10.48047/jocaaa.2024.33.06.118

A Review on Image Forgery Detection based on Pixel

Harish Sahu[1], Dr. Ranu Pandey[2]
1 Research Scholar, Shree Rawatpura Sarkar University, Raipur, Chhattisgarh, India,
sahu.harish@gmail.com
2 Asst. Prof., Shree Rawatpura Sarkar University, Raipur, Chhattisgarh, India
ranu_pandey8@hotmail.com

ABSTRACT

With the development of digital image processing software and editing tools, it has become easier to alter digital images. Detecting image manipulation is crucial because images can serve as legal evidence, be used in forensic investigations, and have applications in many other areas. Pixel-based image forgery detection aims to check the authenticity of digital images without needing prior knowledge of the original image. There are various methods used to tamper with images, including splicing or copy-move techniques, resampling (such as resizing, rotating, or stretching), and adding or removing objects from the image.Currently, the main objective of digital image tampering detection is to ensure the consistency and reliability of digital images. Maintaining the integrity of digital content is essential across different fields such as journalism, media, social media, forensics, and national security. This survey examines both active and passive image forgery techniques to identify signs of tampering and manipulation within image content. Forgeries in manipulated images are detected through methods like camera source identification, JPEG compression tampering, illumination inconsistencies, and mathematical manipulations. These varied approaches offer a comprehensive understanding of the image forensic field. To tackle key research challenges, standardized input sets, evaluation metrics, and analysis criteria are employed. In this paper, various pixel-based techniques for image forgery detection are discussed.

Keywords:
Image forgery, Image forgery detection, Copy-move, Splicing, Tampering.

INTRODUCTION:

Forgeries have been a longstanding issue throughout human history. It is a well-known fact that images often convey more truth than words. With the progress of technology, it has become increasingly difficult for people to trust images presented as proof or evidence. Today, images play a crucial role in communication media. Technological advancements have led to the development of more sophisticated editing tools and software, making it easier to alter images. Popular image editing software such as Cameran360, Adobe Image Shop, Skylum Luminar, ACD See Image Shop Pro, and Corel Paint Shop Pro are widely available, allowing anyone to manipulate images with relative ease. This can result in serious consequences, as altered images may be used as evidence in legal proceedings, leading to incorrect outcomes. Digital image forgery is a key aspect of image forensic, where images from specific situations are analyzed to determine their authenticity and reliability using various techniques. These manipulated images spread rapidly across the internet and multimedia platforms. The rise of advanced digital technologies, along with the affordability and accessibility of processing devices and tools, combined with the widespread sharing of

10.48047/jocaaa.2024.33.06.118

images on platforms such as Facebook, Twitter, Telegram, and Pinterest, as well as through news broadcasting, has created a significant and dangerous problem for the world. This also highlights a major issue, contributing to the increasing contamination of digital images.

In this context, the primary aim of image forensics is to identify if an image has been forged. Therefore, confirming the authenticity of images is crucial, particularly because they are commonly used as evidence in legal matters. These images can include a person's fully verified documents such as an Aadhar card, ID card, bank passbook, financial records, newspapers, or sections of medical and educational records from schools, colleges, or universities. Additionally, image files are often recompressed and resized, which makes them easier to share online. This is further supported by the increasing use of cloud-based image sharing and editing platforms such as Picasa and Flickr, as well as the popularity of social media apps like WhatsApp, Instagram, and Snapchat. This review paper discusses various aspects related to image forgery detection.

2.Literature Review:

The classification of image forgery is based on whether the images are original or modified. Forgery detection techniques are generally categorized into two main types [1].

These categories are:

A. Active authentication.

B. Passive authentication.

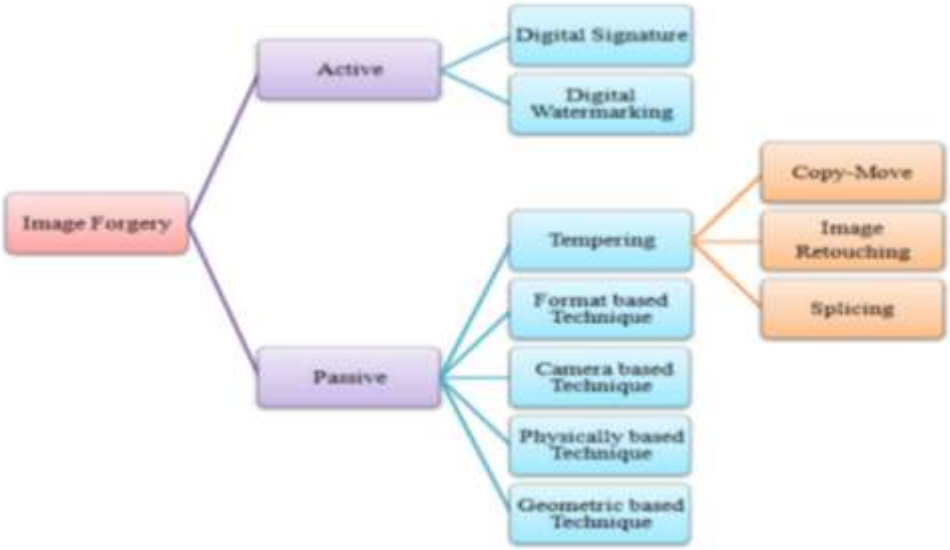


Fig1: Classification of Image Forgery.

A.) Active authentication:

From this perspective, digital images needs preprocessing steps such as a watermark inserting or creating a signature on the picture, thus limits their practical usage [3]. Digital signatures and the process of authentication are involved. Additionally, techniques of active authentication are categorized into two main types: first one is digital signature and the other one is watermarking. This process is used during the time of checking the codes and validating the originality of the picture.

1) Digital signature:

It is a mathematical approach which is used to confirm the authenticity and integrity of a Picture.A digital signature falls under active methods used for image forgery detection. A digital signature is similar to a handwritten signature, as it contains a key or signature,

10.48047/jocaaa.2024.33.06.118

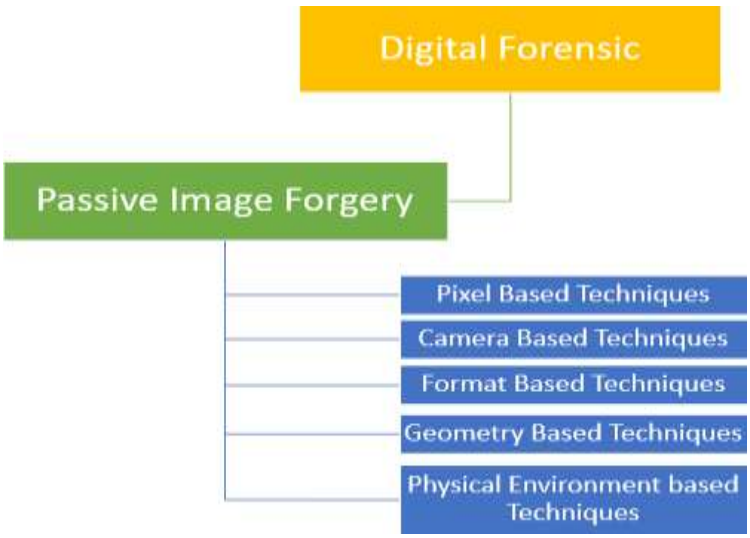
offering more additional implicit security. in a digital signature A secret key X is used to generate Y arbitrary matrices with entries that are evenly distributed in the range [0, 1]. In [2], authors proposed a new method which involving the use of a low phase filter for generating very random matrices repeatedly to obtain X random patterns. The proposed model generates a digital signature to the image by the applying signing operation. The image signing process includes the following steps: i) Applying parameterized wavelet features to decompose the image. ii) Extracting the standard digital signature. iii) Producing a cryptographic signature through the private key and cryptographically hashing the extracted standard digital signature. iv) Delivering the digital images along with the cryptographic signature to the client.

(2) Digital watermarking :is a technique that originated from the traditional practice of adding a visible watermark to paper. This method, which uses an active approach, is often used to detect image forgery by hiding data within the image. In contrast, inactive authentication methods do not need prior knowledge of the image and are not necessary for embedding the watermark. Digital watermarking has several important features, including imperceptibility, which means the watermark is not easily noticeable, and robustness, which means it can survive different types of manipulation. Some techniques use maximum distance calculations combined with linear shift register ranges applied to pixel data. These watermarks are then identified using a spatial cross-correlation function. This type of watermark is hidden within the image and can be either partially visible or fully visible. Additionally, there are watermarking patterns that are not visually identifiable, which may cause slight changes in individual pixels, helping to locate the watermark [4]. When a digital image is created, watermarks are embedded into it. However, active techniques have certain limitations because they often require some level of human involvement and specialized equipment. To address these issues, a passive image authentication method has been introduced, which also works as a non-blind detection system.

(B). Passive authentication:

In this method, the client's identity is confirmed without the need for any additional authentication steps. It also operates as a blind detection system. This technique does not rely on any prior knowledge about the image. To evaluate the originality and authenticity of an image, a passive detection approach is used, without the use of active techniques such as watermarking or digital signatures. These methods are based on the assumption that there are no visible signs of a fabricated area in the digital image, and that such modifications could disrupt the natural consistency of the original image, resulting in the creation of new artifacts and various anomalies. A modified region in an image is also regarded as an anomaly in the image. Passive image authentication techniques are primarily classified into five types: [1] light and object interaction with 3D. Light plays a significant role in capturing an image. Consider the twinkling of stars at night or seeing stars while walking in a garden. Both types of images are created through cloning and combined to form one image, which falls under physical-based forgery. [5] Geometric-based technique—this method detects forgeries by measuring objects at the geometric level. The characteristics of passive image forgery detection are discussed in this section, which is currently considered the most advanced method for detecting image manipulation. Passive image science, also referred to as blind image science, aims to determine the accuracy and source of an image without depending on pre-existing information [6]. It includes five main approaches: pixel-based detection, format-based detection, physical-based detection, camera-based detection, and geometry-based

10.48047/jocaaa.2024.33.06.118



detection. These techniques incorporate a variety of detection methods, as shown in Figures 2

Fig.2 Types of Passive Tampering Detection

and 5. These methods are commonly used regardless of the device to manipulate or replicate images for malicious or harmful purposes [7]. Various image formatting methods are necessary to achieve these objectives. Passive image forgery detection techniques analyze one or more images to uncover complex traces of inconsistencies within the forged image. These inconsistencies may include overlapping artifacts, missing data, deformations, and additional features like the identifiable impression of a thumb, which serve as clues in image forensics.

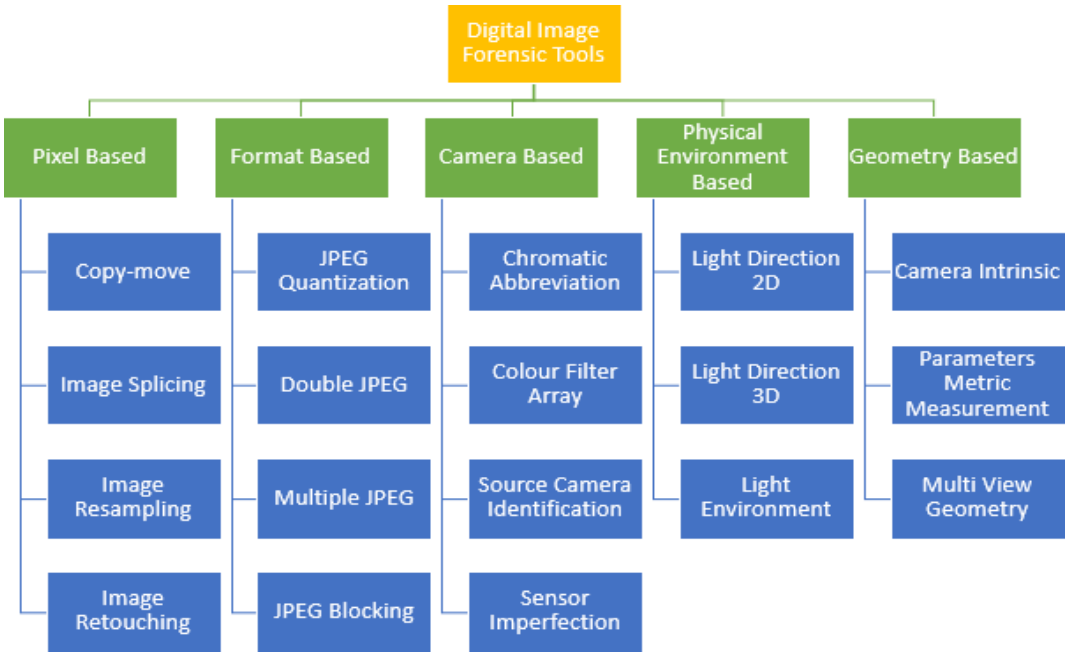


Fig.3 Passive image tampering techniques-classification

Pixel Based image forgery

Classification of bits involves looking at individual pixels by using the specific spectral information found in each pixel. These methods are often used to extract information from an image that isn't visible at a higher level, and they classify the image based on the data it contains [8]. However, there can be errors in areas where different classes are mixed together, causing confusion. Pixel-based forgeries include major types like copy-move, photo segmentation, photo interpolation, and photo editing. A lot of research has been done to create different detection methods, and the current focus is on using deep learning techniques to address these issues effectively.

Methods Based on Copy and Move

Copy and Move methods are widely used techniques for altering images, and they are difficult to detect because the duplicated parts are often hard to trace back to their original source. In Copy-Move image manipulation, a portion of an image is copied and pasted onto another area within the same image [9]. There are two main types of these attacks: Class-1, which involves copying and shifting a section, and Class-2, which involves cloning and creating a new section. Examples of these two types are shown in Figures 6a and 6b [10,11]. Detection methods for Copy-Move manipulation are typically categorized into block-based and key point-based approaches, as outlined below. This technique is often used by individuals to alter images for harmful or deceptive purposes, such as changing the original message or concealing certain elements using other images or real-time effects. Applications like duplication and cloning filters are commonly used [12]. Because of this, the altered image often shows clear signs of distortion, real-time adjustments, convergence, and other visual effects. The dimensions of the altered portion can also be analyzed to identify instances of image manipulation.

Fig.4a: Class-1type clone-attach image tampering. b:Class-2 type Clone Make picture imitation .

A new method introduced by Lu et al. [13] makes use of the circular domain extent (ECDC) process. This method blends block-based and keypoint-based techniques for identifying

imitations. Initially, features like scale-invariant feature transform (SIFT) and speed-up robust features (SURF) in log-polar space are extracted from the full image. After this, using the generalized two nearest neighbors (g2NN) method a very large number of matched pairs are created .To detect altered areas, Popescu et al. [14] used principal components analysis (PCA) as a feature. Yao et al. [15] applied non-negative matrix factorization to identify copy-move forgery. In this approach, non-negative matrix factorization (NMF) coefficients are obtained from all blocks after splitting the image into fixed-size overlapping blocks. It is important to note that all coefficients are quantized before matching, which enables the identification of a sub-image using a smaller amount of data.Raniet al. [16] introduced a technique called tampering detection using infrastructure for clone-shift and slicing-based imitations. In their study, image information is preprocessed to enhance the data that can be used for analysis. The proposed method generates multiple attributes for improved SURF and corresponding frameworks to detect forged areas in images. The estimated main features suggest a pre-set boundary value. The CASIA forged image dataset is used to perform the evaluation. The enhanced SURF approach achieved a limit identification accuracy of 97%, while the compatible frameworks achieved a fraud detection rate of approximately 100%

Methods for picture-enhancing tampering identification

This method is widely used in magazines and film photography. Although these changes are intended to improve the visual appeal of an image and are not classified as forgery, they are included here because they involve adjustments that impact the image's originality [17]. The image is modified to make it more visually pleasing, with specific elements altered, such as removing wrinkles to create the final shot. Figure 5a shows the enhanced image, while Figure 5b presents the original image. These techniques are commonly used for enhancement and are generally less harmful compared to other forms of image manipulation [18,19]. A key part of image retouching is the removal or reduction of imperfections. Professional editors carefully work to eliminate blemishes, acne, scars, or any other elements that might distract from the subject or the intended composition [20].

(A) (B)

Fig.5 B is a Retouched image and A is an original image

Xuetal. [21] introduced another technique that uses the 8-neighborhood fast comprehensive tasks to improve both the speed and quality of image painting. They also developed a Pyramid model based on down sampling in painting (PDI), which incorporates the ASP principles. Experimental results showed that integrating the PDI model significantly enhanced existing techniques [22]. Additionally, a picture image-restoration method was explored, which relies on a self-organizing map (SOM) to recover important structural data from damaged images.Kumaretal. [23] examined various bits-based and scientific algorithms for fraudulent identification and performed a comparative analysis of these techniques. Moreover, despite differences in imaging devices and processing procedures, they all share a common pattern in the image. Any interference within this pattern leads to deviations from the original image, making it possible to detect image counterfeiting. This method provides more accurate detection of forgeries and works particularly well on images with uniform lighting. For more detailed methods, references such as [24,25] can be consulted. As the field continues to develop, it is essential to keep researching and creating strong methods for detecting and reducing image retouching forgeries. This will help maintain the integrity of visual content and support trust and authenticity in digital media.

Methods for photo slicing or mixed-media art tampering identification

Image splicing, also called photo arrangement, is a common type of digital image manipulation where parts of images from similar or different sources are copied and pasted together to form a composite image [26]. This process can lead to the loss, distortion, or damage of original information from the source images. Figure 8 illustrates the effect of this process.Image splicing can be divided into two main categories: boundary-based slicing and region-based slicing.

Forensic methods are used to detect these techniques and analyze the areas where images have been altered to determine the authenticity and location of the changes.Fan et al. [20] developed a method that estimates brightness in flat and upright areas by combining algorithms based on low-level numerical values. This method identifies area-slicing forgeries by looking for inconsistencies in the color of light within object regions.

Kumar et al. [27] proposed a new blind forgery detection technique that uses regional turbulence discrepancies to identify small areas affected by regional distortions. This technique involves dividing images into consistent segments based on homogeneity and analyzing low-cut oblique fluctuation parameters, which are vital for making a conclusive determination. These methods work well on images with consistent distortion levels, which do not show similar characteristics when examined closely.

Pine et al. [28] also used regional upright distortion to detect small areas affected by regional distortion in a blind forgery detection technique.

This method takes into account non-overlapping blocks and high-pass inclined fluctuation factors for a precise determination. The image is divided into similar sub-areas using normal regions with the help of fusion methods based on a homogeneity criterion. While these methods are effective for images with static distortion levels, they may face challenges when applied to images with similar noise patterns. By continuing to develop new forensic techniques, researchers aim to improve the detection and analysis of image splicing forgeries.

These efforts help in creating stronger tools and methods for identifying and reducing deceptive manipulations of digital images.

Original Image 1

Original Image 2

Tempered Image using Splicing

Fig.6 Image splicing forgery

Tampering detection of image resampling

Digital picture processing imitation identification relies on the manipulation of mathematical properties such as stretching, flipping, distorting, twisting, and resizing, applied to specific areas to produce visually compelling forged images. Estimating the level is crucial in the digital picture process as it highlights significant mathematical differences. Resampling an image results in the appearance of distinct periodic correlations that can be efficiently used [17]. Figure 7 shows a digital picture processing technique [18].

To improve the robustness of detection, fusion-based approaches have been introduced.

These methods combine various features or classifiers from different detection techniques to achieve enhanced performance. Blending techniques, including feature-level, decision-level, and score-level blending, aim to take advantage of the strengths of individual detection methods, thereby increasing overall accuracy and reliability.

Wang et al. [29] showed the effectiveness of monitored understanding as a strong and flexible method for tackling the issue of anonymous image mathematics and hidden passcodes.

A key part of understanding the process involves selecting informative features with a low-dimensional representation.

Liu et al. [18] examined the relationship between neighboring Discrete Cosine Transform (DCT) parameters and developed a technique to identify altered JPEG images, including sliced images used for picture duplication.

Detailed extraction of adjacent saturation characteristics from the DCT parameters supports the detection process, which uses Support Vector Machines (SVM).

Fig7. 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

Tampering detection-compression-based

It may be challenging to identify forged images because these images are often altered for compression and other reasons. Forgeries are hard to detect because JPEG images tend to lose quality during compression. JPEG stands for Joint Photographic Experts Group. To determine if an image has been manipulated, forensic analysis uses specific features of JPEG compression [30]. These methods include techniques that rely on JPEG discretization, dual JPEG compression, and various forms of JPEG compression, along with JPEG obstruction. Some compression methods introduce statistical correlations, which are helpful in recognizing fake images. A quantization matrix is used in the literature [31] to detect double JPEG compression.

Based on the assumption, when block-wise DCT is applied according to the main JPEG compression grid, it will behave like an integer periodic function.

A method for detecting unaligned double JPEG compression was identified in [32]. Kee et al. [33] developed a hidden message detection method based on a normal function to model images. Afterward, the ratio of two Fourier parameters, which spread across the DCT factors, is measured. The spread of DCT parameters is modeled using a normal function model. The LSB (Least Significant Bit), SSIS (Spread Spectrum Image Steganography), and the graph-theoretic Steg-Hide tool are three steganographic techniques that are compared to this derived steganalysis measure. Datasets of visual features are classified using various classification techniques, such as SVM.

CONCLUSION:

In this paper, different methods for detecting image forgery based on pixels have been examined and analyzed. All the techniques and approaches covered in this paper are capable of identifying forged content. However, certain algorithms are not very effective at pinpointing the exact areas that have been altered. Additionally, some of these algorithms require a significant amount of time to process. Therefore, there is a need to create more efficient and accurate algorithms for detecting image forgeries.

References:

[1] H. Farid, “Image forgery detection,” IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, 2009, doi: 10.1109/MSP.2008.931079.

[2] S. . P. Doke, Kanchan K, “Digital Signature Scheme for Image,” vol. 49, no. 16, pp. 1–6, 2012, doi: 10.5120/7708-1012.

[3] J. Fridrich, “Robust Bit Extraction from Images,” pp. 536–540, 1999.

[4] X. Zhao, J. Li, S. Li, and S. Wang, “Detecting Digital Image Splicing in Chroma Spaces,” pp. 12–13, 2011, doi: 10.1007/978-3 642-18405-5_2.m

[5] S. B. Ã and A. K. Nandi, “Automated detection and localisation of duplicated regions affected by reflection , rotation and scaling in image forensics,” Signal Processing, vol. 91, no. 8, pp. 1759–1770, 2011, doi: 10.1016/j.sigpro.2011.01.022.

[6] 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

[7] 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.

[8] 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.

[9] N.K. Gill, R. Garg, and E. A. Doegar, "A review paper ondigital 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.

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

[11]M.Hussain,S.Qasem,G.Bebis,G.Muhammad,H.Aboalsamh,andH.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.

[12] 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.

[13]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.

[14] 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,NewHampshire,pp.1–11,2004.

[15] 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.

[16]A.Rani,A.Jain,andM.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.
[17]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.
[18]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.
[19]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.
[20]J.M.Pinel,H.Nicolas,andC.L.Bris,"Estimationof2Dilluminantdirectionandshadowsegmentationinnatural video sequences," *Proceedings of VLBV*, pp. 197–202, 2001
[21]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.
[22]J.Fridrich, "Sensor defects in digital image forensic," in *Digital Image Forensics*, pp. 179–218, Springer, New York, NY, 2013.
[23]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.
[24]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.
[25] 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 ProcessingConference(EUSIPCO)*,pp.1777–1781.
[26]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
[27]M.Kumar,S.Srivastava,andN.Uddin,"Forgery detection using multiple light sources for synthetic images,"*Australian Journal of Forensic Sciences*, vol.51,no.3,pp.243–250,2019.
[28]J. Pine and H. Nicolas, "Estimation of 2D illuminant direction and shadow segmentation in natural video sequences," in *proceedings of VLBV*, p. 197, 2001.
[29]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.
[30]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
[31]M.KumarandS.Srivastava,"Image authentication by assessing manipulations using illumination, "*Multimedia Tools and Applications*, vol. 78, no. 9, pp. 12451–12463, 2019.
[32]B.Peng,W.Wang,J.Dong,andT.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.
[33]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