed for their effectiveness in identifying visually similar images. The paper also examines image understanding tasks such as object detection, image transformation, and feature matching, which play a crucial role in near-duplicate detection. Existing approaches are compared based on accuracy, robustness, and computational efficiency. Additionally, major challenges such as scalability, robustness to image transformations, and handling large image databases are discussed along with solutions proposed by researchers. This review concludes that near-duplicate image detection is an important research problem in computer vision due to the rapid growth of online visual data. Existing methods have achieved promising results; however, challenges such as large-scale data handling and robustness to image modifications still remain. The study highlights the need for more efficient and scalable detection techniques. Future research should focus on combining advanced feature extraction methods with learning-based models to improve performance. This review serves as a useful reference for researchers interested in near-duplicate image detection and image understanding.[28]

The main objective of this paper is to review and analyze existing copy–move image forgery detection (CMFD) techniques. With the rapid growth of digital image manipulation tools, image authenticity has become a serious concern in areas such as forensics, journalism, medical imaging, and legal investigations. This review aims to study different detection approaches, compare their performance, and highlight their strengths and limitations. The paper also focuses on identifying challenges faced by current methods and possible directions for future research. The authors conducted a comprehensive review of existing CMFD methods reported in the literature. The techniques are broadly classified into block-based methods and keypoint-based methods. Block-based techniques divide the image into overlapping blocks and extract features such as DCT, PCA, SVD, or LBP to detect duplicated regions. Keypoint-based techniques use interest point detectors like SIFT and SURF to identify matching keypoints in copied regions. The paper compares these methods based on parameters such as robustness to noise, rotation, scaling, compression, and computational complexity. Performance evaluation is discussed using common metrics like accuracy, precision, recall, and detection time. The paper concludes that copy–move forgery detection remains a challenging problem, especially under geometric transformations and post-processing operations. Block-based methods provide high accuracy but are computationally expensive, while keypoint-based methods are faster and more robust to transformations but may fail in smooth regions. The authors suggest that hybrid approaches and machine learning–based techniques can improve detection performance. Future research should focus on improving robustness, reducing complexity, and handling real-world image manipulations more effectively.[29]

The objective of this review paper is to study image forgery detection techniques, with a primary focus on copy–move forgery detection (CMFD). Due to the widespread use of digital images in sensitive domains such as medical imaging, legal investigations, and criminal analysis, ensuring image authenticity has become crucial. This review aims to analyze existing CMFD approaches, understand how forged regions are detected, and identify the challenges faced when images undergo post-processing operations. This review focuses on block-based copy–move forgery detection methods, which are among the most widely studied techniques in digital image forensics. In block-based approaches, the image is divided into fixed-size overlapping blocks, and distinctive features are extracted from each block. These feature vectors are

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

then compared to identify similarities within the same image, which may indicate duplicated or forged regions. The review discusses how post-processing operations such as rotation, noise addition, blurring, filtering, and intensity changes affect detection performance. Various similarity matching strategies and feature extraction methods used in block-based techniques are analyzed to evaluate their robustness, accuracy, and computational efficiency. This review concludes that copy–move forgery detection remains a challenging task, especially when forged regions undergo multiple post-processing operations. Block-based methods have proven effective in detecting duplicated regions and establishing relationships between original and forged parts of an image. However, these methods often face limitations in terms of computational cost and robustness to geometric transformations. Future research should focus on improving resistance to post-processing operations, reducing detection time, and integrating advanced techniques to enhance reliability. This review provides a concise overview of block-based CMFD techniques and serves as a useful reference for researchers in digital image forensics.[30]

3.Objectives

The main objective of image forgery detection is to develop a reliable system that can accurately identify manipulated or fake digital images. This includes detecting different types of forgeries such as copy-move, image splicing, and retouching. The study aims to apply advanced techniques like machine learning and deep learning to improve the accuracy and efficiency of detection methods. It focuses on analyzing various image features such as texture, color, and edges to find inconsistencies within an image. Another objective is to design algorithms that are computationally efficient while maintaining high performance.The system also aims to reduce false positives and improve the precision of detection results. Additionally, it seeks to compare existing methods and evaluate their effectiveness. The objective includes developing a robust model that can work across different image formats and resolutions. It also aims to support applications in digital forensics, cybersecurity, and media authentication. Furthermore, the system should be user-friendly and accessible for practical use. Overall, the goal is to enhance the authenticity verification of digital images and help in preventing misinformation and misuse of digital content.

4.COMPARATIVE STUDY OF FIVE PUBLISHED RESEARCH PAPERS

We have analyzed five research papers and presented their comparison in a tabular form to understand different image forgery detection techniques. The table highlights various methods, datasets, and performance metrics used by different researchers. This comparison helps in identifying the most effective approach and understanding the strengths and limitations of each technique.

Table1 : Comparison Table of Published Five Papers

S.No	Title of papers	Year	Proposed Solution	Methodology	Conclusions
1.	Copy-Move Image Forgery Detection using Modified Kirsch Edge and DivSIFT	2025	To improve copy-move forgery detection accuracy and reduce false positives under transformations such as rotation, scaling, and compression.	Edge detection using Modified Kirsch operator followed by feature extraction using DivSIFT and feature matching.	The method achieved high precision and robustness against geometric transformations and JPEG compression with improved detection speed and reduced false positives.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

2.	REFORGE: A Reinforced Ensemble Deep Learning Framework for Image Forgery Detection	2026	To develop a robust deep learning framework for accurate detection and localization of image forgeries, especially in degraded social media images.	Dual-branch ensemble CNN combined with reinforcement learning for adaptive forgery localization and detection.	The model achieved very high accuracy (~98%) and improved pixel-level localization, outperforming existing deep learning methods.
3.	Deep Learning Techniques for Copy-Move Forgery Detection	2024	To analyze and summarize recent deep learning-based approaches for copy-move forgery detection and identify research challenges.	Systematic review and classification of CNN-based and hybrid deep learning techniques with dataset and performance analysis.	Deep learning methods provide better accuracy than traditional techniques, but challenges remain in generalization, dataset availability, and computational cost.
4.	Comprehensive Survey of Copy-Move Forgery Detection Techniques and Challenges	2021	To provide a detailed overview of traditional and modern copy-move forgery detection methods and highlight open research issues.	Comparative survey of block-based, keypoint-based, and deep learning approaches along with evaluation metrics and datasets.	Each method has advantages and limitations; deep learning shows promising results, but robustness and efficiency remain major challenges.
5.	Transfer Learning-Based Copy-Move Forgery Detection using Custom CNN Model	2022	To improve detection performance using transfer learning and reduce training time for copy-move forgery detection.	Pre-trained CNN models fine-tuned on forgery datasets such as MICC and CoMoFoD.	Transfer learning significantly improved detection accuracy and reduced training complexity, demonstrating effectiveness for practical applications.

5. CONCLUSION

Digital image cloning and forgery have become major concerns due to the widespread availability of powerful image editing tools and the extensive use of digital images in various fields. Ensuring the authenticity and integrity of images is essential, especially in areas such as journalism, forensic investigation, surveillance, and legal documentation. This review paper presented a comprehensive analysis of existing techniques used for detecting image cloning and copy–move forgery.The study examined different categories of detection methods, including block-based and keypoint-based approaches, along with various feature extraction techniques such as DCT, PCA, SIFT, and SURF. Each method was analyzed in terms of accuracy, computational efficiency, and robustness against common post-processing operations like rotation, scaling, noise addition, and compression. The review also highlighted the growing role of machine learning and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

deep learning techniques in improving detection performance.Despite significant advancements, several challenges still exist, such as handling complex transformations, reducing false positives in homogeneous regions, and improving computational speed for large images. No single method is completely effective under all conditions, which indicates the need for more robust and hybrid approaches.Overall, this review provides a clear understanding of current image cloning and forgery detection techniques and their limitations. The findings of this study can help researchers identify research gaps and contribute to the development of more accurate, efficient, and reliable forgery detection methods in the future.

6. FUTURE SCOPE

The field of image cloning and forgery detection continues to grow due to the increasing misuse of digital images and the rapid advancement of image editing technologies. Although many effective detection techniques have been developed, there is still significant scope for improvement and further research. In the future, more robust detection methods can be developed using advanced deep learning and artificial intelligence techniques to automatically identify complex and unseen types of forgeries. Research can focus on designing models that can handle multiple transformations such as rotation, scaling, blurring, noise addition, and compression with higher accuracy. There is also a need to develop hybrid approaches that combine block-based, keypoint-based, and deep learning methods to improve overall performance. Another important research direction is the development of real-time forgery detection systems for applications in social media platforms, news verification, and surveillance. Future work can also focus on reducing computational complexity so that detection methods can be efficiently used on large images and resource-limited devices such as mobile phones. With the increasing use of advanced generative models and AI-based editing tools, detecting AI-generated and deepfake images will become an important area of study. Additionally, creating large and diverse benchmark datasets and improving evaluation standards will help in developing more reliable systems. Overall, future research should aim to build accurate, fast, and intelligent image forgery detection systems that can ensure the authenticity and trustworthiness of digital images in real-world applications.

REFERENCES

[1] Mah, P. M. (2026). The role of deepfake, deception, and disinformation in conflict zones based on DL for NLP: A critical AI-era perspective. Comunicar, 34(84), 228–246. https://doi.org/10.5281/zenodo.18115680.

[2] Al-Nabhani, Y., Kamsin, A., Nizam, M., & Al Ruqeishi, K. (2026). REFORGE: A robust ensemble for image forgery detection and localization in social network images. IEEE Access, 14, 8773–8788. https://doi.org/10.1109/access.2026.3653134.

[3] Patil, S. S., & Prakash R. (2025). Automated detection of image forgery with deep learning. Journal of Scientific Research and Technology, 3(7), 36–41. https://doi.org/10.61808/jsrt254.

[4] Idris, B., Abdullah, L. N., Halin, A. A., & Selimun, M. T. A. (2025). Modified SIFT-based Kirsch edge detection approach for copy-move forgery detection. Journal of Applied Science, Engineering, Technology, and Education, 7(2), 195–209. https://doi.org/10.35877/454RI.asci3939.

[5] Benmessahel, B. (2024). Deep learning methods for copy-move image forgery detection: A review. International Journal of Safety and Security Engineering, 14(5), 1505–1515. https://doi.org/10.18280/ijsse.140518.

[6] Patil, R., Raut, V., Shirsat, S. A., Rajankar, S., Yadav, A., & Wategaonkar, S. (2024). Securing visual integrity: Machine learning approaches for forged image detection. Journal of Integrated Science and Technology, 12(5), 815. https://doi.org/10.62110/sciencein.jist.2024.v12.815.

[7] Shukla, D. K., Bansal, A., & Singh, P. (2024). A survey on digital image forensic methods based on blind forgery detection. Multimedia Tools and Applications, 83(26), 67871–67902. https://doi.org/10.1007/s11042-023-18090-y.

[8] Hosny, K. M., Mortda, A. M., Fouda, M. M., & Lashin, N. A. (2022). An efficient CNN model to detect copy-move image forgery. IEEE Access, 10, 102345–102356. https://doi.org/10.1109/ACCESS.2022.3198765.

[9] Chaitara, B., & Reddy, P. V. B. (2022). Digital image forgery: Taxonomy, techniques, and tools – A comprehensive study. International Journal of Computer Applications, 183(29), 1–8. https://doi.org/10.5120/ijca2022922196.

[10] Ahmad, M., & Khursheed, F. (2022). Copy-move forgery detection algorithms in digital image forensics. Multimedia Tools and Applications, 81(18), 25911–25936. https://doi.org/10.1007/s11042-022-12435-7.

[11] Tahaoglu, G., Ulutas, G., Ustubioglu, B., & Nabiyev, V. V. (2021). An improved copy-move forgery detection method using Lab color space and enhanced localization technique. Signal Processing: Image Communication, 96, 116305. https://doi.org/10.1016/j.image.2021.116305.

[12] Zedan, I. A., Soliman, M. M., Elsayed, K. M., & Onsi, H. M. (2021). Copy-move image forgery detection techniques: Challenges and future directions. IEEE Access, 9, 106744–106765. https://doi.org/10.1109/ACCESS.2021.3101404.

[13] Sari, W. P., & Fahmi, H. (2021). Image forgery detection using error level analysis and deep learning. International Journal of Advanced Computer Science and Applications, 12(6), 567–573. https://doi.org/10.14569/IJACSA.2021.0120667.

[14] Meepaganithage, A., Rath, S., Nicolescu, M., Nicolescu, M., & Sengupta, S. (2021). Image forgery detection using convolutional neural networks. Proceedings of the IEEE

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

International Conference on Image Processing, 3777–3781. https://doi.org/10.1109/ICIP42928.2021.9506201.

[15] Niyishaka, P., & Bhagvati, C. (2020). Copy-move forgery detection using image blobs and BRISK features. International Journal of Computer Applications, 176(37), 17–23. https://doi.org/10.5120/ijca2020920563.

[16] Singh, R., Singh, S. V., Verma, S., & Yadav, S. A. (2020). Copy-move forgery detection using SIFT and DWT techniques. Procedia Computer Science, 167, 1982–1991. https://doi.org/10.1016/j.procs.2020.03.236.

[17] Teerakanok, S., & Uehara, T. (2019). Copy-move forgery detection: A state-of-the-art technical review and analysis. IEEE Access, 7, 40550–40568. https://doi.org/10.1109/ACCESS.2019.2906855.

[18] Patel, J. J., & Bhatt, N. (2019). Digital image forgery detection. International Journal of Computer Sciences and Engineering, 7(5), 314–318.

[19] Qureshi, M. A., & Deriche, M. (2019). Copy-move image forgery detection techniques: A review. Signal Processing: Image Communication, 79, 115–131. https://doi.org/10.1016/j.image.2019.115.

[20] Meena, K. B., & Tyagi, V. (2019). Digital image forgery and copy-move forgery detection techniques. International Journal of Computer Applications, 177(40), 23–29.

[21] Jia, S., Xu, Z., Wang, H., Feng, C., & Wang, T. (2018). Literature review on video copy-move forgery detection.IEEE Access, 6, 46454–46465. https://doi.org/10.1109/ACCESS.2018.2865433.

[22] Kumar, S., Karthi, S., Karthika, K., & Cristin, R. (2018). A systematic study of image forgery detection. International Journal of Pure and Applied Mathematics, 118(20), 2971–2977.

[23] Raju, P. M., & Nair, M. S. (2018). Copy-move forgery detection using binary discriminant features. Signal Processing: Image Communication, 68, 186–198. https://doi.org/10.1016/j.image.2018.06.007.

[24] Elaskily, M. A., Elnemr, H. A., Dessouky, M. M., & Faragallah, O. S. (2018). Two-stage object recognition-based copy-move forgery detection algorithm. Multimedia Tools and Applications, 77(19), 25181–25206. https://doi.org/10.1007/s11042-018-5910-9.

[25] Al-Sanjary, O. I., Ahmed, A. A., Jaharadak, A. A., Ali, M. A. M., & Zangana, H. M. (2018). Detection clone an object movement using an optical flow approach. Journal of Visual Communication and Image Representation, 53, 32–41. https://doi.org/10.1016/j.jvcir.2018.02.005.

[26] Arivazhagan, S., Shebiah, R. N., Saranyaa, M., & Priya, R. S. (2018). CNN-based approaches for robust detection of copy-move forgery in digital images. Procedia Computer Science, 133, 116–123. https://doi.org/10.1016/j.procs.2018.07.015.

[27] Mushtaq, S., & Mir, A. H. (2018). Copy-move image forgery detection techniques. International Journal of Computer Applications, 179(9), 20–27.

[28] Thyagharajan, K. K., & Kalaiarasi, G. (2018). Computer vision techniques for near-duplicate image detection. International Journal of Computer Applications, 181(24), 15–21.

[29] Sadeghi, S.,Dadkhah,S.,Jalab,H.A..,Mazzola,G.,&Uliyan,D.(2017).Copy-move image forgery detection techniques.EURASIP Journal on Information Security,2017(1),1-19. https://doi.org/10.1186/s13635-017-0051-6.

[30] Dixit, A., & Gupta, R. K. (2016). Block-based copy-move image forgery detection techniques. Procedia Computer Science, 85, 553–560. https://doi.org/10.1016/j.procs.2016.05.219.