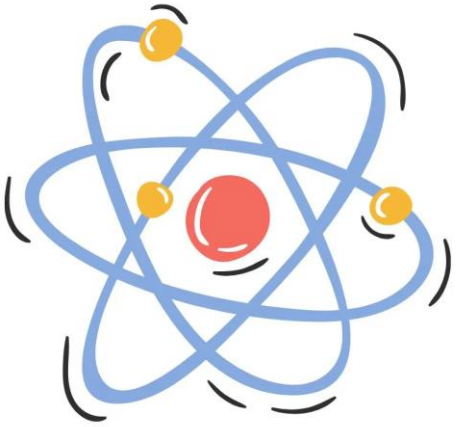

JOURNAL OF DYNAMICS AND CONTROL

VOLUME 8 ISSUE 11

IMAGE TAMPERING DETECTION: A REVIEW OF MULTI-TECHNIQUE APPROACH FROM TRADITIONAL TO DEEP LEARNING

Vitthal B. Kamble[1], Dr. Nilesh J. Uke[2]

[1]research Scholar, Department of Computer Engineering, Vishwakarma Institute of Technology, Kondhwa Budruk, Pune, Maharashtra - 411048, India
[2]professor, Department of Computer Engineering, Indira College Of Engineering And Management, Parandvadi, Pune, Maharashtra – 410506, India

IMAGE TAMPERING DETECTION: A REVIEW OF MULTI-TECHNIQUE APPROACH FROM TRADITIONAL TO DEEP LEARNING

Vitthal B. Kamble[1], Dr. Nilesh J. Uke[2]

[1]Research Scholar, Department of Computer Engineering, Vishwakarma Institute of Technology, Kondhwa Budruk, Pune, Maharashtra - 411048, India
(Affiliated to Savitribai Phule Pune University, Pune India)
[2]Professor, Department of Computer Engineering, Indira College of Engineering and Management, Parandvadi, Pune, Maharashtra – 410506, India
(Affiliated to Savitribai Phule Pune University, Pune, India)
ORCD Ids: [1]0000-0003-4684-0104, [2]0000-0002-3281-5429
[1]vitthalk13@gmail.com, [2]nilesh.uke@gmail.com

Abstract: Digital images have applications in many different fields, including journalism, forensic analysis, police inquiry, smart systems, and radiologic diagnostics. Social media and online photographs are trustworthy sources of information. Photos can be changed or utilized for personal gain with the help of easily accessible software or editing programs like Photoshop, Corel Paint Shop, PhotoScape, PhotoPlus, GIMP, Pixelmator, etc. Photo-realistic photographs are now difficult to differentiate from actual photographs due to advancements in deep learning techniques like GAN (deep reinforcement learning) and other active, passive, and other techniques. Today, the goal of digital picture tampering detection is to guarantee the consistency and dependability of digital photographs. Maintaining the integrity of digital content is very important in different domains such as journalism, media, social media, forensics, and national security. This survey analyzes both active and passive image forgery techniques to identify the tampering signs and manipulation done in the image content. The forgeries in manipulated images are identified using camera source identification, JPEG compression tampering, illumination inconsistencies, and mathematical manipulation. These diverse approaches provide a clear overview of the image forensic field. To address the primary research challenges, normalized input sets, gauges, and analysis standards are used. In this paper, the numerous tampering techniques for recognition are summarized. In addition to comparing image criminological (forensic) approaches, this work also briefly discusses image datasets. Over the last little while the expanded deep neural network techniques and also its shortcomings have been examined. Here, in this paper, you will find fully examined photo tampering identification techniques using both standard and cutting-edge neural network techniques. The most recent methods were unable to reliably identify multiple attacks including whirligig, smearing, proportioning, JPEG compression, and illumination strength. Computational intensity, feature dimensionality, detection accuracy, and resistance against further creation are additional issues that must be resolved.

Keywords: Digital image forensics, GAN, Copy-move tampering identification, Deep Learning techniques

1. INTRODUCTION

Digital image tampering presents a formidable challenge, involving the deceptive manipulation and alteration of computer-generated images. It is emerging as a matter of grave uneasiness for the people at large, prompting heightened attention and scrutiny. Merriam-Webster defines image forgery as the fraudulent and deceptive modification of digital pictures, a practice that dates back to as early as 1840. The act of image forgery entails the replication of images with altered parameter values [1]. Law enforcement agencies worldwide are increasingly alarmed by the proliferation of serious image forgery cases [2]. The widespread availability of image alterations like editing, enhancement and correction, modification, and creation tools further contribute to the escalation of these illicit activities.

The advancement of online image editing software has increased the risk of image tampering and this impact can be noted in multiple sectors. When conducting multiple legal investigations, image tampering techniques can alter the evidence affecting the judicial outcomes. In the journalism field, fabricated information can affect public opinion. Researchers often use tampered images in their scientific research to support their fraudulent findings affecting the integrity of the scientific research. In social media, people spread fake information which causes more harm to society. Hence, this arises the need for effective techniques to identify image tampering and safeguard the integrity of visual content.

Digital images hold immense significance in various fields like journalism, detective work, decision support structure, diagnostic scans, claim submissions, and also forensic investigation where they often serve as crucial evidence. Consequently, ensuring the originality of these images and detecting any tampering has become a matter of paramount importance. So as a result, the significance of image tampering detection techniques has grown significantly within society [3]. To underscore the gravity of the issue, this paper presents two instances of image forgery in Figures 1 [5] and 2 [4] (Fig. 2).

Figure 1 depicts an incident involving Deepfakes, an advanced technology based on deep learning. Deepfakes leverage Generative Adversarial Networks (GANs) to create counterfeit images or videos by seamlessly alerting one's face to another. The dissemination of tampered faces and videos on online media gives rise to ethical, communal, and safety concerns, namely the proliferation of misinformation with fraudulent activities [5,6]. Deep fakes can achieve face manipulation through various techniques, including complete facial integration, personality swap, and characteristic exploitation, coupled with utterance alteration. GANs, consisting of deep learning one generating data and other discerning between bogus and valid information which operates in an unsupervised manner, thereby introducing an "adversarial" element to the model [7,8].

With the rapid emergence of new GAN variations, forensic models face increasing challenges in recognizing novel types of forged images [9]. Consequently, the advancement in the facial deception identification model capable of generalizing its performance to unknown sources or datasets has become a pressing need, propelling digital forensics research toward addressing more generic problems. Thus, the implementation of a global approach, including the establishment of equalized information, and standards, included with analysis requirements, assumes paramount importance in developing new frameworks and mitigating the risks associated with digital tempering.

Fig.1 The forge image is showing that the Bollywood actor Shahrukh khan is with Salman khan where as in reality the real image of the left shows the actor Salman Khan is with a totally different Bollywood actor Amir khan

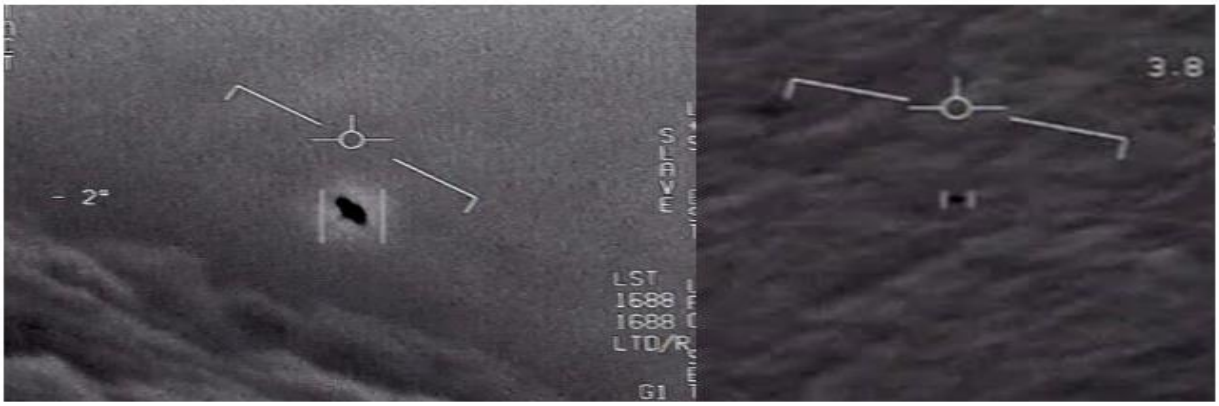

Fig.2 The trail left by a plane was captured by a gimble camera of a fighter jet and mistaken by many as a UFO Sighting. Which spread fake news and chaos around June 2021 when the Pentagon confirmed that the footage was real

Research on image forgery indicates that these crimes are predominantly committed with the intent to disseminate misleading or false information, gain political influence, and achieve immoral exposure with its strong points. Halting the dissemination of inaccurate data or finding urgent solutions to address this issue is imperative. Visual media analysis, which is a branch of computer investigation, focuses on the detection and validation of image tampering [10]. This burgeoning field aims to ascertain the origin and authenticity of digital media, playing a crucial role in preventing far-reaching consequences stemming from forgery at national and global levels. Given the increasing reliance on vast amounts of data across various domains like the legal profession, forensics, online networking, health field, and online photographs forensics guarantees the integration included with validation for such kind of information [11].

Copy-move forgery, splicing, image retouching, resizing, image warping, noise addition and removal, and deep fakes are some of the most common image tampering techniques. Copy-move forgery is also called cloning which copies a certain area of an image and pastes it within the same image to create a duplicate image or conceal certain parts of the image. This technique is normally used by people to enhance their appearance or remove unwanted objects from the scene. Splicing which is known as image composition integrates two images into one for a seamless transition. This is mainly used by people to spread fake information on social media to improve one's reputation or harm others.

Image retouching makes minimal changes in the image to alter its appearance. The operations performed here are smoothing color enhancement and lighting adjustment. This technique is used by advertising agents and normal people to improve their facial features and advertise their cosmetic procedures/products. Resizing modifies the aspect ratio of an image to distort the actual visual representation. It mainly alters the object's size to increase the product's quality or efficiency.

Image warping manipulates the image’s geometry to alter the faces or objects in an image. Warping is used by celebrities to modify their body shapes to give a slimmer face and physique and even perform muscle enhancements. Noise addition and removal affect the image's authenticity by performing random variations in the color of the image. It is mostly used in forensic scenarios, where the evidence in the surveillance footage is altered to help someone who performed illegal activities. Deep fakes are one of the popular techniques that use AI algorithms to generate fake videos that are highly realistic in nature. These techniques are mainly used to impersonate popular figures to generate fake news or spread political misinformation. Image forensics employs techniques classified into two main categories of photograph tampering identification: dynamic picture imitation, and inactive or vision-impaired imitation identification, as illustrated in Figure 3.

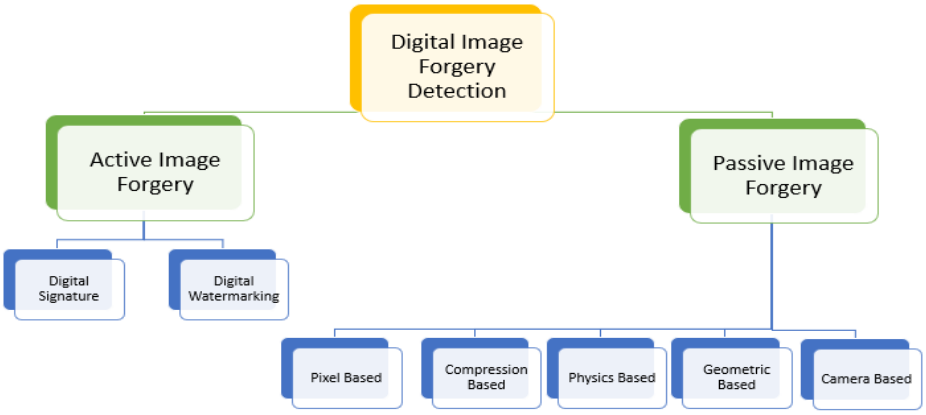

Fig.3 Dynamic and passive image imitation

Active forgery identification techniques encompass two approaches: electronic autograph and image tracking. These methods necessitate the pre-embedding of information in the image during capture, picture gathering, or at a later stage. However, in practical scenarios involving forensic investigations like biometric identification, culprit images, incident location photos, etc., it is highly unlikely to encounter watermarks or signatures. Consequently, active forgery detection techniques have been proven more effective in the forensic examination of digital images but offer limited utility in forensic investigations [12,13].

Conversely, passive forgery detection does not rely on prior imprinted data of the pictures. Instead, it operates with identifying the natural characteristics of the picture which is typically presented on the type of manipulation employed or by discerning the picture's origin. This paper comprehensively explores traditional and modern forgery detection techniques as discussed by various authors, providing valuable insights into image tampering, its various categories, approaches, accessible information sets, utility programs, constraints also with current advancements in neural networks. As a result, it serves as a solid foundation for researchers entering this domain, while also suggesting promising avenues for future research.

The main focus of different image forgery techniques used in this review is copy move and splicing attacks, deep learning techniques, dataset utilization, generalization performance improvement, and performance comparison. Deep learning techniques identify the manipulated facial images using feature extraction, binary classification, advanced architectures, and benchmark datasets (FaceForensics++). The features can be learned using convolutional layers and classified using GANs and transformers for improved detection accuracy. This paper mainly analyzes the advances in digital image tampering detection and the major issues faced in this field. It also identifies their role in radiologic diagnostics, smart systems, police inquiry, journalism, and forensic analysis. The main contributions of this research are presented as follows:

- This paper's main novelty lies in the extensive summary conducted using different artificial intelligence techniques and comparing various image forensic applications.
- This paper also evaluates the different deep-learning techniques for photo tampering identification and the various image datasets.
- A detailed discussion is provided regarding the challenges faced in deploying the developed technique practically and the potential areas of future research.

2. **Challenges in tampering detection:**

The major challenges associated with tampering detection are:

- **Advanced tampering techniques:** The modern-day image editing tools help people to generate highly realistic tampered images. The deep fake technology often complicates the tampering detection process of the novel techniques developed.
- **The increasing complexity of tampering images:** The tamperers often alter the faces of people using multiple layers of editing complicating the anomaly detection process. The programmer often needs deep learning and understanding of the contextual information of the image which is not an easy concept.
- **Lack of proper countermeasures:** The image manipulator often creates new techniques to evade detection and hide their tampering process. The techniques used to achieve this manipulation are watermark removal, compression artifacts, and noise addition.
- **Absence of ground truth data:** There is only a minimal number of datasets present online with the ground truth details. The information associated with the actual and tampered image details is very little which infers the ability of the novel techniques developed to withstand image tampering.
- **Real-time tampering detection:** Real-time tampering detection is often complex when dealing with multimedia datasets due to the high computational cost and complexity associated with them.
- **Ethical considerations:** Privacy violations need to be focused on when conducting image tampering analysis in surveillance videos or law enforcement analysis.

3. ACTIVE IMAGE TAMPERING DETECTION CLASSIFICATION

Active approaches in image manipulation detection rely on the inclusion of additional information, such as digital watermarks, at the procurement stage of the picture or individuals authorized at later stages. This embedded information is then used for manipulation detection (Barad & Goswami, 2020). Dynamic picture tampering identification encompasses two main approaches: image tracking and electronic autographs. These techniques are used within the field of dynamic scientific investigation to feed authentic data into pictures, thereby ensuring the integrity and authenticity of the visual content. When there is doubt regarding the validation of an image, the implanted genuine data is gained back to originate the credibility of the picture [14]. The presence of multiple processing steps in digital image handling poses a limitation in the realm of active picture imitation identification. To overcome this challenge, two essential techniques, namely image tracking and electronic autographs, are employed to identify and uncover instances of image manipulation [15,16].

3.1 Image Tracking

To discern the presence of embossment, the image is subjected to the topmost extent of a straight conversion record arrangement. This process involves computing the spatial cross-correlation function of the sequence and the watermarked image itself [17] This data incorporates or links with real-time photo authentication, which guarantees the presence of a validation code during image production or transmission. Nevertheless, deceptive image-capturing or manipulation tools have the potential to modify the provided data. If a duplicate photo matches its actual picture and is imitated with the help of various editing tools that means it is not that efficient to do so. That means it lacks some basic data needed to do so and hence desired result is not produced. Ferrara et al. [7] introduced a scientific tool that focuses on the approximation steps to evaluate both sections genuine and tampered segments of an image. This technique is employed in imitation identification, where the conditional co-occurrence probability matrix (CCPM) plays a crucial role in identifying third-order statistical characteristics. The numeric characteristics are instrumental in detecting picture splicing, which is a form of tampering with different portions where multiple images are combined together to obtain a deceptive synthesized picture. The conditional co-occurrence probability matrix (CCPM) is a computational tool that is very useful in image forensics. It captures the likelihood of specific pixel values appearing together in a particular spatial arrangement. An innovative approach to detect copy-move forgeries was done by extracting circular blocks using the Local Binary Pattern (LBP) [17]. The detection of forgeries in rotated regions at various angles is acknowledged to be particularly arduous in this context. Hussain et al. [13] put forward a novel technique for identifying image forgeries, known as the multiresolution Weber Local Descriptors (WLD) technique. The technique simply focuses on analyzing the characteristics of saturation of the constituents. For detecting imitation,

the technique employs the Support Vector Machine (SVM) categorizer in conjunction with the WLD histogram building blocks.

3.2 Digital Signature

In the realm of photo imitation or tampering detection, electronic autographs serve as a prevalent method. These signatures utilize a mathematical structure to represent the authenticity and reliability of a computerized record. Digital signatures are domain-specific utilities that imbibe genuine customers concerning the available data on the device [18].

To ensure the integrity of the image during production or transfer, digital signatures are augmented with dynamic photo validation, which incorporates a validation code. A resilient pixel is extracted from the real image and included in e-autographs. The picture is separated into parts of 16x16 bits pieces, and every piece is subjected to a series of random matrices produced with the help of a confidential code, k. These matrices undergo regular low pass filtering, resulting in N unpredictable even patterns. By using the method of applying the signing technique to a computerized image, the computer generates a unique electronic signature.

Key Qualities of Digital Signatures:

1) only the sender has the ability to sign a real picture, while its receiver solely verifies the autograph.2) The autograph can be recognized as unreal by authenticated users. 3) Remains valid and verifiable over an extended period.4) Digital signatures provide integrity and prevent tampering. Doke et al. [8] introduced a method involving low-phase filters to obtain an X unpredictable design to a haphazard matrix in a recurring manner. The image signing operation comprises several phases:

- Decomposing images using configurable pulse attributes.

- Removing the guideline for real-time autographs.

- Securely generate the encryption signature by applying the confidential passcode and encrypting the removed configurable pulse attributes.

- The receiver takes in both the real-time pictures and the encrypted autographs.

A shared picture-based recognition structure based on a difficulty-acknowledgment strategy was developed for imagery passwords and picture disordering [19]. The software application window is divided into k grids, each containing h cells. Users are required to correctly identify images during the image selection procedure, where k-pass images are randomly chosen from a database of N JPEG images. This framework enhances authentication by leveraging image-based challenges and responses. Techniques to identify digital image tampering are Statistical analysis, feature-based techniques, machine learning and deep learning, forensic analysis, and contextual analysis are the digital image tampering techniques.

Statistical analysis: Histogram analysis, noise analysis, and correlation analysis are the techniques used to evaluate the distribution of pixel values, noise patterns, and correlation in the image and identify the inconsistencies.

Feature-based methods: Here, the inconsistencies and artificial textures in the image are identified using edge detection, texture analysis, and watermarking detection.

Machine learning and deep learning models: CNNs, GANs, and autoencoders analyze the underlying structure of real images to detect the abnormalities in the tampered images. The CNN can be trained on large datasets to learn new features and patterns whereas the GAN can generate real tampered images.

Forensic analysis: Here, the inconsistencies and tampering signs are detected by analyzing the metadata, file format, and compression artifacts.

Contextual analysis: This technique detects inconsistencies and signs of tampering using image content, image history, and cross-reference analysis.

The summary of the active image tampering detection techniques is presented in Table 1.

Table 1: Summary of active image tampering detection techniques

Technique name	Purpose	Dataset used	Advantage	Drawbacks
Conditional concurrency probability matrix [7]	For image tracking by identifying third-order statistical characteristics.	CASIA, TIDEv2	It is applicable for image splicing since it identifies complex image combinations	This model cannot identify image tampering done using deep fakes and it also involves complex computations
Circular Blocks and Local Binary Pattern (LBP) [17]	Uses LBP and circular blocks to detect forgeries done using copy-move operation	MICC-F600	Efficiency is high when identifying rotated forgeries and regions with repeated image patches.	It is not effective when detecting global tampering or splicing
Multiresolution web local descriptors (WLD) [13] and SVM	The image forgery is mainly identified by focusing on saturation features via WLD and SVM	CoMoFoD	Can detect subtle variations in images along with low-light forgeries	The performance deteriorates for heavily edited images.
Digital signature [8]	An authentication procedure using digital autographs with a validation code	Surveillance dataset	Efficient in legal and forensic authentication	However, this approach is susceptible to attacks from the cryptographic system since it involves a complex signing process
Image-based password recognition [19]	An image challenge-response system which helps users to identify images from a randomized database	Login mechanism dataset	The image-based challenges improve security	Since it is an authentication mechanism it cannot be directly applied for tampering detection.
Image inpainting detection [18]	The tampering location is identified by the 8-neighborhood fast-sweeping method	Image restoration datasets	Identified the restored regions accurately	Not focused on splicing detection.

4. PASSIVE IMAGE TAMPERING DETECTION CLASSIFICATION

This section focuses on the characterization of inactive picture imitation identification, which currently is the utmost advanced identification strategy for addressing picture imitation. Passive image science, which is also recognized as blind picture science, aims to identify the accuracy and the source of the picture apart from relying on pre-installed information [20]. It encompasses five main methods: Pixel-based detection, Format-based detection, Physical-based

detection, Camera-based detection, and Geometry-based detection. These methods incorporate various detection techniques as illustrated in Figures 4 and 5.

These techniques are commonly employed (regardless of the device used) to manipulate or replicate a picture to see the malicious or culprit purposes [21]. Various picture formatting methods must be utilized to achieve these objectives. Passive image forgery detection techniques analyze one or more images to unveil intricate traces of inconsistencies within the forged image. These inconsistencies may include overlapping artifacts, lack of data, deformations, also with added features of the identifiable impression of thumb that serve as hints in picture science.

4.1 Tampering detection with the help of bits

Classification of bits involves examining individual pixels by utilizing the available spectral information specific to each pixel. These techniques are commonly employed for fetching applications from the picture itself that are not located at a high level and classify it according to the data available [22]. However, misclassifications may occur in areas where different classes overlap, leading to confusion. Pixel-based forgeries encompass significant categories such as Copy-move, photo segmentation, photo interpolation, and photo editing. Extensive research has been conducted in developing various detection methods, with a current focus on utilizing Deep Learning Approaches to tackle these challenges effectively.

4.1.1 Methods Based on Copy and Move

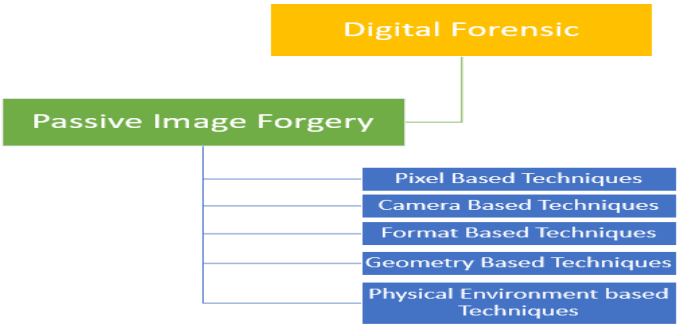

Fig.4 Types of Passive Tampering Detection

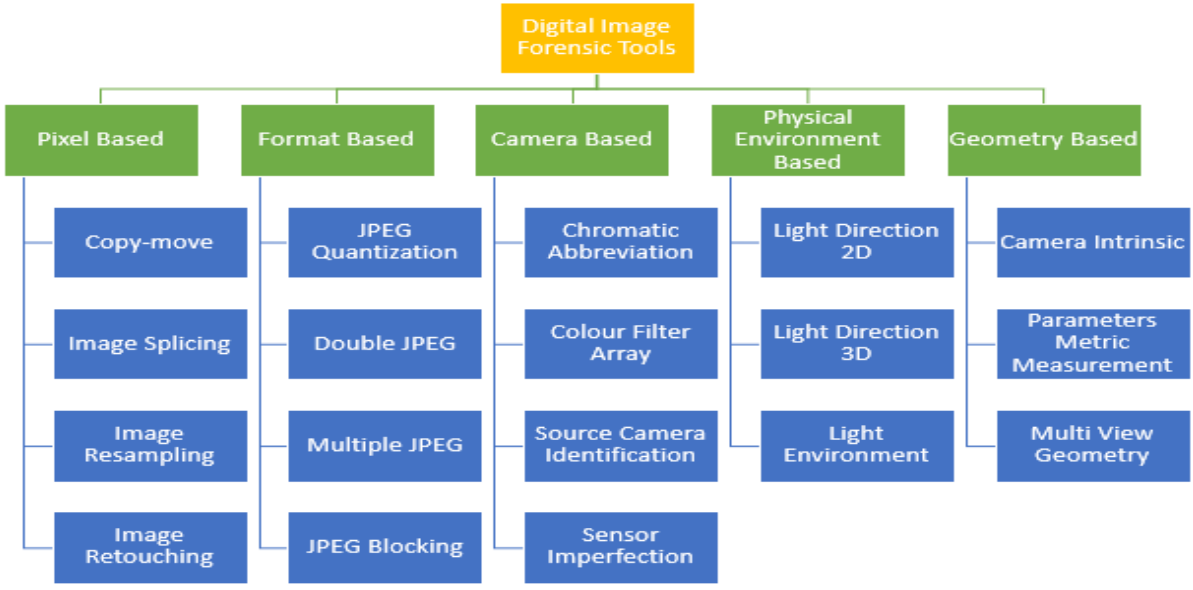

Fig.5 Various image tampering detection techniques- classification

Copy and Move-based methods are among the most commonly employed image tampering techniques and are also quite challenging to detect the duplicated picture being sourced from its original picture. In Copy-Move image imitation, a section of a picture is replicated and attached to another part of the same picture [11]. There are two types of attacks: class-1 copy-shift imitation and class-2 clone and create imitation. Examples of class-1 and class-2 attacks can be seen in Figures 6a and 6b [12, 13]. The detection methods identified for Copy-Move imitation can be characterized as block-based and key point-based, as listed below.

This technique is frequently utilized as a means of maliciously manipulating images to alter their message or hide specific portions using other images or real-time consequences. Photo-changing applications like duplicate and clone filters are employed [23]. Due to this, the forged picture exhibits distinct evidence for deformation, real-time corrections, converging, and various other beautiful effects. The length and width of a manipulated piece also can be studied to identify picture imitation.

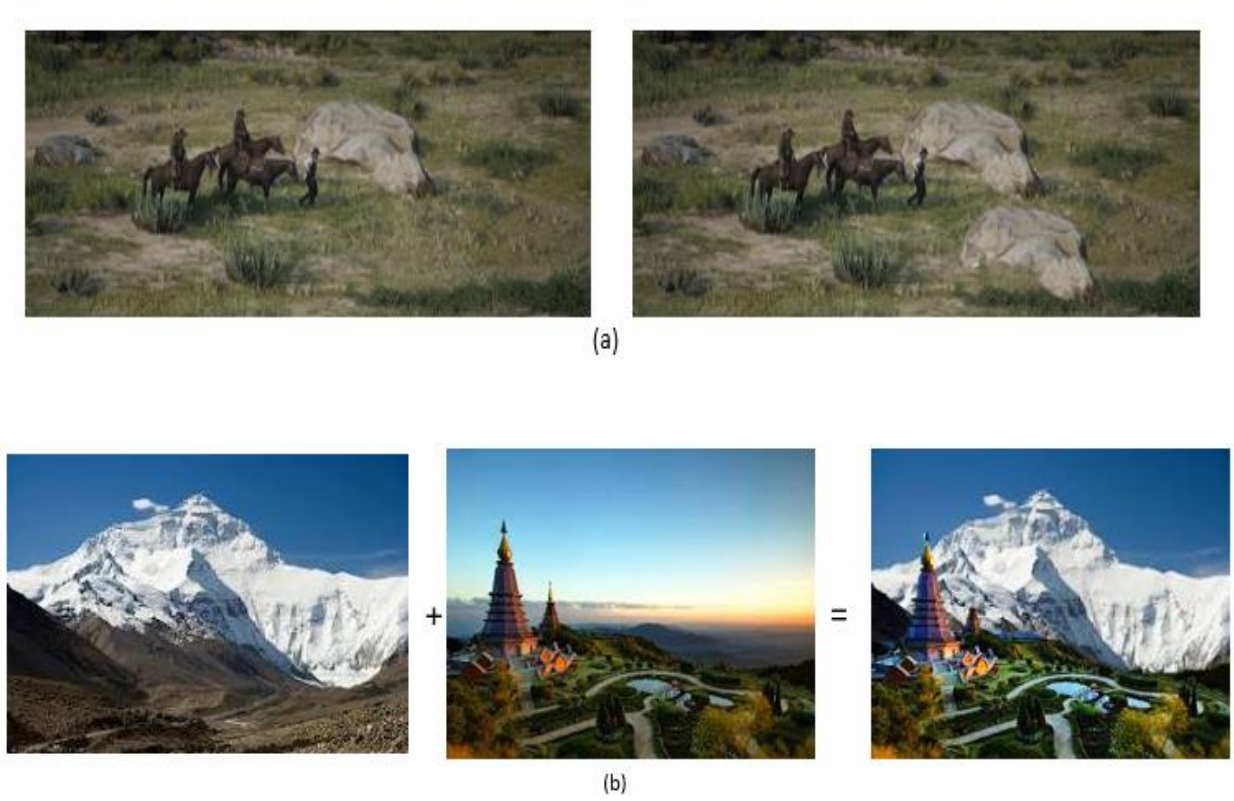

Fig. 6 a: Class-1 type clone-attach image tampering. b: Class-2 type Clone-Make picture imitation

A novel scheme proposed by Lu et al. [14] utilizes the circular domain extent (ECDC) procedure. This strategy combines block-oriented and key point-oriented imitation identification techniques. Firstly, features such as speed-up robust features (SURF) in log-polar space and scale-invariant feature transform (SIFT) are extracted from the entire image. Secondly, a large number of matched pairs are generated using the generalized two nearest neighbors (g2NN) approach. To identify intruded areas, Popescu et al. [15] employed principal components analysis (PCA) as a feature. Yao et al. [16] detect copy-move forgery using non-negative matrix factorization. Non-negative matrix factorization (NMF) coefficients are extracted from a list of all blocks after partitioning the image into fixed-size overlapped blocks. It is worth mentioning that all the coefficients are quantized before matching, which allows for the interpretation of a sub-image with a small amount of data.

Rani et al. [17] proposed one of the techniques named tampering detection with the help of its infrastructure for clone-shift and slicing-based imitations. In this research, the picture information is pre-processed to enrich the touchable data. The suggested method brings out multiple attributes for augmented SURF and corresponding frameworks to

identify forged regions in the image. The approximated main characteristics imply a predetermined boundary price. The evaluation is conducted using the CASIA forged picture dataset. The enhanced SURF approach achieves a limitation identification approximation of 97%, with the compatible frameworks achieving a fraud identification of approximately 100%.

4.1.2 Methods for picture-enhancing tampering identification

This approach finds significant utility in magazines and film photography. While these modifications aim to enhance the image's aesthetics and are not considered forgery, we include them here as they involve alterations or manipulations that affect the image's originality [24]. The image is enhanced to achieve a visually appealing result, and specific parts are modified, such as extracting furrows to create the last shot. Figure 7a displays the enhanced picture, while 7b shows the real picture. These techniques are used for enhancement which commonly are employed and are relatively harmless compared to other forgery methods [25,26]. One significant aspect of image retouching is the removal or reduction of imperfections. Professional editors meticulously work on eliminating blemishes, acne, scars, or any distracting elements that may detract from the subject or desired composition [27].

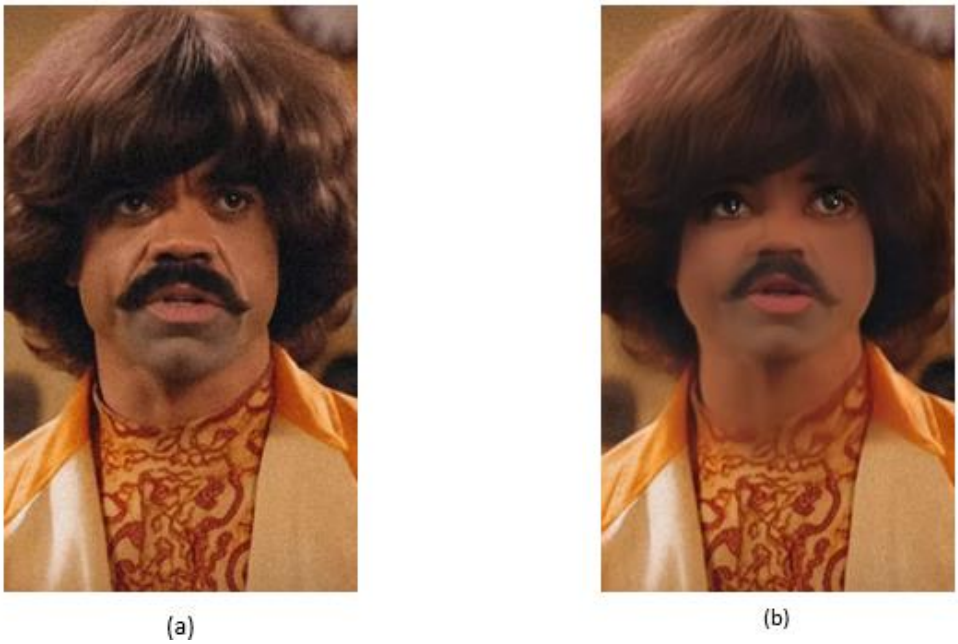

Fig. 7 b is a Retouched image and an original image

Through careful and precise retouching techniques, these flaws are seamlessly eliminated, ensuring the focus remains on the intended subject matter. They involve using professional image enhancement equipment for the accuracy entire photo in its specific portions. Such modifications are widely accepted as standard picture improving practices in mark and online content. Detailed editing tasks, including tonal correction, saturation adjustments, sharpening, or noise reduction, are performed with such precision that these alterations are often imperceptible unless examined with the help of knowledgeable equipment.

Xu et al. [28] introduced another technique based on 8-neighborhood fast comprehensive tasks to enhance the rate and quality of image inpainting. They further introduced a Pyramid model based on downsampling inpainting (PDI) using the ASP principles. Experimental results demonstrated a significant improvement in existing techniques by integrating the PDI model [29]. Additionally, a picture image-restoration method was investigated relying on a self-organizing map (SOM) for recovering important structural data from damaged pictures.

Kumar et al. [30] went through various bits-based and scientific algorithms for fraudulent identification and conducted a comparative analysis of these techniques. Moreover, regardless of the diversity in imaging devices and processing

procedures, they all exhibit the same whereabouts in the picture. Any interference within this pattern introduces deviation from the real picture, enabling the detection of image counterfeiting. This approach offers more accurate forgery detection and works particularly well on uniformly lit surfaces. For more detailed methods, references such as [31,32] can be consulted.

As the field progresses, it is crucial to continue investigating and developing robust methods for detecting and mitigating image retouching forgery. This will not only help in preserving the integrity of visual content but also contribute to building trust and authenticity in digital media.

4.1.3 Methods for photo slicing or mixed-media art tampering identification

Image splicing, also referred to as photo arrangement, basically is a prevalent form of digital picture manipulation that involves copying and pasting regions from similar or different sources [33]. This technique is used to create a composite image by merging multiple images together, resulting in the loss, distortion, or damage of primary information from each source image. Figure 8 illustrates the impact of this process.

Image slicing can be characterized in the following ways: boundary-based slicing and region-based slicing. Forensic methods are employed to identify these techniques used for tampering and to analyze the nature and locations of the deformations offered with these manipulated pictures.

Fan et al. [22] proposed a method that estimates the brightness for the planar and upright bands by mixing these algorithms based on a low-level number. By analyzing inconsistencies in illuminant color within object regions, this approach detects area-slicing forgeries. Kumar et al. [34] introduced a blind forgery detection technique that utilizes regional turbulence discrepancy to identify little areas affected due to regional distortions. The method involves segmenting available pictures into constant distractions based on the homogeneity criterion and analyzing low-cut oblique fluctuation parameters for that which is at the utmost decisiveness. These approaches perform relatively well on pictures with constant distortion stages, which intensively do not exhibit similar characteristics when examined.

Fig. 8 Image splicing forgery

Pine et al. [35] also utilized regional upright distortion for identifying little areas affected due to regional distortion in a blind imitation identification technique. This method takes into consideration non-overlapping blocks and high-pass inclined fluctuating factors for the utmost determination. The image is segmented into identical sub-areas with the help of normal regions using fusion methods based on a homogeneity criterion. Although these approaches demonstrate effectiveness on pictures with static distortion levels, they may encounter limitations if they are applied to images with similar noise patterns.

By continuously exploring innovative forensic techniques, researchers aim to enhance the detection and analysis of image-splicing forgeries. These efforts contribute to the development of robust tools and methodologies for identifying and mitigating the deceptive manipulation of digital images.

4.1.4 Tampering detection of image resampling

Digital picture processing imitation identification is situated on the manipulation of mathematical properties, such as extending, upending, distorting, twisting, and resizing, applied for specific regions to create visually striking forged images. For estimating level plays a vital role in the digital picture process as it puts forward important mathematical

differences. Resampling the image leads to the emergence of distinct periodic correlations that can be effectively utilized [24]. Figure 9 illustrates a digital picture process technique [25].

To enhance the robustness of detection, fusion-based approaches have been proposed. These methods combine multiple features or classifiers from different detection techniques to achieve better performance. Blending techniques, such as feature-level blending, decision-level blending, and score-level blending, aim to leverage the strengths of individual detection methods and improve overall accuracy and reliability.

Wang et al. [18] demonstrated the effectiveness of monitored understanding for a strong and also versatile method for addressing this problem posed by anonymous image mathematics and hidden passcodes. An essential aspect of understanding the process which involves selecting informative features with low-dimensional representation. Liu et al. [26] explored the bond of neighboring Discrete Cosine Transform (DCT) parameters and proposed a technique to identify modified JPEG pictures including sliced pictures, those employed for picture duplication. Detailed extraction of adjacently attached saturation characteristics from the DCT parameters enables the detection process, which utilizes Support Vector Machines (SVM) [Tables 2, 3,4, 5, and 6].

Fig 9. Resampled Images: one portion for a real picture and another portion for the dragon with a purple border is resampled and indicated by a red border

Through ongoing research, the development of advanced techniques and algorithms in image resampling forgery detection continues to progress. This research aims to forecast these detection capabilities to improve their precision for identifying forged pictures created through geometric modifications and resampling operations.

Table 2. Picture size techniques used for image point transformation

Sr.no	Type of Forgery Detection Area	Researchers	Year	Approach	Dataset	Accuracy (%)
1	Picture imitation adaption by mixing recorder, application, and image sample-dependent methods	Cozzolino et al.	2014	Localization, PRNU	Ad-hoc	FM =0.1620

2	Dependent on cloning imagery identification including enhanced identification precision	Dixit et al.	2016	DyWT	USC SIPI Photo Repository, CVG UGR Photo Repository	99.7304%
3	Cloning imitation identification dependent on curiosity tip and geographical analysis method	Mei et al.	2019	SIFT	Benchmark Dataset	91.32%
4	Cloning imitation identification in social pictures	Kang et al.	2010	Singular value decomposition, LBP	Casia V2 a UCID	92%
5	Rapid imitation identification with inherent sampling rate attributes	Lien et al.	2010	Resampling Intake Asset	Ad Hoc	97.5%
6	Cloning imitation identification in social picture with affine-sift	Shahroudnejad et al.	2016	Affine-SIFT	CASIA TIDE v2.0 dataset	77%
7.	Cloning imitation identification dependent on the main grouping and proximity search method	Chen et al.	2020	Main Grouping and proximity search method	GRIP and FAU dataset	95%

8.	Validation for in-demand cloning imitation identification strategy	Christlein et al.	2012	DCT, PCA, KPCA, Zernike and DWT	Benchmark Database	90%
9.	Efficient hierarchical aspects for picture splicing identification	Ahmed et al.	2021	CNN, AlexNet	CASIA v1.0	98.79 %
10.	A novel algorithm of image splicing detection	Kaizhen et al.	2012	SVM	Columbia Picture Splicing Identification Analyzing Information	86.70%
11.	Picture splicing regionalization with image patch division along with distortion stage evaluation	Li et al.	2019	SLIC algorithm	Columbia University image database DVMM	98.28%
12.	Image splice detection through noise pattern analysis	Mahawatta et al.	2018	2D DWT	Columbia Uncompressed Image Splicing Detection Dataset and CASIA dataset	81%

13.	An integrated method for splicing and cloning imitation picture identification	Lin at el.	2011	DCT and SURF	ISCAS images database	90%
14.	Picture splicing change identification dependent on neural network and application system	Wang et al.	2021	CNN	CASIA1.0 and CASIA2.0 data sets	99.60%
15.	Picture splicing identification using saturation boundary discrepancy	Fang et al.	2010	Photometric quasi-invariants	Columbia Picture Splicing Identification AnalysisDatase	84%
16.	A technique for Cloning and Picture Splicing Imitation Identification using Advanced Neural Network	Hingrajiya et al.	2023	DenseNet-201	CASIA v1.0, CASIA V2.0 , and CoMoFoD v2.0	94.12%
17.	Picture processing identification dependent on filtering in deep learning	Liang et al.	2019	CNN	Dresden image database and Uncompressed Color Image Database (UCID)	98%

18.	Pre-processing imitation identification in jpeg-condensed pictures	Li et al.	2010	FFT	Columbia University Graphics Lab Database	97%
19.	Cloning and picture splicing imitation identification dependent on filtering in deep learning	Nikalje et al.	2022	CNN, LBP and SVM	CASIA v1.0 and CASIA v2.0	99.1%

Table 3. Analysis of JPEG compression tampering techniques

Type of Forgery Detection Area	Researchers	Year	Approach	Dataset	Accuracy
Point out unauthorized pictures in various picture themes	Zhang Y, Goh J, Win LL, Thing VL	2016	Stacked Autoencoder model (SAE)	CASIA	91.09%
MPEG Dual Condensing dependent on Intra-picture Film imitation identification with CNN	Bakas et al., Kumar et el., Naskar et al.	2018	CNN	Trace yuv video sequences dataset	90%,
Analysis of misinterpretation for unscathed picture condensing depending on imitation identification	Sri CG, Bano S, Deepika T, Kola N, Pranathi YL	2021	CNN	MICC-F2000, CASIA v2	99%
Regionalization of JPEG dual condensing with cross-domain CNN	Amerini I, Uricchio T, Ballan L, Caldelli R	2017	Two-branch CNN Model	UCID	99.60%
Dual JPEG Condensing Identification dependent on Distortion less DCT Factor Aggregation Frequency Distribution diagram	Zhou, P, Han, X, Morariu, VI, Davis, LS	2019	Two-branch R-CNN Network; ResNet 101 network	NIST Nimble 2016 (NIST16), CASIA, COVER, Columbia	78%

Table 4. Analysis of camera source identification techniques

Type of Forgery Detection Area	Researchers	Year	Approach	Dataset	Performance
Blind origin recorded detection	Mehdi Kharrazi ', Husrev T Sencur ', Nasir Memon '	2004	Multi-class SVM	ADHOC	88.02%
Recorder Picture Imitation Identification	Hagit Hel-Or and Ido Yerushalmy	2015	PFA	Lens and sensor aberration dataset	72%
Camera Model Fingerprint Detection	Cozzolino, D, Verdoliva, L	2019	Siamese	Ad-hoc dataset	100%
Parameter picking in Origin Recorder Detection	Kai San Choi, Edmund Y Lam, and Kenneth K. Y. Wong	2006	SVM	ADHOC	96.67%
PRNU-based Origin Recorder Detection for mixed media science	Eitan Plot', Ramazan Aygunt, Suat Mercan*, Kemal Akkaya*	2021	PRNU noise patterns with Jaccard similarity algorithm	Camera dataset (apple iphone, Panasonic DMCFZ1000, and Sony ILCE)	98%
Origin recorder detection dependent on CFA estimation	Sevinc Bayram a, Husrev T. Sencarb , Nasir Memon b,IsmailAvcibasa	2005	EM algorithm, SVM classifier	AD-HOC	83.33%
Source Camera Using Sensor Fingerprints	Lekshmi K, Vaithiyanathan V	2018	Wavelet Transform, SVM classifier	AD-HOC	85%

Table 5. Analysis of mathematical tampering detection

Type of Forgery Detection Area	Researchers	Year	Approach	Dataset	Performance
Synthetic Media Identification for Facial pictures and footage	Asad Malik, Minoru Kuribayashi, Sani M. Abdullah And Ahmad Neyaz Khan	2022	DNN-based methods for Deep Fakes	AD-HOC, Synthetic Media-in-the-Wild footage information set, and VGGFace2 dataset respectively for each type of approach	98%

Identification of artisanal face pictures influence as well as GAN-made face pictures.	Lee S, Tariq S, Shin Y, Woo SS	2021	Background Architecture: ResNet18 SFFNV3 (SuperficialUnreal Facial Net), CNN	Handcrafted Facial Manipulation (HFM) dataset	73%
Inherent Detector Distortion Parameters for Scientific Experimentations	Hongmei Gou, Member, Ashwin Swaminathan and Min Wu	2009	Picture noise reduction, oscillation transform, and environment identification	AD-HOC	97%
Identification for GAN-made Forged Pictures over Social team	Marra F, Gragnaniello D, Cozzolino D, Verdoliva L	2018	Neural network	AD-HOC	96%
Mechanized origin recorder detection with inherent optic spoked-noise	Kai San Choi, Edmund Y. Lam, and Kenneth K. Y. Wong	2006	SVM classifier	AD-HOC	80.8%
Digital face manipulation	Hashmi MF, Anand V, Keskar A	2020	XceptionNet, VGG16	AD-HOC	99%

Table 6. Analysis of illumination-based tampering techniques

Type of Forgery Detection Area	**Researchers**	**Year**	**Approach**	**Dataset**	**Advantage**	**Drawbacks**
3D Lighting-based picture imitation identification	Wei Fana , Kai Wanga , Francois Cayrea , and Zhang Xiong	2012	Shape-from shading (SFS)	Lightning probe images captured in different conditions	Improves the lighting-based forensic potential	Has poor accuracy in estimating the 3D shape of the object
Manufacturing Item Identification using Physics-Based Visualization	Eversberg L, Lambrecht J	2021	RCNN with 5000 in-process pictures	PASCAL, COCO	Creates more realistic representations using physics-based visualization	Not effective for different manufacturing items
Detecting Picture Imitation Illuminating Factors	Manoj Kumar1 and Sangeet Srivastava2	2016	Light source estimation using 3D shape	Experimental dataset	Uses 3D shape information for light source estimation	No details regarding the lighting factors
Slope Light Information for Picture Imitation Identification	Falko Matern, Christian Riess	2020	Robust physics-based lighting	ALOI object dataset, COCO dataset.	Use lighting inconsistency to detect image forgery	The generalizability of the model is low
Picture science for chromatic lighting,	Thakur A, Jindal N	2018	Crossbreed DWT, chromatic	ImageNet and COCO	Models robustness is tested using	The image manipulation detection part

stop and main point method			lightning technique, SLIC technique; SIFT technique, Association Indicator Chart period technique, Obstruct Pairing Entrance technique Application Removal Technique		two large datasets	was not clearly illustrated
Revealing Social Imitations by Identifying Discrepancy in Illumination	Micah K. Johnson, Hany Farid	2005	Lighting direction estimation and color analysis	AD-HOC	Analyzes lighting inconsistencies for detecting social image forgeries	Does not handle diverse image manipulations
Difference in improvement Identification dependent on CNN	Deng H, Qiu Y	2019	VGG-CNN	Picture Handling Information set 1, COCO Information set	Increased accuracy in identifying image manipulations	The computational cost of physics-based visualization is not provided

4.2 Tampering detection- compression-based

It might be difficult to spot forgeries since fabricated images frequently undergo modification for compression and other factors. Forgeries are challenging to detect due to JPEG picture shrinking. JPEG's full form is the Joint Photographic Experts Group. To detect manipulation, forensics analysis leverages some JPEG compression features [36]. These techniques include ways based on JPEG discretization, dual JPEG shrinking, and numerous JPEG shrinking, also accompanied by JPEG obstructing. In some compression methods, statistical correlation is introduced, which is useful for identifying phony images. A quantization matrix is used in the literature [37] to identify double JPEG compression.

On the basis of the given assumption, the block-wise DCT will behave as an integer periodic function when applied in accordance with the principal JPEG compression grid. A strategy for identifying double JPEG compression that is not aligned was identified in [38]. Kee et al. [39] created a concealed message identification measure dependent on normal function for modeling pictures. The ratio of two Fourier parameters which spread across the DCT factors is then measured afterwards where the spread of DCT parameters is modelled using a normal function model. The LSB (Least Significant Bit), SSIS(Spread Spectrum Image Steganography), and the graph-theoretic Steg-Hide tool are three stenographic techniques that are compared to this derived steganalysis measure. Datasets of visual features are classified using various classification techniques, such as SVM.

4.2.1 JPEG discretization technique

This provided picture is in the JPEG (Joint Photographic Expert Group) format, which is a widely recommended technique for photo shrinking. JPEG changes the original picture into an RGB representation, which preserves the colour and brightness details. Red, green, and blue make up these three channels that form the RGB colour system. Each channel is represented by a range of low to high integer values. Each color channel's intensity is determined by

these numbers. The Discrete Cosine Transformation (DCT), transforms the picture into an occurrence region depiction, which is used in the JPEG shrinking process. Using a specified quantization table to scale down the coefficients and divide the image into blocks, the DCT quantization phase further decreases the amount of information [40]. This quantization procedure aids in compression and file size reduction. The final compressed image data in the JPEG standard is calculated using a quantization matrix of 64 values, which is then multiplied by the DCT coefficients. The intended level of compression and visual quality of the final image are often taken into consideration when choosing the quantization parameters.

4.2.2 Dual JPEG discretization and JPEG hindering technique

Pictures are often put into a software application when being worked on, where they are then altered and saved. The most necessary thing is the broad usage of JPEG encoding for photo storage suggests that this format is primarily used for real images. In contrast to photos compressed in a single pass, unique patterns appear when JPEG images are encoded in a lossy manner. The JPEG shrinking method is evaluated with the discrete cosine transform (DCT) [41]. This picture is then separated into 8x8-pixel blocks in this procedure, and each block is separately quantized and transformed. At the margins of adjacent blocks, these blocks display observable patterns in equidistant and perpendicular corners. Its abstaining patterns can alter the manipulated photos, creating questions.

4.2.3 Camera-based tampering detection

A shot taken with a digital camera goes through several processing steps before being stored in memory. Discretization, chroma interconnection, gamma amendment, snowy balance, purifying, and JPEG shrinking are some of its processes, however, the precise ones depend on the type and features of the camera. These techniques include a variety of strategies, including chromatic aberration correction, color filter arrays (CFA), camera response calibration, and sensor noise reduction, and they comply with accepted standards. If there is a widespread difference in intensity, lighting flaws in pixels could become apparent in darker or lighter places. These problems are caused in part by pixel flaws brought on by temperature fluctuations and the lens bending of light at various wavelengths [42].

Such pixel errors can be reduced using post-processing techniques such as picture enhancement, contrast correction, compression, and blurring. Many manufacturers use a single sensor to capture natural color scenes in order to reduce the cost of sensors. Color filter arrays are used to limit the wavelength range that can reach the CCD array. To recreate full-resolution color images from CFAs, various approaches have been put forth [43]. In its field of picture science, it has a variety of methods that are used for enriching pictures captured through standard recorders by making use of artifacts in camera systems. With firms like Leica, Sony, Fujifilm, Pentax, Panasonic, Canon, and Nikon adding CCD arrays sensitive to particular wavelength ranges, traditional cameras are gradually being supplanted by affordable alternatives.

4.2.4 Colorful Anomaly

Colorful Anomaly is due to a visionary framework's inability to concentrate the light of various frequencies accurately, which causes color fringing or blurring. As a first-order estimation, lateral chromatic anomaly frequently is noticed. It denotes the expansion or contraction of color channels relative to one another. However, when an image is altered, this aberration frequently varies over the entire image. A drawback of employing chromatic aberration as a forensic technique is that it depends on a sizeable section of the image being legitimate to get a trustworthy overall evaluation. The total estimation may be off if a significant piece of the image is altered, which could result in erroneous inferences [44].

4.2.5 Color Filter Array

The three channels that make up a digital color image each contain samples from a different color band, such as red, green, or blue. A single charge-coupled device (CCD) or two correlated CCDs with metal-oxide-semiconductor (CMOS) color sensors are two configurations that are used by the majority of digital cameras. To take pictures, these sensors use a color filter array (CFA). The most prevalent CFA is the Bayer array, which has three color filters: red, blue, and green. By allocating various filters to various pixels in this widely used array configuration, the camera can capture and separate color information, enabling the reconstruction of a full-color image.

4.2.6 Source camera abbreviation

Applications for forensics include identifying cameras, detecting image tampering, and figuring out how old a digital photo is. Similar to human fingerprints or skin blemishes, digital imaging sensor flaws can serve as distinctive identifiers. The primary areas of interest for forensic analysts include numerous weaknesses in production, internal camera procedures, and environmental conditions. These flaws offer insightful information that can extract the approximate period for a computerized picture, identify fraudulent image alteration, and link photographs to particular cameras [45].

4.2.7 Sensor imperfection

Digital imaging forensic applications cover great areas of activities, including camera identification, picture tamper detection along age estimation. Due to these goals, it is possible to take advantage of the distinguishing qualities of digital imaging sensors, similar to a person's fingerprints or skin imperfections. The focus of forensic analysts is on numerous flaws, which might be from external influences, internal camera operations, or manufacturing flaws. These flaws act as distinctive identifiers and provide insightful data for forensic investigations [46].

4.3 Physics-based tampering detection

In the splicing processes, the forged zone's lighting may differ from the original in natural images, which are typically captured under diverse lighting situations. Physics-based approaches leverage variations in light sources among detailed equipment in the background for unveiling evidence of altering. During the modification stage, images are blended while being captured under various lighting conditions. Matching the thinking while utilizing the pictures can pose challenges. Its lightning disparity resulting from blending the photos could be employed to indicate the forged regions in image counterfeiting. A solution to these challenges was proposed by Johnson et al. [47]. This method was devised by them to evaluate the portion of a lighting source in the first degree of freedom, aiming to showcase the interference. Wu et al. [48] introduced a technique that can be applied to photographs featuring any item at the back, without being limited to male faces or picture picking based on identical fierce areas. This method takes into consideration the changed items for determining the angle of incidence concerning the direction of the light source concerning the factors. When tested over an information set comprising diverse types of changed pictures, its result achieved an imitation identification evaluation of about 92%.

4.3.1 Illumination Setting

The scientific picture identification technique has been developed to detect lighting aberrations in difficult serene lighting. These objects when sliced across different pictures, ensuring consistent illumination becomes challenging, and studies have shown that such discrepancies are hard to detect visually [49]. Further discussion on lighting-based forensics reveals that it can be categorized into three types: simple directional lighting, 2D complex lighting, and 3D complex lighting, with a more detailed exploration of light direction in both 2D and 3D contexts. The latter techniques operate initially by reconstructing its illumination setting using a set of round resonance factors. Subsequently, estimated parameters of various regions of the image are compared to identify any disparities [50]. In complex lighting situations, where a multitude of lights can be placed arbitrarily, resulting in sophisticated lighting scenarios, Nirmalkar et al. [33] explain estimating a minimal depiction for these intricate brightness criteria. Kumar et al. [34] propose this technique for identifying picture alterations by employing a comprehensive lighting-based analysis. This approach proves effective in detecting counterfeits in photographs captured under one or more light sources. The method involves calculating elevation angles concerning certain items with different light mediums there in the background. By utilizing bits through specific locations, its approach identifies light mediums with their corresponding altitude angles. Thus, the conclusion in the suggested method correlates with evaluating its strength in identifying interference caused due to artificial photos, when considering information that is precalculated.

4.3.2 Illumination Angle (2D)

The focus of the approach is to identify the direction coming from the light source in a two-dimensional space, also known as "Light Zone" (LZ). The LZ estimation is calculated with the outline region for the present photo, utilizing outlining fragmentation techniques that rely on both the firstly calculated outline region and the current estimation of the Light Zone [51]. The specific area within an image where the location of the light direction is evaluated is called a Light Zone. Its determination is evaluated based on the calculation of the outlined region along with its correlation with the evaluated Light Zone. The understanding of the distribution and impact of lighting in the image is facilitated

by the concept of the Light Zone, which is crucial for various image analysis tasks, such as relighting or the detection of lighting anomalies. An image manipulation detection method is presented by Stojkovic et al. [36], which utilizes blind identification techniques to estimate the normal matrix of the image plane. The accuracy of forgery detection using this method it was evaluated at 87.33%. Another proposed technique presented by Kumar et al. [37], picture forgery is detected after finishing inconsistencies in the light origin orientation. During the preprocessing step, a surface texture profile is generated using the RED band for collecting consistent data for calculating normal surface. The incidence angle (θi) is then evaluated keeping in mind different photo spots based on the calculated lighting dossier. An inconsistency in θi values serves as evidence of tampering and has proven effective in identifying manipulated objects within a picture.

4.3.3 Illumination Angle (3D)

The topmost contemplation prototype of the picture applies bulge along with steady reflecting power as the main factors, which serves as the basis of this method. A major consideration is given to closure mathematics with the topmost consistent data in detecting forgery, particularly face forgery. Spherical harmonics are a set of functions used to represent the distribution of light in a scene or on a surface. The estimation of 3D lighting SH parameters involves determining the coefficients that best approximate the lighting conditions in a three-dimensional space. These coefficients capture the intensity and direction of the incident light and are useful for various lighting-related calculations and analyses. The estimation of 3D lighting SH (spherical harmonics) parameters is accomplished by recreating a 3D portrait example using several facial pictures utilizing 3D sufficient data [38]. A normal example for examining the 3D lighting environment is described by Kee et al. [39], wherein model parameters are evaluated based on a single image. Light-related forensics are the focus of Fan et al.'s work [40], demonstrating a rival method in science for a misguided imitation identification situated on 2D lighting parameters. However, for further difficult 3D lighting parameters, this information path supports the application of intermediate results, necessitating a ballpark figure for conjecture items over a 3D platform. The cutting-edge imitation identification application developed with lighting thumbmarks based on computerized pictures is proposed by Kumar et al. [41]. Any alterations in the picture result in real thumbmarks that are used for verifying its integrity. This method gives a chance to various methods for identifying its strength along with architectural data, utilizing the Laplacian technique for fetching different applications within a picture, along with extraordinary computation. By applying the Laplacian operator, areas of rapid intensity change or sharp transitions in the image can be highlighted. Based on the illumination factors and the recognition of distinct fingerprints, this method serves as very useful equipment for computerized picture imitation identification.

4.4 Mathematical tampering detection

Imitation identification systems that utilize perspective views make use of geometric constraints. This method is broadly categorized in inherent recorder factors (focal length, central idea, proportion, and tilt), tilt dimension-oriented also with numerous mathematic-oriented methods [51]. For such cases of original pictures, the image’s key focus is situated at the center of the picture. However, maintaining the correct perspective of the image's main point becomes challenging when a small portion of the picture is shifted or changed (e.g., copy-move) or when two or more pictures are bought together (e.g., slicing) [52]. A review by Johnson et al. [44] recommends various representational mathematical equipment, taking into consideration a technique to correct horizontal areas with its capability for performing in its actual form. One technique involves the usage of figures such as polygons, while another technique is rooted in from idea of fading marks, which can be situated on any surface. Each technique calculates a world-to-image change, which is utilized for removing the surface noise and performing calculations.

4.4.1 Recorder Inherent parameters

The inherent parameters of a recorder, including scale parameter, focal length, lens noise, tilt, and leading agenda, allow mapping of the recorder points to bits points. The charting, which is a 3D to 2D charting, is dependent on multiple independent parameters [53]. The process of mapping recorder points to bits points is known as 3D to 2D charting. It involves determining how the three-dimensional world captured by the camera is projected onto a two-dimensional image. Consistency in the internal parameters across a non-tampered image is expected, and the changes among these factors for the picture are utilized for detecting interference [54]. In their review, Ng et al. [47] recommended various mathematical equipment, along with a technique for correcting the horizontal areas with the

capability for performing real-world calculations on horizontal areas. One technique involves the utilization of figures by drawing polygons by identifying and analyzing the shapes of polygons within the image, geometric distortions can be corrected, aiding in the detection of tampering, while another technique is rooted in the concept of fading areas, that are locations where parallel lines appear in the three-dimensional world to converge in a two-dimensional picture. By identifying some vanishing points on a plane, the world-to-image change can be estimated. This transformation allows for the removal of planar distortions and enables accurate measurements. Each approach involves estimating the world-to-image change, that is used for diminishing horizontal noise while calculating dimensions.

4.4.2 Standard Dimensions

Standard dimensions are obtained from horizontal areas after rectifying the picture. When using perspective projection, there are three techniques for correcting horizontal areas, each utilizing a single image. The first technique involves the usage of known-shape polygons, the second technique relies on some fading spots, and the third method attains the presence of some circles lying on the same plane. These methods enable the recovery of a picture of world change, permitting standard dimensions to be captured on the plane itself. Even if the region of interest lies outside the reference plane, metric measurements aid in its detection [55].

Among the global alignment framework, the marks on the plane are denoted as X and are projected onto the image plane which is then represented as coordinates x. This projection is described by the equation x = HX, where x and X are uniform 3-vectors in the allocated reference frameworks. For resolving the imaginative evaluation array H, four points with similar points X and x are required. The estimation of H is determined up to an unknown scale factor[56], which must be determined using a single image and a known length on the world plane[57]. By warping the image according to H−1 with a known H, a rectified image is generated, facilitating the taking of measurements. Koppanati et al. [58] provide a review and recommendation of various projective geometry tools, including a method for rectifying planar surfaces and the capability to perform real-world measurements from a planar surface. The first method employs polygons with well-defined shapes, while the second method is based on the concept of vanishing points, which can exist as one or two points on a plane. In each approach, the world-to-image transformation is estimated, enabling the removal of planar distortions and the acquisition of measurements.

4.4.3 Varied Mathematical Modelling

A method for detecting composite images is defined through the application of prospective mathematical limitations, namely H limitation also with F limitation, to pairs of images. The H constraint becomes apparent when a camera undergoes rotation, resulting in a relationship between equivalent units ×1, ×2 for two flat surfaces, as expressed in the equation x2 = K[R | 0]X = KRK^−1x1. On the other hand, the F limitation arises when the recorder faces universal movement, also the units involved are on different planes. To establish a connection between such points, a Fundamental Matrix, denoted as F, is employed. This matrix allows for linking a point x1 from a picture to a stroke named l1 on another image and is denoted by the equation x2^Tl1 = x2^TFx1, where the correspondence between x2 and x1 is established [59].

5 Deep learning-based image tampering models and issues

Aberna et al.[61] presented an optimal semi-blind watermarking technique to extract crucial features from the image. The tampering region is detected using the swin transformer model which is also used for watermark generation and embedding in the suboptimal blocks.Lin et al.[62] presented a Network to learn and Enhance multiple tampering traces (EMT-NET) technique to extract local and global noise features. The local and global noise are extracted using a transformer-based noise encoding branch and fused using a CNN-based RGB encoding branch. Yan and Li [63] designed a hybrid transformer architecture named TransU2Net to identify image splicing tampering. This model captures both long-range semantic details and low-level non-semantic features.

Sun Y et al.[64] improved the accuracy of tampered region localization using edge-enhanced transform (ET). A two-branch edge-aware transformer is identified to capture rich tampering traces. Lee et al.[65] developed a Shallow Fake Face Net (SSFN) model to detect GAN-generated facial images. This model detects facial forgeries on social networking sites in real time. GAN is a powerful tool for image tampering detection since it is capable of generating realistic images by recognizing patterns. The discriminator in GAN differentiates between the actual and tampered

images. It extracts the subtle differences that exist between the actual and tampered images. The generator network in GAN is used to generate real or fake images based on the input. It is capable of recognizing the patterns and anomalies associated with tampering.

As per the name, the generator generates realistic tampered images whereas the discriminator classifies the tampered images with high accuracy. The GAN is mainly trained in an adversarial manner to provide more realistic results. The GAN identifies the tampering regions by generating saliency maps that highlight the tampering region. GAN can be also applied to unsupervised anomaly detection by training the discriminator on a massive dataset. The advantages of GAN for image tampering is high accuracy, robustness, scalability, and real-time tampering detection. Sushir et al.[66] presented a hybrid deep convolutional capsule autoencoder (Hybrid DCCAE) framework for improved blind image forgery detection. The improved horse herd optimization algorithm is used for dimensionality reduction and similar pixel regions are differentiated using adaptive density-based fuzzy clustering. The summary of these techniques is presented in Table 7.

Table 7: Deep learning-based image tampering methods

References	Technique used	Purpose	Dataset	Advantage	Drawback
[61]	Swin transformer model, optimal semi-blind watermarking technique, and Singular Value Decomposition (SVD)	The content authenticity is evaluated by the semi-blind watermarking technique by comparing the regenerated actual watermark with the recovered scrambled watermark	LVZ-TMO dataset and CASIA dataset	PSNR value of 65 dB and SSIM of 0.999	Struggles to process high dynamic range videos
[62]	Transformer-based noise encoding branch and CNN	Identifies homologous and heterologous tampering traces	CASIA, NIST, Columbia, COVER, CoMoFo, and DEFACTO	Identifies different traces such as global noise correlations and local noise inconsistencies.	Does not focus on unintentional attacks
[63]	TransU2Net	The hybrid transformer architecture extracts both spatial and contextual information	Casia 2.0 and Columbia datasets	Can be applied to detect complex image forgeries	Not suitable for cross-dataset training
[64]	Edge-enhanced Transformer (ET)	To improve the tampered region localization accuracy	CASIA v1.0, CASIA v2.0 and NC2016	Identifies rich tampering traces	The contextual information present in the image is not analyzed
[65]	SSFN	Minimize facial forgeries in online social networks	Handcrafted facial manipulation dataset	Area Under the Receiver Operating Characteristic (AUROC) of 72.52%	Generalization issues
[66]	Hybrid DCCAE	Detects blind image forgeries with higher accuracies.	CASIA VI, Coverage, and GRIP datasets	Accuracy of 99.23%, 98.75%, and	Sensitivity to noise

				98.07% in CASIA VI, Coverage, and GRIP datasets	

5.1 Issues

5.1.1 Absence of ideal Prototype of picture tampering

Complex algorithms and ineffective classifiers cause problems for many picture forgery detection models, leading to subpar or flawed performance. These models have additional difficulties due to the dataset's selection or its absence. Defective image forgery detection models thus frequently experience higher time consumption and excessive expenses. Furthermore, methods used for neural network picture imitation identification show notable heterogeneity in connection with data preparation, mentoring, and assessment stages for human decision-making.

5.1.2 Absence of the ideal Prototype of mechanized image Tampering Anticipation

The efficiency of image forgery detection still strongly depends on classifiers in modern times. These classifiers frequently perform poorly when asked to find intricate forgeries like Deep Fakes. Additionally, the choice of the commencement manner and the identification site element (picture element or area) may conflict at the analysis stage. It isn't easy to achieve optimum automation at this stage. Professional participation is nearly always necessary to guarantee accurate detection and analysis of image forgeries.

5.1.3 Absence of the ideal prototype of neural network-oriented equipment

Only a few applications, like machine recognition and content manipulation identification, show that deep learning-based image tampering detection algorithms function effectively. It should be mentioned, nonetheless, that the choice and use of the information set have great consequences over the experimental outcomes of the strategies. Deep learning algorithms for image tampering detection rely on well-curated datasets covering many of the forgery types and variants to function successfully and accurately. As a result, the proper selection and application of datasets during the training and evaluation processes play a crucial role in the efficacy and dependability of these methods.

5.1.4 Lack of Cost-effectiveness

Because of discriminators, and sophisticated techniques with various requirements, many methods associated with the study of image forensics are not cost-effective. The accessibility and caliber of the dataset utilized for model building and training are equally important. In picture forensics, various dataset types are used to support studies. These comprise genuine data sets like the UCID dataset, RAISE dataset, and Vision Dataset as well as altered data sets like the CASIA V1, CASIA V2, and MICC-F220 information. As it provides the necessary samples for training, testing, and evaluating the algorithms and methodologies used in the field, choosing an adequate dataset is crucial for ensuring image forensic models' accurate and dependable performance.

6 PROTOTYPES FOR NETWORK TAMPERING IDENTIFICATION METHODS

Currently, the dominating, challenging, and prototype identification methods required for various fields of forensic sciences are defined here. A simple prototype reducing core duplication for CNN was stated by Joudar et al. [50]. It is suggested by Junior et al. [51] that a particle swarm optimization-based algorithm could be employed to search for the most effective convolutional neural networks.

6.1 Synthetic Media

In addition to the traditional techniques listed before, many more complex picture imitations have been carried out recently. An emerging Artificial Intelligence technique known as Synthetic Media utilizes certain information such as facial features, their forms, contours, etc, which are guided by deep learning methods that are competent for area/facial identification including precise modifications [52].In a scenario where a computer-generated face, often bearing a striking resemblance successfully alters the face of an individual [53,54].

6.2 Data obfuscation

Data obfuscation, or counter-forensics, refers to the techniques employed for discontinuing scientific experiments. In response to limitations observed in neural networks picture imitation methods, where Convoluted Neural Network (CNN) which stands as an example for image processing proves to be weak against adversarial attacks. Hence, different smart techniques have been developed that can evade detection by neural network systems. Some of them are Jacobian-based Saliency Map Attack (JSMA), Fast Gradient Sign Method (FGSM), and deep sparse rectifier neural network [55].

6.3 Picture origin

Picture origin area, also known as location forensic approaches, refers to the techniques and methods used for identifying its the origin or origin of a picture. The field of exploration focuses on extracting and analyzing various types of digital information embedded within images to gain insights into where the image was captured or created.

Camera artifact source location is a technique used for detecting the origin of a picture by analyzing specific artifacts or characteristics developed by to recorder during the picture capture stage. These relics are already in-built in the recorder hardware and software which provides valuable information about the recorder utilized for capturing the picture. Aberration quantity differs based on the recorder specifications, lens characteristics, and color filter. Last, what cannot be examined in a digital image frame through analysis is determining the location of the camera. An image source location approach based on lens aberration analysis was implemented by San Choi et al. [56], where Devernay's line extraction method was utilized. Various authors employed a Support Vector Machine (SVM) [42] as a model training scheme to analyze chromatic aberration as a fingerprint for identifying the correct image source.

The Image Forensic Experts utilize three key sensor defects to locate the picture's origin. The defects include fixed pattern noise (FPN), Photo Response Non-Uniformity (PRNU), and pixel defects[57]. FPN refers to a consistent and repeatable pattern of noise that appears in images captured by digital cameras. It happens because of the imperfections in the recorder’s sensor including other components, resulting in variations in pixel values across the image. FPN can be utilized as a unique identifier to identify specific recorder sources of pictures. PRNU is a characteristic inherent to individual camera sensors. It represents the slight variations in the sensitivity of pixels across the sensor, resulting in non-uniformity in the captured image. Pixel defects are abnormalities or flaws in individual pixels on a camera sensor. These defects can manifest as stuck pixels (always on or off) or hot pixels (excessively bright). A comparative study was conducted on pattern noise exhibited through FPN and PRNU to identify the correct image source [58,59]. Koppanati [56] emphasizes a novel encryption model for multimedia data on the cloud, employing the use of the RGB channels and the Logistic Map and Linear Feedback Shift Register (LFSR) for data encryption. A Pre-Encryption and detection method aimed at detecting crypto-ransomware attacks at the pre-encryption level (PEI) was also presented.

The identification of actual Image Sources is eased by programming and completing inherent applications in commonly used real-time holding tools. In line with this principle, the camera can be positioned by using dimension rectification and tincture treatment before saving the fingerprints. The model employed SVM as a training scheme. In the context of maintaining security during transmission and storage, a ciphertext method named V $\oplus$ SEE is used which requires less bandwidth and CPU compared to AES and DES.

7. DISCUSSION

The difficulty of confirming the authenticity of digital content has been made more difficult by the proliferation of fast availability of the World Wide Web (WWW) and the accessibility of unrestricted, powerful image modification software. Finding the source of digital content has been harder as social networking platforms have proliferated. To establish the reliability of digital resources, it has become essential to trace their development and flow across time. It is difficult to identify alterations and forgeries made in modified digital assets (to improve information clarity). Hence one of the main challenges encountered in the studies is to identify the minor alterations made in the media.

The widespread transmission of content via various social media sites on the internet, the availability of community-developed applications, and the emergence of new digital acquisition methods, processing techniques, and easily accessible tools have played a role in identifying the serious and urgent issue of social imitations. As an evolving area,

digital forensics peeps to identify sources of digital media and evaluate its reliability. The existing techniques often fail to identify different types of attacks such as JPEG compression, illumination variation, scale and rotation, and blurring. The changes in lightning, lossy compression, blurred images, and variations in scale and rotation make it hard to identify manipulated traces.

As counterfeiting can have serious consequences, it is crucial to assess the veracity of images or films, with substantial ramifications on both a national and international level. Digital forensics uses a variety of methodologies, such as active, passive, and deep learning-based methods like Generative Adversarial Networks (GANs) to modify the content. Researchers in this field are increasingly concentrating on tackling more general issues and looking for comprehensive strategies and solutions. Establishing new frameworks that may successfully limit the dangers associated with digital forgeries requires the development of generalized procedures, standardized datasets, benchmarks, and evaluation criteria.

The increasing usage of digital forensics raises the need for complete solutions to tackle digital forgery. To ensure the field's growth and strengthen its capacity to counter the evolving threat of digital manipulation and forgeries, efforts must be made to establish standardized practices, shared resources, and evaluation standards. The field of digital forensics can significantly enhance the protection of the integrity and authenticity of digital resources in the interconnected world of today by encouraging collaboration and regulating methodologies [60]. Deep Neural networks have various shortcomings such as data dependency, overfitting, and computational complexity. They need large amounts of data to train the network and they are also prone to overfitting. The interpretability of the model is low due to the black box nature making it impossible to identify why the particular image is labelled as tampered.

Standardization is important to maintain the consistency and comparability of different datasets and methods. Data preprocessing, feature extraction, model evaluation, and dataset creation are the steps used here. Data preprocessing applies techniques such as normalization, resizing, and color space conversion. This step minimizes the variability and improves the detection performance of algorithms. The feature extraction steps extract the crucial features and improve the training process of the new algorithms developed. The model is mainly evaluated using standard evaluation protocols and metrics to identify comparable and reproducible results. Dataset creation should be standardized to minimize biases and errors while training the algorithms. The standardization techniques should ensure consistency in detection, improve model interoperability, minimize bias, and enhance benchmarking. The benchmarking process identifies the standardization between the forged and actual images using the following procedures:

Uniform evaluation metrics: The methods taken for comparison need to be evaluated using standardized evaluation metrics such as F1-score, recall, and precision.

Controlled experimental setup: Here, every models that are taken for comparison should be involved in a controlled experimental environment where every image is processed in a same pipeline. In this way, variations in image quality can be dismissed during preprocessing and the detection accuracy will not be compromised.

Ground truth labels: Conventional benchmark datasets have ground truth labels to distinguish between actual and tampered images. Standard labeling is needed to validate the benchmarking tests conducted.

Consistent data usage: We need to ensure that the forged and actual images are obtained from the same datasets to achieve direct comparisons and efficient evaluations.

The creation of new open-access datasets is important for researchers because they offer research advancement, method comparison, real-world testing, and community collaboration. In this way, they can promote new open-source tools and test their methods in the real world in different conditions to identify the challenges present.

When analyzing image datasets, one needs to focus on diversity and size, annotation quality, and benchmarking for accurate training and validation of the algorithms. The main challenges focused on by researchers to identify multiple image attacks are adversarial attacks, computational complexity, detection accuracy, and limited adaptability. Adversarial attacks are conducted by making subtle changes to the image which is hard to observe. When deploying techniques such as multilayer filters and noise injection one needs to be aware of their computational complexity.

Resampling detection, compression artifact analysis, error level analysis, and noise analysis are the techniques used in this review to identify tampering and its use in criminology. These techniques identify inconsistencies, variance in compression levels, and noise patterns to detect anomalies. When used in conjunction with image criminology methods, these techniques can identify tampered areas in crime scenes.

7.1 Real-world image tampering applications

This section demonstrates different image tampering applications used for law enforcement and media verification. In law enforcement, image tampering is crucial since it analyzes whether any modifications are made to the images or not. For example, the crime scene images can be tampered with different timestamps or objects to misguide the investigation. Sometimes the CCTV footages are tampered with using splicing operations to misguide the investigations. The court mainly accepts the evidence based on its authenticity and tampered images should be taken from legal proceedings. In these cases, an error can lead to misjudgment which affects law enforcement.

In media, the information needs to be verified accurately since fake information is often spread worldwide. Popular social media platforms should verify the authenticity of the images before publishing them online. The misleading content is mainly generated using deepfake and novel image manipulation techniques. The misinformation operations can be prevented using image tampering detection. The breaking news I soften shared across multiple platforms needs to be authenticated by medial verification systems to differentiate between real and fake footage. Social media platforms should automatically remove tampered content to stop the spread of fake information.

8. CONCLUSION AND FUTURE WORK

This paper conducts an extensive systematic review of image forgery identification techniques (active and passive). The study mainly highlights the use of cutting-edge deep learning techniques in identifying manipulated facial images or passive image forgeries. The deep learning techniques utilize both geometric-based detection and pixel-based detection to identify the forgeries present in large-scale datasets such as DeepFake and CASIA. To achieve a tradeoff between operational cost and execution time, efficient image forensics methodologies need to be developed. The existing techniques were not capable of accurately detecting different attacks that involve JPEG compression, illuminating power, smudging, proportioning, and whirligig. Other challenges that need to be addressed are computational intensity, feature dimensionality, detection accuracy, and resistance against subsequent production. To tackle the increasingly intricate forgeries prevalent in today's digital landscape, the paper advocates for the development of advanced, unrestricted, and strong imitation avoidance techniques along with a proper identification strategy. These approaches not only demonstrate high accuracy but also exhibit efficiency in real-world scenarios. By addressing these research directions, the area of picture imitation identification can continue to evolve, ensuring the integrity and trustworthiness of digital imagery despite the ever-advancing imitation methods. Besides accuracy and efficiency, other factors such as robustness, scalability, user-friendliness, and privacy and security are crucial when designing image forensic methods. The image forgery techniques can be applicable in real-time by improving the accuracy and efficiency of handling large datasets. In this way, the methods can be applied in real-time scenarios and minimize the number of false positives and negatives.

Real-time detection, scalability, and resource constraints are the needs that arise in the development of efficient image forensic techniques to achieve a tradeoff between operational cost and execution time. Timely identification is crucial for image forensics techniques and computationally intensive techniques are not reliable for real-time detection. The scalability issue identifies whether the method can handle large amounts of data. Adversarial examples (minute perturbations), complex manipulations (deepfake and GAN-based manipulation), and unknown attacks targeting logical flaws in protocols are the different types of attacks the recent techniques fail to identify. The advanced mimicry avoidance techniques use contrastive learning, unsupervised clustering, and feature-level concatenation. These steps enhance feature extraction, and detection performance, and separate forged and pristine regions. Image mimicry recognition can be improved by focusing on unexplored challenges, creating diverse datasets, utilizing new deep-learning techniques, and working with experts to create novel solutions.

In the future, image forensic protocols can be improved via standardization, benchmarking, open-access datasets, and real-world applicability. The standardization techniques identify the common protocols for datasets, parameters, and

training. The benchmarking process ensures that standardized datasets using forged and actual images created with the help of GAN can be used for collaborative research. If new open-access datasets are created it will help the researchers to train their algorithm with large forgery types. These areas need to be addressed by the researchers when developing novel solutions to minimize the risks associated with digital forgery in modern multimedia transmissions. Advanced AI and deep learning techniques can be integrated for automatic feature extraction and detect complex forgeries. Novel techniques needed to be developed to identify complex forgery types such as adversarial manipulations, deepfake, and inpainting. The image forensic protocols developed should be robust enough to handle low-quality data and technical variations. Cross-domain adaptability is another research area that needs to be focused on to apply the model in different types of domains that contain medical and satellite images. The following are other areas of future research. New mimicry avoidance techniques need to be developed to detect and prevent mimicry. Standard techniques need to be developed which use unique protocols for evaluation. Developing diverse open-access datasets is an important area of research. To compare different techniques, comprehensive benchmarks need to be developed.

ACKNOWLEDGEMENT

Thank you my guide for supporting to preparing this paper.

REFERENCES

[1] K. B. Meena and V. Tyagi, "Image Forgery Detection: Survey and Future Directions," in *Image Forgery Detection: Survey and Future Directions*, pp. 163–194. Springer, Singapore, 2019.

[2] N. K. Gill, R. Garg, and E. A. Doegar, "A review paper on digital image forgery detection techniques," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7. DOI: 10.1109/ICCCNT.2017.8203904.

[3] B. Chaitra and P. V. B. Reddy, "A study on digital image forgery techniques and its detection," in *2019 International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 127–130. DOI: 10.1109/IC3I46837.2019.9055573.

[4] S. Bourouis, R. Alroobaea, A. M. Alharbi, M. Andejany, and S. Rubaiee, "Recent advances in digital multimedia tampering detection for forensics analysis," *Symmetry*, vol. 12, no. 11, p. 1811, 2020.

[5] A. H. Saber, M. A. Khan, and B. G. Mejbel, "A survey on image forgery detection using different forensic approaches," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 3, pp. 361–370, 2020.

[6] S. D. Mahalakshmi, K. Vijayalakshmi, and S. Priyadharsini, "Digital image forgery detection and estimation by exploring basic image manipulations," *Digital Investigation*, vol. 8, no. 3–4, pp. 215–225, 2012.

[7] P. Ferrara, T. Bianchi, A. De Rosa, and A. Piva, "Image forgery localization via fine-grained analysis of CFA artifacts," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 5, pp. 1566–1577, 2012.

[8] K. K. Doke and S. M. Patil, "Digital signature scheme for image," *International Journal of Computer Applications*, vol. 49, no. 16, pp. 1–6, 2012.

[9] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," *IEEE Access*, vol. 6, pp. 70025–70034, 2018.

[10] D. Kaur and N. Kanwal, "An analysis of image forgery detection techniques," *Statistics, Optimization and Information Computing*, vol. 7, no. 2, pp. 486–500, 2019.

[11] N. K. Gill, R. Garg, and E. A. Doegar, "A review paper on digital image forgery detection techniques," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7. DOI: 10.1109/ICCCNT.2017.8203904.

[12] P. Sharma, M. Kumar, and H. Sharma, "Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation," *Multimed. Tools Appl.*, vol. 82, no. 12, pp. 18117–18150, 2023.

[13] M. Hussain, S. Qasem, G. Bebis, G. Muhammad, H. Aboalsamh, and H. Mathkour, "Evaluation of image forgery detection using multi-scale Weber local descriptors," *International Journal of Artificial Intelligence Tools*, vol. 24, no. 4, p. 1540016, 2015.

[14] S. Lu, X. Hu, C. Wang, L. Chen, S. Han, and Y. Han, "Copy-move image forgery detection based on evolving circular domains coverage," *Multimedia Tools and Applications*, pp. 1–26, 2022. DOI: 10.1007/s11042-022-12755-w.

[15] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Report TR2004-515, Department of Computer Science, Dartmouth College, Hanover, New Hampshire, pp. 1–11, 2004.
[16] H. Yao, T. Qiao, Z. Tang, Y. Zhao, and H. Mao, "Detecting copy-move forgery using non-negative matrix factorization," in *2011 Third International Conference on Multimedia Information Networking and Security (MINES)*, pp. 591–594. DOI: 10.1109/MINES.2011.104.
[17] A. Rani, A. Jain, and M. Kumar, "Identification of copy-move and splicing based forgeries using advanced SURF and revised template matching," *Multimedia Tools and Applications*, vol. 80, no. 16, pp. 23877–23898, 2021.
[18] J. Xu, D. Feng, J. Wu, and Z. Cui, "An image inpainting technique based on 8-neighborhood fast sweeping method," in *2009 WRI International Conference on Communications and Mobile Computing*, pp. 626–630. DOI: 10.1109/CMC.2009.369.
[19] M. Kumar and S. Srivastava, "Image forgery detection based on physics and pixels: a study," *Australian Journal of Forensic Sciences*, vol. 51, no. 2, pp. 119–134, 2019.
[20] A. Kaur and J. Rani, "Digital Image Forgery and Techniques of Forgery Detection," *International Journal of Technical Research and Science*, vol. 1, no. 4, pp. 18–24, 2016. Available: www.ijtrs.com
[21] V. D. Mohite, U. Athawale, S. Athawale, and B. Vidyapeeth, "Survey on Recent Image Forgeries and their Detection Methods," *International Journal of Research in Engineering, Applied and Management (IJREAM)*, vol. 2, pp. 885–892, 2019.
[22] Y. Fan, P. Carré, and C. Fernandez-Maloigne, "Image splicing detection with local illumination estimation," in *2015 IEEE International Conference on Image Processing (ICIP)*, pp. 2940–2944. DOI: 10.1109/ICIP.2015.7351341.
[23] S. Li, P. Xunyu, and Z. Xing, "Exposing region splicing forgeries with blind local noise estimation," in *Proceedings of the 2014 IEEE International Conference on Information Forensics and Security (WIFS)*, pp. 92–97, 2014. DOI: 10.1109/WIFS.2014.7084317.
[24] A. Kashyap, R. S. Parmar, M. Agrawal, and H. Gupta, "An evaluation of digital image forgery detection approaches," *arXiv preprint arXiv:1703.09968*, 2017. DOI: 10.48550/arXiv.1703.09968.
[25] M. A. Qureshi and M. Deriche, "A review on copy-move image forgery detection techniques," in *2014 IEEE 11th International Multi-Conference on Systems, Signals and Devices (SSD14)*, pp. 1–5. DOI: 10.1109/SSD.2014.6808907.
[26] Q. Liu and A. H. Sung, "A new approach for JPEG resize and image splicing detection," in *Proceedings of the First ACM Workshop on Multimedia in Forensics*, pp. 43–48, 2009. DOI: 10.1145/1631081.1631092.
[27] J. M. Pinel, H. Nicolas, and C. L. Bris, "Estimation of 2D illuminant direction and shadow segmentation in natural video sequences," *Proceedings of VLBV*, pp. 197–202, 2001.
[28] J. Xu, D. Feng, J. Wu, and Z. Cui, "An image inpainting technique based on 8-neighborhood fast sweeping method," in *2009 WRI International Conference on Communications and Mobile Computing*, vol. 3, pp. 626–630. IEEE, 2009.
[29] J. Fridrich, "Sensor defects in digital image forensic," in *Digital Image Forensics*, pp. 179–218, Springer, New York, NY, 2013.
[30] M. Kumar, A. Rani, and S. Srivastava, "Image forensics based on lighting estimation," *International Journal of Image Graphics*, vol. 19, no. 3, p. 1950014, 2019.
[31] J. F. O'Brien and H. Farid, "Exposing photo manipulation with inconsistent reflections," *ACM Transactions on Graphics*, vol. 31, no. 1, pp. 4-1–4-11, 2012.
[32] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "3D lighting-based image forgery detection using shape-from-shading," in *2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, pp. 1777–1781.
[33] N. Nirmalkar, S. Kamble, and S. Kakde, "A review of image forgery techniques and their detection," in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1–5. https://doi.org/10.1109/ICIIECS.2015.7193177
[34] M. Kumar, S. Srivastava, and N. Uddin, "Forgery detection using multiple light sources for synthetic images," *Australian Journal of Forensic Sciences*, vol. 51, no. 3, pp. 243–250, 2019.
[35] J. Pine and H. Nicolas, "Estimation of 2D illuminant direction and shadow segmentation in natural video sequences," in *proceedings of VLBV*, p. 197, 2001.
[36] A. Stojkovic, I. Shopovska, H. Luong, J. Aelterman, L. Jovanov, and W. Philips, "The effect of the color filter array layout choice on state-of-the-art demosaicing," *Sensors*, vol. 19, p. 3215, 2019. https://doi.org/10.3390/s19143215
[37] M. Kumar and S. Srivastava, "Image authentication by assessing manipulations using illumination," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 12451–12463, 2019.

[38] B. Peng, W. Wang, J. Dong, and T. Tan, "Optimized 3D lighting environment estimation for image forgery detection," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 479–494, 2016.
[39] E. Kee and H. Farid, "Exposing digital forgeries from 3-D lighting environments," in *2010 IEEE International Workshop on Information Forensics and Security*, pp. 1–6. [
[40] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "3D lighting-based image forgery detection using shape-from-shading," in *2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, pp. 1777–1781.
[41] M. Kumar and S. Srivastava, "Image tampering detection based on inherent lighting fingerprints," in *Computational Vision and Bio Inspired Computing*, pp. 1129–1140, Springer, Cham, 2018.
[42] A. T. Alhussainy, "Forensic source camera identification by using features in machine learning approach," Ph.D. dissertation, Université Montpellier, 2016.
[43] G. K. S. Gaharwar, P. V. V. Nath, and R. D. Gaharwar, "Comprehensive study of different types of image forgeries," *Int. J. Sci. Technol. Manage.*, vol. 6, pp. 146–151, 2015.
[44] M. K. Johnson and H. Farid, "Metric measurements on a plane from a single image," Computer Science Technical Report TR2006-579, 2006. [Online]. Available: (https://farid.berkeley.edu/)
[45] B. S. Kumar, S. Karthi, K. Karthika, and R. Cristin, "A systematic study of image forgery detection," *J. Comput. Theor. Nanosci.*, vol. 15, no. 8, pp. 2560–2564, Aug. 2018.
[46] G. K. S. Gaharwar, P. V. V. Nath, and R. D. Gaharwar, "Comprehensive study of different types of image forgeries," *Int. J. Sci. Technol. Manage.*, vol. 6, pp. 146–151, 2015.
[47] L. Wu, X. Cao, W. Zhang, and Y. Wang, "Detecting image forgeries using metrology," *Mach. Vis. Appl.*, vol. 23, no. 2, pp. 363–373, Mar. 2012.
[48] A. Morgand, M. Tamaazousti, and A. Bartoli, "A multiple-view geometric model for specularity prediction on non-uniformly curved surfaces," arXiv preprint arXiv:2108.09378, 2021. [Online]. Available: (https://doi.org/10.48550/arXiv.2108.09378)
[49] N. E. Joudar and M. Ettaouil, "KRR-CNN: Kernels redundancy reduction in convolutional neural networks," *Neural Comput. Appl.*, pp. 1–12, 2021.
[50] F. E. F. Junior and G. G. Yen, "Particle swarm optimization of deep neural network architectures for image classification," *Swarm Evol. Comput.*, vol. 49, pp. 62–74, Aug. 2019.
[51] I. Castillo Camacho and K. Wang, "A comprehensive review of deep-learning-based methods for image forensics," *J. Imaging*, vol. 7, no. 4, p. 69, Apr. 2021.
[52] S. Sharma and K. Kumar, "Guess: Genetic uses in video encryption with secret sharing," in *Proc. 2nd Int. Conf. Comput. Vis. Image Process.*, Singapore, Jan. 2018, pp. 51–62.
[53] S. Sharma, K. Kumar, and N. Singh, "D-FES: Deep facial expression recognition system," in *2017 Conf. Inf. Commun. Technol. (CICT)*, 2017, pp. 1–6.
[54] S. Sharma, K. Kumar, and N. Singh, "D-FES: Deep facial expression recognition system," in *2017 Conference on Information and Communication Technology (CICT)*, 2017, pp. 1–6. DOI: https://doi.org/10.1109/INFOCOMTECH.2017.8340635
[55] X. Glorot, A. Bordes, and Y. Bengio, "Deep sparse rectifier neural networks," in *Proc. Fourteenth Int. Conf. Artif. Intell. Stat.*, 2011, pp. 315–323. [Online]. Available: (https://proceedings.mlr.press/v15/glorot11a)
[56] K. San Choi, E. Y. Lam, and K. K. Wong, "Source camera identification using footprints from lens aberration," in *Proc. SPIE 6069, Digital Photography II*, 2006, p. 60690J. DOI: https://doi.org/10.1117/12.649775
[57] R. K. Koppanati and K. Kumar, "P-MEC: Polynomial congruence-based multimedia encryption technique over cloud," *IEEE Consum. Electron. Mag.*, vol. 10, no. 5, pp. 41–46, Sept. 2020.
[58] R. K. Koppanati, S. Qamar, and K. Kumar, "SMALL: Secure multimedia technique using logistic and LFSR," in *2018 Second Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, 2018, pp. 1820–1825.
[59] R. K. Koppanati, K. Kumar, and S. Qamar, "E-MOC: An efficient secret sharing model for multimedia on cloud," in M. Tripathi and S. Upadhyaya (Eds.), *Conf. Proc. ICDLAIR2019. Lect. Notes Networks Syst.*, vol. 175, Springer, Cham, 2021.
[60] A. Mantri, N. Singh, K. Kumar, and S. Dahiya, "Pre-encryption and identification (PEI): An anti-crypto ransomware technique," *IETE J. Res.*, pp. 1–9, 2022.
[61] Aberna, P. and Agilandeeswari, L., 2024. Optimal semi-fragile watermarking based on maximum entropy random walk and swin transformer for tamper localization. IEEE Access.
[62] Lin, X., Wang, S., Deng, J., Fu, Y., Bai, X., Chen, X., Qu, X. and Tang, W., 2023. Image manipulation detection by multiple tampering traces and edge artifact enhancement. Pattern Recognition, 133, p.109026.
[63] Yan, C., Li, S. and Li, H., 2023. TransU 2-Net: A Hybrid Transformer Architecture for Image Splicing Forgery Detection. IEEE Access, 11, pp.33313-33323.

[64] Sun, Y., Ni, R. and Zhao, Y., 2022. ET: Edge-enhanced transformer for image splicing detection. IEEE Signal Processing Letters, 29, pp.1232-1236.
[65] Lee, S., Tariq, S., Shin, Y. and Woo, S.S., 2021. Detecting handcrafted facial image manipulations and GAN-generated facial images using Shallow-FakeFaceNet. Applied soft computing, 105, p.107256.\
[66] Sushir, R.D., Wakde, D.G. and Bhutada, S.S., 2024. Enhanced blind image forgery detection using an accurate deep learning based hybrid DCCAE and ADFC. Multimedia Tools and Applications, 83(1), pp.1725-1752.