International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 01 | Jan - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

A Comprehensive Review of Deep Learning Techniques for Image Forgery Detection

Amrik Singh[1], [2] Isha Rani
[1]*Assistant Professor* ,[2]*PG Student*
Faculty of Computing ,Guru Kashi University
Talwandi Sabo,Bathinda,Punjab,India
[1]ratandeep2@gmail.com,[2] uppalisha968@gmail.com

Abstract

The rapid growth of multimedia content and advanced editing tools has led to widespread manipulation of digital images. While image editing serves artistic and legitimate purposes, it also presents significant risks, including misinformation, fraud and cybercrimes. As a result, image forgery detection has become a critical research area aimed at preserving the authenticity and reliability of visual content, especially in fields like journalism, law enforcement and digital forensics. Image forgery techniques have evolved from basic manipulations, such as splicing and copy-move, to more advanced methods like deepfakes, which use deep learning to generate hyper-realistic altered visuals. These challenges demand the development of sophisticated detection methods capable of adapting to these advanced forgeries.

Introduction

In today's digital era, the exponential growth of multimedia data and sophisticated editing tools has led to widespread manipulation of digital images. While image editing can serve artistic and legitimate purposes, it also poses significant threats in the form of forgeries used for misinformation, fraud, and cybercrimes. Image forgery detection, therefore, has emerged as a critical field of research, aiming to safeguard the authenticity and reliability of visual content. This domain seeks to address pressing concerns in journalism, law enforcement and digital forensics.

Image forgery techniques have evolved significantly, ranging from simple splicing and copy-move manipulations to advanced methods like deepfake creation. Copy-move forgery, for instance, involves duplicating and relocating parts of an image to conceal or highlight particular objects. Similarly, splicing entails merging multiple images to fabricate new content. Emerging challenges such as deepfakes, which leverage deep learning to generate hyper-realistic altered videos and images, represent an advanced frontier in forgery. These complexities necessitate the development of robust detection methods that can adapt to evolving manipulation techniques.

Machine learning (ML) has revolutionized the field of image forgery detection by automating the identification process and increasing detection accuracy. Unlike traditional approaches that rely heavily on handcrafted features, ML techniques can extract and analyse complex patterns and anomalies in images. By training models on large datasets of manipulated and authentic images, machine learning algorithms can distinguish between legitimate and tampered content with significant precision. This capability is particularly vital as forgeries become more sophisticated and imperceptible to the human eye.

Among the prominent machine learning techniques, supervised learning has been extensively utilized for forgery detection. Models such as Support Vector Machines (SVM), k-Nearest Neighbours (k-NN) and Random Forests have demonstrated success in classifying manipulated versus authentic images. Additionally, feature extraction methods like Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG) are commonly employed to enhance detection capabilities. These techniques focus on identifying inconsistencies in textures, edges, or lighting conditions that often arise during manipulation.

Deep learning, a subset of machine learning, has further advanced the field with the development of Convolutional Neural Networks (CNNs). These architectures excel at extracting hierarchical features from images, making them particularly effective for forgery detection. CNNs can identify subtle artifacts, inconsistencies in pixel distributions, or compression anomalies introduced during manipulation. Moreover, pre-trained models like ResNet, VGGNet, and MobileNet have been widely adopted for this purpose, enabling rapid deployment with minimal computational overhead.

Despite these advancements, image forgery detection still faces significant challenges. The diversity of manipulation techniques, variations in image quality and the introduction of adversarial forgeries complicate detection efforts. Additionally, the lack of standardized datasets for training and evaluation hinders the generalizability of machine learning models. As a result, researchers are actively exploring hybrid approaches that combine traditional and ML-based methods to achieve higher robustness and reliability.

Ethical and privacy considerations also play a crucial role in the development of forgery detection systems. Ensuring that such systems do not inadvertently violate user privacy or perpetuate biases remains a critical concern. Furthermore, there is a growing need for collaboration between academia, industry and policymakers to establish guidelines for the responsible use of image forgery detection technologies.

the integration of machine learning techniques in image forgery detection represents a transformative step in combating digital image manipulation. By leveraging advanced algorithms and computational power, researchers aim to create reliable and scalable solutions to ensure the authenticity of visual content. The dynamic nature of this field underscores the importance of continuous innovation, collaboration and ethical vigilance to address emerging challenges in the digital age.

Challenges in Forgery Detection

Image forgery detection is a complex and evolving field that faces a range of challenges due to the increasing sophistication of manipulation techniques and the subtlety of artifacts introduced during the modification process.

Invisible Manipulations: Many modern image manipulation techniques, such as high-quality splicing or retouching, introduce subtle changes that are difficult to detect. These changes can be so seamless that they are imperceptible to the human eye but still leave detectable traces that can be identified through advanced detection methods. For instance, slight inconsistencies in lighting, shadows, and reflections can be difficult to spot but can reveal signs of forgery when analyzed using machine learning.

Compression Artifacts: When an image is edited, it may undergo multiple stages of compression, especially when shared over social media or other online platforms. These compression algorithms can blur or smooth out forensic clues, making it harder to detect manipulated regions.

Blending and Seamlessness: Advanced forgery techniques aim to seamlessly blend manipulated sections with the rest of the image to make it appear as natural as possible. This blending can erase common signs of tampering, such as pixel-level inconsistencies or noticeable seams.

Deepfakes: One of the most advanced and alarming forgery techniques, deepfakes, involves the use of deep learning methods like Generative Adversarial Networks (GANs) to create hyper-realistic images or videos. These forgeries can be nearly indistinguishable from authentic content, making it extremely challenging for both humans and automated systems to detect them. Deepfake videos can manipulate facial expressions, voice synchronization and body language raising serious concerns about their use in spreading misinformation or committing fraud.

Face and Body Manipulation: With deep learning, it's possible to manipulate faces or even entire bodies in videos and images. The subtle shifts in facial expressions, gaze and movements, which are nearly impossible to discern without detailed analysis, pose a major challenge for forgery detection algorithms. As these techniques improve, the forged content becomes increasingly harder to detect, especially when coupled with AI-driven algorithms that generate realistic-looking content.

Neural Style Transfer: This technique, often used in image editing tools, allows the transfer of artistic features from one image to another. While it can serve legitimate creative purposes it can also be used to alter the style of an image or video to make it appear different complicating the forgery detection process.

Sophisticated Editing Software: The availability of advanced image manipulation software (Adobe Photoshop,GIMP) allows even novice users to perform complex edits with little to no visible traces of tampering. These tools enable the precise control over pixel-level details and can automate many aspects of the editing process, making forgery detection more difficult.

Deep Learning Tools for Forgery Creation: In addition to using deep learning for detection, malicious actors have access to deep learning-based tools that automatically generate realistic forgeries. For example, GANs and Variational Autoencoders (VAEs) can synthesize new images that appear authentic, often leaving no obvious indications of manipulation. These tools are continually improving, which makes detecting manipulated images a moving target.

Multiple Manipulation Methods: Forgers may use a combination of different techniques, such as splicing, copy-move, and deepfake creation, within the same image or video. These multiple manipulation methods can be difficult to detect using a single forensic approach, requiring models that can handle and differentiate between various types of forgeries.

Multimedia and Contextual Manipulations: Forgery detection is further complicated when different types of media (images, videos, and even audio) are involved. For instance, an image may be altered, and then combined with a manipulated video or audio, creating a multi-modal forgery. Detecting such forgeries requires analyzing different media types together, which can be technically challenging.

Adaptation to Detection Methods: As detection methods improve, so too do forgery techniques. Attackers often adapt their methods to counter detection algorithms by incorporating more subtle manipulations or even using AI to generate content that is designed to avoid detection. For example, adversarial attacks can subtly modify a forgery so that it evades traditional machine learning-based detection systems.

Real-Time Forgery Generation: Emerging techniques for real-time content generation (such as in the case of live-streamed deepfakes) add another layer of difficulty to detection. Detecting such forgeries in real-time requires highly efficient models capable of processing and analyzing content on the fly, which remains a major technological hurdle.

Dataset Limitations: The effectiveness of machine learning models in forgery detection heavily depends on the availability of large, diverse datasets that contain both authentic and manipulated images. However, high-quality labeled datasets for training models are scarce, particularly for emerging forgery techniques like deepfakes. Furthermore, dataset diversity is crucial, as forgeries can vary significantly based on factors like image resolution, manipulation tools, and the environment in which the image was taken.

Real-World Variability: In real-world scenarios, manipulated images may have been compressed, resized, or altered in ways that are not present in training datasets. These changes introduce additional challenges in ensuring the generalizability of detection systems.

Resource-Intensive Detection Models: Deep learning-based detection methods, particularly those involving CNNs and GANs, can be computationally expensive and require large amounts of memory and processing power. This makes it difficult to deploy forgery detection systems at scale or in real-time applications, such as social media platforms or online news websites.

Latency in Real-Time Applications: For real-time applications like live-streaming platforms, the latency introduced by deep learning models can be problematic. Ensuring both high accuracy and low latency is a difficult balance to achieve in real-world systems.

Literature Review

Selvaraj, S., & IM, R. (2021) declare that Images are used to convey information through newspapers, magazines, the internet, and scholarly journals. Software like Photoshop, GIMP, and Coral Draw make it difficult to distinguish between manipulated and genuine images. Handcrafted characteristics are mostly used in traditional methods for detecting image forgeries. The issue with conventional methods for detecting image tampering is that they often identify a certain kind of tampering by looking for particular elements in the image. We use an image dataset in this paper. To determine whether an image is fabricated or not, the CNN algorithm is employed [1].

Zanardelli, Et **al (2023)** illustrate that A significant quantity of manipulated and fraudulent photos have been created in recent years and disseminated via the media and the internet because image editing software are readily available and simple to use. Numerous methods have been put forth to evaluate an image's authenticity and, in certain situations, to pinpoint the manipulated (forged) regions. In this research, we explore several of the state-of-the-art Deep Learning (DL)-specific picture forgery detection approaches, with a particular focus on copy-move and splicing assaults that are frequently seen. Insofar as DeepFake-generated content is applied to photographs, it is also addressed, producing an effect akin to splicing. Given that deep learning-powered techniques yield the best overall outcomes on the benchmark datasets that are currently available, this survey is very pertinent. Along with outlining the datasets that these methods are trained and validated on, we also examine the salient features of these approaches. We also talk about their performance and, when feasible, compare it. Expanding on this study, we wrap off by discussing potential avenues for future research in deep learning architectural and assessment methodologies, as well as dataset construction for convenient technique comparison [2].

Kumar, Et al (2023) The widespread use of digital image editing tools in the digital age has led to the rise of picture counterfeiting as a regular problem. Image fraud can be harmful to a number of businesses, including journalism, forensics, and the arts.
Therefore, it is essential to offer reliable methods for spotting image forgeries. One effective tactic is to use machine learning techniques to identify signs of image manipulation automatically. In this review paper, we provide an overview of recent advances in machine learning-based image forgery detection. We discuss many techniques for image forgeries, such as splicing, retouching, and copy-move. We also provide an overview of popular machine learning methods, such as SVM, CNN, and Random Forests, that are used to detect picture forgeries. Next, the effectiveness of several feature extraction methods—such as the Scale-Invariant Feature

Transform and convolutional neural network-based features—to capture the unique characteristics of diverse kinds of picture forgeries is examined. There is also a discussion of several datasets that have been used to train and assess machine learning models for the detection of image forgeries. In conclusion, we assess the inadequacies of existing methods and outline possible directions for further research. We emphasize the need for real-time, workable solutions and the significance of developing trustworthy techniques that can detect novel forms of picture counterfeiting, such deepfakes.

This review paper aims to provide a comprehensive overview of current advancements in picture forgery detection using machine learning, making it a useful resource for academics and practitioners working in this subject [3].

Syed Sadaf Ali, Et al (2022) said that the prevalence of cameras has led to a rise in the popularity of taking pictures in recent years. In order to get additional information, it is frequently necessary to enhance photos, which makes them indispensable in our day-to-day existence due to their abundance of information. Many technologies are available to enhance the quality of photos; nevertheless, they are also sometimes used to manipulate images, which leads to the dissemination of false information. This makes picture forgeries more severe and common, which is currently a big cause for concern. Throughout time, a wide range of conventional methods have been developed to identify image forgeries. Convolutional neural networks, or CNNs, have drawn a lot of interest lately. CNNs have also had an impact on the field of image forgery detection. Nevertheless, the majority of CNN-based picture forgery methods found in the literature are only capable of identifying one particular kind of forgery—either image splicing or copy-move. Therefore, a method that can effectively and precisely identify the existence of hidden forgeries in an image is needed. In this research, we present a strong deep learning-based method for double image compression picture forgery detection. Our model is trained using the difference between an image's original and recompressed versions. The suggested model is small and light, and its results show that it is quicker than current methods. The experiment's overall validation accuracy of 92.23% is encouraging [4].

Sheikh pour ,Et al (2023) declare that One of the ways that people communicate with each other is through images. The proliferation and accessibility of digital devices, such smartphones and cameras, have made shooting photos anywhere in the world simple. Numerous applications in the fields of medicine, forensic science, and the judiciary use images. Since photos can occasionally be used as proof, digital images' validity and dependability are becoming more and more crucial. Some image manipulation techniques involve adding or removing portions of the image, rendering it incorrect. Consequently, it's critical to recognize and locate image forgeries. In the realm of computer vision, this topic has gained importance due to the advent of image altering tools. Numerous techniques have been put forth in recent years to identify image and pixel forgeries. Traditional and deep-learning approaches are the two basic categories into which all of these algorithms fall. One of the most significant areas of artificial intelligence research is deep learning. Because of its automatic identification and prediction capabilities, resilience to geometric alterations, and post-processing activities, this approach has grown to be one of the most often used approaches for the majority of computer vision issues. This study presents a thorough analysis of the various types of image forgeries, benchmark datasets, evaluation metrics, and traditional forgery detection techniques. It also identifies the shortcomings and restrictions of traditional techniques, explores forgery detection using deep learning techniques, and evaluates the effectiveness of this approach. Our primary focus in this work is deep learning-based counterfeit detection due to the approaches' popularity and their effective use in the majority of computer vision challenges. A researcher looking to get a thorough background in the topic of forgery detection may find this survey useful [5].

K. J. Et al (2022) Recent years have seen enormous advancements in imaging technology, enabling a wide range of portable devices, including tablets, mobile phones, wearables, and camcorders, to take digital photographs. Every day, these photos are posted on social media. In the meantime, photo-editing software features that date back to the early days of social networking are returning, and filtering is as simple as a few taps on your smartphone. The integrity and authenticity of digital photographs are now questioned, undermining consumer confidence in them due to recent advancements in image altering software. Here, we employ a machine learning method (SVM) to identify edited photographs with high accuracy and prevent users from trying to submit them [6].

Agarwal ,Et al (2020) describe that the prevalence of image modification software has increased due to its easy accessibility. Because the altered photos are indistinguishable with the human eye, they are spreading across multiple platforms, sparking rumours and deceiving a lot of people. This has prompted scientists to develop a number of methods for more accurately identifying altered photos. Conventional approaches to image forgery detection mostly rely on the extraction of basic features tailored to identifying a certain kind of fake. Recent research on neural network-based forgery detection has shown to be incredibly effective at identifying fake images. With more precision, neural networks can extract intricate hidden information from images. Since a deep learning model automatically creates the necessary features in contrast to more conventional methods of forgery detection, it has emerged as the new field of study in image forgery. The study analyses many methods utilizing neural networks to detect fabricated photos after first discussing several kinds of image forging strategies [7].

S. S. , Et al (2022) illustrate that Image forgery is the act of manipulating or modifying an image. At first glance, this picture alteration can seem innocent. To preserve the integrity of the evidence, however, images used in forensic investigations or legal actions must not be altered. One can manipulate an image in a number of ways. Just as there are many methods to anticipate forgery, there are also many methods to predict image forgery. The issue with those techniques, though, is that the average people cannot use them due to their extreme sophistication. This paper suggests creating a Deep Learning (DL) model as a solution to this problem. A dataset made up of authentic and fake photos is gathered for this purpose from the CASIA database. After that, this dataset is pre-processed. Preprocessing methods include denoising and scaling images. The DL model is then trained using the photos that have been processed. Next, the accuracy and loss are used as the primary parameters to verify the model's functionality. Ultimately, it is discovered that the model outperforms several existing DL models in terms of accuracy, producing results with greater than 95%. Similar to accuracy, it is discovered that the loss value is likewise so low as to be insignificant. As a result, the model performs better. The model can be implemented into a website in the future, which would make it practical [8].

Preeti Sharma ,Et al (2023) said that The digital image serves as vital proof in a variety of industries, including insurance claims, medical imaging, intelligence systems, criminal investigations, forensic inquiry, and journalism. Social media and the internet are reliable sources of information when it comes to images. However, photos can be maliciously manipulated or used for personal gain by using readily available software or editing programs like Photoshop, Corel Paint Shop, PhotoScape, Photo Plus, GIMP, Pixelate, etc. It is becoming more challenging to discern between actual and photo-realistic images when using active, passive, and other cutting-edge deep learning techniques like GAN methods. Nowadays, the main goal of digital picture tamper detection is to ascertain the consistency and legitimacy of digital images. Common tactics and solutions, like standardized data sets, benchmarks, evaluation criteria, and generalized methodologies, are employed to address the main research concerns. The assessment of several picture tamper detection techniques is summarized in this publication. This paper includes a comparative examination of picture criminological (forensic) approaches and a brief discussion of image datasets. Additionally, the limitations of recently emerging deep learning approaches have been discussed. This study uses both traditional and cutting-edge deep learning techniques to thoroughly assess image forgery detection techniques [9].

Satyendra Singh & Rajesh (2024) said that In the digital age, images are an effective means of disseminating information. Images can be found in periodicals, newspapers, healthcare, education, entertainment, social media, and electronic media, among other places. picture modification is now quite simple even for those without any prior knowledge or experience thanks to the development of picture editing software and affordable mobile devices with cameras. Thus, the veracity of the image has been questioned. While some may exploit the falsified image for amusement, others might have malicious intent. Political groups can use the altered image to disseminate their fake propaganda. People use fake photos to incite gossip and convey misinformation. Fake photos can hurt people, but they can also tarnish media outlets' reputations and erode public confidence in them. The need for trustworthy and effective picture forgery detection techniques to thwart propaganda, frauds, disinformation, and other nefarious applications of altered images. These are a few recognized problems with digital photos. Tools for identifying and detecting phony images are being developed by scientists, researchers, and picture forensic specialists. Digital picture forgery detection is currently a popular area of study. This paper's primary goal is to present a thorough analysis of methods and tools for detecting digital image forgeries. Additionally, it talks about different machine learning methods that can be used for image forgery detection, including supervised, unsupervised, and deep learning approaches. These methods highlight the difficulties that the field is currently facing [10].

Chunyin Shi, Et al (2023) said that In the information era, digital images have grown in importance as a means of information access. However, as this technology has advanced, digital photographs have grown increasingly susceptible to unauthorized access and manipulation, endangering social order, personal privacy, and national security. As a result, image forensic methods are now a hot topic for research in the area of multimedia information security. Deep learning technology has been used extensively in the field of visual forensics in recent years, and the results have greatly outperformed traditional forensic techniques. This survey contrasts the most recent iterations of deep learning-based picture forensic methods. There are two categories for picture forensic techniques: passive and active. The basic framework, assessment metrics, and frequently used datasets for forgery detection are described, along with an overview of forgery detection strategies in passive forensics. The effectiveness, benefits, and drawbacks of current techniques are also contrasted and examined in light of the various detection kinds. Robust image watermarking approaches are reviewed in the context of active forensics, and their fundamental framework and assessment criteria are provided. Based on the many kinds of picture attacks, the technical features and efficacy of current techniques are examined. In order to offer helpful recommendations for those working in image forensics and related study domains, future research paths and findings are finally presented. [11]

Qianwen Li ,Et al (2022) picture forging poses a severe threat to the security of picture material due to the growing significance of image information. Since the anomaly of copy-move forgery detection (CMFD) is less than that of other forgeries, it presents a larger problem. Super boundary-to-pixel direction (super-BPD) segmentation and deep CNN (DCNN) are the foundations of the proposed SD-Net image copy-move forgery detection and localization system, which aims to address the issue of the majority of image CMFD based on convolutional neural networks (CNN) having relatively low accuracy detection results. First, by strengthening the link between identical or comparable image blocks, segmentation technology improves detection accuracy. Second, DCNN is utilized to extract features from images, substituting automatic learning features for traditional hand-crafted features. By using the feature pyramid, the scaling assault resistance is increased. Thirdly, the final detected picture is obtained by optimizing the edges of the rough detected image using the image BPD information. The trials demonstrated how successfully the SD-Net could locate and identify numerous, rotating, and scaling forgeries, particularly large-scale scaling forgeries. When compared to alternative techniques, the SD-Net provides more precise location and resilience to a range of post-processing procedures, including noise addition, brightness and contrast modifications, color reduction, image blurring, and JPEG compression.[12]

Ivan Castillo Camacho and Kai Wang (2021) illustrate that Seeing no longer equates to believing. The capacity to alter an image is now at our fingers thanks to many approaches. The organizations that develop and market these technologies have focused on reducing the need for specialist knowledge as the difficulty of utilizing these strategies lowers. Moreover, modern image forgeries are so lifelike that it is challenging for the unaided eye to distinguish between authentic and fraudulent media. This may lead to a variety of issues, such as skewed public perception and the use of fabricated evidence in court. These factors make it crucial for us to have instruments at our disposal that can aid in truth-finding. This study provides an extensive assessment of the literature on picture forensics techniques, emphasizing deep learning-based approaches in particular. We address a wide range of picture forensics issues in this paper, such as identifying cameras, classifying computer graphics images, identifying purposeful image falsifications, detecting routine image alterations, and identifying Deepfake images as they emerge. This review has shown that, despite the fact that picture forgeries are getting easier to make, there are a number of ways to identify each type of one. Additionally provided are an overview of anti-forensic techniques and an evaluation of several image databases. Lastly, we propose a few future research avenues that the scientific community may take into account to address the proliferation of doctored photographs more successfully.[13]

.

Jian Zhang ,Et al (2024) The quick development of generative AI has two consequences: it makes content production faster, but it also makes image manipulation harder to spot. Despite their general effectiveness, existing image forgery detection and localization (IFDL) systems typically suffer from two issues: 1) their black-box nature, which leaves the detection principle undisclosed; and 2) their limited applicability across a variety of tampering techniques (such as Photoshop, DeepFake, and AIGC-Editing). In order to tackle these problems, we devise the explainable IFDL job and create FakeShield, a multi-modal framework that can assess the authenticity of images, produce tampered region masks, and offer a basis for judgment based on tampering clues at the pixel and image levels. Furthermore, we use GPT-4o to improve the quality of the already-existing IFDL datasets, resulting in the Multi-Modal Tamper Description dataSet (MMTD-Set), which is used to train FakeShield's tampering analysis functions. In the meantime, to handle different kinds of tamper detection interpretation and accomplish forgery localization guided by comprehensive textual descriptions, we integrate a Multi-modal Forgery Localization Module (MFLM) and a Domain Tag-guided Explainable Forgery Detection Module (DTE-FDM). Numerous tests show that FakeShield successfully locates and identifies different tampering methods, providing a more explicable and improved solution than earlier IFDL strategies [14].

R Sheth, C Parekha (2024) declare that the act of identifying photos that have been altered or manipulated for a variety of reasons, such as disinformation or malevolent intent, is known as picture forgery detection techniques. In digital image forensics, where academics have developed a variety of ways to identify picture forgery, image forgery detection is a critical task. These methods can be divided into four main categories: hybrid, machine learning-based, active, and passive. In active techniques, the image is created with digital watermarks or signatures embedded in it that can be used to identify any manipulation later. Conversely, passive methods depend on examining the image's statistical characteristics to find any discrepancies or anomalies that might point to fraud. This research proposes a deep learning algorithm utilizing ResNet for the detection of scaling and cropping attacks. The suggested technique, Res-Net-Adam-Adam, can distinguish between real and fraudulent photos with the highest level of accuracy, 99.14% (0.9914) [15].

Gurpreet Kaur , Et al (2023) illustrate that the study of digital photographs to find evidence of image modification is known as image forensics. The availability of several inexpensive gadgets for taking pictures has led to the rise in popularity of digital images these days. These photos are routinely altered, either intentionally or unintentionally, giving false information to the viewer. Since digital images are frequently utilized as evidence in court, by the media, and for record keeping, methods for spotting forgeries in digital images used in court trials and for maintaining visual records must be developed. Since digital images are frequently utilized as evidence in court, by the media, and for record keeping, methods for spotting forgeries in digital images used in court trials and for maintaining visual records must be developed. This article presents a thorough analysis of several image forgery detection strategies, along with comparisons between the approaches, advantages and disadvantages, and experimental findings [16].

Zhiyuan Yan , Et al (2024) illustrate that The development of current deepfake video detection is hampered by three major challenges: (1) Given the complexity and diversity of temporal variables, how may general temporal artifacts be found to improve model generalization? (2) Spatiotemporal models frequently favor one kind of artifact over another; how can we be sure that we are learning equally from both? Videos use a lot of resources by nature. How can we increase efficiency without sacrificing accuracy? The three difficulties are attempted to be simultaneously addressed in this paper. Firstly, we explore if and how video-level blending might be useful in video, motivated by the remarkable generality of employing image-level blending data for picture forgery detection. After conducting a comprehensive investigation, we discover a temporal forgery artifact that has not been thoroughly studied before: facial feature drift (FFD), which is a prevalent occurrence in several forgeries. Next, we suggest a novel Video-level Blending data (VB) that serves as a hard negative sample to mine more generic artifacts. VB is implemented by blending the original image and its distorted counterpart frame-by-frame. This allows for the replication of FFD. Second, we meticulously create a lightweight Spatiotemporal Adapter (StA) to enable the simultaneous and effective capture of both spatial and temporal information in a pretrained image model (both ViTs and CNNs). Because StA is built using two-stream 3D-Conv and different kernel sizes, it can process temporal and spatial information independently. Comprehensive tests confirm the efficacy of the suggested techniques and demonstrate how well our system generalizes to never-before-seen counterfeit movies, including the just revealed (in 2024) SoTAs. Our pretrained weights and code are publicly available at \url{https://github.com/YZY-stack/StA4Deepfake} [17].

Marcello Zanardelli ,Et al declare that Due to the ease of use and accessibility of image editing programs, a significant number of manipulated and fraudulent photos have been created in recent years and disseminated via the media and the internet.
Numerous methods have been put forth to evaluate an image's authenticity and, in certain situations, to pinpoint the manipulated (fabricated) regions. We examine some of the most recent Deep Learning (DL)-based image forgery detection approaches in this study, with a particular focus on copy-move and splicing attacks that are frequently seen. Insofar as DeepFake generated content is applied to photographs, it is also addressed, producing an effect similar to splicing. Given that deep learning-powered techniques yield the best overall outcomes on the benchmark datasets that are currently available, this survey is very pertinent. We talk about the important features of these techniques, together with a description of the datasets that are used for training and validation. We also talk about their performance and, when feasible, compare it. We discuss potential future research trends and directions in deep learning architectural and assessment methodologies, as well as dataset construction for convenient method comparison, as we expand upon this analysis in our conclusion [18].

Zankhana J. Barad; Mukesh M. Goswami (2020) Images of the material are disseminated via the internet, scientific publications, magazines, and newspapers. It is now exceedingly difficult to tell the difference between a tampered image and a genuine one because of programs like Photoshop, GIMP, and Coral Draw. Handcrafted characteristics are the mainstay of traditional image fraud detection techniques. The issue with conventional methods of picture tampering detection is that most of them can detect a particular kind of tampering by recognizing particular aspects in the image. Deep learning techniques are now employed to detect picture manipulation. Because these algorithms can extract complicated features from images, they reported higher accuracy than older methods [19].

Shruti Ranjan, Et al (2018) said that Recent years have seen a sharp increase in the number of cybercrimes. With advanced photo editing software still widely available, it has been demonstrated that creating phony papers is incredibly simple. These programs, which have resources easily accessible for that purpose, can scan and forge documents in a matter of minutes. There are ways to carefully examine these altered papers, even though photo editing software is widely available and convenient. The investigation of digitally altered documents is established in this study, which also offers a method for differentiating between the original and altered documents. The purpose of the Graphical User Interface (GUI) was to recognize photographs that had been digitally altered. This approach has shown itself to be effective and convenient, with a 96.4% accuracy rate [20].

Future Directions

As image and video manipulation techniques continue to evolve, there is a growing need for more sophisticated and adaptive detection methods.

Enhanced Deepfake Detection: Deepfake technologies, powered by Generative Adversarial Networks (GANs) and other advanced models, are becoming increasingly realistic. Future research should focus on improving the detection of deepfakes by developing models that can analyze finer details, such as inconsistencies in facial expressions, eye movement and micro-expressions, as well as detecting subtle distortions in the underlying audio and video synchronization.

Hybrid Approaches: One promising direction is the combination of different deep learning architectures to leverage the strengths of each model. For example, combining **Convolutional Neural Networks (CNNs)** for feature extraction with **Recurrent Neural Networks (RNNs)** or **Long Short-Term Memory (LSTM)** networks for temporal data analysis could improve detection in videos. Similarly, integrating **Generative Adversarial Networks (GANs)** for adversarial training and **Autoencoders** for anomaly detection could enhance model robustness.

Self-Supervised and Few-Shot Learning: Current deep learning models require large datasets for training, which can be a limitation. Future research could explore **self-supervised learning** and **few-shot learning** approaches to reduce dependency on large labeled datasets. These methods allow models to learn from fewer examples, making them more adaptable to new and emerging forgery techniques.

Cross-Domain Detection: The ability to detect forgeries across different types of media (images, videos, and audio) is another avenue for research. Cross-domain models that can jointly analyze image and audio data (for example, in deepfake videos) could significantly enhance the accuracy and versatility of forgery detection systems.

Conclusion

This review highlights the significant progress made in the field of image forgery detection, particularly through the application of deep learning techniques. Various models such as Convolutional Neural Networks (CNNs), Generative Adversarial Networks (GANs), Recurrent Neural Networks (RNNs) and Autoencoders have demonstrated promising results in identifying forged images and videos. The combination of feature extraction, anomaly detection, and temporal analysis offers a robust framework for detecting increasingly sophisticated manipulation techniques, such as deepfakes.

REFERENCES

[1] Selvaraj, S., & IM, R. (2021). Image Forgery Detection Using Machine Learning. *Available at SSRN 3950994*.

[2] Zanardelli, M., Guerrini, F., Leonardi, R., & Adami, N. (2023). Image forgery detection: a survey of recent deep-learning approaches. *Multimedia Tools and Applications*, *82*(12), 17521-17566.

[3] Kumar, Y., Kumar, R., Kumar, R., Kumawat, R., Soren, N., Kumar Jangir, S., & Singh, T. (2023). A Review on Image Forgery Detection Techniques Using Machine Learning. *Kilby*, *100*, 7th.

[4] Ali, S. S., Ganapathi, I. I., Vu, N. S., Ali, S. D., Saxena, N., & Werghi, N. (2022). Image forgery detection using deep learning by recompressing images. *Electronics*, *11*(3), 403.

[5] Mehrjardi, F. Z., Latif, A. M., Zarchi, M. S., & Sheikhpour, R. (2023). A survey on deep learning-based image forgery detection. *Pattern Recognition*, 109778.

[6] Latha, K., Kavitha, D., Hemavathi, S., & Velmurugan, K. J. (2022, December). Image Forgery Detection Using Machine Learning. In *2022 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS)* (pp. 1-6). IEEE.

[7] Agarwal, R., Khudaniya, D., Gupta, A., & Grover, K. (2020, May). Image forgery detection and deep learning techniques: A review. In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1096-1100). IEEE.

[8] Gupta, P., Rajpoot, C. S., Shanthi, T. S., Prasad, D., Kumar, A., & Kumar, S. S. (2022, October). Image forgery detection using deep learning model. In *2022 3rd International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 1256-1262). IEEE.

[9] Sharma, P., Kumar, M., & Sharma, H. (2023). Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation. *Multimedia Tools and Applications*, *82*(12), 18117-18150.

[10] Singh, S., & Kumar, R. (2024). Image forgery detection: comprehensive review of digital forensics approaches. *Journal of Computational Social Science*, 1-39.

[11] Shi, C., Chen, L., Wang, C., Zhou, X., & Qin, Z. (2023). Review of image forensic techniques based on deep learning. *Mathematics*, *11*(14), 3134.

[12] Li, Q., Wang, C., Zhou, X., & Qin, Z. (2022). Image copy-move forgery detection and localization based on super-BPD segmentation and DCNN. *Scientific Reports*, *12*(1), 14987.

[13] Castillo Camacho, I., & Wang, K. (2021). A comprehensive review of deep-learning-based methods for image forensics. *Journal of imaging*, *7*(4), 69

[14] Xu, Z., Zhang, X., Li, R., Tang, Z., Huang, Q., & Zhang, J. (2024). FakeShield: Explainable Image Forgery Detection and Localization via Multi-modal Large Language Models. *arXiv preprint arXiv:2410.02761*.

[15] Sheth, R., & Parekha, C. (2024). An intelligent approach to classify and detection of image forgery attack (scaling and cropping) using transfer learning. *International Journal of Information and Computer Security*, *24*(3-4), 322-337.

[16] Kaur, G., Singh, N., & Kumar, M. (2023). Image forgery techniques: a review. *Artificial Intelligence Review*, *56*(2), 1577-1625.

[17] Yan, Z., Zhao, Y., Chen, S., Fu, X., Yao, T., Ding, S., & Yuan, L. (2024). Generalizing deepfake video detection with plug-and-play: Video-level blending and spatiotemporal adapter tuning. *arXiv preprint arXiv:2408.17065*.

[18] Zanardelli, M., Guerrini, F., Leonardi, R., & Adami, N. (2023). Image forgery detection: a survey of recent deep-learning approaches. *Multimedia Tools and Applications*, *82*(12), 17521-17566.

[19] Barad, Z. J., & Goswami, M. M. (2020, March). Image forgery detection using deep learning: a survey. In *2020 6th international conference on advanced computing and communication systems (ICACCS)* (pp. 571-576). IEEE.

[20] Ranjan, S., Garhwal, P., Bhan, A., Arora, M., & Mehra, A. (2018, May). Framework for image forgery detection and classification using machine learning. In *2018 2nd international conference on trends in electronics and informatics (ICOEI)* (pp. 1-9). IEEE.